ManageEngine
PAM360

Help Guide

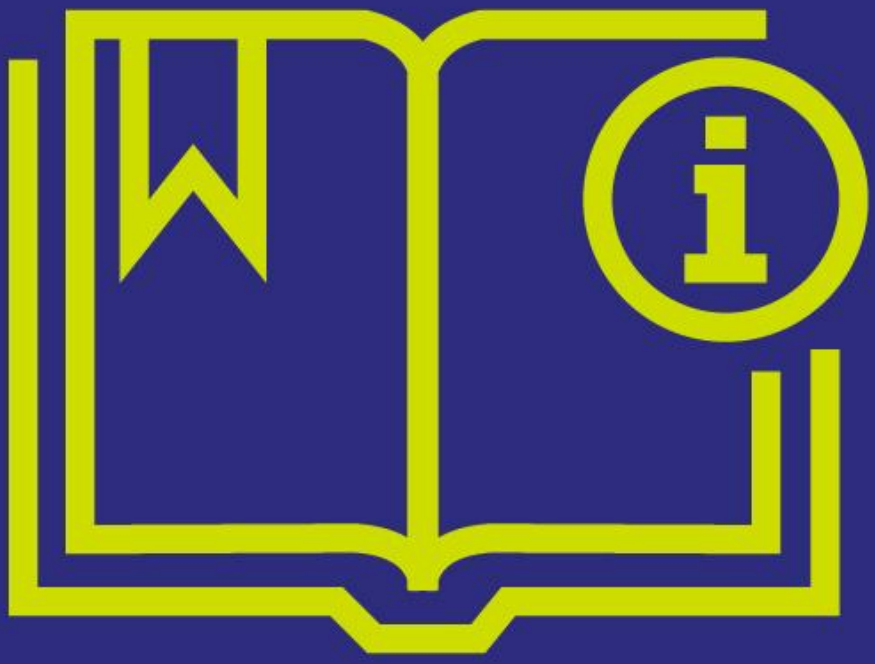


TABLE OF CONTENTS

ManageEngine PAM360 10
List Of Modules And Features In PAM360 13
Glossary Of Terms And Abbreviations 18
The Architecture Of PAM360 21
What Is In This Guide? 25
Setting Up PAM360 26
Basic Requirements 27
Installing PAM360 31
The Workflow In PAM360 36
Working With PAM360 Agent 38
Installing PAM360 Agent 40
PAM360 Agent-Based Operations 61
Getting Started With PAM360 69
Using MS SQL Server As The Backend Database 77
Using MS SQL Cluster As The Backend Database 86
Configuring PostgreSQL Cluster As The Backend Database 93
Using Azure MS SQL As The Backend Database 98
Configuring Amazon RDS MS SQL As The Backend Database 107
Configuring Amazon RDS PostgreSQL As The Backend Database 111
Managing The PAM360 Database Password 112
Migrating From PostgreSQL Database To MS SQL / Azure MS SQL Database 113
Migrating Data From Local MS SQL To Microsoft Azure SQL Database 118
Migrating Data From Local MS SQL To Amazon RDS MS SQL Database 126
Migrating Data From Local PostgreSQL To Amazon RDS PostgreSQL Database 129
Migrating Data From Local PostgreSQL Database To An External PostgreSQL Database 131
Managing User Roles And Permissions 134

Super Administrator In PAM360 144
Adding User Accounts In PAM360 150
Adding Users Manually Into PAM360 151
Adding Users Manually Into PAM360 154
Adding API User Accounts In PAM360 158
Adding API User Accounts In PAM360 162
Scim-Based User Provisioning In PAM360 166
Understanding PAM360 SCIM APIs 173
Import Users From A File 206
Importing Users From Active Directory 209
Importing Users From Microsoft Entra ID 216
Importing Users From LDAP 226
Managing PAM360 User Accounts 232
User Groups 239
Active Directory Synchronization Schedules 247
Importing Users From LDAP 255
Integrating Radius Server & Leveraging Radius Authentication 263
Smart Card / PKI / Certificate Authentication 265
Configuring Single Sign-On (SSO) Using SAML 2.0 For Okta 274
Configuring Saml Single Sign-On (SSO) For Azure AD Users 288
Configuring Single Sign-On (SSO) Using SAML 2.0 For ADFS 315
Configuring Saml Single Sign-On (SSO) Using G Suite 323
Configuring Saml Single Sign-On (SSO) For Active Directory Users 328
Setting Up Two-Factor Authentication (TFA) 331
Setting Up Two-Factor Authentication (TFA) - Phonefactor Authentication 336
Setting Up Two-Factor Authentication (TFA) With RSA SecurID 345
Setting Up Two-Factor Authentication (TFA) - Google Authenticator 350

Setting Up Two-Factor Authentication (TFA) - Microsoft Authenticator 354
Setting Up Two-Factor Authentication (TFA) – Oracle Authenticator 359
Setting Up Two-Factor Authentication (TFA) – Zoho OneAuth Authenticator 365
Setting Up Two-Factor Authentication (TFA) - Okta Verify.....372
Setting Up Two-Factor Authentication (TFA) - Radius Authenticator 377
Setting Up Two-Factor Authentication (TFA) - Duo Security 380
Setting Up Two-Factor Authentication - YubiKey 385
Two-Factor Authentication (TFA) - One-Time Password 391
Resources And Resource Groups..... 394
Discovering Resources And Privileged Accounts 403
Adding Resources Manually 440
Importing Resources.....451
Managing Resources..... 457
Exporting Passwords For Secure Offline Access 459
Managing Resources..... 466
Copying Resources..... 473
Transferring Resource Ownership At Different Levels 475
Sharing Individual Resources..... 482
Sharing Resources In Bulk 488
Managing Accounts And Passwords..... 495
Managing Resource Types 512
Password Action Notification..... 520
Password Reset Plugin..... 524
Password Reset Listener 532
Password Policies..... 539
Password Access Control Workflow 547
Password Reset.....572

Remote Password Reset 573
Password Reset Using The PAM360 Agent 603
Configuring Remote Password Reset For Resources In Bulk 605
Periodic Password Reset 607
Windows Service Account Password Reset 614
IIS AppPool Account Password Reset 620
Windows Scheduled Tasks Password Reset 631
Remote Password Reset Using SSH Command Sets 639
Self-Service Privilege Elevation In PAM360 654
Application Control Via PAM360 671
Managing Resource Groups 677
Nested Resource Groups 684
Export Resource Groups 691
Folders 695
Discovery Of IIS Web.Config And Password Reset 701
Connections And Privileged Sessions 709
Connection Actions And Configurations 711
Connection Settings For Accounts 723
SSH Command Control (Filtering) In PAM360 730
PAM360 Remote Connect 748
Configuring PAM360 Remote Connect 751
Privileged Session Recording 759
Gateway Settings 767
HTTPS Gateway Server 769
Working With Files In PAM360 779
Working With Remote Apps 787
Auto Logon Helper 790

Remote Connection To SSH-Based Devices Using SSH Keys 798
Remote File Transfer During Windows RDP Sessions 805
Configuring Landing Servers For Data Center Remote Access 809
Managing SSH Keys And Key Groups 813
Manage SSL Certificates 831
Integration With Trusted Public Certificate Authorities 878
Integrating PAM360 With Let's Encrypt SSL Certificate Authority 880
Integrating PAM360 With GoDaddy Ssl Certificate Authority 900
Integrating PAM360 With The SSL Store Certificate Authority 909
Integrating PAM360 With DigiCert SSL Certificate Authority 928
Integrating PAM360 With GlobalSign SSL Certificate Authority 935
Integration With Buypass Go SSL 950
Integration With ZeroSSL 964
Integration With AWS-ACM Certificate Manager 979
Integration With Azure Key Vault 988
Integration With Sectigo Certificate Manager 997
Manage Certificates Using Microsoft Certificate Authority (MSCA) 1004
Integration With ManageEngine Mobile Device Manager Plus (MDM) 1010
Share SSL Certificates With Users 1017
Deploy SSL Certificates To Target Web Servers 1024
SSL Vulnerability 1055
SSH And SSL Audit And Reports 1063
SSH/SSL Admin Settings 1072
Manage SSH/SSL Schedules 1078
Ticketing System Integration For SSL Certificates 1084
Integration With ServiceDesk Plus' CMDB 1090
Manage PGP Keys 1095

Additional Fields For SSH Keys And SSL Certificates 1100
SSL Agent 1106
Working With Multiple Servers 1114
Certificate Tools 1121
High Availability And Disaster Recovery Options 1125
High Availability With PostgreSQL Database 1126
High Availability For Microsoft SQL Server 1129
High Availability For MS SQL With Replication Using SQL Server Management Studio 1137
Steps To Remove High Availability (MS SQL Server As Backend Database) 1167
Monitor High Availability Using PAM360 1170
Read-Only Server With PostgreSQL Database 1178
Failover Service For PAM360 (MS-SQL Server Clusters) 1185
Database Backup (PostgreSQL) 1190
Database Backup (MS SQL Server) 1192
Data Restore 1194
Application Scaling In PAM360 Using Microsoft SQL Server 1203
Application Scaling In PAM360 Using PostgreSQL Server 1209
Security Hardening Dashboard 1216
Rebranding PAM360 1223
Displaying Messages To PAM360 Users 1227
Managing General Settings 1229
Mail Server Settings 1244
Privacy Settings 1254
SNMP Traps 1257
Remote Host 1259
IP Restrictions 1262
Email Templates 1265

Additional Fields 1268
Managing Schedules..... 1273
Storing Personal Passwords In PAM360 1278
Changing PAM360 Login Password 1290
Advanced Analytics 1292
Integrating PAM360 With Enterprise Ticketing Systems 1299
Secure Cloud Storage Options For Anytime, Anywhere Access To Passwords 1327
PAM360 Plugins For CI/CD Platforms 1338
PAM360 Plugins For Jenkins 1339
PAM360 Plugin For Ansible 1344
PAM360 Plugins For Chef And Puppet 1347
Integrating PAM360 With Other ManageEngine Products..... 1354
Integrating PAM360 With ManageEngine ServiceDesk Plus..... 1356
Integrating PAM360 With ManageEngine ServiceDesk Plus Cloud 1361
Integrating PAM360 With ManageEngine ADSelfService Plus (ADSSP) 1368
Integrating PAM360 With ManageEngine Analytics Plus 1374
Integrating PAM360 With ManageEngine ADManager Plus 1379
Integrating PAM360 With ManageEngine Eventlog Analyzer 1385
Integrating PAM360 With ManageEngine Log360 UEBA 1391
Integrating PAM360 With Robotic Process Automation Tools 1397
Integrating PAM360 Automation Anywhere..... 1399
Integrating PAM360 With Cortex XSOAR 1409
Integrating PAM360 With Kubernetes.....1419
Integrating ManageEngine PAM360 With SIEM Tools.....1431
Integrating PAM360 With Microsoft Sentinel..... 1437
Integrating PAM360 With Vulnerability Scanner 1444
Integrating With SafeNet Luna PCIe Hardware Security Module (HSM).....1450

Integration With The Entrust nShield Hardware Security Module (HSM) 1453
How To Use Custom Cryptography (Encryption And Decryption) In PAM360 1462
Software Development Kit For DevSecOps - Java 1471
Software Development Kit For DevSecOps - Python 1476
Implementing Zero Trust Approach Via PAM360 1481
Configuring Trust Score Parameters For Zero Trust Approach 1497
Access Policy Configuration For Zero Trust Approach 1512
Practical Implementation Scenario And Use Cases 1521
PAM360 Integration With Zoho Flow 1538
Working With Zoho Flow Agent 1539
Integrating PAM360 With Zoho Flow 1545
How PAM360 Integration With Zoho Flow Aids In Real-Time? 1550
Configuring Different APIs 1559
RESTful API 1569
Reports 1687
Query Reports 1711
Audit And Notifications 1725
PAM360 Mobile Application - Android 1736
PAM360 Mobile Application - Ios 1767
Chrome Browser Extension 1796
Firefox Browser Extension 1807
Edge Browser Extension 1816
PAM360 User Account Settings 1826
PAM360 - Frequently Asked Questions 1831
PAM360 MSP Edition - Getting Started 1878

ManageEngine PAM360

Comprehensive Privileged Access Management Solution

1. Privileged Access Management - The Definition

Privileged access management (PAM), a subdivision of Identity and Access Management (IAM), is a solution that provides organizations with better control and monitoring capabilities that decide who can have privileged access to critical assets, say, a computer or information system.

The solution should include the following functionalities:

- Defining user roles
- Granting required privileges or access rights for the roles defined
- Distributing user information and access grants to all devices and systems that enforce access rights in organizations
- Monitoring privileged user activities and analyzing the same to detect anomalies

2. The Goal

The primary goal of any PAM solution is to primarily lock the credentials of privileged accounts, i.e., the admin accounts, inside a secure vault, thus confining the use of those accounts, thereby reducing the risk of those credentials getting robbed. Administrators can access the credentials inside the vault only via the PAM system, provided they are well authorized and their access is logged in. Once a credential is checked back in, it is reset, and for subsequent access, the administrators have to use the PAM system again.

On the whole, the PAM system unites all privileged credentials at a single point. This results in a high level of security, gives good control of who is accessing what, and logs all accesses, and monitors for suspicious activities.

3. The Challenges in Privileged Access Management

In this modern age of IT revolution, infrastructure setups are comprised of an ever-growing mix of critical assets spanning across physical, virtual, and cloud platforms. Apart from that, every enterprise also runs numerous business applications that deal with sensitive intellectual property and strategic information.

But, cyber risks grow along with businesses and there will be constant attempts to gain access to sensitive IT resources in enterprises by compromising privileged accounts. Once an attacker manages to acquire a privileged account credential, breaking in to the enterprise's IT network becomes a child's play. To thwart such threats and stay in control, we need to put

tighter locks on privileged accounts and also keep a round-the-clock check on privileged access by employees and third parties likewise.

So, proper management of privileged accounts ultimately lies in protecting the administrative passwords of those accounts. However, in large organizations with extensive infrastructure, it is a tedious task to keep track of all administrative passwords. Also, users tend to store user names and passwords locally in their systems, or some central location when multiple administrators need to use the information.

4. Why PAM360?

The best way to overcome the above challenges is to use a secure privileged access management solution that guides enterprises in establishing strict control and direction over administrative access and permissions for users, systems, and applications across their IT infrastructure. So, we have come up with PAM360, a complete privileged access management software that uses a set of policies to secure, control, and monitor privileged activities and sessions on critical enterprise systems without compromising the business productivity. PAM360 encompasses the following capabilities into a single platform:

1. Credential Vaulting
2. Privileged Account Governance
3. Remote Access Management
4. Remote Session Management
5. Privileged User Monitoring
6. Threat Analytics
7. Comprehensive Reporting
8. Audit and Compliance
9. Web-based SSH Key and SSL Certificate Management Solution

5. PAM360 - The 360 Degree Approach to Securing Privileged Access

ManageEngine PAM360 is a complete solution to control, manage, and audit the entire life cycle of privileged accounts and their access. It fully encrypts and consolidates all your privileged accounts in one centralized vault, reinforced with granular access controls. It also mitigates security risks related to privileged access and pre-empts security breaches and compliance issues.

Using PAM360, IT administrators can centrally create users, assign them with specific roles and define access levels. Only authorized users will get access to view, edit or manage the permitted 'resources' (the resources assigned to them) based on their role. Moreover, the

comprehensive auditing mechanism of PAM360 helps in tracking who accessed what and when, thereby ensuring accountability in a multi-member environment.

6. Unique Capabilities of PAM360

- A highly secure and easy-to-use PAM solution for IT administrators that enables admins to create accounts, grant and revoke access, and handle urgent situations, like user account, lockout as quickly and as easily as possible.
- Allows easy discovery of privileged accounts on systems, devices, and applications for effective control and management.
- Establishes transparency and control of all privileged access to critical data.
- Provides secured access to your Active Directory environment and other endpoints such as Linux/Unix and Windows.
- Provides strong access controls that restrict access to critical systems by demanding approvals from administrators and automatically check-in and reset the access credentials after the stipulated period.
- Provides role-based access, i.e., it has a built-in user and role management system that provides each user with the required level of access for the required time frame, thus providing the ability to configure access with utmost granularity.
- Provides uninterrupted access to passwords in mission-critical environments, thus offering more uptime and High Availability.
- Provides an effective point of control and management for audit and compliance, thereby ensuring that the required security controls are in place.

7. Password Management in PAM360

Ensuring the secure storage of passwords and offering high defence against intrusion are the mandatory requirements for privileged account security. The following measures in PAM360 provide the required security levels:

- Establish and enforce strict password policies, such as rotating the passwords regularly so that users do not use default passwords, changing the privileged account passwords regularly to lessen the risk of any old employees compromising the systems, and securing privileged accounts with Two-Factor Authentication.
- Ability to scan networks and discover critical assets to automatically on-board privileged accounts into a secure vault that offers central management, AES-256 encryption, and role-based access permissions. AES functions have been adopted and also recommended as an encryption standard by the U.S. Government.
- Role-based, fine-grained user authentication mechanism ensures that the users are allowed to view the passwords based on only the authorization provided.
- All transactions through the PAM360's browser take place through HTTPS.

List of Modules and Features in PAM360

The following table presents the list of all features grouped under different modules that altogether demonstrate the working strategy of PAM360:

Module	Feature	Description
User Management	AD / LDAP support /Azure AD Smart Card Authentication	Integration with an external directory server for user management and authentication. If you have a smart card authentication system in your environment, you can configure PAM360 to authenticate users with their smart cards, bypassing other first factor authentication methods like AD, LDAP or Local Authentication.
	User Roles	Five different user roles providing fine-grained access control.
	Custom Roles	In addition to the pre-defined roles in PAM360, the administrator can also create custom roles for your users. The role customization option allows you to create new role from scratch, by selecting the desired options from the list of 100+ operations available in PAM360.
	Super Administrator	Enabling an administrator to see all the resources in the system unconditionally.
	User Groups	Create groups of users for carrying out operations in bulk.
	Domain Single Sign On	Pass through authentication for PAM360 server, when integrated with AD.
	Single Sign on using SAML	PAM360 offers support for SAML 2.0, which facilitates integration with Federated Identity Management Solutions for Single Sign-On.
Resource Management	Resource types	Categorize resources based on their types (for e.g. Windows Servers). Create and manage your own resource types, in addition to the default types.
	Resource Groups	Create groups of resources / passwords and manage the groups. Carry out password management operations in bulk.

Module	Feature	Description
	Nested Resource Groups	Maintain resource groups in hierarchical structure (groups, sub-groups) for navigational convenience.
	Share Resources/Groups	Share resources /resource groups with desired users/user groups.
	Exporting Resources	PAM360 provides multiple export options for secure offline access and safekeeping of password information. The basic option is to export password in plain text. The more secure option is to export the passwords to an encrypted HTML file.
	PAM360 Agents	The agents periodically check for tasks by opening a secure connection with the server and no longer need to have a port open in the system they are installed.
Password Management	Resource Customization	Add attributes to resources and accounts according to your needs.
	Password Access Control Workflow	Helps enforce enhanced access control in the product. The user, who requires a password, will have to 'request the release' and one or more administrators will authorize the request. The password availability to the user is time limited. It will be automatically reset thereafter and the user will thereby forfeit the access.
	Password Policies	Create and manage your own password policies for enforcing their adoption through PAM360.
	Password Resets	Perform password resets to resources from PAM360 (Windows, Windows Domain, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQL server, Oracle DB Server, Sybase ASE, HP ProCurve and Cisco Devices (IOS, CatOS, PIX)).
	Password Reset Schedules	Automate password resets
	Password Actions / Notifications	Generate alerts for various password events and specify action to be taken on password events.
	Password Reset Listener	Invoke a custom script to initiate desired action on password changes.

Module	Feature	Description
	Windows Service Account Management	Keep your windows service account and scheduled task passwords synchronized with the corresponding domain account.
	IIS App Pool Account Password Reset	Support for automatically resetting the passwords of associated IIS AppPool accounts when the domain account passwords are reset through PAM360.
	Auto Logon Helper	Connect to target systems with a single click from PAM360 console without having to actually see the passwords.
	Password Management API	Setup your applications to query PAM360 for A-to-A and A-to-DB passwords.
	Remote Access Management & Privileged Session Recording	Privileged sessions launched from PAM360 can be recorded, archived and played back to support forensic audits and allow enterprises to monitor all actions performed by privileged accounts during privileged sessions.
	Ticketing System Integration	PAM360 provides the option to integrate a range of ticketing systems to automatically validate service requests related to privileged access.
	Privileged Accounts Discovery	PAM360 provides the option to automatically discover the IT assets in your environment and enumerate the privileged accounts associated with them, thus helping enterprises to secure all their privileged identities in quick time.
Audit and Reports	Audit	Comprehensive audit of all operations done on resources, passwords and users. Export to pdf and email.
	Audit Filters	Create Filters to view only those audit records that are of interest.
	Audit Notification	Choose to send/receive notification as e-mail / SNMP trap / Syslog on the occurrence of desired audit events.
	Canned Reports, Custom Reports	Intuitive reports on password inventory, compliance, expiry, resource and user activity. Print reports, export to pdf and email.

Module	Feature	Description
		Provision for generating various custom reports to suit specific business requirements.
	Query Reports	This new addition to the Reports section now allows administrators to construct reports by writing their own SQL statements. The statements can be used to directly query the PAM360 database and fetch required information to address unique reporting requirements.
	Dashboard	Password and user dashboard providing a snapshot on password management activities.
Non-functional Features	Two-Factor Authentication	Enforcing users to identify themselves with two unique factors before they are granted access to the web-interface.
	Backup for Disaster Recovery	Setup backup of the PAM360 database for disaster recovery purposes.
	High Availability	setup redundant PAM360 servers to provide high availability of PAM360 application.
	Failover Service	The Failover Service in PAM360 is also aimed at ensuring uninterrupted access to passwords and other privileged resources.
	Customize Email Notification Content	By default, PAM360 has a specific content for the email notification for various password actions. If you want, you can customize the content and have your own content.
	Re-brand	Use your own logo in the PAM360 user interface.
	General Settings	Switch on and off various features on need basis.
	Manage Encryption Key	Option to quickly change the location of the master encryption key and store it outside of the machine in which PAM360 is installed, in another machine, or an external drive.
	Manage Schedules	Option to quickly view and edit all the schedules created in the product single, centralized page.
	RESTful API	RESTful APIs, help you to connect, interact and integrate any application with PAM360 directly.
	Browser extension	Seamlessly auto-logon to websites and applications, launch RDP and SSH sessions, access existing

Module	Feature	Description
		passwords, and add new ones - all from PAM360's extensions for Chrome and Firefox browsers, without leaving the browser tab you're in.

Glossary of Terms and Abbreviations

While working with PAM360, you will come across some terminologies having unique meanings. It is worthwhile to take a note of those terminologies before proceeding further:

1. Glossary of Terms

Term	Description
Resource	Denotes the server/application/device whose user accounts and passwords are to be managed by PAM360.
Resource Group	Denotes the group to which a particular resource belongs. For example, if you have some Windows XP servers among a number of other windows servers, you can group all the XP servers as one resource group.
User Account	Denotes the 'User Account' & 'Password' that are to be managed by PAM360.
User	Denotes the PAM360 user accounts created as part of PAM360 User Management.
User Group	Group of PAM360 Users.
Agent	PAM360 utilizes an agent for establishing connections with remote resources.
Password Policy	Refer to this section.
Audit	PAM360 maintains the complete record of every single action performed by the users within the application by using a timestamp and IP address. Three types of audit are performed, Resource Audit, User Audit, and Task Audit.
Reports	PAM360 presents the entire password management process in your enterprise in the form of comprehensive reports.
ZRLE	ZRLE stands for Zlib Run-Length Encoding. It is considered to be best for low-bandwidth network environments.
Raw	The raw encoding sends width*height pixel values. Raw encoding minimizes processing time and increases connection speed when the server and VNC viewer are on the same machine.
Tight	Tight encoding is considered to be the best choice for low-bandwidth network environments such as e.g. slow modem connections. Tight encoding uses zlib library to compress raw pixel

	data, but it pre-processes data to maximize compression ratios and to minimize CPU usage on compression. JPEG compression may be used to encode color-rich screen areas.
Hextile	Hextile encoding is considered to be the best choice for high-speed network environments such as Ethernet local-area networks.
CopyRect	Copy Rectangle or CopyRect encoding is useful when data is being moved; the only data sent is the location of a rectangle from which data is to be copied to the current location.
Request	The user has to make a request to view the password.
Waiting for Approval	User's password release request is pending with administrator(s) for approval.
Check Out	Administrator has approved the request and the user can view the password.
Approve/Reject	Administrator can either approve or reject the password request.
Yet to Use	Indicates that the user is yet to view the password released by the administrator.
In Use	Password is being used exclusively by a user.
Check In	Giving up/revoking password access.

2. Abbreviations

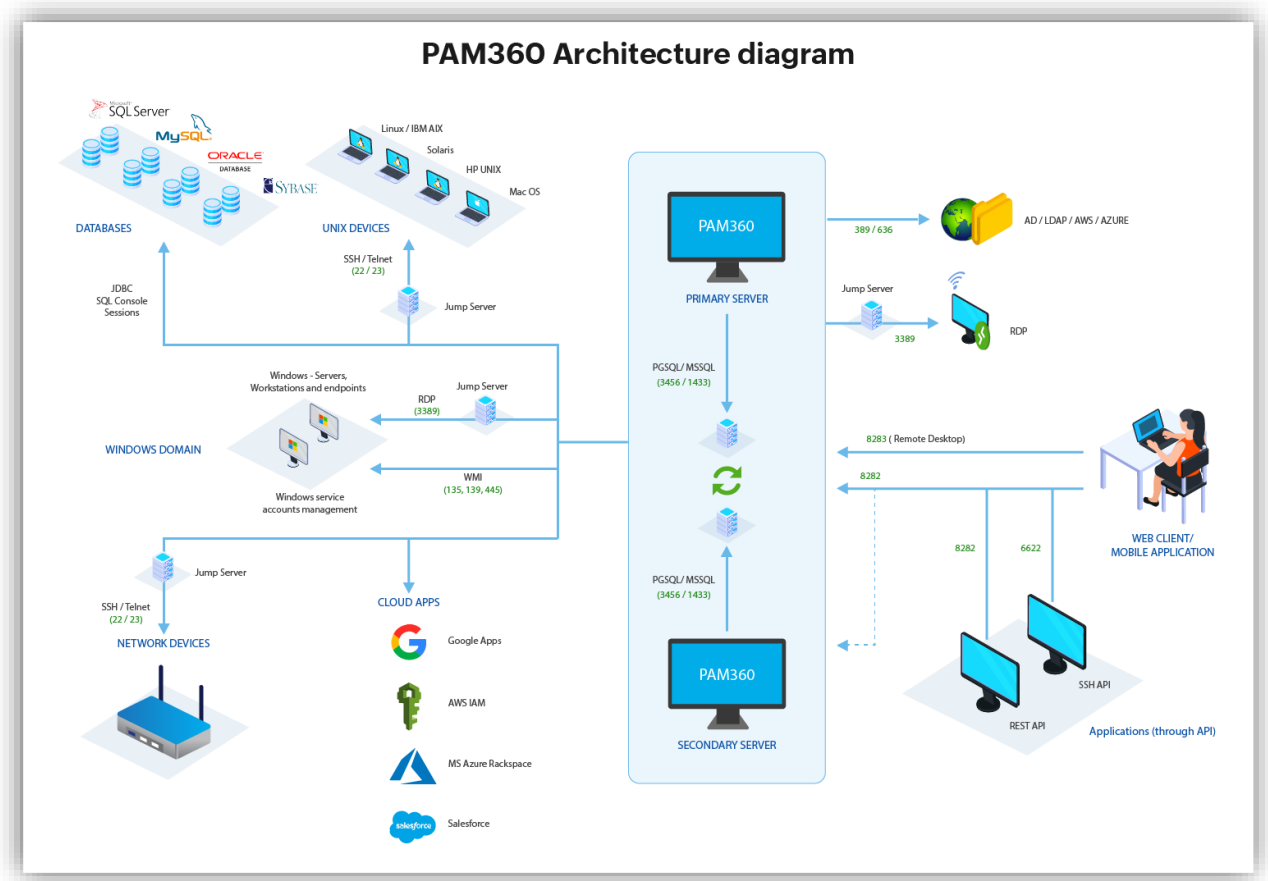
Abbreviation	Expansion
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
RADIUS	Remote Authentication Dial-In User Service
SSO	Single Sign-On
SAML	Security Assertion Markup Language
TFA	Two Factor Authentication
MFA	Multi-Factor Authentication
ADFS	Active Directory Federation Services
RSA	Rivest-Shamir-Adleman
SSH	Secure Shell

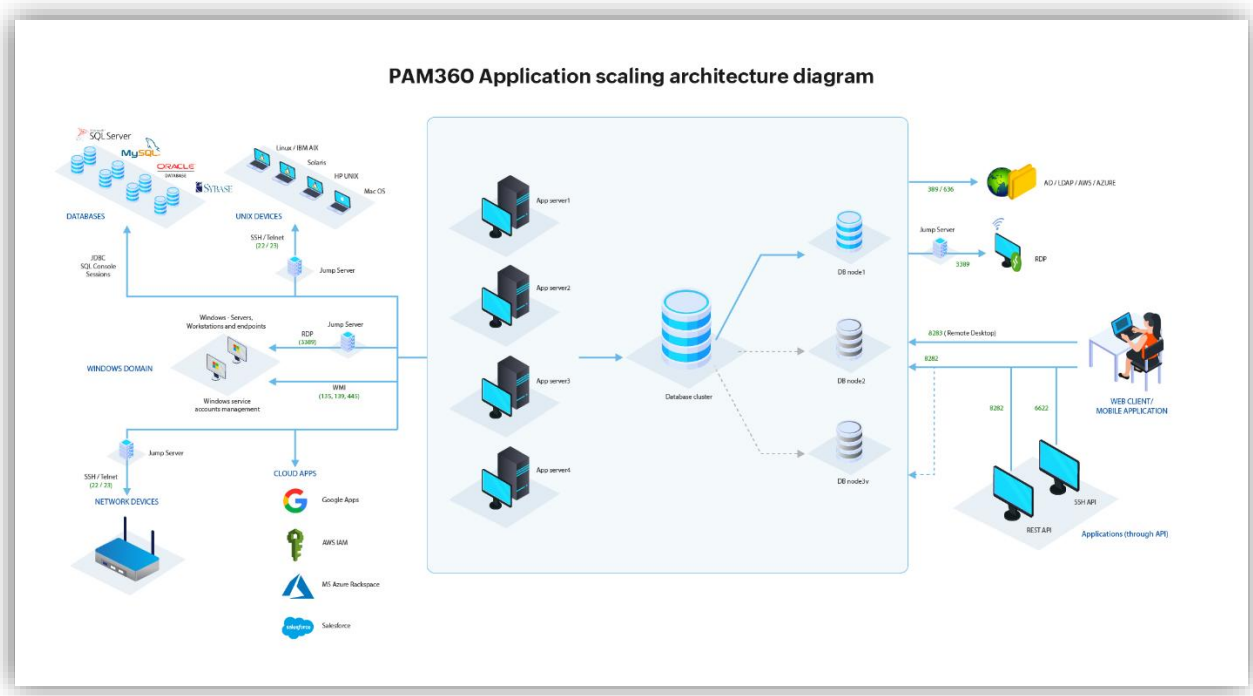
SSL	Secure Socket Layer
CLI	Computing Command-line Interface
CI/CD	Continuous integration and Continuous Delivery
DevOps	Development and Operations
IIS	Internet Information Server
FQDN	Fully Qualified Domain Name
HA	High Availability
CA	Certificate Authority
RDP	Remote Desktop Protocol
HSM	Hardware Security Module
PCIe	Peripheral Component Interconnect Express
PKI	Public Key Infrastructure

The Architecture of PAM360

Now that you have finished learning the basic concepts of PAM360, you may now proceed to get to know how exactly PAM360 works, its overall architecture, and the process flow. This document provides a comprehensive architectural overview of the PAM360 system by focusing on different key quality attributes.

The below diagram thoroughly illustrates the complete functional architecture of PAM360.





The above illustration depicts the different components of PAM360 and how they interact with each other. Read further to know more about each component and their functionalities in detail.

1. Different Components in PAM360

PAM360 comprises of multiple components that work in hand with each other to protect your enterprise passwords and strengthen security in your environment. Read further to know more about each component in details. To know more about the list of modules and features in PAM360, click here.

1.1 Web Servers

PAM360 can be installed in any **Windows** and **Unix** based machines as a web application. These systems can be configured based on the users' requirements. PAM360 is accessible via both **Web Clients** and **Mobile Application**s.

PAM360 offers three disaster recovery options to web servers:

1. High Availability
2. Failover Service
3. Application Scaling

1.2 User Import

A user is an individual who has a user account that has access to the application through a computer or mobile using a network service. Users are identified to the system by the user's id or user's name.

In PAM360, you will be able to import users using Active Directory, Azure AD, and LDAP. You can also add users manually, API users or import users using a file. The added users can be assigned with appropriate access roles and password policies. You can also add new user roles with different set of permissions tailored to your needs.

1.3 Supported Databases

PAM360 supports PostgreSQL, MS SQL, Amazon RDS MS SQL, Amazon RDS PgSQL, and MS Azure SQL. By default, PAM360 comes bundled with PostgreSQL. PAM360 allows you to migrate from one database to another as per your convenience.

1.4 Resource Types

Resources in PAM360 refer to any server, application, network device, or appliance in your environment that has authentication credentials that need to be secured. PAM360 supports various database types, Unix devices, Windows Domains, Cloud apps, and network devices. PAM360 allows you to discover a variety of devices such as Windows, Linux, VMware and Network devices.

1.5 Supported API's

In PAM360, users are allowed to choose between the two API types which are SSH CLI, and RESTful API. Users can configure and use PAM360 API's for application to application password management.

2. Process Flow

Right until now you have read about the different components of PAM360. In this section, you will learn in detail how these components work and interact with each other to provide a seamless experience.

PAM360 is an on-premise, self-hosted solution available as a binary for installation on Windows & Linux, which can be configured accordingly based on the user's requirements.

1. After installing PAM360, users can access the PAM360 web application through the port 8282 or using the mobile application. Ports play an essential role in PAM360 for remote access. Click here to know about the different ports used by PAM360.
2. Also, refer to this document to know more about the initial stages of setting up PAM360 in your environment.
3. Now, use the port 3456 to access PostgreSQL or port 1433 to access MS SQL database.
4. After setting up the database, administrators can now import users and resources into PAM360 using AD or LDAP using ports 389 and 636 respectively.
5. In PAM360, users are allowed to choose between the two API types which are SSH CLI,

and RESTful API. Use the port 5522, to establish a SSH CLI connection.

6. PAM360 allows you to establish a secure connection to any windows resources via landing servers.
    i. After associating the resources to the landing server, PAM360 allows you to launch direct connections to the target systems.
    ii. Likely, for connections, respective ports should be opened.
    iii. PAM360 establishes direct connection (using TELNET, SSH or RDP) to the data center. Use the ports 22 and 23 to connect using TELNET and SSH respectively.
    iv. A native port 3389 must be used to establish a successful RDP connection between PAM360 and your target system.
    v. When the connection is established PAM360 allows users to transfer files to and from the connected machine using the PAM360 session gateway.
7. You can also use PAM360 to replace your VPN systems, as the product offers Gateway-based RDP, SSH, and SQL connection features bundled with session recording.

What is in this Guide?

ManageEngine PAM360 is a secure solution that allows you to store, control, authenticate, record, audit, and analyse privileged access and activities in a business IT environment. The solution thrives to achieve the designated PAM goals through different modules, each designed to accomplish a specific task and work together under a central console.

This help guide will help you understand the concepts of each module and its complete configurations. Click the below links to go to the respective help pages and learn about the configurations in detail.

- Effective User Management
- Authentication
- Resources and Resource Groups
- Password Access Control
- Privileged Session Monitoring
- Remote App Support
- SSL Certificate Management
- SSH Keys & Certificates
- Ticketing System Integration
- Disaster Recovery
- Centralized Control
- Comprehensive Reporting
- Audit and Compliance

Setting up PAM360

To set up PAM360 to work in your environment, follow the below steps sequentially:

1. Download the product
2. Check the installation requirements
3. Verify if the prerequisites are met
4. Install the product
5. Run the product

Once you have downloaded PAM360, refer to the help section Basic Requirements to know about different system requirements, prerequisites, license information, etc.

After installing PAM360, refer to the 'Get Started' tab for steps to connect to the PAM360 web portal to start working with the solution. The 'Get Started' tab also has links to documents explaining the database migration procedure, Database Management, etc. The rest of the other tabs provide information on different modules of PAM360 used to carry out various privilege management activities.

Basic Requirements

Before installing a product or application in your environment, first, you have to verify if certain requirements are satisfied. This document explains in detail the prerequisites, system requirements, components, ports, other and conditions that are essential for PAM360 to function in your environment. You will also know about the supported operating systems and the recommended hardware requirements for the different types of deployments of the PAM360 installation.

Make sure that your system environment meets all the below requirements, and then begin the installation.

1. Prerequisites
2. System Requirements
3. Components of PAM360
4. Ports used by PAM360
5. Licensing and User Roles
   5.1. License Types
   5.2. User Roles

1. Prerequisites

Apart from the standard system requirements (both hardware and software), the following elements are essential for the proper functioning of the PAM360 server:

> **Note**: The following are required, if you're planning to make use of PAM360's account discovery and password reset provisions.

1. An external mail server **(SMTP server)** for the functioning of PAM360 server and to send various notifications to users.
2. A service account that has either domain admin rights or local admin rights in the PAM360 server and in the target systems that you would like to manage.
3. Microsoft **.NET framework.**
4. **Visual C++ Redistributable for Visual Studio 2015 and above** (for PAM360's Account Discovery and Password Reset features).

2. System Requirements

The below table provides an overview of the hardware and software configurations required by PAM360:

Hardware	Operating systems	Web interface
Processor • Dual Core/Core2Duo or above **RAM** • 4 GB or above **Hard Disk** • 200 MB or more for the product • 10 GB or more for the database **Note:** For Session Recordings, the disk space requirement may vary based on the usage levels.	**Windows** Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 Windows Server 2012 R2 Windows 8 Windows 10 **Linux** • Ubuntu 9.x and above • CentOS 4.4 and above • Red Hat Linux 9.0 • Red Hat Enterprise Linux 7.x • Red Hat Enterprise Linux 6.x • Red Hat Enterprise Linux 5.x **Note:** In general, PAM360 works well with any flavor of Linux and can also be run on VMs of the above operating systems.	HTML client requires one of the following browsers** to be installed in the system: Microsoft Edge (on Windows) Chrome, Firefox, and Safari (on Windows, Linux and Mac) ** PAM360 is optimized for 1280 x 800 resolution and above. **Database** PostgreSQL 10.18, bundled with the product. Supports MS SQL Server 2008 and above. SQL server should be installed in Windows 2008 Server and above.

3. Components of PAM360

PAM360 comprises of the following components:

1. The **PAM360 server**
2. The **PAM360 Agent** (optional)**:**

   - for establishing connections with the remote resources.

3. The database **PostgreSQL 10.18:**

   - bundled with PAM360 that runs as a separate process.

   - accepts connections only from the host where it is running.

4. Ports used by PAM360

The below table lists the set of all ports used by PAM360 for remote access:

Port Name	Port Number	Direction
PostgreSQL port	3456	Outbound
Web client port	8282	Inbound
SSH port	22	Outbound
Telnet port	23	Outbound
LDAP without SSL port	389	Outbound
LDAP with SSL port	636	Outbound
SMTP port	25	Outbound
MS SQL port	1433	Outbound
Oracle port	1521	Outbound
Sybase ASE port	5000	Outbound
Password Verification port	135, 139, 445	Outbound
SSH API	6622	Inbound
Auto Logon Spark View Gateway port	8283	Inbound
RDP	3389	Outbound
REST API	8282	Inbound

5. Licensing and User Roles

5.1 License Types

There are three license types:

1. **Evaluation download / Trial Version:** You can straightaway download and install this trial version. It is fully functional, capable of supporting a maximum of **5 administrators** and you can evaluate all the features for 30 days.
2. **Free Edition:** Licensed software that allows you to have **1 administrator** and manage up to **10 resources**. Valid forever.
3. **Registered Version:** You get the Enterprise edition, and Licensing is based on the Number of Administrators. This is useful if you require more enterprise-class features such as auto discovery of privileged accounts, integration with ticketing systems and SIEM solutions, jump server configuration, application-to-application password management, out-of-the-box compliance reports, SQL server / cluster as backend database, etc.

5.2 User Roles

PAM360 comes with six user roles:

1. Privileged Administrator
2. Administrator
3. Password Administrator
4. Password Auditor
5. Password User
6. Connection User

The term **administrator** denotes Administrators, Password Administrators and Privileged Administrators. So, licensing restricts the number of administrators as a whole, which includes Administrators, Password Administrators and Privileged Administrators. There is no restriction on the number of Password Users and Password Auditors. To get more details on the user roles, click here.

Installing PAM360

Install PAM360 by following any of the following installation procedures that best suit your needs. Before commencing the installation on your operating system, ensure if all the prerequisites are satisfied. To learn more about each component and its capabilities, check the basic requirements section.

In this document, you will learn the step-by-step procedures to install PAM360 in different operating systems in your environment. You may either click each of the below links to jump to the respective sections in this document or scroll down to read further.

1. Installing PAM360
   1.1 In Windows
   1.2 In Windows Core Server 2019
   1.3 In Linux
2. Silent Install
3. Transferring PAM360 Installation

1. Installing PAM360

You can install PAM360 in both Windows and Linux operating systems.

1.1 Steps to Install PAM360 in Windows

1. Download and execute the file **ManageEngine_PAM360.exe**. The PAM360 installation wizard shows up.
2. Follow the step-by-step instructions in the installation wizard.
3. Choose an installation directory. By default, PAM360 will be installed in the path **"C:\Program Files\ManageEngine\PAM360".** Henceforth, this installation directory shall be referred to as **PAM360_Home**.
4. In the final wizard, you will have the following options:
   i. Option to view the **ReadMe** file.
   ii. Option to choose to start the server immediately.
   iii. Option to start the server later after installation. Use the Windows tray icon to start the server manually later. Using the tray icon, you can also perform other actions such as stopping the server and uninstalling the product.

1.2 Steps to Install PAM360 in Windows Core Server 2019

1. Execute the command "**powershell**" to open Microsoft Powershell.

2. Execute the following command to download the build:

   start-bitstransfer -source <full URL of the executable> -destination <full path to which you would like the executable to be downloaded>

   Example: *start-bitstransfer -source https://www.manageengine.com/privileged-access-management/6167/ManageEngine_PAM360_64bit.exe -destination C:|Users|Administrator*

3. Execute the following command to download the silent installation file:

   start-bitstransfer -source <full URL of the executable> -destination <full path to which you would like the executable to be downloaded>

   Example: *start-bitstransfer -source https://www.manageengine.com/privileged-access-management/help/WindowsPrimaryNonMSP.zip -destination C:|Users|Administrator*

4. Execute the following command to extract the silent installation file:

   Expand-Archive -LiteralPath <full path of the executable file> -DestinationPath<full path to which you would like the file to be extracted>

   Example: *Expand-Archive -LiteralPath C:|Users|Administrator|WindowsPrimaryNonMSP.zip -DestinationPathC:|Users|Administrator|WindowsPrimaryNonMSP*

5. Execute the following commands to install the Nano Text editor:

   - **Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))**
   - **choco install nano**

6. Execute the following command to edit the extracted file, **WindowsPrimaryNonMSP.iss:**

   nano WindowsPrimaryNonMSP.iss

7. Now, edit the **Name, MailId** (mandatory), **Phone, Company, Country** (mandatory), and **Save** the file.

8. Next, execute the following command:

   ManageEngine_PAM360_64bit.exe -a -s -f1"C:\Windows\WindowsPrimaryNonMSP.iss" -f2"C:\Windows\WindowsPrimaryNonMSP.log"

PAM360 has been installed successfully. The service will start automatically.

1.3 Steps to Install PAM360 in Linux(non-root)

1. Download the file **ManageEngine_PAM360.bin** for linux.
2. Execute the command **chmod a+x <file-name>** to assign the executable permission.

3. Execute the command: **./<file_name>** or **./<file_name> -i console** (if you are installing on a headless server).
4. Follow the step-by-step instructions as they appear on the screen. Now, PAM360 will be installed in your machine in the location chosen. Henceforth, this installation directory shall be referred to as **PAM360_Home**.

2. Silent Install

A silent install is used to install an application without the need to interact with the UI. This type of installation is helpful for applications with limited installation steps. Before commencing the silent install, certain parameters such as Name, EmailId, Path, etc., are automatically set or manually entered. Execute the commands as instructed below to install the application automatically.

1. **Steps to Silent Install PAM360 in Windows Server**

   1.1 Primary Server

   1.2 Secondary Server

2. **Steps to Uninstall PAM360 in Windows Server**
3. **Steps to Silent Install PAM360 in Linux Server**

   3.1 Primary Server

   3.2 Secondary Server

1. Steps to Silent Install PAM360 in Windows Server

1.1 Primary Server

1. Download the file ManageEngine_PAM360_64.bit.exe.
2. Download the installation file WindowsPrimaryNonMSP.iss.
3. Open **WindowsPrimaryNonMSP.iss** file in Notepad and edit **Name, MailId, Phone, Company, Country,** and save.
4. Move **WindowsPrimaryNonMSP.iss** file to **C:\Windows**.
5. Open Command Prompt as an administrator and navigate to the **ManageEngine_PAM360_64.bit.exe** file location.
6. Execute the command:

   ManageEngine_PAM360_64bit.exe -a -s -f1"C:\Windows\WindowsPrimaryNonMSP.iss" -f2"C:\Windows\WindowsPrimaryNonMSP.log"

PAM360 will get installed, and the service will start automatically.

1.2 Secondary Server

1. Download the file ManageEngine_PAM360_64.bit.exe.
2. Download the installation file WindowsSecondaryNonMSP.iss.
3. Open **WindowsSecondaryNonMSP.iss** file in notepad and edit **Name, MailId, Phone, Company, Country,** and save.
4. Move **WindowsSecondaryNonMSP.iss** file to **C:\Windows\.**
5. Open Command Prompt as administrator and navigate to the **ManageEngine_PAM360_64.bit.exe** file location.
6. Execute the command:

   ManageEngine_PAM360_64bit.exe -a -s -f1"C:\Windows\WindowsSecondaryNonMSP.iss" -f2"C:\Windows\WindowsSecondaryNonMSP.log"

PAM360 will get installed, and the service will start automatically.

2. Steps to Uninstall PAM360 in Windows Server

1. Download the uninstallation file WindowsUninstallNonMSP.iss.
2. Move **WindowsUninstallNonMSP.iss** file to **C:\Windows\.**
3. Open Command Prompt as administrator and navigate to the **ManageEngine_PAM360_64.bit.exe** file location.
4. Execute the command:

   ManageEngine_PAM360_64bit.exe -a -s -f1"C:\Windows\WindowsUninstallNonMSP.iss" -f2"C:\Windows\WindowsUninstallNonMSP.log"

PAM360 will get uninstalled.

3. Steps to Silent Install PAM360 in Linux Server

3.1 Primary Server

1. Download the file ManageEngine_PAM360_64.bit.bin for Linux.
2. Download the installation file LinuxPrimaryNonMSP.txt.
3. Open **LinuxPrimaryNonMSP.txt** in notepad.
4. Mention the user installation directory's path (**USER_INSTALL_DIR**) and file overwrite's (**-fileOverwrite_**) path.
5. Save and move **LinuxPrimaryNonMSP.txt** to home directory.
6. Open the Console and navigate to **ManageEngine_PAM360_64bit.bin** file location

7. Execute the command:

   chmod a+x ManageEngine_PAM360_64bit.bin

8. Execute the command:

   ./ManageEngine_PAM360_64bit.bin -i silent -f /home/LinuxPrimaryNonMSP.txt

PAM360 will get installed.

3.2 Secondary Server

1. Download the file ManageEngine_PAM360_64.bit.bin for Linux.
2. Download the installation file LinuxSecondaryNonMSP.txt.
3. Open **LinuxSecondaryNonMSP.txt** in notepad.
4. Mention the user installation directory's path (**USER_INSTALL_DIR**) and file overwrite's (**-fileOverwrite_**) path.
5. Save and move **LinuxSecondaryNonMSP.txt**to home directory.
6. Open the console and navigate to **ManageEngine_PAM360_64bit.bin** file location
7. Execute the command:

   chmod a+x ManageEngine_PAM360_64bit.bin

8. Execute the command:

   ./ManageEngine_PAM360_64bit.bin -i silent -f /home/LinuxSecondaryNonMSP.txt

PAM360 will get installed.

3. Transferring PAM360 Installation

If you want to move the PAM360 installation from one machine to another, or to a different location within the same machine, follow the procedure detailed below:

3.1 Prerequisites

Do not remove the existing installation of PAM360 until the new installation works fine. This is to ensure a backup and to overcome any disaster/data corruption during the movement.

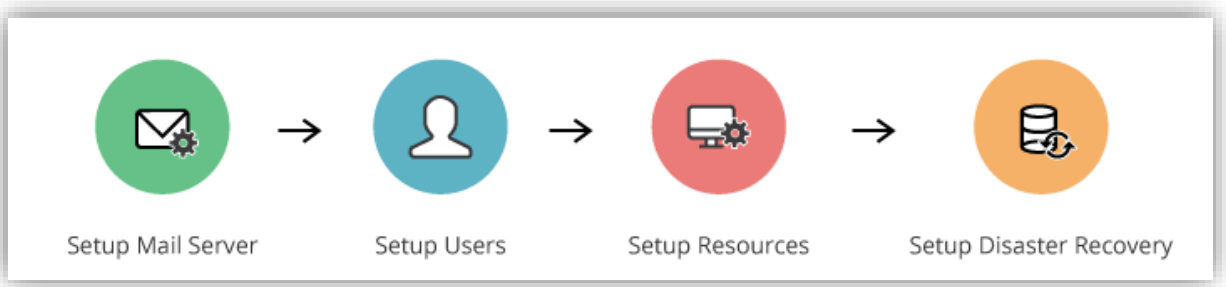
3.2 Steps Required

1. Take a backup of the current database and install PAM360 in the new machine.
2. Restore the backup data in the new installation.

The Workflow in PAM360

If you are an administrator engaged in the job of setting up PAM360 in your environment and managing passwords, following is the ideal work flow:

1. Setting up Mail Server
2. Adding Users
3. Adding Resources
   3.1 Access Control Workflow
4. Setting up Disaster Recovery



1. Setting up Mail Server

Prior to adding users, the important step to be done is configuring your mail server. Users will be notified of their PAM360 access details through email only, so ensure the mail server is set up properly.

2. Adding Users

1. Add users either manually or import user information from ActiveDirectory, LDAP or CSV file.
2. Specify appropriate access roles and password policies for the PAM360 users.
3. Group users together for the convenience of performing operations in bulk.
4. Enable authentication to any one of AD, LDAP or Local.

> **Note:** Change the password of the default 'admin' user or delete the account after adding another administrator user.

3. Adding Resources

The first step to actual Password Management in PAM360 starts with adding your "resource" to the PAM360 database. Here, resource denotes the server/application/device whose user accounts and passwords are to be managed by PAM360.

1. Add resources either manually or import from a CSV file along with their user account and password information.
2. Setup the password reset method to one of remote or agent-based, if you need.
3. Group resources together for the convenience of performing operations in bulk.
4. Create Nested Resource Groups: Maintaining resource groups in hierarchical structure (groups, sub-groups) for navigational convenience.
5. By default, the passwords added by you could be viewed and edited only by you. If required, share resource passwords with other PAM360 users or user groups.
6. Access and modify passwords that are owned by you and that are shared to you.

3.1 Access Control Workflow

After adding the resources, administrators can put in place access control work flow for extra level of security. After successful authentication into PAM360, users get access to the passwords that are owned by them or shared to them. In some cases, administrators wish to give temporary access to passwords for certain users for a specified period of time. In other instances, there would be requirements to give users exclusive privilege to passwords. That means, only one user should be allowed to use a particular password at any point of time. When more than one user is required to work on the same resource, problems of coordination arise. Access control on concurrent usage would help resolve such issues.

- Set up access control work flow as per the requirements of your organization

4. Setting up Disaster Recovery

If you are a password user follow the below steps to set up disaster recovery:

- Configure the database backup schedule to backup the entire contents of the PAM360 database
- Export resource information in the format of your choice to have readable copies of resource information only

If you are a Password user engaged in the job of viewing the passwords allotted to you, there is no need to carry out any configuration. You may directly view the passwords of resources/accounts and edit passwords if you have that permission.

Working with PAM360 Agent

Notes:

1. From build 5711 onwards, PAM360 will no longer support both the 32 and 64-bit versions of the C++ agent for Windows and Windows Domain systems and the C Agent for Linux. The C and C++ agents will still be functional in the older versions of PAM360 past this date. But, we highly recommend using the C# agent for Windows and Windows Domain machines and the Go agent for Linux machines, as they come with additional features, such as password reset listeners, dynamic account filtering, and self-service privilege elevation in Windows. Refer to the forum post to learn more about the end of support announcement.
2. Click here to learn how to install and uninstall agents in bulk using a script file invoked via the Windows GPO.
3. PAM360 agent will work only on Redhat versions up to 7.9, and CentOS.
4. For Go agent, from build 5301, the AMD64 version is supported for Ubuntu, Centos, RedHat, Debian, and other Linux flavors, and the ARM64 version is supported for Redhat.

PAM360 Agent - Overview

By deploying the PAM360 agent, you can establish connection with remote resources that are not connected to the PAM360 server and manage them from PAM360. PAM360 agent is available for Windows, Windows domain, and Linux servers. The agent package is available for download in the PAM360 web interface and it contains the necessary executable/configuration files, and an SSL certificate to use for the HTTPS communication between the agent and the PAM360 web server. During installation, you must supply a unique Agent Key (copied from the PAM360 UI) for each agent in the target machine. You can also keep an Agent Key active for a specified number of hours and use it for multiple installations.

The PAM360 agent is useful in the following cases:

- When PAM360 server runs in a Linux system and password reset has to be carried out for a Windows machine.
- If the target systems are in a Demilitarized Zone(DMZ) or a different network to which PAM360 server does not have direct connectivity.
- If the required administrative credentials are not stored locally in the PAM360 server to execute remote password resets.
- To change the password of domain accounts without the domain controller's admin

credentials.

Communication between the PAM360 Server and the PAM360 Agent

All password-related communication between the PAM360 server and the agent is carried out securely over HTTPS. Since the agent always initiates the connection, the communication is one-way. The agent residing in the target machines only needs access to the PAM360 web interface, thereby only the PAM360 web server needs to be available for the agent. Since the agent uses the outbound traffic to reach the login page of PAM360, there is no need to punch firewall holes or create VPN paths to allow inbound traffic for the server to reach all the deployed agents.

The agent will periodically ping the PAM360 web server through HTTPS to check if any operation is pending for execution. By default, the agent pings the server once every 60 seconds but the interval can be changed according to requirements. Once the agent contacts the PAM360 web server, the server will trigger the list of tasks to be carried out by the agent in the remote resource. Once the tasks have been executed, the agent will notify the results to the PAM360 web server.

> **Note:** Since the tasks are triggered by the web server only upon contact from the agent, the time taken for successful task execution will depend on how quickly the agent can connect with the PAM360 web server.

Installing PAM360 Agent

Before installing the agent, ensure that the account that you use to install the agent in the remote host has sufficient privileges to carry out password modifications.

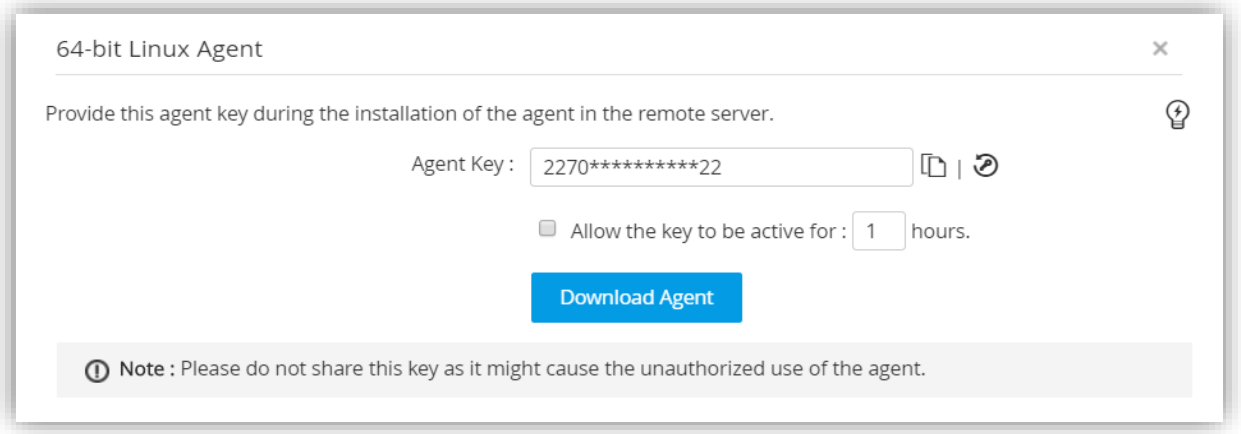
Note: You need administrative privileges in the target system to execute the above commands.

In this section, you will learn about the follwoing in details:

1. Downloading the PAM360 Agents
2. Installing Windows/Windows Domain Agent in the Resources/User Devices
3. Installing Linux Agent in the Linux Resources/User Devices
4. Configuring Agent Settings

1. Downloading the PAM360 Agents

1. Navigate to 'Admin >> PAM360 Agents' and select the agent packages available for the following operating systems:
    - Windows
    - Windows Domain
    - Linux
2. In the pop-up that appears, copy the Agent Key using the copy icon beside it. This Agent Key is necessary to install the PAM360 agent in the target system and it can be used one time only. Once the Agent Key is supplied for an installation, it will become invalid.



3. To keep the agent key in active status for a longer period, select the option **Allow the key to be active for: X hours** and specify the number of hours. Now, the same Agent Key can be used for any number of agent installations within the specified time.

Notes:

1. Please do not share this key as it might cause the unauthorized use of the agent.
2. Navigate to the **<PAM360 Installation Folder>/conf/system_properties.conf** directory and mention the following command to extend the key validity up to 999 hrs.

   - agent.gpo.time=999

4. Click **Download Agent** to download the agent zip. Once the agent package zip file is downloaded, unzip the content in the respective resource/user device.

2. Installing Windows/Windows Domain Agent in the Resources/User Devices

2.1 Installation using Command Prompt

a. To Install the Agent in the Resources

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the following command as per your agent installation requirements:

i. To install the agent as a service for password management, self-service privilege elevation, and zero trust implementation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> 1,2,3**.
ii. To install the agent as a service for password management, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> 1**.
iii. To install the agent as a service for self-service privilege elevation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI>2**. To learn more about configuring Self-Service Privilege Elevation in Windows, click here.
iv. To install the agent as a service for zero trust implementation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI>3**. To learn more about zero trust implementation in PAM360, click here.

3. Upon the respective action, the Windows/Windows Domain agent will be installed and the respective PAM360 agent service will start automatically.

b. To Install the Agent in the User Devices for Zero Trust Approach

1. Execute the command - **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> userdevice <PAM360 username>**.

> **Note:**
>
> If you install the agent as a service for a user device, it will be utilized to retrieve data from the user device for user trust score calculation. However, any device that has the agent configured in this manner will not be added as a resource in PAM360. Therefore, operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

c. To Start the Agent Service in the Resources/User Devices

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **AgentInstaller.exe start**.
3. The previously installed PAM360 agent service will start now.

d. To Update the Agent in the Resources

In case the PAM360 agent was previously installed by a different administrator, use this command to update the user account under which the agent server will be added as a resource. The agent server will be added as a resource under the new admin user without the need to uninstall and reinstall the agent. However, the new administrator will not have access to the accounts that were previously under the agent server. To gain access to the accounts, the previous admin has to transfer the ownership of the resource to the new admin.

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the following command as per your agent update requirements:
    i. To update the agent as a service for password management, self-service privilege elevation, and zero trust implementation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> 1,2,3**.
    ii. To update the agent as a service for password management, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> 1**.
    iii. To update the agent as a service for self-service privilege elevation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI>2**. To learn more about configuring Self-Service Privilege Elevation in Windows, click here.
    iv. To update the agent as a service for zero trust implementation, execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI>3**. To learn more about zero trust implementation in PAM360, click here.
3. Upon the respective action, the Windows agent will be updated and the PAM360 agent service will start automatically.

e. To update the Agent in the User Devices for Zero Trust Approach

1. Execute the command - **AgentInstaller.exe install <Agent Key copied from the PAM360 UI> userdevice <PAM360 username>**.

Note:

If you update the agent as a service for a user device, it will be utilized to retrieve data from the user device for user trust score calculation. However, any device that has the agent configured in this manner will not be added as a resource in PAM360. Therefore, operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

f. To Stop the Agent Service in the Resources/User Devices

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **AgentInstaller.exe stop**.
3. Now the PAM360 agent service will stop and it will be uninstalled.

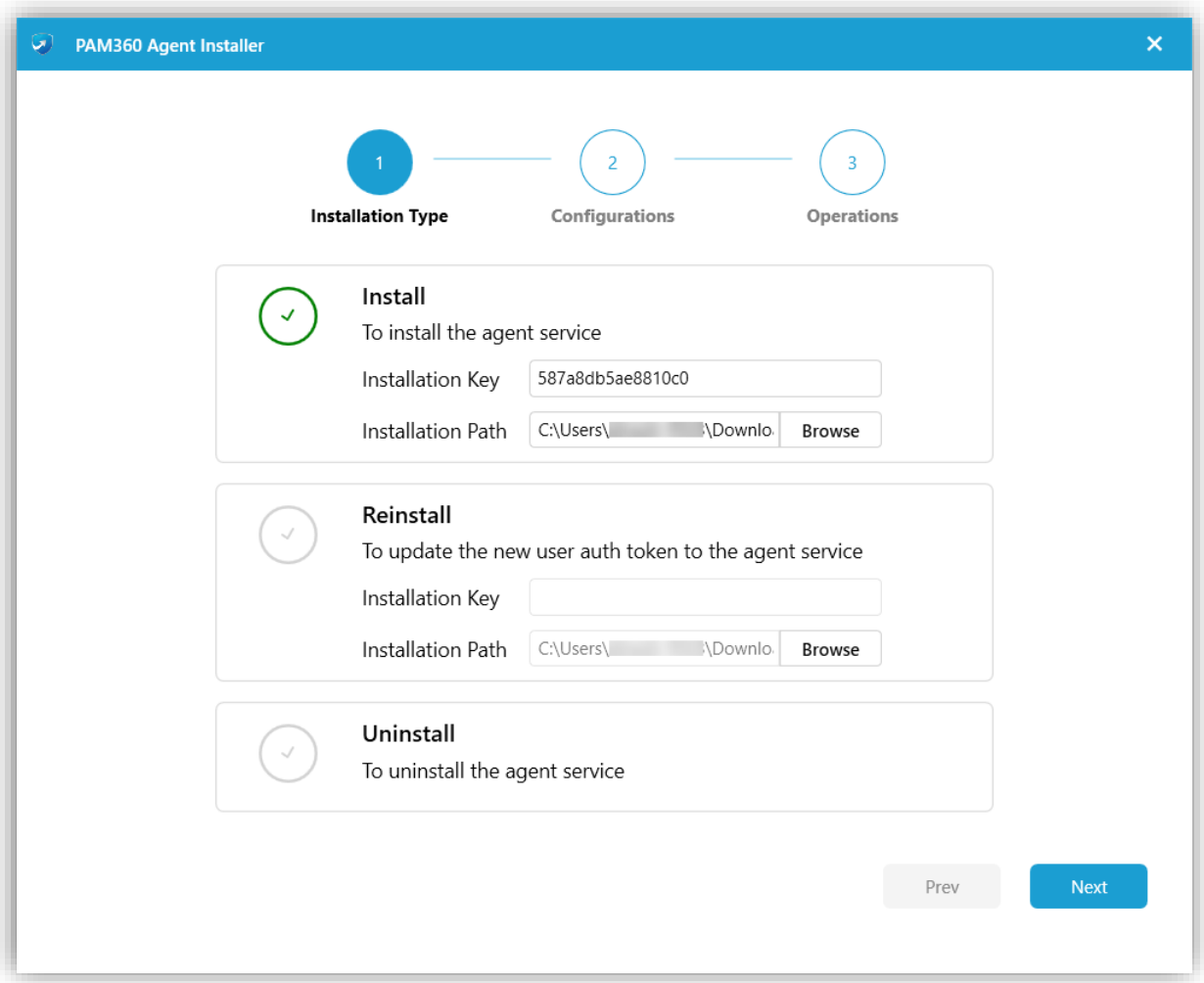
2.2 Installation using PAM360 Agent Installer

Prerequisite: Ensure that the agent-installed folder has complete permission for both the privileged account and the user account.

After downloading the agent, extract the folder and navigate to **PAM360Agent >> bin.**

a. To Install the Agent in the Resources/User Devices

1. Right-click **AgentInstaller.exe** and select **Run as administrator.**
2. The **PAM360 Agent Installer** wizard appears on the screen.
3. Select the **Install** option.
4. Enter the **Installation Key** and mention the **Installation Path.** Click **Next.**

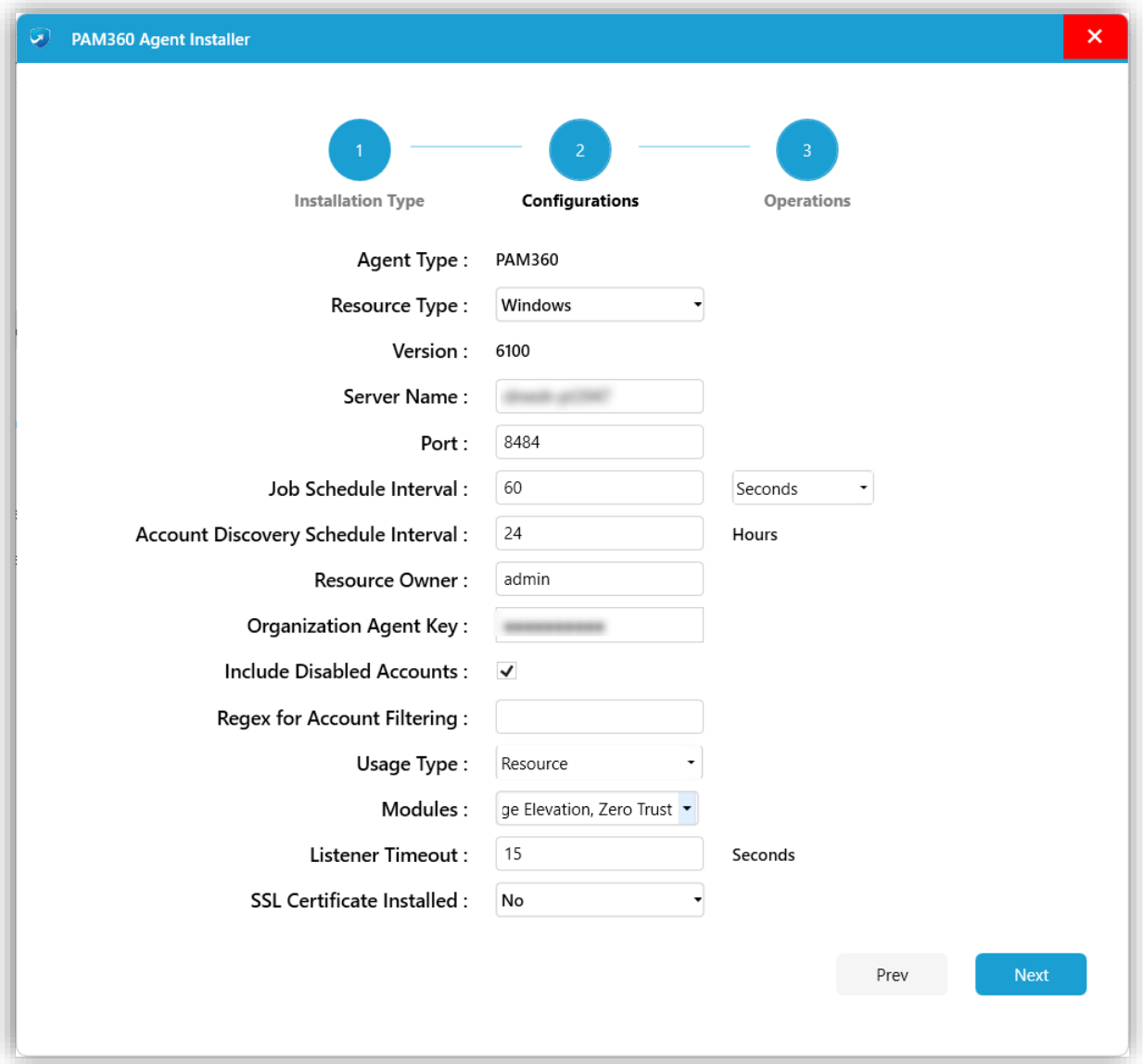


5. In the **Configurations** page that opens:
   i. Enter/modify the fields, such as **Resource Type, Server Name, Port, Schedule Interval, Resource Owner**, etc., based on your agent installation requirements.
   ii. Select the respective **Usage Type** of the agent. If you are installing the PAM360 agent in a user device to fetch user device data for user trust score calculation, select the **Usage Type** as **User Device** and enter the PAM360 user name to whom the user device is associated. If you are installing the PAM360 agent in an organization resource to fetch device data for resource trust score calculation, select the **Usage Type** as **Resource**.

Notes:

If you choose **User Device** as the **Usage Type**, the **Modules** section will automatically select **Zero Trust** by default. Any device that has the PAM360 agent installed with **Usage Type** - **User Device** will not be added as a resource in PAM360. The operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

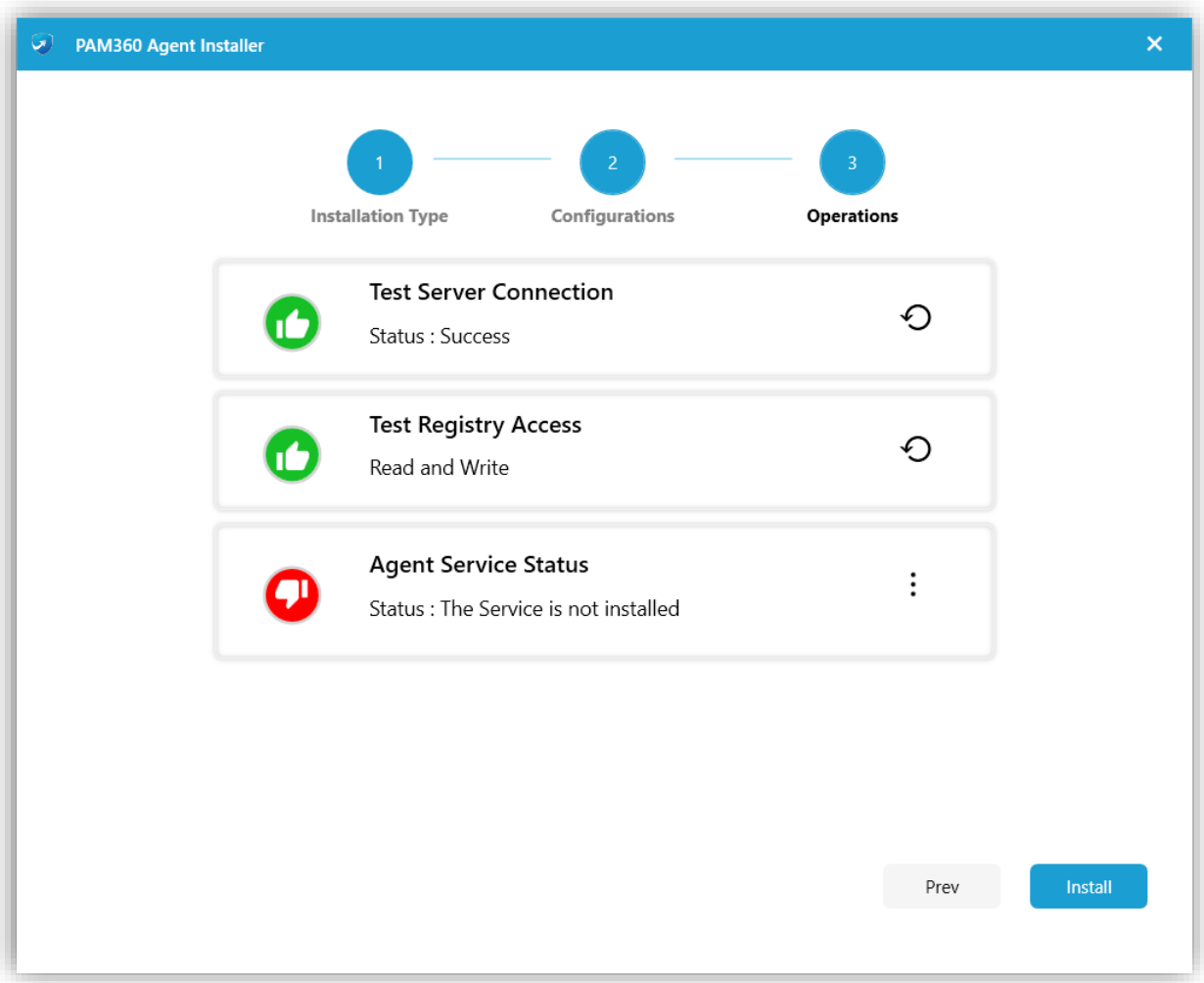
iii. Select the desired modules for your requirements from the PAM360 agent by enabling the corresponding checkboxes for '**Manage Passwords**', '**Self-Service Privilege Elevation**', and/or '**Zero Trust**' in the Modules section.
   a. If you enable **Manage Passwords**, a service will be added that will request the server periodically to verify and/or reset the password of accounts.
   b. If you enable **Self-Service Privilege Elevation**, a Self-Service Privilege Elevation module will be added.
      To learn more about configuring Self-Service Privilege Elevation, click here.
   c. If you enable **Zero Trust**, a service will be added that will request the user devices or resources' system data periodically, as defined above in the **Usage Type** for the trust score parameter validation.
      To learn more about implementing the Zero Trust approach in an organization, click here.



iv. By default, the **SSL Certificate Installed** field will be selected with **Yes**. If there is no valid SSL certificate installed in the PAM360, change this **SSL Certificate Installed** field to **No**.

Notes: The **Test Server Connection** status will be failed if selected **Yes** in the **SSL Certificate Installed** field, with no valid SSL certificate installed in the PAM360 server.

6. On the **Operations** page, check if the first two conditions are met and click **Install.**



You have now successfully installed the Windows/Windows Domain agent.

Notes:

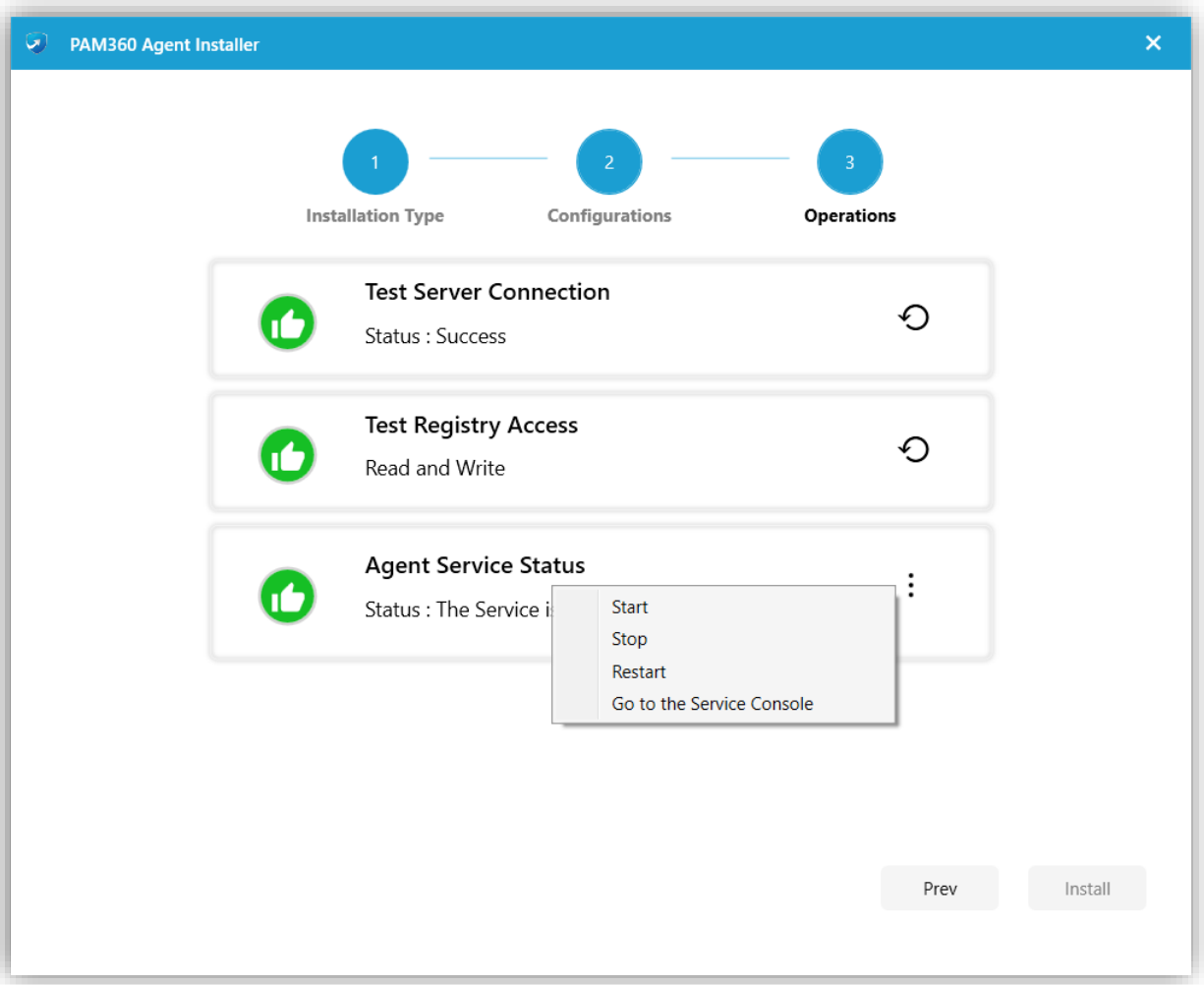
1. By default, all the files/applications (.exe, .msc, .msi, .cmd, and .bat) will have "Run as PAM360 Privilege Account" in the right-click menu. But the privilege elevation works only for those files/applications that are configured in PAM360.

2. When Self-Service Privilege Elevation is installed, the agent information will not be available in the services console.

b. To Start the Agent Service in the Resources/User Devices:

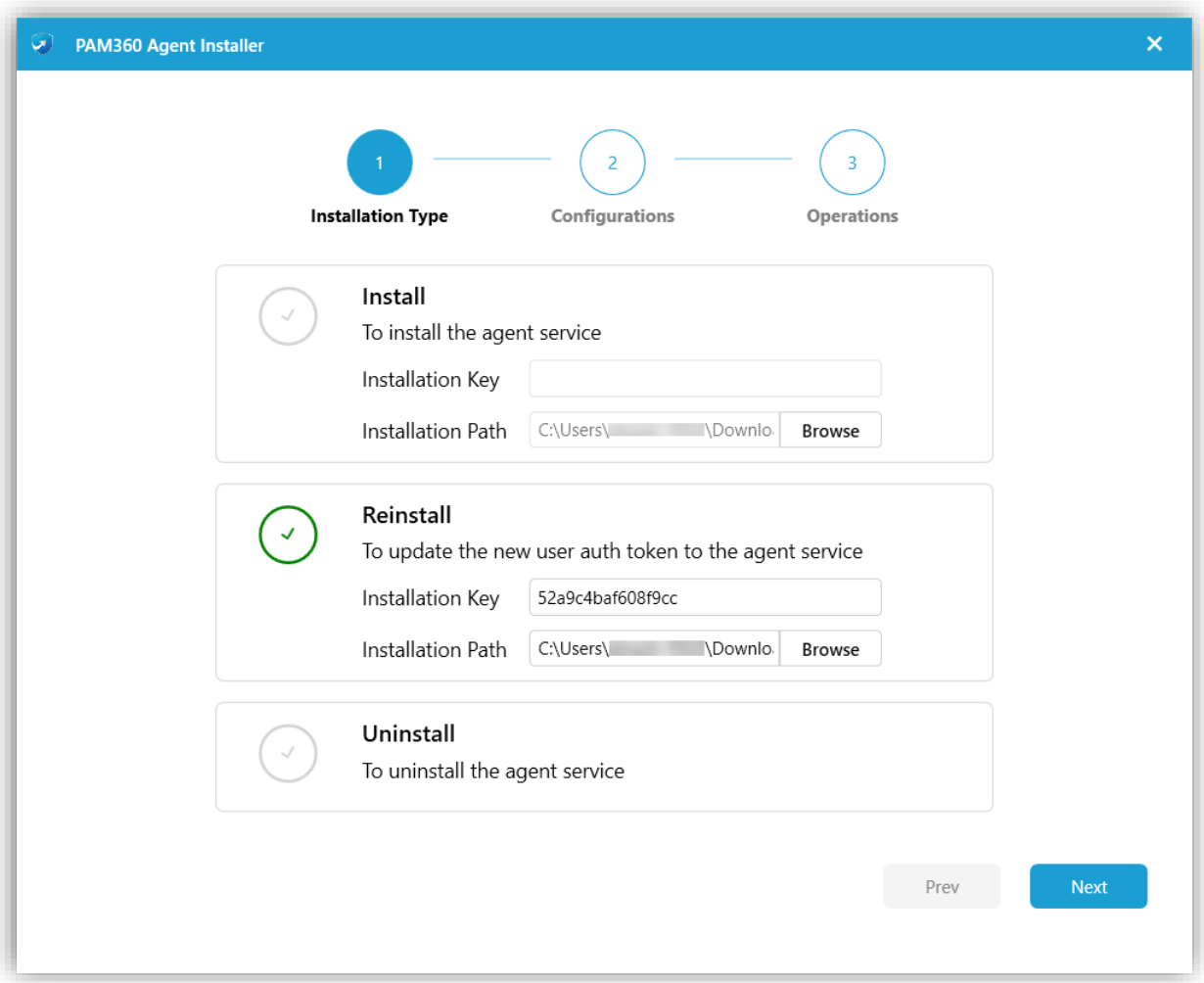
1. Right-click **AgentInstaller.exe** and select **Run as administrator.**
2. The **PAM360 Agent Installer** wizard appears on the screen.

3. Click the **Operations** icon.
4. Right-click the three dots beside **Agent Service Status** and click **Start.**
5. From here, you can also **Stop, Restart the agent** and **Go to the Service Console.**



c. To Update the Agent in the Resources/User Devices

1. Right-click **AgentInstaller.exe** and select **Run as administrator.**
2. The **PAM360 Agent Installer** wizard appears on the screen.
3. Select the **Reinstall** option.
4. Enter the **Installation Key** and mention the **Installation Path.** Click **Next.**

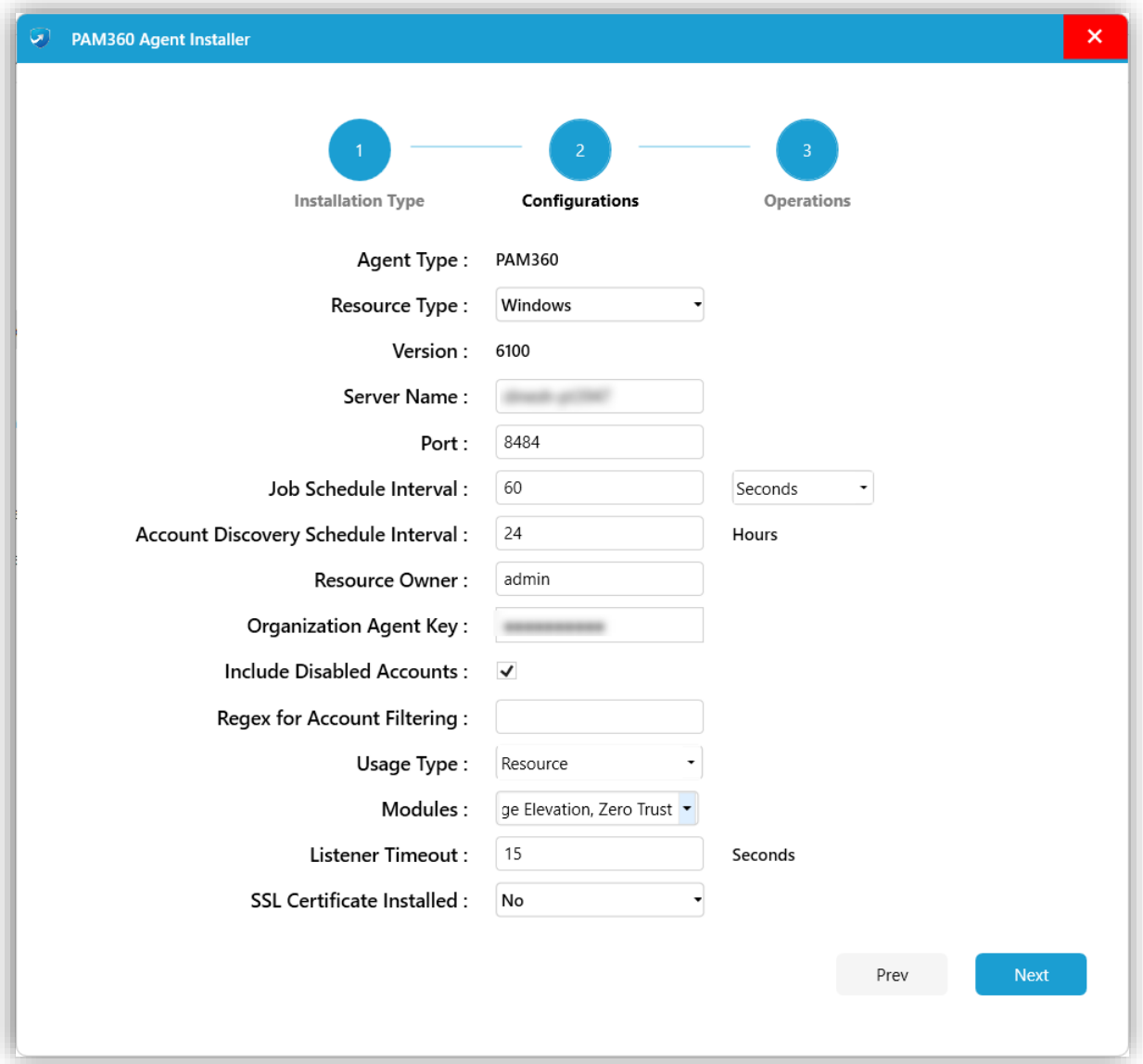


5. In the **Configurations** page that opens:
    i. Modify the fields, such as **Resource Type, Server Name, Port, Schedule Interval, Resource Owner**, etc., based on your agent installation requirements.
    ii. Select the respective **Usage Type** of the agent. If you are updating the PAM360 agent in a user device to fetch user device data for user trust score calculation, select the **Usage Type** as **User Device** and enter the PAM360 user name to whom the user device is associated. If you are updating the PAM360 agent in an organization resource to fetch device data for resource trust score calculation, select the **Usage Type** as **Resource**.

Notes:

If you choose **User Device** as the **Usage Type**, the **Modules** section will automatically select **Zero Trust** by default. Any device that has the PAM360 agent updated with **Usage Type** - **User Device** will not be added as a resource in PAM360. The operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

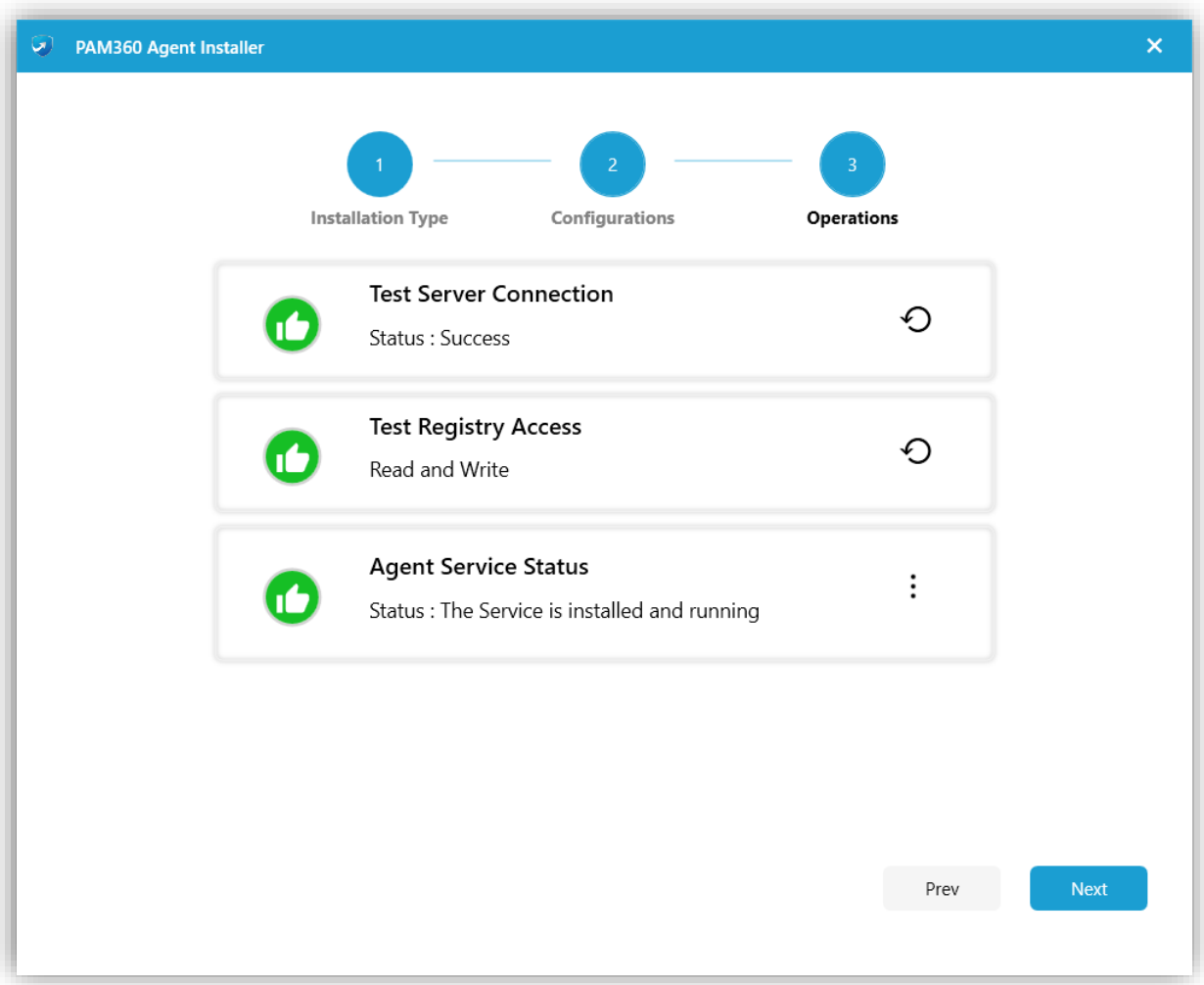
iii. Select the desired modules for your requirements from the PAM360 agent by enabling the corresponding checkboxes for '**Manage Passwords**', '**Self-Service Privilege Elevation**', and/or '**Zero Trust**' in the Modules section.
   a. If you enable **Manage Passwords**, a service will be added that will request the server periodically to verify and/or reset the password of accounts.
   b. If you enable **Self-Service Privilege Elevation**, a Self-Service Privilege Elevation module will be added.
      To learn more about configuring Self-Service Privilege Elevation, click here.
   c. If you enable **Zero Trust**, a service will be added that will request the user devices or resources' system data periodically, as defined above in the **Usage Type** for the trust score parameter validation.
      To learn more about implementing the Zero Trust approach in an organization, click here.



iv. By default, the **SSL Certificate Installed** field will be selected with **Yes**. If there is no valid SSL certificate installed in the PAM360, change this **SSL Certificate Installed** field to **No**.

Notes: The **Test Server Connection** status will be failed if selected **Yes** in the **SSL Certificate Installed** field, with no valid SSL certificate installed in the PAM360 server.

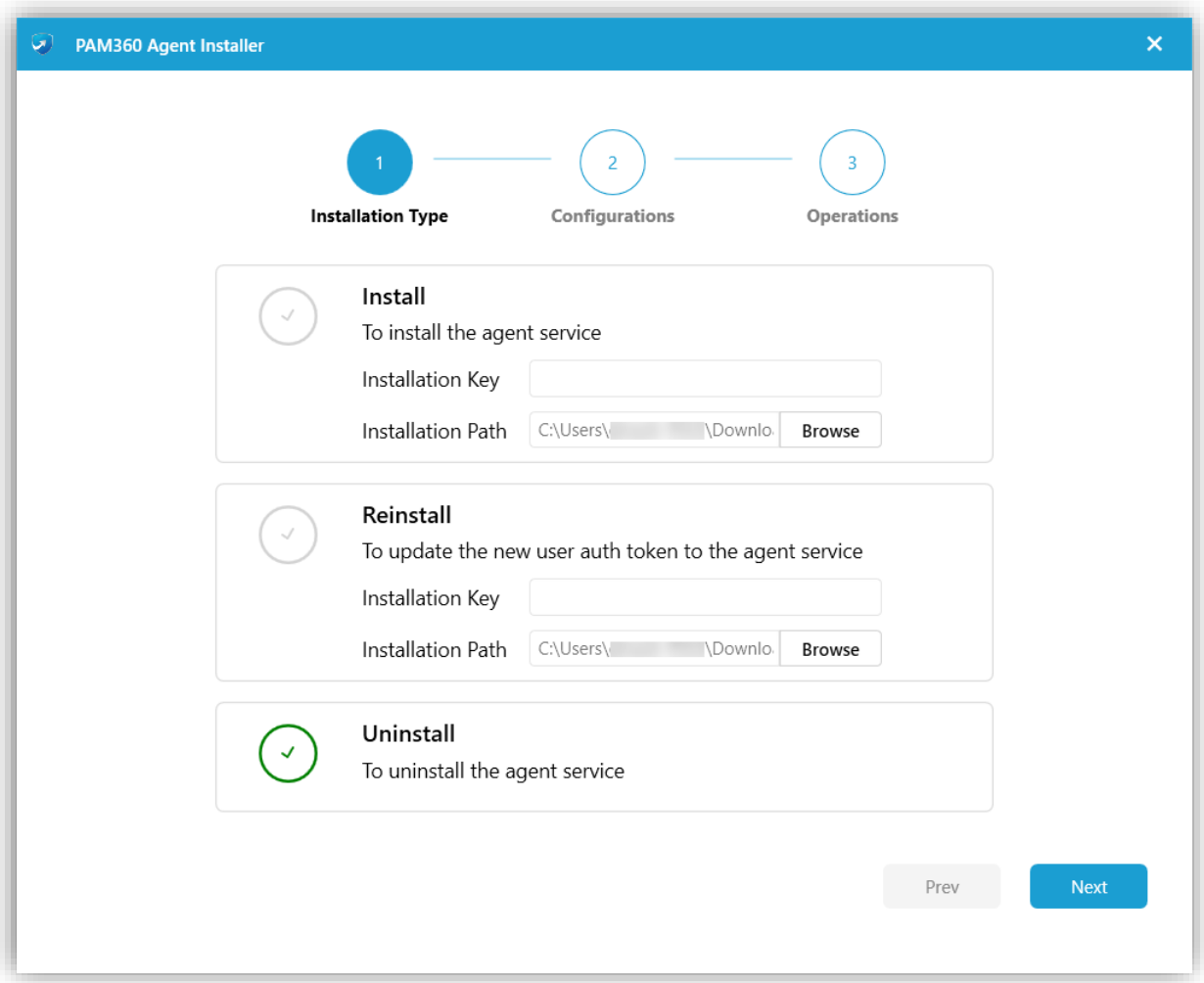
6. On the **Operations** page, check if the first two conditions are met and click **Next** to reinstall the agent.



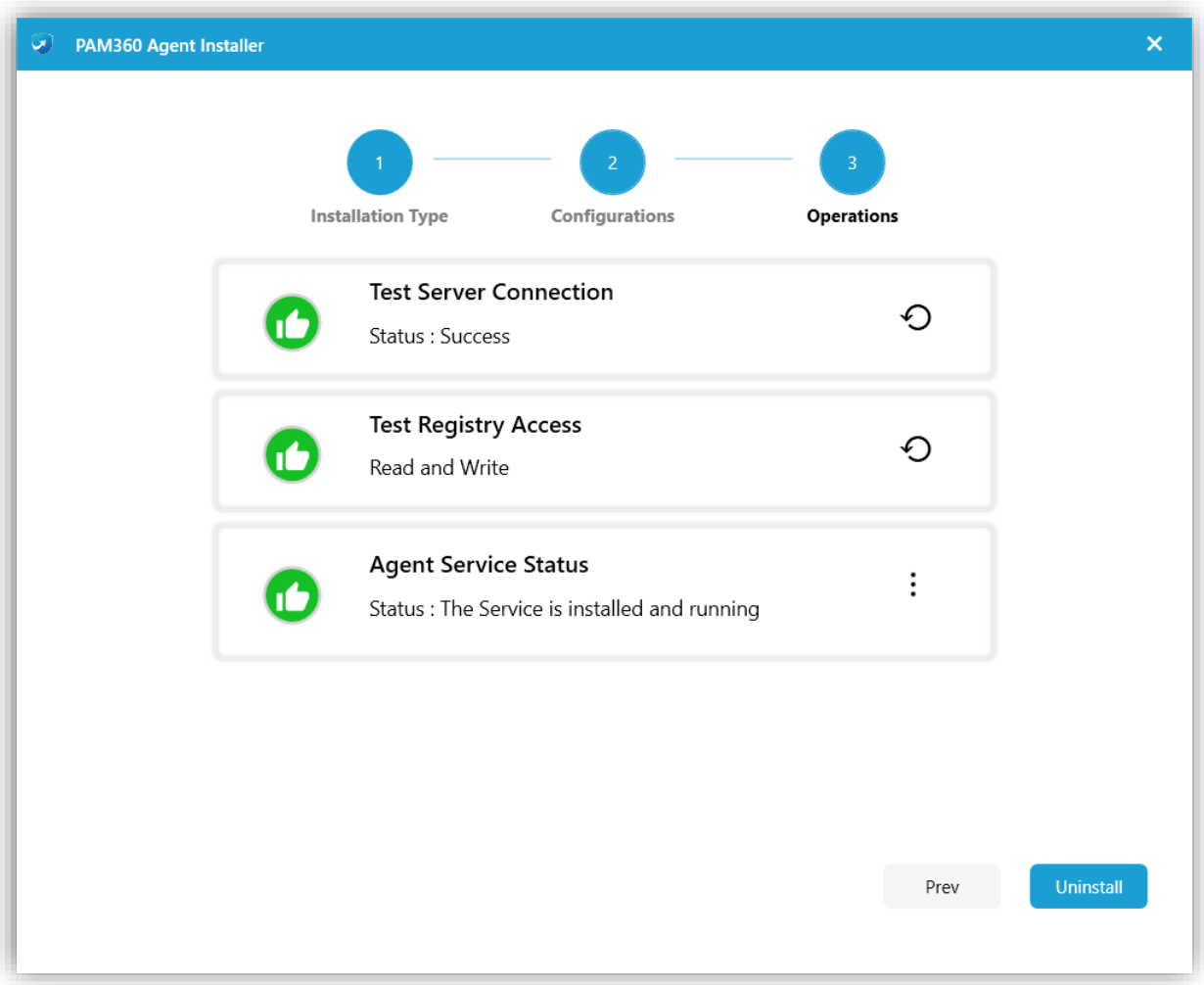
You have now successfully reinstalled the C# agent.

d. To Uninstall the Agent from the Resources/User Devices

1. Right-click **AgentInstaller.exe** and select **Run as administrator.**
2. In the wizard that appears, select **Uninstall** and click **Next.**



3. In the **Configurations** page, select the **Modules** (**Manage Passwords**, **Self-Service Privilege Elevation**, and/or **Zero Trust**) you want to uninstall and click **Next.**
4. In the **Operations** page, check if the first two conditions are met. Click **Uninstall.**



You have now successfully uninstalled the Windows/Windows Domain agent.

3. Installing Linux Agent in the Linux Resources/User Devices

Notes:

1. You need root privileges in the target system to execute the above commands.
2. PAM360 agents (32bit, 64bit) support the Linux flavors with the default OpenSSL library only.
3. Go-Agent supports all Linux flavors.

3.1 To Install the Agent in the Resources

1. Open a command prompt and navigate to the PAM360 agent installation directory.

2. Refer to the below steps to install the agent as per your requirement (bash command applicable for Go Agent only):
    i. To install the agent as a service for password management, self-service privilege elevation, and zero trust implementation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI> 1,2,3**.
    ii. To install the agent as a service for password management, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI> 1**.
    iii. To install the agent as a service for self-service privilege elevation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI>2**.
    To learn more about configuring Self-Service Privilege Elevation in Linux, click here.
    iv. To install the agent as a service for zero trust implementation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI>3**.
    To learn more about zero trust implementation in PAM360, click here.
3. The Linux agent will be installed and the PAM360 agent service will start automatically.

3.2 To Install the Agent in the User Devices for Zero Trust Approach

1. Execute the command - **installAgent-service.sh install <key> userdevice <PAM360 username>**.

> **Note:**
>
> If you install the agent as a service for a user device, it will be utilized to retrieve data from the user device for user trust score calculation. However, any device that has the agent configured in this manner will not be added as a resource in PAM360. Therefore, operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

3.3 To Start the Agent Service in the Resources/User Devices

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **sh installAgent-service.sh/bash installAgent-service.bash start** (bash command applicable for Go Agent only).
3. The previously installed PAM360 agent service will start now.

3.4 To Update the Agent in the Resources

In case the PAM360 agent was previously installed by a different admin user, use this command to update the user account under which the agent server will be added as a resource. The agent server will be added under the new admin user without the need to uninstall and reinstall the agent. However, the new admin will not have access to the accounts that were previously under the agent server. To gain access to the accounts, the previous admin has to transfer the ownership of the resource to the new admin.

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Refer to the below steps to update the agent as per your requirement (bash command applicable for Go Agent only):
    i. To update the agent as a service for password management, self-service privilege elevation, and zero trust implementation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI> 1,2,3**.
    ii. To update the agent as a service for password management, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI> 1**.
    iii. To update the agent as a service for self-service privilege elevation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI>2**.
    To learn more about configuring Self-Service Privilege Elevation in Linux, click here.
    iv. To update the agent as a service for zero trust implementation, execute the command **sh installAgent-service.sh/bash installAgent-service.bash install <Agent Key copied from the PAM360 UI>3**.
    To learn more about zero trust implementation in PAM360, click here.
3. The Linux agent will be updated and the PAM360 agent service will start automatically.

3.5 To Update the Agent in the User Devices for Zero Trust Approach

1. Execute the command - **installAgent-service.sh install <key> userdevice <PAM360 username>**.

> **Note:**
>
> If you update the agent as a service for a user device, it will be utilized to retrieve data from the user device for user trust score calculation. However, any device that has the agent configured in this manner will not be added as a resource in PAM360. Therefore, operations such as **Self-Service Privilege Elevation** and **Password Management** will not apply to those devices.

3.6 To Stop the Agent Service in the Resources/User Devices

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **sh installAgent-service.sh/bash installAgent-service.bash stop** (bash command applicable for Go Agent only).
3. The Linux agent service will be stopped.

3.7 To Uninstall the Agent from the Resources/User Devices

1. Open a command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **sh installAgent-service.sh/bash installAgent-service.bash remove** (bash command applicable for Go Agent only).
3. The Linux agent will be uninstalled and removed.

4. Configuring Agent Settings

Open the agent.conf file available in the downloaded agent package. The following are the parameters listed in the conf file, some of which can be modified to suit your needs:

1. **AgentType:** This denotes the type of agent i.e., agent with PAM360 features.
2. **ServerName:** This is the server/IP Address that the PAM360 agent will try to reach to contact the PAM360 server.
3. **ServerPort:** This indicates the port in which the PAM360 server is running. If you have changed the default port of PAM360 to any other port such as 443, the same port number must be updated here.

4. **ScheduleInterval:** By default, the agent pings the server once every 60 seconds. To configure the time interval at which the agent should ping the PAM360 web server, modify the time interval value in seconds.
5. **UserName:** This is the admin user account under which the agent server will be added as a resource.
6. **OSType:** Denotes the OS to which the agent belongs - Windows/Windows Domain/Linux.
7. **TrustedCertifcate:** By default, this value will be 'yes'. If there is no valid SSL certificate installed in the PAM360 server, edit this value to 'no'.

PAM360 allows the restriction of user accounts that are added via agents (C# and Go) during account discovery, using regex patterns. To do the same, use the below **UserQuery** and **accountFilter** commands:

- **UserQuery:** To filter the accounts in Linux (Go Agent).

  UserQuery = "awk -F: '$1 ~ /^admin.*/ {print$1}' /etc/passwd"

  //to discover accounts that starts with admin.

- **accountFilter:** To filter accounts in Windows/Windows Domain (C# Agent).

  accountFilter = ^admin.*

  // to discover accounts that starts with admin.

  Note: Windows Domain agent will not automatically add user accounts unless you specify the pattern in the account filter.

- **fetchDisabledAccount:** To fetch disabled accounts in Windows/Windows Domain (C# Agent).

  fetchDisabledAccount = True

The commands **UserQuery, accountFilter** and **fetchDisabledAccount** are applicable from build 5301 and later only.

Once any of the above parameters are modified, **restart** the agent service.

PAM360 Agent-Based Operations

Once you have installed the PAM360 agent with the respective usage and modules, you can proceed with the further operations related to the PAM360 agents that follow.

1. Discovering Local Accounts using the PAM360 Agent
2. Finding Tasks Awaiting Execution by the PAM360 Agent
3. Associating and Disassociating PAM360 Agents
4. Deleting a PAM360 Agent
5. Remapping a PAM360 Agent
6. Frequently Asked Questions

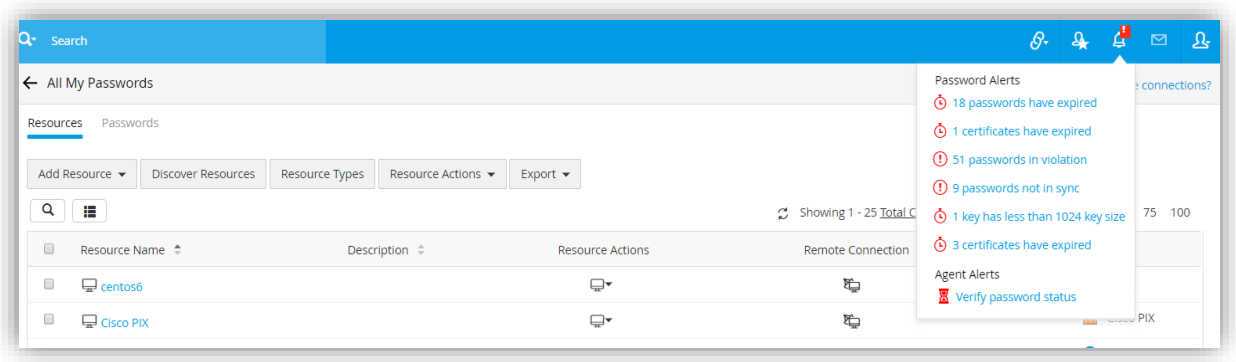
1. Discovering Local Accounts using the PAM360 Agent

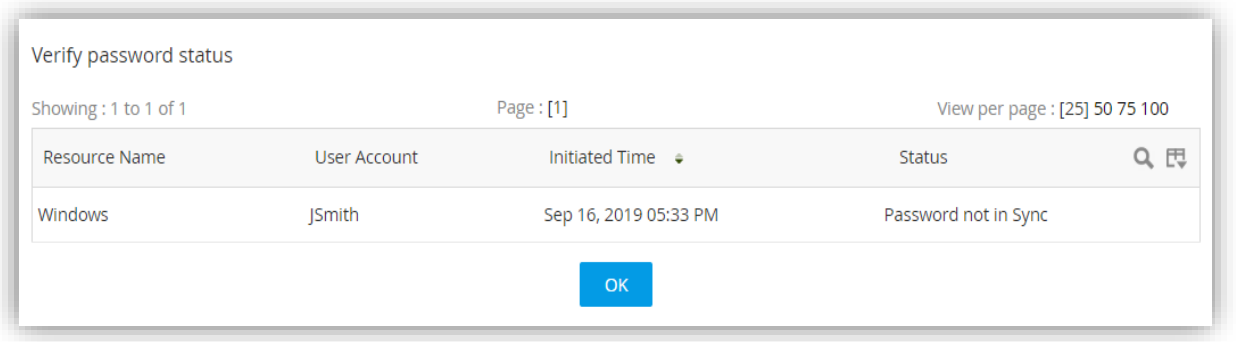
When the agent is started for the first time on the target machine, it will automatically add the machine as a resource in PAM360 and discover the local accounts. After discovery, you can reset the passwords of the local accounts. To learn more about resetting passwords using the PAM360 agent, click here.

2. Finding Tasks Awaiting Execution by the PAM360 Agent

Follow the below steps to find the tasks have been triggered by the user but awaiting execution by the PAM360 agent.

1. Click the bell icon in the top panel of the interface for viewing **Notifications**.
2. Under **Agent Alerts,** you will find the agent related statuses:
    - The number of password reset and password verify actions triggered.
    - Status of password reset actions triggered earlier.
    - Status of password verify actions triggered earlier.





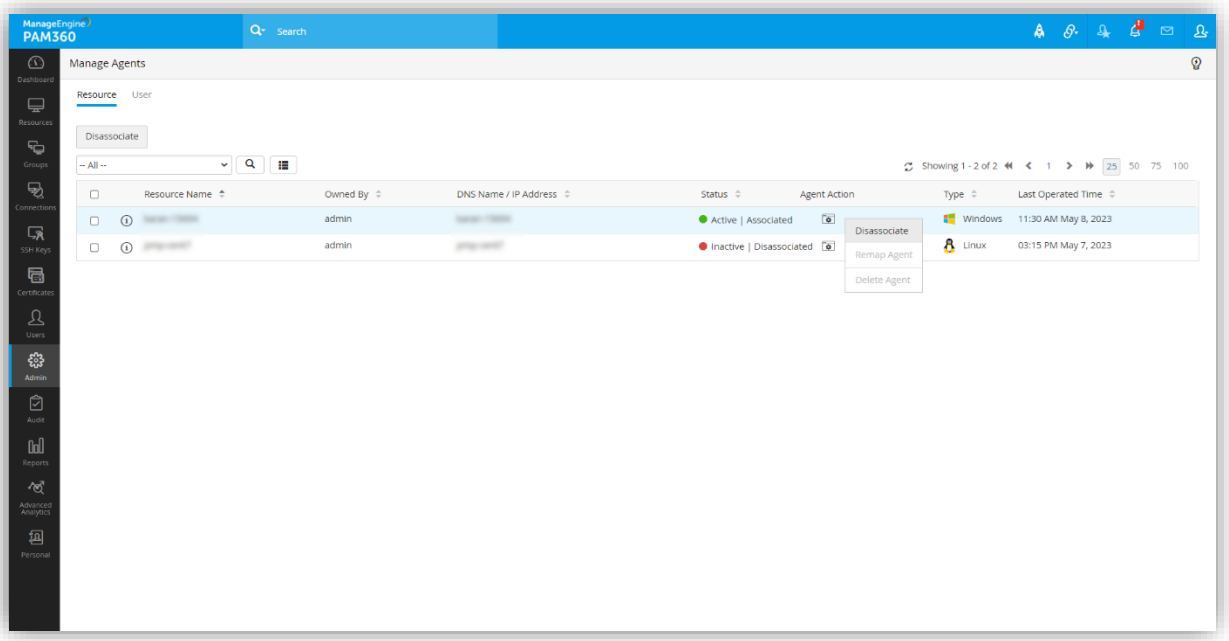
3. The notifications are user-specific i.e., users will be notified of only those tasks that they have triggered.

3. Associating and Disassociating PAM360 Agents

(This feature is available from PAM360 build 5710 for C# and Go Agents only)

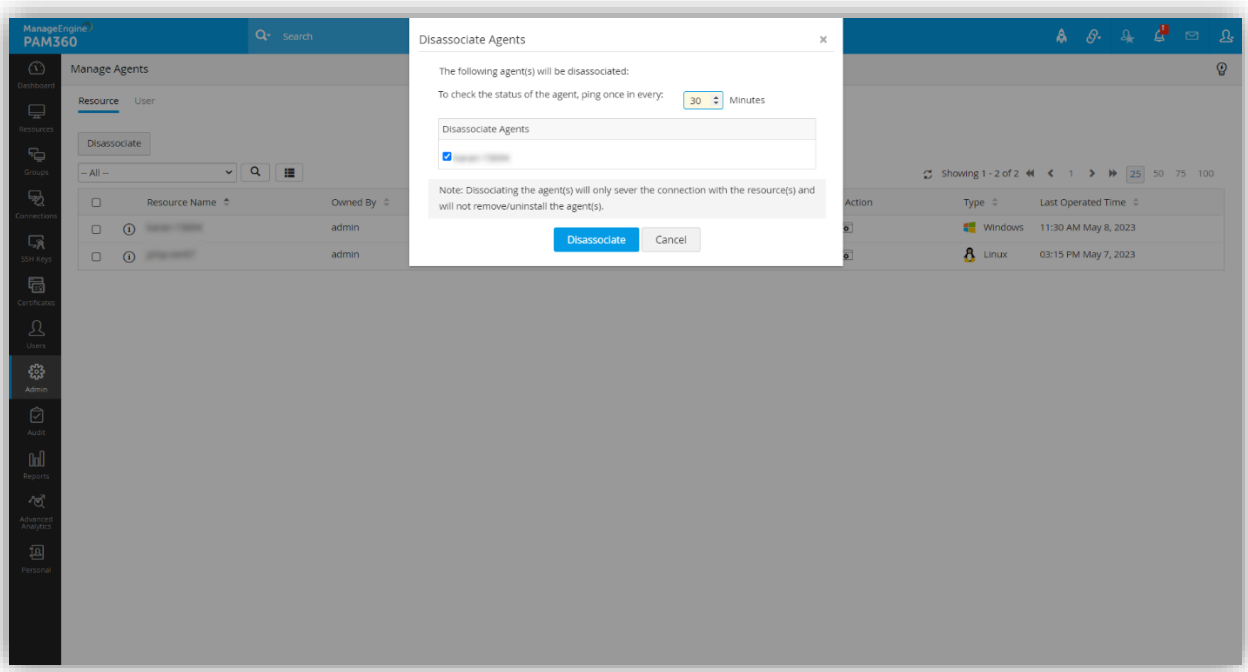
PAM360 allows users to associate and disassociate agents to/from their resources. Associating an agent will allow the agent to perform remote operations on the resource, while disassociating the agent will pause all the operations performed by it.

1. Navigate to **Admin >> PAM360 Agents >> Manage Agents.** Here, you will be able to view a list of agents mapped with their resources.
2. **To Disassociate a resource/user from an agent,**
    i. Click the **agent action** icon beside the desired resource/user name and click **Disassociate.**



ii. In the popup that appears, mention the time interval (in minutes) between which the agent should check its status.

iii. Click **Disassociate** to disassociate the selected agent. You have successfully disassociated the resource/user from the agent.

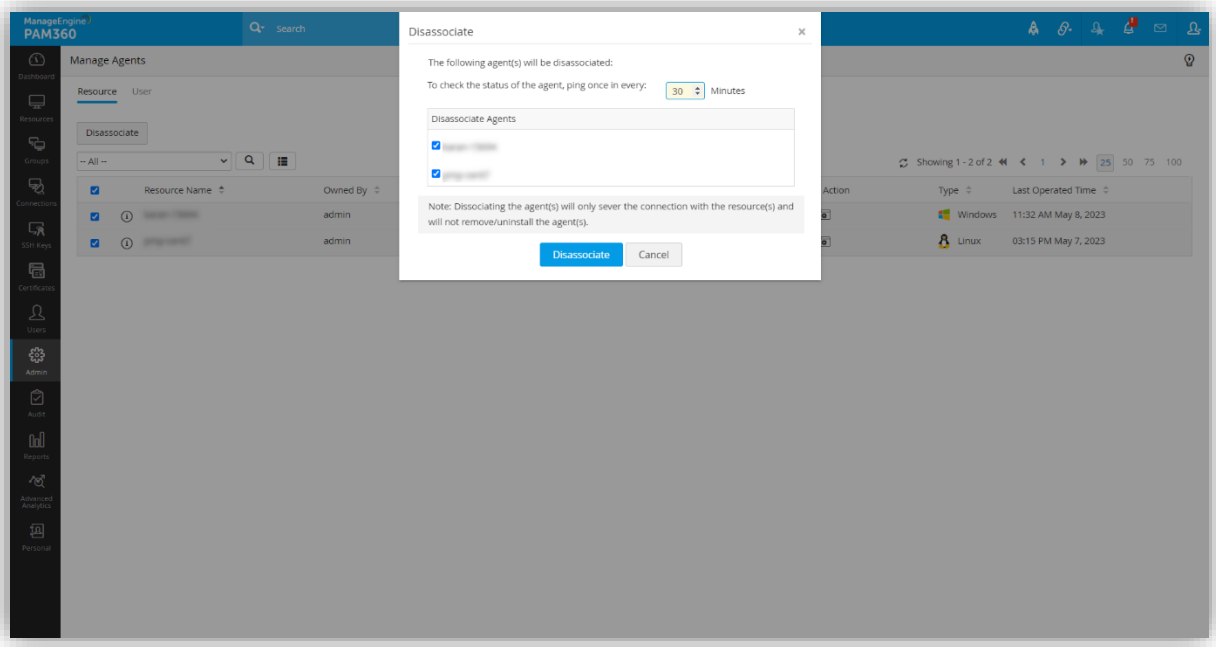


3. **To Disassociate agents in bulk,**

i. Select the required resources/users to be disassociated and click the **Disassociate** button from the top pane.

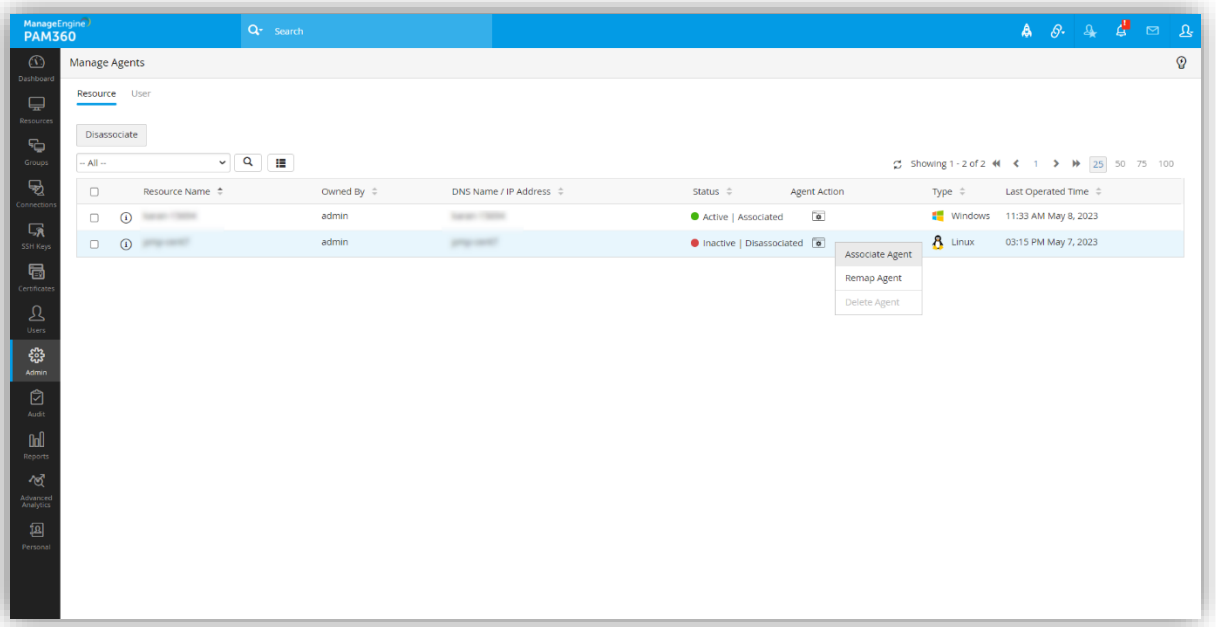
ii. Mention the time interval (in minutes) between which the agent should check the status.

iii. Click **Disassociate** to disassociate the selected agent. You have successfully disassociated the resource from the agent.



4. **To Associate a resource/user with an agent,**

i. Click the **agent action icon** beside the desired resource/user name and click **Associate.** You have successfully associated the resource/user with the agent.



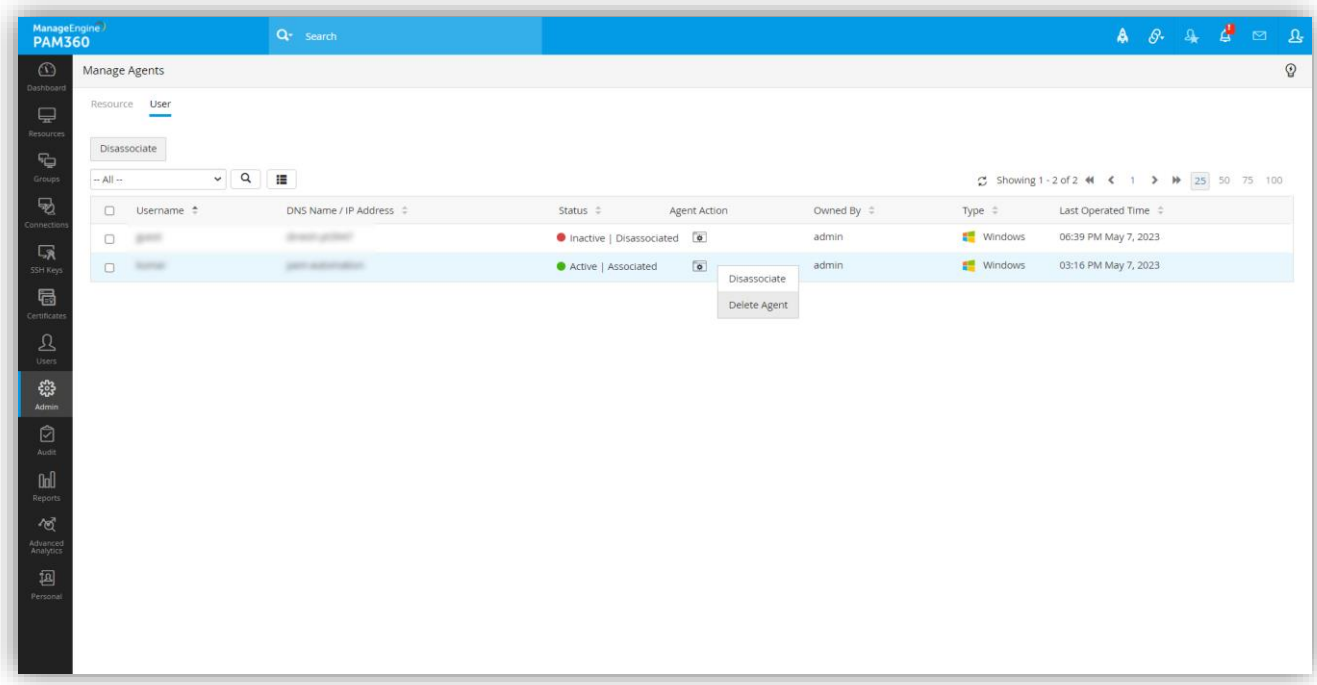
4. Deleting a PAM360 Agent

(This feature is available from PAM360 build 5710)

1. Navigate to the **Resources/Users** tab and delete the resource/user whose agent you wish to delete.
2. Now, navigate to **Admin >> PAM360 Agents >> Manage Agents.**

> **Note:** The 'Resource Name/User Name' for the agent whose resource/user got deleted will be displayed as 'N/A'.

3. Click the **agent action** icon beside the agent whose resource/user you deleted and click **Delete Agent.**



4. In the pop-up that appears, click **Delete.**

You have successfully deleted the agent.

Notes:

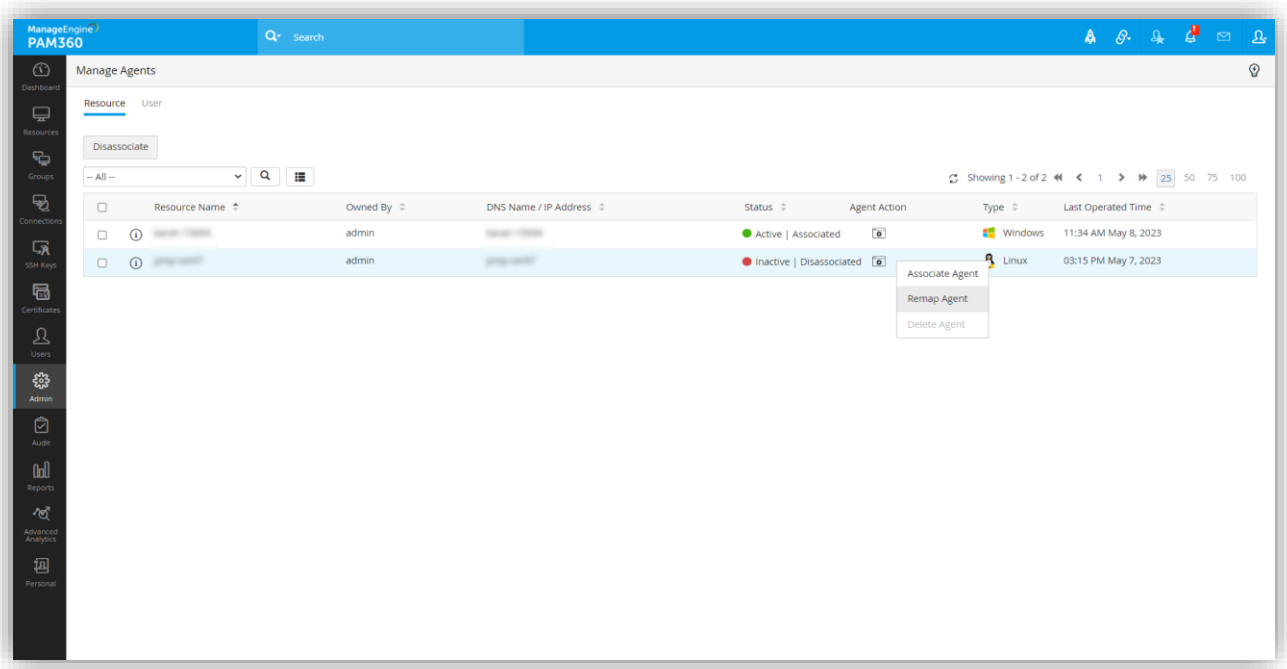
1. The resource gets deleted along with the agent, so it is recommended for the resource owner to take a copy of the resource before deleting the agent.
2. This operation will only remove the agent from the PAM360 server and will not uninstall the agent from the resource.
3. To add a deleted agent to the PAM360 server, reinstall the agent in the target machine.

5. Remapping a PAM360 Agent

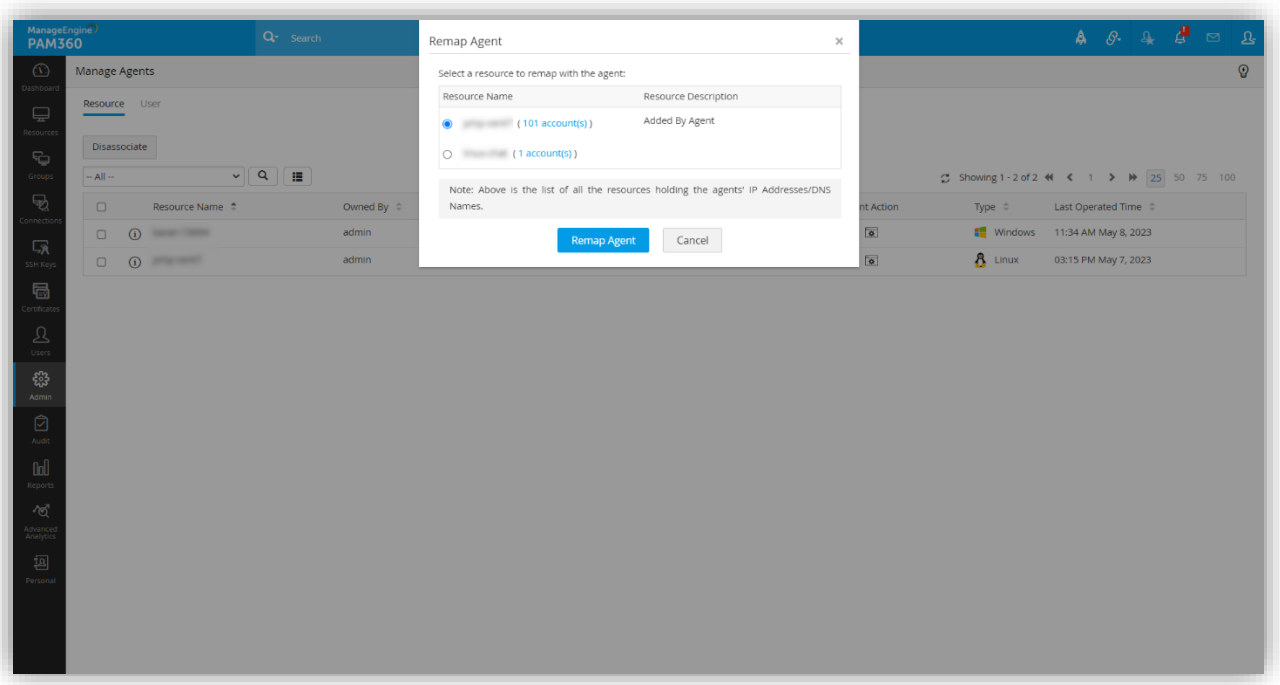
(This feature is available from PAM360 build 5710 for C# and Go Agents only)

The **Remap Agent** option is used when the resource of an agent is accidentally deleted. Administrators will be able to remap the agent to its resource using the following steps:

1. Navigate to the **Resources** tab and add a resource with the same DNS name as the agent.
2. Now, navigate to **Admin >> PAM360 Agents >> Manage Agents >> Resource.**
3. Click the **resource action** icon beside the agent belonging to the added resource and click **Remap Agent.**



4. In the pop-up that appears, select the resource with which you want to remap the agent and click **Remap Agent.**



You have successfully remapped the agent to the resource.

6. Frequently Asked Questions

1. **How to create a custom role to manage agents?**

   To manage agents, the user must have **Add** and **Edit** permission to the **Resources** and permission to **Download PAM360 Agents.** Follow the below steps:

   1. Navigate to **Admin >> Customization >> Roles.**
   2. Click **Add Roles.** In the pop-up that appears,
      - i. Mention the **Name** and **Description.**
      - ii. Click **Password.**
        - a. Click the **Resource** tab and enable **Add** and **Edit.**
        - b. Click the **Password Reset** tab and enable **Password Reset**.
      - iii. Click **Custom Settings** and enable **Download PAM360 Agents.**
   3. You have successfully created a role to manage agents.

   Note: The user will have to be the owner of the resource in which the agent is installed.

2. **Are there any reports for Manage Agents?**

   Navigate to **Reports >> Query Reports >> Resources** and search for '**Agents Installed**'. This report will contain a list of agents installed in their respective resources.

3. **What will happen to the existing agents & what functionalities are applicable after upgrading to 5710?**

   - When PAM360 is upgraded to build 5710, all the existing agents from the older build will be added to **Admin >> PAM360 Agent >> Manage Agent.**
     You will only be able to **view** and **Delete** the old agents from the **Manage Agents** window.
   - It is recommended that you reinstall the latest agent in the target machine to use other functionalities such as **Associate, Disassociate** and **Remap.**

4. **What will happen in the Manage Agents window if the agent is removed/uninstalled from the target machine?**

   The status of the agent is updated once every 30 min by default. If the agent is inactive for that period of time, the status of that agent will be marked as inactive.

5. **If a resource is shared with an admin with full access, will the agent be displayed under the Manage Agents window?**

   No, the agent details will be displayed under the Manage Agents page only when the resource ownership is transferred to a different admin-privileged user.

6. **What will happen when the ownership of the agent-installed resource is transferred to a different admin-privileged user?**

   The agent installed in the resource will be displayed in the **Manage Agents** window to the user to whom the ownership of the resource is transferred.

Getting Started with PAM360

Once you have finished setting up PAM360, you can get started to work with the PAM360 application. Before you begin to work with the PAM360 console and configure the required settings, you will have to know about a set of configurations that will help you get started with PAM360.

In this help section, you will have learned about:

1. Starting and Shutting Down PAM360
    1.1 In Windows
    1.2 In Linux
2. Launching the PAM360 Web Client
    2.1 Connecting to Web Client from PAM360 Server
    2.2 Connecting to Web Client in Remote Hosts
    2.3 Authenticating PAM360 from the Web Client
3. Running the PAM360 service using a group Managed Service Account
4. Managing PAM360 Encryption Key
5. Rotating the Encryption Key
6. Updating Web Server Certificates using PAM360 Web Console

1. Starting and Shutting Down PAM360

1.1 In Windows

Using the Start Menu	Using the Tray Icon
1. Navigate to **Start >> Run** [OR] press **Win+r.** The Run box appears. Type **services.msc** and hit **Enter**. 2. Locate the **PAM360** service in the Services console. 3. You can start, stop or restart the service from the services console.	1. Once you have successfully installed PAM360 in your system, you will find the PAM360 icon in the windows tray area on the far right end of your task bar. 2. Right click the tray icon and click the desired operation: • Start the PAM360 Service • Stop the PAM360 Service • Launch the PAM360 web console

1.2 In Linux

Installing PAM360 as a Startup Service	Starting & Stopping the Server as as Service
1. Login as a root user. 2. Open the console and navigate to the **<PAM360_Home>/bin** directory. 3. Execute **"sh pam360.sh install"** (In Ubuntu, execute as "bash pam360.sh install"). 4. To uninstall, execute the script **"sh pam360.sh remove"**.	**To Start PAM360 as a service in Linux:** 1. Login as non-root user. 2. Execute **/etc/rc.d/init.d/pam360-service start**. 3. PAM360 server runs in the background as service. **To Stop PAM360 Server started as a service, in Linux:** • Execute **/etc/rc.d/init.d/pam360-service stop.**(as non-root user)

2. Launching the PAM360 Web Client

There are different ways of connecting to the PAM360 web client:

2.1 Connecting to Web Client from PAM360 Server

a. Automatic Browser Launch

Once the PAM360 server has started, the login screen will appear in a browser window. Upon each server startup, the browser window will be launched automatically.

b. Launching the Web Client Manually

For Windows: Right-click the **PAM360 tray** icon and click **PAM360 Web Console** to launch the web client manually. The PAM360 Login screen shows up in a browser window.

For Linux: Open a browser and connect to the URL specified below.

https://<hostname>:portnumber/

where,

<hostname> - the host where the PAM360 server is running.

<portnumber> - the default port is 8282.

Example: https://localhost:8282

2.2 Connecting to Web Client in Remote Hosts

If you want to connect to the PAM360 web client in a remote machine (different from the one where PAM360 is running), open a browser and connect to the below URL:

https://<hostname>:portnumber/

where,

<hostname> - the host where the PAM360 server is running.

<portnumber> - the default port is 8282.

Example: https://localhost:8282

2.3 Authenticating PAM360 from the Web Client

PAM360 utilizes a secure HTTPS connection, so you will receive a prompt to accept the Security Certificate (if trusted web server certificate is not installed already). Click Yes, input your **Username** and **Password** on the login screen, and then press **Enter**.

For an unconfigured setup, the default **Username** and **Password** is **'admin'**. You will be prompted to update the password after your initial login. The administrator can change the initial authentication mechanism via AD/LDAP/Microsoft Entra ID as required, followed by a 2FA.

For a more streamlined and passwordless authentication process, use the available **Smart Login** method by scanning the QR code through the PAM360 mobile application.

Administrators can enable smart login or set the smart login as the preferred initial login method by navigating to **Admin >> Settings >> General Settings >> User Management**.

3. Running the PAM360 Service using a group Managed Service Account

PAM360 allows you to run/manage services using group Managed Service Account (gMSA). To learn about gMSA in detail, refer to Microsoft's documentation.

To create a group Managed Service Account,

1. Open **Powershell ISE** as administrator.
2. Execute the following commands:
   i. **Import-Module ActiveDirectory**
   ii. **Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))**
   iii. **New-ADServiceAccount -Name <MSA_AccountName> -DNSHostName <DNSNAme> -PrincipalsAllowedToRetrieveManagedPassword <Machine_Name>$**
   iv. **Add-ADComputerServiceAccount -Identity <Machine_Name> -ServiceAccount <MSA_AccountName>**
   v. **Install -ADServiceAccount -Identity <MSA_AccountName>**
3. Provide Full Control Permission to the installation folder.
4. To configure **LogOn Services,**
   i. Navigate to **Services >> Properties >> LogOn.**
   ii. Browse for **MSA Account.**
   iii. Now, clear the **Password field** and click **Apply.**
   iv. Click **Ok.**

Now you have successfully configured the LogOn Services.

You have successfully created a group Managed Service Account (gMSA) account. Now, you can run your PAM360 service using the gMSA account.

Troubleshooting Step:

If you are unable to Install the Service Account, execute the below command before executing Install statement:

Set-ADServiceAccount -Identity <MSA_AccountName> -KerberosEncryptionType AES128,AES256

Reference links:

- https://www.tutorialspoint.com/windows_server_2012/windows_server_2012_group_managed_service_accounts.htm
- https://blogs.technet.microsoft.com/askds/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting/

4. Managing PAM360 Encryption Key

PAM360 uses AES-256 encryption to secure the passwords and other sensitive information in the password database. The key used for encryption is auto-generated and is unique for every installation. By default, this encryption key is stored in a file named **pam360_key.key** under the **<PAM360_HOME>/conf** folder. For production instances, PAM360 does not allow the encryption key to be stored within its installation folder. This is done to ensure that the encryption key and the encrypted data, in both live and backed-up database, do not reside together.

We strongly recommend that you move and store this encryption key outside of the machine, where PAM360 is installed, in another machine or an external drive. You can supply the full path of the folder, where you want to move the **pam360_key.key** file, manually move the file to that location and delete any reference within PAM360 server installation folder. The path can be a mapped network drive or an external USB (hard drive / thumb drive) device.

PAM360 will store the location of the **pam360_key.key** in a configuration file named **manage_key.conf**, present under the **<PAM360_HOME>/conf** folder. You can also edit that file directly to change the key file location. After configuring the folder location, move the **pam360_key.key** file to that location and ensure the file or the key value is not stored anywhere within the PAM360 installation folder.

PAM360 requires the **<PAM360 installation directory>PAM360\conf** path to be accessible with necessary permissions, to read the **pam360_key.key** file, when it starts up every time. After a successful start-up, it does not need access to the file anymore and the device with the file can go offline.

IMPORTANT NOTES:

1. Always ensure sufficient protection to the key with multiple layers of encryption (such as by using Windows File Encryption) and access control.
2. Since only the PAM360 application needs access to this key, make sure no other software, script or person has access to this key under any circumstances.
3. Take care of securely backing up the pam360_key.key file by yourself. You can recover the PAM360 backups only if you supply this key. If you misplace the key or lose it, PAM360 will not start.
4. If you store the database_params.conf file at a different location, you will have to copy the file back to the original location (i.e. to <PAM360 Installation Folder>/conf/), whenever you perform an application upgrade.

5. Rotating the Encryption Key

Even if you are sure of managing the encryption key securely outside of PAM360, one of the best practices is to periodically change the encryption key. PAM360 provides an easy option to automatically rotate the encryption key.

5.1 How does the key rotation process work?

PAM360 will look for the current encryption key present in the file **pam360_key.key,** available in the path specified in the **manage_key.conf** file, present under the **<PAM360_HOME>/conf** folder. Only if it is present in the specified path, the rotation process will continue. Before rotating the encryption key, PAM360 will take a copy of the entire database. This is to avoid data loss, if anything goes wrong with the rotation process.

During the key rotation process, all passwords and sensitive data will be decrypted first using the current encryption key and subsequently encrypted with the new key. Later, the new key will be written in the **pam360_key.key** file present in the location as specified in the **manage_key.conf** file. At the end of successful key rotation, PAM360 will write the new encryption key in the same file that contains the old key. If any error occurs while writing the key, the rotation process will be aborted.

5.2 Steps to rotate the encryption key (if you are NOT using High Availability)

1. Ensure that the current encryption key (**pam360_key.key file**) is present in the location as specified in the **manage_key.conf** file. Also, ensure that PAM360 gets the **read/write** permission while accessing the **pam360_key.key** file.

2. Stop the PAM360 server.
3. Open the command prompt and navigate to **<PAM360-Installation-Folder>/bin** directory. Execute **RotateKey.bat** (in Windows) or **sh RotateKey.sh** (in Linux).
4. Based on the number of passwords managed and other parameters, the rotation process will take a few minutes to complete.
5. Start the PAM360 server once you see the confirmation message.

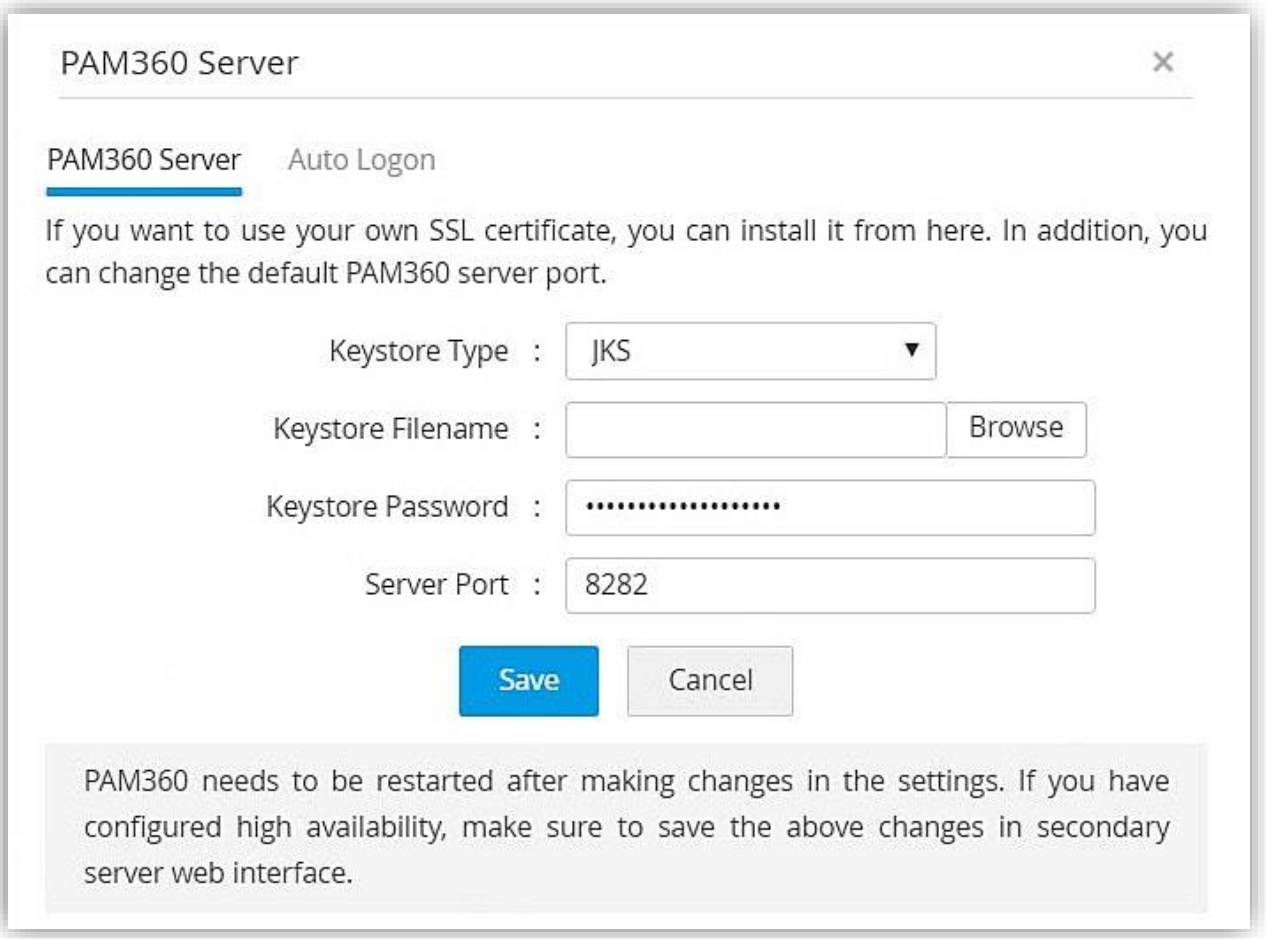
5.3 Steps to rotate the encryption key (if you are USING High Availability)

1. Navigate to **Admin >> General >> High Availability** in the PAM360 web interface. Make sure High Availability and Replication Status are alive.
2. Check if the current encryption key (**pam360_key.key file**) is present in the location as specified in the **manage_key.conf** file. Also, ensure that PAM360 gets the read/write permission when accessing the **pam360_key.key** file.
3. Stop the PAM360 Primary server and **make sure PAM360 Secondary server is running.**
4. Open the command prompt in the PAM360 Primary installation, navigate to the **/bin** directory and execute **RotateKey.bat** (in Windows) or sh **RotateKey.sh** (in Linux).
5. Based on the number of passwords managed and other parameters, the rotation process will take a few minutes to complete. You will see confirmation message ons successful completion of the rotation process.
6. Copy the new encryption key from the Primary installation and paste it in the location, as specified in the **manage_key.conf** file. This is the location from where the Standby will fetch the **pam360_key.key** file.
7. Now, start the Primary and the Standby servers.

6. Updating Web Server Certificates using PAM360 Web Console

If you want to use PAM360 web console to update the web server certificates, follow the below steps:

1. Navigate to **Admin >> Configuration >> PAM360 Server.**
2. In the PAM360 Server page that opens, install your **keystore** file belonging to the SSL certificate and/or change the default PAM360 server port.
3. To update your SSL certificate, select the type of the keystore file **(JKS, PKCS12 or PKCS11)** from the **Keystore type** drop down menu.
4. Browse the keystore file from your system and upload it in the **Keystore Filename** field.
5. Enter the password of your keystore file beside the Keystore Password field.



6. If you want to change the default PAM360 server port, enter the port number against the **Server Port** field.
7. Click **Save.**
8. Restart PAM360 after saving the changes.

Using MS SQL Server as the Backend Database

PAM360 uses PostgreSQL as the default backend database that comes bundled with the product. However, you can configure the product with other databases as well, such as MS SQL standalone, MS SQL cluster, Azure SQL, Azure Postgres, etc. In this document, you will learn in detail the steps to set up MS SQL as the backend database for your PAM360 installation.

Steps Required

1. Creating the SSL Certificate and Installing it in the Windows Certificate Store
2. Importing the SSL Certificate to PAM360
3. Enabling SSL Encryption in SQL Server
4. Executing ChangeDB.bat in PAM360

> **Note:** To ensure high level of security, PAM360 has been configured to connect to the SQL server only through **SSL**.

1. Creating the SSL Certificate and Installing it in the Windows Certificate Store

(in the machine where SQL server is running)

Prior to connecting PAM360 with the SQL server, you need to enable SSL encryption in the SQL Server. For this, you need to create an SSL Certificate and get it signed by either a Certificate Authority (CA) or self-sign it (See more).

A) Generating the certificate and getting it signed by a third-party CA:

Create the certificate using **openssl.** This involves two steps - **generating private key** and **generating certificate request**. Use the following commands to create the certificate.

a. **Generating Private Key:** Execute the following command:

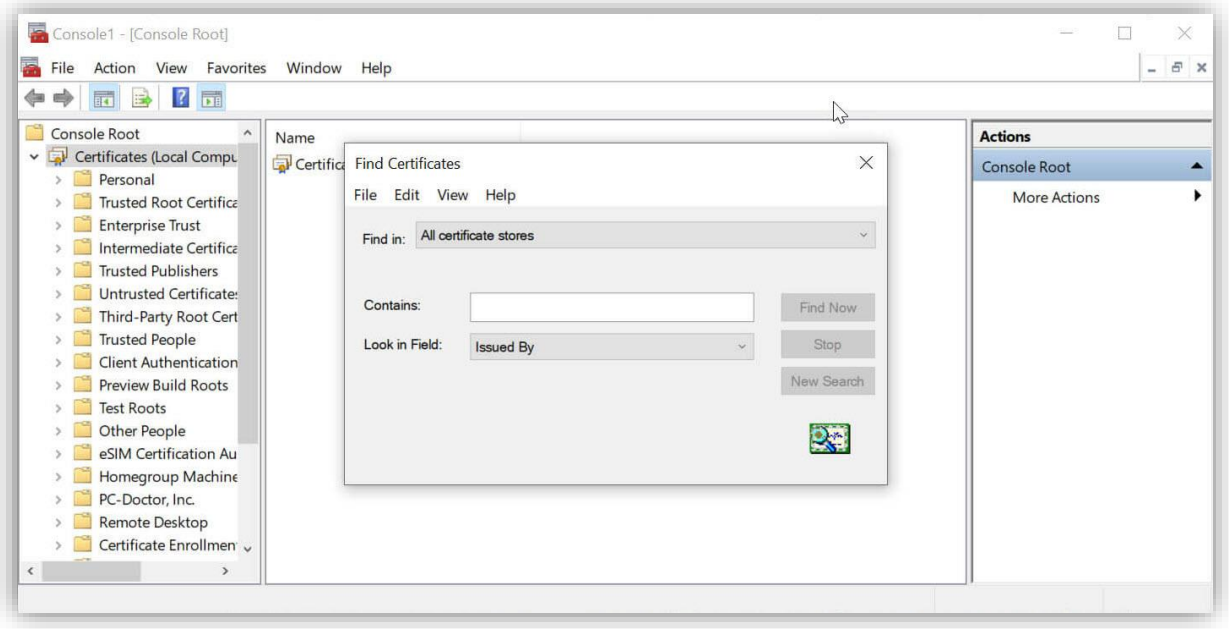
> *openssl genrsa -des3 -out server.key 2048*

b. **Generating Certificate Request**: Follow the below steps:
   i. Use the server's **Private Key** to create a certificate request. Enter the **Passphrase** for the key, **Common Name, Hostname** or **IP Address,** when prompted. For the **Common Name,** specify the **FQDN** of the SQL Server.

```
openssl req -new -key server.key -out server.csr
```

   ii. Once the certificate is generated, get it signed by a third-party CA such as VeriSign, Thawte, RapidSSL, etc, or self-sign it, based on your environment's requirement. For more details on submitting the CSRs, refer the corresponding CA's documentation/website. Remember, this is a paid service. In a few days, you will receive your signed SSL certificate and the CA's root certificate as **.cer** files.
   iii. Install the server certificate in the machine where the SQL server is running.
   iv. Install the CA root certificate in the PAM360 server.

c. **Installing the server certificate in the machine where the SQL server is running:** Use MMC
   i. Click **Start >> Run** in the machine where the SQL server is running. In the **Run** dialog box type **MMC**. The MMC console is displayed.
   ii. From the **Console** menu, click **Add/Remove Snap-in**. Click **Add** and then click **Certificates**. Click **Add** again. You will be prompted to open the **snap-in** for the current user account, the service account, or for the computer account. Select the **Computer Account**.
   iii. Select **Certificates (Local Computer) >> Personal >> Certificates.**
   iv. Right-click **Certificates** and click **All Tasks >> Import.**
   v. **Browse** and select the certificate to be installed.



d. **Installing the CA's root certificate in PAM360:**
   i. Copy the CA's root certificate and paste it under **<PAM360 Installation Folder >/bin** directory.
   ii. From **<PAM360 Installation Folder>/bin** directory, execute the following command:

```
importCert.bat <name of the root certificate pasted as explained above>
```

   iii. This adds the certificate to the PAM360 certificate store.

B) Creating a self-signed certificate using Powershell:

To create a self-signed certificate and use it, carry out the following steps in the machine where SQL server is installed:

1. Navigate to the **SQL Server** and open **Powershell** (run as Administrator).
2. Execute the following command:

```
New-SelfSignedCertificate -DnsName FQDN of the SQL server -CertStoreLocation cert:|LocalMachine|My
```

3. The above command will install and store a self-signed certificate in your local store.

2. Importing the SSL Certificate to PAM360

Follow the below steps:

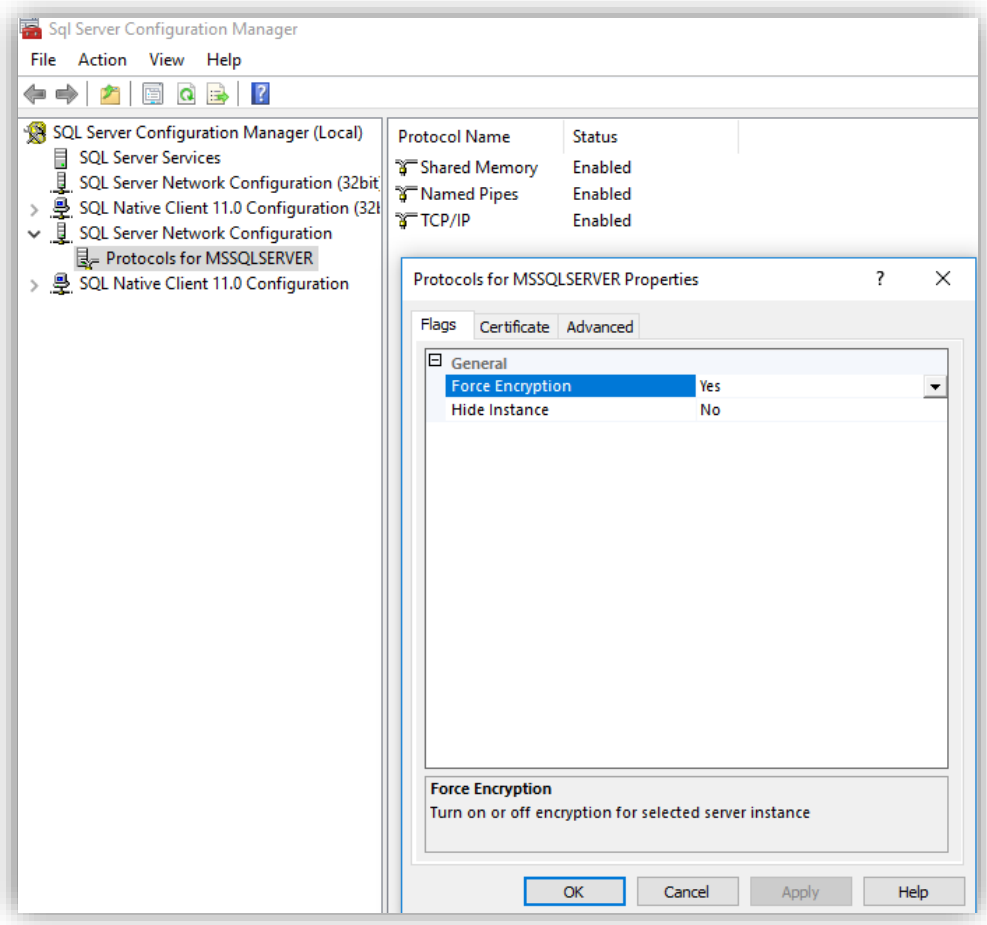
1. Copy the server certificate and paste it under the **<PAM360 Installation Folder>/bin** directory.
2. Execute the following command:

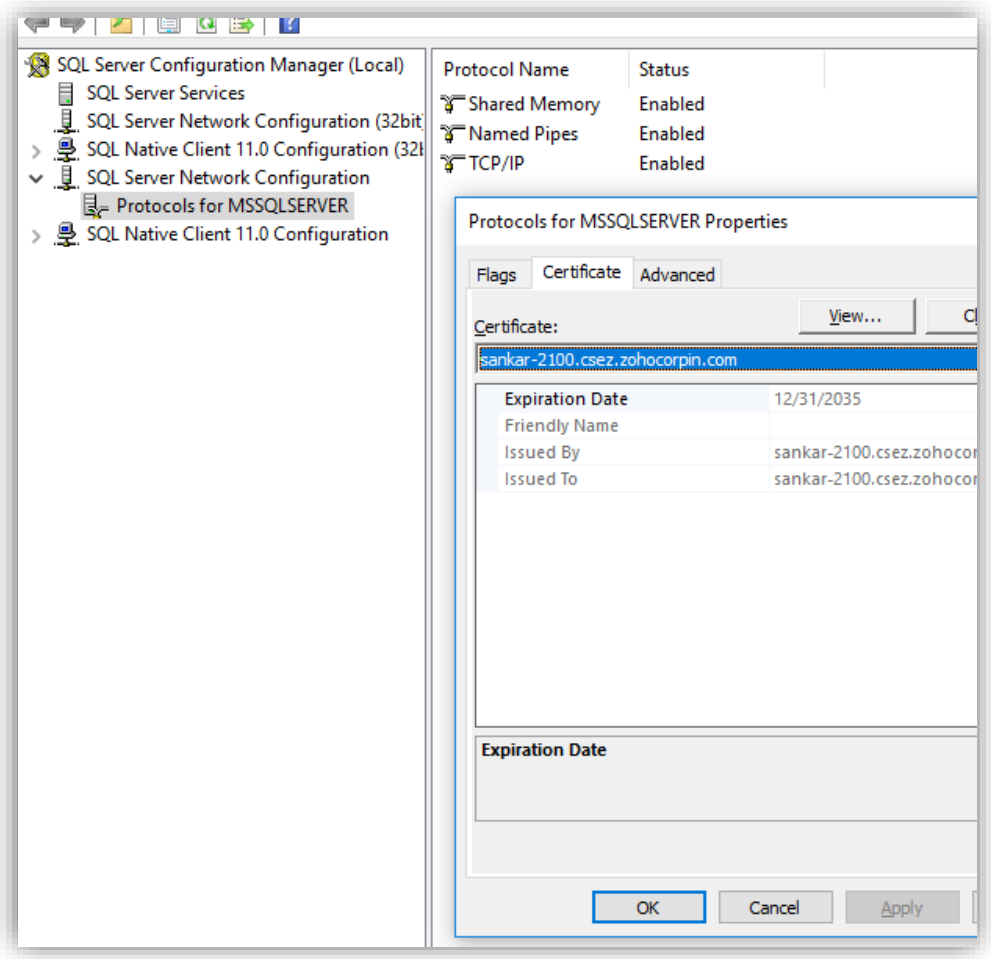
```
importCert.bat <name of the server certificate>
```

3. This adds the certificate to the PAM360 certificate store.

3. Enabling SSL Encryption in SQL Server

1. Click **Start** in the machine where the SQL server is running. From the Microsoft SQL Server program menu, click **Configuration Tools,** and then click **SQL Server Configuration Manager**.
2. Expand the SQL Server Network Configuration, right-click the **Protocols** for the server you want, and then click **Properties**. (Remember to click the Protocols for section in the left pane of the tool and not the specific Protocols in the right pane.)
3. On the **Certificate** tab, configure the **Database Engine** to use the certificate.
4. Set the **ForceEncryption** option for the Database Engine to **Yes**, so that all the client/server communication is encrypted and the clients that cannot support encryption are denied access **(recommended)**. Set the **ForceEncryption** option for the Database Engine to **No**, if you want the encryption to be requested by the client application **(not recommended)**.
5. Restart the SQL Server.


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32
SQL Server Network Configuration
Protocols for MSSQLSERVER
SQL Native Client 11.0 Configuration
Protocol Name
Status
Shared Memory
Enabled
Named Pipes
Enabled
TCP/IP
Enabled
Protocols for MSSQLSERVER Properties
Flags
Certificate
Advanced
General
Force Encryption
Yes
Hide Instance
No
Force Encryption
Turn on or off encryption for selected server instance
OK
Cancel
Apply
Help



For more details, refer to the section Configuring SSL for SQL Server in the Microsoft's knowledge base article.

4. Execute ChangeDB.bat in PAM360

Provide the details about the SQL server to PAM360 by editing the file **ChangeDB.bat (Windows)** or **ChangeDB.sh (Linux)**. Follow the below steps:

1. Navigate to the **<PAM360 Installation Folder>/bin** folder and execute the file **ChangeDB.bat** (Windows) or **sh ChangeDB.sh** (Linux).
2. In the window displayed, enter the below details:
    i. Select the **Server Type** as SQL Server.
    ii. **Host Name:** The name or the IP address of the machine, where the MS SQL server is installed.
    iii. **Instance Name:** Specify the named instance of the SQL server, to be used for PAM360. If the instance name is not specified, PAM360 will try establishing connection with the default instance on port **1433**.

Since PAM360 connects to MS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.

iv. **Database Name:** Name of the PAM360 database. Default is **PassTrix.** If you want to have a different database name, specify it here. PAM360 will take care of creating the Master Key, Symmetric Key, etc.

v. **Authentication:** The way by which you wish to connect to the SQL server. Choose **Windows**, if you are connecting to the SQL server from Windows. Make use of the **Windows Single Sign On** facility, provided the PAM360 service is running with a service account, which has the privilege to connect to the SQL server. Otherwise, select the option **SQL**.

It is recommended to choose the option **Windows**, as the Username and Password used for authentication are not stored anywhere.

vi. **User Name and Password:** If you have selected the option **SQL** in step v, specify the user name and password with which PAM360 can connect to the database.

The **User Name and Password** entered here will be stored in the **database_params.conf** file in PAM360. So, take care of hardening the host.
You can use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the **User Name** as **<domain-name>\<username>**.

vii. **Encryption Key:** The key to encrypt your data and store it in the SQL server. You may either leave it **Default** allowing PAM360 to generate a key. If you want to have

your custom key, select the option **Custom**.

If you have selected the option **Custom**, do the following:

Create Database >> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx
Create Master Key >> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx
Create Certificate >> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx
Create Symmetric Key >> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

viii. Provide the **Certificate Name** and **Symmetric Key Name** in the GUI.

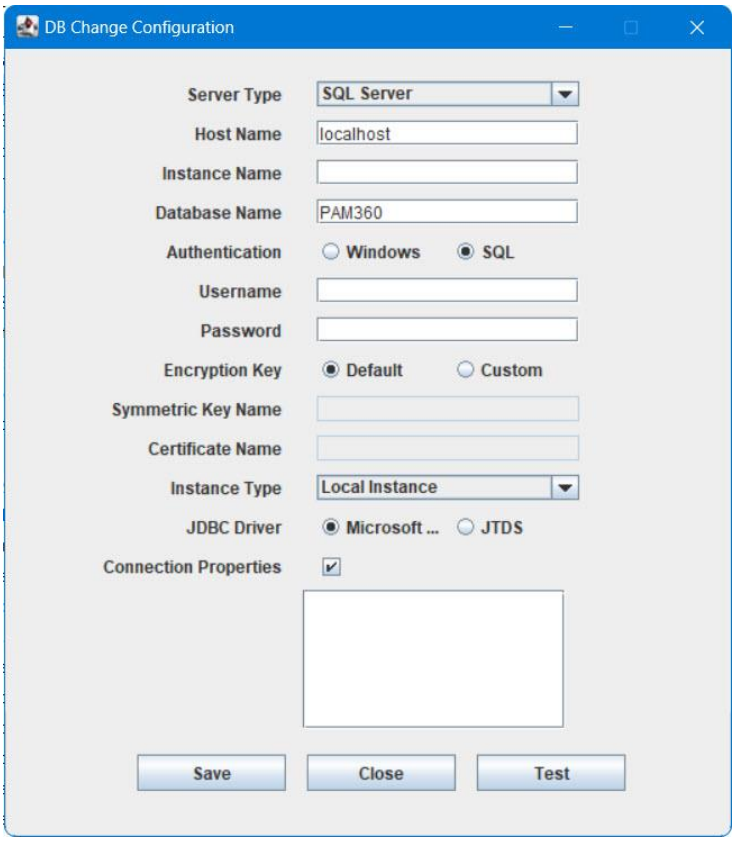
ix. **Instance Type:** PAM360 allows both 'Local Instance' (on-premise) and 'Azure SQL' as backend databases. Here, select 'Local Instance' as your instance type to continue with the DB change configuration.

x. **JDBC Driver:** The driver works seamlessly with the MS SQL server database. Microsoft (Recommended) is the default driver selected in the field and is recommended for most installations because it is compatible with the latest SQL server versions and features. The alternative JDBC driver available for selection is 'jTDS', which supports specific compatibility features.

xi. **Connection Properties:** After selecting this checkbox, you will have the option to specify custom connection properties in the following format: "key1=value1;key2=value2".

> **Note:** The existing server details in the DB migration setup window and properties, such as SSL and encrypt, cannot be added as custom connection properties.

xii. Finally, click **Test** to ensure that the connection settings are proper and then click **Save**.



IMPORTANT NOTES: After performing the above steps, navigate to the **<PAM360 Installation Folder>/conf** directory and move the masterkey.key file to a secure location. The SQL Server encrypts the data with a hierarchical encryption and key management infrastructure. Each layer encrypts the layer below it by using a combination of certificates, asymmetric keys, and symmetric keys. One among them is the Database Master Key, which in turn is created by the Service Master Key and a Password. This password is stored in PAM360 under the **<PAM360 Installation Folder>/conf** directory in a file named **masterkey.key.** It is highly recommended that you move the **masterkey.key** file to a secure location. This is to ensure data security. Take care to keep this key safe. You will require it while performing High Availability and Disaster Recovery. If you lose this key, you will have to configure MS SQL/Azure MS SQL server setup all over again.

For more details on encryption and key management in MS SQL, refer to this MSDN document.

Using MS SQL Cluster as the Backend Database

PAM360 allows you to use MS SQL cluster as backend database. The steps to configure PAM360 to use MS SQL cluster as backend are significantly different from using a standalone SQL server as the backend database because PAM360 has been configured to connect to SQL server cluster only through SSL to ensure high level of security.

To use a standalone SQL server as the backend database, the SSL certificate is created with the fully qualified DNS name of the SQL server and it imported in the LOCAL COMPUTER PERSONAL certificate store. In the SQL server configuration manager, the certificates matching the DNS name of the SQL server get listed in the certificate configuration screen. But, this procedure will not work in the case of SQL server cluster setup.

In the case of SQL server cluster, you need to obtain the server certificate with the fully qualified DNS name of the failover clustered instance and install it on all the nodes in the failover cluster. For example, assume that you have a two-node cluster with nodes named test1.yourcompany.com and test2.yourcompany.com and a failover clustered instance of SQL Server named pam360cluster. To use the cluster with PAM360, you need to obtain a certificate for pam360cluster.yourcompany.com and install the certificate on both nodes.

> **Note**: It is recommended to try these steps in a test setup first and verify if everything is working fine. You may download PAM360 and try using MS SQL cluster as backend.

To use **MSSQL Always-On failover cluster**, you need to add an entry in the **pam360_key.key** as instructed below:

```
ENCRYPTIONKEY=n2Z(-*zcPioHfYpmrQwrmICiXmiRUbhQ
MASTERKEY=s4X)6@ajSXCETRC
```

You can find the master encryption key in **masterkey.key** file which is placed under **<PAM360-Home>\conf directory.**

Using MS SQL Cluster as backend database involves the following topics:

1. **Enable SSL Encryption in SQL Server**
   - **1.1 Create an SSL Certificate and Install it in Windows Certificate Store**
   - **1.2 Generate the Certificate and get it Signed by a third-party CA (OR)**
   - **1.3 Create a Self-Signed Certificate**

2. Install the Server Certificate in all the Nodes where SQL Server is Running
3. Install the CA's Root Certificate/Server Certificate in PAM360
4. Enable SSL Encryption in all the Nodes where SQL Server is Running
5. Execute ChangeDB.bat

1. Enable SSL Encryption in SQL Server

1.1 Create an SSL Certificate and Install it in Windows Certificate Store (in the machine where SQL server is running)

Prior to trying to connect PAM360 with SQL server, you need to enable SSL encryption in SQL Server. You may create an SSL Certificate and get it signed by a Certificate Authority (CA) **OR** it could be self-signed.

> **Note**: The SQL certificate used for SQL cluster should contain the following attributes:
>
> **CN: cl-sql.example.com**
> **SAN:**
> **<li>sql-node1**
> **sql-node1.example.com**
> **sql-node2**
> **sql-node2.example.com**
> **sqlinstance**
> **sqlinstance.example.com**
> **
**

1.2 Generate the Certificate and get it Signed by a third-party CA

You can create the certificate using openssl and it involves two steps:

- Generating a private key
- Generating a certificate.

Use the following commands to create the certificate:

Generating a private key:

openssl genrsa -des3 -out server.key 2048

Generating a certificate:

Use the server private key to create a certificate request. Enter the passphrase for the key, Common Name, hostname or IP address when prompted:

openssl req -new -key server.key -out server.csr

Here, in the place of Common Name, specify the **FQDN** of the **SQL Server cluster instance**.

1. After generating the certificate, you need to get it signed by a third-party CA. Some of the prominent CAs are Verisign, Thawte, RapidSSL. Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA.
2. This process usually takes a few days' time and you will be returned your signed **server SSL certificate** and the **CA's root certificate** as .cer files.
3. The server certificate has to be installed in all the nodes where SQL server is running. The CA root certificate has to be installed in PAM360 server.

1.3 Create a Self-Signed Certificate

To create a self-signed certificate and use it, carry out the following steps **in one of the nodes where SQL server is installed:**

1.3.1 Create a self-signed certificate using Powershell:

1. Navigate to the **SQL Server** and open **Powershell** (run as Administrator).
2. Execute the following command:

   New-SelfSignedCertificate -DnsName FQDN of the SQL server -CertStoreLocation cert:\LocalMachine\My

3. The above command will install and store a self-signed certificate in your local store.

1.3.2 Exporting self-signed .pfx file:

1. Click **Start >> Run** (in the machine where SQL server is running). In the Run dialog box type **MMC**.
2. On the Console menu, click **Add/Remove Snap-in**. Click **Add >> Certificates**. Click **Add** again. You will be prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the **Computer Account**.
3. Select **Certificates (Local Computer) >> Personal >> Certificates**.
4. Locate the self-signed certificate just created, right click and export .pfx file.

1.3.3 Importing self-signed .pfx file in all the nodes where SQL server is running:

1. Click **Start >> Run** (in the machine where SQL server is running). In the Run dialog box type **MMC**.
2. On the Console menu, click **Add/Remove Snap-in**. Click **Add >> Certificates**. Click **Add**

again. You will be prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the Computer Account.

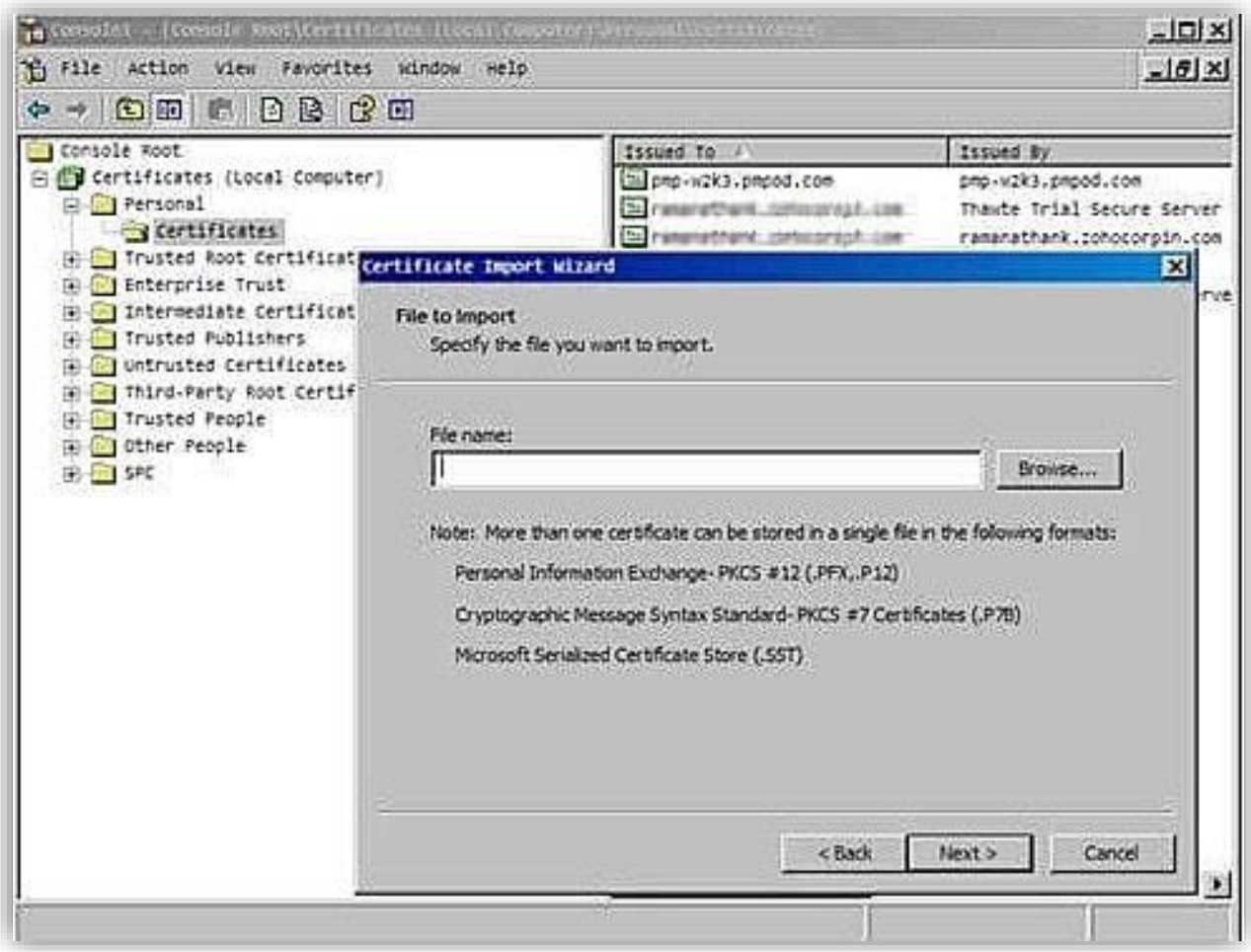
3. Select **Certificates (Local Computer) >> Personal >> Certificates**.
4. Right-click **Certificates >>** Click **All Tasks >> Import**.
5. Browse select the exported .pfx file certificate to be installed.

1.3.4 Install the server certificate in PAM360:

1. Copy the server certificate and paste it under **<PAM360 Installation Folder>/bin** directory.
2. From **<PAM360 Installation Folder&/bin** directory, execute the following command: importCert.bat **<name of the server certificate>**
3. This adds the certificate to the PAM360 certificate store.

2. Install the Server Certificate in all the Nodes where SQL Server is Running

1. Click **Start >> Run** (in the machine where SQL server is running). In the Run dialog box type **MMC**.
2. On the Console menu, click **Add/Remove Snap-in**. Click **Add >> Certificates**. Click **Add** again. You will be prompted to open the snap-in for the current user account, the service account, or for the computer account.
3. Select the **Computer Account**.
4. Select **Certificates (Local Computer) >> Personal >> Certificates**.
5. Right-click **Certificates >>** Click **All Tasks >> Import**.
6. **Browse** and select the certificate to be installed.



3. Install the CA's Root Certificate in PAM360

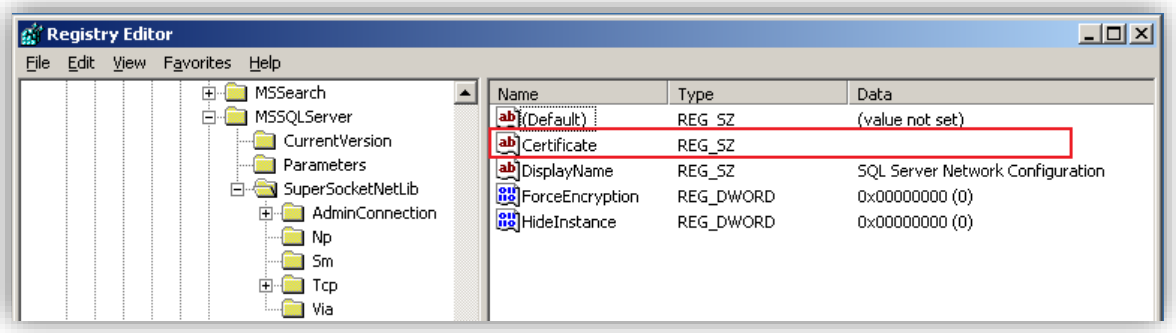
1. Copy the CA's root certificate and paste it under **<PAM360 Installation Folder >/bin** directory.
2. From **<PAM360 Installation Folder>/bin** directory, execute the following command: **importCert.bat <name of the root certificate pasted as explained above>**
3. This adds the certificate to the PAM360 certificate store.

4. Enable SSL Encryption in all the Nodes where SQL Server is Running

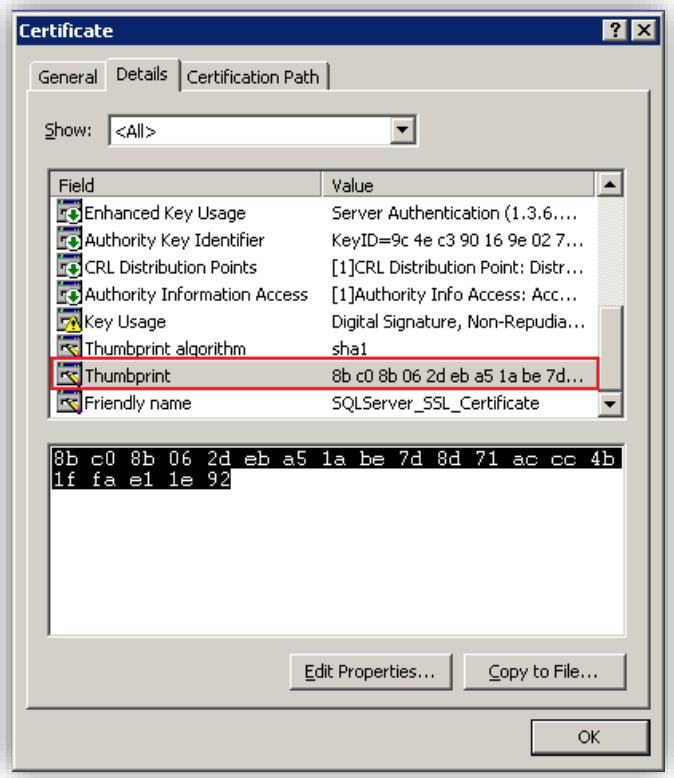
- The certificate used by SQL Server to encrypt connections is specified in the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\SuperSocketNetLib\Certificate

- This key contains a property of the certificate known as thumbprint that uniquely identifies each certificate in the server.

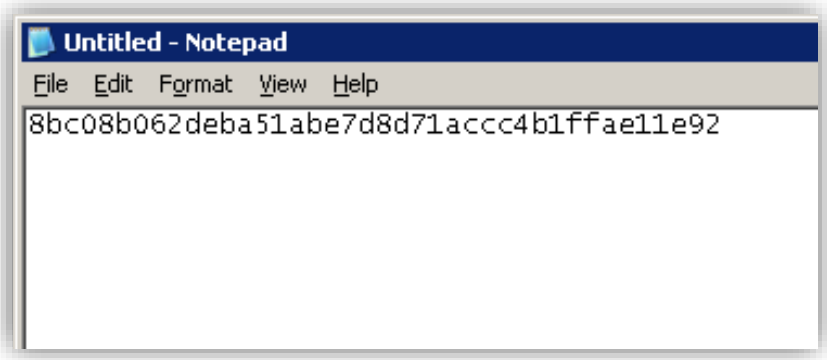


- The **Thumbprint** value from the certificate which is created using the above steps, should be copied and updated in the registry's certificate property.



For copying the thumbprint, follow the steps detailed below to copy it properly:

1. Eliminate the Unicode character from the thumbprint. You can do this by pasting the thumbprint in a notepad.



2. **Save** the notepad content as a different file in ANSI format which will prompt the following dialog, click **Ok** and proceed.



3. Then, open the ANSI format file and remove the **?** characters from the file.
4. Eliminate the spaces between characters in the thumbprint.
5. Save this thumbprint to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\Certificate property.**

5. Execute ChangeDB.bat

After completing the above steps, you need to execute **ChangeDB.bat** in PAM360. Refer to Step 1.1.4 in the section Using MS SQL Server as Backend of the help documentation for details.

Configuring PostgreSQL Cluster as the Backend Database

PostgreSQL is an advanced open-source RDBMS system with unique features, like fault-tolerant capabilities, scalability, stability, etc., designed to handle huge workloads. PAM360 already employs PostgreSQL as its default database, which comes bundled with the product.

Now, to increase the scalability on a large scale and improve the operations and functionality of the application, PAM360 allows users to configure the PostgreSQL cluster as a standalone external backend database.

At the end of this document, you will have learned about configuring the PostgreSQL cluster as the backend database.

Steps Required

1. Download and install PAM360 on the preferred machine/server.

   Note: Do not start the PAM360 service after the installation.

2. Download and install PostgreSQL.
3. Create a database cluster in the PostgreSQL provided with the database owner's permission.
4. Following the database cluster creation, ensure that the extension '**pgcrypto**' is available in the extension drop-down. If there is no such available extension, create it using the command - **CREATE EXTENSION pgcrypto;**
5. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** and open the file **pg_hba.conf**:
   i. Add an entry at the end with the IP address of the machine/server on which the PAM360 is running. E.g., **host all <user name> <ip address>/32 md5**

> **Note:** The above step applies only to users who use an external PostgreSQL enterprise database as their backend database. For users with cloud-based databases, the process will be performed in an automated process.

6. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** in Windows or **<PostgreSQL_Installation_folder>pgsql_installation\main** in Linux and open the file **postgresql.conf**:
   i. Search for listen_addresses and provide the IP address of the server where PAM360 is running.
1. Restart the PostgreSQL server.
2. Navigate to **<PAM360_Installation_folder>\conf** and open the file **customer-config.xml**:
   i. Search for **startdbserver= true** and change its value to **false**.
   ii. Now, save and close the file **customer-config.xml**.
3. Navigate to **<PAM360_Installation_folder>\conf** and open the file **database_param.conf**.
   i. Replace **localhost** with the listener name of the server where the PostgreSQL database cluster is running.
   ii. Change the **port number** to the actual port number of the PostgreSQL cluster in the database. By default, the initial port number for the PostgreSQL will be **5432**.
   iii. Update the **username** and **password**.
   iv. Update the database name as provided while creating the cluster.
   v. Update the **db.password.encrypted** to **false**.
   vi. Now, save and close the file **database_param.conf**.

> **Notes:** The password given here will be in plain text at that instance and will be encrypted from the next consequent occurrence.

4. Download the root CA certificate of the PostgreSQL database cluster.
5. If you are unaware of creating an SSL for the PostgreSQL database, follow the steps below to generate the required SSL certificates and validate the SSL connection.
6. Now, import the root CA certificate of the file PostgreSQL database cluster into PAM360.
7. Start the PAM360 service.

Now, you have successfully configured the PostgreSQL cluster as the backend database.

SSL Generation for PostgreSQL Cluster

An SSL connection is required for a secured connection between the PostgreSQL database cluster and the PAM360 application. To establish the SSL connection, the root CA of the PostgreSQL database cluster is required.

The following steps educate you on creating the required SSL certificates for the PostgreSQL database cluster and verify the SSL configuration of the PostgreSQL database cluster.

a. Creating a Self-Signed Root CA for the PostgreSQL Database Cluster

1. Navigate to **<PostgreSQL Installation Directory>\data** where the certificates are to be created and open the command prompt as an administrator to proceed with the following steps to create an SSL root CA for the PostgreSQL database cluster.
2. Execute the command - **openssl genrsa -passout pass:1111 -des3 -out rootca.key 4096** (where **'pass:1111'** is the PEM pass phrase and **'rootca.key'** is the trust certificate key)
3. Execute the command - **openssl req -passin pass:1111 -new -x509 -days 365 -key rootca.key -out rootca.crt**
4. Enter the required certificate details accordingly to create a root certificate. E.g, The common name as the server name and the SAN name with the server IP address.
5. Execute the command - **openssl genrsa -passout pass:1111 -des3 -out server.key 4096** (where **'pass:1111'** is the PEM pass phrase and **'server.key'** is the trust certificate key)
6. Execute the command - **openssl req -passin pass:1111 -new -key server.key -out server.csr**
7. Enter the required certificate details accordingly to create a server certificate. E.g, The common name as the server name and the SAN name with the server IP address.
8. Execute the command - **openssl x509 -req -passin pass:1111 -days 365 -in server.csr -CA rootca.crt - CAkey rootca.key -set_serial 01 -out server.crt**

Notes:

1. Upon execution of the above command, the **server.csr** will be signed with the **rootca.crt**. To trust the certificates issued, add the rootca.crt to the respective trust store on the server.
2. You can also name the private keys, certificates and csr on your own as needed.

Note: If you are about to use a wildcard certificate for the PostgreSQL database, place the wildcard certificate along with the respective private key file in the **<PostgreSQL Installation Directory>\data** directory path.

b. Configuring the PostgreSQL Database Cluster to use the SSL

1. Navigate to **<PostgreSQL Installation Directory>\data** and open the **postgresql.conf** file with the administrator privilege.
2. Look out for the **listen_addresses** under the connection settings and edit/verify the parameter **listen_addresses**, as this allows connection from the external hosts.

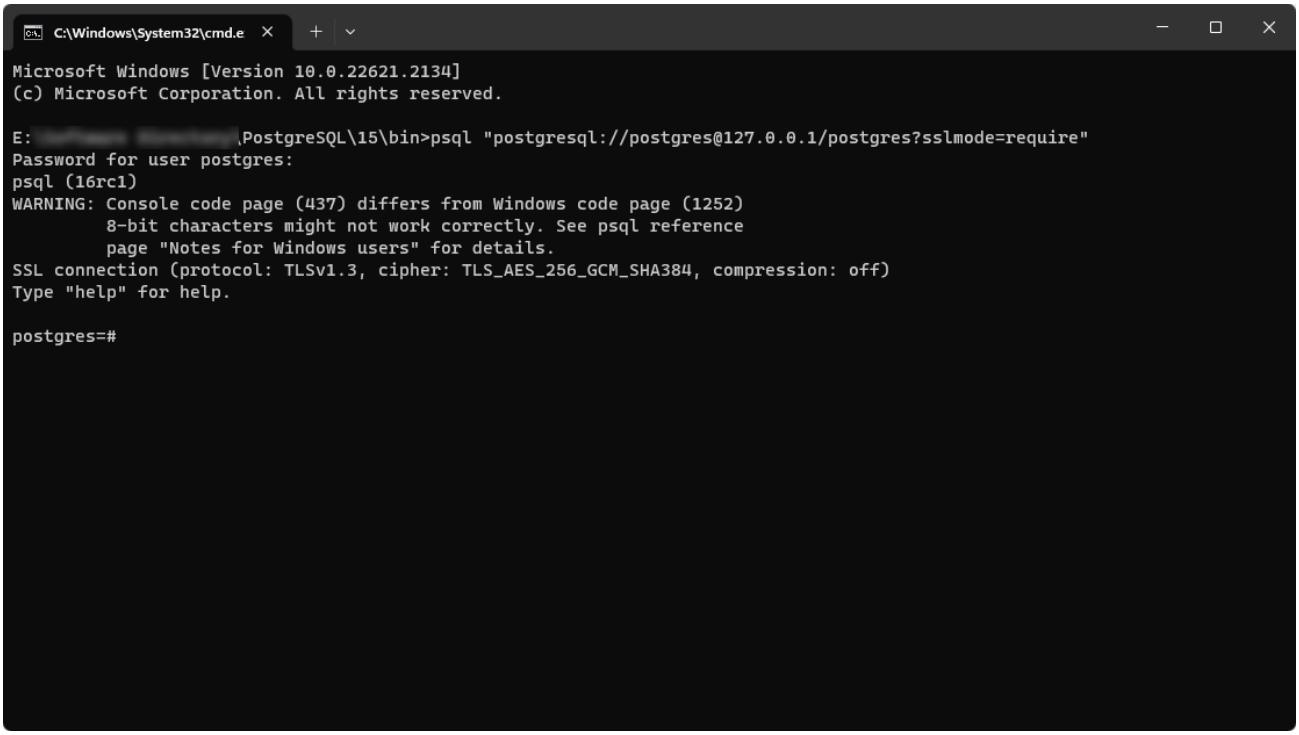
```
listen_addresses = '*'
```

3. Search for the **SSL** section in the **postgresql.conf** and uncomment all the SSL parameters.
4. Now, edit the SSL parameters with our certificate information as shown below.

```
ssl = on
ssl_ca_file = 'rootca.crt'
ssl_cert_file = 'server.crt'
ssl_crl_file = ''
ssl_crl_dir = ''
ssl_key_file = 'server.key'
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
ssl_prefer_server_ciphers = on
ssl_ecdh_curve = 'prime256v1'
ssl_min_protocol_version = 'TLSv1.2'
ssl_max_protocol_version = ''
ssl_dh_params_file = ''
ssl_passphrase_command = ''
ssl_passphrase_command_supports_reload = off
```

Note: If you are using a wildcard certificate for the PostgreSQL database, update the ssl_ca_file parameter with no attribute (ssl_ca_file='').

5. Now, restart the PostgreSQL database for the changes to get in effect.
6. To validate the SSL connection configuration, navigate to **<PostgreSQL Installation Directory>\bin** and open the command prompt with the administrator privilege.
7. Execute the command - **psql "postgresql://username@hostname/dbname?sslmode=require"** Replace username, hostname, and dbname with your PostgreSQL cluster details.
   For example, **psql "postgresql://postgres@127.0.0.1/postgres?sslmode=require"**
8. Now, enter the PostgreSQL database password that you have entered during the PostgreSQL database installation.
9. Upon entering the password, you will be prompted with the below message for the successful SSL connection.



10. Now, navigate to **<PostgreSQL Installation Directory>\data** and use the **rootca.cert** to import it into PAM360.

Using Azure MS SQL as the Backend Database

PAM360 uses PostgreSQL as the default backend database, and it comes bundled with the product. However, you can configure the product with other database servers such as PostgreSQL, MS SQL (both standalone and cluster), and Azure MS SQL. Here in this document, you will learn how to set up other compatible database servers as the backend database for your installation.

Here, in this document, you will learn about the following topics:

1. **Creating the SSL Certificate and Installing it in the Windows Certificate Store**
2. **Importing the SSL Certificate to PAM360**
3. **Enabling SSL Encryption in SQL Server**
4. **Executing ChangeDB.bat in PAM360**

> **Note:** To ensure high level of security, PAM360 has been configured to connect to the SQL server only through **SSL**.

1. Creating the SSL Certificate and Installing it in the Windows Certificate Store

(in the machine where SQL server is running)

Prior to connecting PAM360 with the SQL server, you need to enable SSL encryption in the SQL Server. For this, you need to create an SSL Certificate and get it signed by either a Certificate Authority (CA) or self-sign it (See more).

A) Generating the certificate and getting it signed by a third-party CA:

Create the certificate using **openssl.** This involves two steps - **generating private key** and **generating certificate request**. Use the following commands to create the certificate.

a. **Generating Private Key:** Execute the following command:

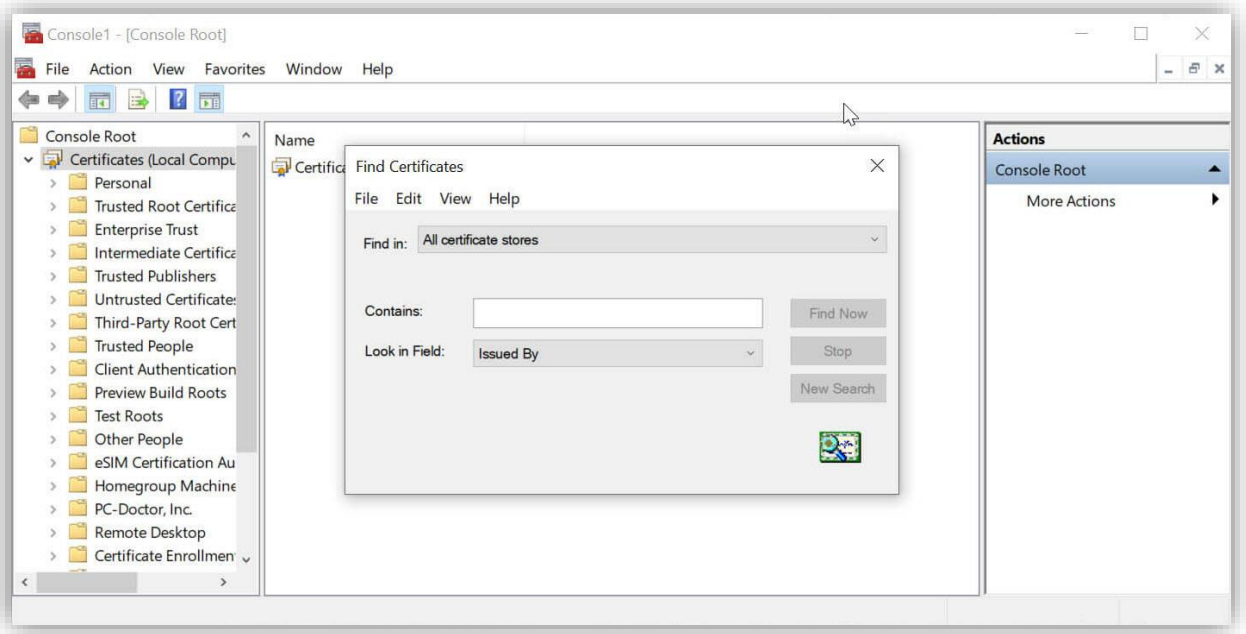
b. Generating Certificate Request: Follow the below steps:

i. Use the server's **Private Key** to create a certificate request. Enter the **Passphrase** for the key, **Common Name, Hostname** or **IP Address,** when prompted. For the **Common Name,** specify the **FQDN** of the SQL Server.

ii. Once the certificate is generated, get it signed by a third-party CA such as VeriSign, Thawte, RapidSSL, etc, or self-sign it, based on your environment's requirement. For more details on submitting the CSRs, refer the corresponding CA's documentation/website. Remember, this is a paid service. In a few days, you will receive your signed SSL certificate and the CA's root certificate as **.cer** files.
iii. Install the server certificate in the machine where the SQL server is running.
iv. Install the CA root certificate in the PAM360 server.

c. Installing the server certificate in the machine where the SQL server is running: Use MMC

i. Click **Start >> Run** in the machine where the SQL server is running. In the **Run** dialog box type **MMC**. The MMC console is displayed.
ii. From the **Console** menu, click **Add/Remove Snap-in**. Click **Add** and then click **Certificates**. Click **Add** again. You will be prompted to open the **snap-in** for the current user account, the service account, or for the computer account. Select the **Computer Account**.
iii. Select **Certificates (Local Computer) >> Personal >> Certificates.**
iv. Right-click **Certificates** and click **All Tasks >> Import.**
v. **Browse** and select the certificate to be installed.



d. Installing the CA's root certificate in PAM360:

i. Copy the CA's root certificate and paste it under **<PAM360 Installation Folder >/bin** directory.

ii. From **<PAM360 Installation Folder>/bin** directory, execute the following command:

```
importCert.bat <name of the root certificate pasted as explained above>
```

iii. This adds the certificate to the PAM360 certificate store.

B) Creating a self-signed certificate using Powershell:

To create a self-signed certificate and use it, carry out the following steps in the machine where SQL server is installed:

1. Navigate to the **SQL Server** and open **Powershell** (run as Administrator).
2. Execute the following command:

```
New-SelfSignedCertificate -DnsName FQDN of the SQL server -
CertStoreLocation cert:|LocalMachine|My
```

3. The above command will install and store a self-signed certificate in your local store.

2. Importing the SSL Certificate to PAM360

Follow the below steps:

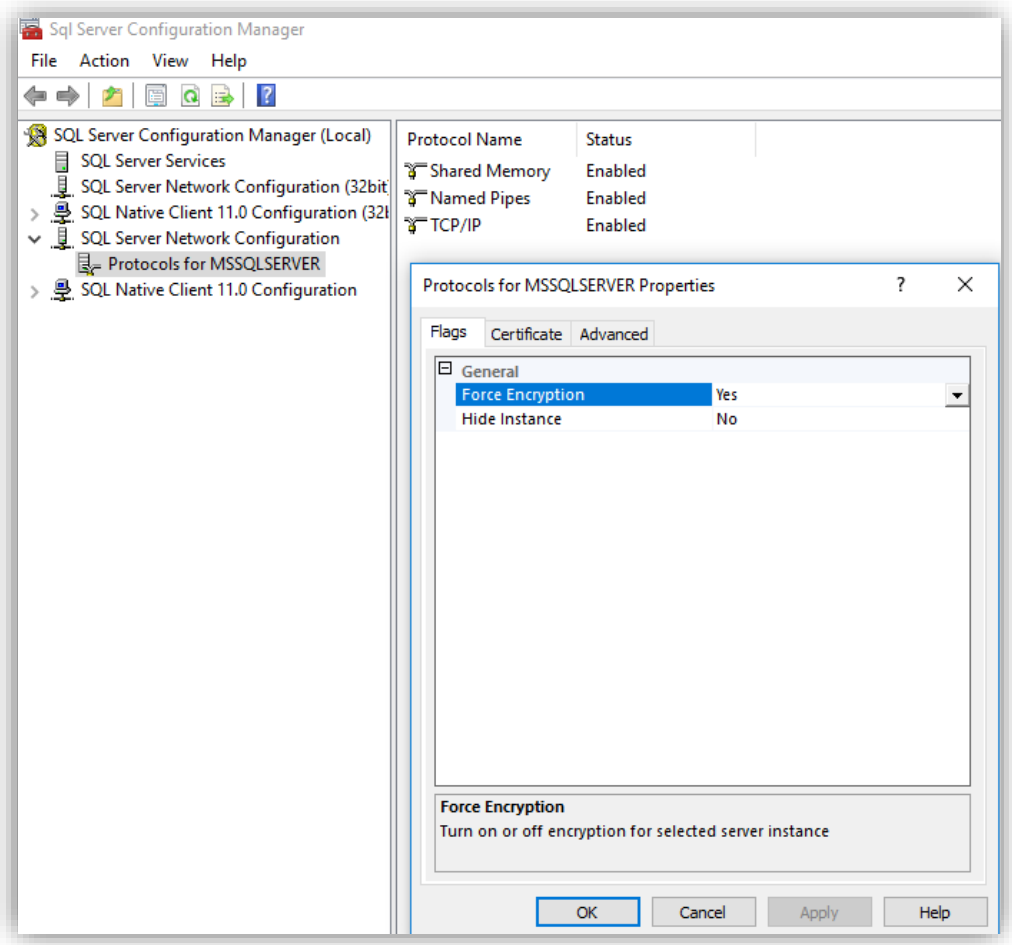
1. Copy the server certificate and paste it under the **<PAM360 Installation Folder>/bin** directory.
2. Execute the following command:

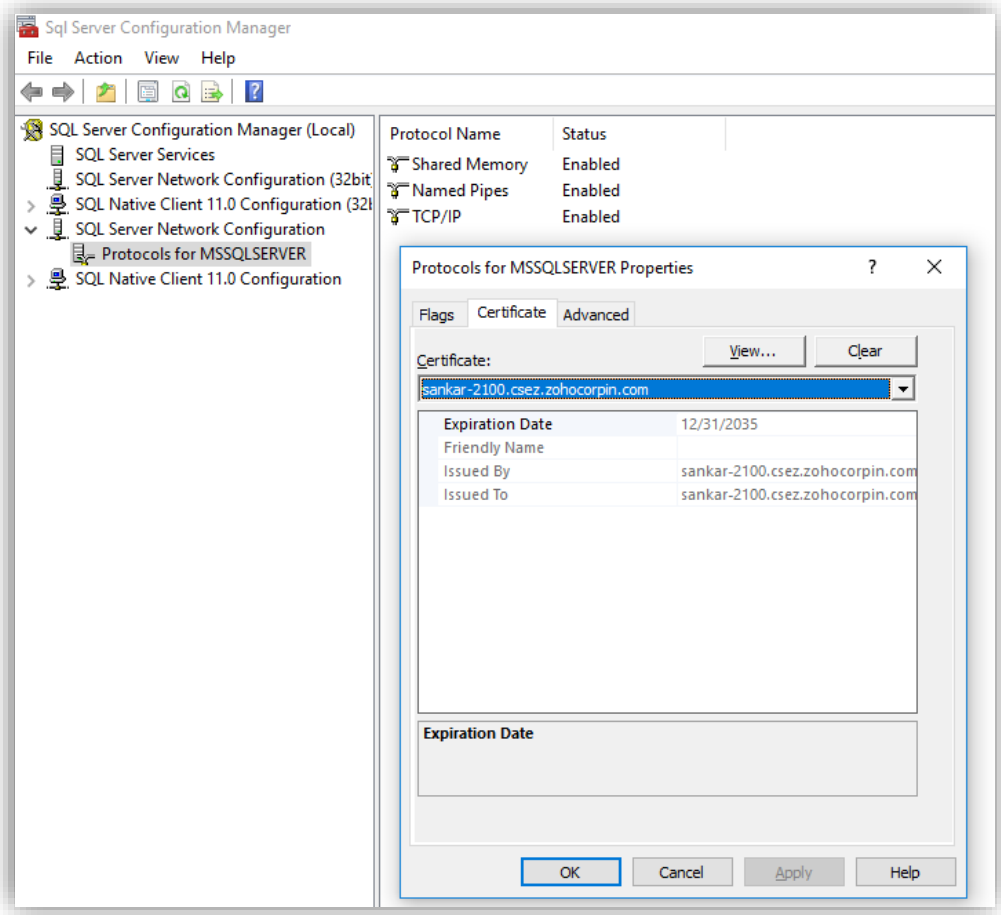
   ```
   importCert.bat <name of the server certificate>
   ```

3. This adds the certificate to the PAM360 certificate store.

3. Enabling SSL Encryption in SQL Server

1. Click **Start** in the machine where the SQL server is running. From the Microsoft SQL Server program menu, click **Configuration Tools,** and then click **SQL Server Configuration Manager**.
2. Expand the SQL Server Network Configuration, right-click the **Protocols** for the server you want, and then click **Properties**. (Remember to click the Protocols for section in the left pane of the tool and not the specific Protocols in the right pane.)
3. On the **Certificate** tab, configure the **Database Engine** to use the certificate.
4. Set the **ForceEncryption** option for the Database Engine to **Yes**, so that all the client/server communication is encrypted and the clients that cannot support encryption are denied access **(recommended)**. Set the **ForceEncryption** option for the Database Engine to **No**, if you want the encryption to be requested by the client application **(not recommended)**.
5. Restart the SQL Server.


Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32
SQL Server Network Configuration
Protocols for MSSQLSERVER
SQL Native Client 11.0 Configuration
Protocol Name
Status
Shared Memory
Enabled
Named Pipes
Enabled
TCP/IP
Enabled
Protocols for MSSQLSERVER Properties
Flags
Certificate
Advanced
General
Force Encryption
Yes
Hide Instance
No
Force Encryption
Turn on or off encryption for selected server instance
OK
Cancel
Apply
Help



For more details, refer to the section Configuring SSL for SQL Server in the Microsoft's knowledge base article.

4. Executing ChangeDB.bat in PAM360

Provide the details about the SQL server to PAM360 by editing the file **ChangeDB.bat (Windows)** or **ChangeDB.sh (Linux)**. Follow the below steps:

1. Navigate to the **<PAM360 Installation Folder>/bin** folder and execute the file **ChangeDB.bat** (Windows) or **sh ChangeDB.sh** (Linux).
2. In the window displayed, enter the below details:
    i. Select the **Server Type** as SQL Server.
    ii. **Host Name:** The name or the IP address of the machine, where the MS SQL server is installed.
    iii. **Instance Name:** Specify the named instance of the SQL server, to be used for PAM360. If the instance name is not specified, PAM360 will try establishing connection with the default instance on port **1433**.

Since PAM360 connects to MS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.

iv. **Database Name:** Name of the PAM360 database. Default is **PassTrix.** If you want to have a different database name, specify it here. PAM360 will take care of creating the Master Key, Symmetric Key, etc.

v. **Authentication:** The way by which you wish to connect to the SQL server. Choose **Windows**, if you are connecting to the SQL server from Windows. Make use of the **Windows Single Sign On** facility, provided the PAM360 service is running with a service account, which has the privilege to connect to the SQL server. Otherwise, select the option **SQL**.

It is recommended to choose the option **Windows**, as the Username and Password used for authentication are not stored anywhere.

vi. **User Name and Password:** If you have selected the option **SQL** in step v, specify the user name and password with which PAM360 can connect to the database.

The **User Name and Password** entered here will be stored in the **database_params.conf** file in PAM360. So, take care of hardening the host.
You can use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the **User Name** as **<domain-name>\<username>.**

vii. **Encryption Key:** The key to encrypt your data and store it in the SQL server. You may either leave it **Default** allowing PAM360 to generate a key. If you want to have your custom key, select the option **Custom**.

If you have selected the option **Custom**, do the following:

Create Database -> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx
Create Master Key -> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx
Create Certificate -> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx
Create Symmetric Key -> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

viii. Provide the **Certificate Name** and **Symmetric Key Name** in the GUI.

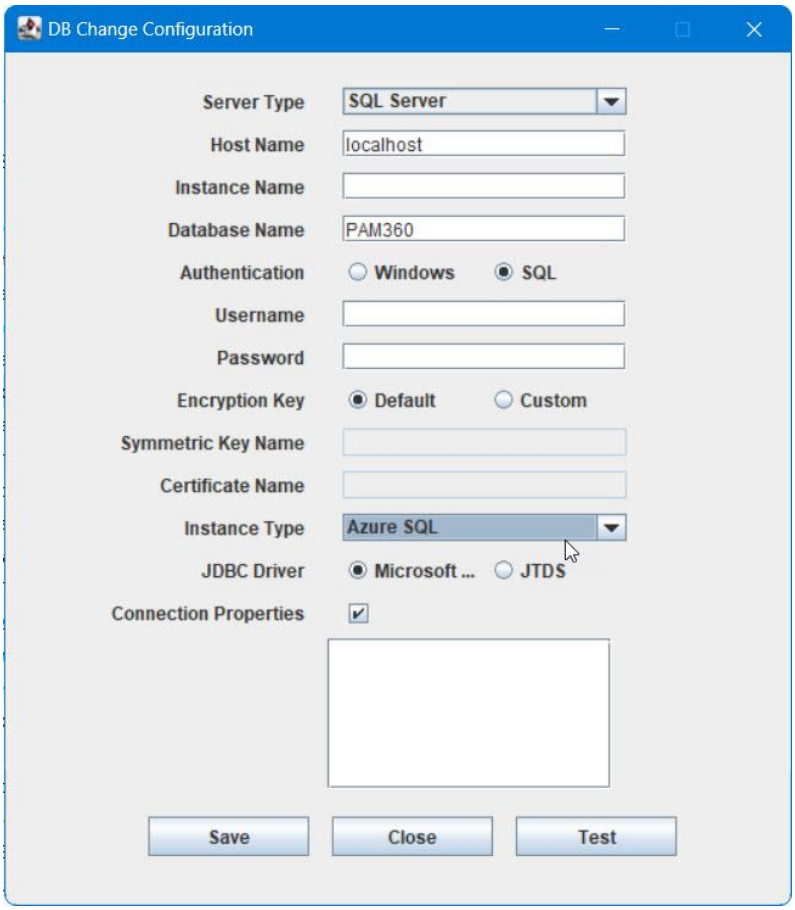
ix. **Instance Type:** PAM360 allows both 'Local Instance' (on-premise) and 'Azure SQL' as backend databases. Here, select 'Azure SQL' as your instance type to continue with the DB change configuration.

x. **JDBC Driver:** The driver works seamlessly with the MS SQL server database. Microsoft (Recommended) is the default driver selected in the field and is recommended for most installations because it is compatible with the latest SQL server versions and features. The alternative JDBC driver available for selection is 'jTDS', which supports specific compatibility features.

xi. **Connection Properties:** After selecting this checkbox, you will have the option to specify custom connection properties in the following format: **"key1=value1;key2=value2"**.

> **Note:** The existing server details in the DB migration setup window and properties, such as SSL and encrypt, cannot be added as custom connection properties.

xii. Finally, click **Test** to ensure that the connection settings are proper and then click **Save**.



IMPORTANT NOTES: After performing the above steps, navigate to the **<PAM360 Installation Folder>/conf** directory and move the masterkey.key file to a secure location. The SQL Server encrypts the data with a hierarchical encryption and key management infrastructure. Each layer encrypts the layer below it by using a combination of certificates, asymmetric keys, and symmetric keys. One among them is the Database Master Key, which in turn is created by the Service Master Key and a Password. This password is stored in PAM360 under the **<PAM360 Installation Folder>/conf** directory in a file named **masterkey.key**. It is highly recommended that you move the **masterkey.key** file to a secure location. This is to ensure data security. Take care to keep this key safe. You will require it while performing High Availability and Disaster Recovery. If you lose this key, you will have to configure MS SQL/Azure MS SQL server setup all over again.

For more details on encryption and key management in Azure MS SQL, refer to the MSDN document.

Configuring Amazon RDS MS SQL as the Backend Database

PAM360, by default, comes bundled with PostgreSQL as the backend database. However, PAM360 allows you to configure different databases to cater to your needs. In addition to configuring various databases, PAM360 allows you to migrate all your data from your local MS SQL database to the Amazon RDS MS SQL database.

This document explains in detail the steps to configure Amazon RDS MS SQL, an on-demanding service in the backend database.

Steps Required

1. **Downloading the Root Certificate and Importing it to PAM360**
2. **Executing ChangeDB.bat in PAM360**

> **Note**: To ensure high level of security, PAM360 has been configured to connect to the Amazon RDS MSSQL only through **SSL**.

1. Downloading the Root Certificate and Importing it to PAM360

1. Download Amazon RDS root CA *(.pem)* based on the AWS region.
2. Copy the server certificate and paste it under the **<PAM360 Installation Folder>/bin** directory.
3. Execute the following command:

> *importCert.bat <name of the RDS root certificate>*

4. This adds the certificate to the PAM360 certificate store.

2. Execute ChangeDB.bat in PAM360

Provide the details about the Amazon RDS SQL server to PAM360 by editing the file **ChangeDB.bat (Windows)** or **ChangeDB.sh (Linux)**. Follow the below steps:

1. Navigate to the **<PAM360 Installation Folder>/bin** folder and execute the file **ChangeDB.bat** (Windows) or **sh ChangeDB.sh** (Linux).
2. In the window displayed, enter the below details:
   i. Select the **Server Type** as Amazon RDS SQL Server.
   ii. **Host Name:** The name or the IP address of the machine, where the Amazon RDS SQL server is installed.
   iii. **Instance Name:** Specify the named instance of the Amazon RDS SQL server, to be used for PAM360. If the instance name is not specified, PAM360 will try establishing connection with the default instance on port **1433**.

> Since PAM360 connects to Amazon RDS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.

   iv. **Database Name:** Name of the PAM360 database. Default is **PAM360.** If you want to have a different database name, specify it here. PAM360 will take care of creating the Master Key, Symmetric Key, etc.
   v. **Authentication:** The way by which you wish to connect to the Amazon RDS SQL server. Choose **Windows**, if you are connecting to the Amazon RDS SQL server from Windows. Make use of the **Windows Single Sign On** facility, provided the PAM360 service is running with a service account, which has the privilege to connect to the Amazon RDS SQL server. Otherwise, select the option **SQL**.

> It is recommended to choose the option **Windows**, as the Username and Password used for authentication are not stored anywhere.

   vi. **User Name and Password:** If you have selected the option **SQL** in step v, specify the user name and password with which PAM360 can connect to the database.

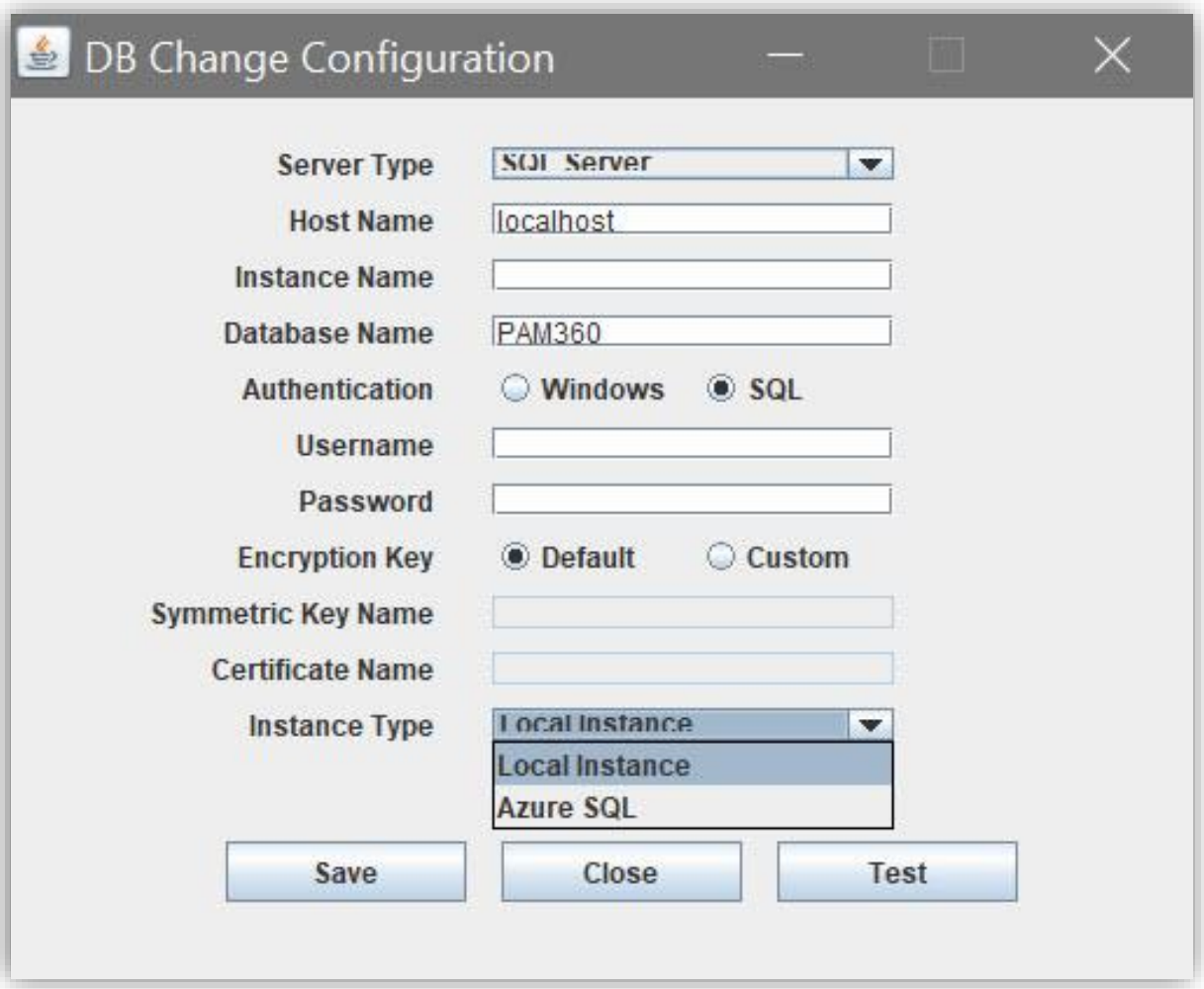
The **User Name and Password** entered here will be stored in the **database_params.conf** file in PAM360. So, take care of hardening the host.
You can use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the **User Name** as **<domain-name>\<username>**.

vii. **Encryption Key:** The key to encrypt your data and store it in the Amazon RDS SQL server. You may either leave it **Default** allowing PAM360 to generate a key. If you want to have your custom key, select the option **Custom**.

If you have selected the option **Custom**, do the following:

Create Database >> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx
Create Master Key >> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx
Create Certificate >> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx
Create Symmetric Key >> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

viii. Provide the **Certificate Name** and **Symmetric Key Name** in the GUI.
ix. Select the **Instance Type** as **Local Instance.**
x. Finally, click **Test** to ensure that the connection settings are proper and then click **Save.**



IMPORTANT NOTES: After performing the above steps, navigate to the **<PAM360 Installation Folder>/conf** directory and move the **masterkey.key** file to a secure location. The SQL Server encrypts the data with a hierarchical encryption and key management infrastructure. Each layer encrypts the layer below it by using a combination of certificates, asymmetric keys, and symmetric keys. One among them is the Database Master Key, which in turn is created by the Service Master Key and a Password. This password is stored in PAM360 under the **<PAM360 Installation Folder>/conf** directory in a file named **masterkey.key**. It is highly recommended that you move the **masterkey.key** file to a secure location. This is to ensure data security. Take care to keep this key safe. You will require it while performing High Availability and Disaster Recovery. If you lose this key, you will have to configure MS SQL/Azure MS SQL server setup all over again.

Now, you have successfully configured Amazon RDS MSSQL as the backend database.

Configuring Amazon RDS PostgreSQL as the Backend Database

PAM360 allows users to configure Amazon RDS PostgreSQL as the backend database. Amazon RDS is an open sourced, fully managed relational database. Amazon RDS comes with a set of features such as easy and managed deployments, dynamic scaling, automated backups, etc.

Here, in this document, you will learn how to configure the Amazon RDS PostgreSQL as the backend database.

Steps Required

1. Download and install PAM360 in a AWS EC2 instance.
2. Create an RDS PostgreSQL database in AWS.
3. Now, make a copy of the below files under **<PAM360_Installation_folder>\conf** directory and rename them:
    - **customer-config.xml** to **customer-config_old.xml.**
    - **database_params.conf** to **database_params_old.conf.**
4. Open **database_param.conf** file.
    - Replace **localhost** with the hostname of the PostgreSQL server running in AWS.
    - Change the **port number** to the actual port number of the PostgreSQL instance in AWS.
    - Set **SSL=true** and provide the user details that were used to restore the dump file to the database.
    - Give the user details that were created while database creation in RDS/ Create a new user in RDS and add it to the super user group.
5. Open **customer-config.xml** and search for **startdbserver= true** and change its value to **false.**
6. Download Amazon RDS root CA *(.pem)* based on the AWS region.
7. Import the root .pem file into PAM360. Refer to the help section **How do I import a root certificate into PAM360?** to know more information.
8. Start the PAM360 service.

You have successfully configured Amazon RDS PostgreSQL Database as the backend database.

Managing the PAM360 Database Password

Apart from AES encryption, the PAM360 database is secured using a separate password, which is auto-generated and unique for every installation. The password for the database can be stored securely in PAM360 itself. There is also an option to store the password at some other secure location, accessible by the PAM360 server.

By default, the database password is stored under **<PAM360 Installation Folder>/conf/database_params.conf**. If you choose to manage the database password by yourself, store the configuration file somewhere securely and instruct the location of the file to PAM360. Follow the below steps:

Steps Required

- **If you are starting PAM360 as service**, navigate to **<<PAM360 Installation Folder>/conf/wrapper.conf** (in Windows) / **<PAM360 Installation Folder>/conf/wrapper_lin.conf** (in Linux) and edit the following entry under "Java Additional Parameters"

  wrapper.java.additional.9=-Ddatabaseparams.file=<full path of the database_params.conf file location>

- **If you are starting PAM360 from command line or through the tray icon**, edit the file **system_properties.conf** present in **<PAM360 Installation Folder>/conf** directory. In this file, edit the following entry under "**Splash Screen default Properties**"

  databaseparams.file=<full path of database_params.conf file>

  Notes:

  - If you misplace the conf file or lose it, PAM360 will not start. So, take care to save it in a secure location.
  - Enclose the full path of **database_params.conf** file in double-quotes. Eg. databaseparams.file="**C:\Program Files\Manage Engine\PAM360\conf\database_params.conf**".

Migrating from PostgreSQL Database to MS SQL / Azure MS SQL Database

ManageEngine \PAM360 supports the following databases: **PostgreSQL, MS SQL and Azure MS SQL**, where PostgreSQL comes bundled with the product, by default. In general, there are various reasons to migrate from one database to another which include performance issues, stability, reliability, High Availability issues, costs for the license (dual license, GPL), etc.

This document walks you through the process of migrating your data from the **PostgreSQL** database to the **MS SQL/Azure MS SQL** databases.

Steps Required

1. **Prerequisites**
2. **Migrating Data from PostgreSQL to MS SQL / Azure MS SQL**
3. **Re-importing Personal Passwords**

1. Prerequisites

1. This section guides you through only the migration process and does not include any database configuration aspects. Hence, if you have decided to use MS SQL/Azure MS SQL as the dedicated backend database, make sure you have already completed these steps under MS SQL/Azure MS SQL Configuration before you begin the migration.
2. Before commencing the migration, ensure the following aspects are taken care of:
    i. **Personal Password Management:** If users in your organization have used the **Personal Password Management** option in PAM360 by specifying their own passwords (which are NOT stored in PAM360), those personal passwords will not be migrated as a part of data migration. You need to use the **Export Passwords** option in the **Personal Passwords** section for the same.
    ii. **Bundled Database Only:** The migration can be carried out only if your current PAM360 installation uses the database bundled with the product (PostgreSQL). This procedure DOES NOT apply if you are using any other external database.

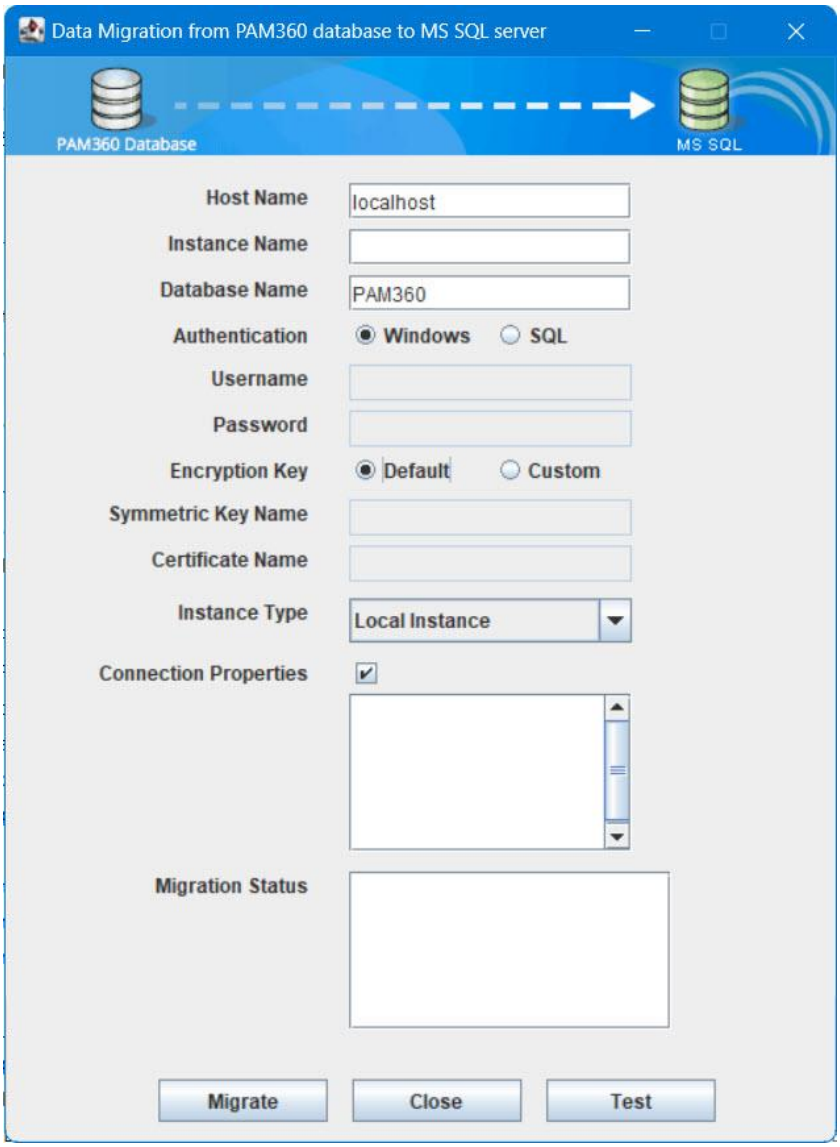
iii. Before initiating the migration, take a complete back up of the existing PAM360 setup. This will be helpful if the migration is unsuccessful.

3. If you have PAM360 installed in a Linux environment, do the steps that follow to migrate data from PostgreSQL to MS SQL/Azure MS SQL database:
   i. Install the respective XRDP based on your Linux operating system.
   ii. Post the XRDP installation, take a remote session to the Linux environment using the native Remote Desktop Connection or any other third-party application from a Windows or Windows Domain resource.
   iii. Enter the username and password of your Linux environment. Ensure that you use the Xvnc module as the session type.

   Now you can manage your Linux environment graphically to execute the below operations for migration.

2. Migrating Data from PostgreSQL to MS SQL/Azure MS SQL

1. Shutdown the PAM360 server and ensure that **PostgreSQL** is not running.
2. Navigate to **<PAM360 Installation Folder>/bin** folder and execute the file **MigrateDB.bat** (Windows) or **sh MigrateDB.sh** (Linux). In the window that pops up, choose the option **Go to Migration Set Up.**
3. In the pop-up that opens, read the **Best Practices Guide** first by clicking the **'Open the best practices document'** button and then click the **'Continue with migration setup'** button to proceed with the migration process.



4. In the pop-up that appears, enter the following details:

   i. **Host Name:** The name or the IP address of the machine where SQL server is installed.

   ii. **Instance Name:** The named instance of SQL server used by PAM360. If the instance name is not specified, PAM360 will try establishing connection with the default instance on port **1433.**

   Since PAM360 connects to MS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.

   iii. **Database Name:** Name of the PAM360 database. If you want to have a different database name, you may specify here. PAM360 will create the Master Key, Symmetric Key etc. If the Database name is not specified, PAM360 will create a database with the name **PassTrix**.

iv. **Authentication:** The way to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single-Sign-On facility, provided the PAM360 service is running with a service account, which has the privilege to connect to the SQL server. In this case, choose the option **Windows**. Otherwise, select the option **SQL**. (It is recommended to choose **Windows**, as the username and password used for authentication are not stored anywhere).

v. **User Name and Password:** If you have selected the option **SQL**, specify the user name and password with which PAM360 connects to the database. [The username and password entered here will be stored in the **database_params.conf** file in PAM360. So, you need to take care of hardening the host].
You can also use your Windows login credentials if you are connecting to the database from Windows. In this case, enter the username as **<domain-name>\<username>.**

vi. **Encryption Key:** The key with which your data is to be encrypted and stored in the SQL server. You may either leave it as **Default**, allowing PAM360 to generate a key, or you can select **Custom.**

vii. If you choose **Custom**, you need to create a new database, create Master Key, create Certificate (this will be certificate name) and Create the Symmetric Key using AES 256 encryption. Follow the below steps:

Create Database >> For details, refer to http://msdn.microsoft.com/en-us/library/aa258257(v=sql.80).aspx
Create Master Key >> For details, refer to http://technet.microsoft.com/en-us/library/ms174382.aspx
Create Certificate >> For details, refer to http://msdn.microsoft.com/en-us/library/ms187798.aspx
Create Symmetric Key >> For details, refer to http://msdn.microsoft.com/en-us/library/ms188357.aspx

viii. Enter the **Certificate Name** and **Symmetric Key Name** in the GUI.

ix. **Instance Type:** PAM360 allows both **'Local Instance'** (on-premise) and **'Azure SQL'** as backend databases. Select either one of them to continue with the DB migration process.

x. **Connection Properties:** After selecting this checkbox, you will have the option to specify custom connection properties in the following format: **"key1=value1;key2=value2;"**.

> **Note:** The existing server details in the DB migration setup window and properties, such as SSL and encrypt, cannot be added as custom connection properties.

xi. Now, mention the **Migration Status** and click **Test** to verify the connection settings.

xii. Click **Migrate**.

5. The status of data migration will be displayed in the textbox. Once the migration is complete, start the PAM360 server.

3. Re-importing Personal Passwords

In general, PAM360 does not allow the migration of personal passwords. Hence, before data migration, personal passwords need to be exported out of PAM360 in the form of an XLS file. Once the migration process is over, the passwords can be re-imported into PAM360.

Troubleshooting Tips

Error	Cause	Effect	Solution
Server seems to be running. Shutdown PAM360 server and try again.	You might have attempted the database migration when the PAM360 server is running,	You will encounter this error in the DB Migration GUI and the GUI will remain open.	Shut down the server and try again. If the error repeats, delete the **.lock** file under the **<PAM360-Installation-Folder>/bin** folder and then try again. If the issue persists, contact PAM360 support with the "**.lock**" file.

> **Important Note:**
>
> After completing the migration, start the PAM360 server and navigate to Admin >> Resource Config >> Resource Additional Fields and Admin >> Resource Config >> Accounts Additional Fields. Open the GUI and click Save. This will restore the additional fields added by you in the migrated instance as well.

Migrating Data from Local MS SQL to Microsoft Azure SQL Database

PAM360 allows you to use Microsoft Azure SQL, a cloud database provided as a part of Microsoft Azure, as a backend database. Migrate all your existing data from the local MS SQL database to the Microsoft Azure SQL database to benefit from a fully-managed database service.

Advantages

The foremost advantage of using a cloud database is that it can be accessed anytime from anywhere as it runs on the Cloud computing platform. Microsoft Azure, an intelligent database as a service and powered by AI, learns your workload patterns and optimizes automatically, thereby resulting in cost optimization. It is a competent database service with salient features, such as built-in availability SLA, dynamic scaling, automatic performance, etc.

This document explains in detail the process of migrating your data from the local Microsoft SQL database to the Azure Microsoft SQL database in PAM360.

Steps Required

The process of migrating data from Local MS SQL to Microsoft Azure SQL database involves three steps. The first step is to transfer the data from the local MS SQL database to the Microsoft Azure SQL database. Next, encrypt the data uploaded to the Microsoft Azure SQL database. Then, the final step is to import an SSL certificate into the PAM360 server.

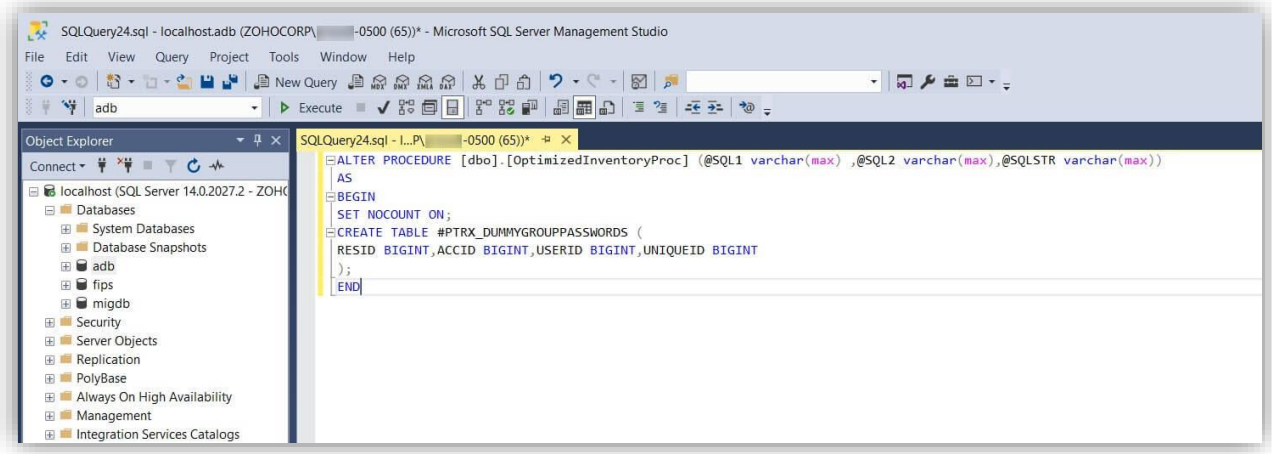
In this help section, you will have learned the following:

1. Migrating Local MS SQL Data
2. Encrypting Azure Database
3. Importing SSL Certificate

1. Migrating Local MSSQL Database

1. Open the **SQL Management Studio** and select local MSSQL Database and execute the below queries:

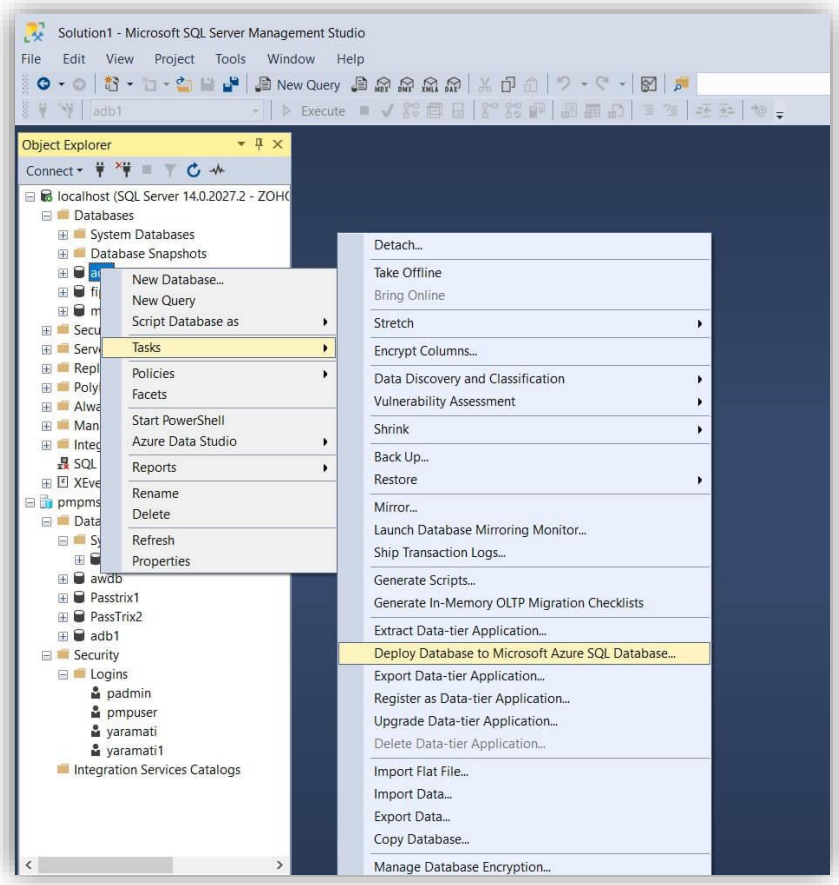
```
ALTER PROCEDURE [dbo].[OptimizedInventoryProc] (@SQL1 varchar(max)
,@SQL2 varchar(max),@SQLSTR varchar(max)) AS BEGIN SET NOCOUNT
ON; CREATE TABLE #PTRX_DUMMYGROUPPASSWORDS ( RESID
BIGINT,ACCID BIGINT,USERID BIGINT,UNIQUEID BIGINT ); END
```



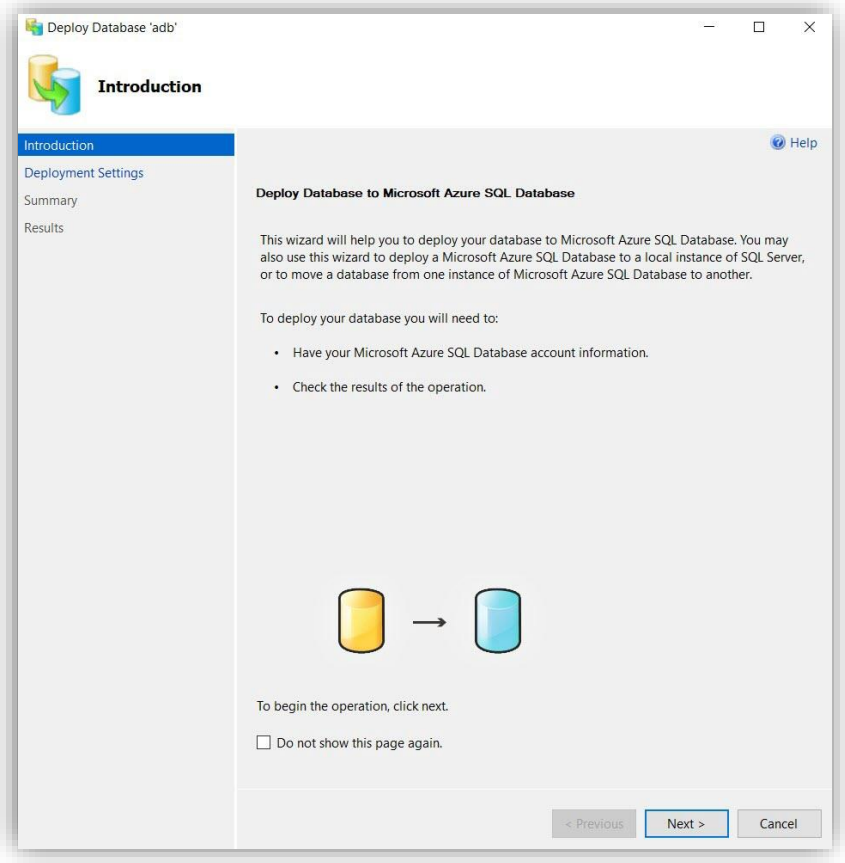

```
ALTER PROCEDURE [dbo].[PasswordActionNotificationProc] (@SQL1
varchar(max),@SQL2 varchar(max)) AS BEGIN SET NOCOUNT ON; DECLARE
@SQl VARCHAR(MAX) EXEC(@SQL2) EXEC(@SQL1) SET @SQL ='SELECT
TOP 1 * from Ptrx_DummyGroupNotification' EXEC(@SQL) SET NOCOUNT
OFF; END
```

```
DROP SYMMETRIC KEY PMP_SYM_KEY DROP CERTIFICATE PMP_CERT DROP
MASTER KEY
```

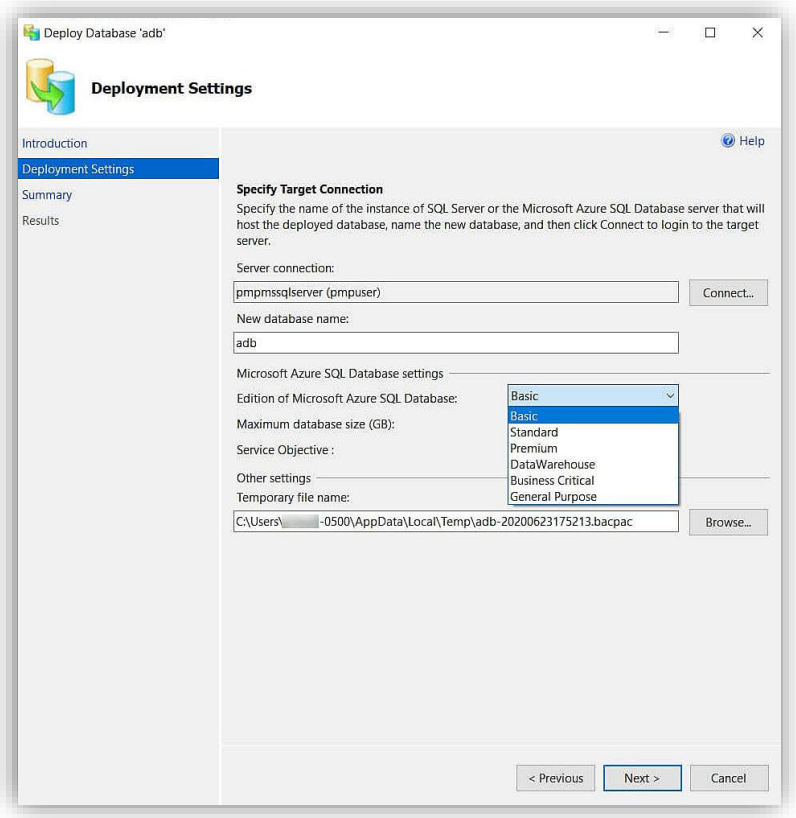
2. Now, right click the database and navigate to **Task >> Deploy Database to Microsoft Azure SQL Database.**



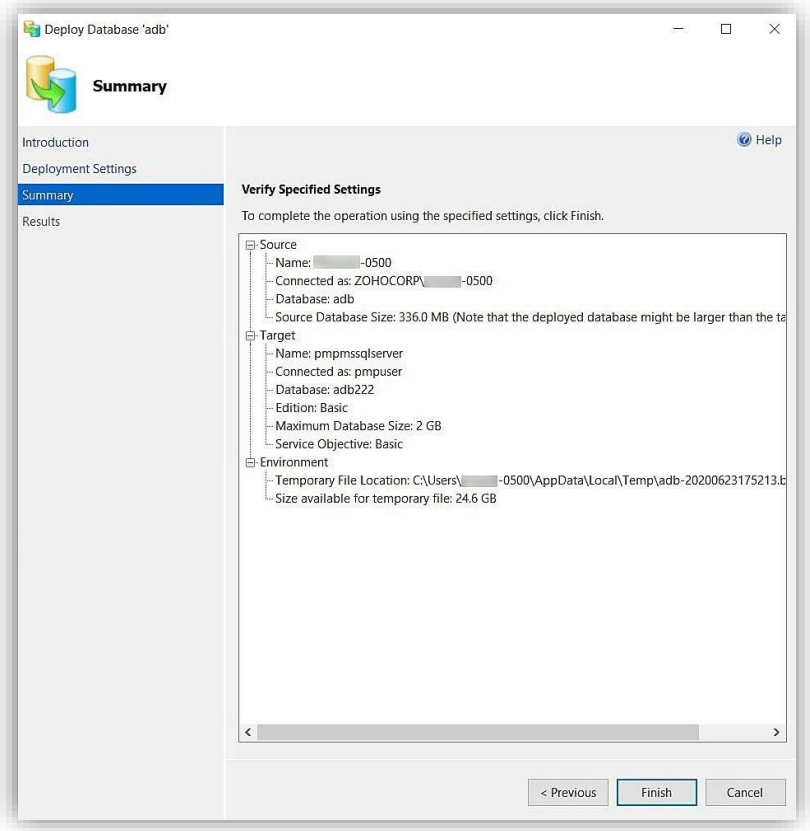
3. Click **Next** in the dialog box that appears.



4. Mention the required details and click **Next.**



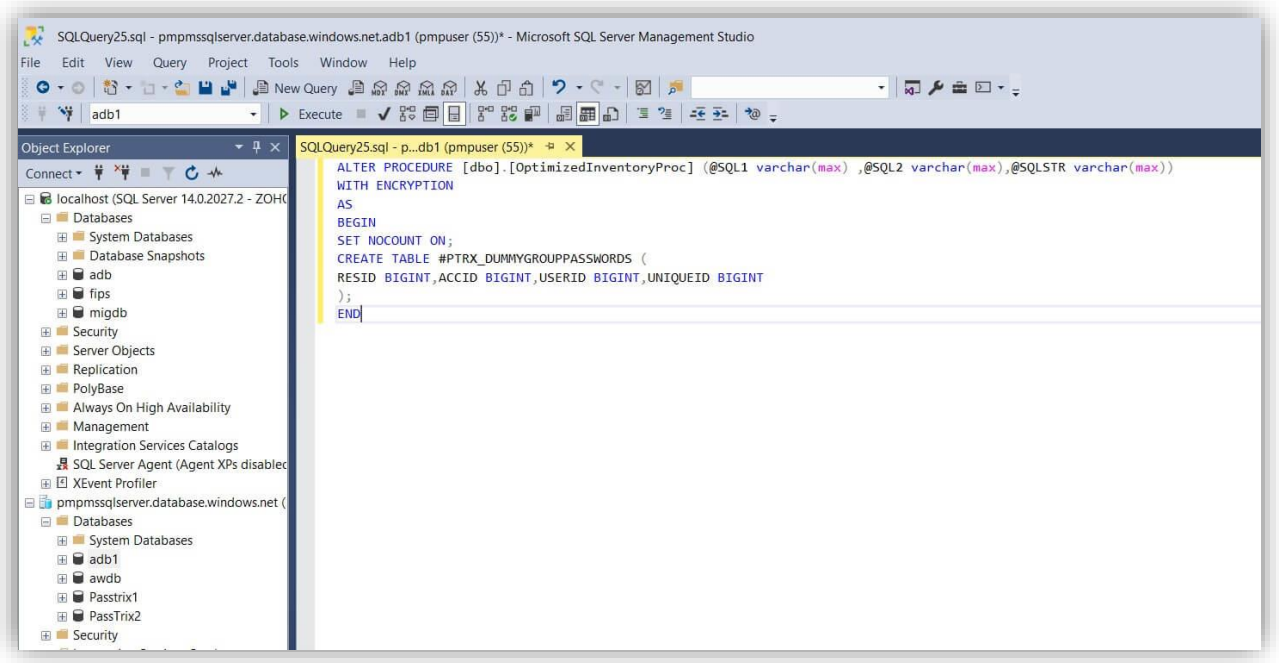
5. Click **Finish.**



2. Encrypting Azure Database

1. Now, in **SQL Management Studio**, connect the database to Azure and execute the following queries:

```
ALTER PROCEDURE [dbo].[OptimizedInventoryProc] (@SQL1 varchar(max)
,@SQL2 varchar(max),@SQLSTR varchar(max)) WITH ENCRYPTION AS BEGIN
SET NOCOUNT ON; CREATE TABLE #PTRX_DUMMYGROUPPASSWORDS (
RESID BIGINT,ACCID BIGINT,USERID BIGINT,UNIQUEID BIGINT ); END
```



ALTER PROCEDURE [dbo].[PasswordActionNotificationProc] (@SQL1 varchar(max),@SQL2 varchar(max)) WITH ENCRYPTION AS BEGIN SET NOCOUNT ON; DECLARE @Sql VARCHAR(MAX) EXEC(@SQL2) EXEC(@SQL1) SET @SQL ='SELECT TOP 1 * from Ptrx_DummyGroupNotification' EXEC(@SQL) SET NOCOUNT OFF; END

CREATE MASTER KEY ENCRYPTION BY PASSWORD='<Password in masterkey.key file>' CREATE CERTIFICATE PMP_CERT WITH SUBJECT='Created by ManageEngine'; CREATE SYMMETRIC KEY PMP_SYM_KEY WITH ALGORITHM = AES_256, KEY_SOURCE = 'ZOHO_Key_Source', IDENTITY_VALUE = 'ZOHO_Identity_Value' ENCRYPTION BY CERTIFICATE PMP_CERT; OPEN SYMMETRIC KEY PMP_SYM_KEY DECRYPTION BY CERTIFICATE PMP_CERT;

2. Open **database_params.conf** file from the conf folder and replace the **<%DNS_NAME%>** with Microsoft Azure SQL instance url and also modify the **username** and **password**.

3. Importing SSL Certificate

In Windows:

Download the Azure Portal's certificate from browser and import **mycertfile.cer** using the command **importCert.sh/bat.**

In Linux:

1. Download the Azure Portal's certificate from the browser or create a certificate by executing the following command:

```
openssl s_client -showcerts -connect <%DNS_NAME%>:443 </dev/null
2>/dev/null|openssl x509 -outform PEM >mycertfile.cer
```

2. Import **mycertfile.cer** using the command **importCert.sh/bat.**

You have successfully migrated from Local MSSQL Database to Microsoft Azure SQL Database. Now, Start the PAM360 server and connect to the PAM360 web client to retrieve the passwords.

Migrating Data from Local MS SQL to Amazon RDS MS SQL Database

PAM360 allows you to use Amazon RDS MS SQL as a backend database. Amazon RDS makes it simple and easy to set-up a relational database in the cloud. You can migrate all your data from the local MS SQL database to Amazon RDS MS SQL database with ease.

Advantages

The main advantage of using a cloud database is that you will be able to access it from any part of the world at any given time. Amazon's RDS MS SQL database has some great set of features such as dynamic scaling, single click high availability, automated backups, etc. You can also create DB instances and DB snapshots, point-in-time restores, and automated or manual backups with Amazon RDS.

This document explains in detail the process of migrating your data from the local MS SQL database to the Amazon RDS MS SQL database in PAM360.

Steps Required

Steps to migrate local MS SQL data to Amazon RDS MS SQL data are as follows:

1. Create a S3 bucket and store the Local SQL backup (.bak) file.
2. Navigate to **RDS >> Option Groups >> Add Options** and create a **RDS Option** named as **SQLSERVER_BACKUP_RESTORE.**
3. Leave the **IAM Role** field as default.
4. Modify the **RDS Instance** and change the **Database Options >> Option Group** to the newly created **SQLSERVER_BACKUP_RESTORE.**
5. Click **Apply changes immediately** to save the DB changes.
6. Connect RDS SQL Instance through EC2 windows instance and execute the following rds_restore_database stored procedure to Restore DB:

   exec msdb.dbo.rds_restore_database

@restore_db_name='database_name',
@s3_arn_to_restore_from='arn:aws:s3:::bucket_name/file_name.extension';

7. Execute the following query after a successful restoration:

   use write_the_name_of the restored_database;
   OPEN MASTER KEY DECRYPTION BY PASSWORD='type_the_master_key_password';

8. Now, rename the below files under **PAM360\conf** directory:
   - **wrapper.conf** to **wrapper.conf_old**
   - **wrapper_lin.conf** to **wrapper_lin.conf_old**
   - **wrapper_lin.conf** to **wrapper_lin.conf_old**
   - **wrapper_lin.conf_mssql** to **wrapper_lin.conf**
   - **pam360_key.key** to **pam360_key.key_old**
   - **database_params.conf** to **database_params.conf_old**
   - **customer-config.xml** to **customer-config.xml_old**
   - **customer-config.xml_mssql** to **customer-config.xml**
9. Replace the **masterkey.key** and **pam360_key.key** files from local instance to the EC2 instance.
10. Download and replace the below files under **PAM360\conf** directory.
    - customer-config.xml
    - database_params.conf
    - masterkey.key
11. Open **database_param.conf** file.
    - Replace **<%DNS_NAME%>** with MS SQL instance name.
    - Replace **<database name>** with the encrypted database name.
    - Replace **Username** and **Password.**
    - **change.db.password.encrypted=false**
12. Download MS SQL root CA.
13. Import a **.pem** file into PAM360 using the following command:
    i. Open command prompt and navigate to **<PAM360_Home>\jre\bin.**

ii. Execute the following command:

'keytool.exe -import -v -alias <alias name> -file <certificate path> -keystore ..\lib\security\cacerts -keypass changeit -storepass changeit -noprompt'

14. Start the PAM360 service.

You have successfully migrated data from Local MS SQL Database to Amazon RDS MS SQL Database.

Migrating Data from Local PostgreSQL to Amazon RDS PostgreSQL Database

PAM360 comes bundled with PostgreSQL that will function as your local backend database. However, PAM360 also allows you to convert your on-premise database into an on-demand service using Amazon RDS. With this, you can migrate all your data from the local PostgreSQL database to the Amazon RDS PostgreSQL database with ease.

Advantages

Amazon RDS provides a high level of security for your PostgreSQL databases. Amazon RDS comes with a set of features such as easy and managed deployments, dynamic scaling, enhanced availability and durability, enhanced monitoring, automated backups, etc. The automated or manual backup feature of Amazon RDS enables point-in-time recovery of your PostgreSQL database instance.

This document explains in detail the process of migrating your data from the local PostgreSQL database to the Amazon RDS PostgreSQL database in PAM360.

Steps Required

Steps to migrate data from bundled PostgreSQL to Amazon RDS PostgreSQL are as follows:

1. Open the Command Prompt and navigate to the **<PAM360_Installation_folder>\pgsql\bin** directory.
2. Create a dump file using the following command:

   pg_dump dbname > pam360.sql

   Example: *pg_dump.exe -U postgres -h 147.0.0.1 -p 2345 -W PassTrix > pam360.sql*
3. Create an Amazon RDS instance and a master user.
4. Login as master user in Amazon RDS and create a database.

5. Now, restore the dump file in the created database.

   Example: *psql.exe -U admin -h postgresrestore.cs2vdnfhjxh3.us-east-1.rds.amazonaws.com -p 5432 -d test -f pam360.sql*

6. Execute the following commands:

   update task_input set admin_status = 4 where schedule_id in (select schedule_id from schedule where schedule_name like 'FWBackupSchedule');

   update DEFAULT_TASK_INPUT set variable_value = 'dump' where variable_name like 'backup.content.type';

7. Replace the **pam360_key.key** from local instance to EC2 instance.
8. Now, make a copy of the below files under **<PAM360_Installation_folder>\conf** directory and rename them:
   - **customer-config.xml** to **customer-config_old.xml.**
   - **database_params.conf** to **database_params_old.conf.**
9. Open **database_param.conf** file.
   - Replace **localhost** with the hostname of the PostgreSQL server running in AWS.
   - Change the **port number** to the actual port number of the PostgreSQL instance in AWS.
   - Set **SSL=true** and provide the user details that were used to restore the dump file to the database.
10. Open **customer-config.xml** and search for **startdbserver= true** and change its value to **false.**
11. Download PostgreSQL root CA.
12. Import the root **.pem** file into PAM360. Refer to the help section **How do I import a root certificate into PAM360?** to know more information.
13. Start the PAM360 service.

You have successfully migrated data from Local PostgreSQL Database to Amazon RDS PostgreSQL Database.

Migrating Data from Local PostgreSQL Database to an External PostgreSQL Database

The PAM360 application comes with PostgreSQL as its integrated backend database. Nonetheless, PAM360 also offers the functionality to migrate from the bundled local database to an external PostgreSQL database, thus enabling seamless data transfer. In this document, you will find a detailed explanation of the process involved in migrating your data between the local and external PostgreSQL databases.

Steps Required

Below are the steps to migrate data from the bundled PostgreSQL database to an external PostgreSQL database:

1. Open the command prompt and navigate to the **<PAM360_Installation_folder>\pgsql\bin** directory.
2. Create a dump file using the command - **pg_dump dbname > pam360.sql**. For example,
   i. **In Windows** - pg_dump.exe -U postgres -h 147.0.0.1 -p 2345 -W PassTrix > pam360.sql
   ii. **In Linux** - ./pg_dump -U postgres -h 147.0.0.1 -p 2345 -W PassTrix > pam360.sql
3. Create a database cluster in the PostgreSQL provided with the database owner's permission.
4. Post the database creation, ensure that the extension '**pgcrypto**' is available in the extension drop-down. If there is no such available extension, create it using the command - **CREATE EXTENSION pgcrypto;**
5. Now, restore the dump file in the created database cluster using the following commands:
   i. **For Windows** - psql.exe -U admin -h 142.10.0.1 -p 5432 -d test -f pam360.sql
   ii. **For Linux** - ./psql -U admin -h 142.10.0.1 -p 5432 -d test -f pam360.sql
6. Execute the following commands:
   i. **update task_input set admin_status = 4 where schedule_id in (select schedule_id from schedule where schedule_name like 'FWBackupSchedule');**
   ii. **update DEFAULT_TASK_INPUT set variable_value = 'dump' where variable_name like 'backup.content.type';**

7. Now, make a copy of the below files under **<PAM360_Installation_folder>\conf** directory and rename them:
   i. **customer-config.xml** to **customer-config_old.xml**.
   ii. **database_params.conf** to **database_params_old.conf**.
8. Open the **database_param.conf** file and do the steps that follow:
   i. Replace **localhost** with the hostname of the PostgreSQL server running in an external database.
   ii. Change the **port number** to the actual port number of the PostgreSQL instance in an external database.
   iii. Set **SSL=true**, and provide the user details that were used to restore the dump file to the database.
   iv. Update the **db.password.encrypted** to **false**.
   v. Now, save and close the file **database_param.conf**.

   > **Notes:** The password given here will be in plain text at that instance and will be encrypted from the next consequent occurrence.

9. Open **customer-config.xml** and search for **startdbserver= true** and change its value to **false**.
10. Download the PostgreSQL root CA certificate. If you are unaware of creating an SSL for the PostgreSQL database, refer to this section to generate the required SSL certificates and validate the SSL connection.
11. Import the root CA certificate into PAM360.
12. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** and open the file **pg_hba.conf**:
    i. Add an entry at the end with the IP address of the machine/server on which the PAM360 is running. E.g., **host all <user name> <ip address>/32 md5**

    > **Notes:** The above step applies only to users who use an external PostgreSQL enterprise database as their backend database. For users with cloud-based databases, the process will be performed in an automated process.

13. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** and open the file **postgresql.conf**:
    i. Search for **listen_addresses** and provide the IP address of the server where PAM360 is running.

14. Restart the PostgreSQL server.
15. Start the PAM360 service.

Now you have successfully migrated your data from the local PostgreSQL database to the external PostgreSQL database.

Managing User Roles and Permissions

PAM360 serves as a repository for sensitive accounts and passwords, ensuring preliminary access control through user roles. Access to the PAM360 application is contingent upon possessing a specific role, which dictates the scope of privileged operations a user can perform. This fine-grained access control mechanism safeguards data from unauthorized access directly through the PAM360 interface, facilitated by role-based access control.

User roles within PAM360 delineate the operations permissible for each user. Regardless of the role assigned, managing personal passwords in PAM360 remains exclusive to individual users, subject to administrator-enabled settings, with other users having no authority over them.

At the end of this help document, you will learn about the following topics relevant PAM360 user roles.

1. PAM360 User Roles
2. Custom Roles
3. Frequently Asked Questions

1. PAM360 User Roles

The various user roles in PAM360 dictate the extent of operations a user can undertake:

i. Privileged Administrator

Users with the role have the authority to configure, customize, and oversee the PAM360 application comprehensively. They can configure privacy and security controls, including settings related to IP restrictions and emergency measures. Additionally, they possess visibility into resources and accounts they create or those shared with them by other users, enabling them to conduct all operations pertaining to resources, accounts, and connections. Moreover, they can elevate other administrators to the status of Super Administrators, thereby granting them full management authority over all server resources.

ii. Administrator

Administrators share similar privileges with Privileged Administrators, albeit with the exception of configuring certain privacy and security controls.

iii. Password Administrator

This role encompasses individuals in executing all configurations and operations related to accounts and password management. Like administrators, they possess the complete management of resources and accounts created by them or those shared with them by other users, with no access to User Management, Audits, Reports, and Dashboards.

iv. Password User

Users with this role can only access accounts shared with them by Administrators, Password Administrators, or Privileged Administrators, as per the permissions granted. They can make modifications to accounts if permitted by the sharing settings.

v. Password Auditor

This role shares privileges with Password Users and additionally grants access to dashboards, audit records, and reports of all resources within PAM360.

vi. Connection User

Individuals with this role have similar privileges to Password Users, with the added capability to establish HTTPS gateway connections, RemoteApp connections (for resources associated with RemoteApp), and perform secure file transfers.

Roles	Operations							
	Manage Users	Manage Resources and Accounts	Access Passwords	Manage Personal Passwords	Access Audit and Reports	Privacy and Security Controls	Remote Access	Secure File Transfer, HTTPS Gateway Server, and RemoteApp Access
Privileged Administrator	✓	✓	✓	✓	✓	✓	✓	✓
Administrator	✓	✓	✓	✓	✓	✗	✓	✓
Password Administrator	✗	✓	✓	✓	✗	✗	✓	✓
Password Auditor	✗	✗	✓	✓	✓	✗	✓	✗
Password User	✗	✗	✓	✓	✗	✗	✓	✗
Connection User	✗	✗	✓	✓	✗	✗	✓	✓

The allocation of these roles to the users ensures that access to sensitive data within PAM360 is tightly controlled, minimizing the risk of unauthorized access or misuse.

Note: An Administrator/Password Administrator/Privileged Administrator can be made as a Super Administrator. A super administrator will have the privilege to manage all the resources stored in PAM360, irrespective of the resource owner. For security reasons, a user with the administrator privilege can be made a super administrator only by other PAM360 administrators.

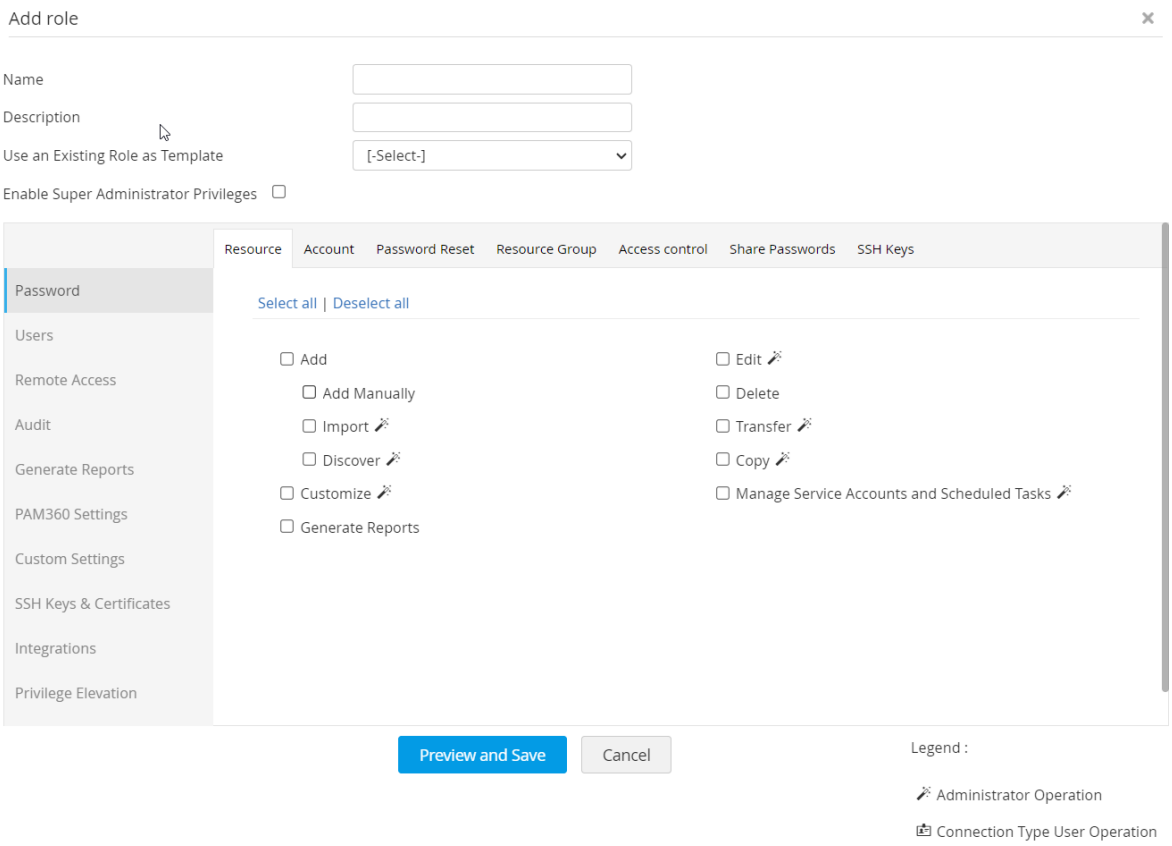
2. Custom Roles

Apart from the above-predefined roles in PAM360, administrators have the flexibility to create custom roles tailored to their organization's specific requirements. This customization feature empowers administrators to design roles from scratch, selecting from over 100+ available operations within PAM360.

To ensure an added layer of security, the creation of custom roles follows a dual-control mechanism, mandating approval from another administrator.

2.1 Adding a New Custom Role

1. Navigate to **Admin >> Customization >> Roles**.
2. Click **Add Role** in the **Roles** window. This prompts a new window to appear.
3. Here, provide a **Name** and **Description** for the new role as per your organizational needs.
4. **Use an Existing Role as Template** to base the new role on an existing template, either from PAM360's predefined roles or previously created custom roles. This facilitates to preset the permission levels for the new role.
5. Define the scope for the role under the desired PAM360 modules, such as **Password**, **Users**, **Organization**, etc., and by selecting the operations from the categorized list of available options under each module to meet the enterprise-specific needs.



Note: While creating a custom user role, ensure that you select the operations for the role as required. The operations with the magic wand icon beside is of administrator privilege. Selecting those operations for a custom role consider it in the administrator category and creating the user accounts with this user role might affect your PAM360 license counts.

For example,

1. If you like to create a role for the sole purpose of user administration, such as new user addition in PAM360, edit/delete user profiles, change roles, and transfer resources between users, here are the basic operations that should be selected from the User module:

Users	User Authentication Protocols	User Groups
▸ Manage Web Users ▸ Add Users Manually ▸ Import From AD ▸ Import From LDAP ▸ Import From Microsoft Entra ID ▸ Import From File ▸ Edit ▸ Lock / Unlock Users ▸ Delete ▸ Manage API Users ▸ Change User Roles ▸ Transfer Resources Owned by a User ▸ Generate Reports	▸ Manage Active Directory ▸ Manage LDAP ▸ Manage Microsoft Entra ID ▸ Manage SAML Single Sign-on ▸ Manage RADIUS Authentication ▸ Manage Smart Card Authentication ▸ Manage Two-factor Authentication ▸ Reset Two Factor Authentication ▸ Manage Browser Extension/Mobile Access for Users ▸ Manage Remote Connect for Users	▸ Add ▸ Manage user group settings ▸ Modify an Existing Group ▸ Generate Reports ▸ Delete

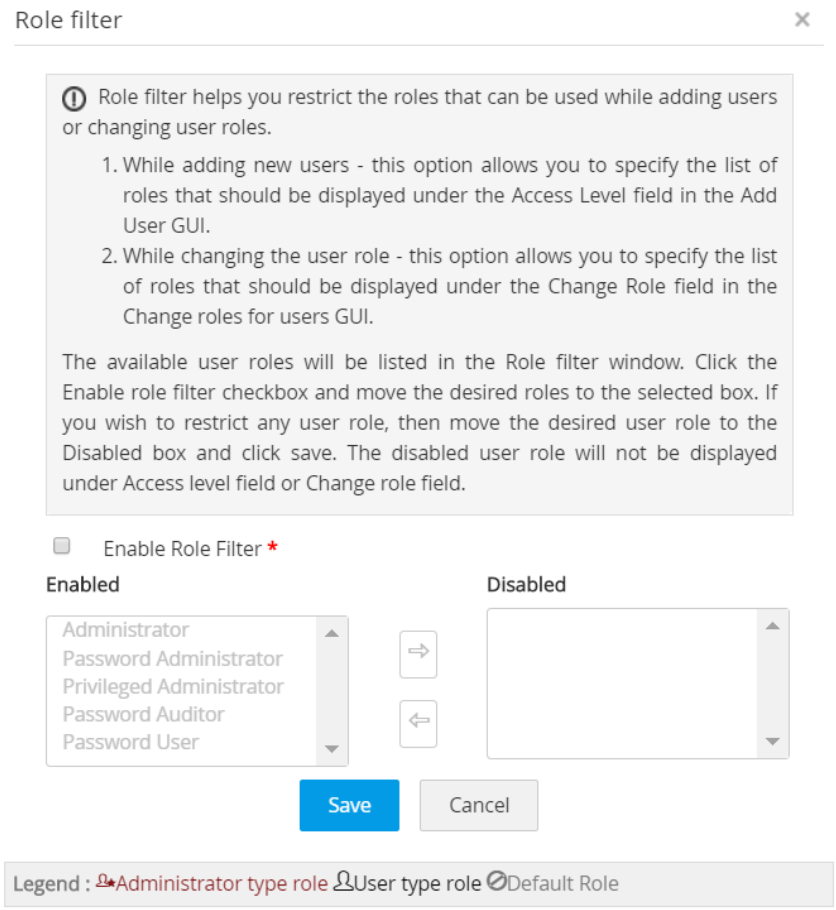
2. If you like to create a role for a junior technicians who maintains a handful of resources in your organization, a role with the following operations is required:

Users	Resource	Accounts	Password Reset
	▸ Add ▸ Edit ▸ Delete ▸ Copy ▸ Generate Reports	▸ Add ▸ Edit ▸ Delete ▸ Copy ▸ Move	▸ Find Out of Sync Passwords ▸ Password Reset
Remote Access	▸ Show ConnectionsTab ▸ Remote Connections to Machines ▸ Manage AutoLogon Helper ▸ File Transfer ▸ RemoteApp ▸ Configure Connection Settings		
Custom Settings	▸ Export Passwords ▸ Allow Users to Manage their Personal Passwords		

2.2 Role Filter

The role filter feature enables administrators to streamline role assignment by specifying which roles should be visible under the Role field in the Add User window. To enable role filtering:

1. Go to **Admin >> Customization >> Roles >> Role Filter**.
2. Enable the **Enable Role Filter** box.



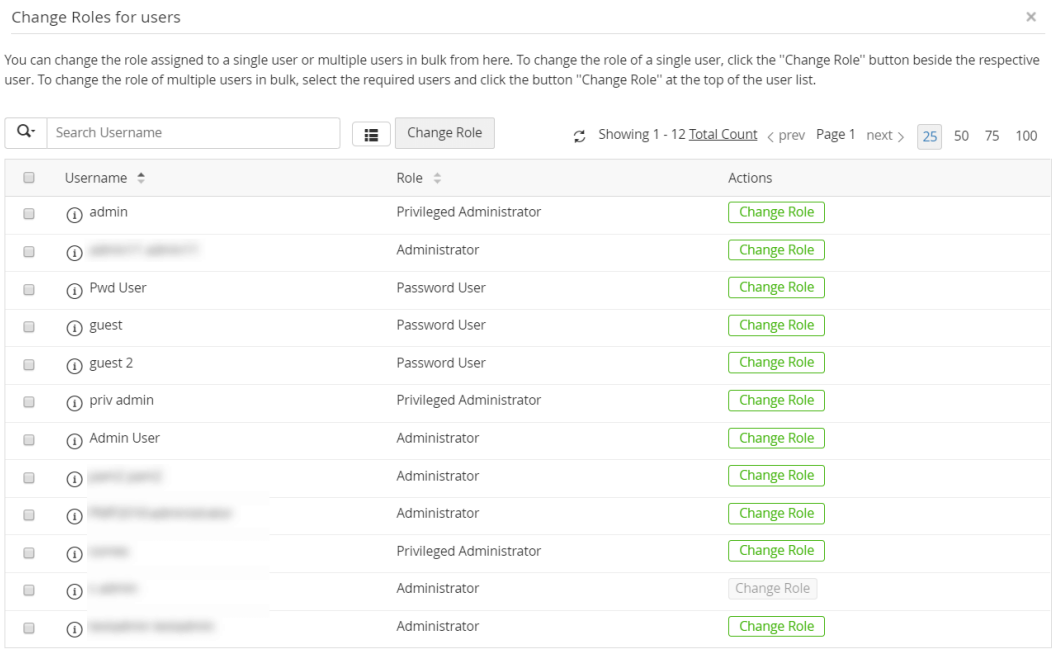
3. Organize and enable/disable roles as needed, ensuring only enabled roles appear during user addition or role changes. **Save** the configured settings to apply the role filter.

2.3 Changing Roles for Users

Administrators can efficiently update roles for individual users or multiple users in bulk. To do so,

1. Navigate to **Admin >> Customization >> Roles >> Change Roles**.
2. Utilize the filter above the table to display users associated with a specific role.
3. To change the role of an individual user, click the **Change Role** button beside the user and assign the desired role as needed.

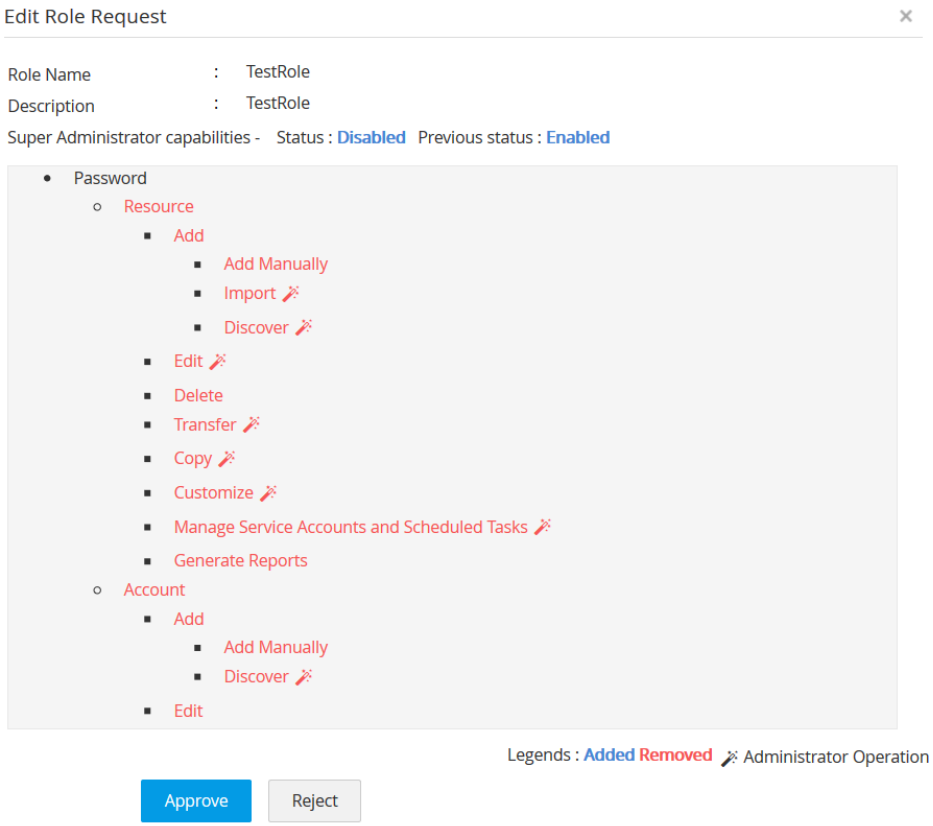
4. To change the role for a group of users, select the users requiring role changes and click the **Change Role** button from the top pane to assign them with the desired role from the available options.



2.4 Editing / Deleting Custom Roles

To edit a custom role,

To edit a custom role, click the Edit icon next to the respective role, make necessary modifications, and click Preview and Save. Verify the modifications once and click Save. The edits undergo an approval process by another administrator before implementation. Edits pending for approval will be shown with the status [Waiting for approval] beside the specific role. In the below image, red denotes operations that have been removed in the edit, and blue denotes operations that have been added to the role.



To delete a custom role,

Click the Delete icon beside the respective role and Delete the custom role. If you have users mapped with the custom role, the dialogue-box which opens prompts to transfer associated users to another role before deletion. Once users are mapped to a new role, click Transfer users and delete role to proceed with the role deletion.

This meticulous approach to role management in PAM360 ensures tailored access control aligned with organizational needs, maintaining security and operational efficiency.

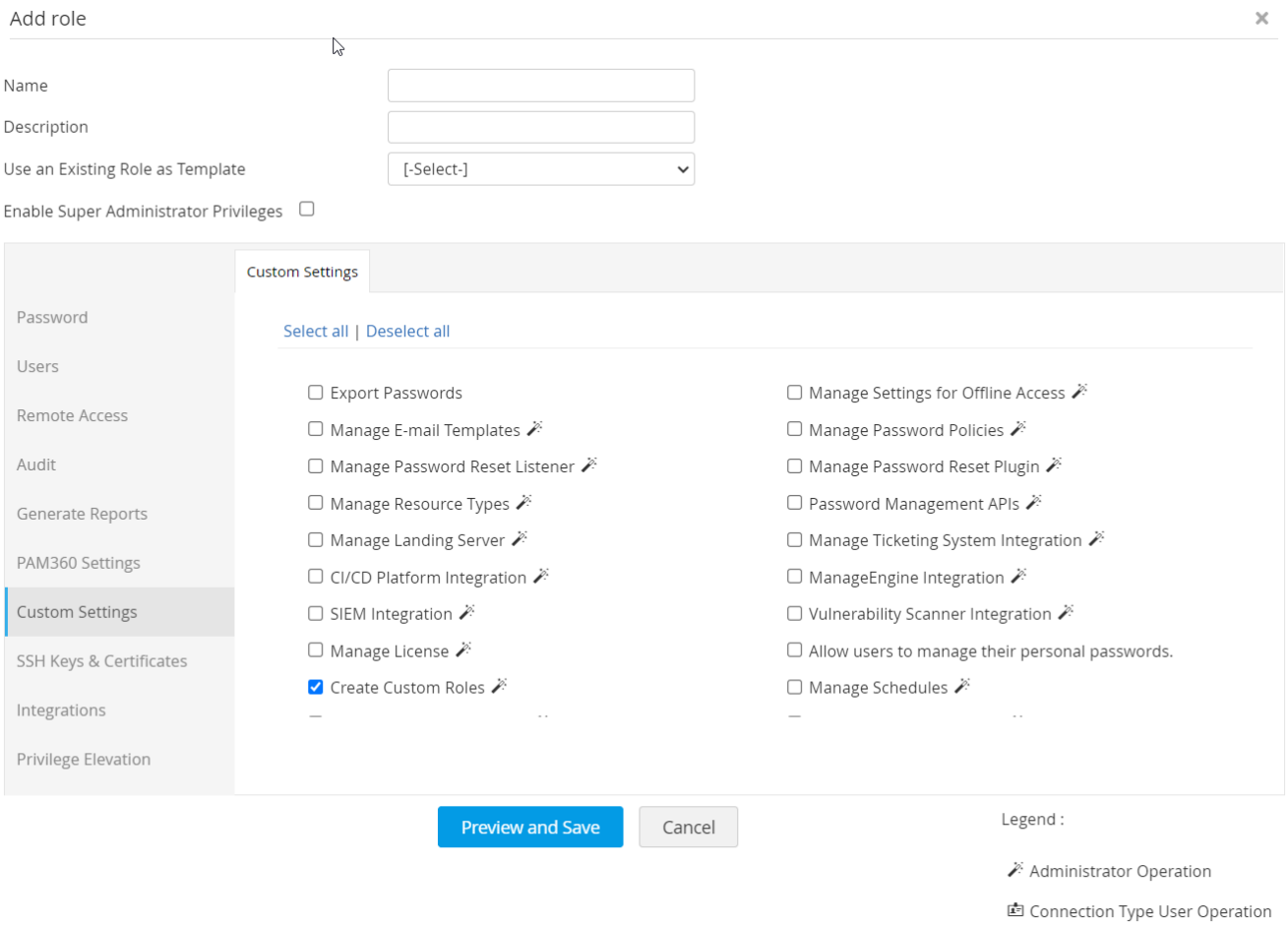
3. Frequently Asked Questions

1. What does the magic wand icon signify next to certain operations?

Operations accompanied by a magic wand icon indicate Administrator-level operations. If a custom role includes any of these wand-marked operations, it is treated akin to an Administrator role. You can create multiple custom roles with such operations, but the role only counts towards the license when assigned to a user in PAM360. For example, if your licensing permits 10 administrators and you assign a custom role with wand-marked operations to a user, it consumes one of the 10 allotted licenses.

2. Who has the authority to create custom roles in PAM360?

Creating custom roles is primarily an administrative task. Only Administrators, Privileged Administrators, and Super Administrators (if created) possess the privilege to create custom roles. Additionally, you can authorize a custom role to create future custom roles by enabling the Create **Custom Roles** option under **Custom Settings**. Moreover, enabling the **Enable Super Admin capabilities for this role** checkbox allows users assigned this role to be promoted to Super Administrator during user creation. After configuring the role settings, clicking on **Preview and Save** initiates a preview listing the chosen operations, and a further Save will create the role and queue it for pending approval from another administrator. Once approved, the role can be assigned to users accordingly.



3. Why am I unable to delete a custom role?

There are two scenarios where a role cannot be deleted immediately:

i. If attempting to delete a user-type role with associated users, those users must first be transferred to another role. The target role for transfer can be either an end-user-type or administrator-type role, provided sufficient administrator licenses are available. However, if no administrator licenses remain, or if there is no existing user-type role for

transfer, deletion is prohibited. In such cases, creating a new user-type custom role or acquiring additional licenses is necessary to delete a custom role.

ii. Role Filters may also impede deletion. If all end-user-type roles are disabled under the role filter settings, transferring associated users becomes restricted to administrator-type roles only. If no administrator licenses are available for transfer, or if no end-user-type roles are enabled in the filter settings, deletion cannot proceed. To resolve this, enabling at least one end-user-type role under role filter settings or obtaining additional licenses is required.

Super Administrator in PAM360

By default, PAM360 comes bundled with six pre-defined user roles that offer specific set of permission levels:

- Privileged Administrators
- Administrators
- Password Administrators
- Password Auditors
- Password Users
- Connection Users

Super administrator is not a user management role directly provided by PAM360, but it is a privilege elevation that gives the administrator an unrestrained access to all resources in PAM360. You can elevate any administrator to a **super administrator** and once it done, they will have unconditional, full-privileged access to all resources created and owned by other administrators.

> **Note:** Super administrator privilege can be provided only to users with admin-level roles such as Privileged Administrator, Administrator, Password Administrator, and custom roles with administrator permissions.

1. **Steps to promote an administrator to a super administrator**

   1.1 **While adding or editing an admin user**

   1.2 **While creating a custom role**

2. **Use case scenarios for creating a super administrator role**

   Case I: **To gain access to all resources in PAM360**

   Case II: **As a precautionary break-glass account**

   Case III: **To transfer ownership of resource groups in bulk**

1. Steps to Promote an Administrator to a Super Administrator

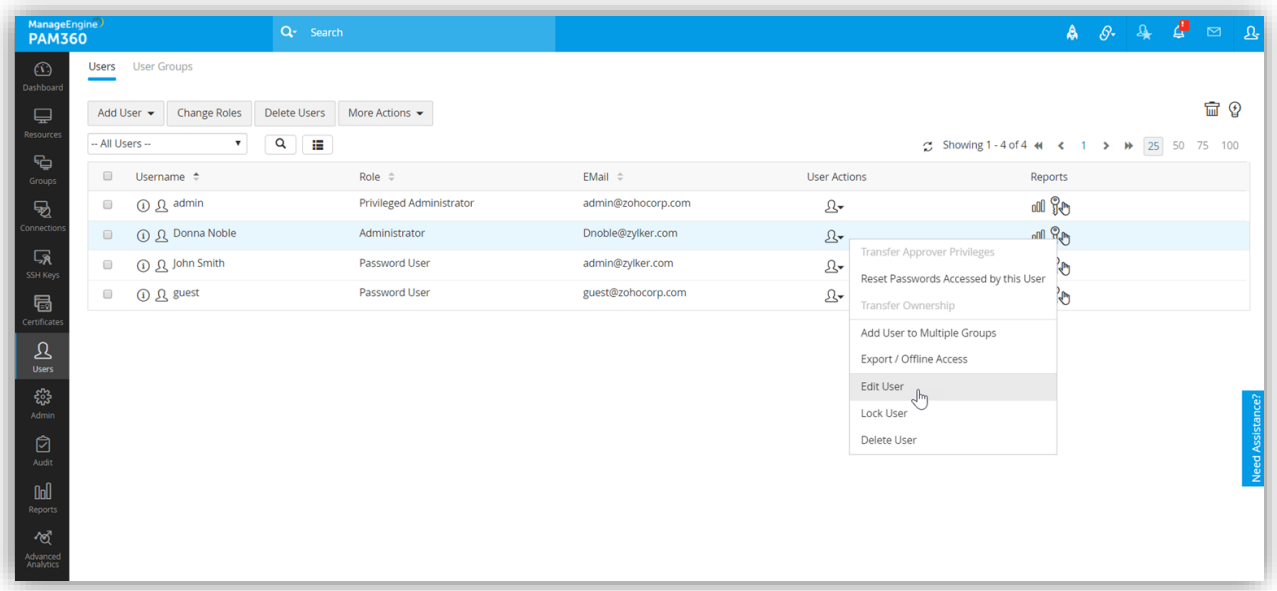
There are two ways to promote an administrator to the super admin role from PAM360's user interface:

- While adding or editing an admin user
- While creating a custom role

1.1 While Adding or Editing an Admin User

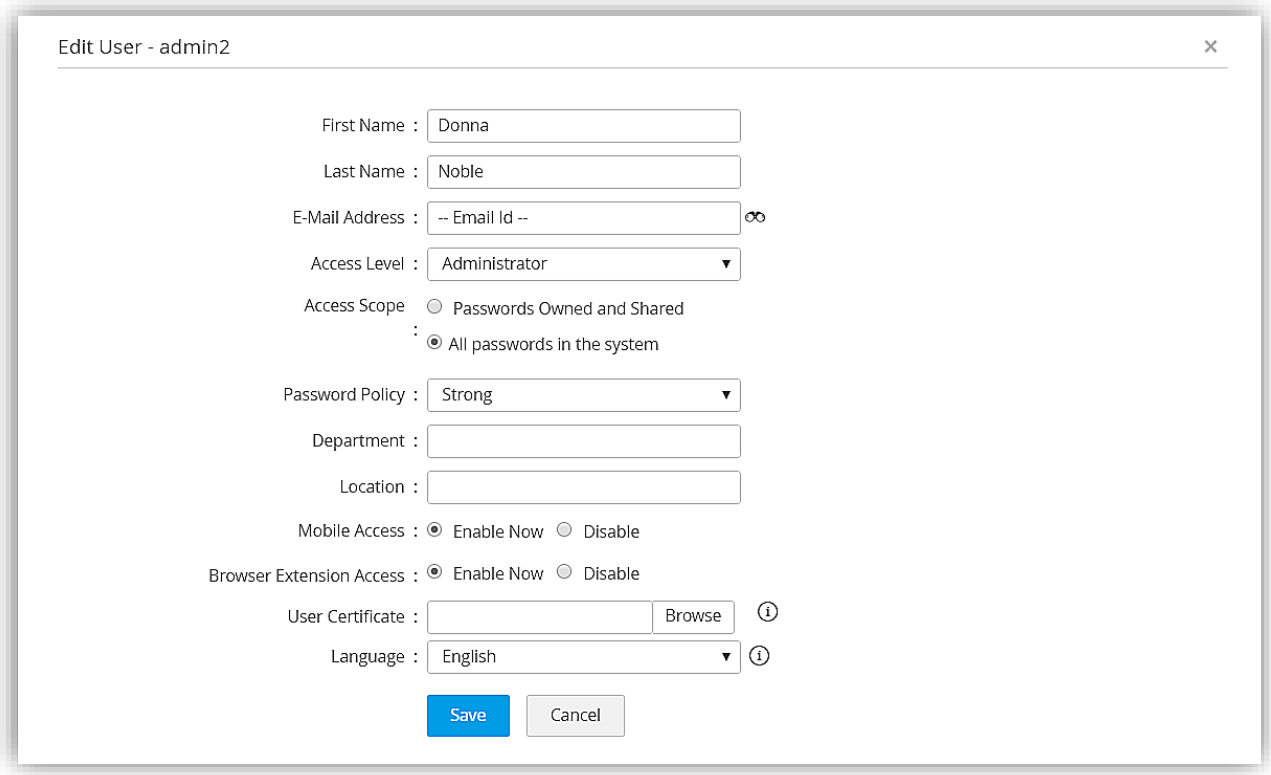
Follow the below steps to give super administrator privileges to an admin either at the time of adding the user or by editing an existing admin user's attributes.

1. Navigate to the **Users** tab.
2. Click **Add User >> Add Manually** or click the **User Actions >> Edit User** option beside an existing user.



3. In the window that opens, ensure that the access level is an Administrator role and choose **All passwords in the system** as the access scope. Click **Save**.

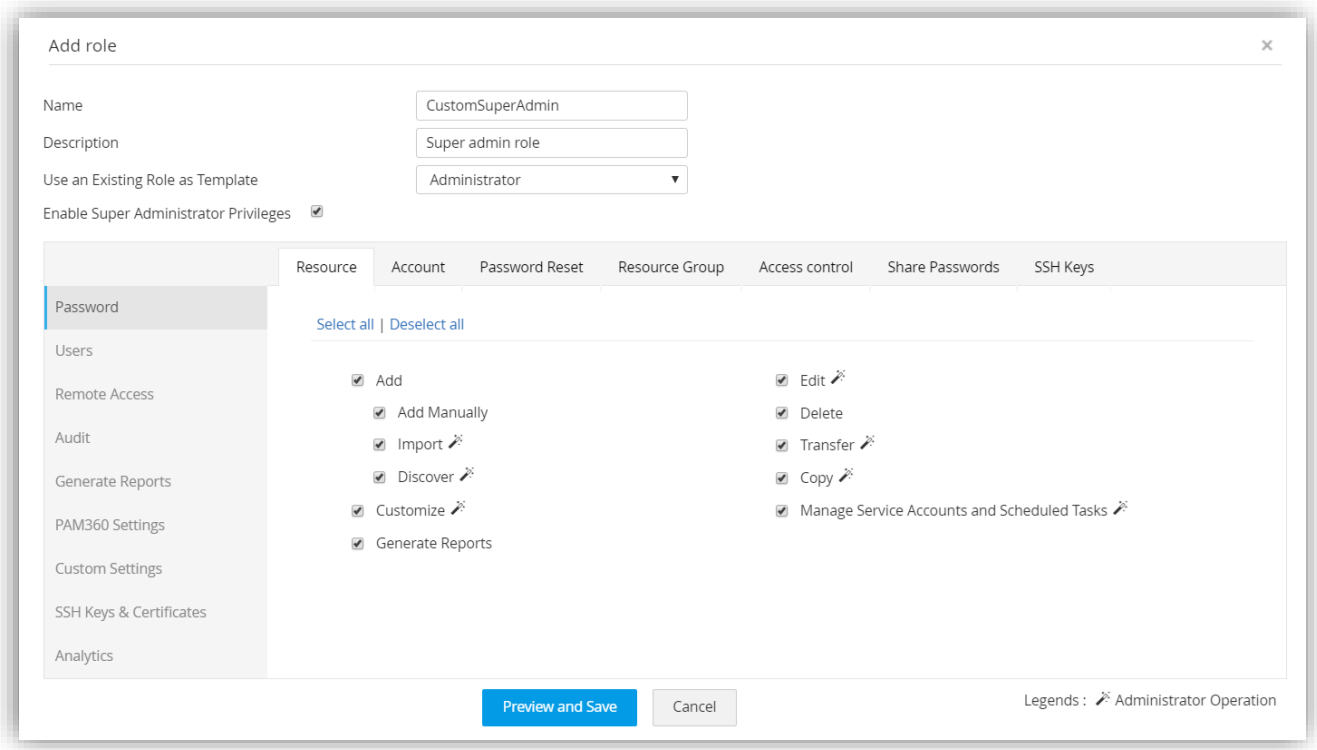
Now, this user will be promoted as a super administrator and they will be notified of the same via email.



1.2 While Creating a Custom Role

You can create a custom admin role and grant super administrator privileges to it, along with other capabilities of your choice. Follow the below steps to create custom roles:

1. Navigate to **Admin >> Customization >> Roles** and click **Add Roles**.
2. In the **Add Role** window, click the **Enable Super Administrator Privileges** checkbox. This option will elevate the user role to a super admin in PAM360.



3. When this custom role is assigned to a user in the future, edit the user attribute as explained in the previous step, and change access scope to **All passwords in the system.**

2. Use Case Scenarios for Creating a Super Administrator Role

Case I: To Gain Access to All Resources in PAM360

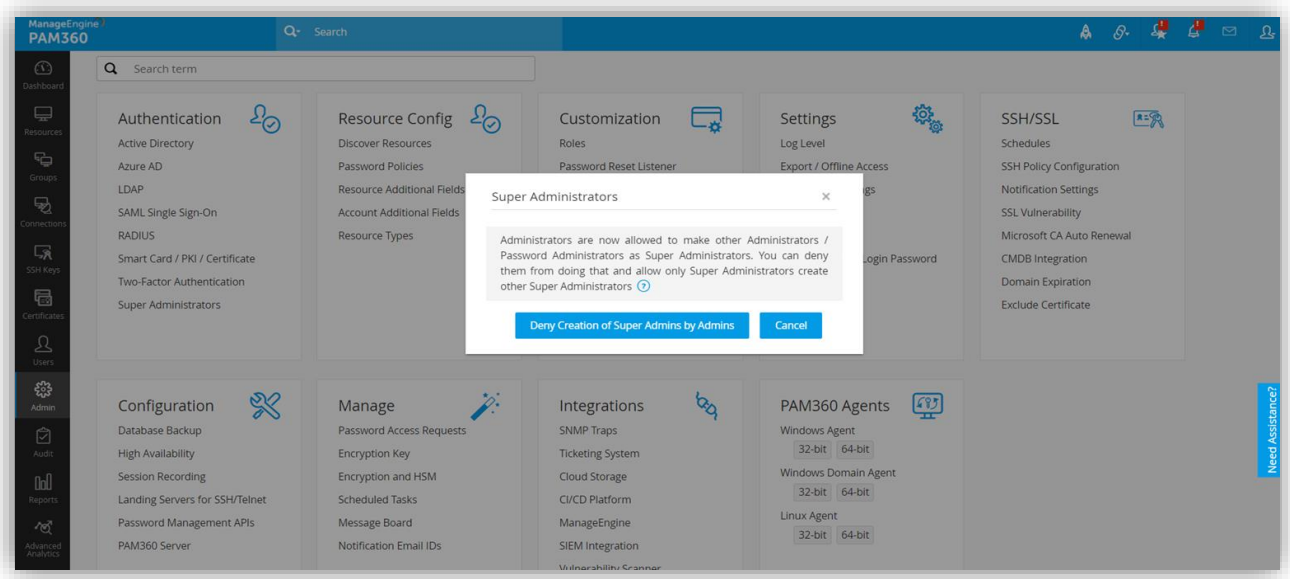
You can promote a manager at the top of your organizational hierarchy such as the organization's CIO/CEO's active directory (AD) or LDAP account to super admin in PAM360 in case they need access to everything that is stored in the PAM360 database. In this case, it is prudent to have Two-Factor Authentication (TFA) enabled for their PAM360 account. This way, even if their AD account is compromised, it cannot be used to gain access to resources without bypassing the TFA in PAM360.

Case II: As a Precautionary Break Glass Account

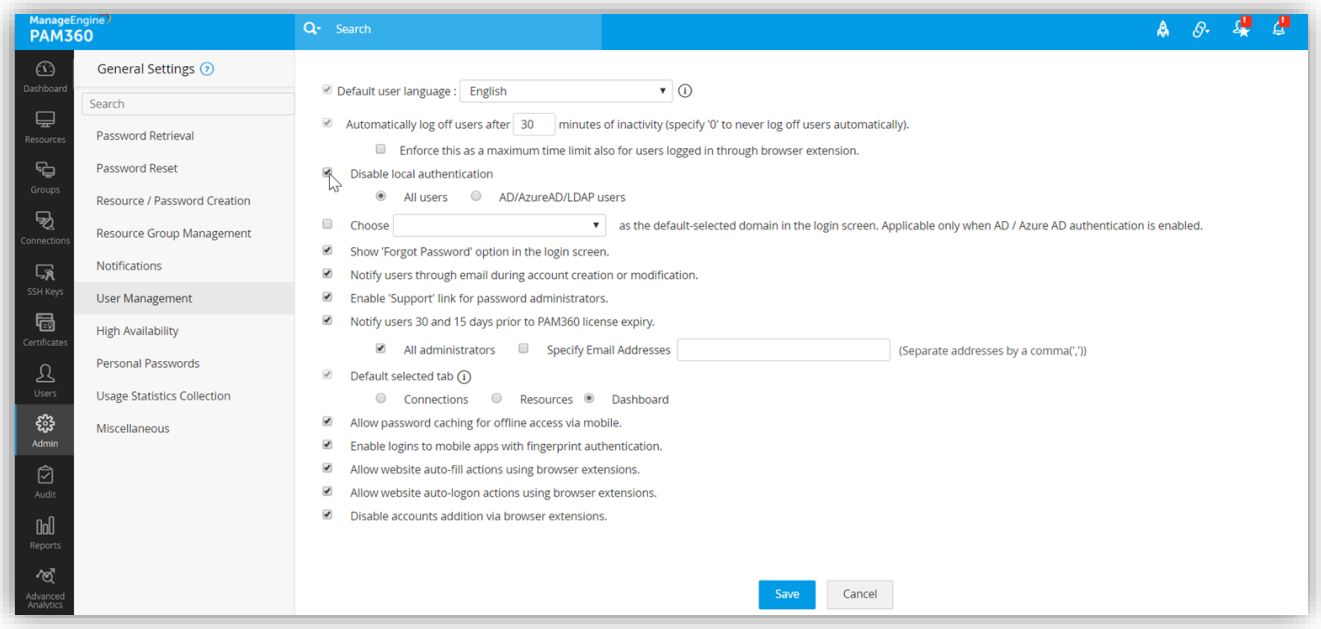
We recommend creating a super administrator account as a precautionary measure for emergency situations such as sudden demise of an employee with admin rights, or to carry out security measures in the server when the server admin is on a vacation so that users in your organization do not lose access to their accounts. However, it is crucial that only one super administrator account is created for this purpose and access to it is highly restricted.

You can disable addition of more than one super administrator in PAM360 and then restrict the login access to the existing super admin account. This action can be carried our only by a super admin user. Follow the steps to disable addition of further super admins in PAM360:

1. Create a local administrator account in PAM360.
2. Import your administrator account from active directory or LDAP and promote the local admin account to be the super admin.
3. Login using the super admin account, navigate to **Admin >> Authentication >> Super Administrators** and click the option **Deny Creation of Super Admins by Admins**.



4. To restrict the usage of the super admin account, navigate to **Admin >> Settings >> General Settings**.
5. Click **User Management** from the left pane and select the option **Disable local authentication**. This option will disable the local authentication of the super admin account.



Once the local authentication option is disabled, it will no longer be available on the login page and the default admin account cannot be used to login to PAM360. To regain access to this account during an emergency, contact our support team to bring back the local authentication option to the login page and use the default admin account to recover your passwords.

Case III: To Transfer Ownership of Resource Groups in Bulk

In PAM360, users with super administrator privileges can transfer ownership of resource groups in bulk. Refer step 1 to promote an administrator to super administrator. Click here to learn how to transfer resources groups in bulk using super administrator privileges.

Adding User Accounts in PAM360

PAM360 allows administrators to add/import users. Administrators can create users manually or import users using different methods and assign user roles based on the level of permission needed. Here, in PAM360, the users can perform various operations based on their assigned user roles. To know more about user roles and how to manage them, click here.

The various methods to add/import users into PAM360 are:

1. Add Users Manually
2. Add API Users
3. Import Users from a File
4. Import Users from AD
5. Import Users from Azure AD
6. Import Users from LDAP

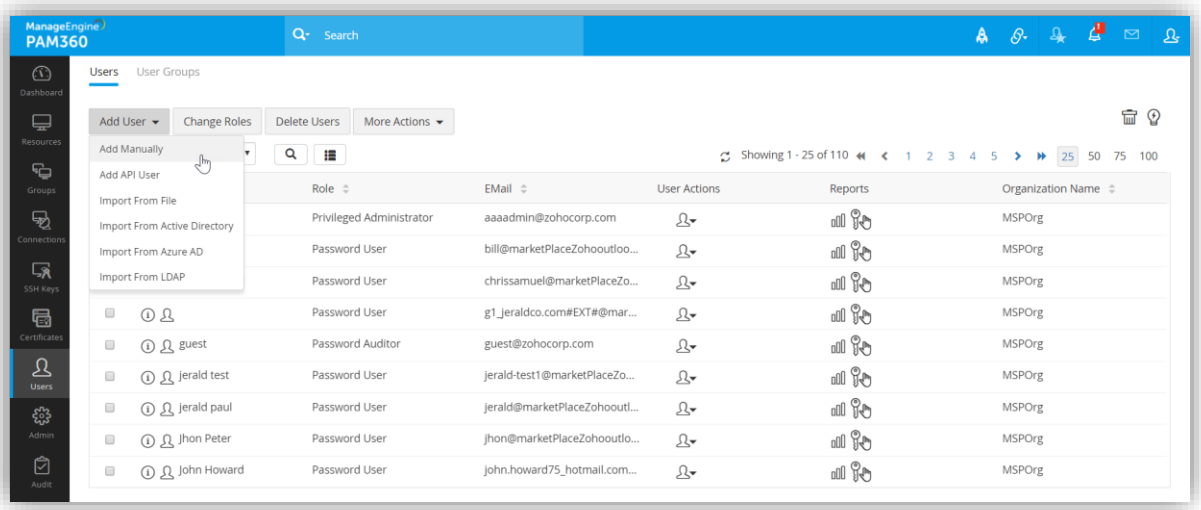
Adding Users Manually into PAM360

PAM360 allows administrators to create users manually and assign different user roles to them based on the level of access they need. Once created, the users will get an email with the details of their account and login credentials. While adding users manually, administrators can tailor the access levels and individual preferences such as GUI language, based on the organization's requirements.

> **Note**: User addition can be carried out only by **Administrators**, or **Privileged Administrators**, or by **users with custom roles** having similar permissions.

Creating a User Accounts Manually in PAM360

1. Navigate to the **Users** tab, click the **Add User** button and select **Add Manually** from the drop-down.



2. In the **Add User** window, enter the following attributes:

    a. **First Name** and **Last Name** - Enter the user's first and last names in the respective fields. This field is mandatory.

    b. **Username** - Enter a unique username with which the user can login to PAM360. This field is also mandatory.

    c. For the password, choose from three options:

        i. **Generate Password** - If this option is selected, PAM360 will randomly generate a password for the account based on the password policy selected in the next

step.

ii. **Use Username as Password -** The password will be the same as the username provided.

iii. **Specify a Password Manually -** Enter a password manually in the text field.

d. **Password Policy -** Select a password policy from the drop-down.

e. **Email** - Enter the user's email address. Login credentials for PAM360 will be emailed to this address once the account is created.

f. **Access Level** - Select an appropriate **access level** for the user from the drop-down, this will determine the type of role this user will have in PAM360.

g. **Access Scope** - Use this option to change an Administrator/Password Administrator/Privileged Administrator into a Super Administrator by choosing the option **All Passwords in the system.** When you do so, the user will be able to access all passwords in PAM360 without any restriction. Click here to learn more about super administrators in PAM360. Conversely, choose the **Passwords Owned and Shared** option to revert a Super Administrator to their earlier role of Administrator/Password Administrator/Privileged Administrator.

h. **Department and Location** - These fields are not mandatory fields. However, populating valid data in these fields with the correct values will be helpful for searching and grouping the resources.

i. **Mobile Access & Browser Extension Access** - Choose **Enable** for both the fields if you wish to allow the user to access PAM360 via the PAM360 mobile app and browser extensions.

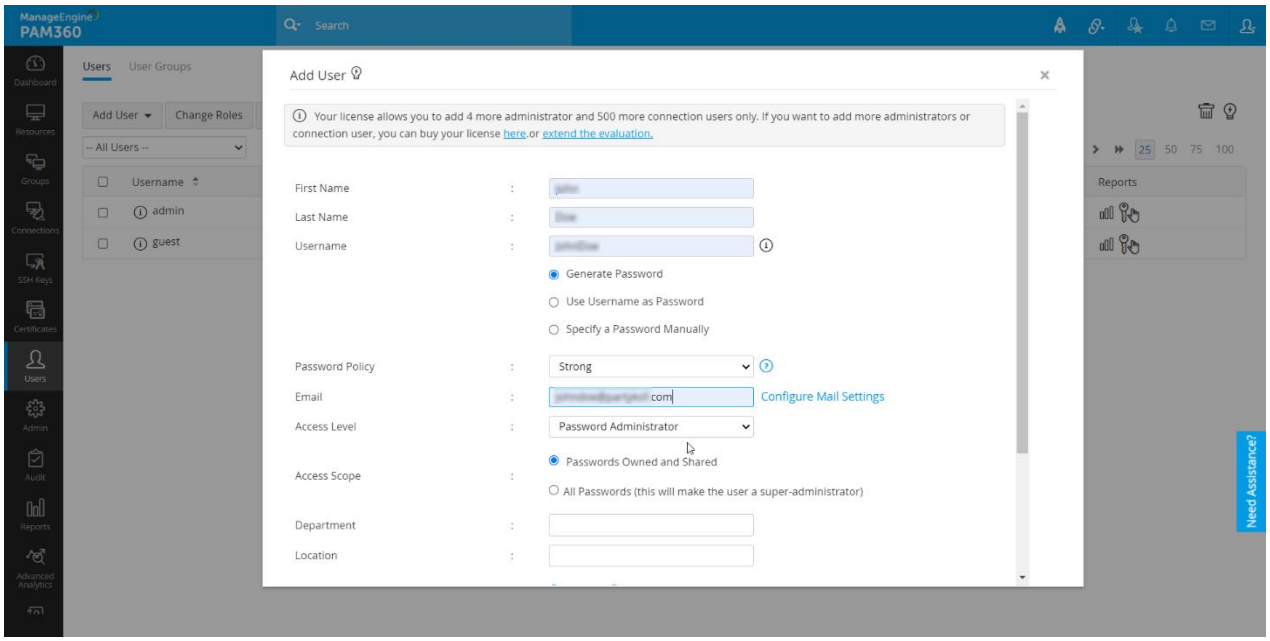
j. **Remote Connect Access** - Choose **Enable** for this field to allow the user to access the **PAM360 Remote Connect** desktop client using their PAM360 login credentials.

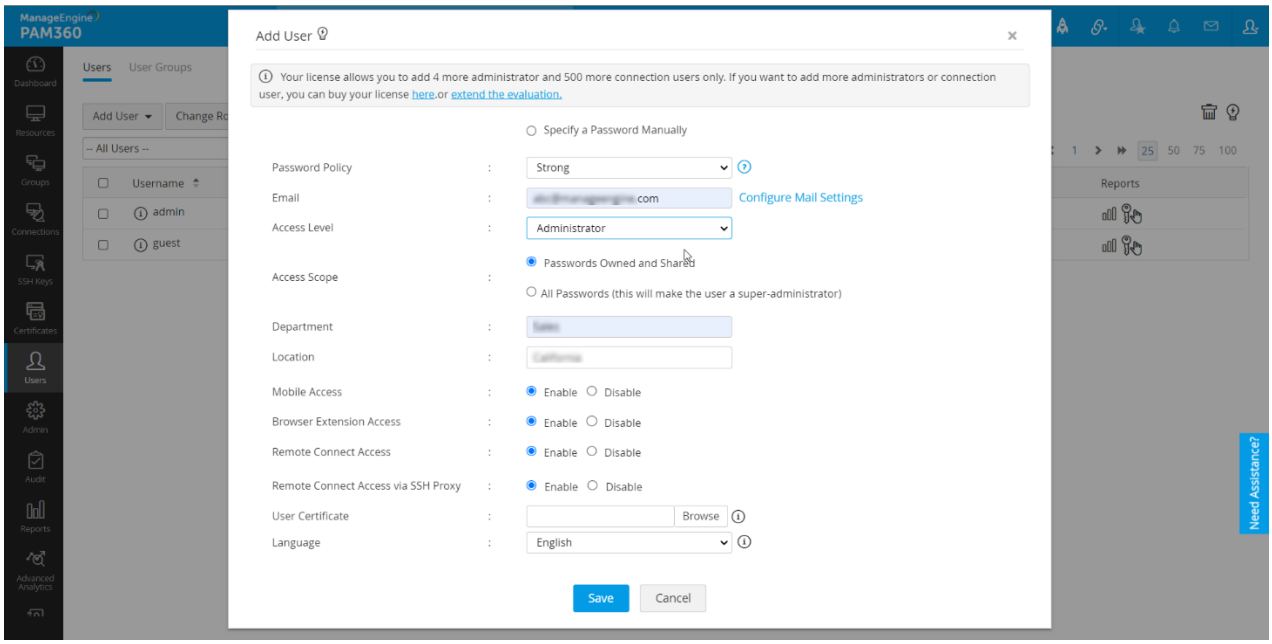
k. **Remote Connect Access via SSH Proxy** - Select **Enable** for this field to allow user remote sessions in the PAM360 Remote Connect application only via the configured SSH proxy.

l. **User Certificate -** Browse and add a certificate for smart card/PKI-based authentication. Click here for more information on that.

m. **Language** - Choose a GUI language for the user from the dropdown.

3. Click **Save** to create the user.





Note: PAM360 users with web access will be forced to reset their local login password when logging in for the first time.

Adding Users Manually into PAM360

(This procedure is applicable from build 6700)

In PAM360, administrators have the capability to create user accounts manually and assign specific roles to them, tailoring access levels and preferences according to organizational needs. This guide outlines the process of adding users manually by allowing administrators to customize user roles, access scopes, and individual settings.

Roles Required to Add Users to PAM360

Any of the below roles is required to add the user manually in PAM360:

- Privileged Administrator
- Administrator
- Any custom role with 'Add Users Manually' or 'Manage API Users' enabled operation

Creating a User Account Manually in PAM360

Below are the steps to create a user account in PAM360 with comprehensive access, including Web, REST API, and SDK functionalities. For more granular access control, administrators can enable or disable specific access as needed for the user. For example, a user can be provided with Web/REST API/SDK access, combination of Web and REST API, Web and SDK, or REST and SDK access, or with all access.

Navigate to **Users** tab and select **Add User**.

> **Note:** Either one access to the **Web** or **REST and Application** is required to create a PAM360 user account.

a. User Details

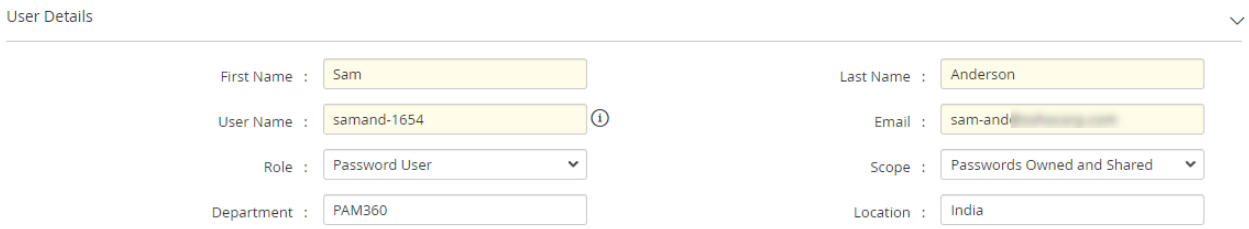
In this section of the add user page, provide basic user information and define the user's role and scope within PAM360.

i. **First Name** | **Last Name**: Enter here the user's first name and last name.

ii. **Username**: Enter here a unique name that the user uses to log into the PAM360 application.

iii. **Email:** Enter the user's email address where the user will be notified for updates. Login credentials for PAM360 will be emailed to this address once the user account is created.

iv. **Role:** Select an appropriate role for the user from the drop-down; this will determine the type of role and privilege this user will have in PAM360. Refer to this section to learn more about the user roles available in PAM360.



v. **Scope:** By default, users created in PAM360 are assigned the scope of Passwords Owned and Shared. This means they can access passwords owned by them or shared with them by other PAM360 users. However, selecting the All Passwords option grants the user Super Administrator privileges. With this privilege, the user gains unrestricted access to all passwords within the PAM360 application. Click here for more information on super administrators in PAM360.

> **Notes:**
> i. Users with the **End-User Type Role** cannot be provided with the **All Passwords** scope.
> ii. Users provided with the **All Passwords Scope** cannot be provided with the **REST and Application Access** in PAM360.

vi. **Department | Location**: Enter the department and the location where the user belongs to. These fields are not mandatory. However, populating valid data in these fields with the correct values will be helpful while searching or grouping the users.

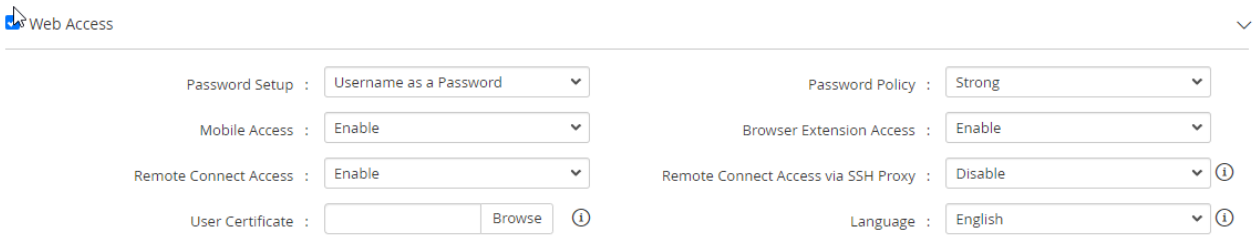
b. Web Access

Enabling the Web Access grants the user account access to the PAM360 web application, along with access via the PAM360 mobile application and browser extension as provided.

i. **Password Setup:** Choose one method for creating the user account password:

a. **Generate a Password** - This option generates a password randomly based on the selected Password Policy.
b. **Username as Password** - The password will match the username provided.
c. **Enter a Password** - Manually enter a password in the text field.

ii. **Password Policy**: Select a password policy from the drop-down menu for the account. The password created/modified for this user account should adhere to the policy selected here.
iii. **Mobile Access**: Enable this option to allow the user to access the PAM360 interface via the mobile application.
iv. **Browser Extension Access**: Enable this option to allow the user to access PAM360 resources via the browser extension.
v. **Remote Connect Access**: Enable this option to permit the user to launch remote sessions via the PAM360 Remote Connect desktop client using their PAM360 login credentials.



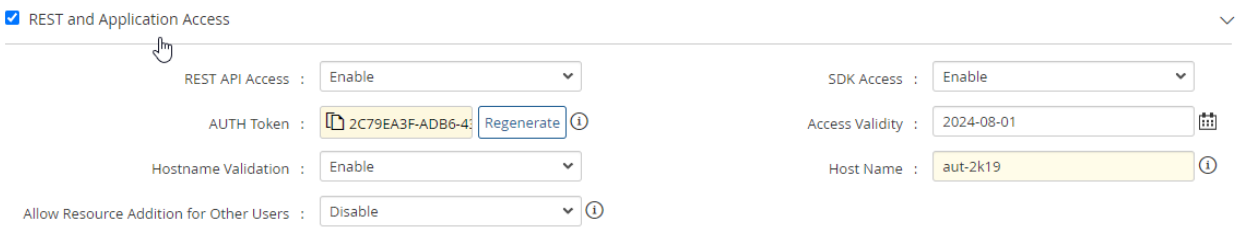
vi. **Remote Connect Access via SSH Proxy:** Enable this option to allow user remote sessions in the PAM360 Remote Connect application only via the configured SSH proxy.
vii. **User Certificate**: Upload the user certificate here for any smart card/PKI-based authentication. Click here for more information.
viii. **Language:** Select the desired web GUI language for the user upon login.
ix. **Two-Factor Authentication:** Enable or disable Two-Factor Authentication (2FA) for the user, if 2FA has been set up on the Admin page.

> **Note:** For a few specific 2FA providers, ensure that the username provided in the 2FA provider portal matches the username in PAM360. In cases where there's a discrepancy (E.g., if a user imported from Active Directory has the username ADVENTNET\rob in PAM360 but recorded as rob in the 2FA provider's portal), you can perform username mapping from here instead of modifying the name in 2FA provider's portal.

c. REST and Application Access

Enabling REST and Application Access grants the user account access to the PAM360 APIs, providing a user Authentication Token for further API access from desired applications or services.

i. **REST API Access**: Enable this option if the user account requires access to the PAM360 REST API.
ii. **SDK Access**: Enable this option if the user account requires access to the PAM360 API via the PAM360 SDK.
iii. **Authentication Token**: Generate an Authentication Token from here if providing with any of the above access. This token serves as a user validation key for API calls received from other applications or services.
iv. **Access Validity**: Select a date until which the Authentication Token will remain valid. Exceeding the provided date will invalidate the Authentication Token, requiring the generation of a new token to extend validity for further use of PAM360 REST APIs.



v. **Hostname Validation**: Enable this validation to verify user machines from which API calls are invoked. Enabling this feature restricts API invocation from the machines that are not predefined in the Host Name field.
vi. **Hostname**: Enter the Host Name of the machine from which the user is allowed to perform REST and Application operations.
vii. **Allow Resource Addition for Other Users**: Enabling this option permits users to create resources via the API and assign them to other users.

Click **Save** to add the user account to the PAM360 repository. By following this, administrators can manually add users to PAM360, customizing their roles, access levels, and preferences to suit organizational requirements.

> **Notes:** PAM360 users with web access will be forced to reset their local login password when logging in for the first time.

Adding API User Accounts in PAM360

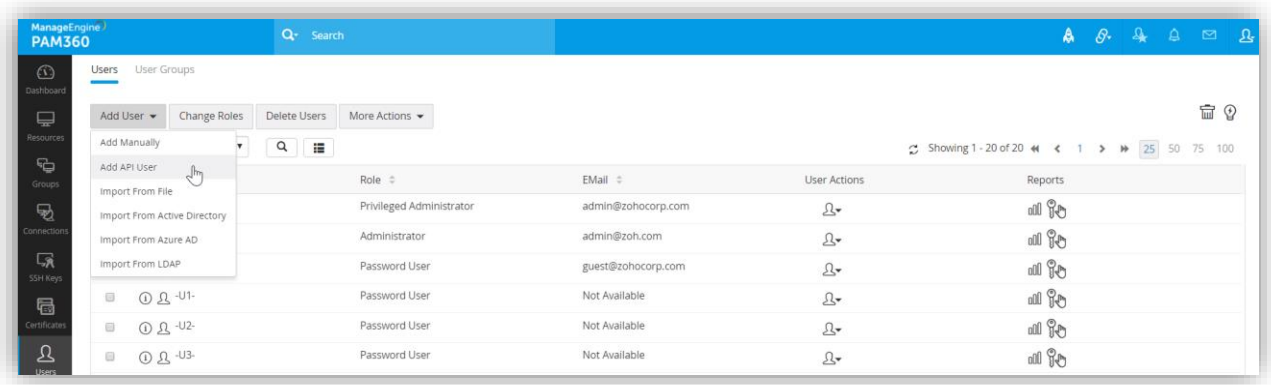
(This procedure is applicable prior to build 6700)

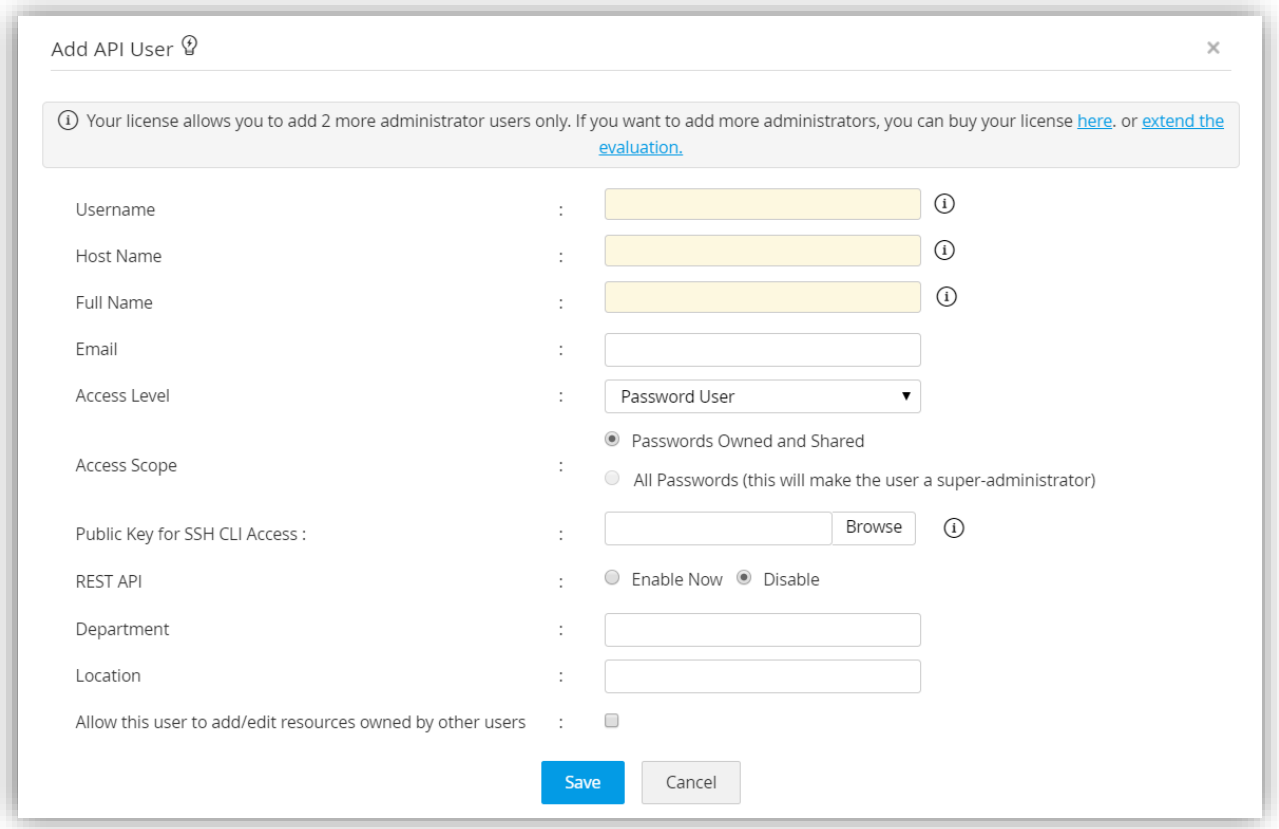
PAM360 allows you to add API users manually. API user accounts are required to configure password management APIs for Application-to-Application password management. You need to create API user accounts in PAM360 for those who will use the password management APIs, where each API user account should be attached to a single endpoint (typically a server or a desktop from which the API is used, so that the user accounts are uniquely identified - for example, as user@hostname).

> User addition can be carried out only by Administrators and Privileged Administrators or by custom roles with similar permissions.

Creating an API User Account in PAM360

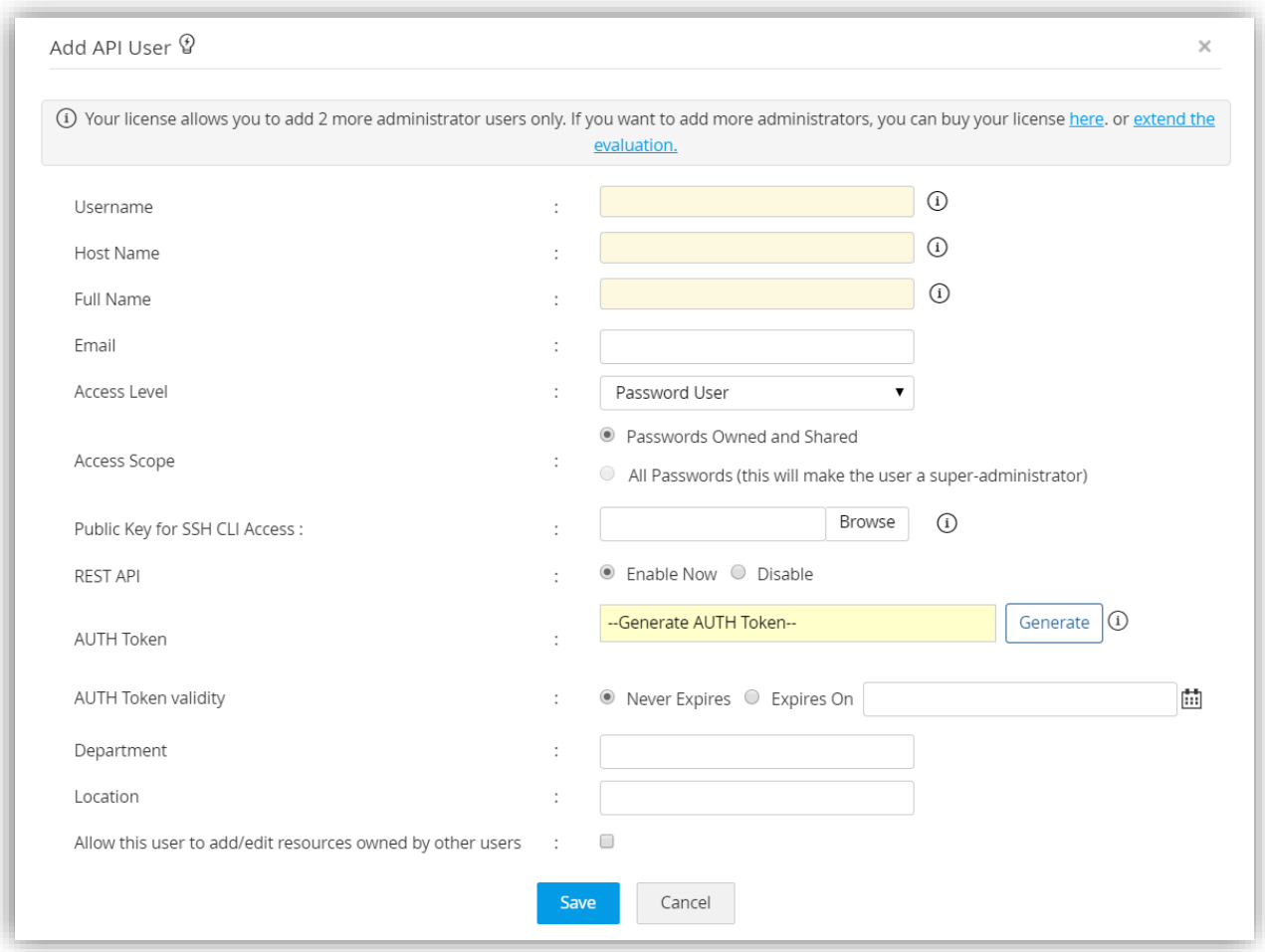
1. Click the **Users** tab and click **Add User >> Add API User** from the drop-down menu.





2. Enter the **Username** in the respective text field. This name identifies the API user.
3. Enter the name of the host from which the API user would access PAM360 for password management operations.
4. **Full Name** refers to the name with which the API user would be identified in the external world such as reports, audit trails and other places where activities are traced to users.
5. Select an **Appropriate Access** level for the API user being added - Administrator/Password Administrator/Privileged Administrator/Password User/Custom Roles.
6. You can use **Access Scope** to change an Administrator/Password Administrator/Privileged Administrator into a Super Administrator by choosing the option **All Passwords in the system.** When you do so, they will be able to access all passwords in PAM360 without any restriction. Conversely, a Super Administrator can be changed to their earlier role of Administrator/Password Administrator/Privileged Administrator by choosing the option **Passwords Owned and Shared.**
7. You can leave the options **Public key for SSH CLI access** and **SSL Certificate for XML-RPC API access** unchanged.

8. Enable REST API by clicking the button **Enable Now** beside REST API.



9. Once you do this, you will see a text box for the API key. Click on **Generate** to generate the API key. The API key is the Auth Token for your access purposes. Copy down this key and store it in a secure location for your future reference. This key will be displayed in the GUI only once and if you were to lose it, the key needs to be regenerated from this window.
10. You can set a validity period for the API key: by choosing the option **Never Expires** you can make the key to be valid forever. Otherwise, specify an expiration date.
11. Enter the department and location.
12. Click **Save**.

Note: API user creation is specific to the host from where an application contacts PAM360 for passwords. To use Password Management APIs from more than one host, you need to create as many API users as the number of hosts. Conversely, if you wish to have many users on a single host, then again you need to create as many API users as needed.

Adding API User Accounts in PAM360

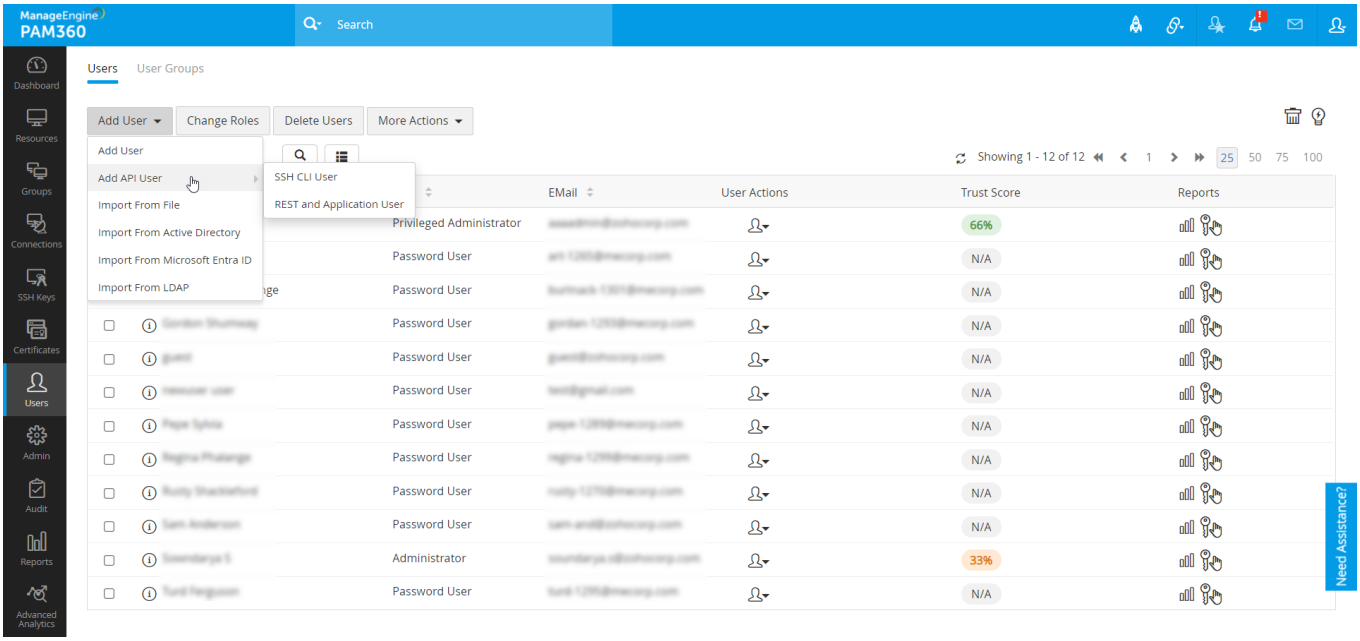
(This procedure is applicable from build 6700)

PAM360 allows you to add API users manually according to the need for access to the available APIs in the PAM360. API user accounts available in PAM360 are:

i. **SSH CLI User** - API user account for password management APIs in Application-to-Application or Application-to-Database password management.

ii. **REST and Application User** - API user account for generic PAM360 operations based on the provided user role and access.

While creating the API user accounts, you can attach the API user account to a single endpoint using the hostname (typically a server or a desktop from which the API is used, so that the user accounts are uniquely identified - for example, as user@hostname).



Roles Required to Add Users to PAM360

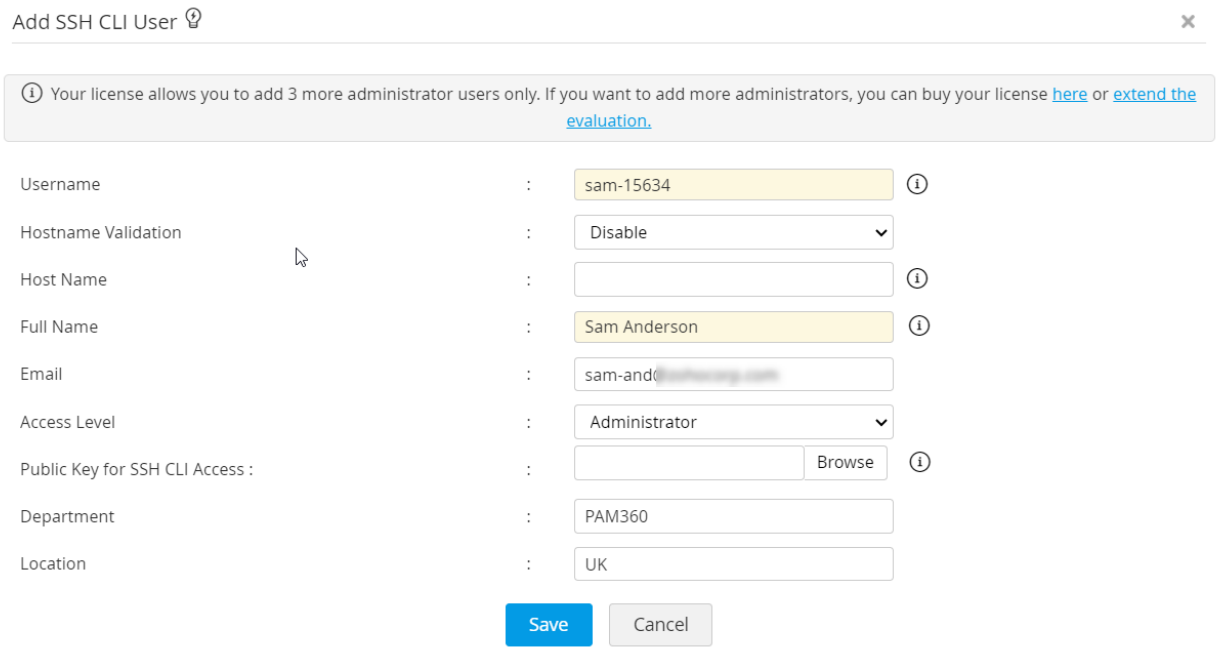
Any of the below roles is required to add the API user manually in PAM360:

- Privileged Administrator
- Administrator
- Any custom role with 'Manage API Users' enabled operation

1. Creating an API User Account with SSH CLI Access

To create an API user account for accessing PAM360 password management APIs in Application-to-Application or Application-to-Database password management, do the steps that follow:

i. Navigate to **Users >> Users >> Add API User >> SSH CLI User**.
ii. **Username**: Enter here a unique name. This name identifies the API user.
iii. **Hostname Validation**: Enable this validation to verify user machines from which API calls are invoked. Enabling this feature restricts API invocation from the machines that are not pre-defined in the Host Name field.
iv. **Hostname:** If you have enabled the Hostname Validation, enter the Hostname of the machine from which the user is allowed to perform the password management operations.
v. **Full Name** refers to the name with which the API user would be identified in the external world, such as reports, audit trails, and other places where user activities are traced.



vi. **Email:** Enter the user's email address where the user will be notified for updates.
vii. **Role**: Select an appropriate Role for the API user being added - Administrator/Password Administrator/Privileged Administrator/Password User/Custom Roles.
viii. **Public Key for SSH CLI Access:** Upload here the generated public key of the user machine from where the user accesses the SSH CLI APIs. This public key acts as the preliminary layer of the user verification method in addition to the hostname validation.
ix. **Department | Location**: Enter the department and the location where the user belongs to. These fields are not mandatory. However, populating valid data in these fields with the correct values will be helpful while searching or grouping the users.

x. Click **Save** to create the user account with the above-provided details.

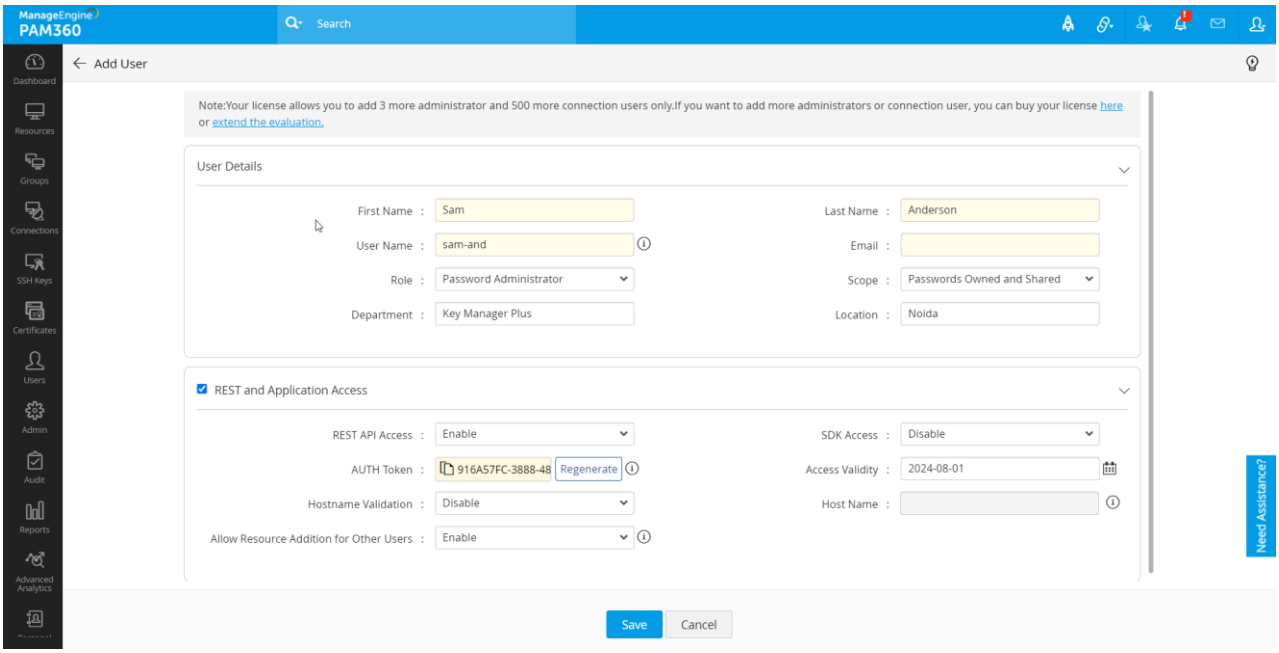
> **Important Note:**
> API user creation is specific to the host from where an application contacts PAM360 for passwords. To use Password Management APIs from more than one host, you need to create as many API users as the number of hosts. Conversely, if you wish to have many users on a single host, then again, you need to create as many API users as needed.

2. Creating a API User Account with REST and SDK Access

To create an API user account for accessing PAM360 REST APIs or SDK via services or applications, do the steps that follow:

> **Note:** PAM360 user granted with web access can later be given REST and SDK access as needed. However, users created via REST and Application User will have no web access to PAM360 permanently. Therefore, we always recommend creating a standard user with REST or SDK access, allowing for future modifications to include web access if necessary.

i. Navigate to **Users >> Users >> Add API User >> REST and Application User**.
ii. **First Name | Last Name**: Enter here the user's first name and last name.
iii. **Username**: Enter here a unique name. This name identifies the API user.
iv. **Email**: Enter the user's email address where the user will be notified for any modifications to the account, access, or role.
v. **Role**: Select an appropriate role for the user from the drop-down; this will determine the type of role and privilege this user will have in PAM360. Refer to this section to learn more about the user roles available in PAM360.
vi. **Scope**: By default, users created in PAM360 are assigned the scope of Passwords Owned and Shared. This means they can access passwords owned by them or shared with them by other PAM360 users.
vii. **Department | Location**: Enter the department and the location where the user belongs to. These fields are not mandatory. However, populating valid data in these fields with the correct values will be helpful while searching or grouping the users.



viii. **REST API Access**: Enable this option if the user account requires access to the PAM360 REST API.

ix. **SDK Access**: Enable this option if the user account requires access to the PAM360 API via the PAM360 SDK.

x. **Authentication Token**: Generate an Authentication Token from here if providing the above access. This token serves as a user validation key for API calls received from other applications or services.

xi. **Access Validity**: Select a date until which the Authentication Token will remain valid. Exceeding the provided date will invalidate the Authentication Token, requiring the generation of a new token to extend validity for further use of PAM360 REST APIs.

xii. **Hostname Validation**: Enable this validation to verify user machines from which API calls are invoked. Enabling this feature restricts API invocation from the machines that are not pre-defined in the Hostname field.

xiii. **Hostname**: Enter the Hostname of the machine from which the user is allowed to perform REST and Application operations.

xiv. **Allow Resource Addition for Other Users**: Enabling this option permits users to create resources via the API and assign them to other users.

Click **Save** to add the user account to the PAM360 repository.

SCIM-Based User Provisioning in PAM360

SCIM (System for Cross-domain Identity Management) provisioning offers a standardized approach for managing user identities across various systems and applications. In the context of PAM360, SCIM integration facilitates seamless provisioning of users and user groups, empowering administrators to efficiently manage access to critical resources. Since PAM360 is an on-premise application, a provisioning agent is required from the identity provider to establish the connection to the PAM360 server. This enables administrators to effortlessly synchronize user and user group details between their existing identity management systems and the PAM360 application using the provided PAM360 SCIM APIs. This eliminates the need for manual intervention, ensuring that user information remains up-to-date and aligned with organizational requirements.

User Account Requirements - An API user account with the Privileged Administrator, Administrator, or custom role with the Manage SCIM Provisioning privilege is required to implement SCIM-based identity provisioning in PAM360.

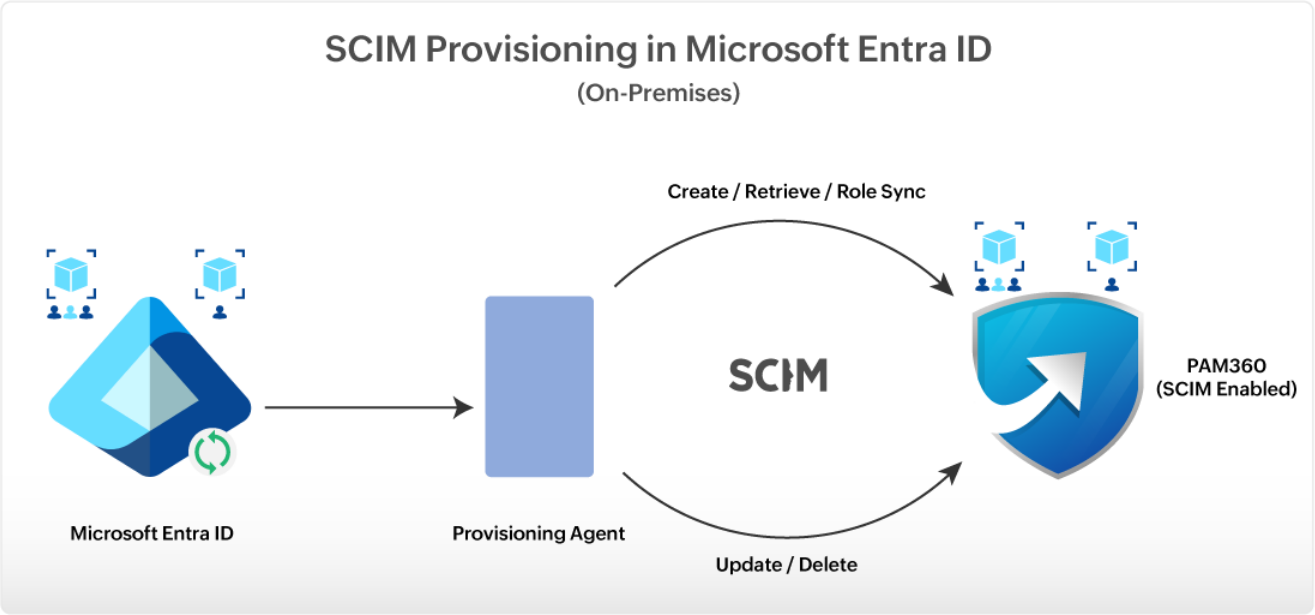
The PAM360 SCIM APIs are divided into three categories, comprising sixteen APIs in total, aimed at facilitating CRUD (Create, Read, Update, Delete) operations:

- Users
- Groups
- SCIM Configuration

These APIs empower users to provision and manage user identities across various identity management systems. For further insights into the PAM360 SCIM APIs and their functionalities, please refer to the SCIM API section.

> **Note:** To disable SCIM functionality in PAM360 at the cost of emergency, navigate to **Admin >> Manage >> Emergency Measures**. Select the Disable SCIM API Access checkbox and click **Save >> OK**.

The image below illustrates how PAM360 SCIM APIs operate to provision users and user groups in Entra ID. This documentation also offers a sample configuration of user and user group provisioning from Microsoft Entra ID to PAM360.



1. Prerequisites
2. Configuring SCIM Provisioning in Microsoft Entra ID for PAM360 Application
3. Limitations

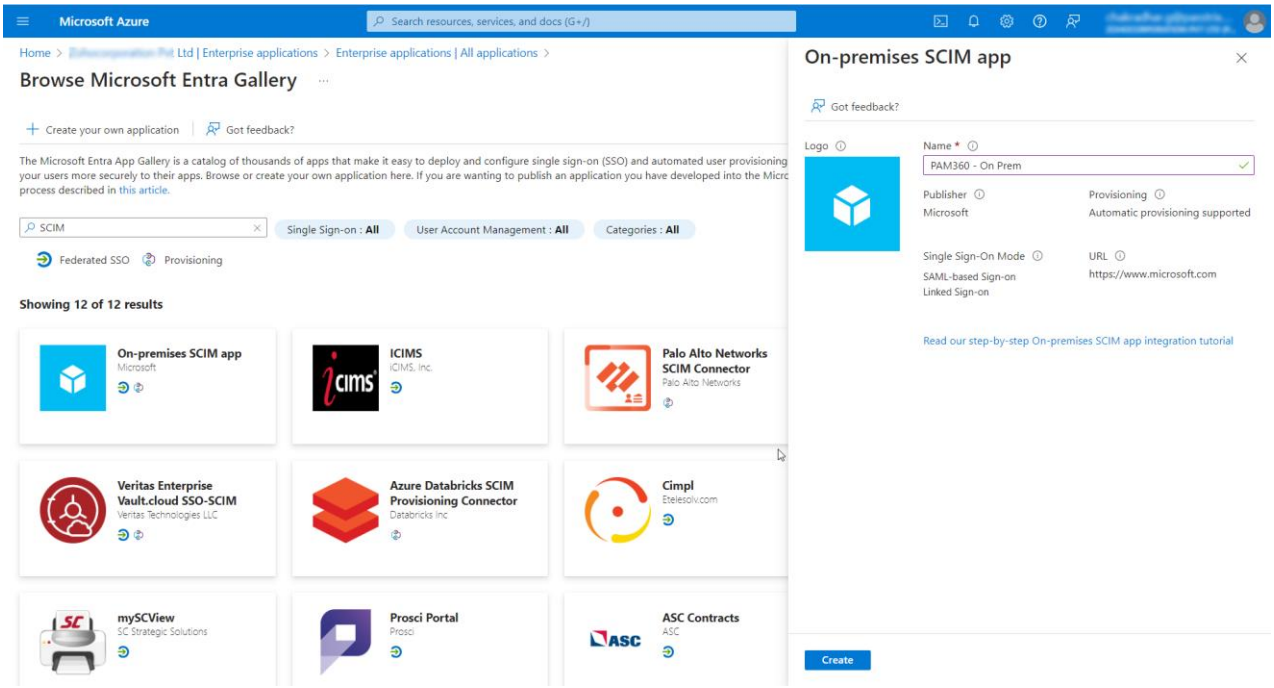
1. Prerequisites

In order to set up SCIM provisioning in Entra ID, create a PAM360 API user account with the Privileged Administrator, Administrator, or custom role with the Manage SCIM Provisioning privilege enabled. Ensure to copy the user Authentication Token generated during the API user creation process, as it will be required for the SCIM configuration in the identity management system or application. In addition to the above requirements, you will need a Windows Server endpoint connected to the PAM360 server network with a proper SSL connection for SCIM agent deployment.

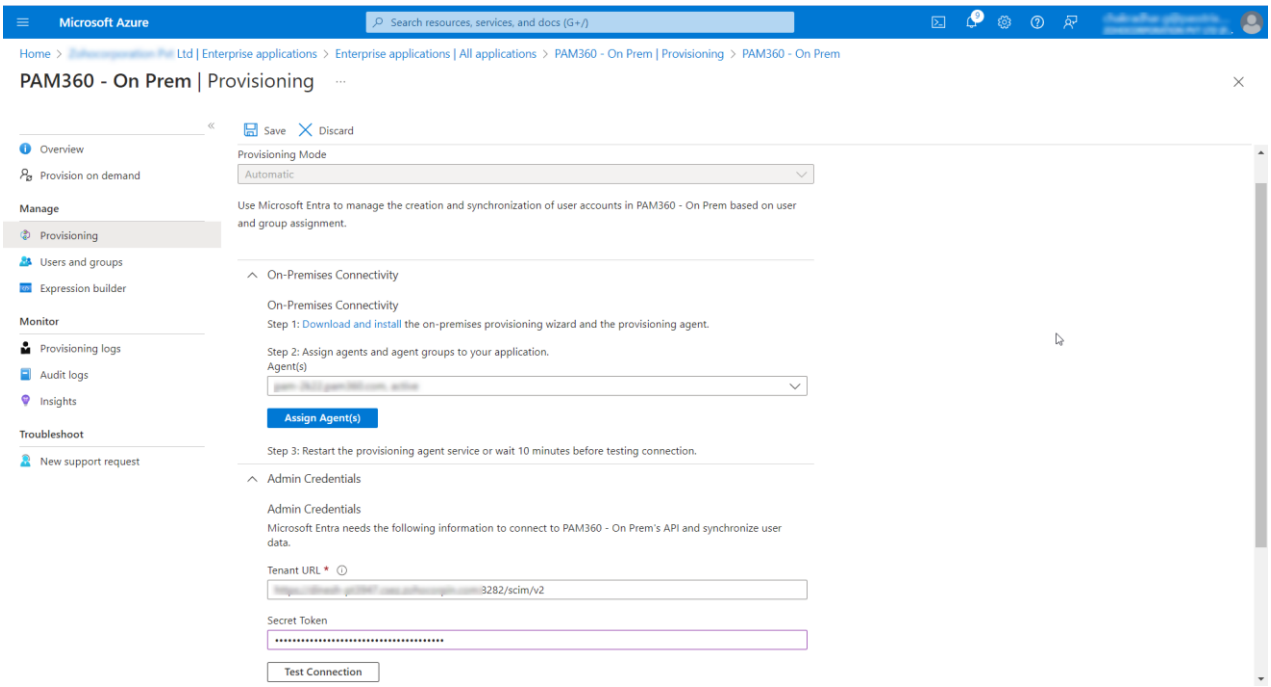
2. Configuring SCIM Provisioning in Microsoft Entra for PAM360 Application

1. Log in to the Azure Portal and navigate to the Microsoft Entra ID.
2. In the left-side pane, click on **Enterprise applications** located under **Manage**.
3. In the new page that appears, click the **Add** button and add a new SCIM application.
4. Look out for the On-premise SCIM app in the search results.

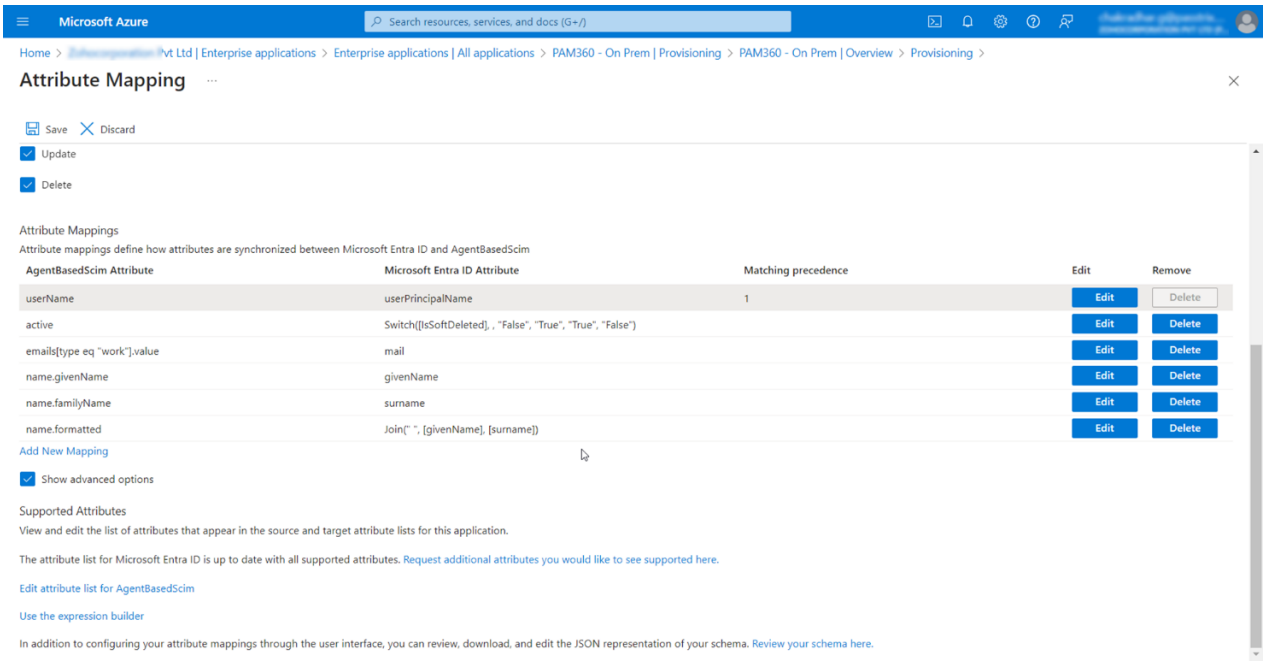
5. Upon clicking the **On-premise SCIM app** application, enter the **Name** for the application and click **Create**.



6. In the application page that opens, click **Provisioning** under **Manage**.
7. Select **Automatic** as your provisioning mode.
8. Expand the **On-Premises Connectivity** tab, and follow the steps given below to assign agents and agent groups to the SCIM application:
   a. Log in to a Windows Server machine that resides in the PAM360 server network using the global administrator credentials.
   b. Download and install the on-premises provisioning wizard and the provisioning agent on the Windows Server machine.
   c. Restart the provisioning agent service and check if the agent name is listed in the **Agent(s)** dropdown on the Entra ID SCIM Provisioning page.
   d. If listed, select your agent from the dropdown and click **Assign Agents**.
9. Next, expand **Admin Credentials** and enter the PAM360 SCIM API endpoint URL in the **Tenant URL**.
   For example: **https://<Hostname-of-the-PAM360-server>:<Port>/scim/v2**
10. Enter the **Authentication Token** copied from PAM360 during the API user creation for the SCIM configuration with the relevant role.
11. Click the **Test Connection** button and wait until the authentication is completed.

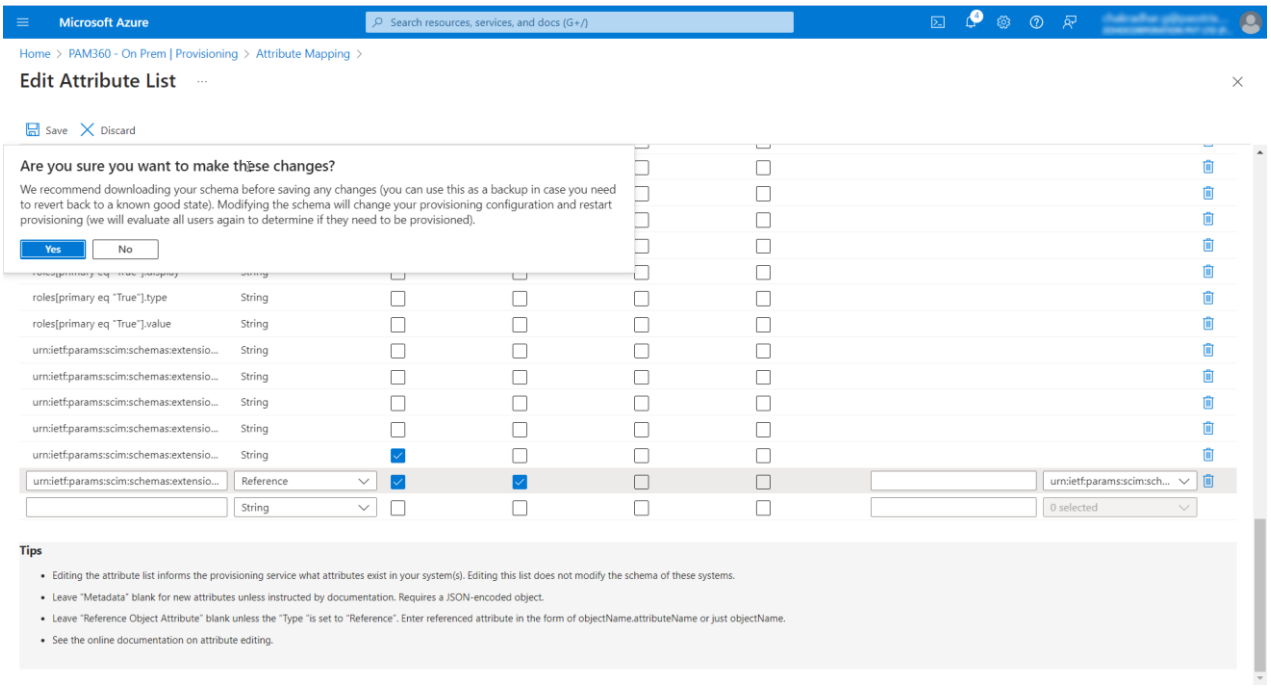


12. Expand the **Mappings** tab and click on **Provision Microsoft Entra ID Users**.
13. Select the supported attributes under **Attribute Mappings** and delete the rest.
    Refer to the below SCIM API section to know more about the supported attributes.

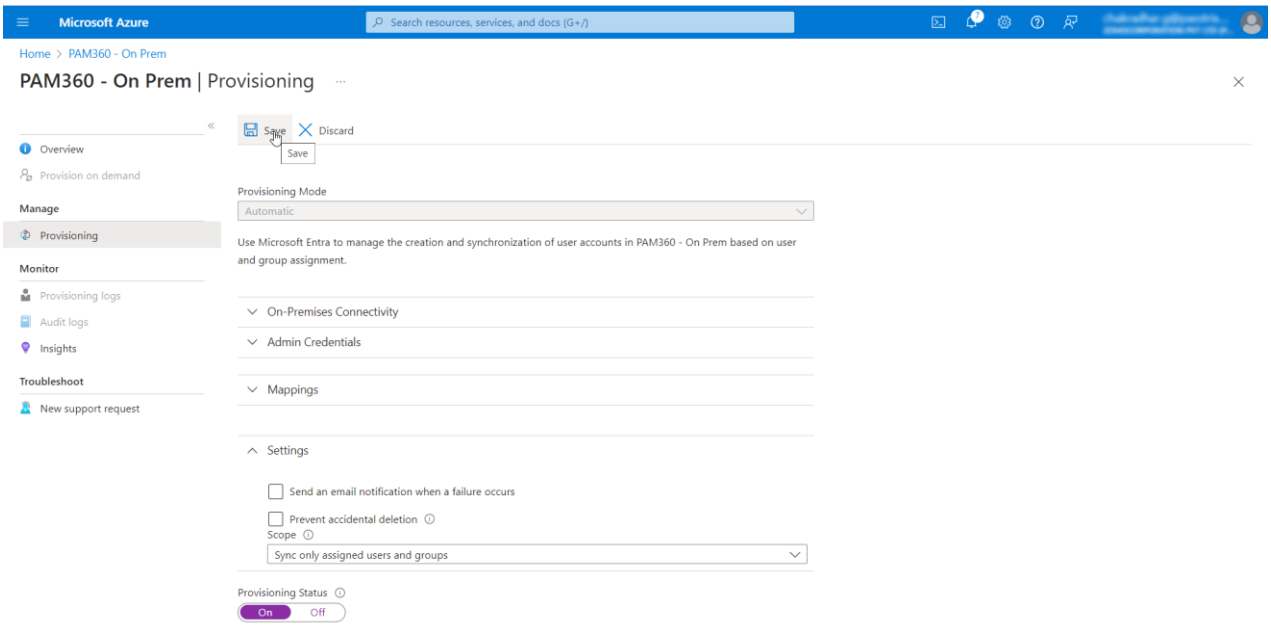


14. Scroll down and select the **Show advanced options** checkbox.
15. Click the **Edit attribute list for AgentBasedScim** link and select your desired attributes as shown in the image below.

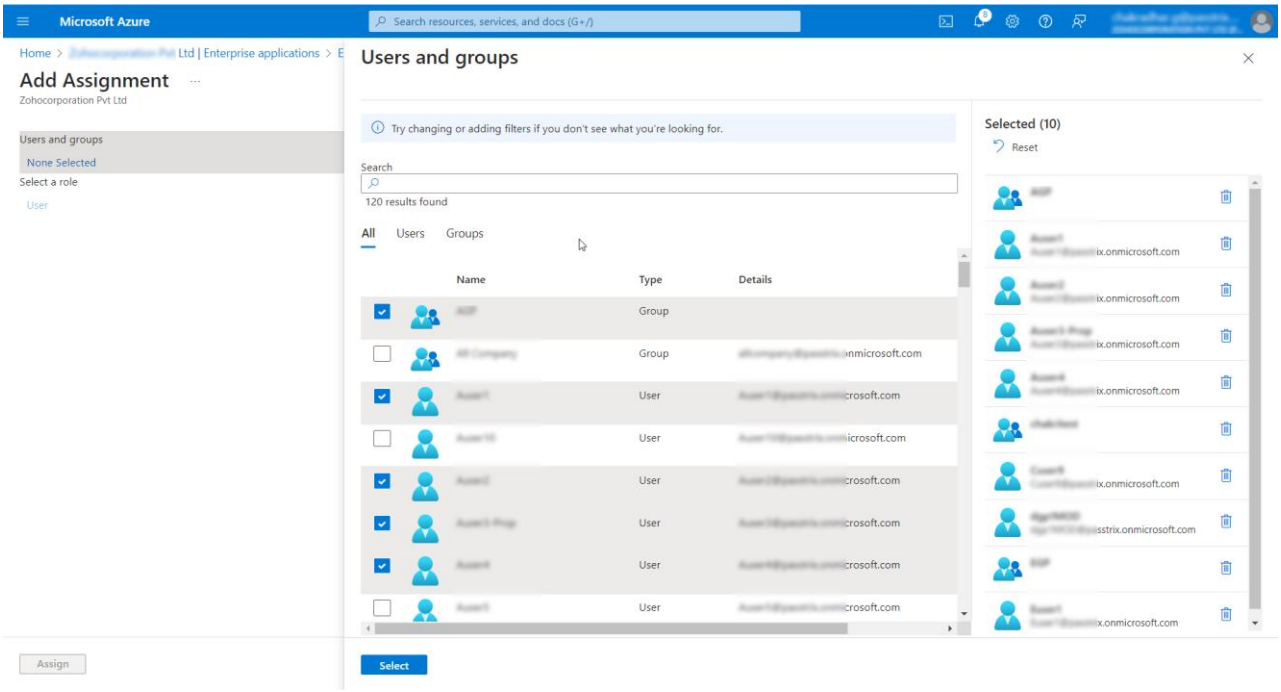
Note: To import SCIM users as Entra domain users in PAM360, add these custom schema extension attributes:
urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User:userType
urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User:domain



16. Click **Yes >> Save** to apply the selected attributes.
17. Click on **Provision Microsoft Entra ID Groups** under **Mappings** and edit the attributes as required.
18. Expand **Settings** and select the **Sync only assigned users and groups** option from the dropdown.
19. Turn on **Provisioning Status** and click **Save**.



20. Navigate to the **Users and groups** tab in the created SCIM application and click the **Add user/group** button at the top menu.
21. Click on **None Selected** and add the users and groups as required.
22. Click **Select >> Assign** to assign the selected users and groups to the application.



Whenever a user or a user group is added/modified in the PAM360 SCIM application of Entra ID, with the PAM360 SCIM APIs and the agent deployed, those user and user group will be synced between the identity management system or application (i.e., Entra ID) and the PAM360 server at synchronization. You can check the status of users and groups provisioned with the PAM360 server in the **Overview** tab.

3. Limitations

1. Exercise caution when deleting users or user groups added via SCIM Provisioning on PAM360, as it can cause synchronization issues with the identity management system or application and PAM360.
2. Only the Authentication Token generated while creating an API user in PAM360 can be used for authentication during SCIM provisioning in any identity management system or application.
3. The data exchange process may encounter errors due to disparities in the structure and storage of group information (nested group) between the identity management system or application and PAM360.
4. SCIM API requests might fail if an unsupported parameter is included.
5. In case the user principal name (UPN) of an imported user is altered in the identity management system or application, any corresponding modifications may not be reflected in the PAM360, nor will a new user with the updated UPN be automatically added.

Understanding PAM360 SCIM APIs

Introduction

SCIM APIs serve as the foundation for seamlessly integrating identity management processes across various systems and applications. With SCIM implementation in PAM360, SCIM APIs enable administrators to automate user and group provisioning tasks, ensuring efficient management of access to critical resources. SCIM APIs use the GET, POST, PUT, PATCH, and DELETE methods to offer a wide range of CRUD operations.
To access PAM360 SCIM APIs, authentication from PAM360 is required. This involves creating a REST API user account with the respective role and using the generated user authentication token for authentication purposes. The generated authentication token can be sent in two ways for authentication:

- As an Authentication Token header, similar to REST APIs.
- As a Bearer Token in the Authorization header.

This document will help you understand the supported SCIM endpoints, APIs, and attributes. The supported SCIM Endpoints are listed below:

1. Users
2. Groups
3. SCIM Configuration
   3.1 ServiceProviderConfig
   3.2 Schemas
   3.3 ResourceTypes

1. Users

To manage users in PAM360, you can make use of the PAM360 SCIM APIs provided in this section.

Supported Core Attributes

Attributes	Data type	Required? (for POST)	Required? (for PUT)
userName	String	Yes	No
givenName	String	Yes	Yes
familyName	String	Yes	Yes
emails	Array	Yes	Yes
password	String	No	No
roles	Array	Yes	No
active	Boolean	Yes	No

Supported Custom Schema Extension Attributes

urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User:userType

urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User:domain

Attributes	Types	Descriptions
userType	0|1|2|3	Types of users. 0 - Local, 1 - AD, 2 - Entra ID, 3- LDAP.
domain	String	Domain to which the domain user is affiliated.

Below are the PAM360 SCIM APIs for the User endpoint:

1.1 Get User

Description

To get the details of a user in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users/{userId}
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users/2101
```

Sample Output


```
{
"emails": [
{
"type": "work",
"value": "john@teams.com", "primary": true
}
],
"roles": [
{
"value": "Privileged Administrator",

"primary": true
}
],
"meta": {
"created": "2024-02-29 13:54:37.451",
"location": "https://192.168.176.251 :8282/scim/v2/Users/2101", "resourceType":
"User"
},
"schemas": [ "urn:ietf:params:scim:schemas:core:2.0:User"
],
"name": { "givenName": "John",
"familyName": "G"
},
"active": true, "id": 2101,
"userName": "john@teams.onmicrosoft.com",
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User": {
"userType": "0"
},
}
```

1.2 Get All Users

Description

To get all the details of users in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users
```

HTTP Method

GET

Query Syntax

Utilize SCIM endpoints for querying users based on attributes. Each query includes an operator, attribute, and attribute value in this format:

<baseURL>/scim/users?filter=<attribute> <operator> "<attributeValue>"

Supported Attributes

Attributes	Descriptions
userName	Identifies a user based on their username.
active	Returns a list of users based on their status, which is `true` (active) or `false` (inactive).

Supported Operators

Operators	Definitions
eq	equals
sw	starts with
co	contains
ew	ends with

Sample Request

For Querying,

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users?filter=userName eq "test1"
```

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users?filter=active eq "true"
```

For Pagination,

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users?startIndex=1&count=50
```

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users?startIndex=51&count=50
```

.

For combining Querying and Pagination,

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users?filter=userName eq "test1"&startIndex=1&count=50
```

Sample Response

{
"totalResults": 2,
"startIndex": 1,
"itemsPerPage": 100, "schemas": [
"urn:ietf:params:scim:api:messages:2.0:ListResponse"
],
"Resources": [
{
"emails": [
{
"type": "work",
"value": "guest@teams.onmicrosoft.com", "primary": true
}
],
"meta": {

"created": "2024-04-02 11:04:45.235",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/2", "resourceType": "User"
},
"roles": [
{
"value": "Password User", "primary": true
}
],
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User": {
"userType": "0"
},
"schemas": ["urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User"
],
"name": { "givenName": "guest", "familyName": ""
},
"active": true, "id": 2,
"userName": "guest"
},
{
"emails": [
{
"type": "work",
"value": "aaaadmin@teams.onmicrosoft.com", "primary": true
}
],
"meta": {
"created": "2024-04-02 11:04:45.235",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/1", "resourceType": "User"
},

```
"roles": [
{
"value": "Privileged Administrator", "primary": true
}
],
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User": {
"userType": "0"
},
"schemas": [ "urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User"
],
"name": { "givenName": "admin", "familyName": ""
},
"active": true, "id": 1,
"userName": "admin"

}
]
}
```

1.3 Create a New User

Description

To create a new user or Entra domain user to PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users
```

HTTP Method

POST

Sample Request

```
{
"userName": "john@teams.onmicrosoft.com", "name": {
"givenName": "John",
"familyName": "G"
},
"emails": [
{
"type": "work",
"value": "john@teams.com", "primary": true
```

```
}
],
"roles": [
{
"value": "Privileged Administrator", "primary": true
}
],
"active": true, "schemas": [
"urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User"
],
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User": {
"userType": "0"
}
}
```

For creating an Entra domain user in PAM360,

```
{
"userName": "john@teams.onmicrosoft.com", "name": {
"givenName": "John",
"familyName": "G"

},
"emails": [
{
"type": "work",
"value": "john@teams.com", "primary": true
}
],
"roles": [
{
"value": "Privileged Administrator", "primary": true
}
],
"active": true, "schemas": [
"urn:ietf:params:scim:schemas:core:2.0:User",
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User"
],
"urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User": {
"userType": "2",
"domain": "teams.onmicrosoft.com"
}
}
```

Sample Output

```
{
"emails": [
{
"type": "work",
"value": "john@teams.com", "primary": true
}
],
"meta": {
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/601", "resourceType": "User"
},
"roles": [
{
"value": "Privileged Administrator", "primary": true
}
],
"schemas": [ "urn:ietf:params:scim:schemas:core:2.0:User"
],
"name": { "givenName": "John",
"familyName": "G"
},
"active": true, "id": 601,
"userName": "john@teams.onmicrosoft.com"
}
```


1.4 Update User Details

Description

To update the details of a user in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/{userId}
```

HTTP Method

PUT

Sample Request

```
{
"userName": "john@teams.onmicrosoft.com", "name": {
"givenName": "John", "familyName": "Doe"
},
"emails": [
{
"type": "work",
"value": "john.doe@teams.com", "primary": true
}
],
"roles": [
{
"value": "Password User", "primary": true
}
],
"active": true, "schemas": [
"urn:ietf:params:scim:schemas:core:2.0:User"
],
}
```

Sample Output

```
{
"emails": [
{
"type": "work",
"value": "john.doe@teams.com", "primary": true
}
],
"meta": {
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/601", "resourceType": "User"
},
"roles": [

{
"value": "Password User", "primary": true
}
],
"schemas": [ "urn:ietf:params:scim:schemas:core:2.0:User"
],
"name": { "givenName": "John", "familyName": "Doe"
},
"active": true, "id": 601,
"userName": "john@teams.onmicrosoft.com"
}
```

1.5 Patch User Details

Description

To update specific values of a user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Users/{userId}
```

HTTP Method

PATCH

Supported Path Values

Paths	Data Types of the Value
active	Boolean
emails	Array
emails[type eq \"work\"].value	String
name	JSON Object
name.familyName	String
name.givenName	String
roles	Array
roles[primary eq\"True\"].value	String

Sample Request

```
{
"schemas": [ "urn:ietf:params:scim:api:messages:2.0:PatchOp"
],
"Operations": [
{
"op": "Replace",
"path": "active", "value": true
},
{
"op": "Replace",
"path": "name.familyName", "value": "asdf"
}
]
}
```

To change the email of a user,

```
{
"schemas": [ "urn:ietf:params:scim:api:messages:2.0:PatchOp"
],
"Operations": [
{
"op": "Replace",
"path": "emails[type eq \"work\"].value", "value": true
}
]
}
```

To change the role of a user,

```
{
"schemas": [ "urn:ietf:params:scim:api:messages:2.0:PatchOp"
],
"Operations": [
{
"op": "Replace",
"path": "roles[primary eq \"True\"].value", "value": "Password User"
}
]
}
```

Sample Output

Upon successful update, you will get the HTTP Status Code 204.

2. Groups

To manage SCIM provisioned groups in PAM360.

Supported Core Attributes

Attributes	Descriptions
displayName	Identifies a group based on its display name.
id	Identifies a group based on its ID.
members	Provides a list of users associated with the group.

Below are the PAM360 SCIM APIs for the Group endpoint:

2.1 Get Details of a Group

Description

To get the details of a group added to PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups/{groupId}
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups/1202
```

Sample Response

```
{
"displayName": "Group4", "meta": {
"created": "2024-01-30 14:01:08.461",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/1202", "resourceType": "Group"
},
"members": [
{

"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
},
{
"value": 301,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/301"
}
],
"schemas": [ "urn:ietf:params:scim:schemas:core:2.0:Group"
],
"id": 1202
}
```


2.2 Get Details of All Groups

Description

To get the details of all the groups added to PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups
```

HTTP Method

GET

Query Syntax

Utilize SCIM endpoints for querying groups based on attributes. Each query includes an operator, attribute, and attribute value in this format:

<baseURL>/scim/groups?filter=<attribute> <operator> "<attributeValue>"

Supported Attributes

Attributes	Description
displayName	Identifies a group based on its display name.

Supported Operators

Operators	Definitions
eq	equals
sw	starts with
co	contains
ew	ends with

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups
```

For Querying,

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups?filter=displayName eq "group1"
```

For Pagination,

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups?startIndex=1&count=50
```

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups?startIndex=51&count=50
```

For combining Querying and Pagination,

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups?filter=displayName eq
"group1"&startIndex=1&count=50
```

Sample Response


```
{
"totalResults": 7,
"startIndex": 6,
"itemsPerPage": 2,
"schemas": [
"urn:ietf:params:scim:api:messages:2.0:ListResponse"
],
"Resources": [
{
"displayName": "Group4",
"meta": {
"created": "2024-01-30 14:01:08.461",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/1202",
"resourceType": "Group"
},
"members": [
{
"value": 301,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/301"
}
],
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
],
"id": 1202
},
{
"displayName": "john",
"meta": {
"created": "2024-01-31 18:13:30.024",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/1501",
"resourceType": "Group"
},
"members": [
{
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
```

```
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
}
],
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
],
"id": 1501
}
]
}
```

2.3 Create a Group

Description

To add a group to PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups
```

HTTP Method

POST

Sample Request

```
{
"displayName": "Group14",
"meta": {
"created": "2024-01-30 14:01:08.461",
"resourceType": "Group"
},
"members": [
{
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
},
```

```
{
"value": 301,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/301"
}
],
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
]
}
```


Sample Response


```
{
"displayName": "Group14",
"meta": {
"created": "2024-01-30 14:01:08.461",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/2101",
"resourceType": "Group"
},
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
],
"members": [
{
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
},
{
"value": 301,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/301"
}
],
"id": 2101
}
```


2.4 Update Group Details

Description

To update the details of the group added in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/{groupId}
```

HTTP Method

PUT

Sample Request

```
{
[
"displayName": "Group24",
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
],
"members": [
{
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
},
{
"value": 2,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/2"
}
]
}
```

Sample Response

```
{
"displayName": "Group24",
"meta": {
"created": "2024-01-30 14:01:08.461",
"location": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/1202",
"resourceType": "Group"
},
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group"
],
"members": [
```

```
{
"value": 9,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/9"
},
{
"value": 2,
"$ref": "https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Users/2"
}
],
"id": 1202
}
```

2.5 Patch Group

Description

To update a detail of the group added to PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/Groups/{groupId}
```

HTTP Method

PATCH

Sample Request

```
{
"schemas": [
"urn:ietf:params:scim:api:messages:2.0:PatchOp"
],
"Operations": [
{
"op": "Replace",
"path": "displayName",
"value": "Group4"
},
```

```
{
"op": "Add",
"path": "members",
"value": [
{
"value": "1504"
}
]
},
{
"op": "Remove",
"path": "members",
"value": [
{
"value": "1501"
},
{
"value": "1502"
}
]
}
]
}
```

Sample Response

Upon successful update, you will receive the HTTP Status code 204.

2.6 Delete Group

Description

To delete a group from PAM360.

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups/{groupId}

HTTP Method

DELETE

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Groups/2101
```

Sample Output

Upon successful deletion, you will receive the HTTP Status code 204.

3. SCIM Configuration

Below are the PAM360 SCIM APIs for the ServiceProviderConfig, Schemas, and ResourceTypes endpoints:

3.1 ServiceProviderConfig

Description

To get all the details of SCIM implementation in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/ServiceProviderConfig
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/ServiceProviderConfig
```

Sample Response

```
{
"patch": {
"supported": true
},
"filter": {
"maxResults": 0,
"supported": true
},
"documentationUri": "https://www.manageengine.com/privileged-access-management/help/scim-config.html",
"authenticationSchemes": [
{
"documentationUri": "https://www.manageengine.com/privileged-access-management/help/scim-config.html",
"name": "API Token",
"description": "Authentication scheme using the API Token",
"type": "apitoken",
"primary": true
},
{
"documentationUri": "https://www.manageengine.com/privileged-access-management/help/scim-config.html",
"name": "OAuth Bearer Token",
"description": "Authentication scheme using the OAuth Bearer Token Standard",
"type": "oauthbearertoken",
"primary": false
}
],
"meta": {
"location": "/ServiceProviderConfig",
"resourceType": "ServiceProviderConfig"
},
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:ServiceProviderConfig"
],
"etag": {
"supported": false
},
"sort": {
"supported": false
},
"bulk": {
"maxPayloadSize": 0,
"maxOperations": 0,
"supported": false
},
"changePassword": {
"supported": false
}
}
```

3.2 Schemas

3.2.1 Get a Schema

Description

To get a schema using its ID.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Schemas/{schemaId}
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Schemas/urn:ietf:params:scim:schemas:core:2.0:Group
```

Sample Response


```
{
"meta": {
"location": "Schemas/urn:ietf:params:scim:schemas:core:2.0:Group",
"resourceType": "Schema"
},
"name": "Group",
"description": "Group",
"attributes": [
{
"uniqueness": "none",
"name": "displayName",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
```

```
"required": false
},
{
"name": "members",
"mutability": "readWrite",
"type": "complex",
"multiValued": true,
"returned": "default",
"required": false,
"subAttributes": [
{
"uniqueness": "none",
"name": "value",
"description": "Identifier of the member of this Group.",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "$ref",
"description": "Location of the member of this Group.",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
}
]
}
],
"id": "urn:ietf:params:scim:schemas:core:2.0:Group"
}
```


3.2.2 Get All Schemas

Description

To get all the schemas implemented and the supported params in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Schemas
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/Schemas
```

Sample Output


```
{
"startIndex": 1,
"totalResults": 3,
"itemsPerPage": 100,
"Resources": [
{
"meta": {
"location": "/Schemas/urn:ietf:params:scim:schemas:core:2.0:User",
"resourceType": "Schema"
},
"name": "User",
"description": "User Account",
"attributes": [
{
"uniqueness": "server",
"name": "userName",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": true
},
{
"uniqueness": "none",
"name": "name",
"mutability": "readWrite",
"type": "complex",
"multiValued": false,
"returned": "default",
"required": false,
"subAttributes": [
{
"uniqueness": "none",
"name": "familyName",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
```

```
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "givenName",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
}
]
},
{
"name": "active",
"mutability": "readWrite",
"type": "boolean",
"multiValued": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "password",
"mutability": "writeOnly",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "never",
"required": false
},
{
"uniqueness": "none",
"name": "emails",
"mutability": "readWrite",
"type": "complex",
"multiValued": true,
"returned": "default",
"required": false,
"subAttributes": [
{
"uniqueness": "none",
"name": "value",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
```

"required": false
},
{
"uniqueness": "none",
"name": "type",
"canonicalValues": [
"work"
],
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"name": "primary",
"mutability": "readWrite",
"type": "boolean",
"multiValued": false,
"returned": "default",
"required": false
}
]
},
{
"name": "roles",
"description": "A list of roles for the User that collectively represent who the User is, e.g., 'Password User', 'Administrator'.",
"mutability": "readWrite",
"type": "complex",
"multiValued": true,
"returned": "default",
"required": false,
"subAttributes": [
{
"uniqueness": "none",
"name": "value",
"description": "The value of a role.",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "display",
"description": "A human-readable name, primarily used for display purposes. READ-ONLY.",

"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "type",
"description": "A label indicating the attribute's function.",
"canonicalValues": [],
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"name": "primary",
"description": "A Boolean value indicating the 'primary' or preferred attribute value for this attribute. The primary attribute value 'true' MUST appear no more than once.",
"mutability": "readWrite",
"type": "boolean",
"multiValued": false,
"returned": "default",
"required": false
}
]
}
],
"id": "urn:ietf:params:scim:schemas:core:2.0:User"
},
{
"meta": {
"location": "Schemas/urn:ietf:params:scim:schemas:core:2.0:Group",
"resourceType": "Schema"
},
"name": "Group",
"description": "Group",
"attributes": [
{
"uniqueness": "none",
"name": "displayName",
"mutability": "readWrite",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",

```
"required": false
},
{
"name": "members",
"mutability": "readWrite",
"type": "complex",
"multiValued": true,
"returned": "default",
"required": false,
"subAttributes": [
{
"uniqueness": "none",
"name": "value",
"description": "Identifier of the member of this Group.",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "$ref",
"description": "Location of the member of this Group.",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
}
]
}
],
"id": "urn:ietf:params:scim:schemas:core:2.0:Group"
},
{
"meta": {
"location":
"Schemas/urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User",
"resourceType": "Schema"
},
"name": "Domain",
"description": "Domain of the User in case of AD, LDAP or Entra ID.",
"attributes": [
{
"uniqueness": "none",
"name": "userType",
"canonicalValues": [
"0",
```

```
"1",
"2",
"3"
],
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
},
{
"uniqueness": "none",
"name": "domain",
"mutability": "immutable",
"type": "string",
"multiValued": false,
"caseExact": false,
"returned": "default",
"required": false
}
],
"id": "urn:ietf:params:scim:schemas:extension:pam360_domain:2.0:User"
}
]
}
```


3.3 ResourceTypes

3.3.1 Get a Resource Type

Description

To get the details of a SCIM resource implemented in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/scim/v2/ResourceTypes/{typeId}
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/ResourceTypes/Group
```

Sample Response

```
{
"schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
"endpoint": "/Groups",
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:ResourceType"
],
"name": "Group",
"description": "Group",
"id": "Group"
}
```

3.3.2 Get all Resource Types

Description

To get the details of all the SCIM resources implemented in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/ResourceTypes
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/scim/v2/ResourceTypes
```

Sample Response

```
{
"totalResults": 2,
"startIndex": 1,
"itemsPerPage": 100,
"schemas": [
"urn:ietf:params:scim:api:messages:2.0:ListResponse"
],
"Resources": [
{
"schema": "urn:ietf:params:scim:schemas:core:2.0:User",
"endpoint": "/Users",
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:ResourceType"
],
"name": "User",
"description": "User Account",
"id": "User"
},
{
"schema": "urn:ietf:params:scim:schemas:core:2.0:Group",
"endpoint": "/Groups",
"schemas": [
"urn:ietf:params:scim:schemas:core:2.0:ResourceType"
],
"name": "Group",
"description": "Group",
"id": "Group"
}
]
}
```

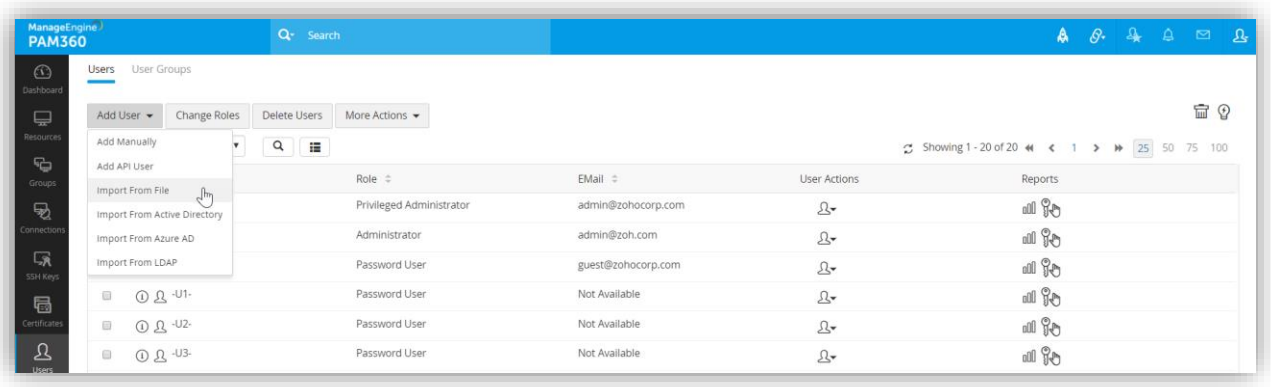
Import Users from a File

PAM360 allows you to import users from an Excel, CSV, TSV, or Text file. Click here to view sample files and learn more about the file formats supported for importing. Apart from standard details such as First Name, Last Name, User Name, Email Address, Department, Location etc, you can also enable/disable Two-Factor Authentication for specific users by adding an additional text Enable/Disable.

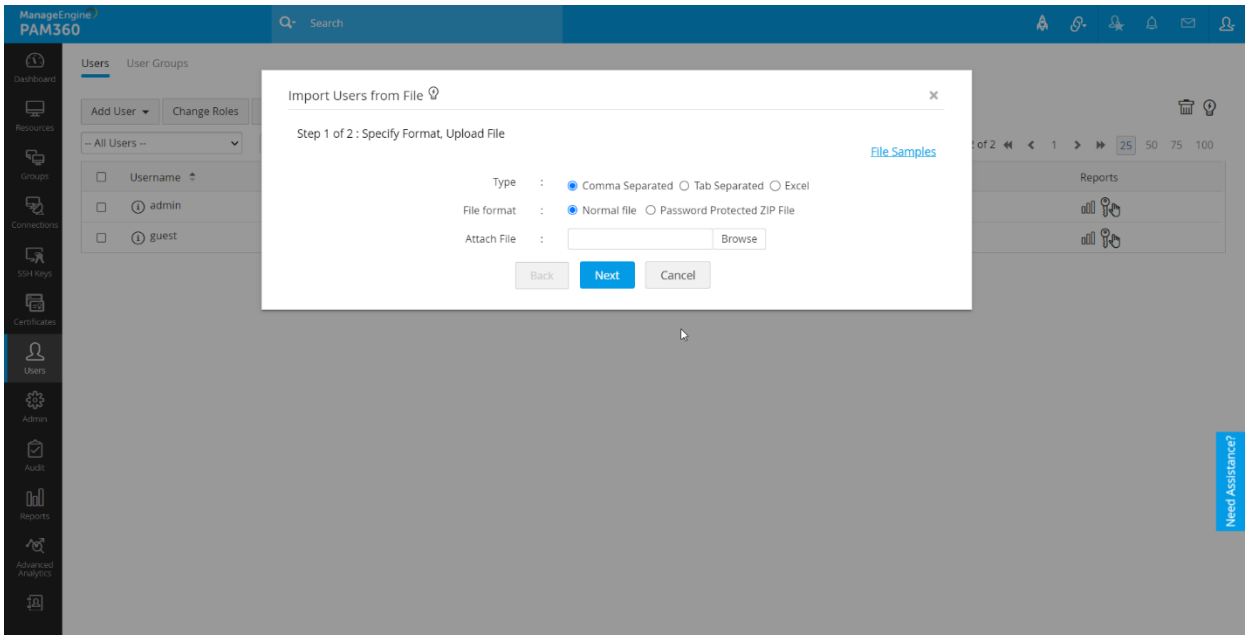
> **Note:** Earlier, it was possible to import a .txt file containing comma-separated data, and in step 2, the data would be listed as expected. However, from build 6400 onwards, if the entries are comma-separated, the file format must be .csv. Files with tab-separated values should be saved as .txt or .tsv for importing.

Steps Required

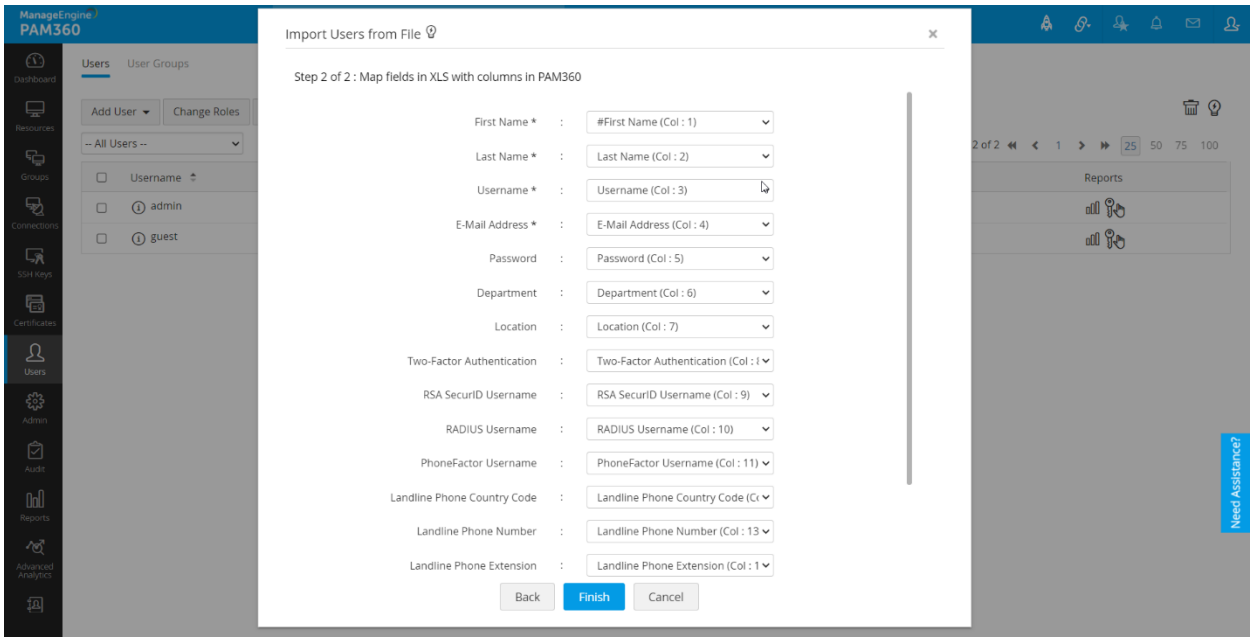
1. Navigate to **Users** tab.
2. Click **Add User** and select **Import From File** from the drop down list.



3. In the pop-up form that appears, specify the file type and file format. Click **Browse** and select the file to import users.



4. Click **Next**.
5. The user inventory of PAM360 contains six fields by default -
    - First Name
    - Last Name
    - User Name
    - Email Address
    - Department
    - Location



6. Among the above six fields, the first four are mandatory, and their attributes must be present in the uploaded file to complete the import process. The attributes in the file will get mapped automatically to their respective fields based on the column names, irrespective of the column order. You can also manually specify the attributes from the

file that corresponds to a specific PAM360 user field.

7. Click **Finish** to complete the user import process.
8. The successful/failed import process will be logged as an audit with detailed information. Navigate to the **User Audit** section in the **Audit** tab for details.

> **Note:** If you are unable to find the reason for import failure from the Audit tab, set the log level to Debug mode and perform the import operation again. Now, you will get the detailed failure traces from the log file available in the <PAM360 Installation Folder>\logs\user_import_errors.txt directory.

Importing Users from Active Directory

PAM360 integrates with Active Directory in your environment and allows import of users from there. Users logged into the Windows system using their domain account can log into PAM360 directly.

Steps Required

There are four steps involved in importing users from Active Directory:

1. **Importing Users**
2. **Specifying Appropriate User Roles**
3. **Enabling AD Authentication**

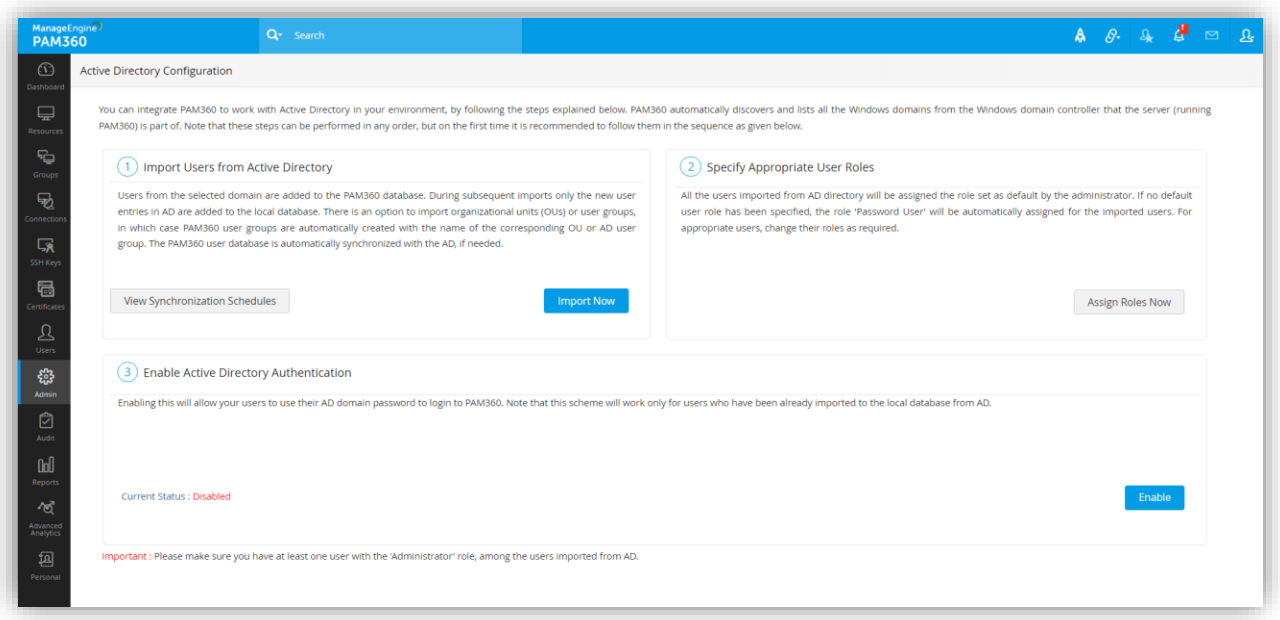
To begin, navigate to **Admin >> Authentication >> Active Directory**. The Active Directory Configuration page is displayed.

1. Importing Users

The first step is to provide credential details and import users from Active Directory. PAM360 automatically gets the list of the domains present under the "**Microsoft Windows Network**" folder of the server of which the running PAM360 is part of. You need to select the required domain from the list and provide necessary domain controller credentials.

To do this:

1. Click the **Import Now** button. Alternatively, you can also access this from **Users >> Add user >> Import from Active Directory.**



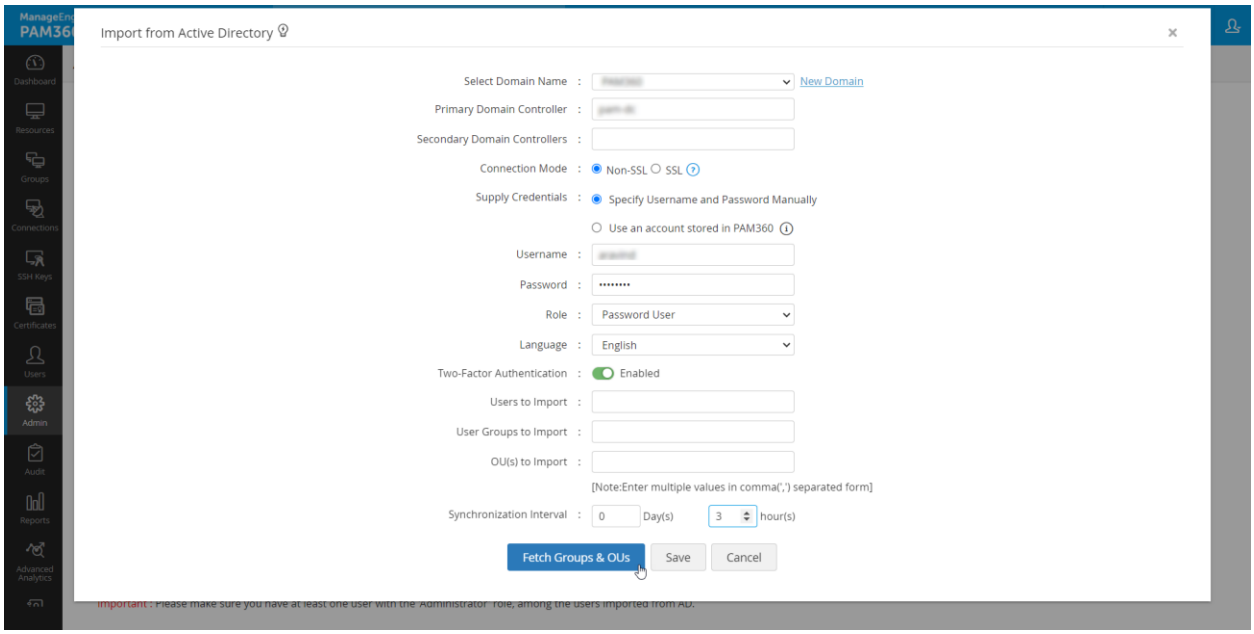
2. In the pop-up form that appears, select the required **Domain Name**, which forms part of the AD from the drop-down.
3. Specify the DNS name of the domain controller. This domain controller will be the primary domain controller.
4. In case, the **Primary Domain Controller** is down, **Secondary Domain Controllers** can be used. If you have secondary domain controllers, specify their DNS names in comma separated form. One of the available secondary domain controllers will be used. When you use SSL mode, make sure the DNS name specified here matches the CN (common name) specified in the SSL certificate for the domain controller.
5. **Supply Credentials:** Enter a valid user credential (user name and password) having read permission in the domain controller. (If you want to import users from multiple domains, you may enter the username as <DomainName>\<username>. For example, if you want to import DOMAIN A users by giving DOMAIN B username/password, you need to enter the username as <DOMAIN B>\username)).
6. **Connection Mode:** For each domain, you can configure if the connection should be over an encrypted channel for all communication. To enable the SSL mode, the domain controller should be serving over SSL in port 636 and you will have to import the domain controller's root certificate into the PAM360 server machine's certificate store.
7. **Role:** By default, the Password User role is assigned to the users imported from Active Directory. Select the desired role from the drop-down menu to change the user roles. The selected role will be applied to all the users imported from the specified Group(s) or Organizational Unit(s) of the Active Directory.

> **Note**: Initial settings applied during import remain consistent in subsequent schedules unless altered.

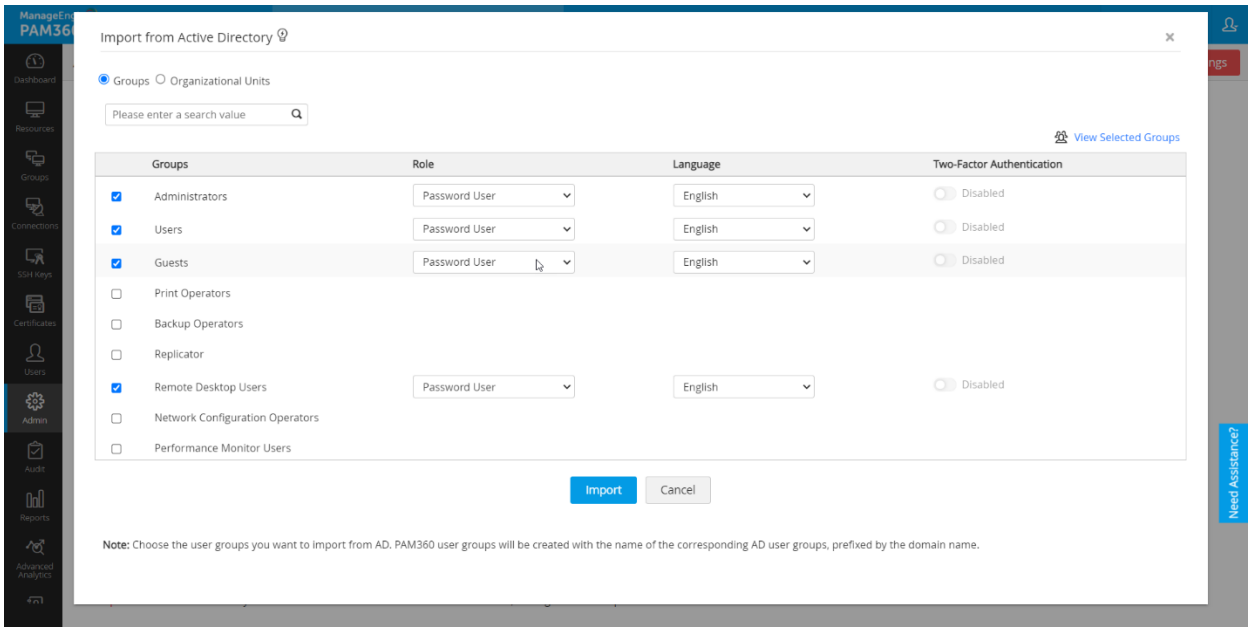
8. **Language:** You can also change the language for the users you intend to import by utilizing the **Language** field.
9. **Two-Factor Authentication**: By default, Two-factor authentication is enabled for the users imported from the Active Directory. Disable the toggle button beside the Two-factor authentication field to disable 2FA for the users to be imported.

> **Note**: If Two-Factor Authentication is disabled globally in the Admin tab, users imported from Active Directory during this period will have the Two-Factor Authentication disabled automatically.

10. **Users to Import:** By default, PAM360 will populate all the organizational units (OUs) and groups from Active Directory. If you want to import only a particular user, enter the required user name(s) in comma separated form.
11. **User Groups to Import / OU(s) to Import:** Similarly, you can choose to import only specific user groups or organizational units (OUs) from the domain. You can specify the names in the respective text fields in comma separated form.
12. **Synchronization Interval:** Whenever new users get added to the Active Directory, there is provision to automatically add them to PAM360 and keep the user database in sync. Enter the time interval at which PAM360 has to query the Active Directory to keep the user database in sync. Please ensure you set the sync interval at 3 hours or more based on the number of Groups and OU's imported.
13. Click **Save**. Soon after hitting this "Save" button, PAM360 will save the domain details. During subsequent imports, only the new user entries in AD are added to the local database.



14. To look out for specific users, user groups, or organizational units, click the **Fetch Groups & OUs** button and execute the following actions:
    i. Select either **Groups** or **Organizational Units** and choose the required groups/OUs you want to import from Active Directory. You can also specify roles and languages for each group or organizational unit.
    ii. To view the selected groups, click the **View Selected Groups** link at the top-right corner.
    iii. After selecting the required groups or organizational units, click **Import**.
15. In case of importing organizational units (OUs) and Active Directory groups, user groups are automatically created with the name of the corresponding OU / AD group.



> **Note**: As mentioned above, to enable SSL mode, the domain controller should be serving over SSL in port 636. If the certificate of the domain controller is not signed by a certified CA, you will have to manually import the certificate into the PAM360 server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.

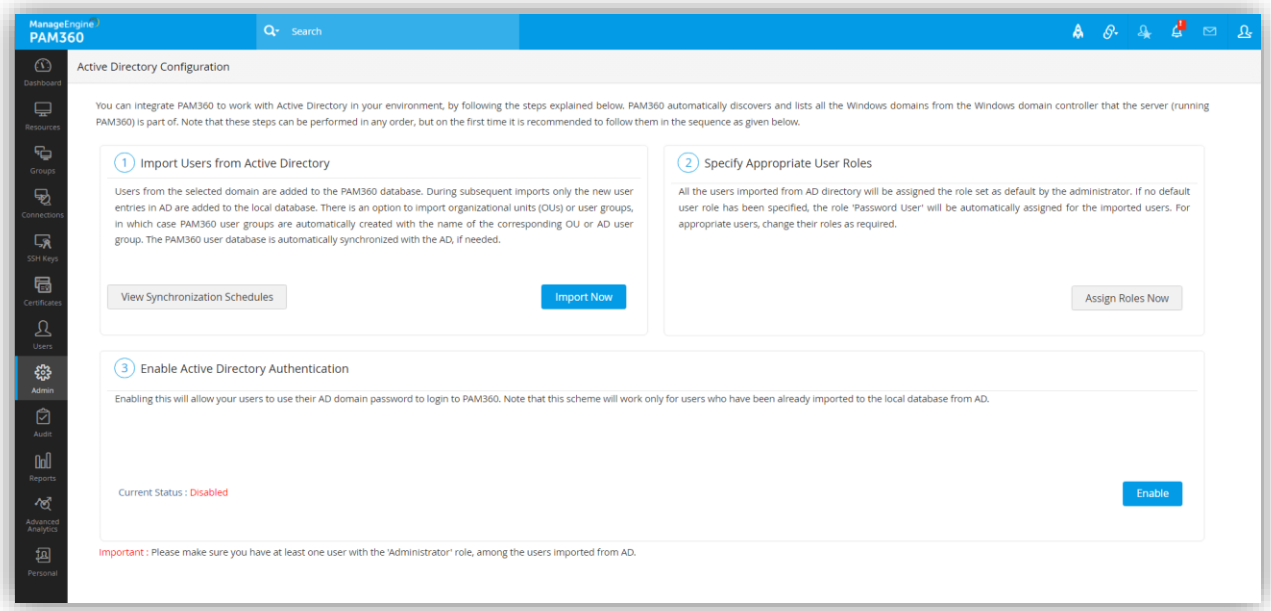
To import domain controller's certificate into PAM360 machine's certificate store: (you can use any procedure that you normally use to import the SSL certificates to the machine's certificate store. One example is given below)

1. In the machine where PAM360 is installed, launch Internet Explorer and navigate to **Tools >> Internet Options >> Content >> Certificates**.
2. Click **Import**.
3. Browse and locate the root certificate issue by your CA.
4. Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
5. Click **Import** again.
6. Browse and locate the domain controller certificate.
7. Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
8. Apply the changes and close the wizard.
9. Repeat the procedure to install other certificates in the root chain.

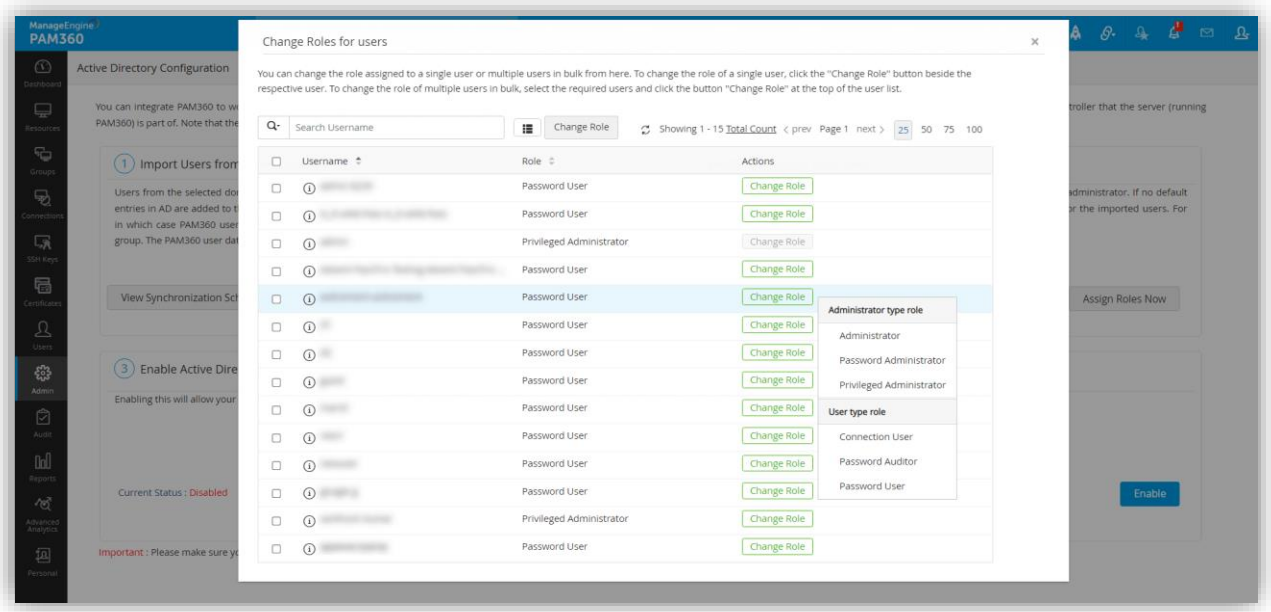
2. Specifying Appropriate User Roles

All the users imported from AD will be assigned the **Password User** role by default. To assign specific roles to specific users,

1. Click the button **Assign Roles Now.**

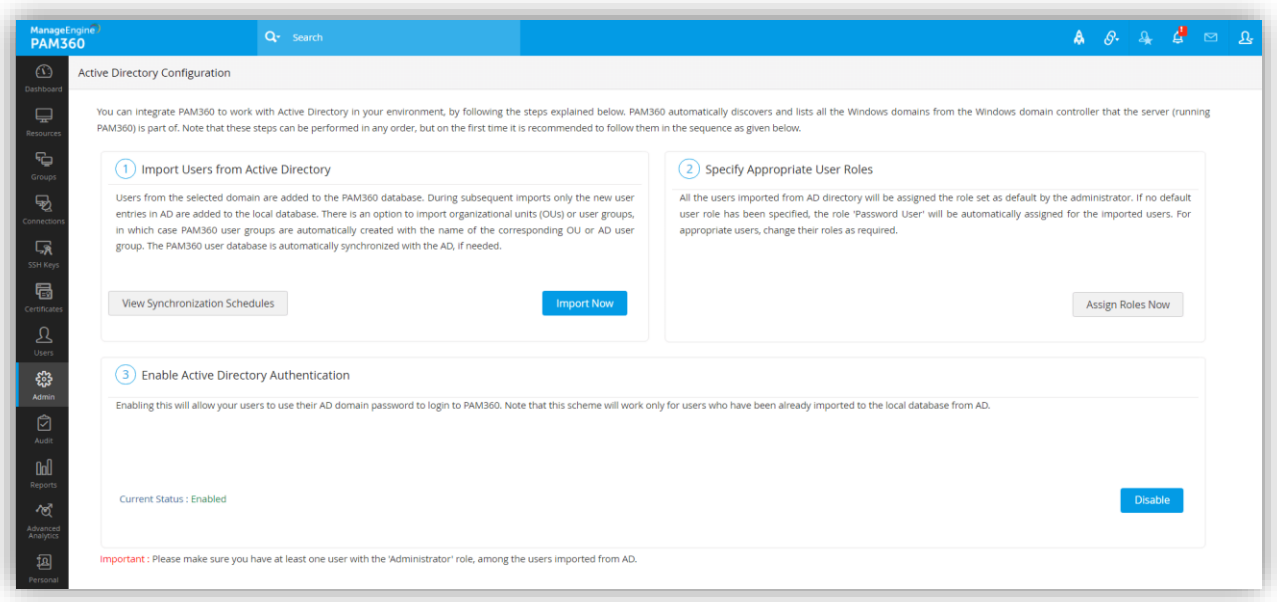


2. In the pop-up form that opens, all the Users imported from AD are listed.
3. Click **Change role** button against desired users for whom you wish to change the role and select the appropriate role from the drop down.
4. Click **Save** and the required roles are set for the users.



3. Enabling AD Authentication

The third step is to enable AD authentication. This will allow your users to use their AD domain password to login to PAM360. Note that this scheme will work only for users who have already been imported to the local database from Active Directory.



Troubleshooting Tip

The browser will keep asking for Domain User credentials on the login page, if computer account credentials are incorrect. In that case, cancel the pop-up to access the PAM360 login page.

Importing Users from Microsoft Entra ID

Integrate Azure Active Directory (AD) with PAM360 and import users and user groups from Azure AD. Through this integration, users can login to PAM360 using their Microsoft Entra ID credentials, in both **Windows and Linux platforms.** After integration into PAM360, the user details and user group structure is maintained exactly as it is in the Azure AD platform.

> **Note:** You can only import users who don't have multi-factor authentication (MFA) enabled in the Microsoft Entra ID portal.

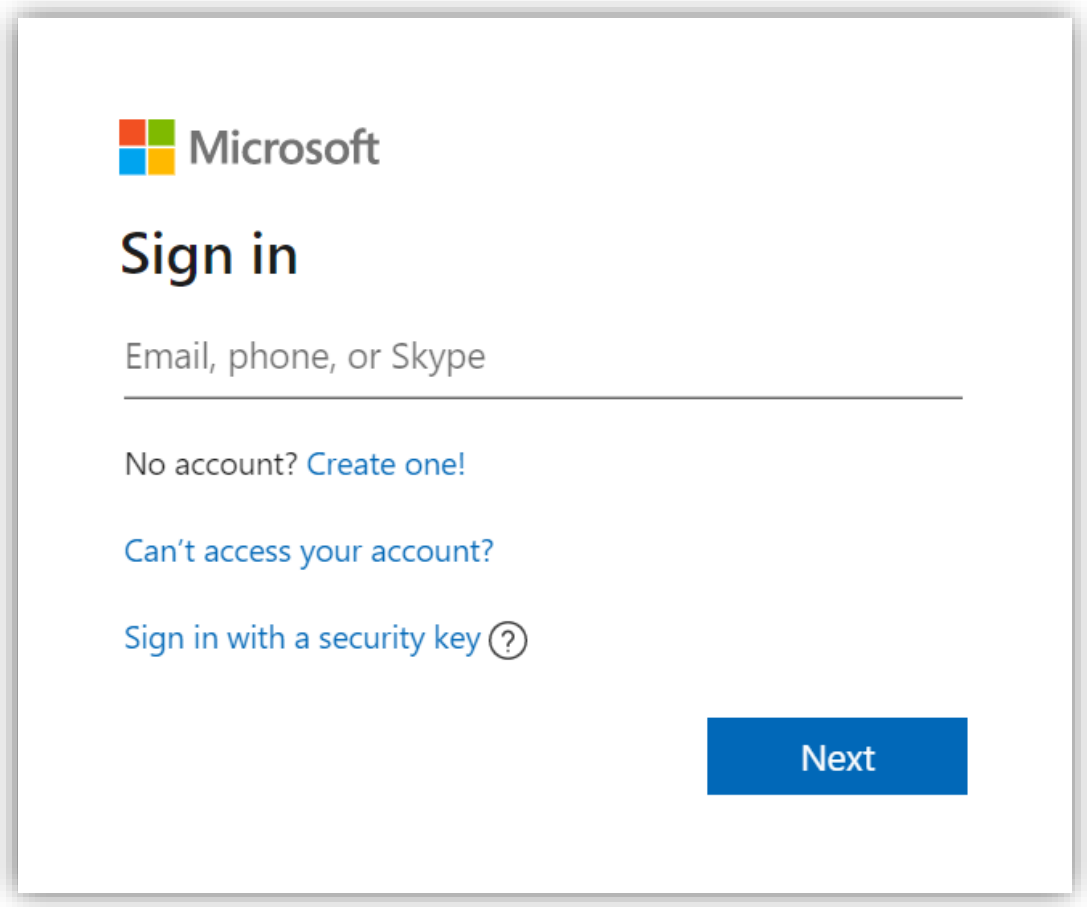
Following are detailed steps to register PAM360 in the Azure portal and import users into PAM360:

1. Registering PAM360 in Microsoft Entra ID Portal
2. Steps to Import Users from Microsoft Entra ID
   - 2.1 Importing Users from Microsoft Entra ID
   - 2.2 Specifying Appropriate User Roles
   - 2.3 Enabling Microsoft Entra ID Authentication
   - 2.4 Troubleshooting Tips

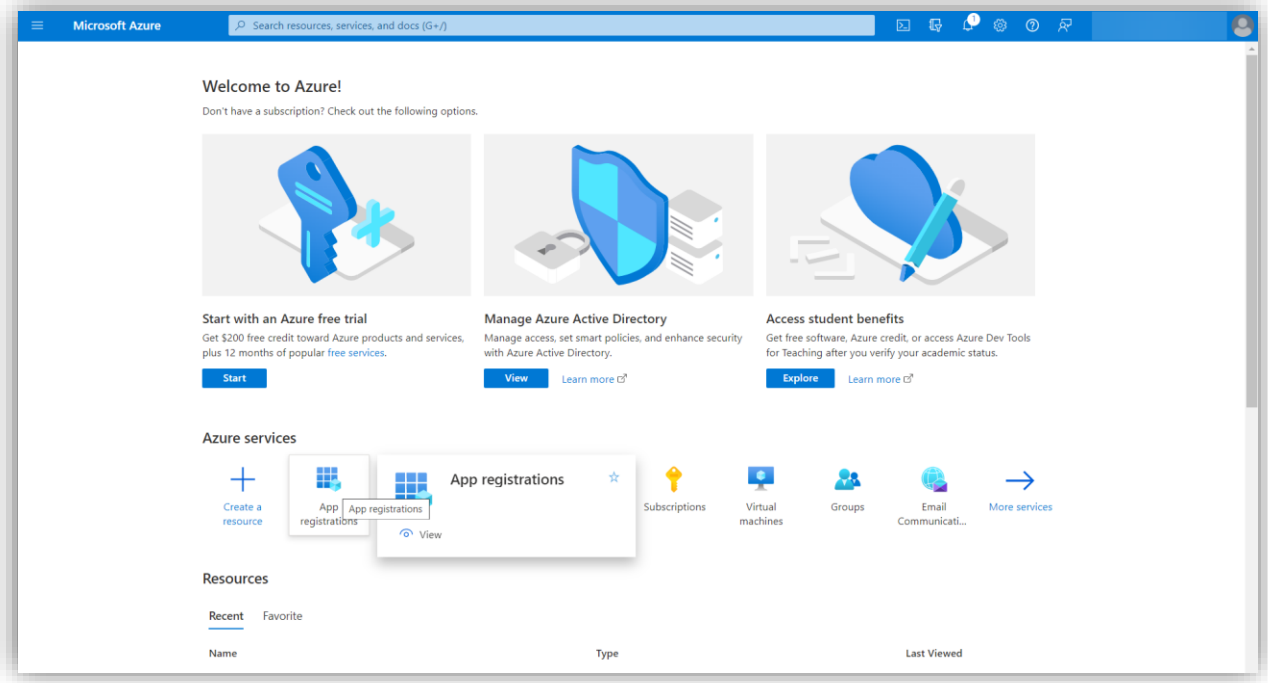
1. Registering PAM360 in Microsoft Entra ID Portal

To integrate PAM360 with Azure AD and import users, PAM360 should first be added as a native client application in your Azure AD portal. Follow the steps given below to register PAM360 as an application:

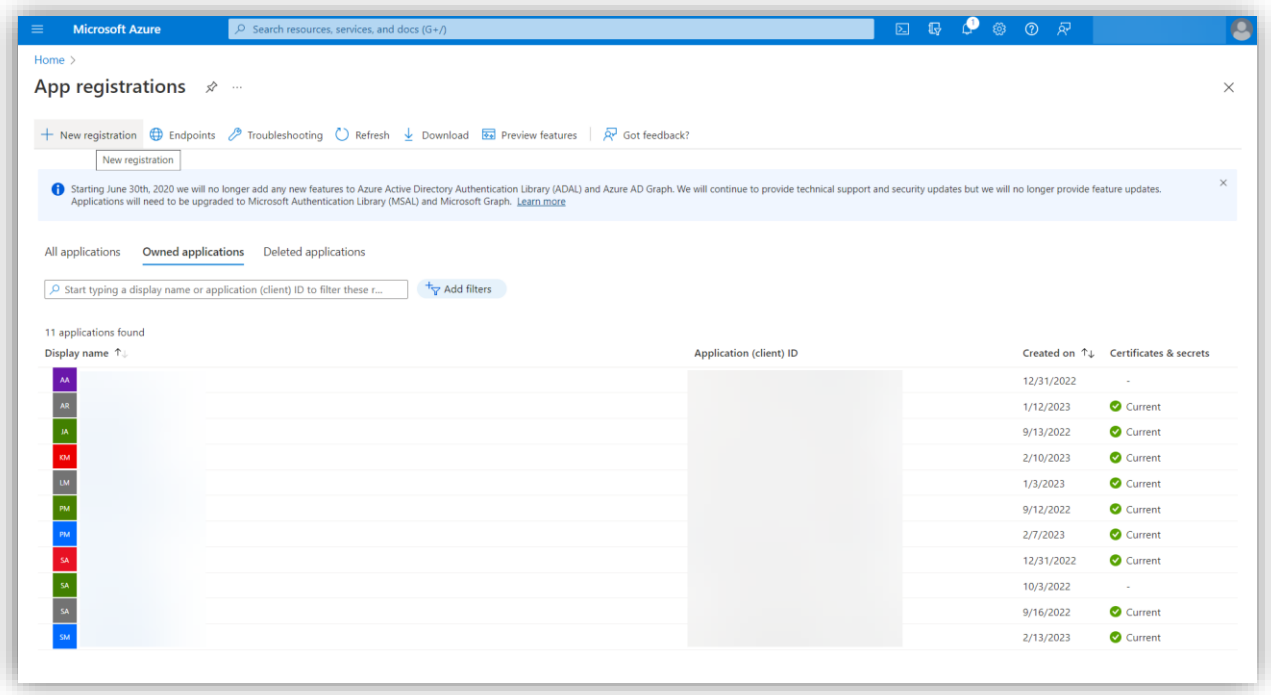
1. Log in to your Microsoft Azure portal.



2. Click **App registrations** from the **Microsoft Azure** home page.

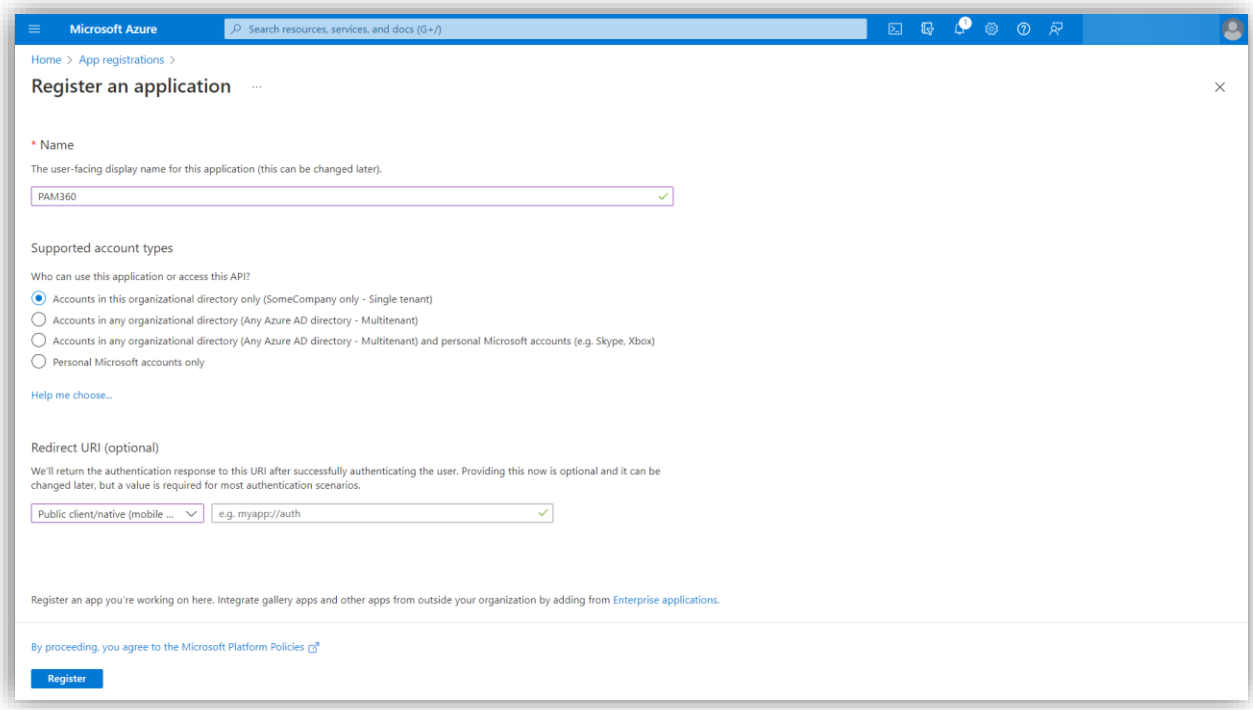


3. Click **+ New registration** from the top bar.

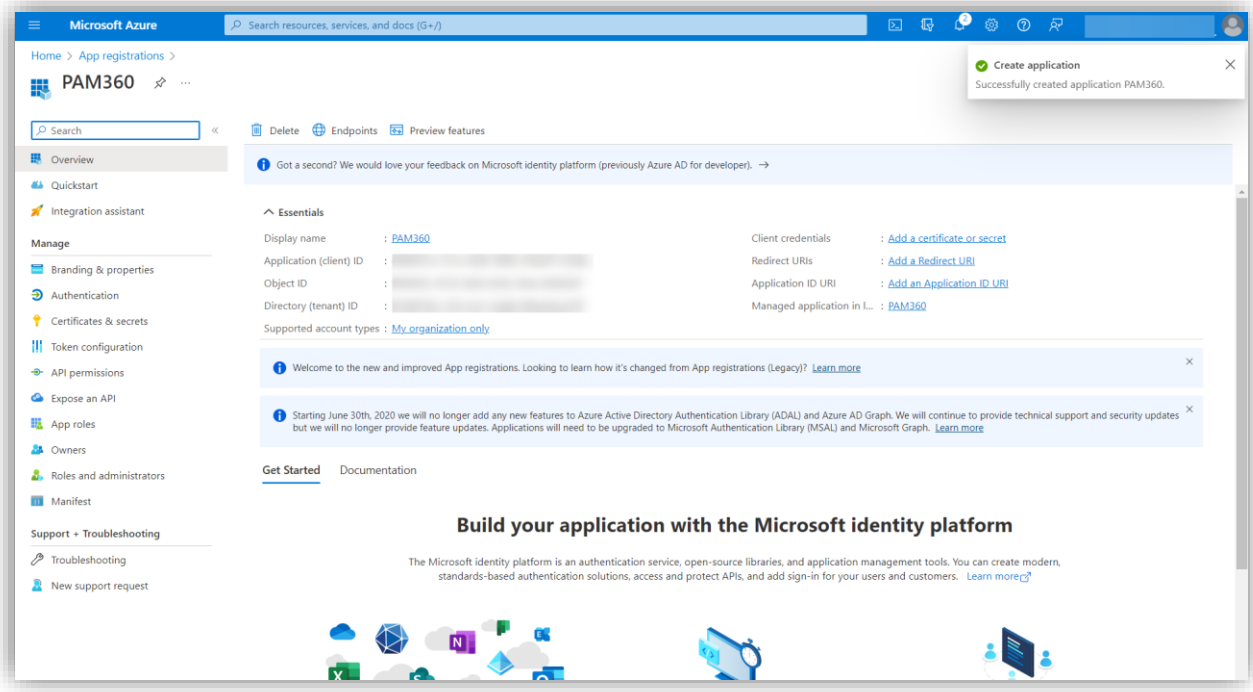


4. In the **Register an application** page, enter the following attributes:
   i. **Enter Name** as PAM360 or any name of your choice.
   ii. **Choose Supported account types - Accounts in this organizational directory only - Single tenant).**
   iii. Enter the **Redirect URI** of PAM360 application.

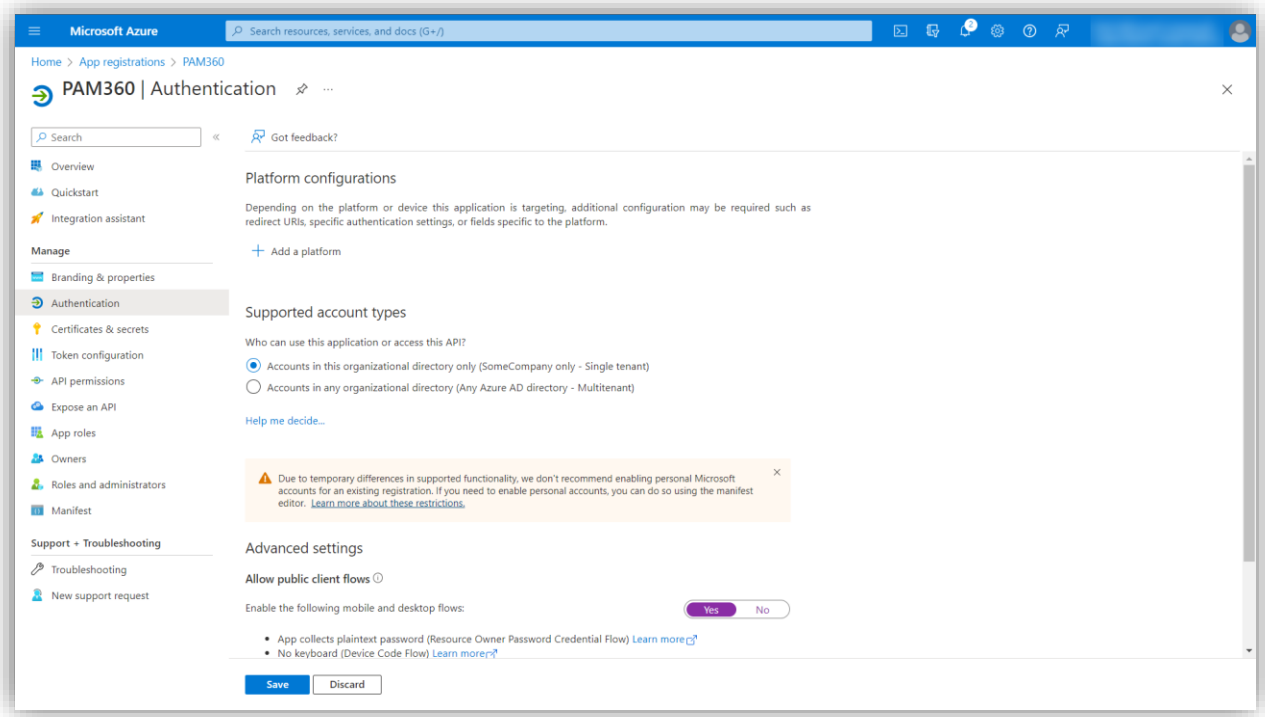
5. Click **Register**. PAM360 will be added as an application in the Azure AD portal.



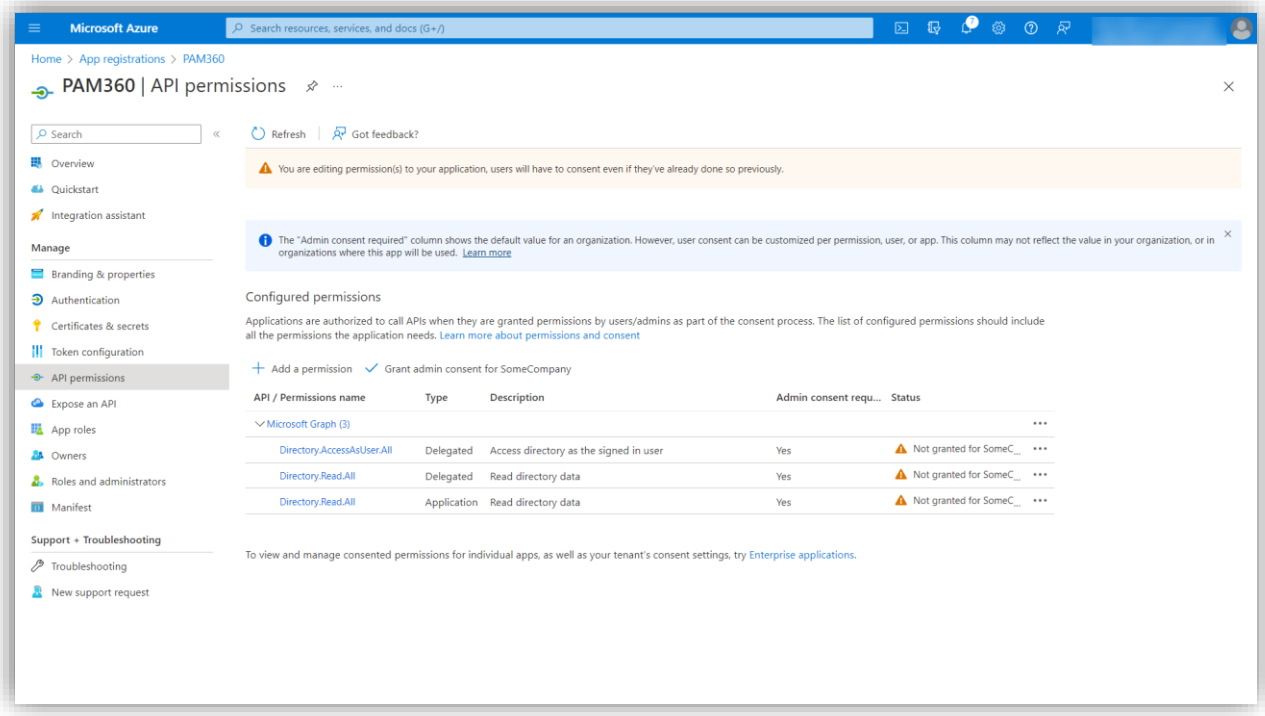
6. You will be taken to the page with the details of the newly registered PAM360 application.



7. Click **Authentication** under **Manage** in the left pane. In the **Authentication** page, under **Advanced settings,** enable **Allow public client flows** by clicking **Yes.**



8. Click **API permissions** under **Manage** in the left pane. In the **API Permissions** page, click **+Add a permission**.



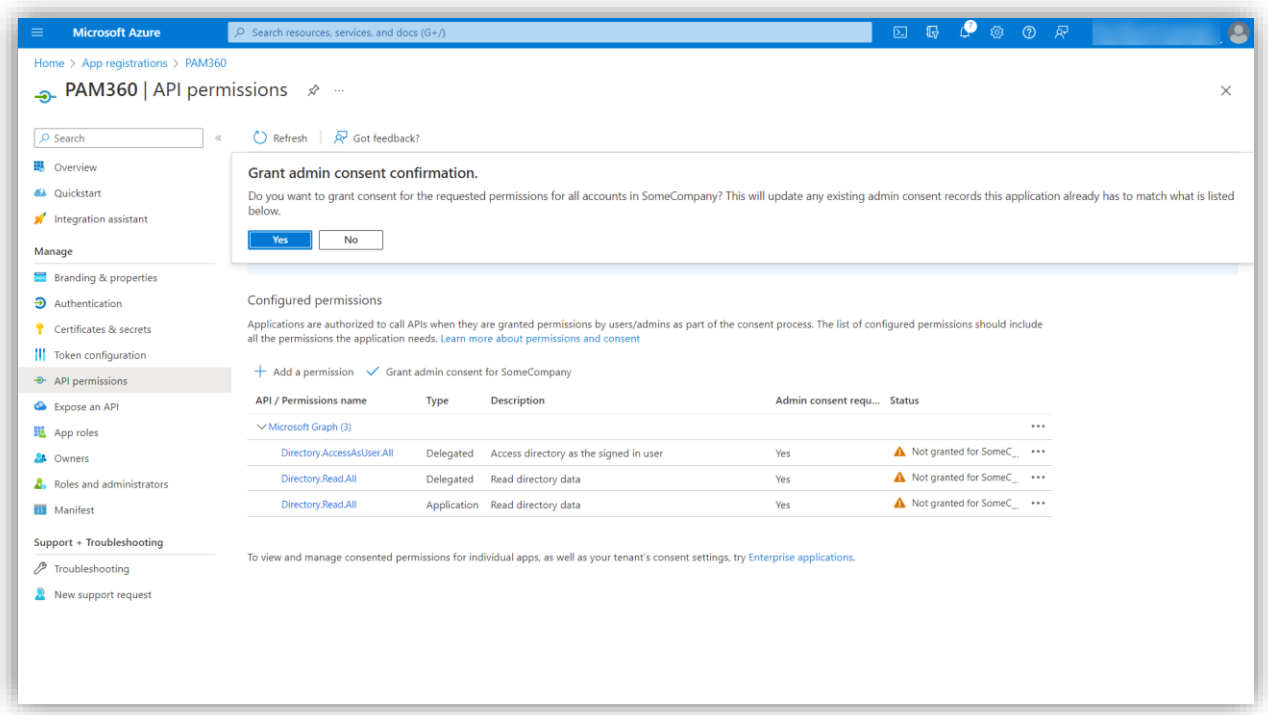
i. In the **Request API Permissions** page, choose **Microsoft Graph.**

   a. Click **Delegated Permissions** and search for "**read**" in the **Select Permissions** search bar to populate relevant permissions. Select the option **Directory.Read.All** and click **Add Permissions.**

b. Click **Application Permissions** and search for "**read**" in the **Select Permissions** search bar to populate relevant permissions. Select the options **Directory.Read.All** and click **Add Permissions.**

c. Click **Delegated Permissions** and search for "**access**" in the **Select Permissions** search bar to populate relevant permissions. Select the options **Directory.AccessAsUser.All** and click **Add Permissions**.

9. Now, click the **Grant admin consent** button under **Grant Consent.**
10. In the pop up that opens, click **Yes** to grant consent for the requested permissions.



Once you have registered PAM360 with appropriate permissions, go to PAM360's web interface and start importing users using the steps detailed below.

2. Steps to Import Users from Azure AD

1. Log in to PAM360 and navigate to **Admin >> Authentication >> Azure AD**.

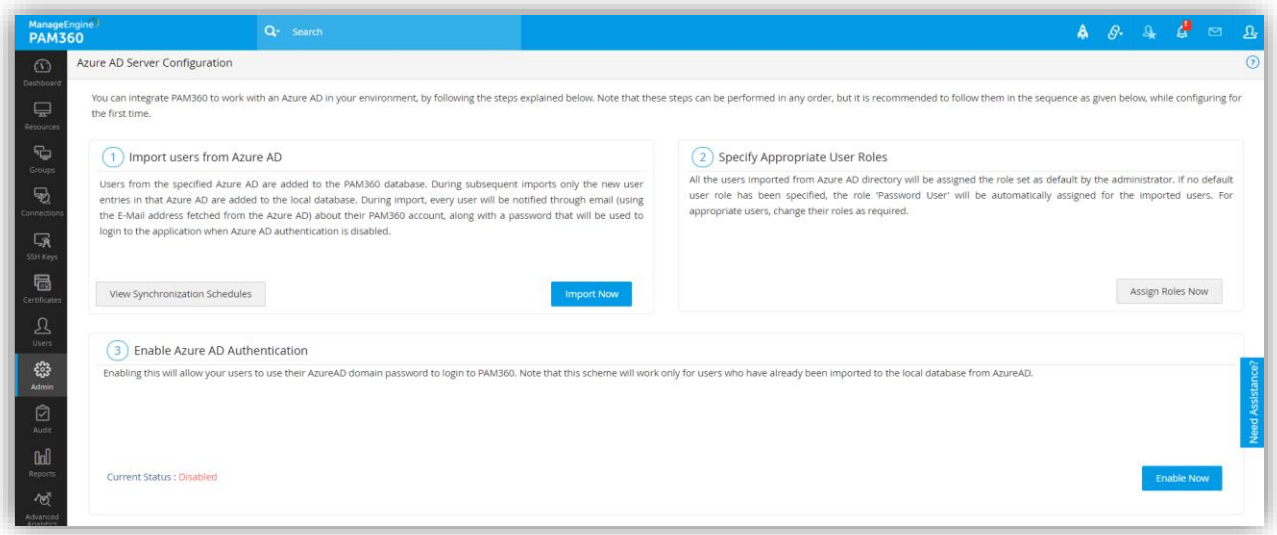
> **Note**: You can also import users by navigating to **Admin >> Users >> Add Users >> Import from Azure AD**. However, Azure AD Authentication can be enabled only from **Admin >> Authentication >> Azure AD**.

2. The **Azure AD Server Configuration** page will be displayed, from where you need to perform the below sequence of steps:

   i. Importing users from Azure AD

ii. Specifying appropriate user roles

iii. Enabling Azure AD authentication



2.1 Importing Users from Azure AD

1. Navigate to '**Users >> Add User >> Import From Azure AD**' or '**Admin >> Azure AD >> Import Now**'.
2. In the pop-up that opens, perform the following operations:

   a. Click the **New Domain** and add the Azure AD domain from which users and groups are to be imported.

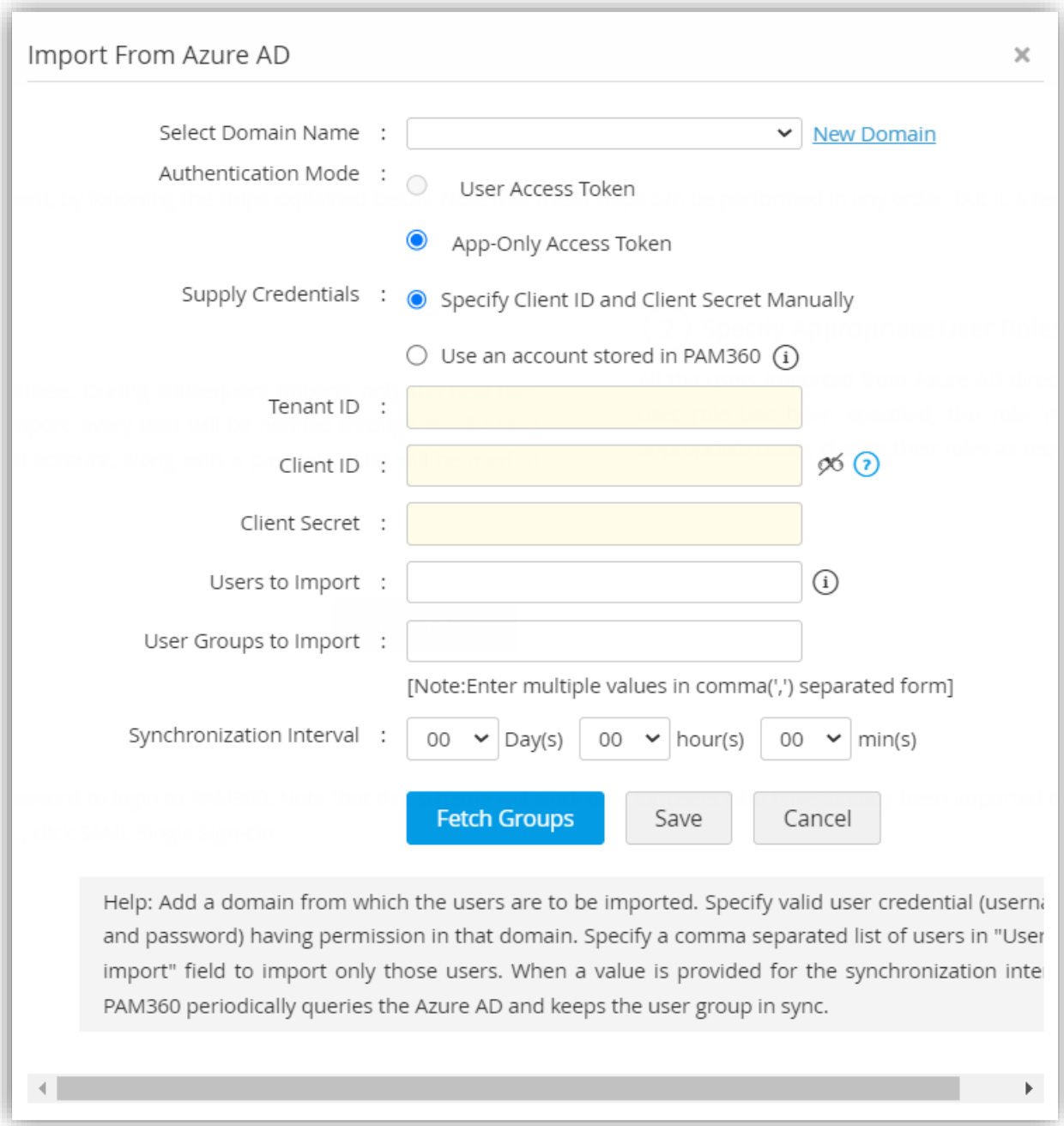
   b. Select the **Authentication mode** as **App-Only Access Token**. User Access Token will be no longer applicable from build 6000.

   c. Select the **Supply Credentials** as **Specify Client ID and Client Secret Manually**. If you have stored the **Azure Application** of **Microsoft Azure** as a resource in PAM360, then select **Use an account stored in PAM360**.

   d. If you have selected **Specify Client ID** and **Client Secret Manually** in the supply credentials:

i. Enter the **Tenant ID** and **Client Secret**.

ii. Enter the **CLIENT ID** generated in the Azure AD server while registering PAM360 as a native client application in your Azure portal.



a. To import only particular users and user groups from the Azure AD, enter the required user name(s) in the comma-separated form in the field **Users to Import** and the required group names in **User Groups to Import**.

b. Add a synchronization schedule to keep the user database constantly in sync with your Azure AD. In the **Synchronization Interval** field, you can enter the time

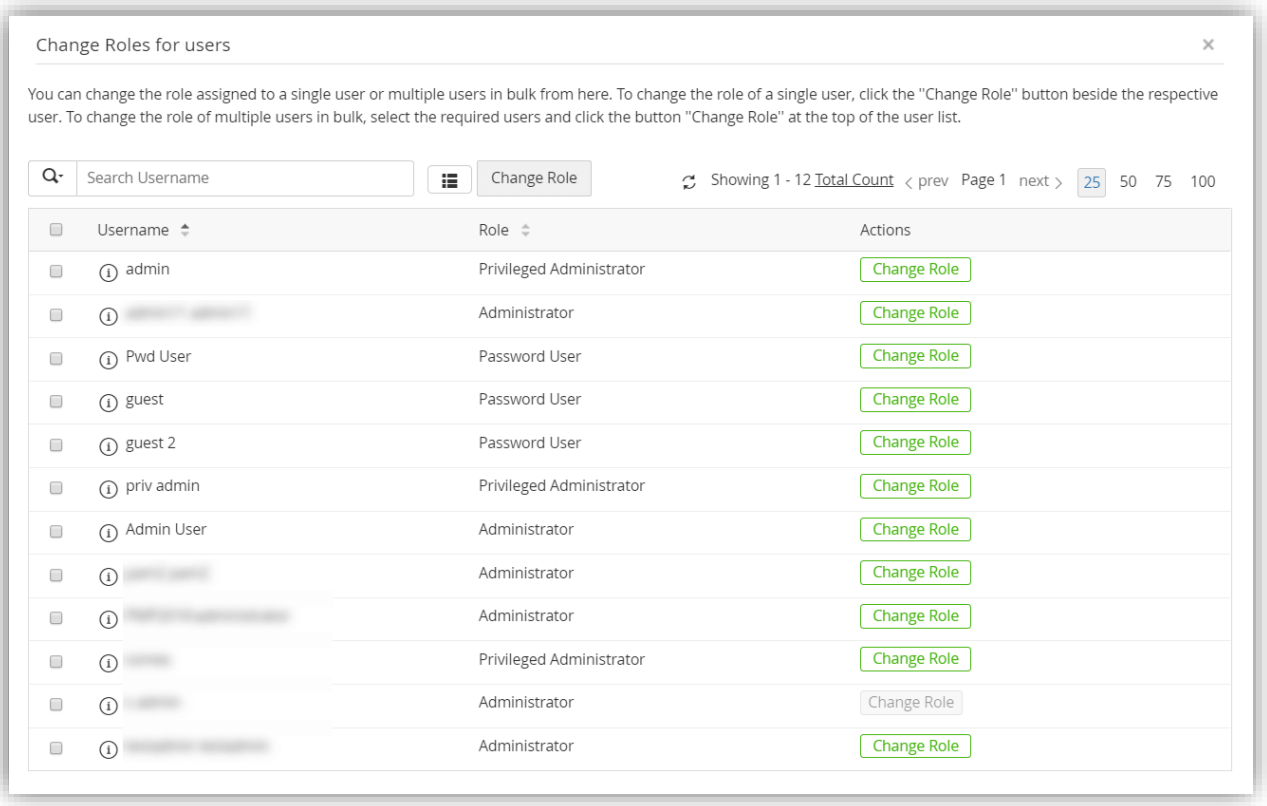
interval at which PAM360 has to query Azure AD and keep the user database in sync with Azure AD.

c. After entering the required details, click **Fetch Groups**. If you have specified users/user groups to import, then click Import. PAM360 will list all the user groups available in your Azure AD domain. Select required groups using the check boxes beside them and import users.

d. Once the import is complete, Import Summary will be displayed with the number of users imported successfully and the ones that failed. Once you click **Close**, you will be automatically taken to **section 2.2**: changing appropriate user roles.

2.2 Specifying Appropriate User Roles

After import, all the users imported from Azure AD will be assigned the **Password User** role as shown in the **Change Roles for users** dialog box.



1. Click **Change Role** button against the users for whom you wish to change the role and choose an appropriate role from the drop-down.
2. To change roles for users in bulk, select the users using the check boxes and click **Change Role** at the top and choose an appropriate role from the drop-down. The

changes will be saved as and when the roles are assigned.

Notes:

- You can change the assigned roles anytime in the future by clicking Assign Roles Now in the Azure AD Server Configuration page.
- Assign Administrator role to at least one user from the list of users imported from Azure AD as administrator privileges are required to carry out user management and other system operations in PAM360.

2.3 Enabling Azure AD Authentication

The third step is to enable Azure AD authentication—enabling this will allow your users to login to PAM360 using their Azure AD domain password. Note that this feature will work only for users who have already been imported to the local database from Azure AD. Before enabling Azure AD authentication, ensure that AD authentication is disabled.

1. Navigate to **Admin >> Authentication >> Azure AD** and click **Enable Now** under **Enable Azure AD Authentication** as shown in this image.
2. Once Azure AD authentication is enabled, you can disable local authentication under **Admin >> Settings >> General Settings >> User Management.**

2.4 Troubleshooting Tips

In PAM360, Azure AD authentication will not work under two circumstances, which are explained below with possible solutions:

1. Users in the Azure AD portal have **Conditional Access** enabled, which prevents sending of auth token to PAM360, leading to authentication failure.
   Solution: Bypass this by disabling **Conditional Access** at both app-level and user level in the Azure AD portal before enabling Azure AD authentication in PAM360.
2. The Azure AD portal has Multi-Factor Authentication (MFA) enabled.
   Solution: Bypass this by disabling MFA in the Azure AD portal.

In the place of **Conditional Access** and MFA, you can enable SAML Single sign-on in the Azure AD portal. Click here to learn how to set up SAML authentication.

Importing Users from LDAP

LDAP (Lightweight Directory Access Protocol) is a widely used standard protocol for accessing and managing directory services that provide a standardized approach to storing and retrieving information about users, devices, and other network resources. In PAM360, you can now integrate your organization's LDAP servers and import users of your organization. Post importation, you can manage their privilege to the respective resources available in the organization.

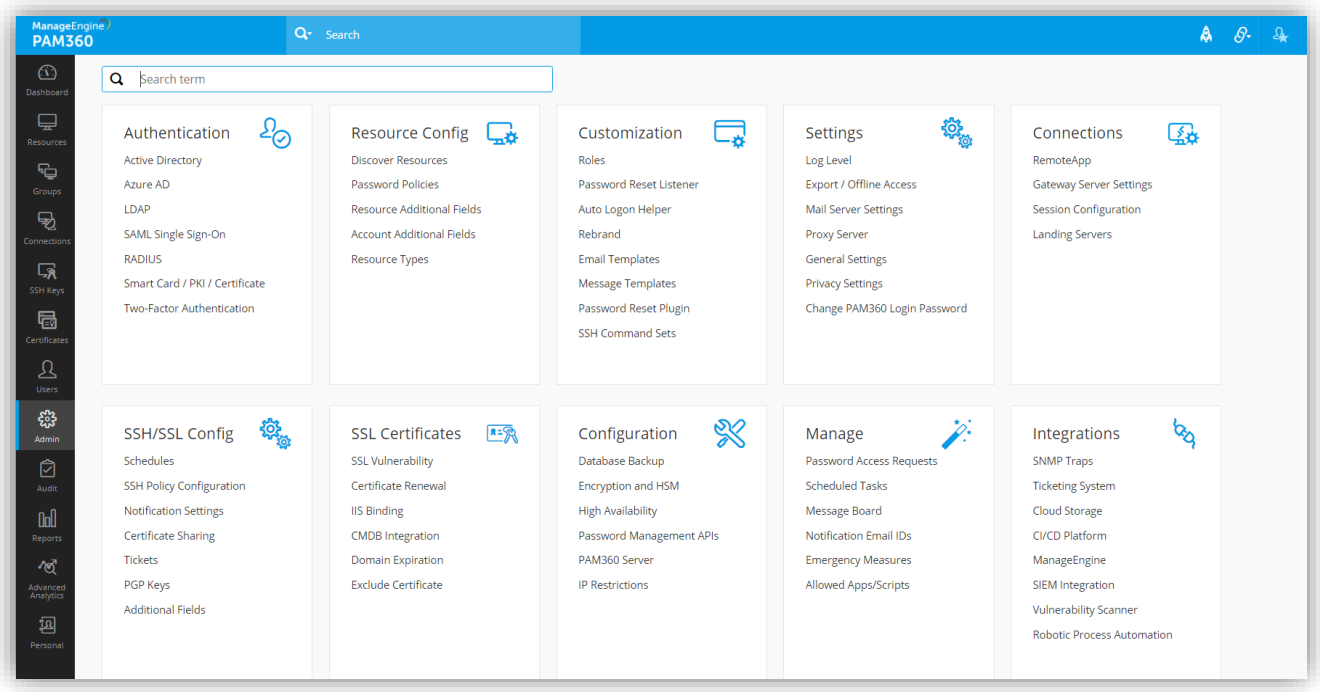
Similar to importing users from file, AD and Microsoft Entra ID, you can also import users from LDAP directory. Read further to know how.

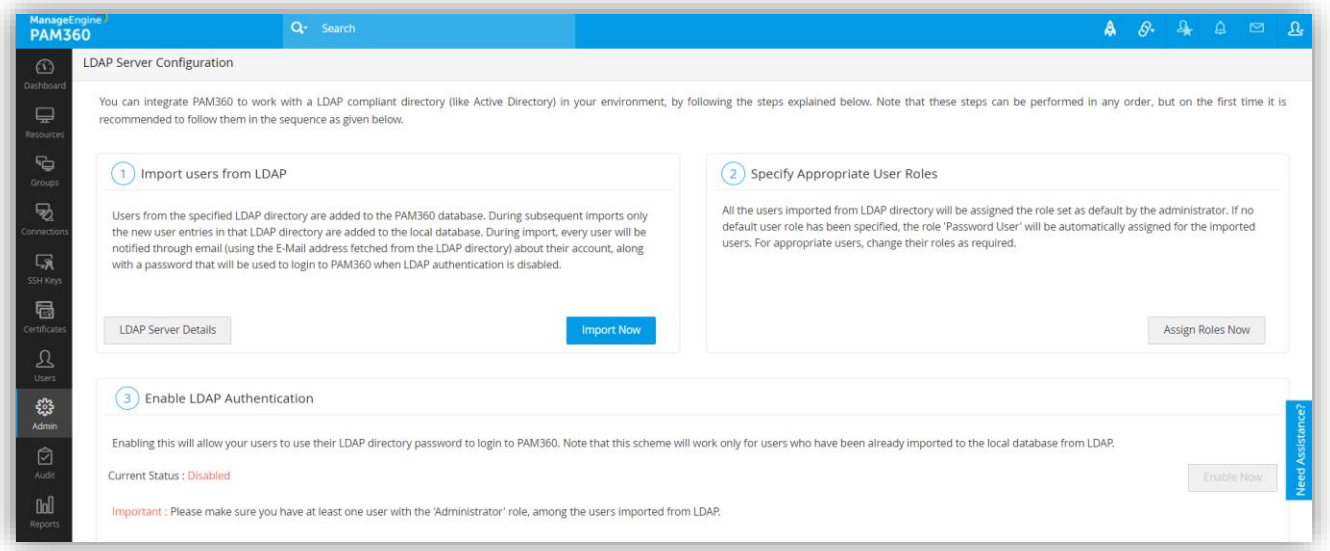
Steps Required

There are three steps involved in importing users from an LDAP directory.

1. **Importing Users from LDAP**
2. **Specifying Appropriate User Roles**
3. **Enabling LDAP Authentication**

Navigate to **Admin >> Authentication >> LDAP**. The **LDAP Server Configuration** page is displayed.

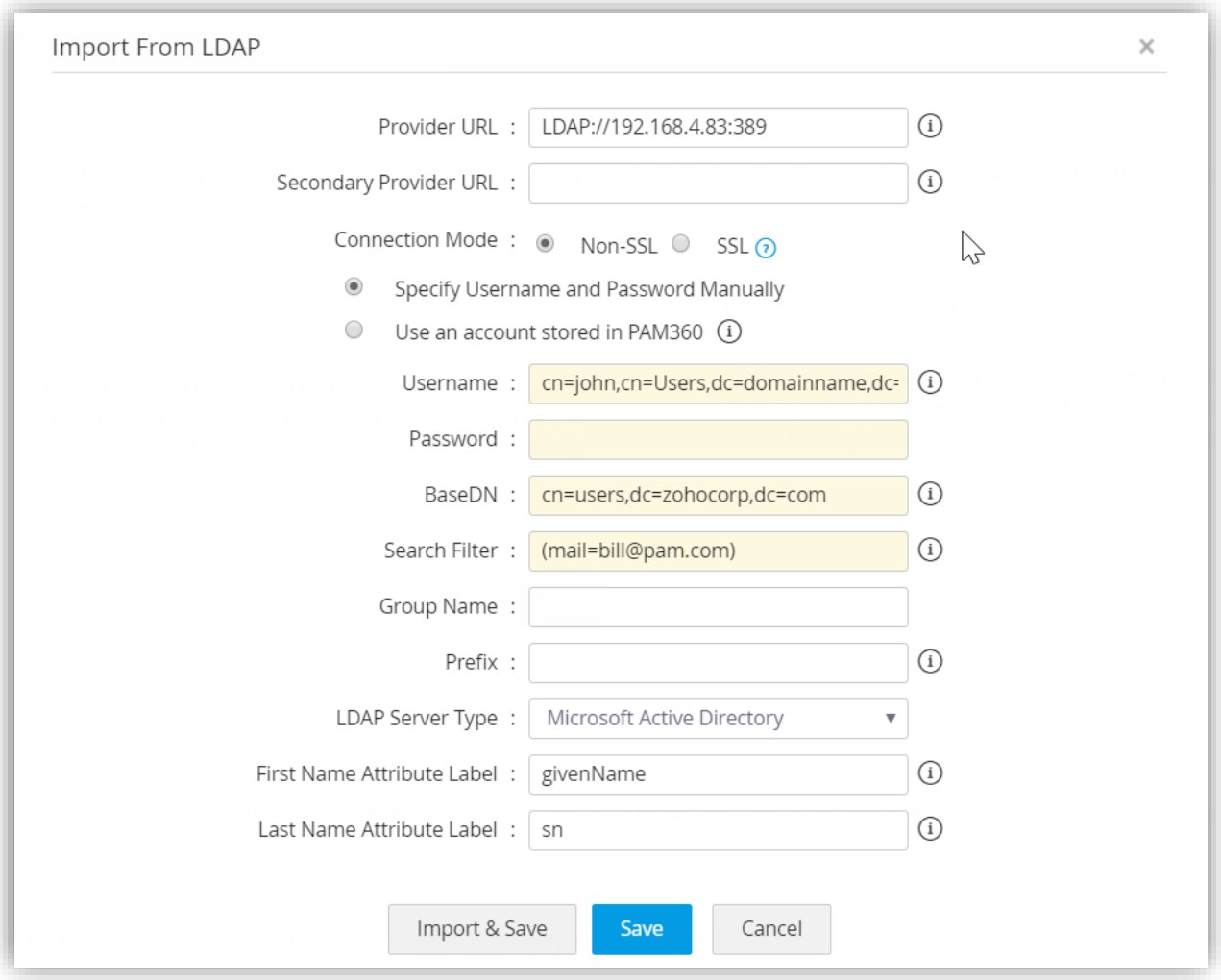




1. Importing Users from LDAP

The first step is to provide the required credential details and import users from LDAP. To do this:

1. Click the **Import Now** button from the **LDAP Server Configuration page.** Alternatively, you can also access this from **Users >> Import from LDAP** button.
2. In the pop-up form that pops-up, fill-in the details as required:



i. You can configure the connection between LDAP Server and PAM360 to be over an encrypted channel (SSL) or Non-SSL. If you choose, SSL mode, do the following. **Otherwise, proceed to Step 2**.

- To enable the SSL mode, the LDAP server should be serving over SSL in port 636 and you will have to import the LDAP server's root certificate, LDAP server's certificate and all other certificates that are present in the respective root certificate chain into the PAM360's server machine's certificate store.
- To import certificates, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

  For Windows:

  importCert.bat <Absolute Path of certificate>

  For Linux:

importCert.sh <Absolute Path of certificate>

Restart PAM360 server. Then, continue with the following steps.

ii. Enter the url of the LDAP provider in the format attribute://ldap server host:port **(Example ldap://192.168.4.83 <:389/)**

iii. Enter the credentials of any one of the user already present in LDAP for authentication. It should be in the format of how the user would have submitted their username when authenticating to your application. For example, a typical entry would look something like: cn=Eric,cn=Users,o=adventnet,c=com.

iv. Enter the password of the user.

v. This is the 'base' or 'root' from where directory lookups should take place. Enter the LDAP base (top level of the LDAP directory tree). Enter it exactly in the format used in your LDAP. No spaces are allowed between the commas or the '=' equal symbol and entries that are case sensitive.

vi. If you want to add only specific users from your LDAP directory, just perform a search using the appropriate search filter. For example, for adding only those users who belong to the category "Managers", a typical search filter would be like: ou=Managers,ou=Groups,o=adventnet,c=com.

vii. Enter the group name. While importing users from LDAP, PAM360 will automatically create a user group with all the imported users. If you enable synchronization, the user group will get synchronized based on the search filter created by you.

viii. Select your LDAP server type

- Microsoft Active Directory (or)
- Novell eDirectory (or)
- OpenLDAP (or)
- Others

xiii. If your LDAP server belongs to the type Microsoft Active Directory/Novell eDirectory/OpenLDAP, you can select that type and click **Save.**

If your LDAP server belongs to types other than Microsoft Active Directory/Novell eDirectory/OpenLDAP, specify the following additional details to authenticate the users:

a. Enter the user login attribute in your LDAP structure in the text field for **"Login Attribute"**. For instance, for LDAP making use of AD, the entry would be **"sAMAccountName"** and

for OpenLDAP, the entry would be **"uid"**. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

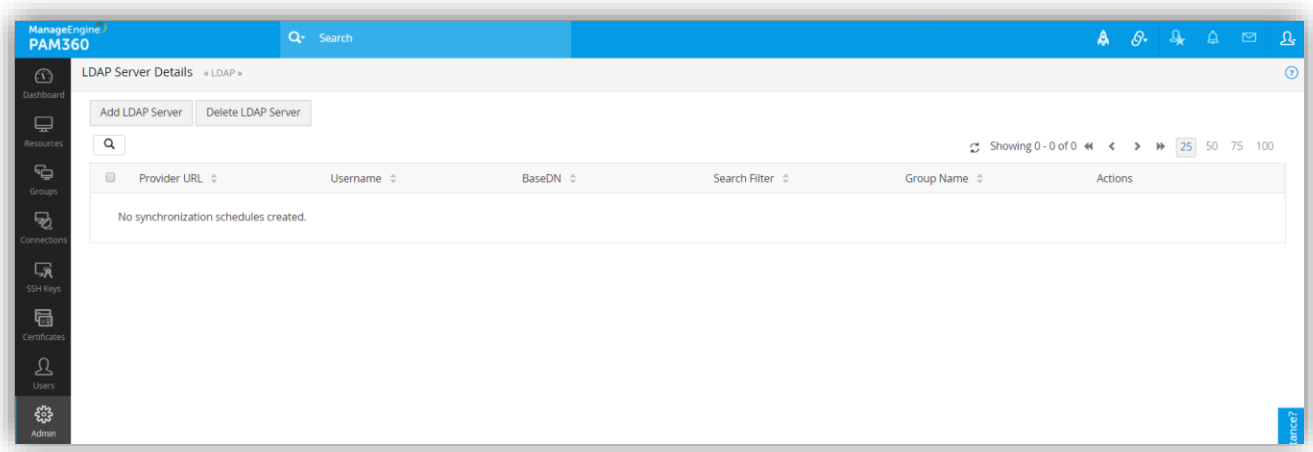
b. Enter the e-mail attribute for the users in your LDAP structure in the text field for **"Mail Attribute"**. For instance, for LDAP making use of AD, the entry would be **"mail"**. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

c. Enter the distinguished name attribute - that is the LDAP attribute that uniquely defines this object. For instance, for LDAP making use of AD, the entry would be **"distinguishedName"** and for OpenLDAP, the entry would be **"dn"**. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

d. Click **"Import"**. Soon after hitting this "Save" button, PAM360 will start adding all users from LDAP. During subsequent imports only the new user entries in LDAP are added to the local database. During import, every user will be notified through email about their account, along with a password that will be used to login to PAM360 when LDAP authentication is disabled.

1.1 Configure Synchronization and Manage LDAP Server Details

Whenever new users get added to the LDAP, there is provision to automatically add them to PAM360 and keep the user database in sync. This can be done from the 'LDAP Server Details' page. Click the button 'LDAP Server Details' under Step 1 in the UI. This UI has been designed to serve as a one-stop place for managing all configurations pertaining to the LDAP servers integrated with PAM360.



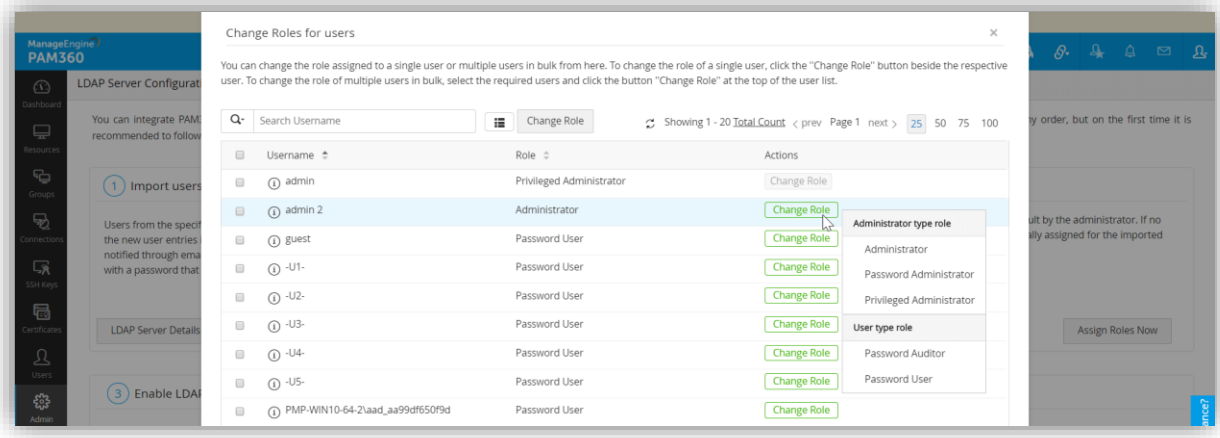
1. In the **LDAP Server Details** UI, you can view the list of LDAP servers already integrated, integrate new LDAP servers, delete existing ones, edit entries and manage the entries pertaining to the LDAP servers.
2. In addition, from the **Actions** section of this page,

- You can edit the existing LDAP server details.
- You can configure user database synchronization. Enter the time interval at which PAM360 has to query the LDAP server to keep the user database in sync. The time interval could be as low as a minute or it can be in the range of hours/days.
- You can also import users from LDAP.

2. Specifying Appropriate User Roles

All the users imported from LDAP will be assigned the **'Password User'** role by default. To assign specific roles to specific users,

1. Go to Step 2 in the UI **(Admin >> Authentication >> LDAP)** and click **Assign Roles Now.**
2. In the pop-up form that opens, all the Users imported from AD are listed.
   i. Click **Change role** button against desired users for whom you wish to change the role and select the appropriate role from the drop down.
   ii. Click **Save** and the required roles are set for the users.



3. Enabling LDAP Authentication

The final step is to enable LDAP authentication. This will allow your users to use their LDAP directory password to log in to PAM360. Note that this scheme will work only for users who have been already imported to the local database from AD.

Note: Make sure you have at least one user with the 'Administrator' role, among the users imported from LDAP.

Managing PAM360 User Accounts

This document provides a comprehensive guidance on managing the user accounts within your PAM360 environment.

Roles Required to Perform this Operation

- Privileged Administrator
- Administrator
- Any custom role with 'Edit', 'Change User Roles', and 'Delete' enabled operations accordingly

1. Editing the PAM360 User Account

User with the provided privilege can modify various details for existing users such as their role, email address, access level, password policy, department, and Two Factor Authentication (2FA), etc. To do so,

1. Navigate to the **Users** tab.
2. Click on the User Actions icon next to the desired user and select **Edit User** from the dropdown menu.
3. In the window that appears, edit the desired fields as required and click Save to imply the changes.

To know more about each user field, refer to the add user help documentation for details. Add Users Manually - Builds Preceding 6700 | Builds Following 6700

> **Note:** If you are currently logged in as an administrator, you will not be able to alter your own access level or scope. In such cases, you will need to request another administrator to make the necessary changes.

2. REST API and SDK Access Modifications

(Applicable only for builds beyond 6700)

You can also modify the REST API and SDK user access from the **Users** tab, instead editing into a user account.

a. From the **Users** tab, select the **REST and Application Access** under the **User Actions** beside the relevant user. In the dialogue-box that opens, enable/disable the relevant access, regenerate the Authentication Token, update the Access Validity, etc, as required.
b. To enable or disable the REST API access in bulk, navigate to **More Actions >> Configure >> REST API Access**. Select the required usernames and click on **Disable** at the top of the user list. Similarly, you can also **Enable** REST API access from here.
c. To enable or disable the SDK access in bulk, navigate to **More Actions >> Configure >> SDK Access**. Select the required usernames and click on **Disable** at the top of the user list. Similarly, you can also Enable SDK access from here.
d. You can also invalidate an Authentication Token of a user by selecting **Invalidate Authentication Token** under the **User Actions** beside the relevant user.

3. Deleting the PAM360 User Account

Users with the provided operation can delete users from PAM360 who are no longer necessary for the organization. To remove a user from PAM360,

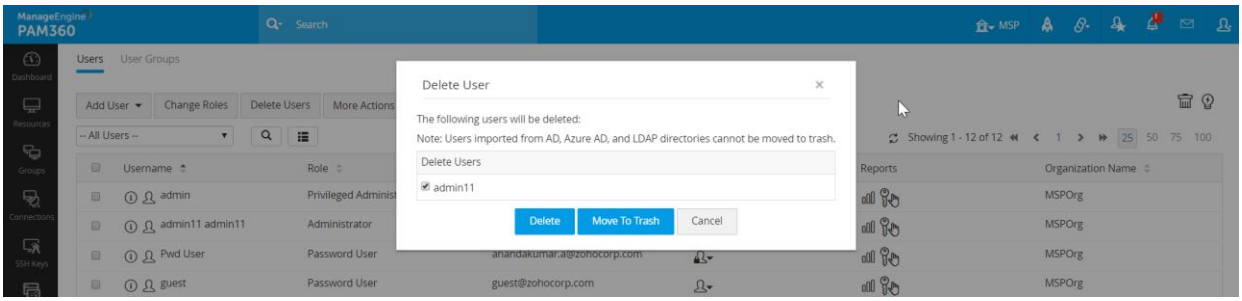
1. Navigate to the **Users** tab.
2. To delete an individual user, click the **User Actions** icon against the desired user and select **Delete** user from the drop-down list. To delete the users in bulk, select the users and click the **Delete Users** button from the top pane.
3. In the pop-up window that opens, you will have two options:
   a. **Delete**: Select this option to delete the user permanently from the PAM360.
   b. **Move To Trash**: Use this option to transfer users to Trash without permanent deletion. Users in the Trash can be restored until PAM360 encryption keys are rotated. After key rotation, users in Trash and associated credentials will be permanently removed from the PAM360 repository.

> **Note:** Users imported from AD, Microsoft Entra ID, and LDAP directories cannot be moved to Trash.

Notes: The below notes apply for both permanent deletion and deletion from trash.

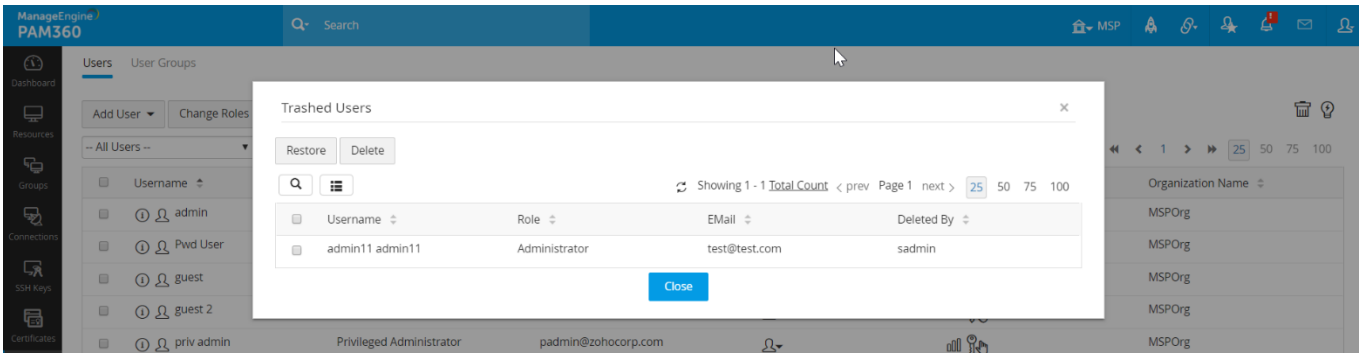
i. PAM360 will allow users to be deleted only if the user/users do not own any resource. If the user owns any resource, then you need to transfer the ownership of all the resources to some other user with an administrator-type role.

ii. The currently logged in user will not be allowed to delete themselves.



3.a Restoring Users from Trash

To restore a user account that has been moved to Trash, go to the Users tab and click on the Trash icon located at the top right corner. A list of users in the Trash will appear in a pop-up box, allowing you to select and restore the desired users.



Since PAM360 requires that the resources owned by a user be transferred to another user before deletion, there will be no loss of enterprise data. However, all personal data stored by the user will be permanently deleted. The audit trails will comprehensively record all such changes and deletions. The audit trails documenting the user's activities will remain intact in the database even after the user is deleted. Audit trails relevant to the deleted users will not be erased.

3.b Deleting an Administrator User Account

Before proceeding to delete an administrator user account, check for any resources owned by the user. If exist, the resources should be transferred to another user with an administrator-type role by the resource owner by following the below steps,

1. Navigate to the **Users** tab.
2. Select all the resources and click **Transfer Ownership** by navigating to **Resource Actions >> Manage**.
3. In the pop-up that opens, select the user with the administrator-type role for whom the resources to be transferred and click **Save**.

> **Note:** The logged in administrator cannot delete their own user account from PAM360.

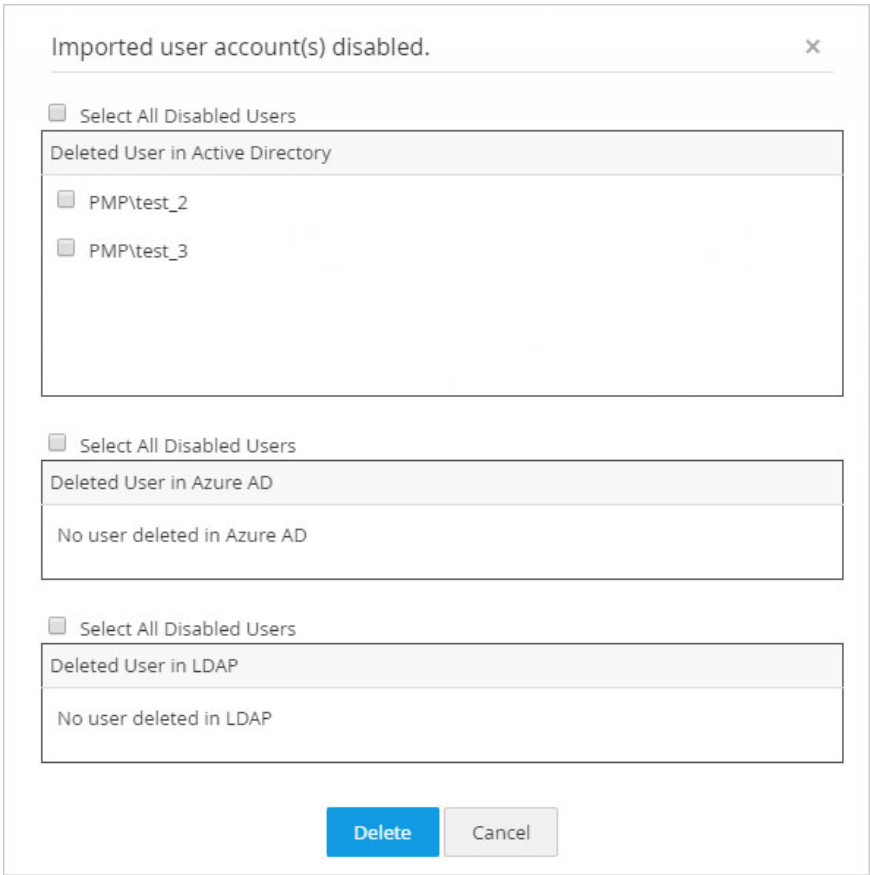
Upon successful ownership transfer, the administrator user account can be deleted from the PAM360 by another administrator.

3.c Handling User Accounts Deleted from AD/Microsoft Entra ID/LDAP Directories

Whenever a user account is deleted directly at the user directory from which it was imported to PAM360 i.e. from AD, Microsoft Entra ID or LDAP directory, PAM360 identifies those deleted user accounts at the time of next synchronization schedule. The identified user accounts are then subsequently disabled in PAM360 and held as locked accounts.

> **Note:** PAM360 will identify deleted user accounts only if you have set up synchronization with the respective user directory.

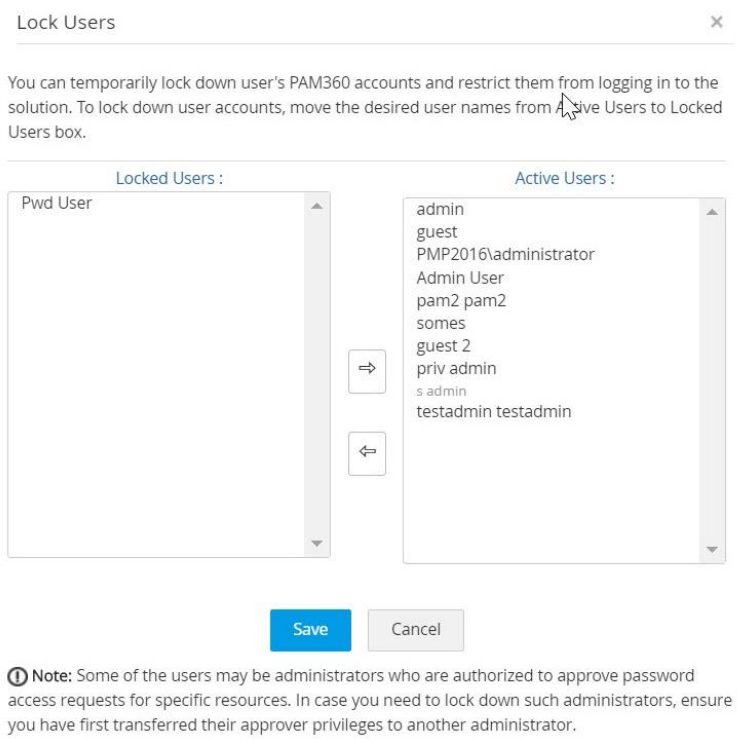
After disabling the user accounts, PAM360 informs the administrators or users with user management privileges via email as well as an alert notification within the product. Clicking the alert notification will open a dialog box as shown below:



The administrator can review the locked accounts and then choose to delete those user accounts permanently from PAM360 by clicking the Delete button. Further, the administrator can also review the locked accounts directly using the user filter provided in the Users page and can delete the disabled accounts individually or in bulk.

On the other hand, to activate the accounts,

1. Navigate to **Users >> More Actions >> Lock Users**.
2. In the new window that opens, you will find the disabled user accounts listed under the **Locked Users** column. Move the required account to the **Active Users** column and click **Save** as shown below:



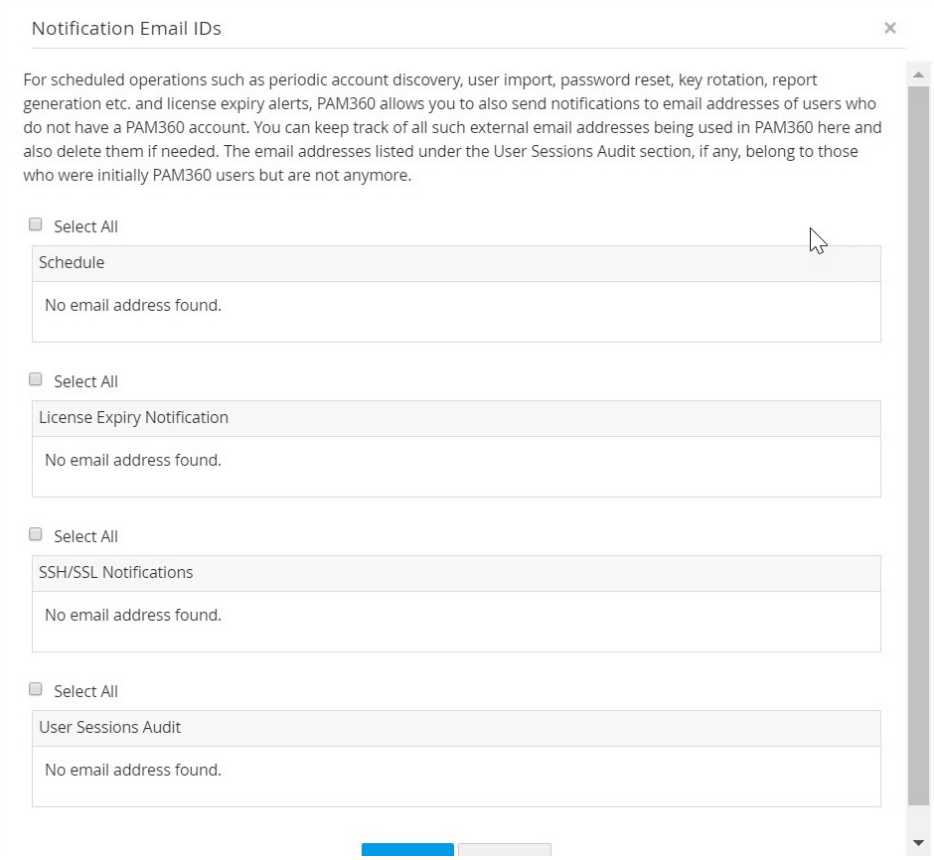
3. Alternatively, you can also activate individual user accounts by locating the required user, clicking on the **User Actions** icon beside the user, and selecting **Unlock User** from the drop-down menu.
4. In a dialogue-box that opens, click **Unlock** to restore the disabled user account.

4. Managing Notification Email Addresses in PAM360

PAM360 allows you to configure generic email addresses as recipients of notification emails for scheduled tasks' completion statuses and license expiry alerts. You can keep track of all such external email addresses being used in PAM360 and also delete them if needed. Additionally, the email addresses of users captured in the User Sessions audit can also be managed using this provision, in the event of those users being removed from PAM360.

To view the list of notification email addresses,

1. Navigate to **Admin >> Manage >> Notification Email IDs**.
2. In the dialog box that opens, you will find the email addresses listed under four different sections - **Schedules**, **License Expiry Notifications**, **SSH/SSL Notifications**, and **User Sessions Audit**, if there are any.
3. Review the listed email addresses under each section, select the one that you want to delete, and click **Delete**.


Notification Email IDs
For scheduled operations such as periodic account discovery, user import, password reset, key rotation, report generation etc. and license expiry alerts, PAM360 allows you to also send notifications to email addresses of users who do not have a PAM360 account. You can keep track of all such external email addresses being used in PAM360 here and also delete them if needed. The email addresses listed under the User Sessions Audit section, if any, belong to those who were initially PAM360 users but are not anymore.
Select All
Schedule
No email address found.
Select All
License Expiry Notification
No email address found.
Select All
SSH/SSL Notifications
No email address found.
Select All
User Sessions Audit
No email address found.

User Groups

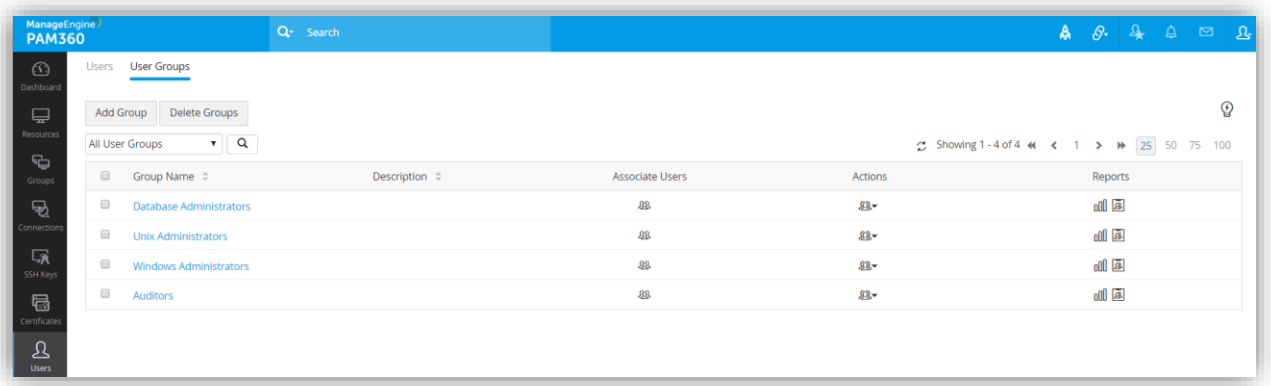
Users can be grouped in PAM360 for easier management. User grouping helps to carry out operations in bulk for all the resources of the group. The resources added to PAM360 can be quickly assigned to a user group instead of choosing each user individually.

1. Adding User Groups
   1.1 Importing User Groups from Active Directory (AD)
2. User Group Privileges
   2.1 Exporting Passwords for Offline Access
3. Managing User Groups
   3.1 Editing a User Group
   3.2 Adding Users to an Existing User Group
   3.3 Deleting a User Group

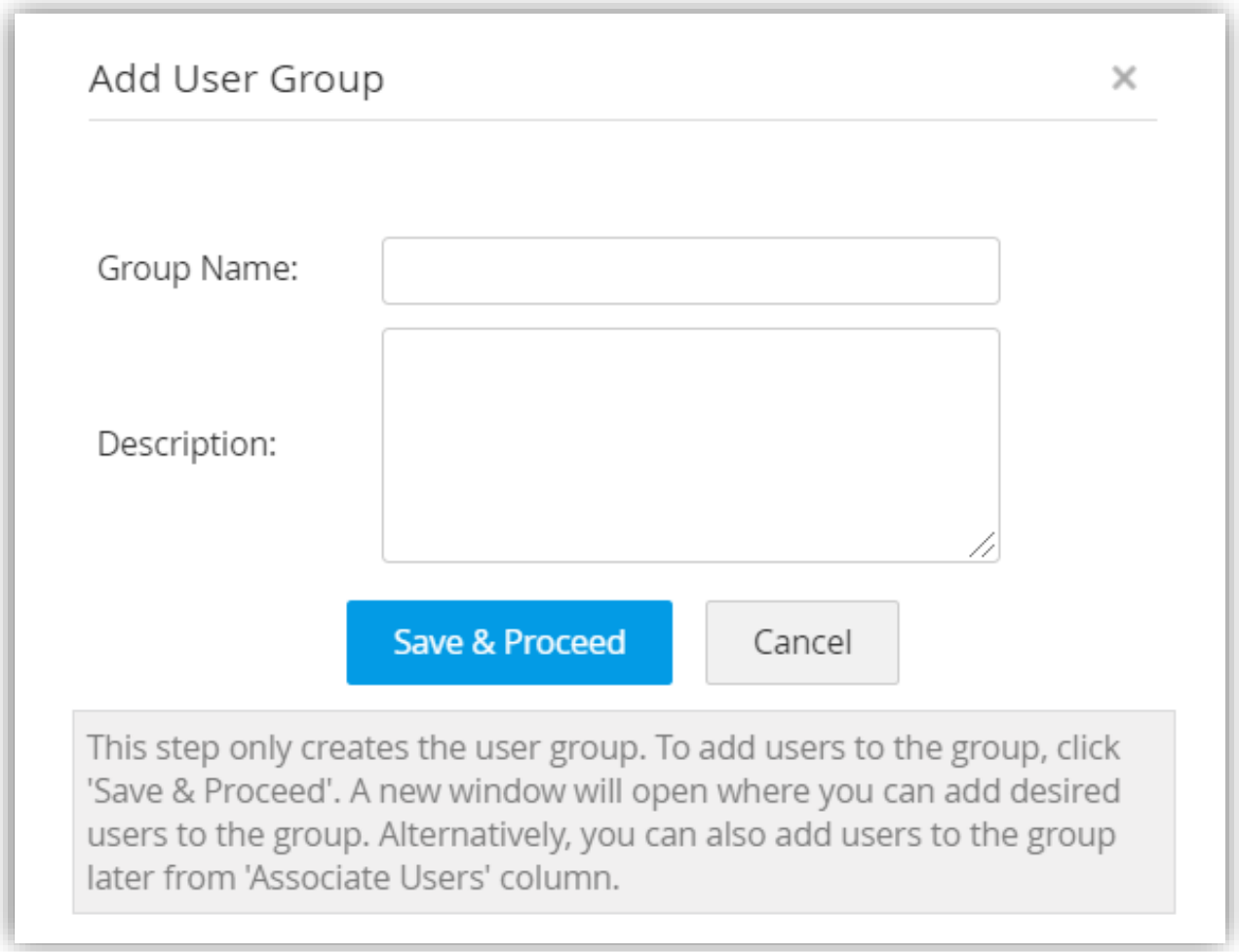
1. Adding User Groups

To create a new user group and add users to it, follow the below steps:

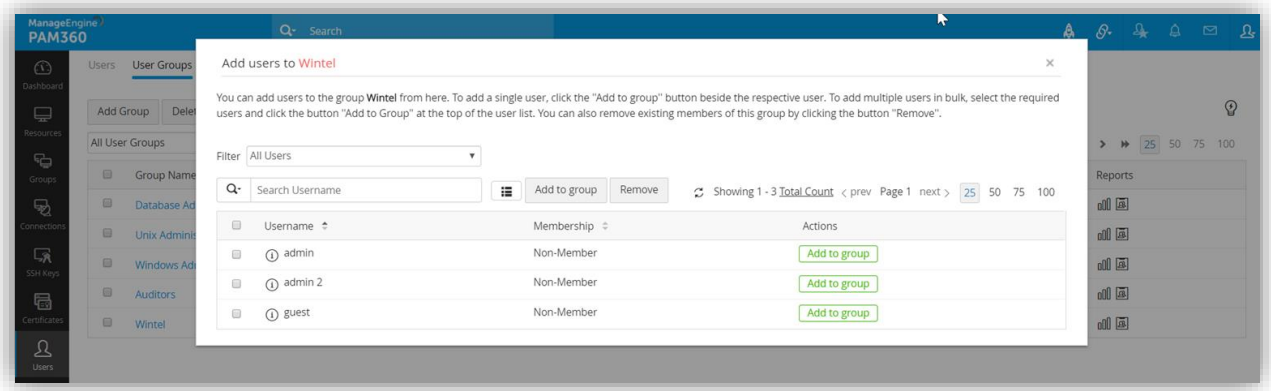
1. Navigate to **Users** >> **User groups** tab.
2. Click **Add Group**.



3. In the pop-up form that appears, enter a name and description for the user group.
4. Click **Save & Proceed**.



5. Once the user group is added, **Add Users** window will open up. Here, click **Add to Group** beside the required users. The changes will take effect as and when you add users.



1.1 Importing User Groups from Active Directory (AD)

1. You can import specific user groups and organizational units (OUs) from AD and retain the same user group structure in PAM360. Refer to the help section Importing Users from Active Directory to know more about importing users from AD.
2. You can choose to synchronize the user group structure in PAM360 with that of AD's at

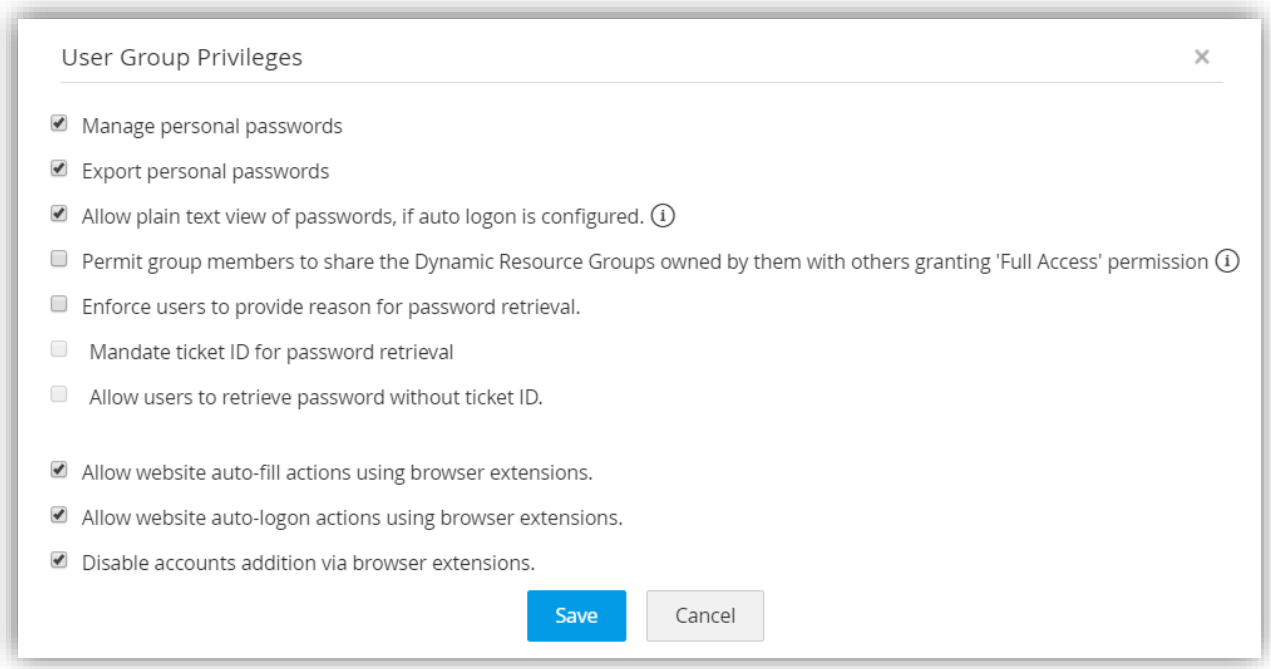
periodic intervals. Refer to the help section Active Directory Synchronization Schedules to know more about AD synchronization schedules.

2. User Group Privileges

Configure user group privileges for groups by following the below steps:

1. Navigate to **Users >> User Groups.**
2. Click the **Actions** icon beside the required user group and click **User Group Privileges**.

> **Note:** The setting changes made in the **User Group Privileges** window is applicable only for the users who are part of the selected user group.



3. The User Group Privileges in PAM360 are as explained below:
    a. **Manage personal passwords:** Individual users can manage their personal passwords such as credit card PIN numbers, bank accounts credentials etc in the **Personal** tab. Unselect this option if you do not wish to allow personal password management for a selected group of PAM360 users. Once disabled, the **Personal** tab will no longer appear in the PAM360 interface for all the members of selected group.
    b. **Export personal passwords:** Enable this option to allow users of the group to export the personal passwords that they store in the **Personal** tab. Unselect this option if you do not wish to allow password export for a particular user group.
    c. **Allow plain text view of passwords, if auto logon is configured:** Enable this option to allow the user group members to view the passwords of shared resources in

plain text when auto logon is configured. If this option is disabled, user group members cannot retrieve the password, however they can still launch remote sessions through auto logon. This restriction applies only to Password Users, Password Auditors and custom user type roles with the same privileges as Password Users and Auditors.

d. **Enforce users to provide reason for password retrieval:** Enable this option to prompt users to provide a reason while retrieving a password. This restriction applies only to Password Users, Password Auditors and custom user type roles with the same privileges as Password Users and Auditors.
e. **Allow users to retrieve password without ticket ID:** Enable this option to allow users to retrieve a password by clicking the 'password' field without the need to raise a ticket request for the same. This restriction applies only to Password Users, Password Auditors and custom user type roles with the same privileges as Password Users and Auditors. This option is applicable only if ticketing system integration is done in your environment.

To disable options **c, d** and **e** for a selection of users, follow the below steps:

i. Create a new user group.

ii. Add the selection of users to it.

iii. Enable or disable the settings for that group alone.

Notes:

1. For the options **c, d,** and **e** to be enforced for a user group, the settings must be enabled both locally i.e., at a user group level (as explained above) and globally i.e., in the general settings.

    i. **Case 1:** If options are enabled globally under General Settings, then the settings will be applied to all user groups by default. However, you can disable the settings for a particular group via the **User Group Privileges** window.

    ii. **Case 2:** If the options are disabled globally under General Settings, then the settings will not be applied to the user groups even if they are enabled locally under **User Group Privileges** for a particular user group.

2. These conditions apply only to Password Users, Password Auditors and custom user type roles with the same privileges as Password Users and Auditors.

4. **Mandate ticket ID for password retrieval:** Enable this option to prompt users to provide a valid ticket ID to retrieve a password. This option is applicable only if ticketing system integration is done in your environment.
5. **Permit group members to share the Dynamic Resource Groups owned by them with others granting Full Access permission:** By default, permission to grant **Full Access** for dynamic resource groups will be disabled in the User Group Settings window.

   Why is the setting disabled by default?

   i. The option is disabled by default for security reasons as there is a possibility that Administrators can use this setting to gain access to resources that are not owned by them.

   ii. If a user is granted access to a dynamic resource group with **Full Access** permission, then that user will get **Full Access** to all the resources currently under the group and also any resources that are added in the future based on matching the specified criteria (for example, conditions such as "Resource name contains").

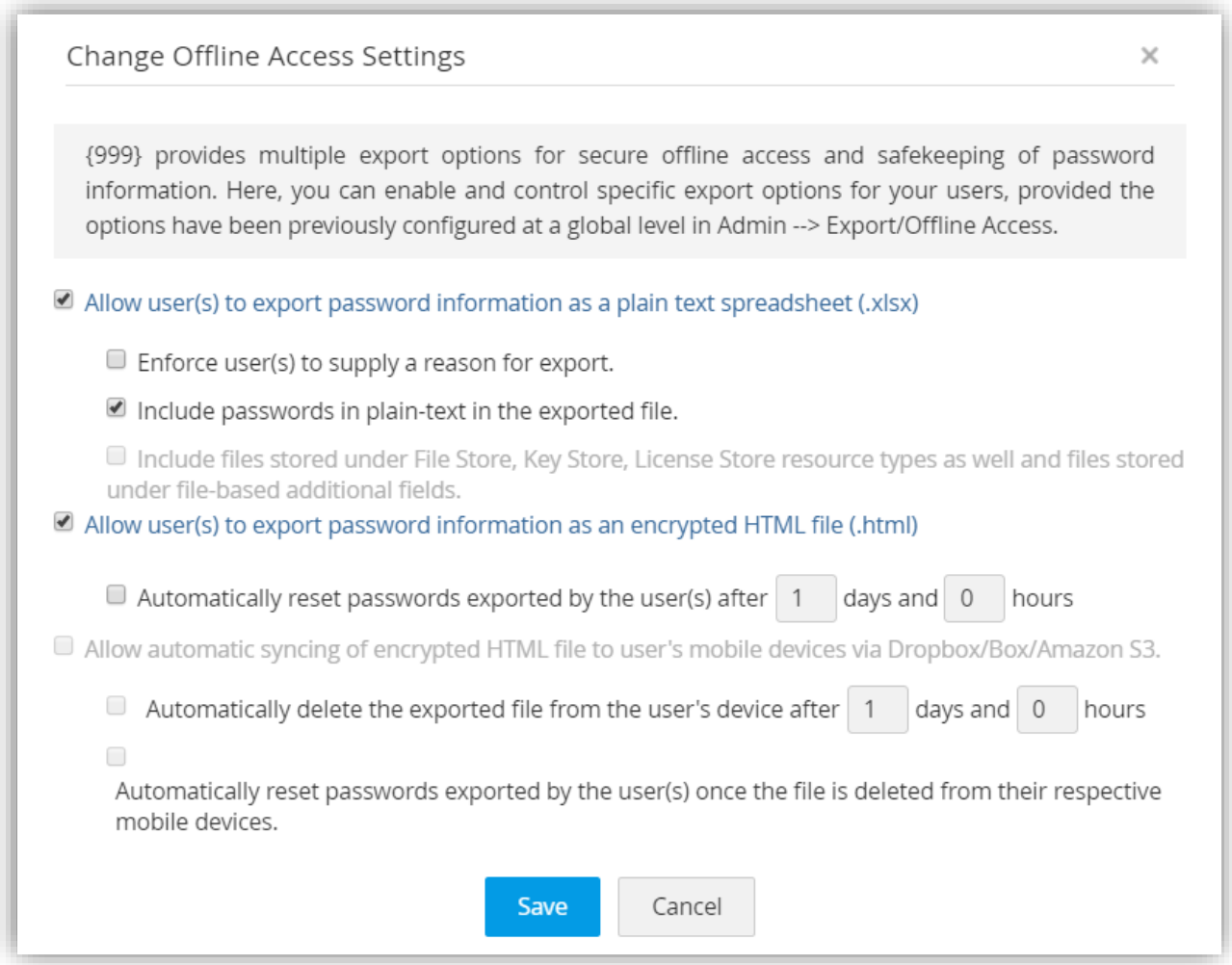
   iii. It is recommended that you create a user group containing only Administrators/Password Administrators/Privileged Administrators who require the authorization to grant **Full Access** permission for their dynamic resource groups with other users.

   iv. After creating the group, enable the option **Permit group members to share the Dynamic Resource Groups owned by them with others granting Full Access permission** under User Group Privileges.
6. **Allow password caching for offline access via mobile:** Enable this option to allow saving password cache in the PAM360 mobile application so that users can access the passwords offline.
7. **Enable login to mobile apps with fingerprint authentication:** Enable this option to allow users to login to their PAM360 mobile applications using their device's fingerprint authentication.
8. **Allow website auto-fill actions using browser extensions:** Enable this option to allow auto filling of login credentials for saved website accounts through the PAM360 browser extensions.
9. **Allow website auto-logon actions using browser extensions:** Enable this option to allow users to connect to a remote resource through the auto logon feature using the PAM360 browser extensions.
10. **Disable accounts addition via browser extensions:** Disable this option to prevent users from adding accounts to resources through the PAM360 browser extensions. The option to add accounts through browser extension is available only for the Chrome browser. Click here for more on PAM360 browser extensions.

2.1 Exporting Passwords for Offline Access

When a user exports PAM360 resources to a CSV file, by default, passwords of the accounts are included in plain text. You can disable password export for members of a specific user group by following the below steps:

1. Navigate to **Users >>Groups** tab.
2. Click the **Actions** icon beside the required group and click **Change Offline Access Settings** from the drop down.
3. In the pop-up form that appears, unselect the option **Include passwords in plain text in the exported file.**
4. Click **Save**.

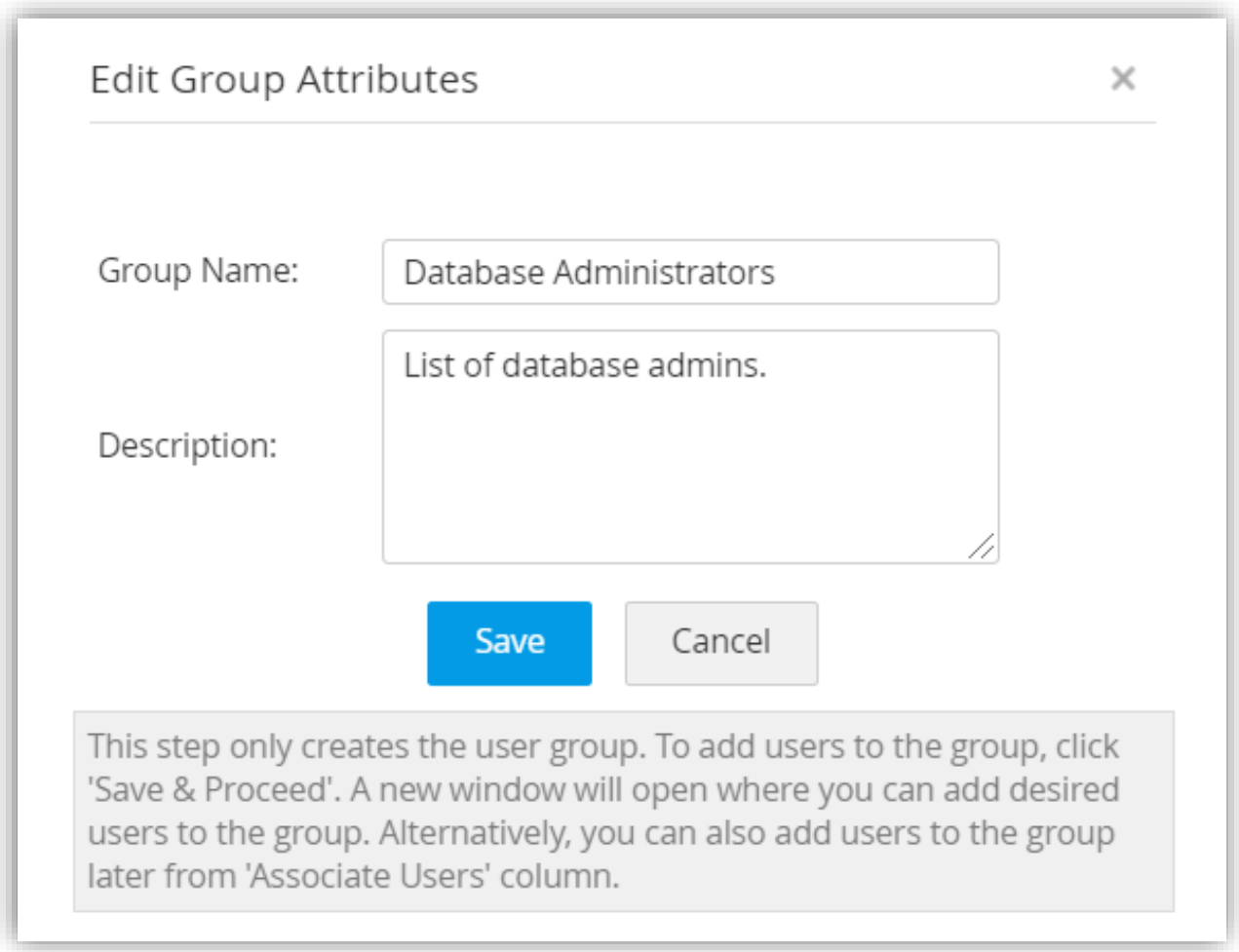


3. Managing User Groups

3.1 Editing a User Group

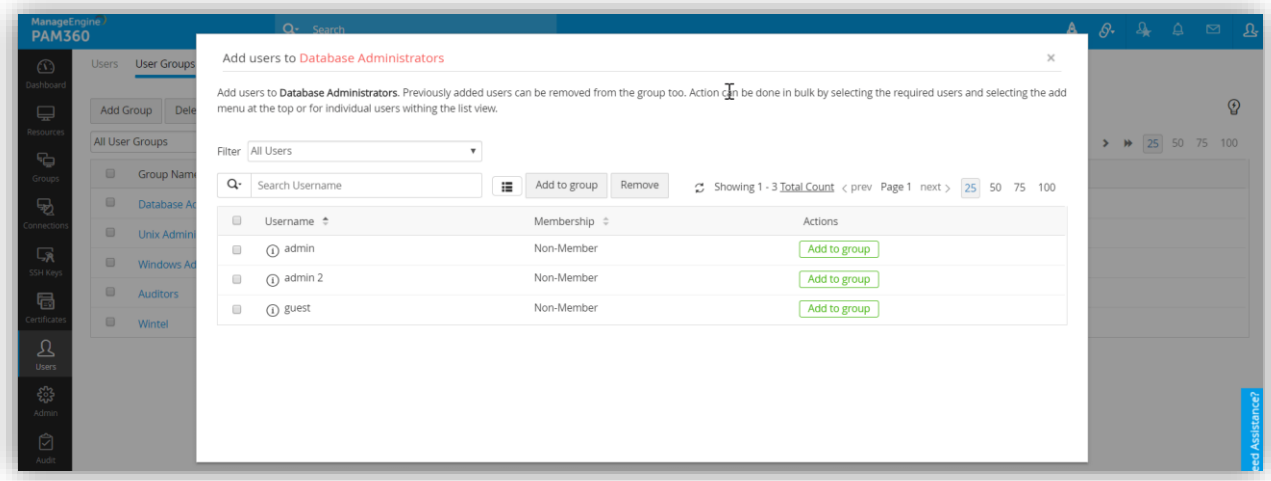
Follow the below steps to edit an existing user group to add more users or to remove existing users.

1. Navigate to **User Groups** tab.
2. Click the **Actions** icon beside the required group and click **Edit Group Attributes**.
3. In the pop-up form that opens, you can change the group name and description.



3.2 Adding Users to an Existing User Group

1. To add new users to the group or remove previously added users from the group, click **Associate Users** icon beside the required group.
2. Click **Add to Group** to add a non-member to the group.
3. Click **Remove** to remove previously added users from the group.
4. The changes will take effect as and when you make them.



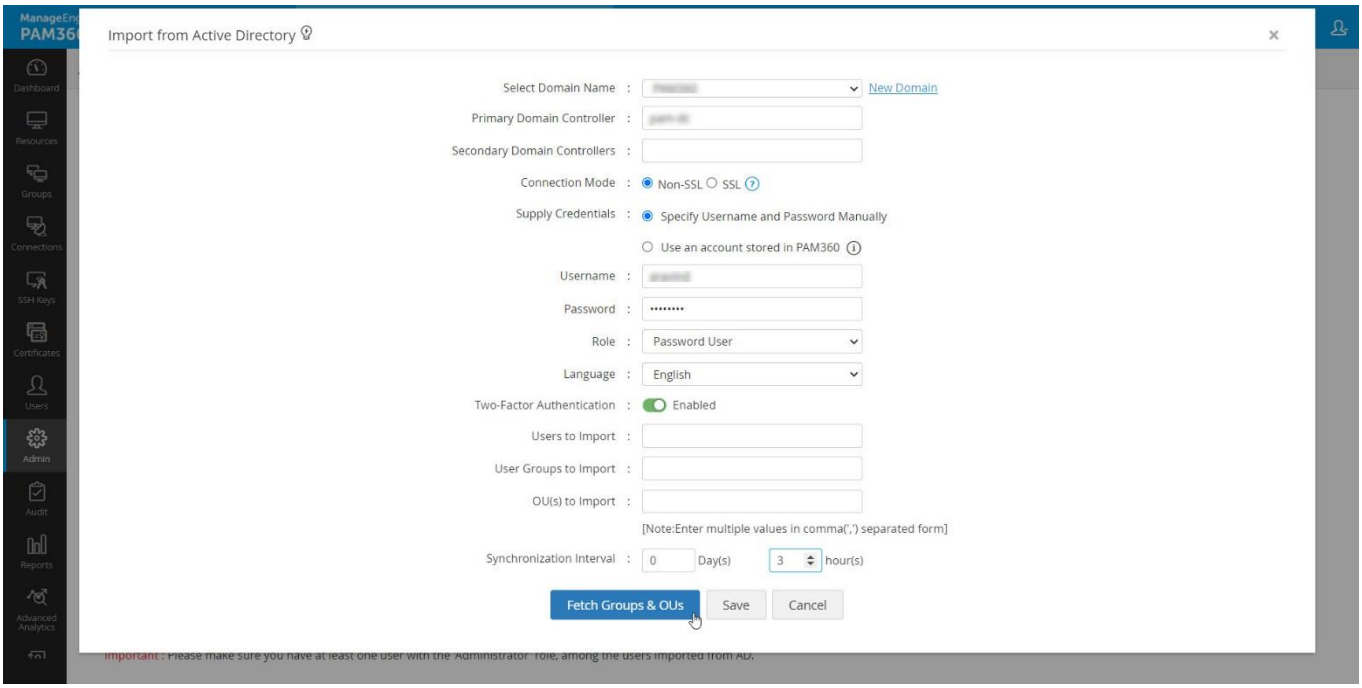
3.3 Deleting a User Group

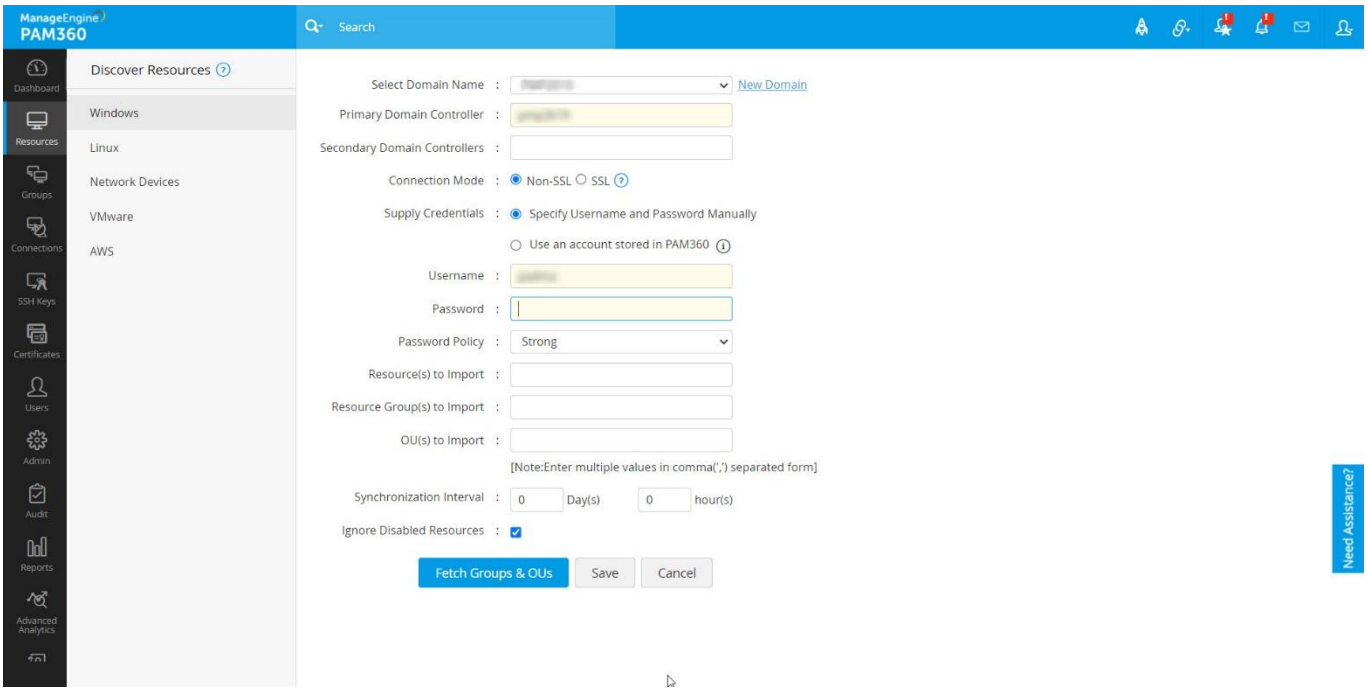
When a user group is deleted, the group level settings done for that group will no longer apply for the users who were members of that group. Deleting a user group will not affect the resources stored in PAM360. However, the resources shared to the group will no longer apply. Follow the below steps to delete an existing user group in PAM360:

1. Navigate to **User Groups** tab and select the required user group.
2. Click the **Delete Groups** button at the top.
3. In the pop-up form that appears, click **OK** to confirm.

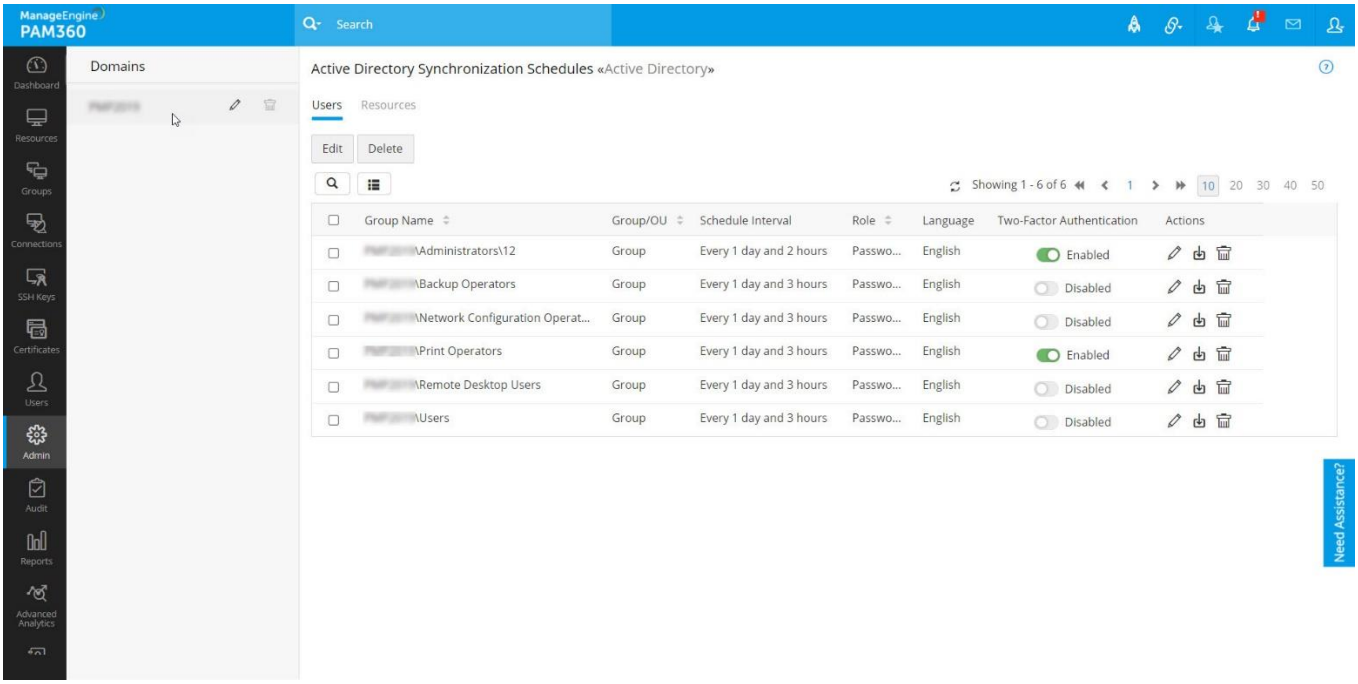
Active Directory Synchronization Schedules

While importing users or resources from Active Directory, PAM360 provides the option to configure auto-synchronization for a specific group or OU of an AD domain, so as to ensure that the user database is always updated. To set up synchronization, you have to initially enter the time interval at which PAM360 has to query the Active Directory to keep the user/resource database in sync, while providing the domain details to initiate import. The time interval could be in the range of hours/days. Refer to the images shown below for the same.





Details about all synchronization schedules that you have configured for different AD domains can be accessed by navigating to **Admin >> Active Directory >> View Synchronization Schedules**. In the page that loads, all AD domains for which synchronization has been configured will be listed in the sidebar navigation tab. Additionally, synchronization schedules configured for users and resources will be individually displayed under different sections respectively, as shown in the image below.



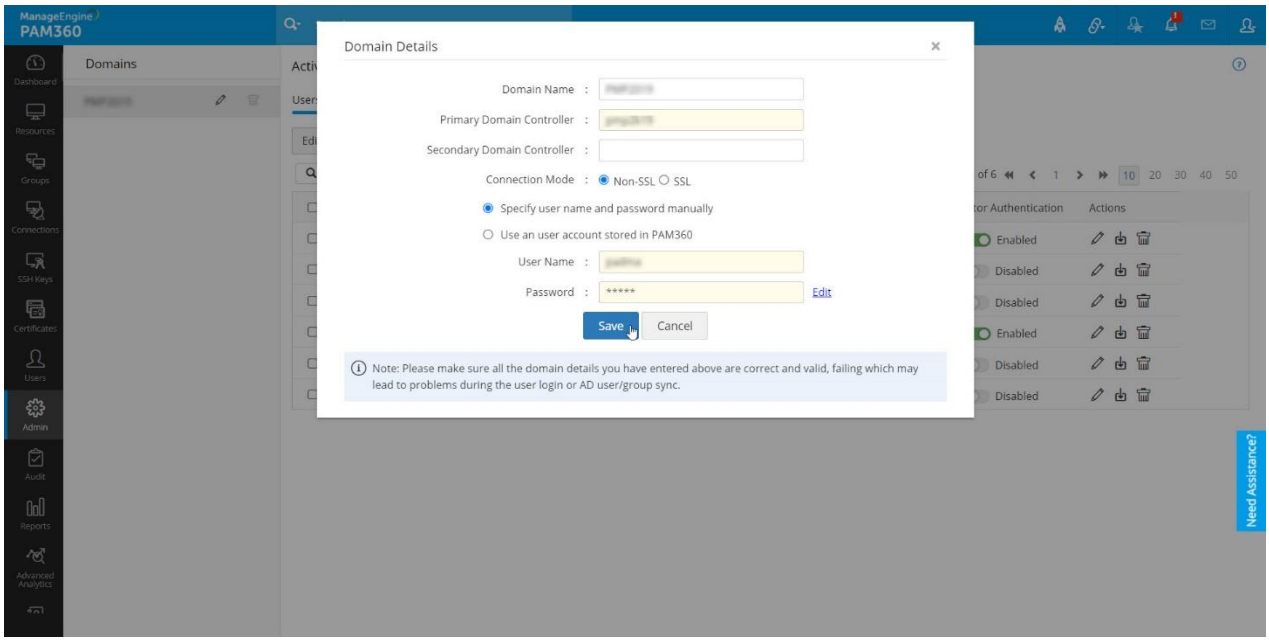
From this page, you can carry out the following activities:

1. **Modify/Delete Domain Details.**
2. **Modify/Delete Schedules.**

1. Modify/Delete Domain Details

To view or modify the details of an AD domain,

1. First locate the desired domain in the sidebar navigation tab and then click on the 'Edit' icon shown beside the domain.
2. In the dialog box that opens, you can make changes to domain details like domain name, primary/secondary domain controllers, connection mode etc.



3. Click **Save** to apply the changes.

> **Note:** Once you have modified the details of a domain, PAM360 will use the modified details the next time when it tried to communicate with the domain for data synchronization.

To delete a domain, locate the desired domain in the sidebar navigation tab and then click on the 'Delete' icon shown beside the domain. Click 'Ok' for confirmation.

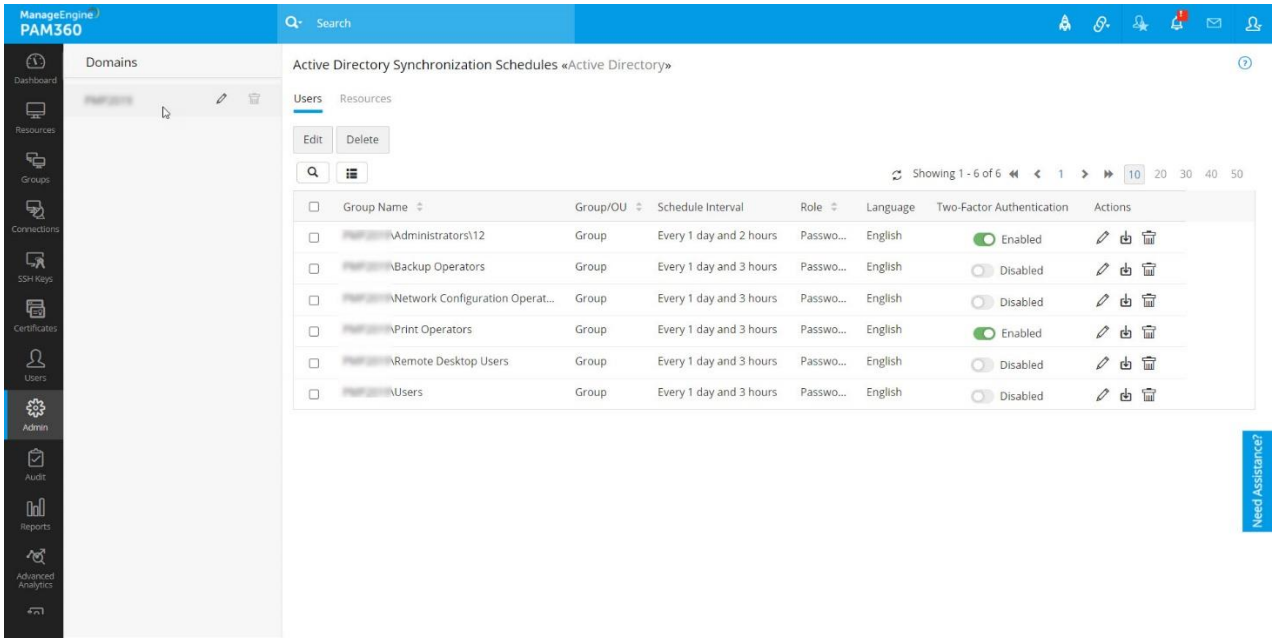
> **Note:** Once a domain is deleted here, all synchronization schedules configured for both user and resource import from that domain will be completely removed. To set up user/resource sync again, go to **Admin >> Active Directory >> Import Now (or) Resources >> Discover Resources.**

2. Modify/Delete Schedules

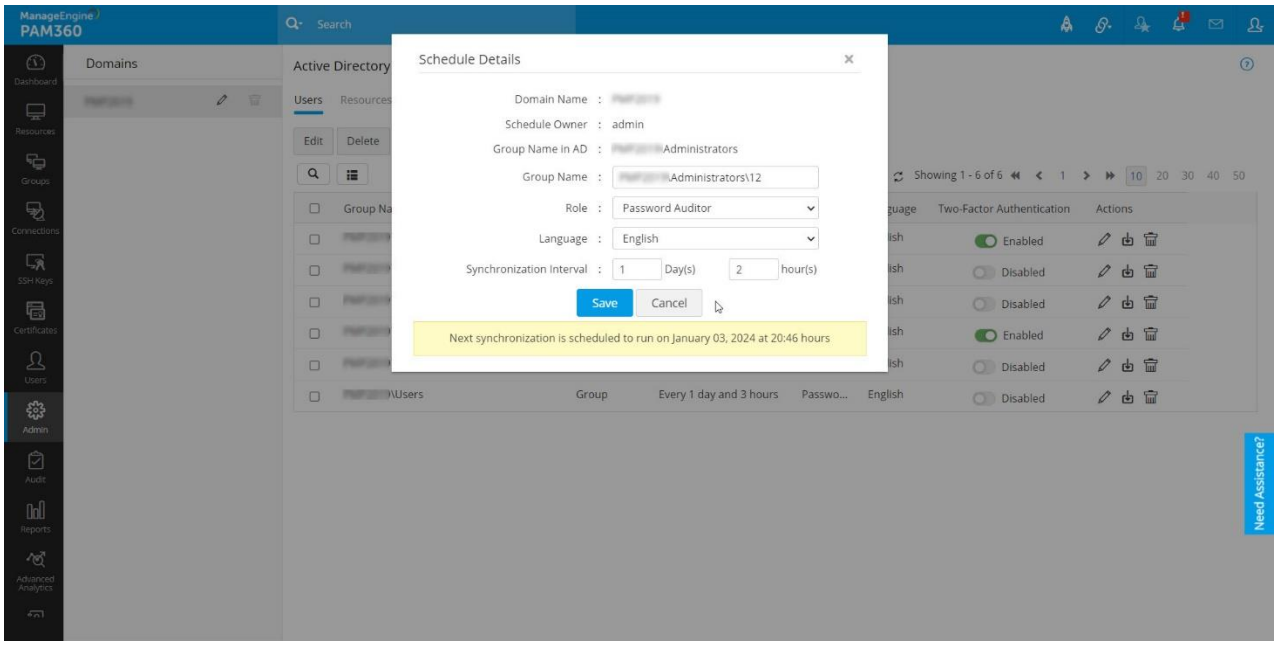
If you have configured a sync schedule for a specific AD domain while carrying out user/resource import operations, you can later modify the schedules and set different sync intervals for individual groups/OUs in that domain, for both user and resource import respectively.

To modify the sync schedule of a specific group/OU,

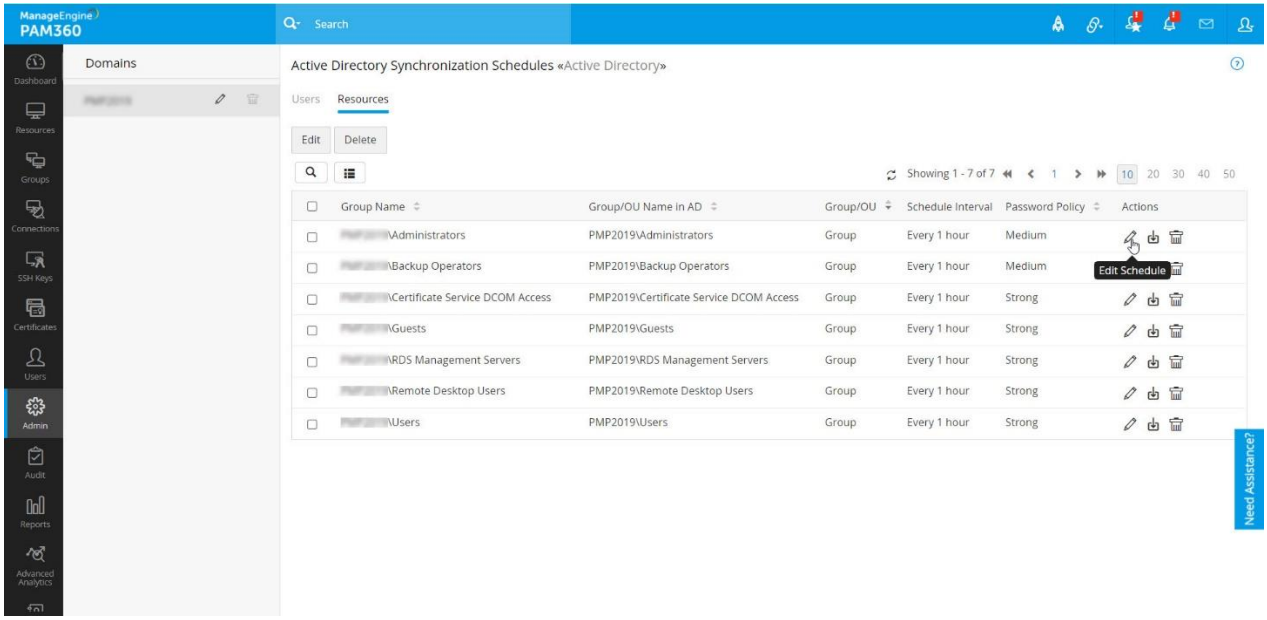
1. Locate the desired AD domain from the list of domains displayed in the sidebar navigation tab and click on it. PAM360 will load the list of all groups/OUs of that domain for which user sync has been scheduled (If you want to modify the schedule of resource sync, switch to the resources section.)



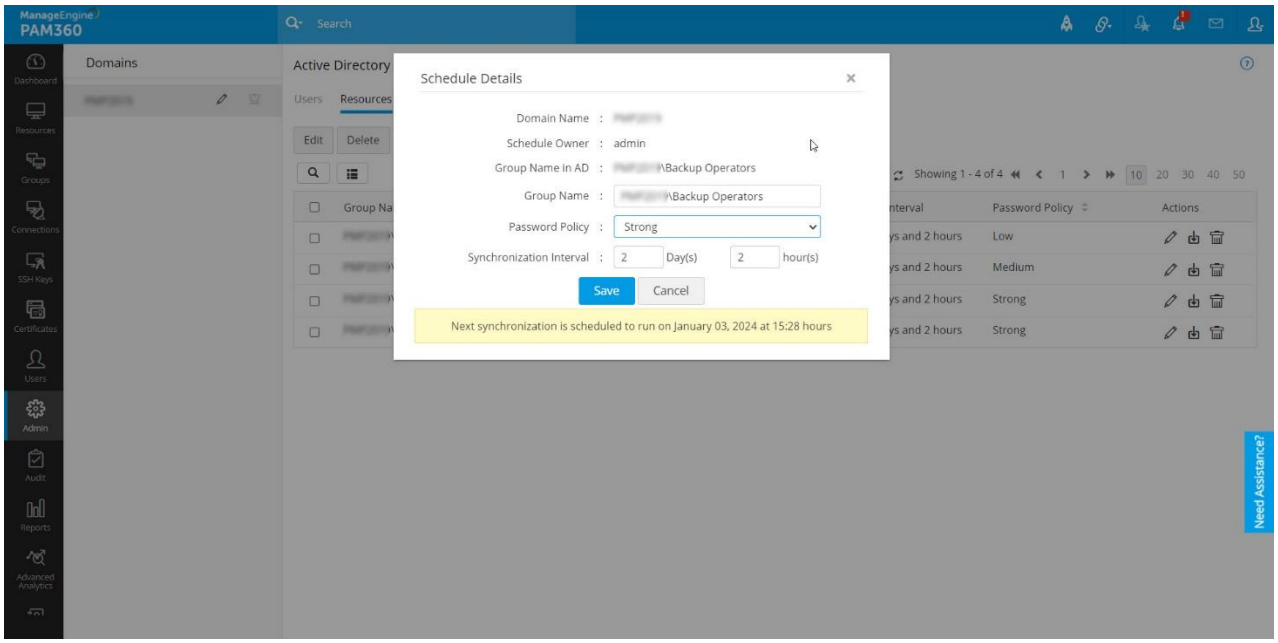
2. Next, locate the required group/OU from the list and click the **Edit Schedule** icon under the **Actions** column. In the dialog box that opens, you can modify the sync interval, role, and language as required. Additionally, you can also set a custom display name for the group/OU which will then be shown as the **Group Name** across all other tabs like **Users** and **Resources** where the group/OU is listed. The new display name can be added in the **Group Name** field in the **Schedule Details** dialog box. Click **Save** to apply the changes.



3. If you want to modify the schedule of resource sync, switch to the **Resources** tab and click the **Edit Schedule** icon.



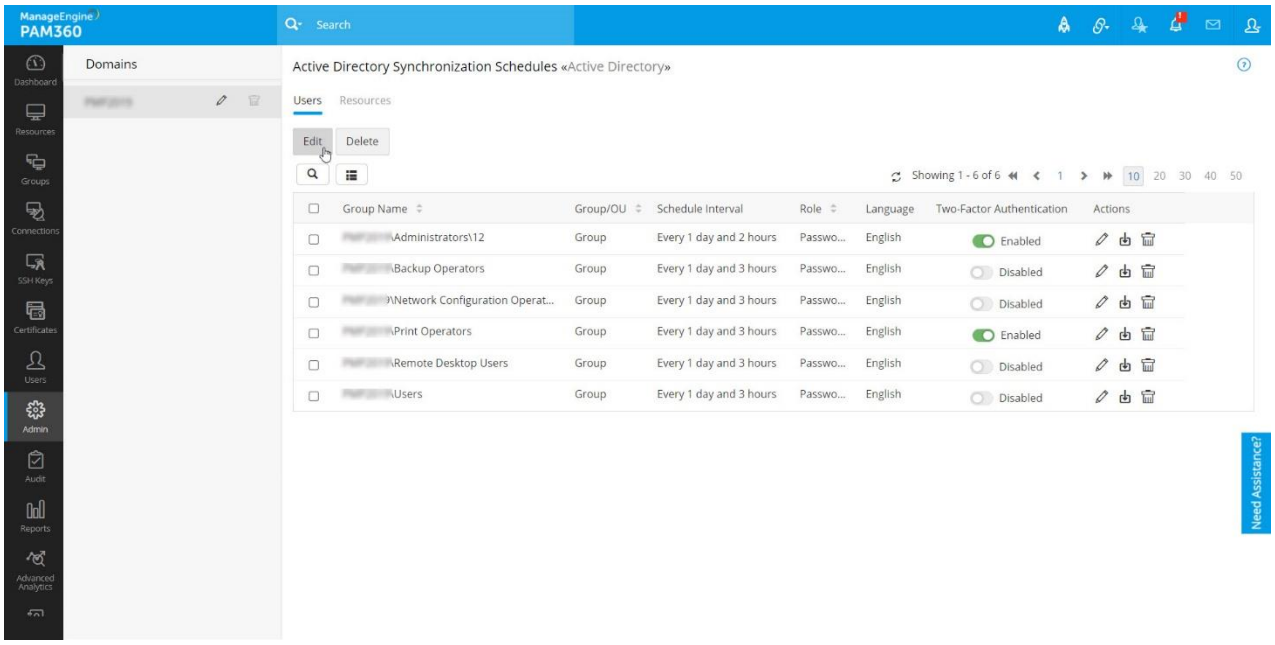
4. In the dialog box that opens, you can modify the group name, password policy, and sync interval. Click **Save** to apply the changes.



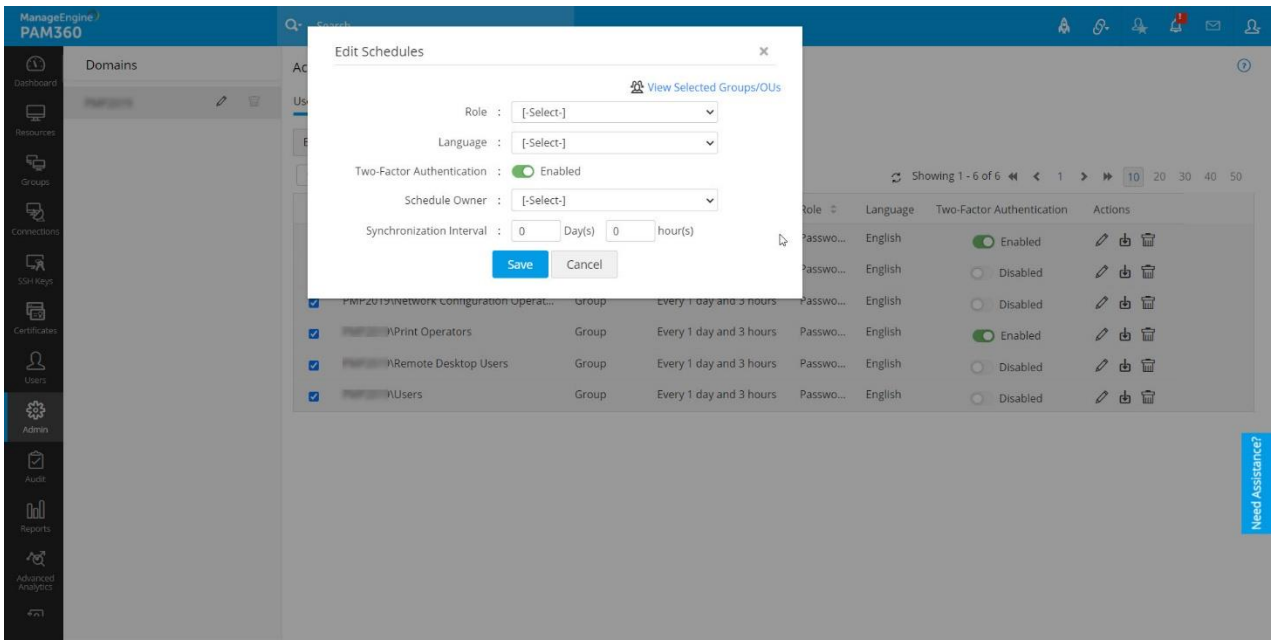
Note: Setting a custom display name will not overwrite the name of the group/OU in AD. The original AD name will also be retained.

To modify/delete schedules in bulk,

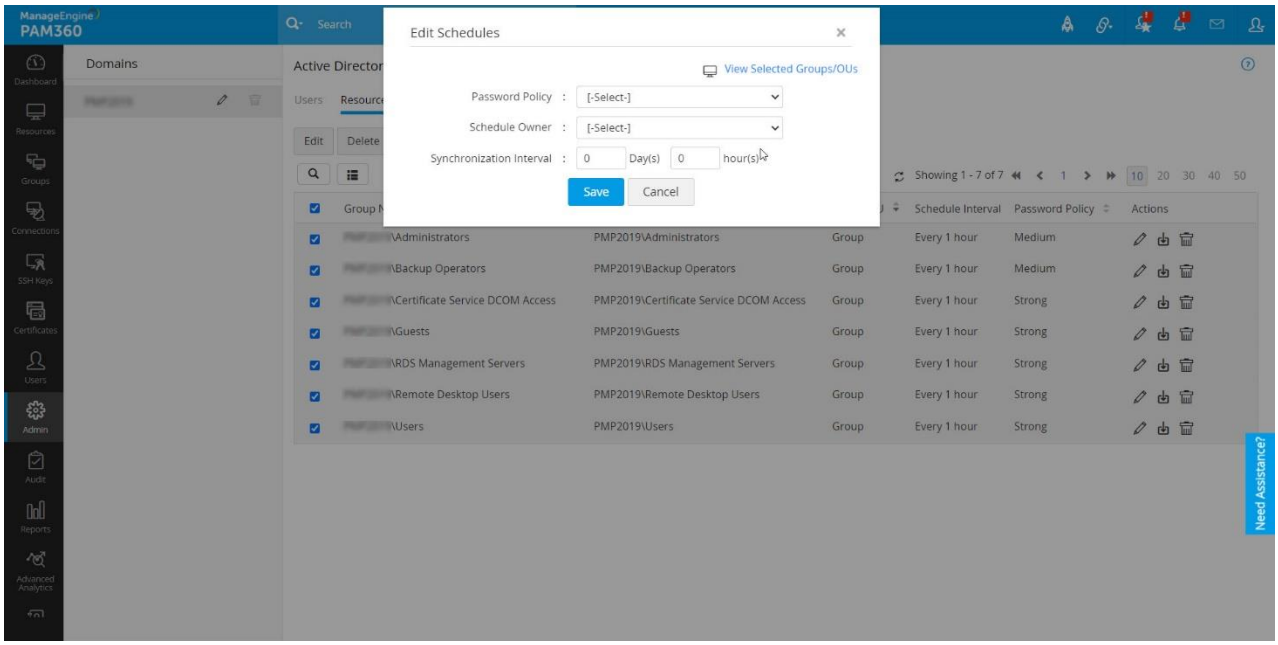
1. Navigate to the **Users** or **Resources** section as required, where the schedules have to be deleted.
2. Next, select the desired schedules.
3. To change the sync interval for the selected schedules in bulk, click on **Edit Schedules** shown above the schedules list.



4. In the dialog box that opens, you can update role, language, 2FA, schedule owner, and sync interval. To view the selected groups or organizational units, click on **View Selected Groups/OUs** at the top-right corner.



5. When modifying the schedule of resource sync in bulk, you can update password policy, schedule owner, and sync interval. Click **Save** to apply the changes.



6. To delete the selected schedules in bulk, click on **'Delete Schedules'** shown above the schedules list and click **'Ok'** to confirm deletion. The schedules will be deleted.

Note: By modifying the schedule owner, the ownership of the existing resources/users remains the same, and the new schedule owner will gain ownership of the new resources/users imported from the further synchronization interval. Also note that the schedule ownership can be transferred only to the users possessing the **Manage Active Directory** privilege in their defined role.

Importing Users from LDAP

(This procedure is applicable from build 6310)

LDAP (Lightweight Directory Access Protocol) is a widely used standard protocol for accessing and managing directory services that provide a standardized approach to storing and retrieving information about users, devices, and other network resources. In PAM360, you can now integrate your organization's LDAP servers and import users of your organization. Post importation, you can manage their privilege to the respective resources available in the organization.

Similar to importing users from a file, AD, and Microsoft Entra ID, you can also import users from LDAP directory. Read further to know how.

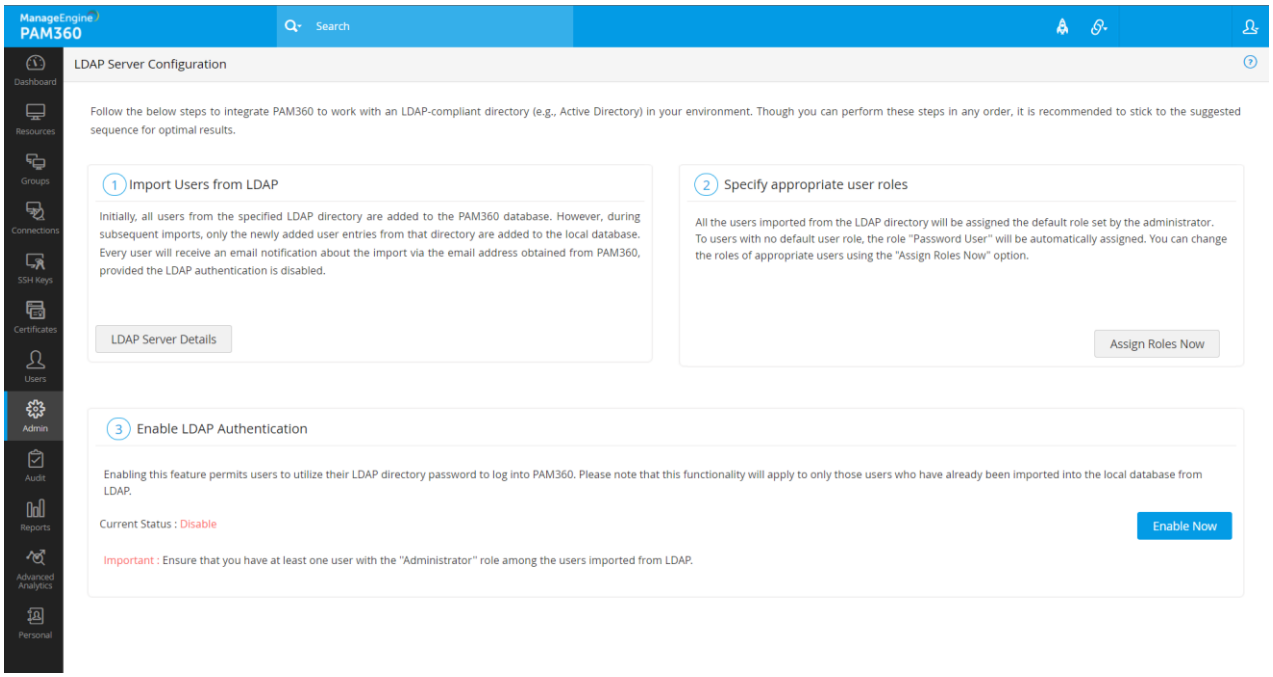
Steps Required for Importing Users

1. Configuring LDAP Server in PAM360
2. Importing Users from LDAP Server
   a. Configuring User Synchronization between LDAP Server and PAM360
3. Specifying Appropriate User Roles
4. Enabling LDAP Authentication
5. Managing LDAP Servers, Organizational Units, and Groups in PAM360

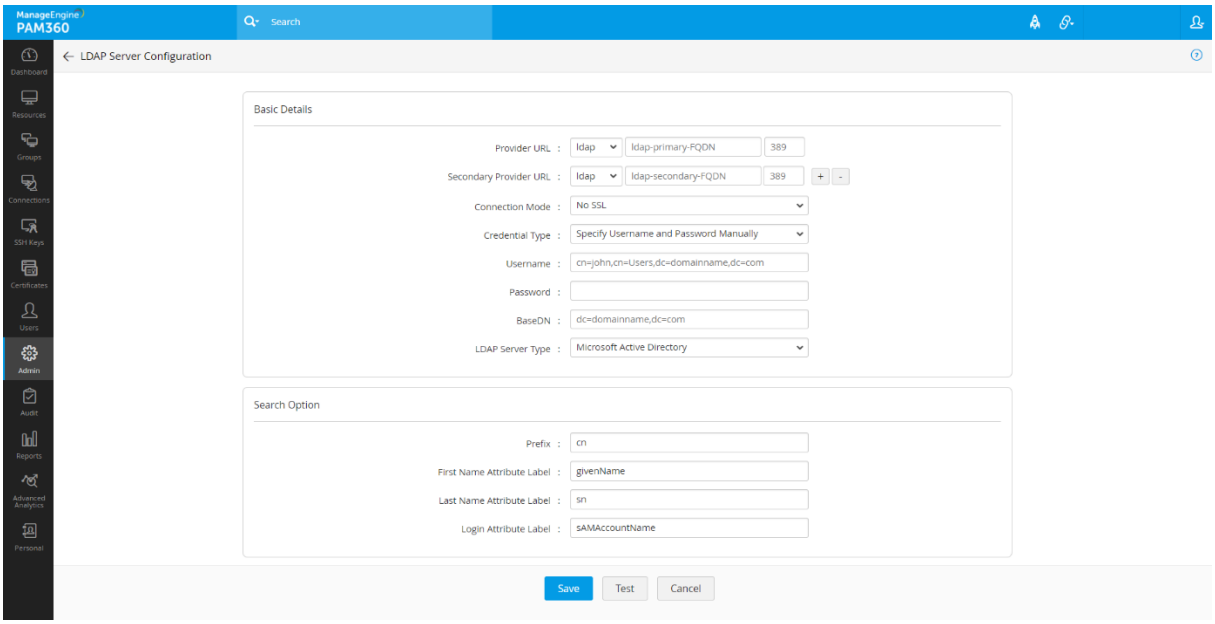
1. Configuring LDAP Server in PAM360

The first step is to provide the required server credential details in PAM360 to configure LDAP Server in PAM360. To do so, navigate to **Admin >> Authentication >> LDAP** and perform the steps that follow:

1. Click the **LDAP Server Details** button from the **LDAP Server Configuration** page to add your LDAP server in PAM360. Alternatively, you can also access this page from **Users >> Add User >> Import from LDAP**.



2. In the window that opens, click **Add** button or **Add New Domain** icon.
3. In the new window that opens, fill in the details as follows:
   i. Enter the URL of the LDAP provider. For example., **ldap pamwinsec23 389**.
   ii. You can configure the connection between LDAP Server and PAM360 to be over an encrypted channel (SSL) or Non-SSL. If you choose SSL mode as the connection mode, proceed with the following steps, else proceed with the next subsequent steps.
      a. To enable the SSL mode, the LDAP server should be serving over SSL in port 636, and you will have to import the LDAP server's root certificate, LDAP server's certificate, and all other certificates that are present in the respective root certificate chain into the PAM360's server machine's certificate store.
      b. To import certificates, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory and execute the following command:
         - **For Windows**:
           importCert.bat <Absolute Path of certificate>
         - **For Linux**:
           importCert.sh <Absolute Path of certificate>



iii. Restart the PAM360 server and continue with the following steps.

iv. In the supply credentials, select **Specify Username and Password manually** or **Use an account stored in PAM360**. If you have selected **Use an account stored in PAM360**, select the respective LDAP **Resource Name** and the **Account Name** from PAM360.

v. If you have selected **Specify Username and Password manually**, enter the credentials of any one of the users already present in LDAP for authentication. It should be in the format of how the user would have submitted their username when authenticating to your application. For example, a typical entry would look something like **cn=eric,cn=users,dc=manageengine,dc=com**

vi. Enter the **Password** of the given user.

vii. Enter the **BaseDN** information. This is the 'base' or 'root' from where directory lookups should take place. Enter the LDAP base (top level of the LDAP directory tree). Enter it exactly in the format used in your LDAP. No spaces are allowed between the commas or the '=' equal symbol and entries that are case-sensitive. For example.,**dc=manageengine,dc=com**.

viii. Select your **LDAP Server Type** from the options that follow:

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- Others

ix. If your LDAP server belongs to the type **Microsoft Active Directory/Novell eDirectory/OpenLDAP**, click **Test**.

x. Upon successful test validation, click **Save**.

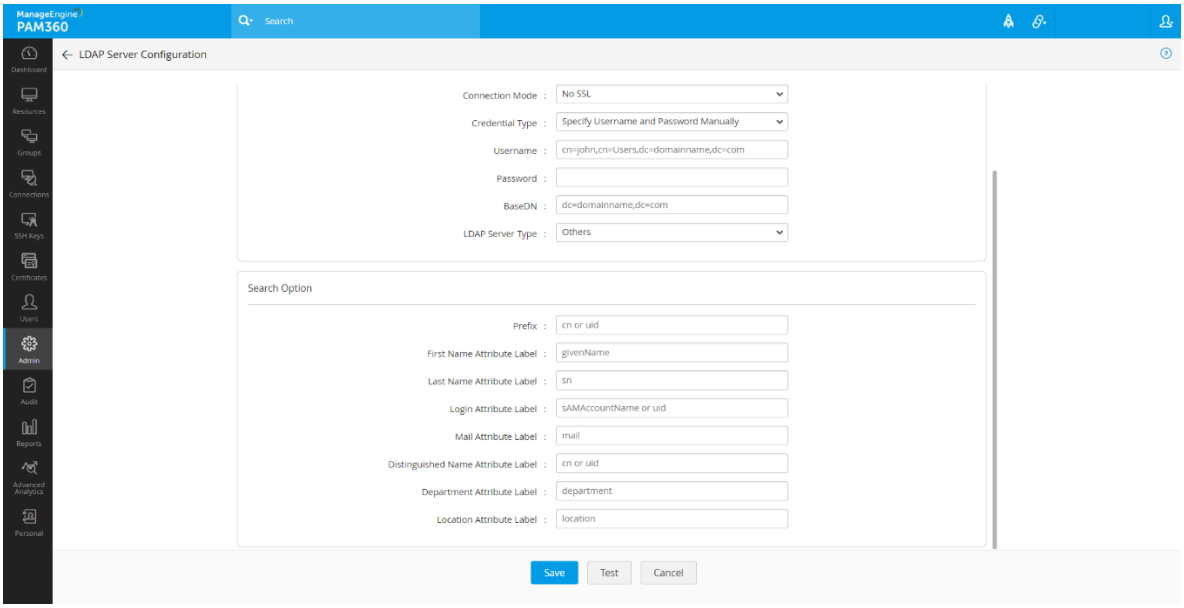
xi. If your LDAP server belongs to types other than **Microsoft Active Directory/Novell eDirectory/OpenLDAP**, specify the following additional details to authenticate the users:

a. Enter the user login attribute in your LDAP structure in the text field for **'Login Attribute Label'**. For instance, for LDAP making use of AD, the entry would be '**sAMAccountName**' and for OpenLDAP, the entry would be '**uid**'. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

b. Enter the e-mail attribute for the users in your LDAP structure in the text field for **'Mail Attribute'**. For instance, for LDAP making use of AD, the entry would be **'mail'**. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

c. Enter the distinguished name attribute - that is the LDAP attribute that uniquely defines this object. For instance, for LDAP making use of AD, the entry would be **'distinguishedName'** and for OpenLDAP, the entry would be **'dn'**. If you are using any other LDAP, make this entry in accordance with your LDAP structure.

d. Enter the remaining attributes accordingly and **Save** the LDAP server configuration.

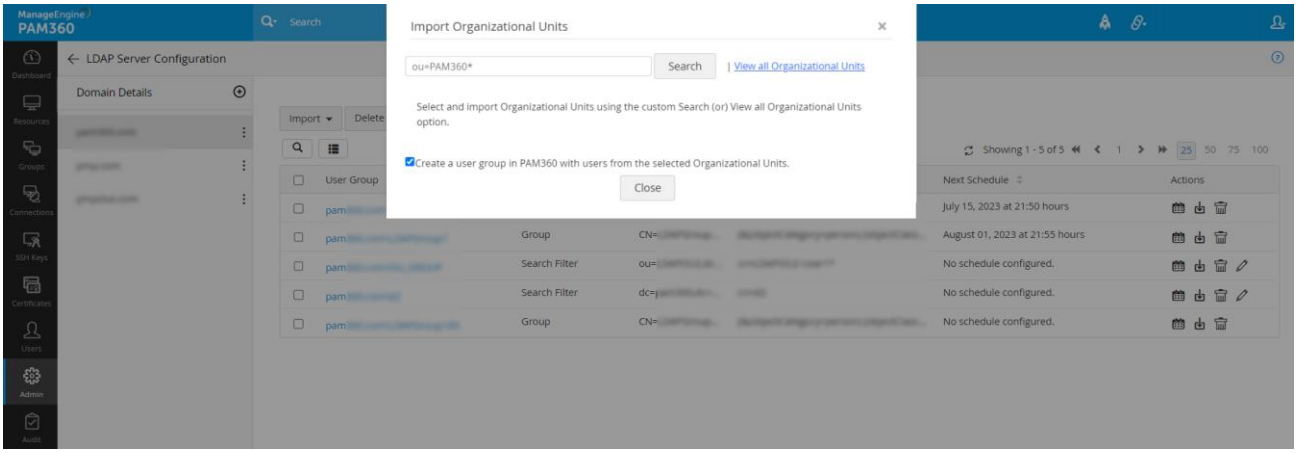


2. Import Users from LDAP

You can import users from LDAP into PAM360 via Organizational Units, Groups, and using Search Filters.

To import users from Groups/Organizational Units:

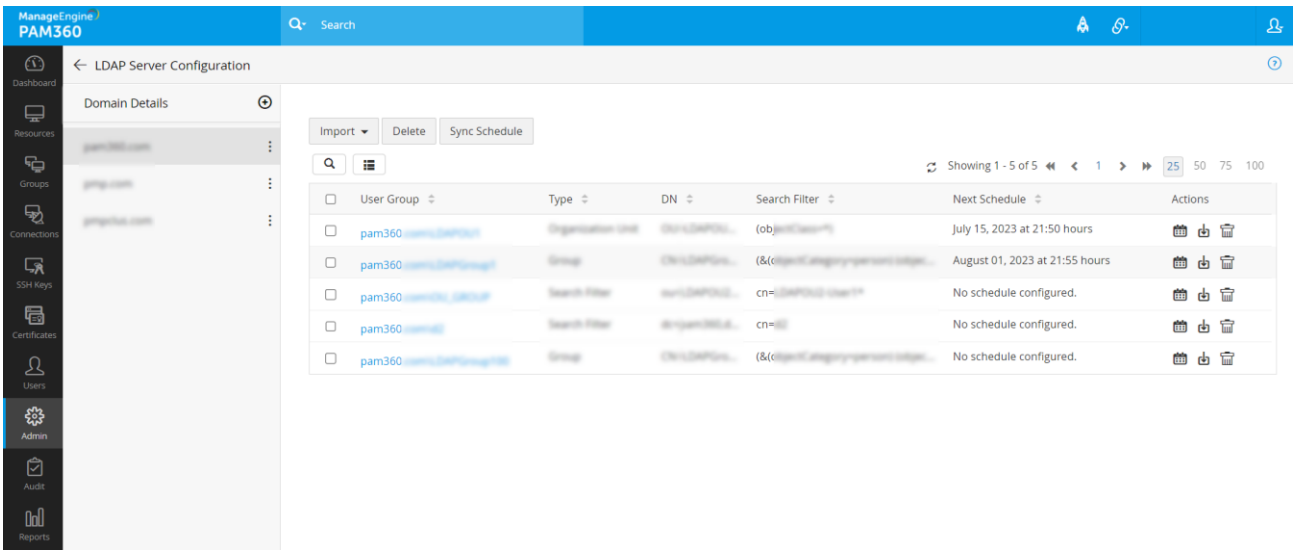
5. Navigate to the **LDAP Server Configuration** page and click **Import >> Groups/Organizational Units**.
6. In the pop-up that opens, look for the required Groups/Organizational Units using the Search option or the **View all Groups/Organizational Units** option.



7. Select the respective Groups/Organizational Units from the available list and click **Save**.

> **Note:** If you need the users present in the selected Group/OU to be created as a specific user group in PAM360, select the **'Create a user group in PAM360 with users from the selected Organizational Units'** before you click the **Save** button.

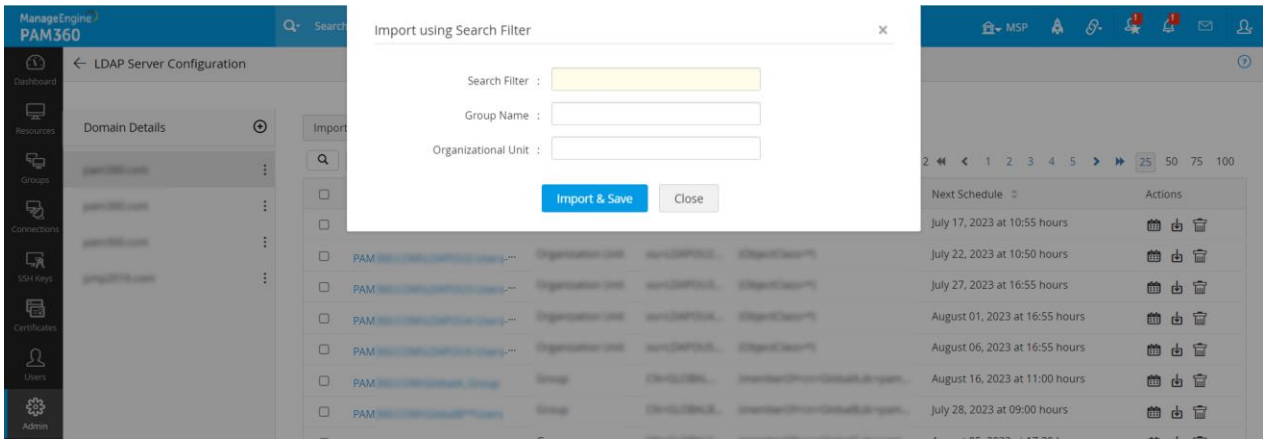
8. The imported Groups/Organizational Units will be listed in the respective window of the **LDAP Server Configuration** page.



To import the users apart from Groups and Organizational Units, you can utilize the Search Filter option as follows:

1. Navigate to the **LDAP Server Configuration** page and click **Import >> Using Search Filter**.

2. In the pop-up that opens, enter the search filter information and click **Save**.
3. Enter the Group name and the Oragnizational Units as the optional information in which the search filter has to be looked for.



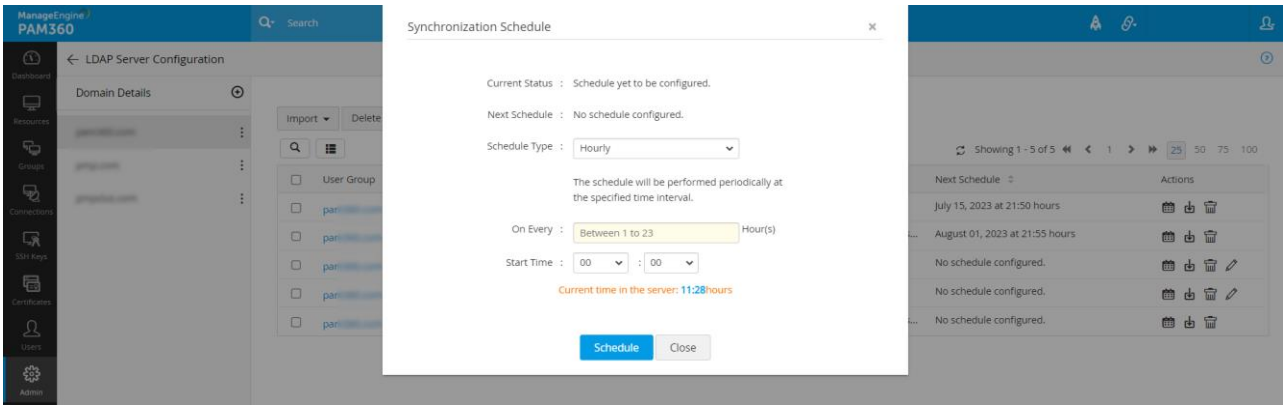
Now, click on the **Import from LDAP** icon beside the respective Groups/Organizational Units/Search Filter configuration to import the users into PAM360.

Soon after hitting this **'Import from LDAP'** button, PAM360 will start adding all users from the respective configurations of the LDAP. During subsequent imports, only the new user entries in LDAP are added to the PAM360. During import, every new user will be notified through email about their account, along with a password that will be used to log in to PAM360 when LDAP authentication is disabled.

2.1 Configure Synchronization between LDAP Server and PAM360

Whenever new users get added to the LDAP, there is a provision to automatically add them to PAM360 and keep the user details in sync. This can be done from the **'LDAP Server Configuration'** page in individual or in bulk.

5. To synchronize the users from LDAP configuration to PAM360, click on the **Sync Schedule** icon beside the desired Groups, Organizational Units, or Search Filter.
6. In the pop-up that opens, enter the time interval at which PAM360 has to query the LDAP server to keep the user details in sync. The time interval could be as low as a minute, or it can be in the range of hours/days.
7. Now, click **Save** to schedule the synchronization accordingly.



8. To schedule the synchronization in bulk,
    a. Select the desired Organizational Units, Groups, or Search Filters and click the **Sync Schedule** button at the top pane.
    b. In the pop-up that opens, enter the time interval at which PAM360 has to query the LDAP server to keep the user details in sync and click **Save**. The time interval could be as low as a minute, or it can be in the range of hours/days.

3. Specifying Appropriate User Roles

All the users imported from LDAP will be assigned the **'Password User'** role by default. To assign specific roles to specific users,

1. Navigate to **Admin >> Authentication >> LDAP** and click **Assign Roles Now**.
2. In the pop-up form that opens, all the users imported from AD will be listed.
    a. Click the **Change Role** button against desired users for whom you wish to change the role and select the appropriate role from the dropdown.
    b. Click **Save**, and the required roles are set for the users.

4. Enabling LDAP Authentication

The final step is to enable LDAP authentication. After this, your users can use their LDAP directory password to log into PAM360. Please note that this will work only for users who were already imported to the PAM360 from LDAP.

Note: Make sure you have at least one user with the 'Administrator' role among the users imported from LDAP.

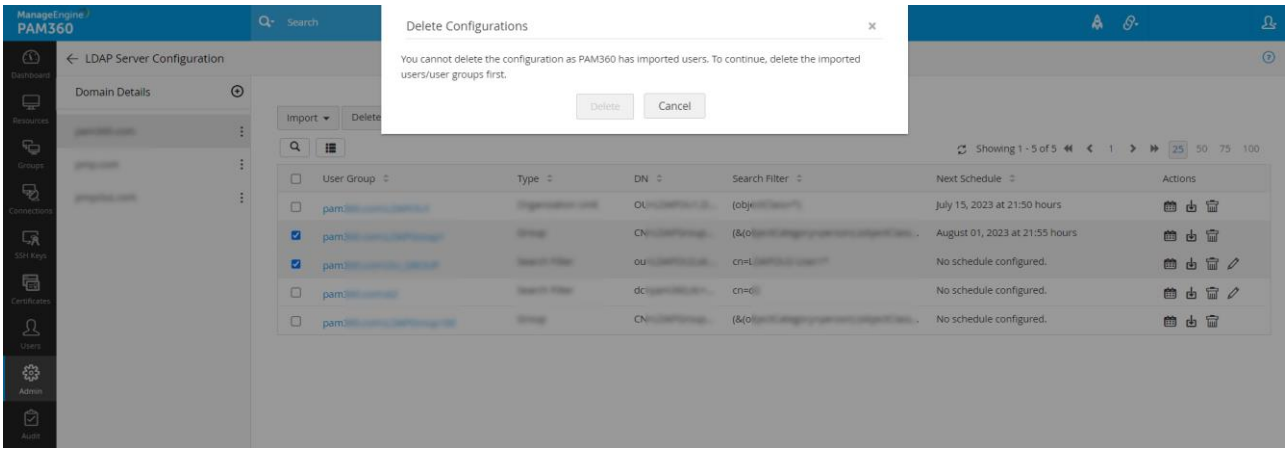
5. Managing LDAP Servers, Organizational Units, and Groups in PAM360

Navigate to **Admin >> Authentication >> LDAP >> LDAP Server Details**. In the window that opens,

a. Click the kebab menu icon () beside the respective LDAP server to delete the existing one or edit entries pertaining to the LDAP server.

b. Click the delete icon beside the respective OU, Group, or Search Filter to delete the imported LDAP configurations from PAM360. In addition, you can also perform this operation in bulk by selecting the respective Organizational Units, Groups, or Search Filter and clicking on the **Delete** button at the top pane.

> **Note:** The deletion of Groups, Organizational Units, and Search Filters will exclusively remove their respective entries from the PAM360 database and will not impact any data within the LDAP server.



Integrating RADIUS Server & Leveraging RADIUS Authentication

You can integrate PAM360 and RADIUS server in your environment and also leverage the RADIUS authentication for user access bypassing the local authentication provided by PAM360. This section explains the configurations involved in integrating RADIUS server with PAM360.

Steps Required

1. **Providing Basic Details about RADIUS Server**
2. **Enabling RADIUS Authentication**

1. Providing Basic Details about RADIUS Server

To configure RADIUS server in PAM360, provide the following basic details about RADIUS server and credentials to establish connection:

1. Go to **Admin >> Users >> RADIUS.**
2. In the UI that opens, click **Configure** on step 1.
3. In the UI that opens, provide the following details
    a. **Server Name/IP Address** - enter the host name or IP address of the host where RADIUS server is running
    b. **Server Authentication Port** - enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication
    c. **Server Protocol** - select the protocol that is used to authenticate users. Choose from four protocols - Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MSCHAP), Version 2 of Microsoft Challenge-Handshake Authentication Protocol (MSCHAP2)
    d. **Authentication Retries** - select the number of times you wish to retry authentication in the event of an authentication failure.
    e. **Server Secret** - You have the option to enter the RADIUS server secret either manually in the text box or you can direct PAM360 to use the secret already stored in the product. In that case, you need to select the resource name and account name from the drop-down. The second option - storing

the RADIUS password in PAM360 and selecting it from drop-down is the recommended approach.

f. Click **Save.**

4. You have successfully configured RADIUS server in PAM360.

2. Enabling RADIUS Authentication

After configuring the RADIUS server, the next step is to leverage the RADIUS server's authentication mechanism. To enable RADIUS authentication, click the button "**Enable**" in step 2. Once you do this, users would be able to login with their RADIUS credentials.

Important Note: The users who will be accessing PAM360 using their RADIUS server credentials, will have to be added as users in PAM360 first. When you do so, you need to ensure that the "user name" in PAM360 is exactly the same as the username used for accessing the RADIUS server. Here, PAM360 does not store the password used for RADIUS authentication.

Smart Card / PKI / Certificate Authentication

Since PAM360 serves as the vault for sensitive passwords, it is essential to have a strong authentication mechanism to grant access to the software. PAM360 provides various authentication options and users can choose the ones that suit their environment better. Apart from PAM360's local authentication, there is provision for leveraging the authentication of external identity stores such as Active Directory/LDAP.

To bolster the security further, PAM360 offers Smart Card Authentication, which makes the authentication stronger because, to get access to PAM360, the user must possess the smart card and should know the personal identification number (PIN) as well.

Smart Card authentication in PAM360 serves as the Primary Authentication and it should not be confused with the Two Factor Authentication.

If you have a smart card authentication system in your environment, you can configure PAM360 to authenticate users with their smart cards, bypassing other first factor authentication methods like AD, LDAP or Local Authentication.

Enabling Smart Card authentication involves the following steps:

1. How does the Authentication Mechanism Work?
2. Workflow
3. Importing the Root of CA
4. Mapping User Details
5. Configuring Status Check for User Certificates
6. Comparing User Certificates for Verifying Authentication
7. Enabling Smart Card Authentication
8. Restarting PAM360 Server & Web Browser
9. Smart Card Authentication in High Availability Scenario

1. How Does the Authentication Mechanism Work? (PAM360)

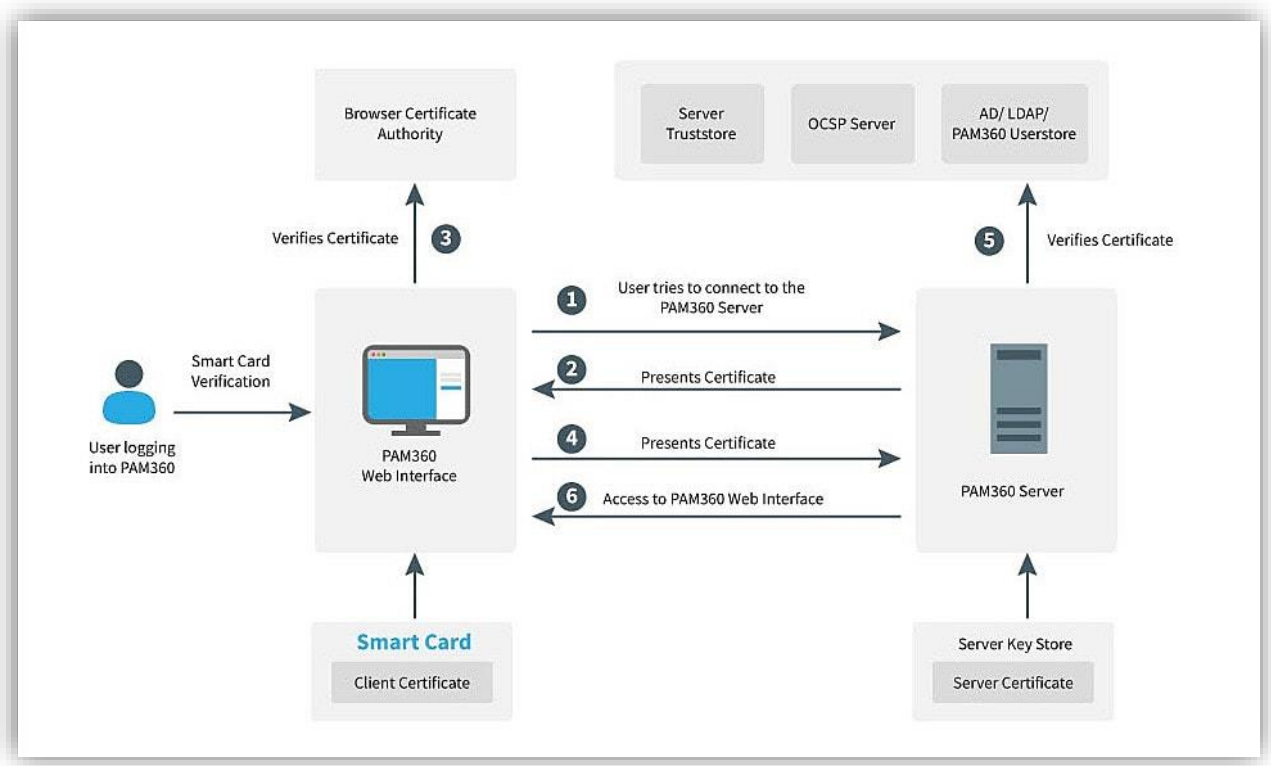
When the user attempts to access PAM360 web-interface, he would be allowed to proceed further only if he had already completed the smart card authentication in the machine by presenting the smart card and subsequently entering the PIN. PAM360's web-interface supplements smart card technology with SSL communication. So, the user is prompted to specify their X.509 certificate for getting access.

The users can choose to provide the certificate from the smart card or the local certificate store, in which case PAM360 performs the steps to authenticate the user with the certificate. The users can also choose to decline providing the certificate and PAM360 takes them to the usual login page for authentication.

2. Workflow

2.1 Smartcard Authentication Workflow

1. User tries to connect to the PAM360 server.
2. The PAM360 server presents its certificate to the client. (web-interface)
3. The client verifies the server's certificate with that of the browser certificate authority.
4. If the above process is successful, the client sends the user's smartcard certificate to the server.
5. The server verifies the client certificate with the server's trustStore and then checks the revocation status with the OCSP server (if applicable); finally checks if the user certificate is same as the one in the AD/LDAP or PAM360 user store.
6. If the above process also succeeds, the PAM360 server grants the user access to the web interface.



2.2 Smart Card Authentication in PAM360

1. User tries to access PAM360 web-interface.
2. The attribute that uniquely identifies the user in the smartcard certificate is compared with the corresponding attribute in PAM360 userstore.
3. Then, the user certificate - the X.509 certificate stored in the PAM360 database in the case of users manually added will be compared with the one presented by the user. In the case of users imported from Active Directory / LDAP, the certificate will be retrieved from AD/LDAP for comparison.

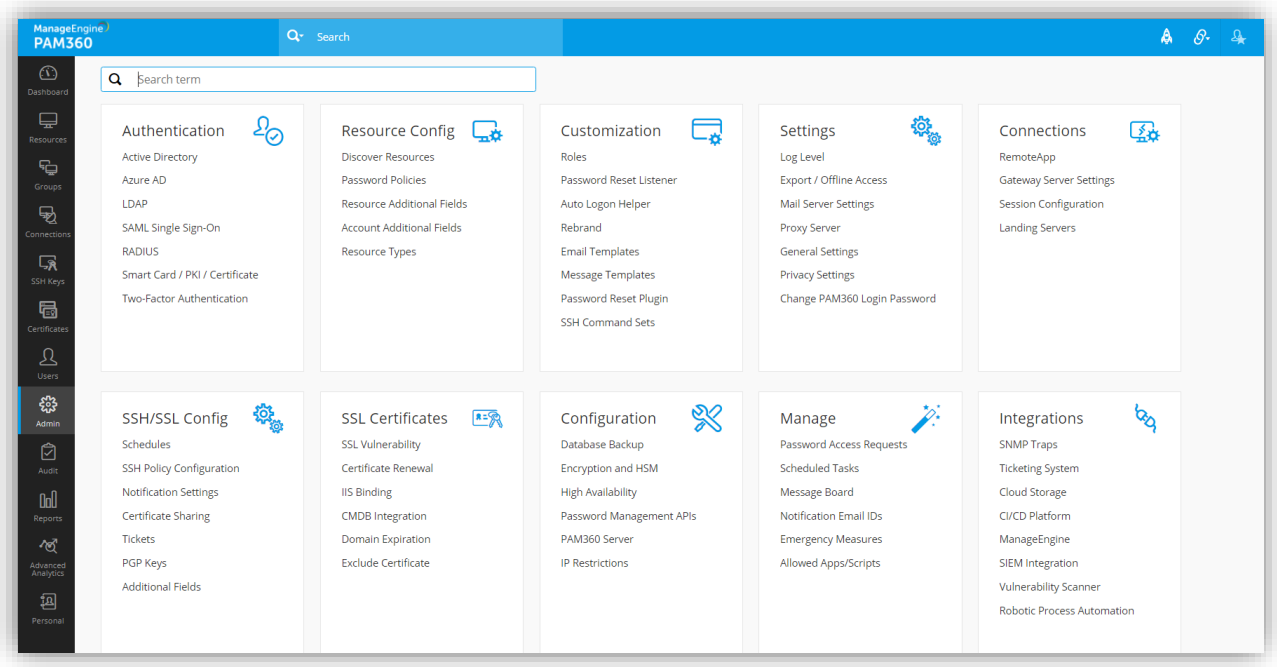
4. If there is perfect matching, user is allowed access.

3. Importing the Root of CA

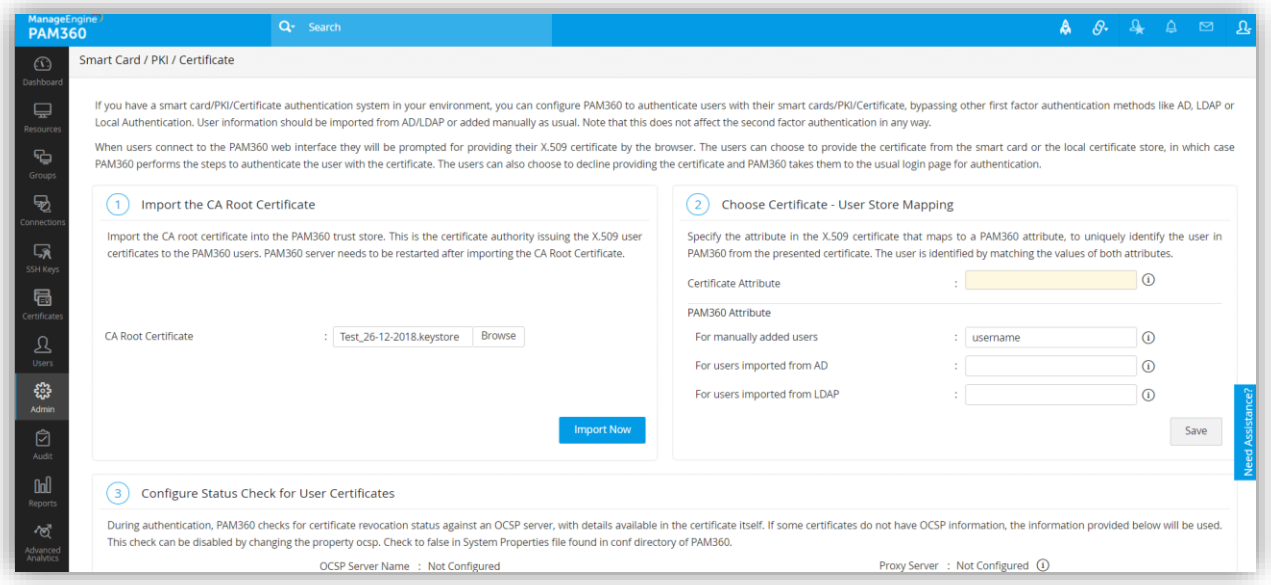
In case, you are using an already available internal certificate (your own certificate), you need to specify the root of the CA. This is the certificate authority issuing the X.509 user certificates to the PAM360 users. If you are using a certificate signed by third-party CA, you may skip this step.

To import the root of the CA,

1. Navigate to **Admin >> Authentication >> Smart card / PKI / Certificate**.



2. In the UI that opens, specify the path of the root of the CA and click **Import Now** button in Step 1.
3. Restart PAM360 server.



Once you execute the above, the root of the CA will be recorded in PAM360. All the certificates signed by the particular CA will henceforth be automatically taken.

4. Mapping User Details (between smartcard certificate and PAM360 user store)

The next step is to choose the mapping between the smartcard certificate and the PAM360 user database. That means, the attribute in the smartcard certificate that uniquely identifies the user should match with the corresponding value in the PAM360 user database.

This mapping involves two things:

1. Specifying which attribute in certificate should be taken up for comparison.
2. Specifying the corresponding matching attribute in PAM360 user store.

4.1 Specifying the certificate attribute

1. PAM360 provides the flexibility to specify any attribute of the smartcard certificate that you feel uniquely identifies the user in your environment. You may choose any attribute among SAN.OtherName, SAN.RFC822Name, SAN.DirName, SAN.DNSName, SAN.URI and Common Name. During authentication, PAM360 reads the value corresponding to this attribute and compares it with the attribute in PAM360 user store.
2. From the drop-down **Certificate Attribute**, select the desired attribute.

> **Note:** In case, in your environment, if any other attribute is used to uniquely identify the user, contact PAM360 support to add that attribute.

4.2 Specifying the matching PAM360 user name

After specifying the Certificate Attribute, you need to specify the mapping attribute in PAM360 user store. That means, you need to specify the particular attribute that uniquely identifies the user in PAM360 user store. This depends on how the user was added in PAM360 - whether by manual addition or imported from Active Directory / LDAP.

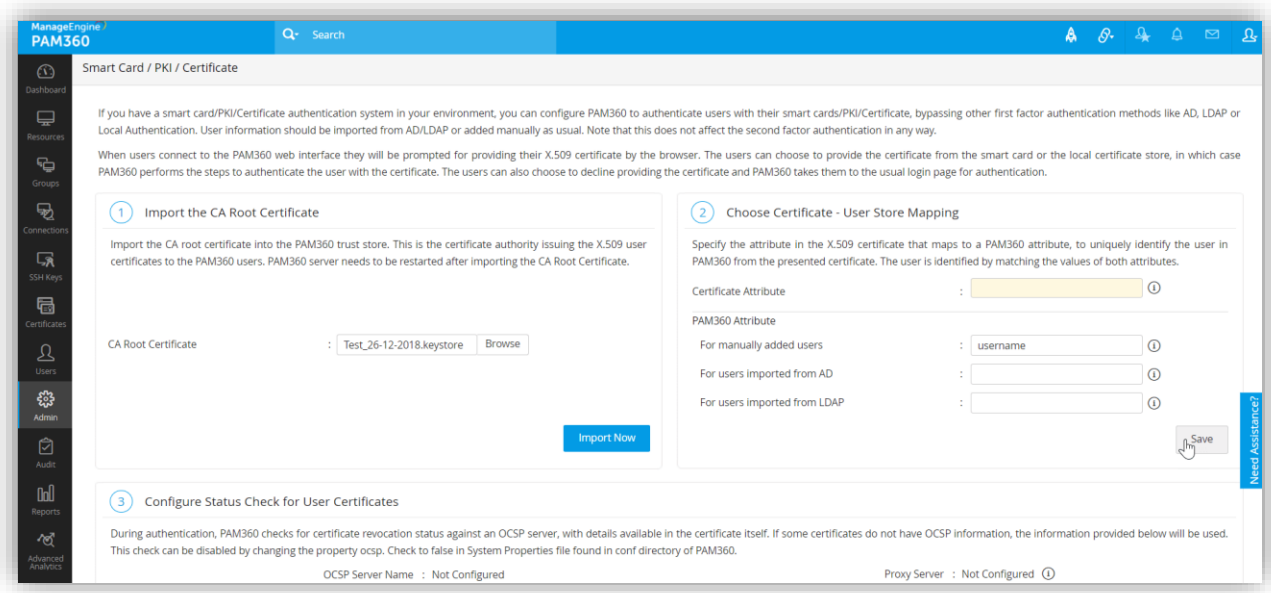
4.3 Users manually added

For the users manually added into PAM360, username in PAM360 is probably the only attribute that could be taken up for comparison with the corresponding attribute in certificate. So, just leave this text field with the default value **username**.

4.4 Users imported from Active Directory / LDAP

In the case of the users imported from Active Directory/LDAP, normally the attribute **userPrincipalName** is used to uniquely identify the user. It is quite possible that in your environment, some other attribute like **distinguishedName** might uniquely identify the user. So, specify the attribute accordingly.

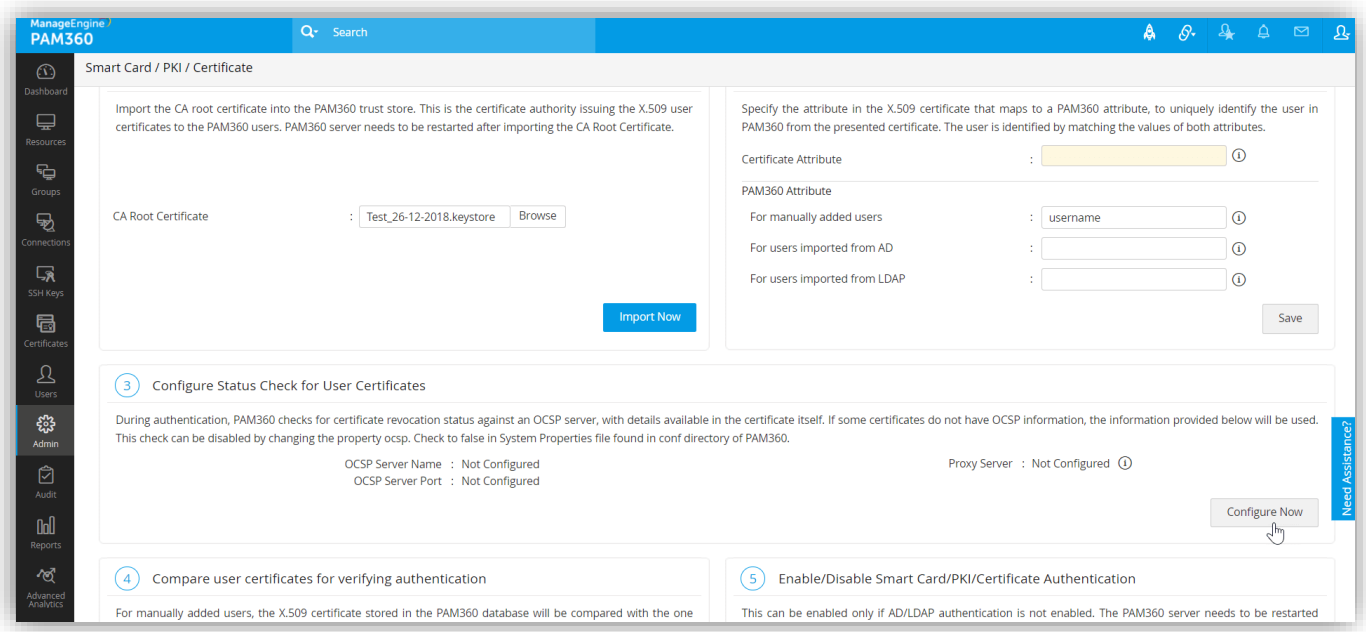
- Finally, **Save** the settings.



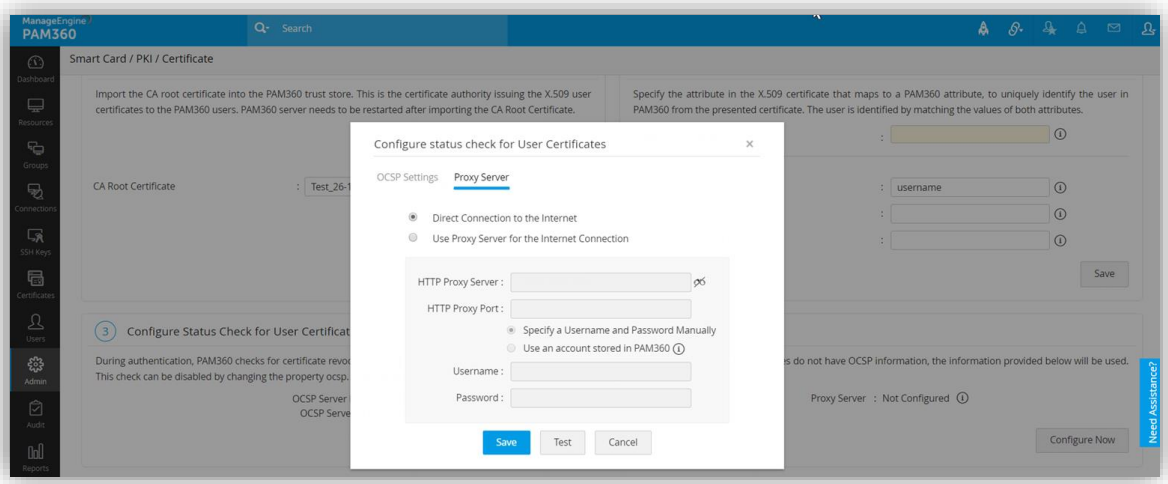
5. Configuring Status Check for User Certificates

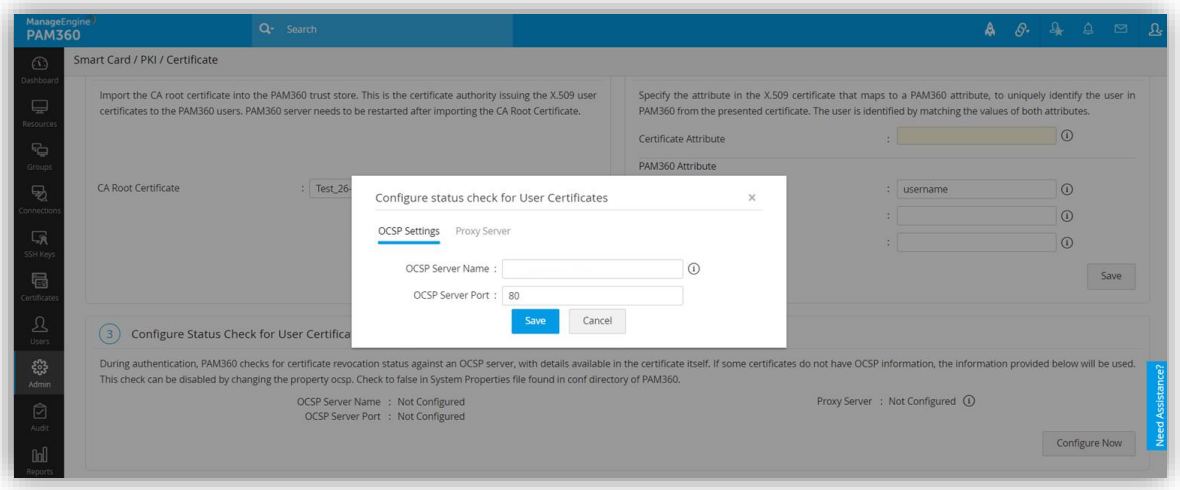
During authentication, PAM360 checks for certificate revocation status against an Online Certificate Status Protocol (OCSP) server, with details available in the certificate itself. If some certificates do not have OCSP information, the information provided in the settings here will be used. This check can be disabled by changing the property ocsp.check to false in **System Properties** file found in conf directory of PAM360.

Also, authentication through OCSP will require access to the internet. In enterprise network setup, you might need to go through a proxy server to access the internet. You may specify proxy server settings if you have not specified it already.



1. Click the button **Configure Now.**
2. In the pop-up form that opens,
    i. Enter OCSP server details such as **OCSP Server Name** and **OSCP Server Port.**
    ii. Click **Save**.



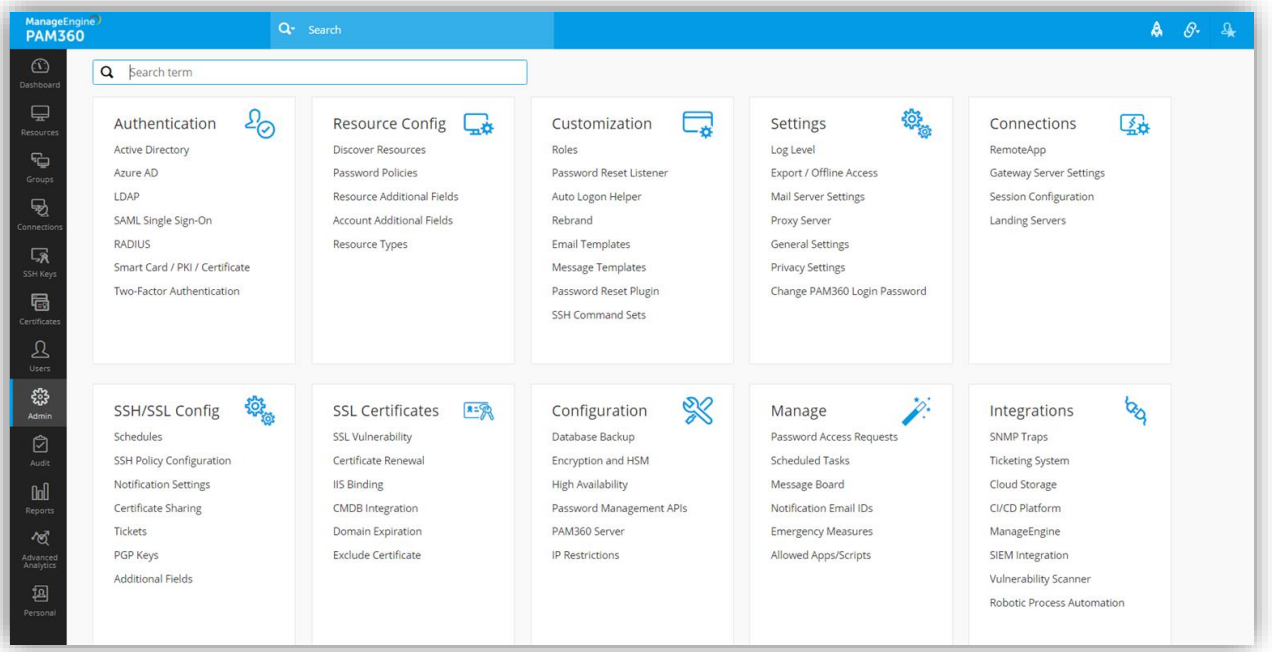


6. Comparing User Certificates for Verifying Authentication

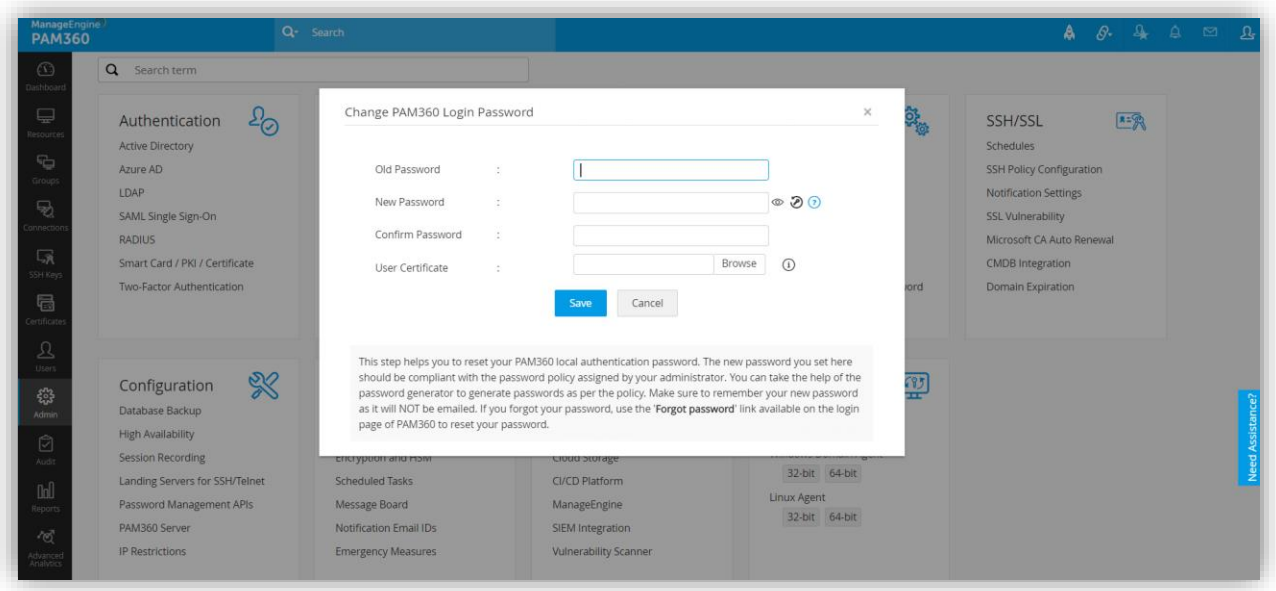
Another step in the authentication process is comparison of the user certificates presented by the user and the ones stored in the system or Active Directory/LDAP. For the users who were added manually, the X.509 certificate stored in the PAM360 database will be compared with the one presented by the user.

Note: In case, you do not have AD or LDAP in your environment, you need to manually put the x.509 format SSL certificate used for smartcard authentication into PAM360.

1. Navigate to **Admin >> Settings >> Change PAM360 Login Password**.



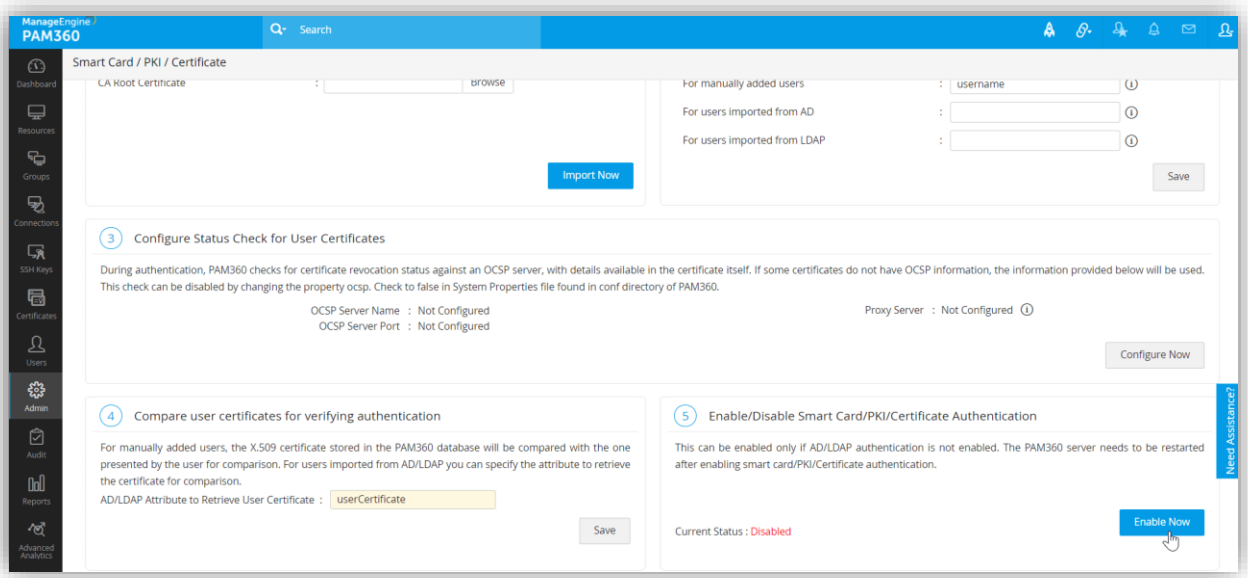
2. In the pop-up form that opens, change the **User Certificate** to specify the path of the x.509 format SSL certificate.
3. Click **Save**.



7. Enabling Smart Card Authentication (PAM360)

After carrying out the settings, you need to enable Smart Card Authentication. Before enabling this, you need to ensure that AD/LDAP authentication is disabled.

- Click **Enable** to enable smart card authentication.



8. Restarting PAM360 Server & Web Browser

After completing aforesaid steps, restart PAM360 server and the web server once to give effect to the settings. Whenever you enable or disable Smart Card authentication in PAM360, you need to restart the server and the browser to give effect to the change.

Important Note:

- Once you enable smart card authentication, it will take effect globally - that means, Smart card authentication will be applied to all the users. However, the users for whom smart card authentication is not applicable, will be prompted to use local authentication automatically.
- When smart card authentication is enabled, AD or LDAP authentication will remain suspended for all users. So, you need to choose between AD, LDAP and Smart card.

9. Smart Card Authentication in High Availability Scenario

If you have configured high availability and if you have enabled smart card authentication in Primary, the same has to be configured in the secondary server too.

To do this,

1. Stop PAM360 primary server
2. Connect to the PAM360 secondary server
3. Go to **Admin >> Authentication >> Smart card / PKI / Certificate.**
4. In the UI that opens, perform Step 1 and Step 5 alone (for details, refer to the section 7 enabling smart card authentication above)
5. Restart secondary after completing the above steps

10. Troubleshooting Tip

In case, you do not get the pop-up that prompts you to select the client certificate during authentication, try again after restarting the browser.

Configuring Single Sign-On (SSO) using SAML 2.0 for Okta

ManageEngine PAM360 offers support for SAML 2.0, which facilitates integration with Federated Identity Management Solutions for Single Sign-On. PAM360 acts as the Service Provider (SP) and it integrates with Identity Providers (IdP) using SAML 2.0. The integration basically involves supplying details about SP to IdP and vice-versa. Once you integrate PAM360 with an IdP, the users have to just login to IdP and then, they can automatically login to PAM360 from the respective identity provider's GUI without having to provide credentials again. PAM360 supports out-of-the-box integration with Okta.

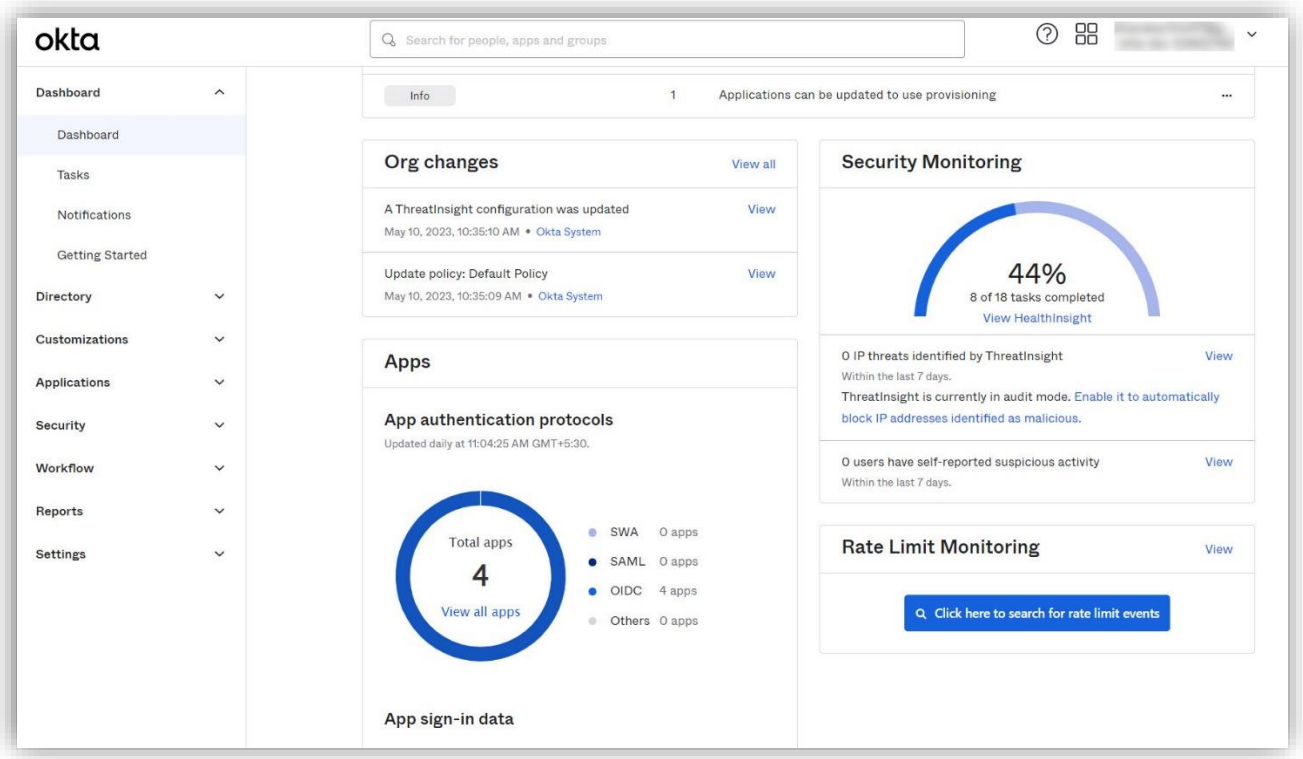
> **Note:** PAM360 allows users to configure SAML SSO for Secondary server as a service provider, which allows users to log in to PAM360 using the Secondary server when Primary is down.

Integrating PAM360 with Okta involves the following four steps:

1. **Adding PAM360 as an Application on the Okta dashboard**
2. **Configuring Okta details in PAM360**
3. **Assigning PAM360 Application to Users in Okta**
4. **Enabling SAML Sign-On in PAM360**

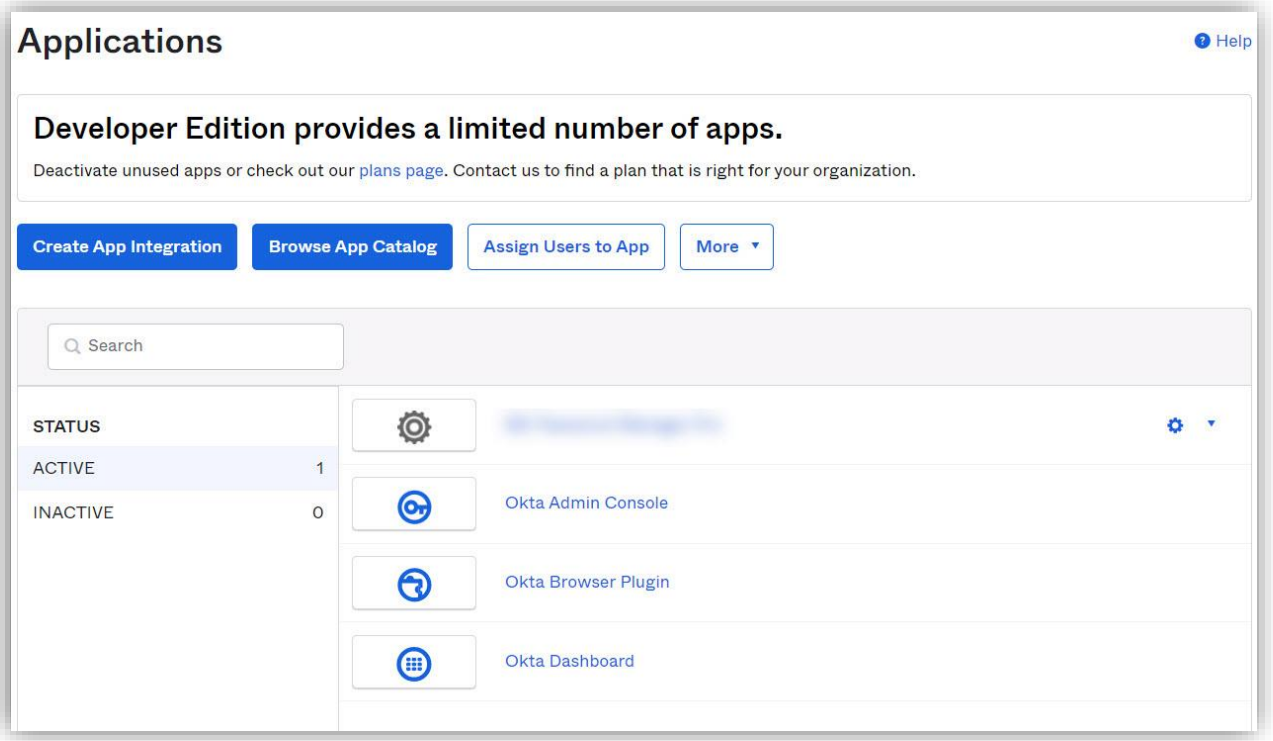
1. Adding PAM360 as an Application on the Okta Dashboard

1. Log in to your Okta Admin account and click the **Applications** tab from the left-side panel.

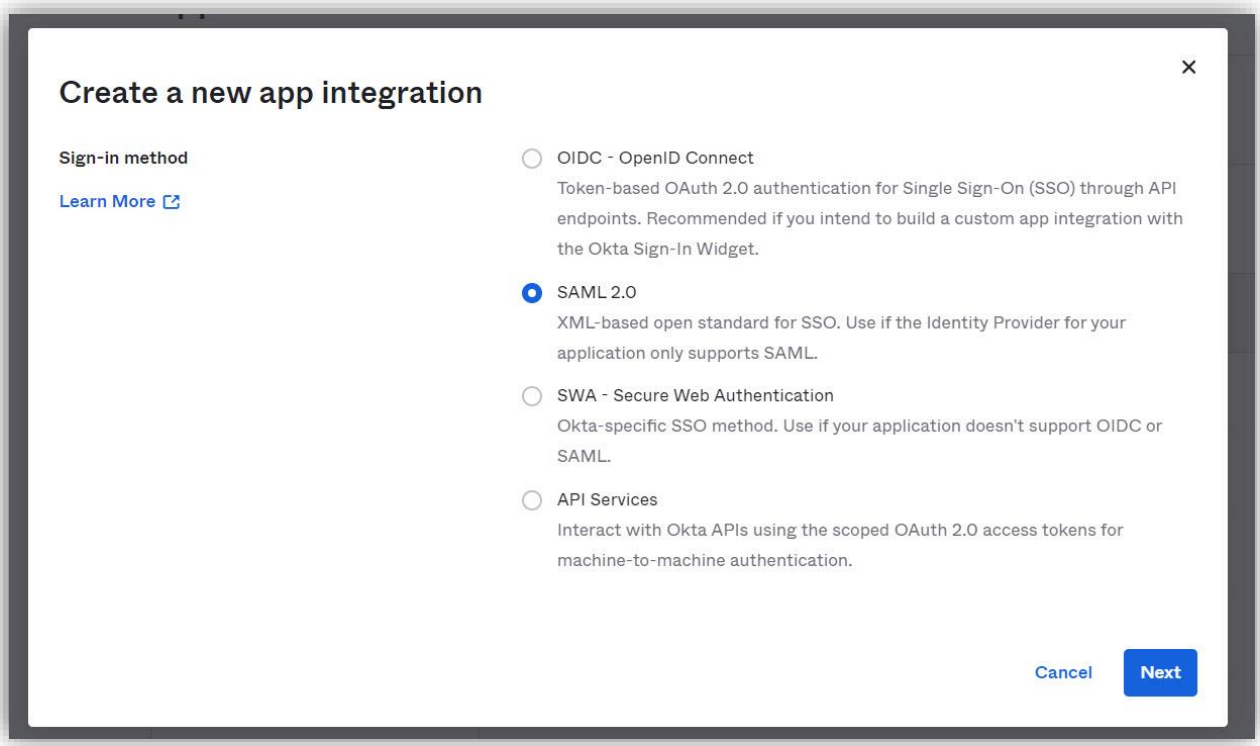


2. In the new page that opens up,

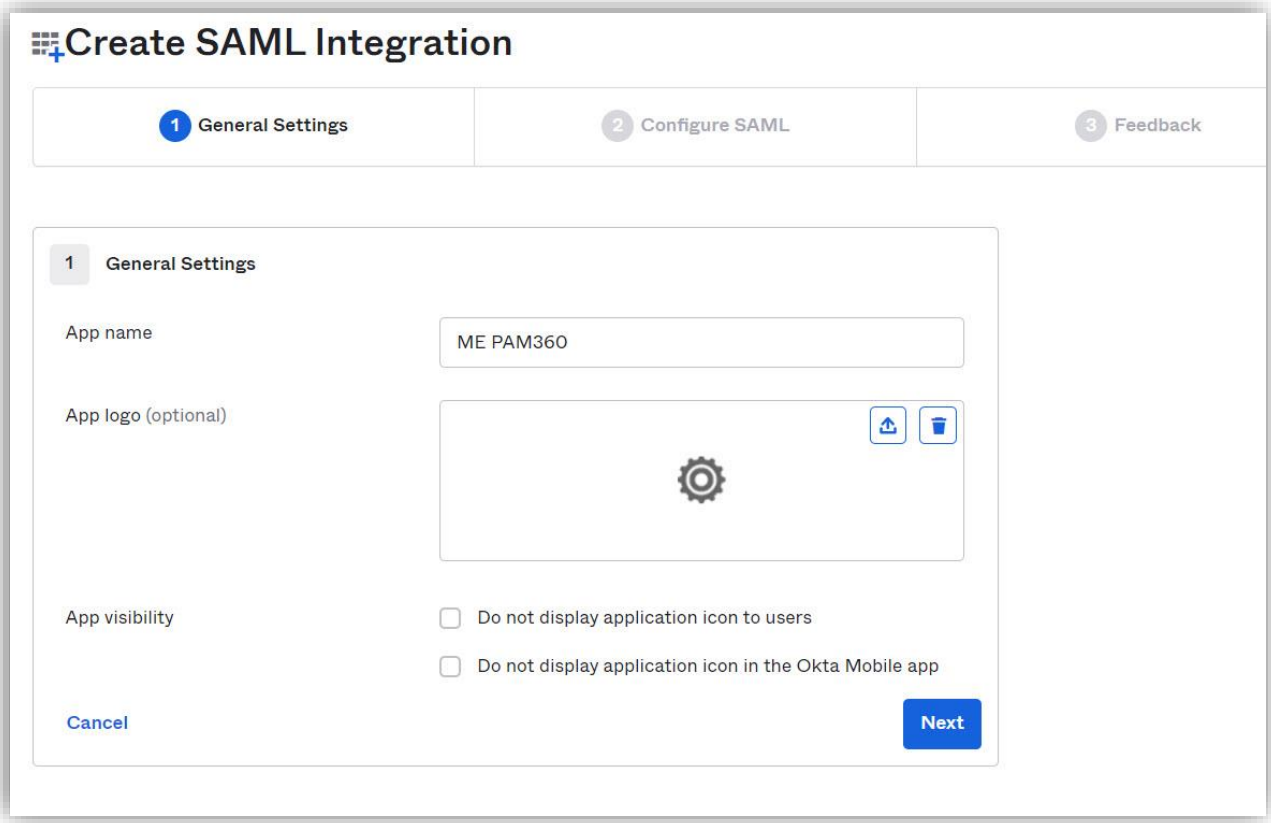
i. Click on **Create App Integration**.



ii. Immediately, a window will pop-up asking information about the type of application integration. Select **SAML 2.0** and click **Next**.

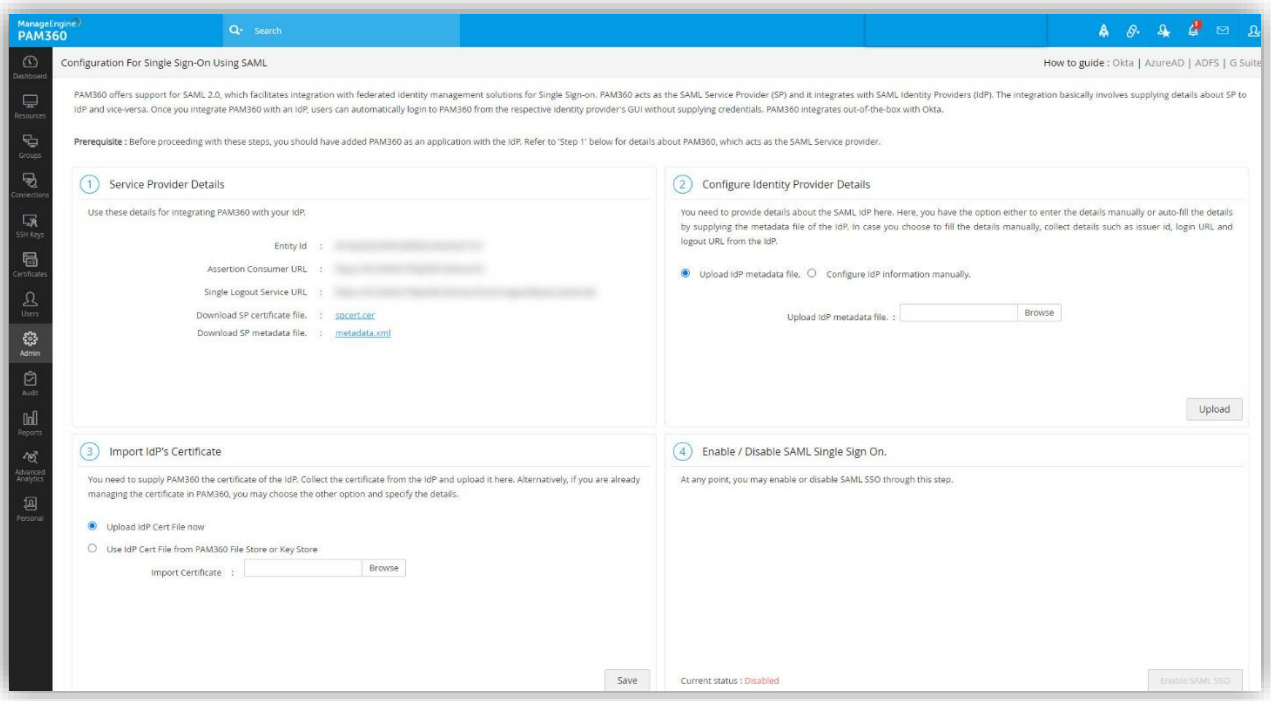


iii. Enter the name of the app being added (ME PAM360) in the **General Settings** section. You can also upload a logo for the app (optional). When you are done, click **Next**.

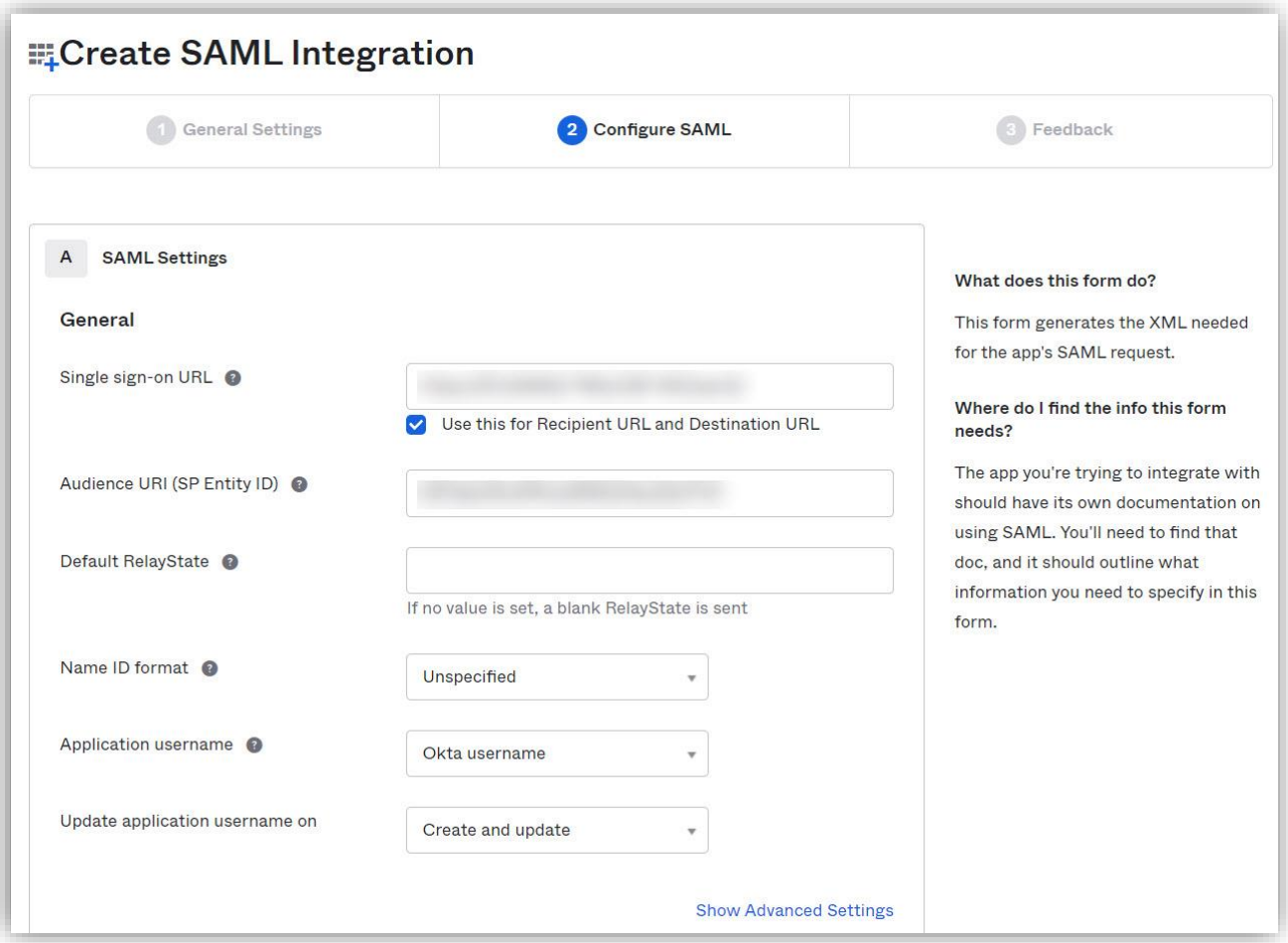


3. Configuring SAML integration consists of providing details about the Service Provider (ME PAM360) to Okta. To access these details, do the following:
   i. Navigate to **Admin >> Authentication >> SAML Single Sign-On from the PAM360 interface.**
   ii. Under **1. Service Provider Details**, you will find **Entity Id, Assertion Consumer URL** and **Single Sign On URL**; copy the values.

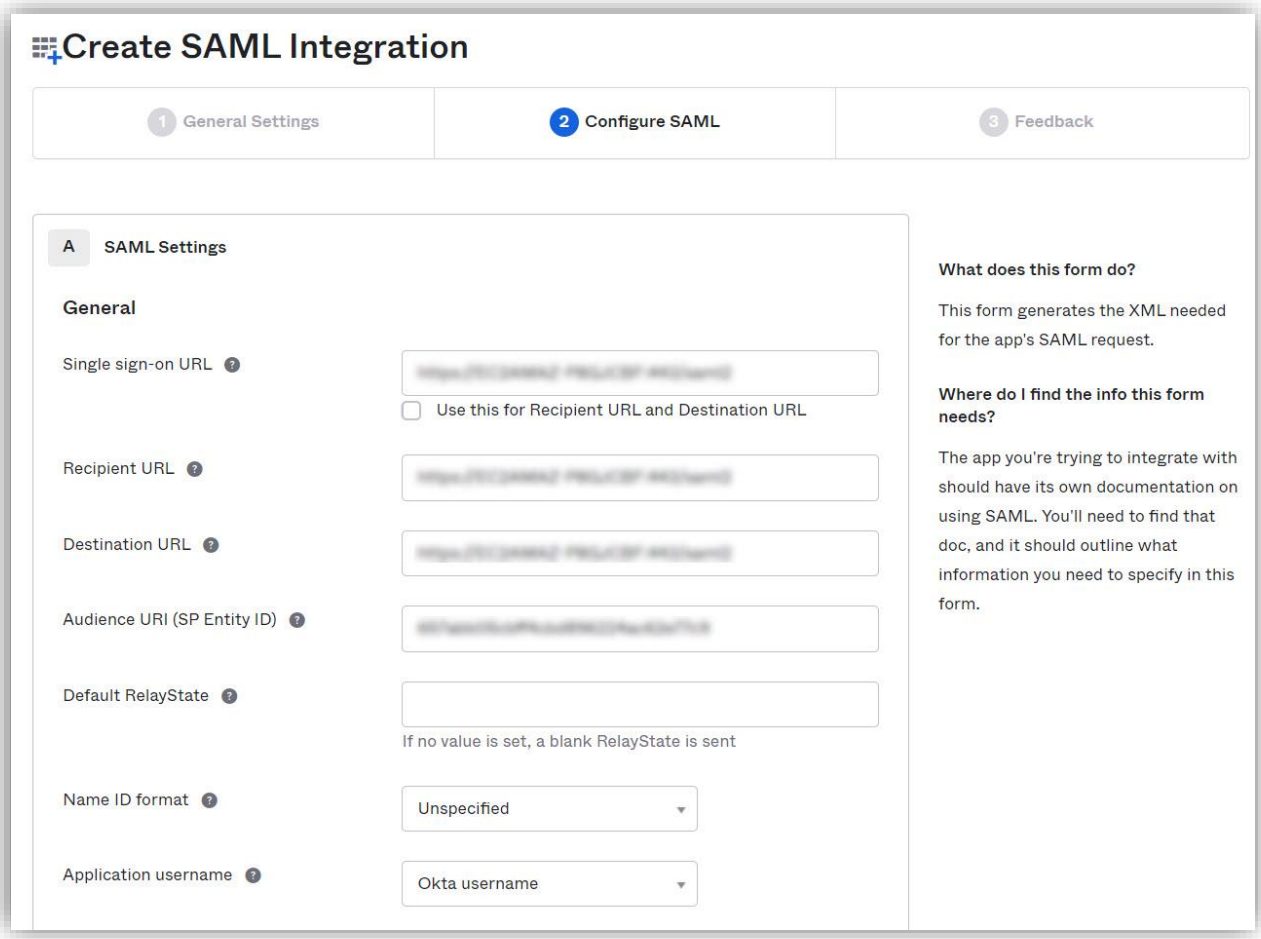
> **Note:** For SAML SSO authentication, the **Assertion Consumer URL** is the hostname of the server, by default. To update the Assertion URL, follow the below steps:
>
> 1. Navigate to **Admin >> Settings >> Mail Server Settings**.
> 2. Under **Access URL**, update the required URL and click **Save**.
>
> Now, the **Assertion Consumer URL** under **Service Provider Details** will be updated.



4. Return to the Okta's SAML Settings page.
5. For MSP, enter **Assertion Consumer URL** (copied from PAM360) in the field next to **Single sign-on URL** and select the checkbox **Use this for Recipient URL and Destination URL**.



6. For Client Organizations, enter **Single Sign On URL** (copied from PAM360) in the **Single sign-on URL** section.
   i. Deselect the **Use this for Recipient URL and Destination URL** checkbox and enter the **Assertion Consumer URL** (copied from PAM360) next to **Recipient URL** and **Destination URL.**



7. Mention the **Entity Id** in the field next to **Audience URI (SP Entity ID)**.
8. After filling-in the Single Sign On URL and SP Entity ID (Audience URI) fields, you need to specify how you want Okta to recognize the names of your users in PAM360. Since the way in which the usernames are displayed in Okta is different from how they are depicted in PAM360, you have to specify the format. There are two scenarios here:
   i. **Scenario 1:** If you have imported users from AD into PAM360, they would have been imported in the format Domain\Username. For more help on integrating Okta with your on-premise AD, please check the help documentation of Okta available here. In Okta GUI, you need to choose the option **Custom** from the dropdown **Name ID format**. Then, you should specify the custom format as given below:

```
${f:toUpperCase(f:substringBefore(f:substringAfter(user.login, "@"),
".")))}${"\\"}${f:substringBefore(user.login, "@")}
```

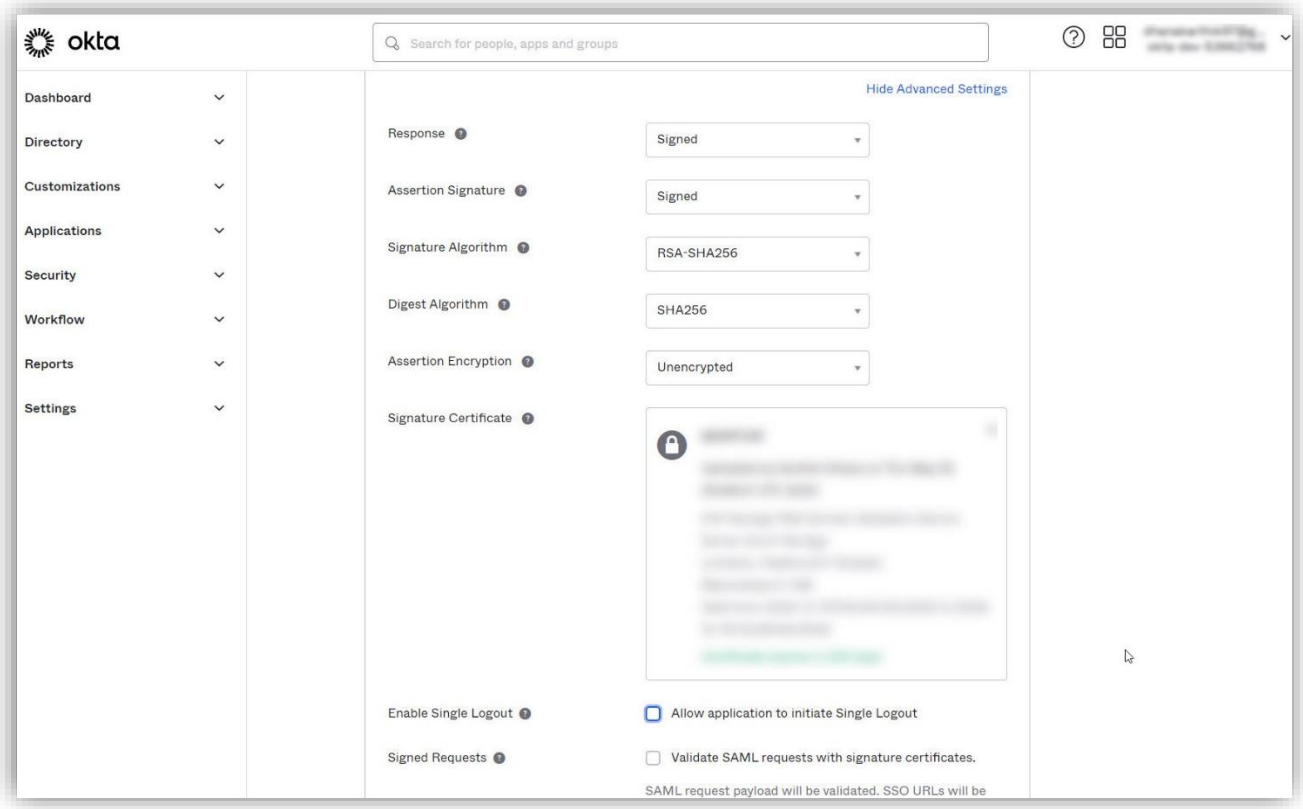
   ii. **Scenario 2:** If you have not used AD integration in PAM360, you should select the option **Okta Username Prefix**. This is because in Okta, user profiling is done in the

format username@domain.com. But, in PAM360, user names are depicted only as usernames.

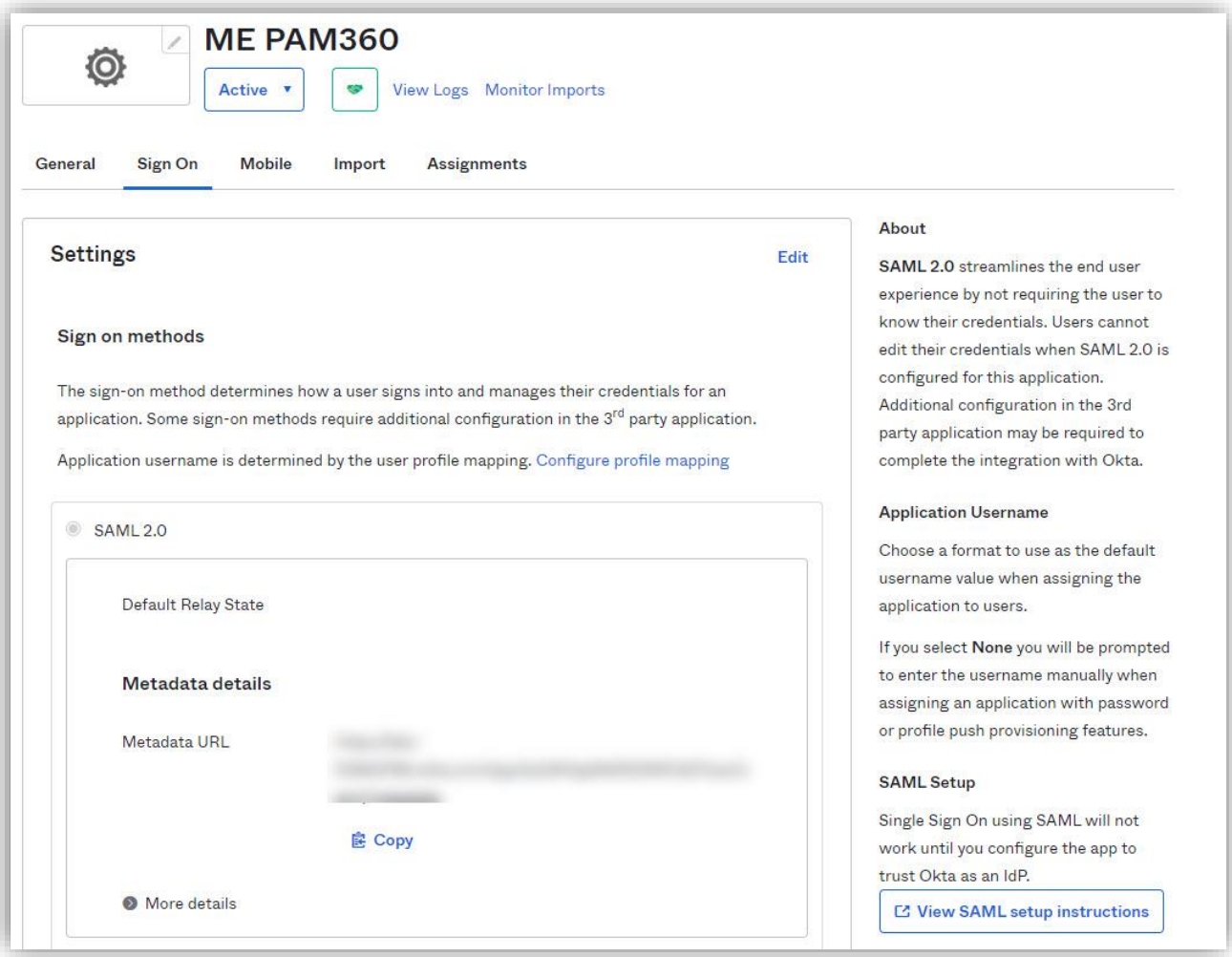
> This step is crucial because, only if you specify the correct **Name ID format** in Okta, you will be able to assign the application (PAM360) to other users in Okta.

9. To configure SAML Single Logout, click on **Show Advanced Settings.**
   i. Click the **Browse files** button next to **Signature Certificate** to upload the PAM360 certificate.
   ii. Select the checkbox **Allow application to initiate Single Logout** next to **Enable Single Logout**.
   iii. Mention the **Single Logout Service URL** (copied from PAM360) in the box next to **Single Logout URL**.
   iv. Enter the **Entity Id** (copied from PAM360) in the box next to **SP issuer**. Click **Next**.

> **Notes:**
>
> 1. SAML Single Logout is applicable from **PAM360 build 5304** and above only.
> 2. To download PAM360 certificate, navigate to **Admin >> Authentication >> SAML Single Sign-On** (Step 1) and **Download SP Certificate File.**



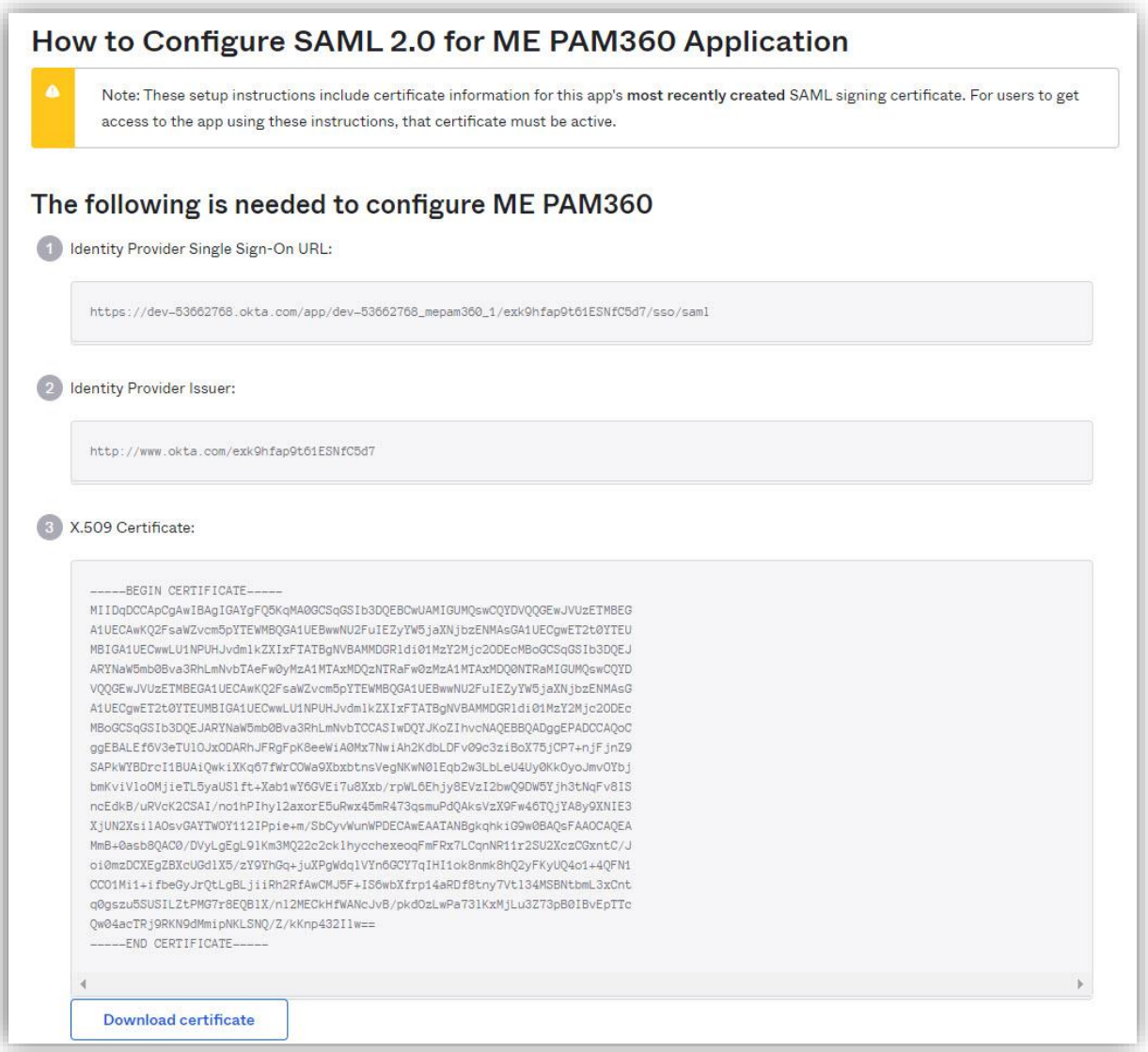
10. In the **Feedback** tab, select an option to confirm how you have configured the application and click **Finish**. Now, the application details will be displayed as shown in the image below. In the right-side pane, select **View SAML setup instructions**. A new tab will open containing the details required to configure SAML 2.0 in PAM360, which is discussed in the next step.



2. Configuring Okta Details in PAM360

You need to configure IdP details in PAM360. This is done as part of the second step, **Configure Identity Provider Details** in PAM360's SAML Single Sign On page. Here, you have the option either to enter the details manually or auto-fill the same by supplying the metadata file from the IdP.

1. **Manual Set-up:** If you choose to fill the details manually, get the IdP details such as Issuer ID, Login URL, and Logout URL from the **Setup Instructions** page of Okta. Configure the same in the step 2 given in PAM360 SAML Sign On configuration page. Enter the details in the corresponding fields and also download the Okta certificate and upload onto the PAM360 client (Listed as the 3rd step in the PAM360 GUI). Alternatively, you can also save the certificate file in the PAM360 File Store or Key Store and then use it here.



How to Configure SAML 2.0 for ME PAM360 Application

Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure ME PAM360

1 Identity Provider Single Sign-On URL:

```
https://dev-53662768.okta.com/app/dev-53662768_mepam360_1/exk9hfap9t61ESNfC5d7/sso/saml
```

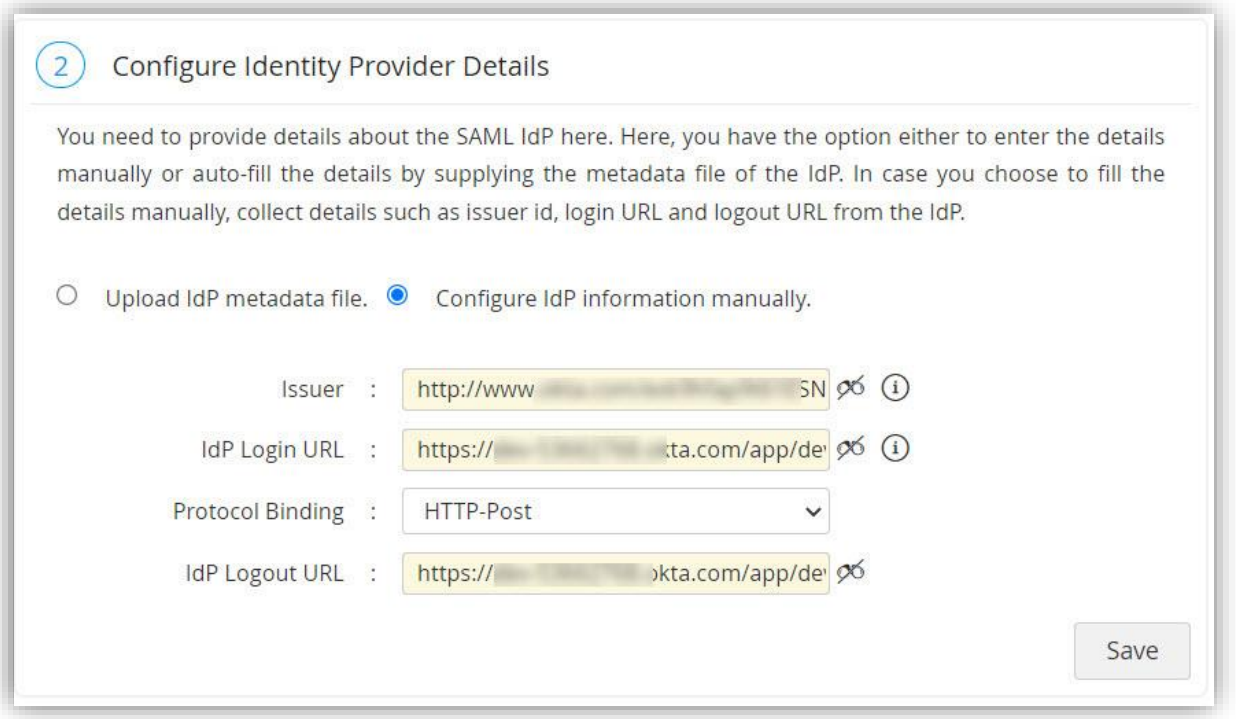
2 Identity Provider Issuer:

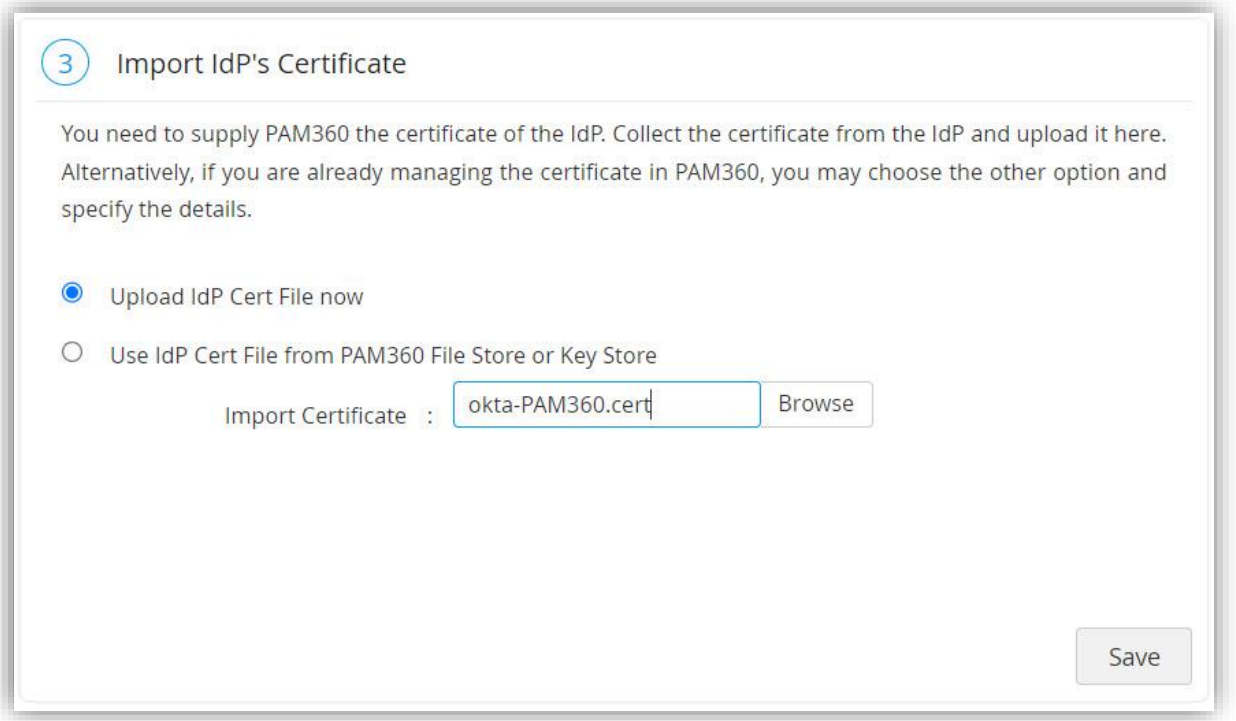
```
http://www.okta.com/exk9hfap9t61ESNfC5d7
```

3 X.509 Certificate:

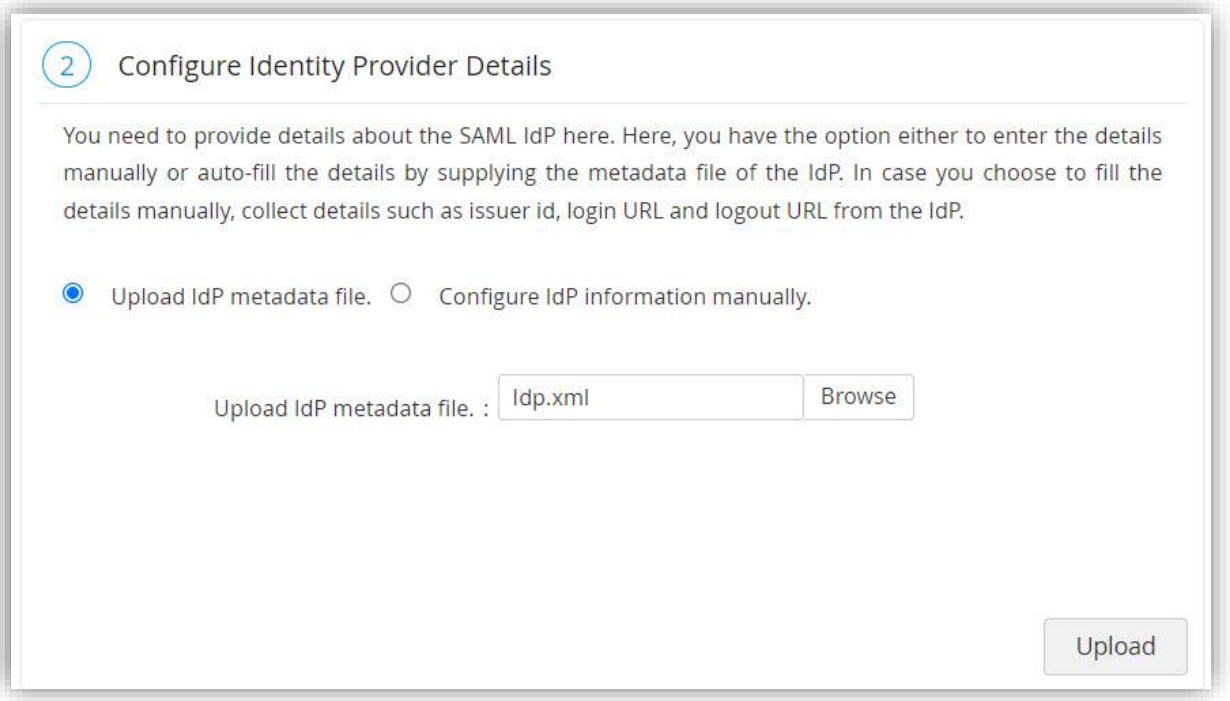
```
-----BEGIN CERTIFICATE-----
MIIDqDCCApCgAwIBAgIGAYgFQ5KqMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi01MzY2Mjc2ODEcMBoGCSqGSIb3DQEJ
ARYNaW5mb0Bva3RhLmNvbTAeFw0yMzA1MTAxMDQzNTRaFw0zMzA1MTAxMDQ0NTRaMIGUMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGRldi01MzY2Mjc2ODEc
MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALEf6V3eTUlOJxODARhJFRgFpK8eeWiA0Mx7NwiAh2KdbLDFv09c3ziBoX75jCP7+njFjnZ9
SAPkWYBDrcI1BUAiQwkiXKq67fWrCOWa9XbxbtnsVegNKwN0lEqb2w3LbLeU4Uy0KkOyoJmvOYbj
bmKviVloOMjieTL5yaUS1ft+Xab1wY6GVEi7u8Xxb/rpWL6Ehjy8EVzI2bwQ9DW5Yjh3tNqFv8IS
ncEdkB/uRVcK2CSAI/no1hPIhyl2axorE5uRwx45mR473qsmuPdQAksVzX9Fw46TQjYA8y9XNIE3
XjUN2XsilAOsvGAYTWOY112IPpie+m/SbCyvWunWPDECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
MmB+0asb8QAC0/DVyLgEgL9lKm3MQ22c2ck1hycchexeoqFmFRx7LCqnNR11r2SU2XczCGxntC/J
oi0mzDCXEgZBXcUGd1X5/zY9YhGq+juXPgWdqlVYn6GCY7qIHI1ok8nmk8hQ2yFKyUQ4o1+4QFN1
CCO1Mi1+ifbeGyJrQtLgBLjiiRh2RfAwCMJ5F+IS6wbXfrp14aRDf8tny7Vtl34MSBNtbmL3xCnt
q0gszu5SUSILZtPMG7r8EQBlX/nl2MECkHfWANcJvB/pkdOzLwPa73lKxMjLu3Z73pB0IBvEpTTc
Qw04acTRj9RKN9dMmipNKLSNQ/Z/kKnp432Ilw==
-----END CERTIFICATE-----
```

Download certificate





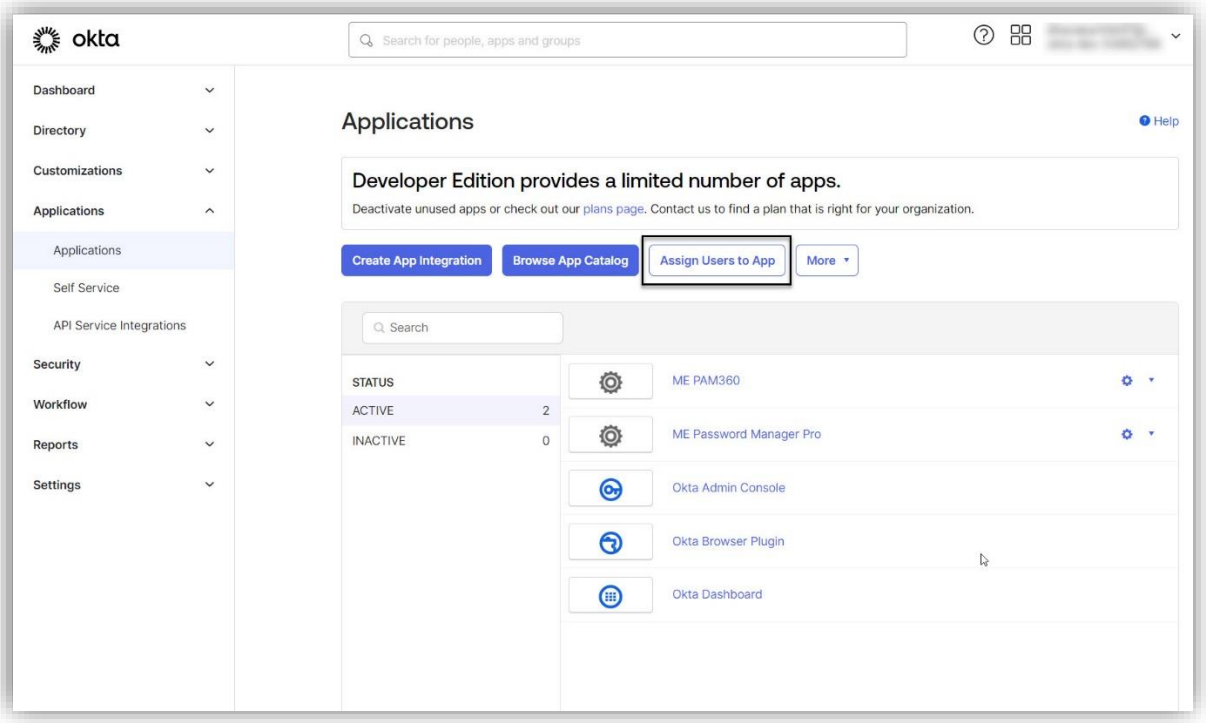
2. **Auto-Filling with IdP Metadata File:** Scroll down on the SAML 2.0 setup instructions page of Okta and you will find the IdP metadata under **Optional**. Copy the text and save in a file with .xml extension. Now, upload the same .xml file onto the PAM360 client. In this case, you needn't import IdP certificate in PAM360. It will be updated automatically.



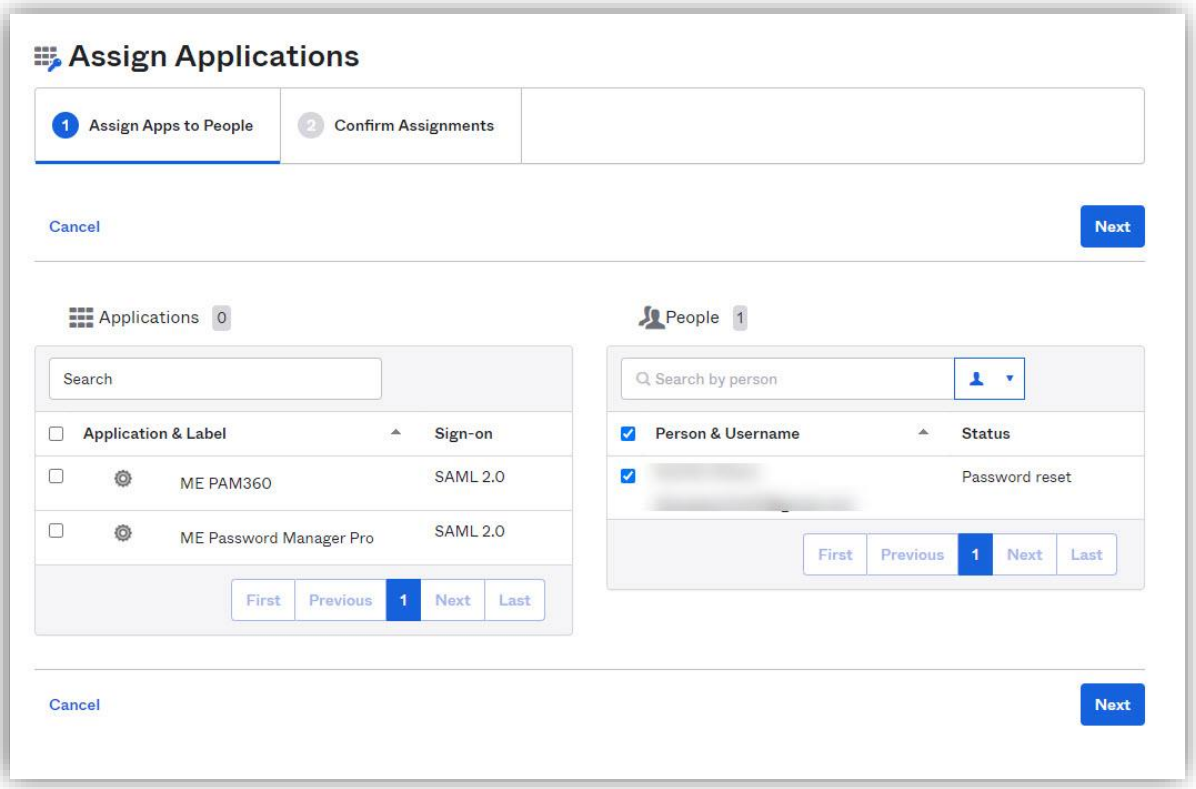
3. Assigning PAM360 Application to Users in Okta

After completing the configurations in PAM360, return to the Okta portal to assign the newly added application to your users. To do so:

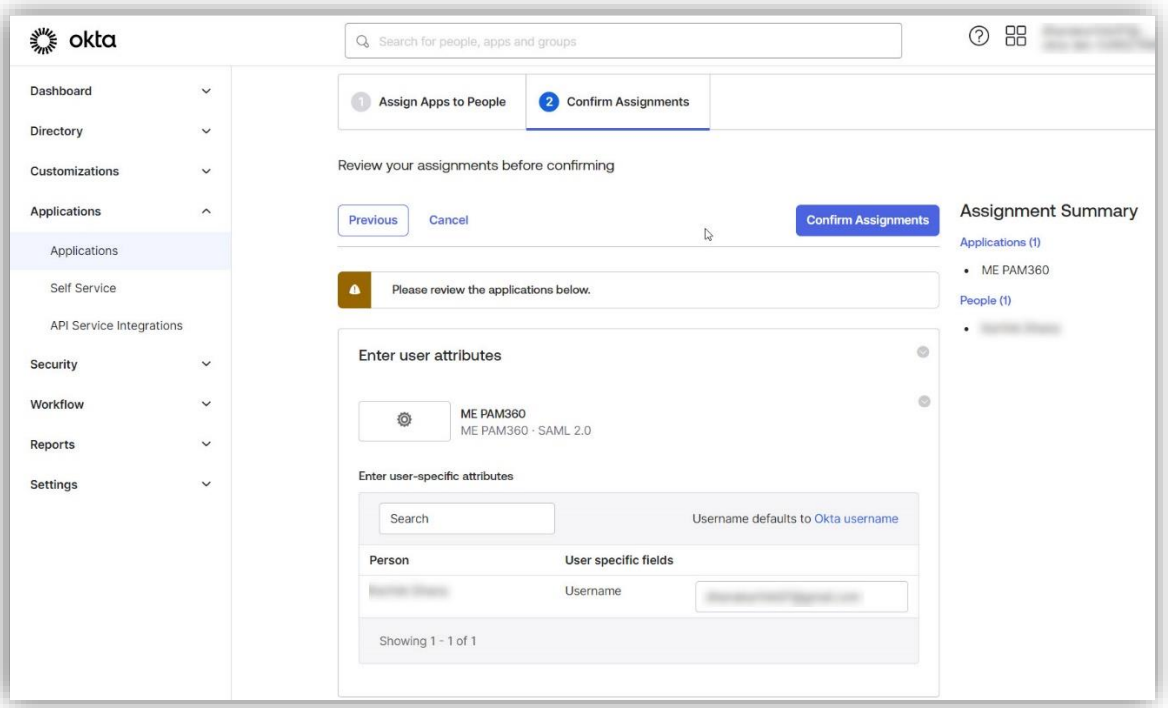
1. Click the **Applications** tab from the left-side panel and select **Assign Users to App**.



2. In the **Assign Apps to People** tab, select **ME PAM360** from the **Applications** section and pick the desired user name from the **People** section.



3. Click **Next**. Review the applications and click the **Confirm Assignments** button.



4. Enabling SAML Sign-On in PAM360

The final step of this configuration is enabling SAML Single Sign On in PAM360. This would be shown as the 4th step in the SAML page in PAM360 GUI. Click **Enable Now** shown at the bottom right to begin using this feature.

Note: In case Active Directory authentication is enabled for PAM360 login, SAML SSO cannot be enabled. To disable AD authentication, go to **Admin >> Active Directory**.



Configuring SAML Single Sign-On (SSO) for Azure AD Users

You can set up SAML single sign-on (SSO) in PAM360 for Azure AD users. This document also details steps to enable multi-factor authentication (MFA) in the Microsoft Azure portal.

> **Note:** PAM360 allows users to configure SAML SSO for Secondary server as a service provider, which allows users to log in to PAM360 using the Secondary server when Primary is down.

Prerequisite

Before setting up SAML SSO, follow the steps provided here to import Azure AD users into PAM360.

Steps to Configure SAML SSO for Azure AD Users

1. Adding an Enterprise Application in the Azure Portal
2. Assigning Azure Users to the Enterprise Application
3. Configuring SAML SSO with PAM360

Steps to Enable MFA and Set up First Login for Azure AD Users

> **Note:** Enabling MFA for Azure AD users in the Microsoft Azure portal is optional and is independent of the SAML SSO configuration.

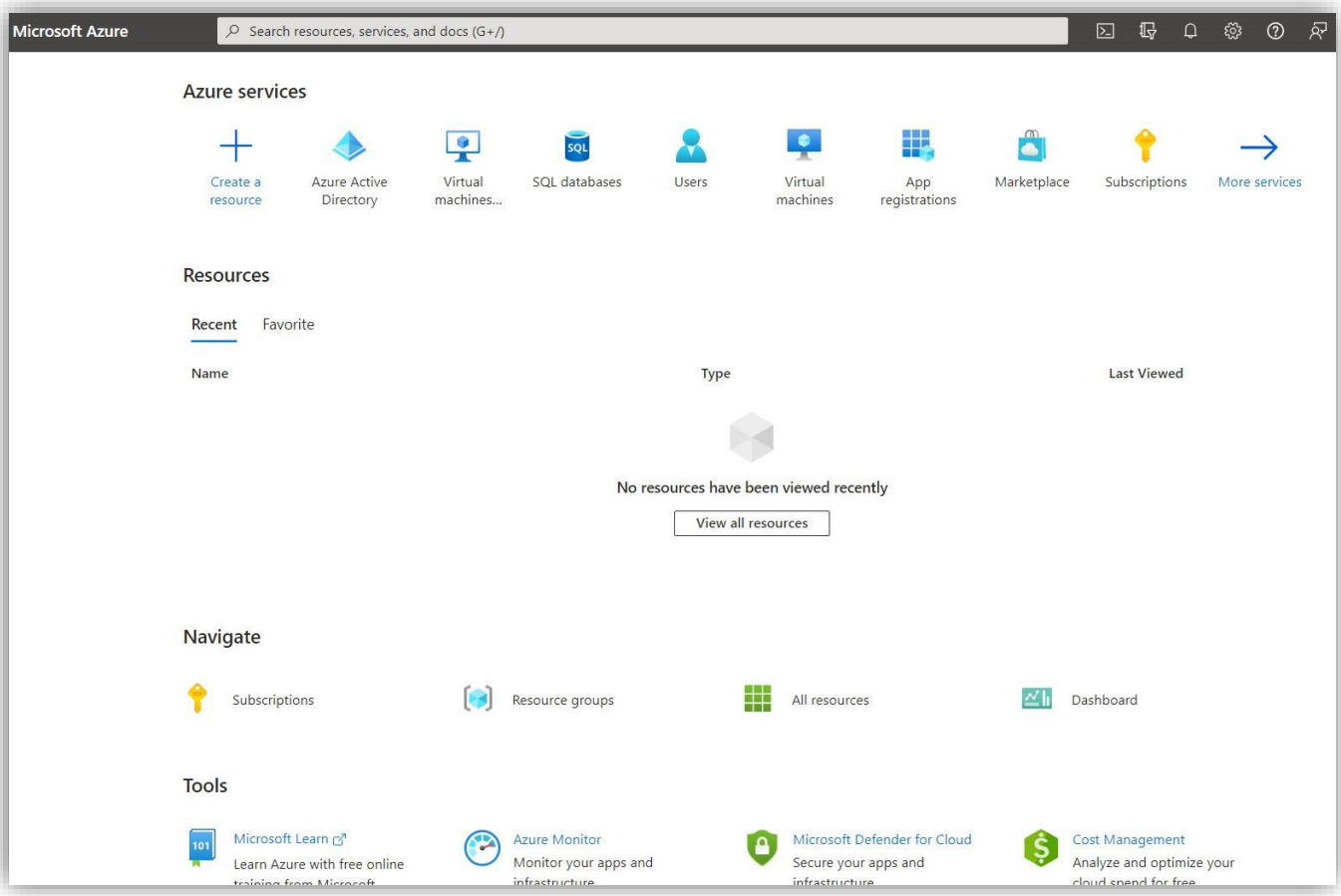
1. Enabling Multi-Factor Authentication for Azure Users
2. Assigning Azure Users to the Enterprise Application
3. Setting up the First Login for the MFA-Enabled Azure Users

Steps to Configure SAML SSO for Azure AD Users

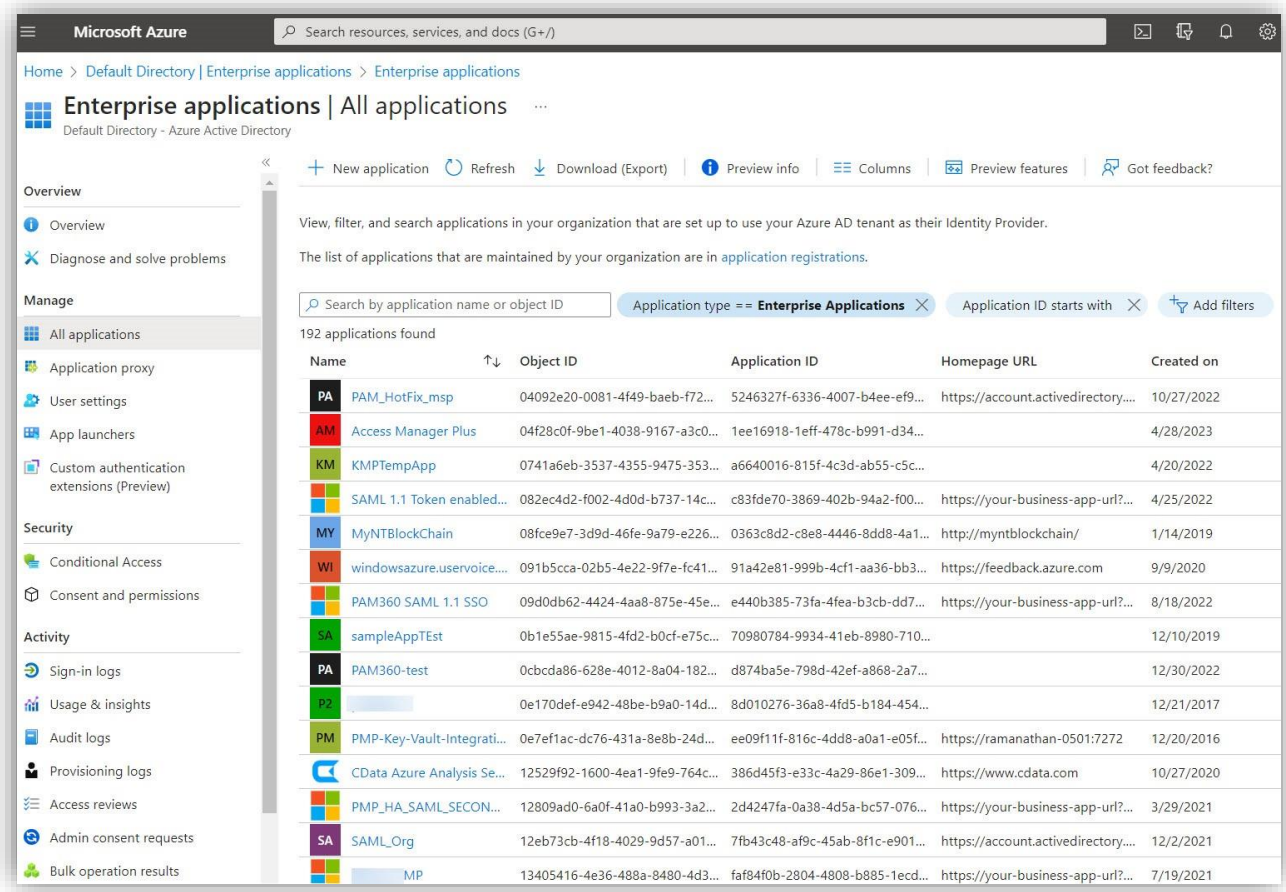
Detailed below are the steps to configure SAML SSO in PAM360 for Azure AD users in the Microsoft Azure portal.

1. Adding an Enterprise Application in the Azure Portal

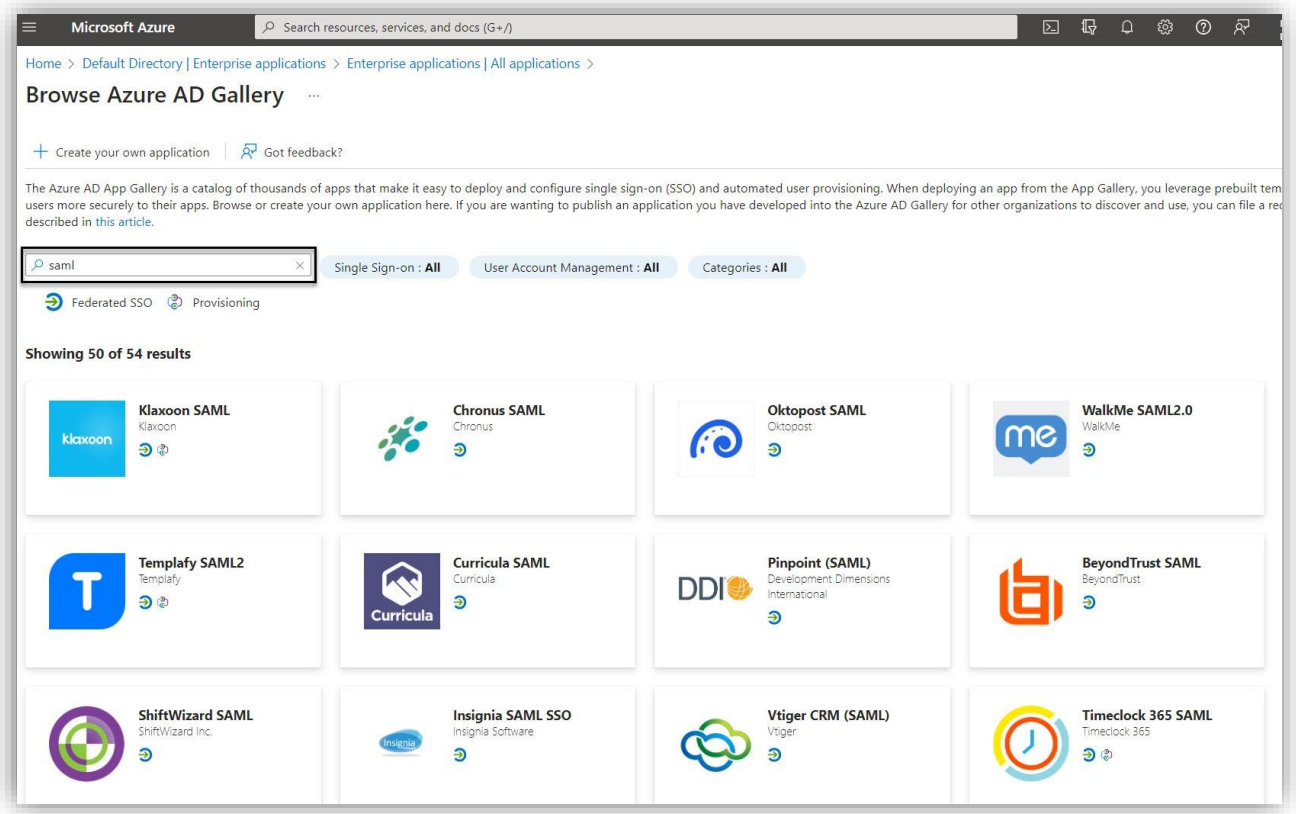
1. Log in to the Microsoft Azure portal through the URL https://portal.azure.com.



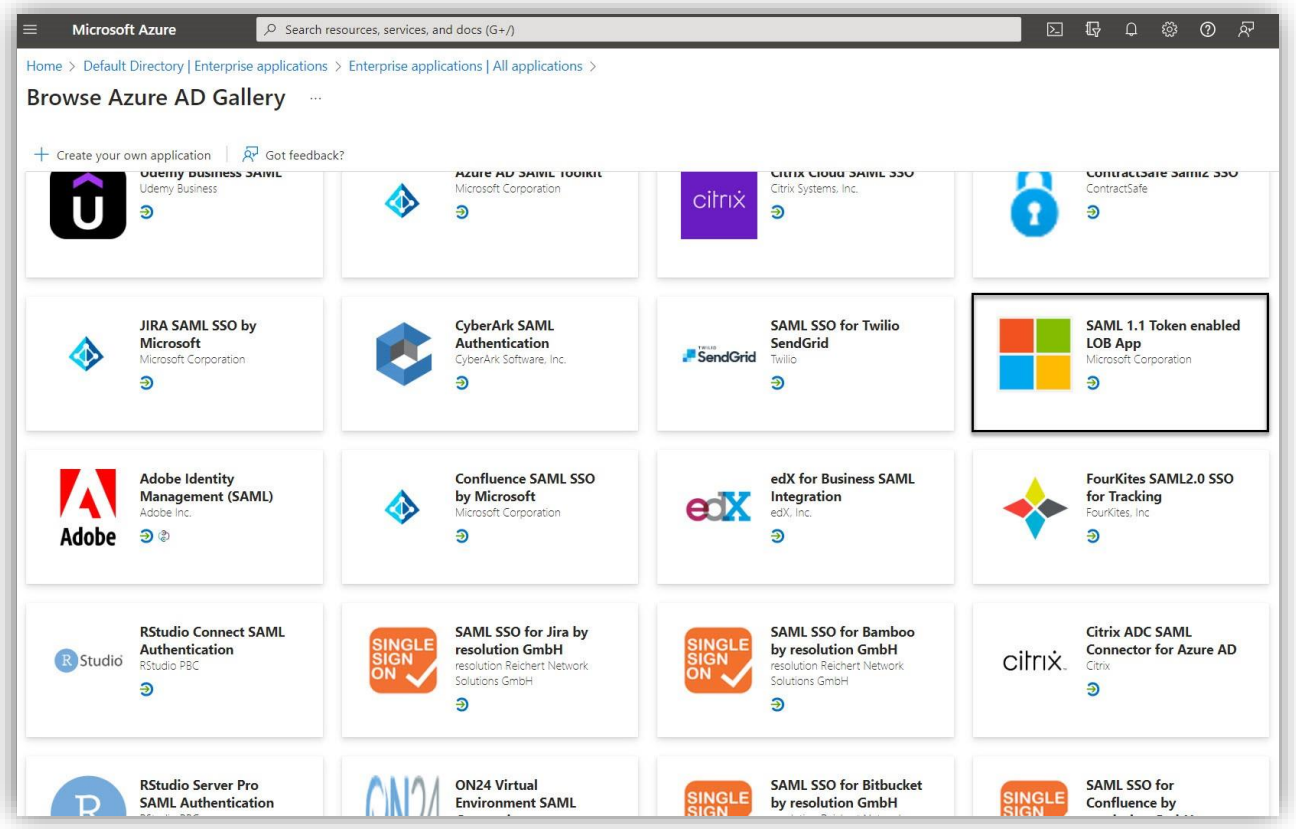
2. Click **Azure Active Directory** below Azure services. Under the **Manage** tab, select **Enterprise Applications.**
3. Click **New Application** available at the top of the **Enterprise applications** page.



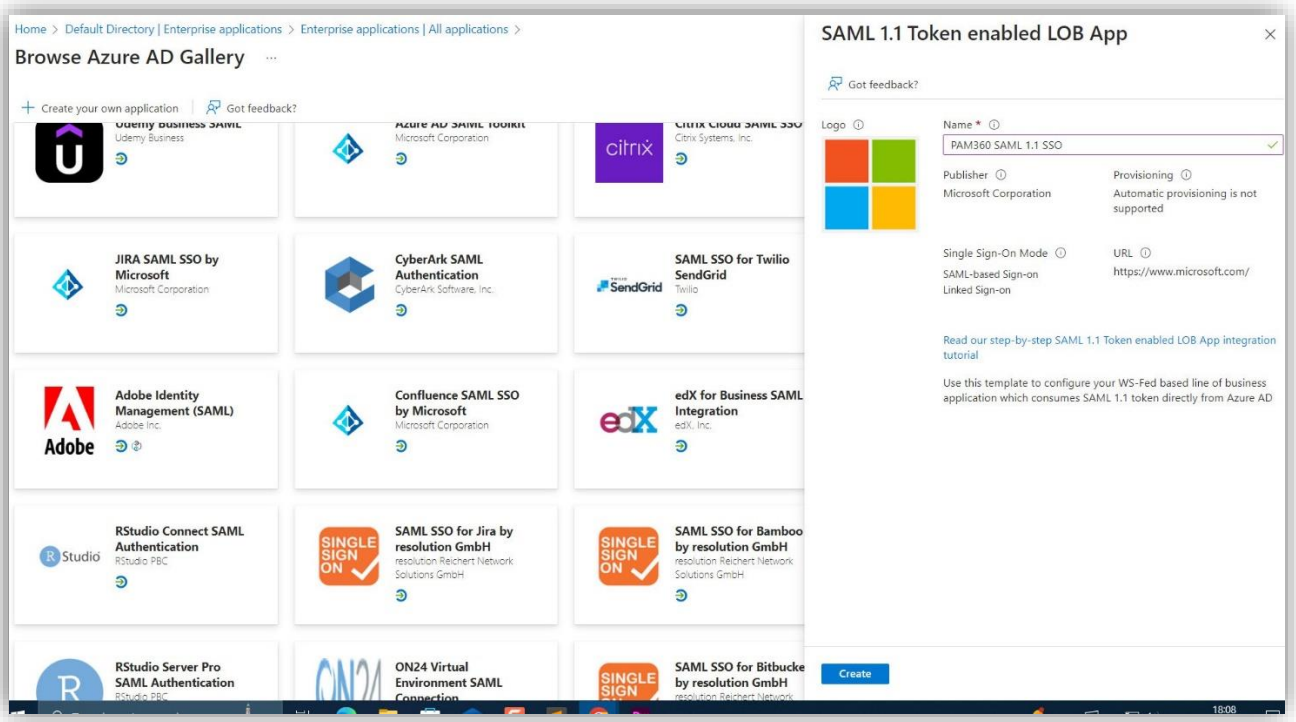
4. You will be taken to the **All Applications** page from which you can choose and add your desired applications. In the search bar, type "SAML" and press Enter.



5. From the search results, click on **SAML 1.1 Token enabled LOB App**. The application will open in a minimized window on the right pane.



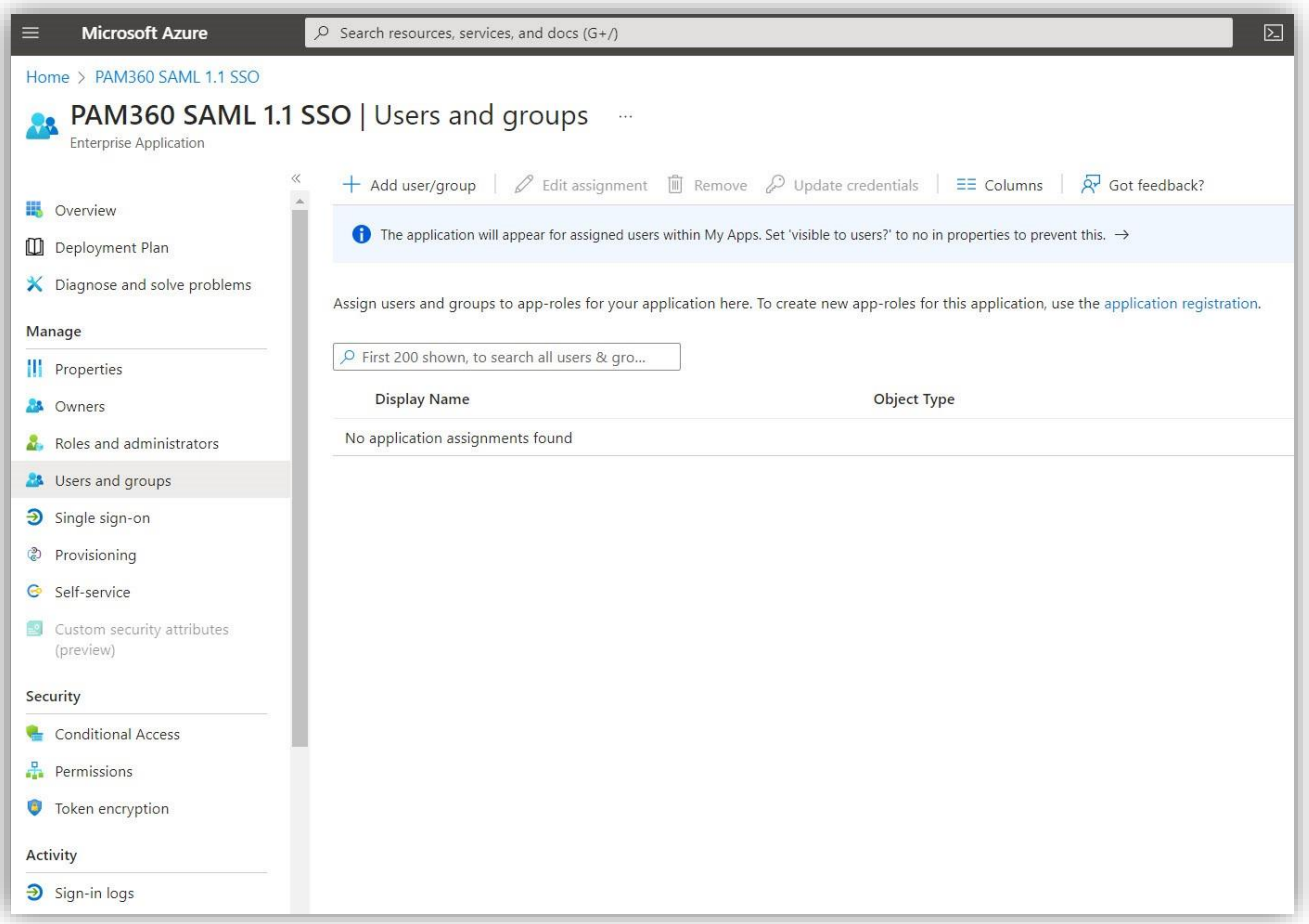
6. Edit the name as **PAM360 SAML 1.1 SSO** and click **Create**.



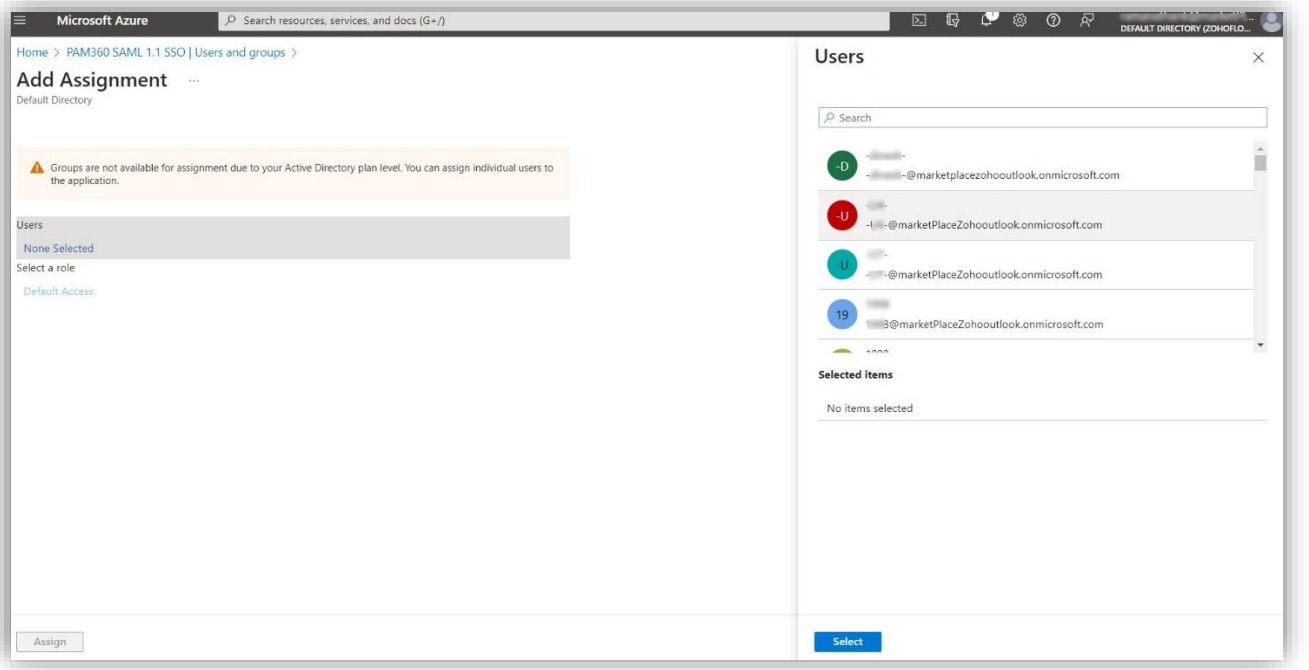
7. **PAM360 SAML 1.1 SSO** will be added as the **Enterprise Application** successfully.

2. Assigning Azure Users to the Enterprise Application

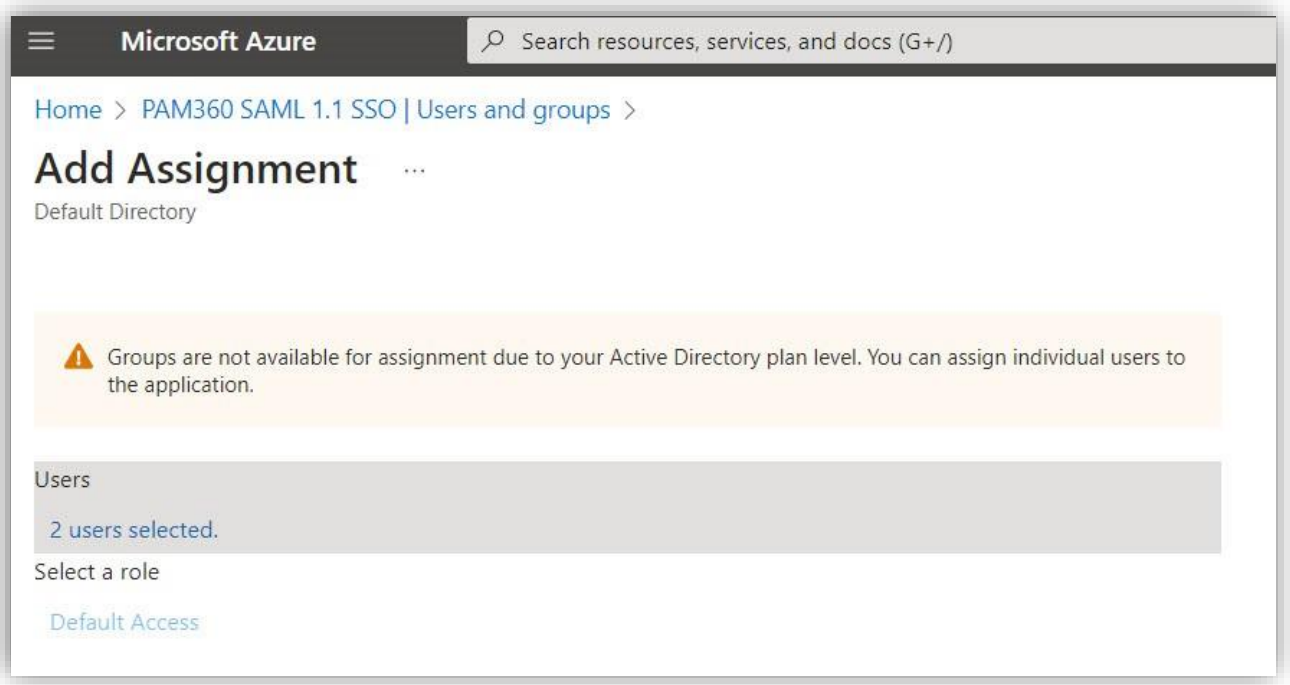
1. Under **Manage** on the left pane, select **Users and groups** and click **Add user/group** at the top.



2. In the **Add Assignment** pane, click on **None Selected** to open up a list of users. Select the required users and then click the **Select** button.

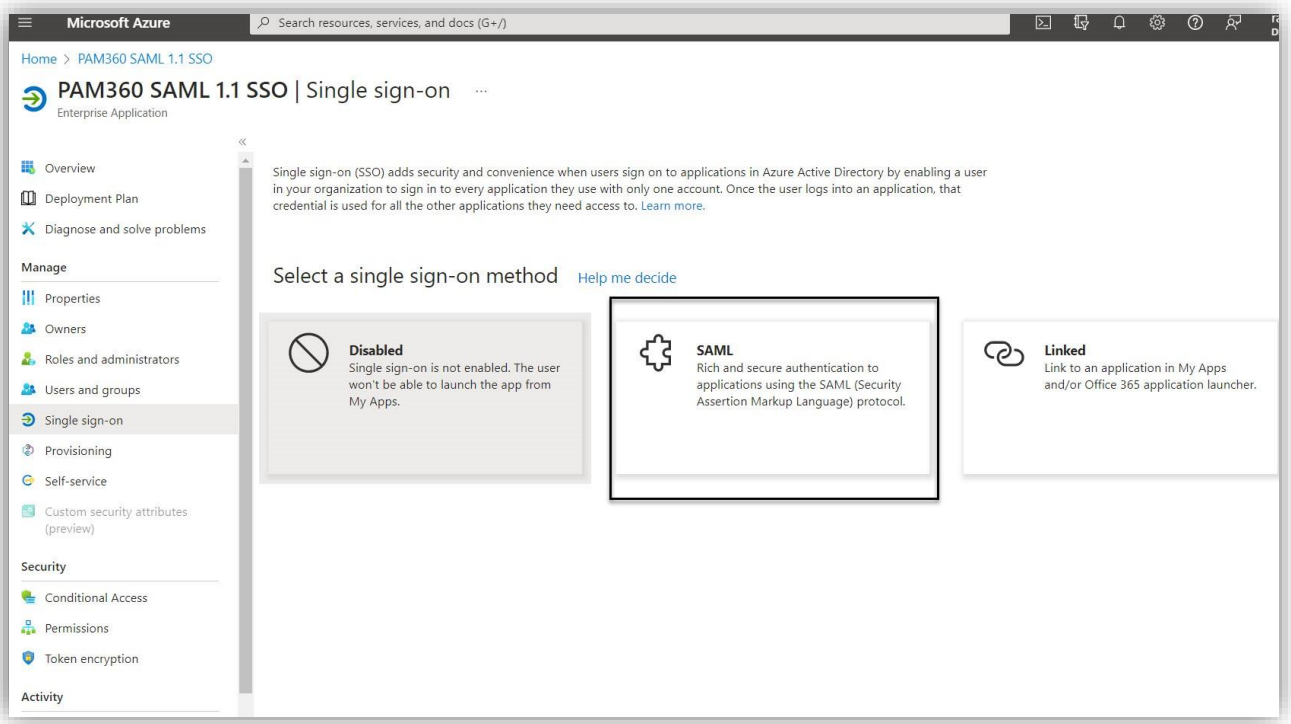


3. After the required users have been selected, click **Assign** to assign them to the enterprise application.

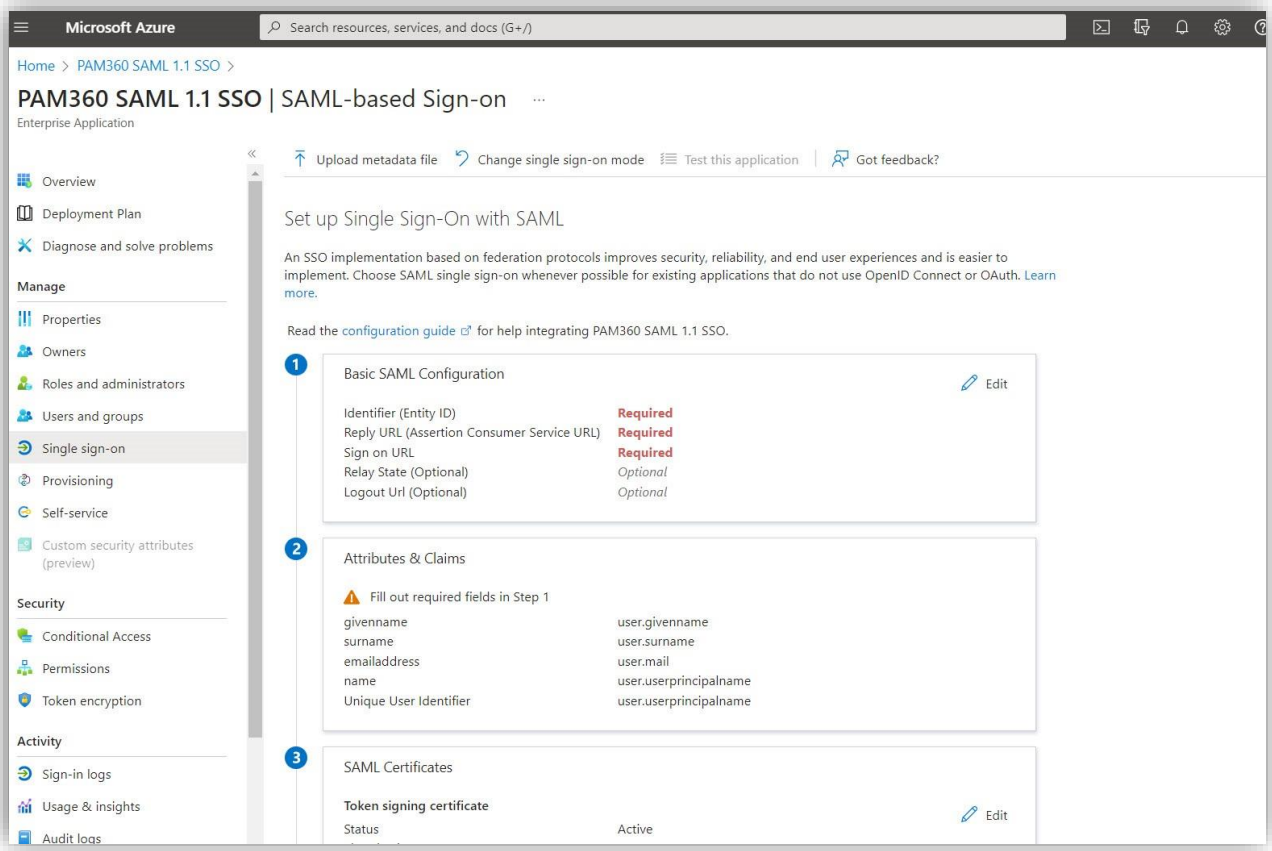


3. Configuring SAML SSO with PAM360

1. Under the **Manage** tab on the left pane, click on **Single sign-on**. In the **Select a single sign-on method** section, select **SAML**.



2. To set up single sign-on with SAML, you need to provide basic SAML configuration details here such as **Identifier (Entity ID)** and **Sign on URL**.



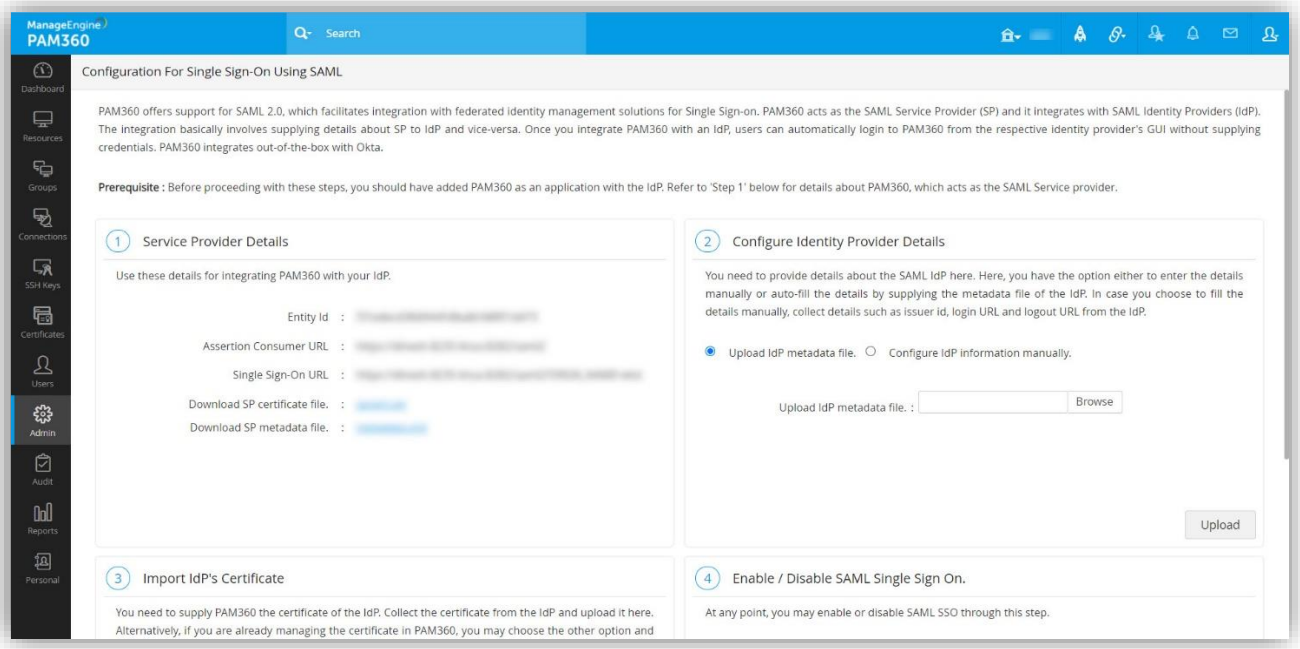
3. You can get the Entity ID and Sign on URL from the PAM360 interface.
   i. Once you have logged in to PAM360, navigate to **Admin >> Authentication >> SAML Single Sign On.**
   ii. Under **1. Service Provider Details**, you will find **Entity Id** and **Assertion Consumer URL**; copy both the values.

Notes:

By default, the **Assertion Consumer URL** is the hostname of the server. To update this, follow the below steps:

1. Navigate to **Admin >> Settings >> Mail Server Settings.**
2. Under **Access URL**, update the required URL and click Save.

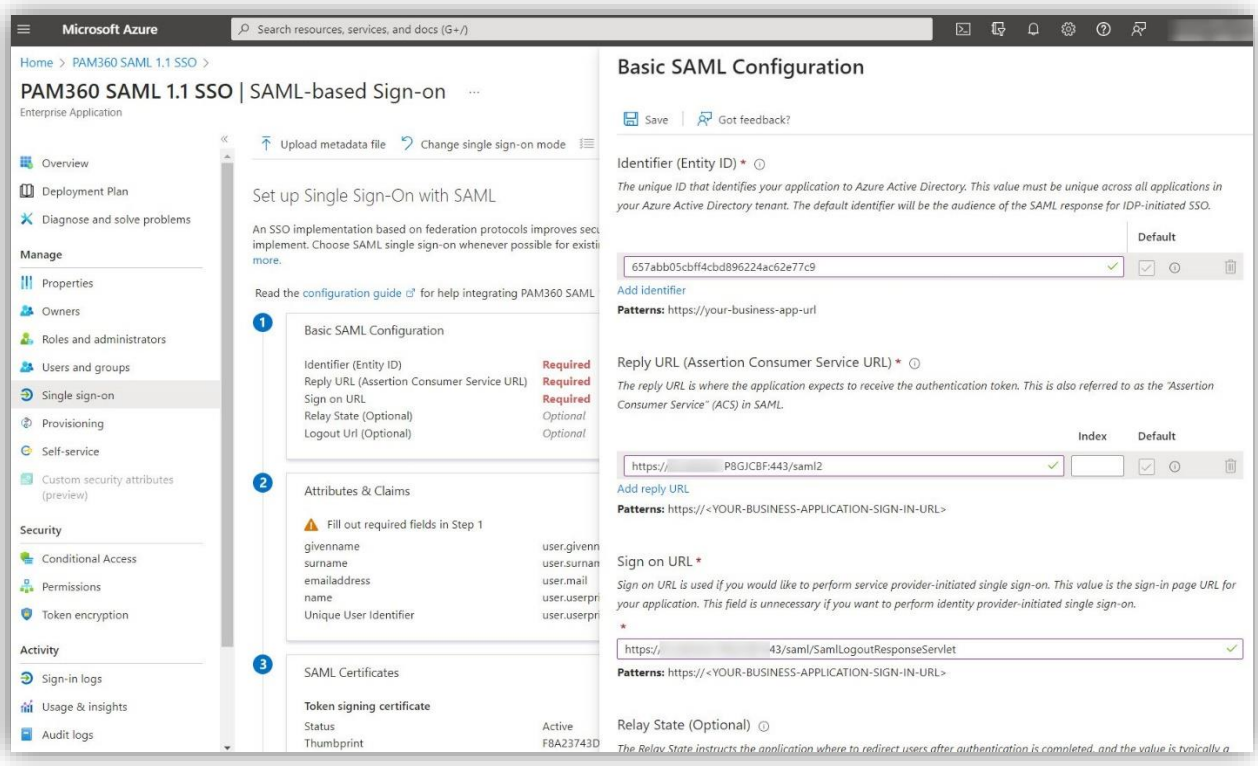
Now, the **Assertion Consumer URL** under **Service Provider Details** will be updated.



4. Go back to the Azure portal, click the edit icon to edit the **Basic SAML Configuration** details:
   i. For Non-MSP, enter the **Entity Id** (copied from PAM360) under **Identifier (Entity ID).** Enter your **PAM360 web interface URL** under the **Sign on URL** (eg. https://<Host-Name-of-PAM360-Server OR IP address>:<Port>) and provide the **Assertion Consumer Service URL** under **Reply URL.**

ii. For MSP Client Organizations, enter the **Entity Id** (copied from PAM360) under **Identifier (Entity ID)**. Enter the **Assertion Consumer URL** under the **Reply URL (Assertion Consumer Service URL)** and enter the **Org URL** (eg. https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/<Org_name>) under **Sign on URL.**

iii. Click **Save.**



5. To configure SAML Single Logout,

i. Mention **Single Logout Service URL** (copied from PAM360) in the field next to **Logout URL.**

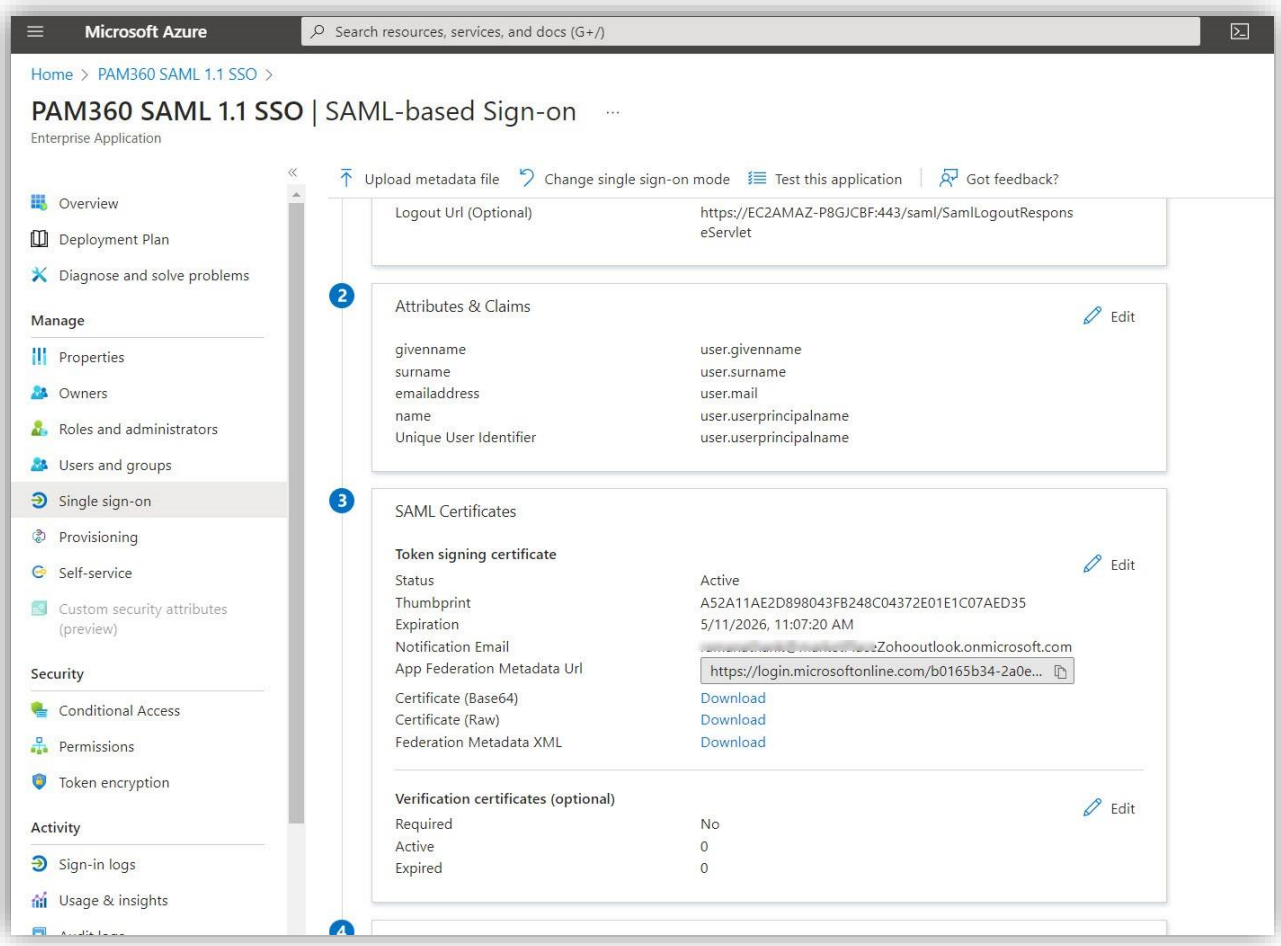
ii. Navigate to **<PAM360_Installation_Directory\PAM360\conf\system_properties.conf>** and append the following system property under the existing properties.

- **saml.logout.redirect.slo=true**

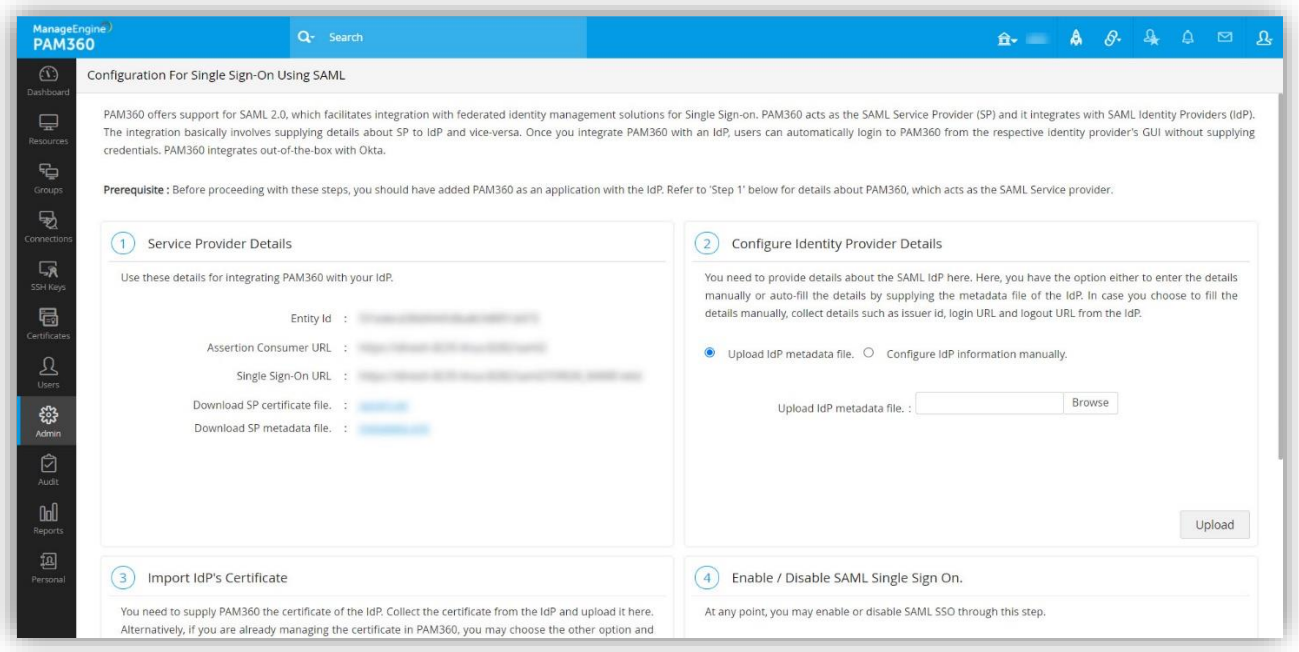
> **Note:** SAML Single Logout is applicable from **PAM360 build 5304** and above only.

6. Now the SAML configuration details taken from PAM360 will be saved in the Azure portal.

7. In the SAML configuration settings window, scroll down and go to the **SAML Certificates** section and download the XML file named **Federation Metadata XML.**



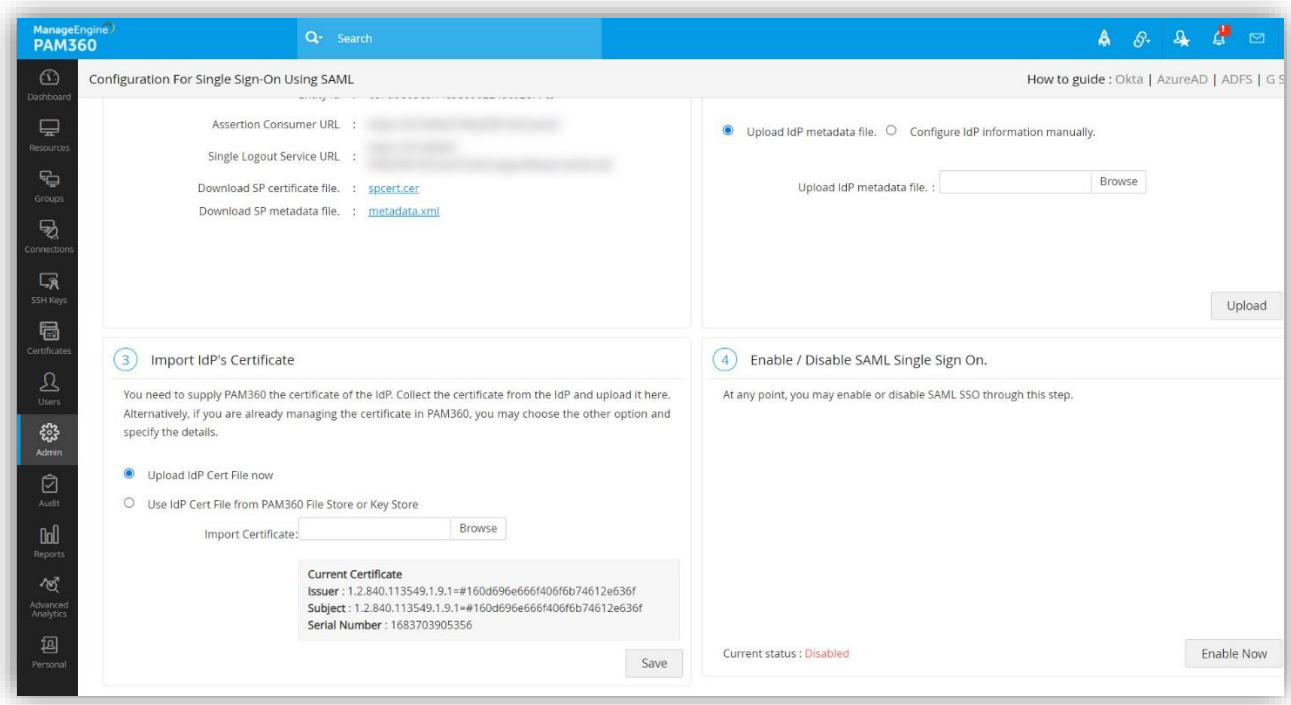
8. Return to the PAM360 interface and navigate to **Admin >> Authentication >> SAML Single Sign-On.**
9. Under **2. Configure Identity Provider Details**, select **Upload IdP metadata file** and click **Browse** to select the downloaded **Federation Metadata XML** file. Click **Upload** to save the Azure SAML SSO settings in PAM360.



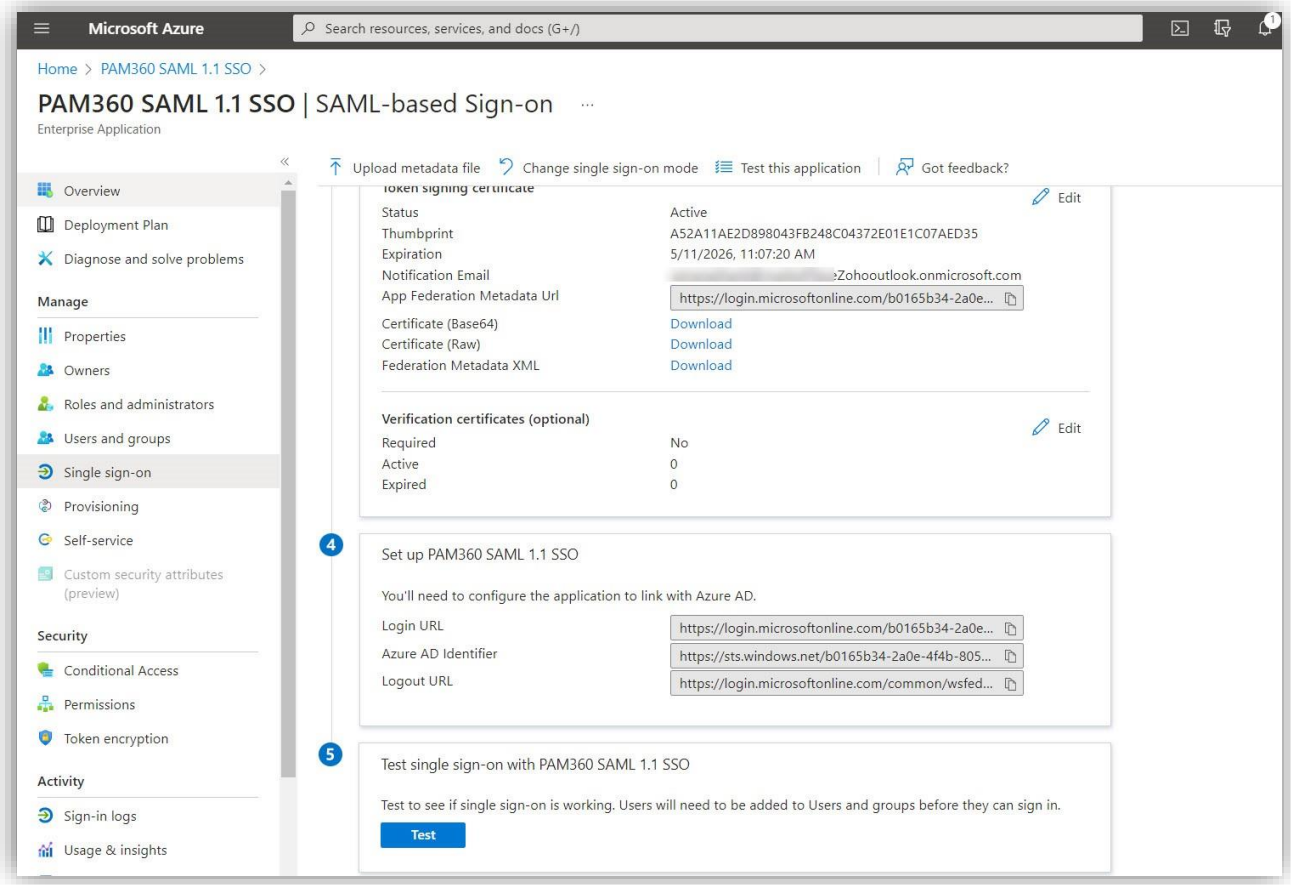
10. Refresh the current page in PAM360. Now, under **3. Import IdP's Certificate**, you will see the **Current Certificate** details such as **Issuer**, **Subject**, and **Serial Number**. Click **Save**.
11. For Azure SAML to function properly, go to path: **<PAM360_Installation_Directory\PAM360\conf\system_properties.conf>** and verify if the below-mentioned system properties are available in the conf file. If not, append them below the existing properties.

```
saml.redirect.idpprotocolbindingpost=true
saml.authcontext.comparison.exact=true
saml.AuthreqForceAuthn=false
saml.nameidFormat=unspecified
saml.idp.version=1.1
saml.authnContextClassRef=Password
```

12. Once the properties are added, restart the PAM360 server for the changes to take effect.
13. Finally, under **4. Enable/Disable SAML Single Sign On**, click **Enable Now** to activate the SAML SSO.



14. To validate if the single sign-on works, go to the Azure portal, click **Test** under **Test single sign on with PAM360 SAML 1.1 SSO**.

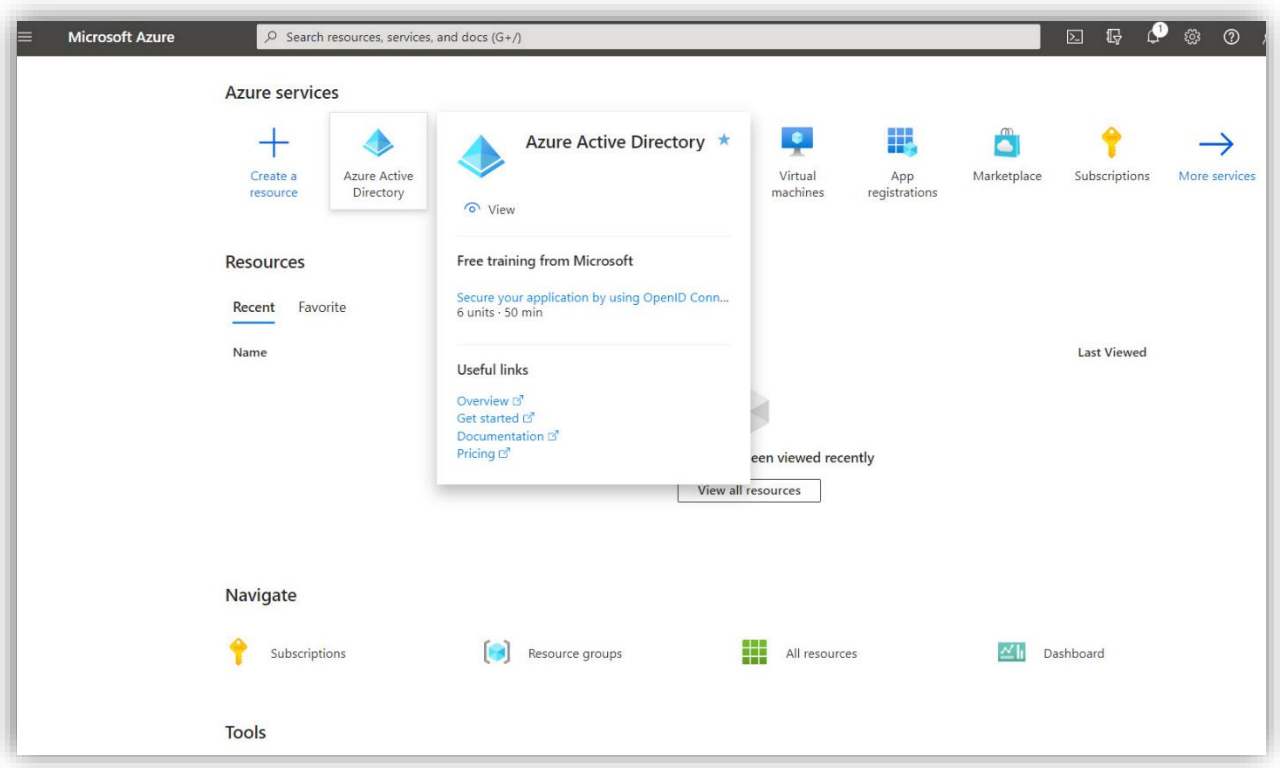


Steps to Enable MFA and Set up First Login for Azure AD Users

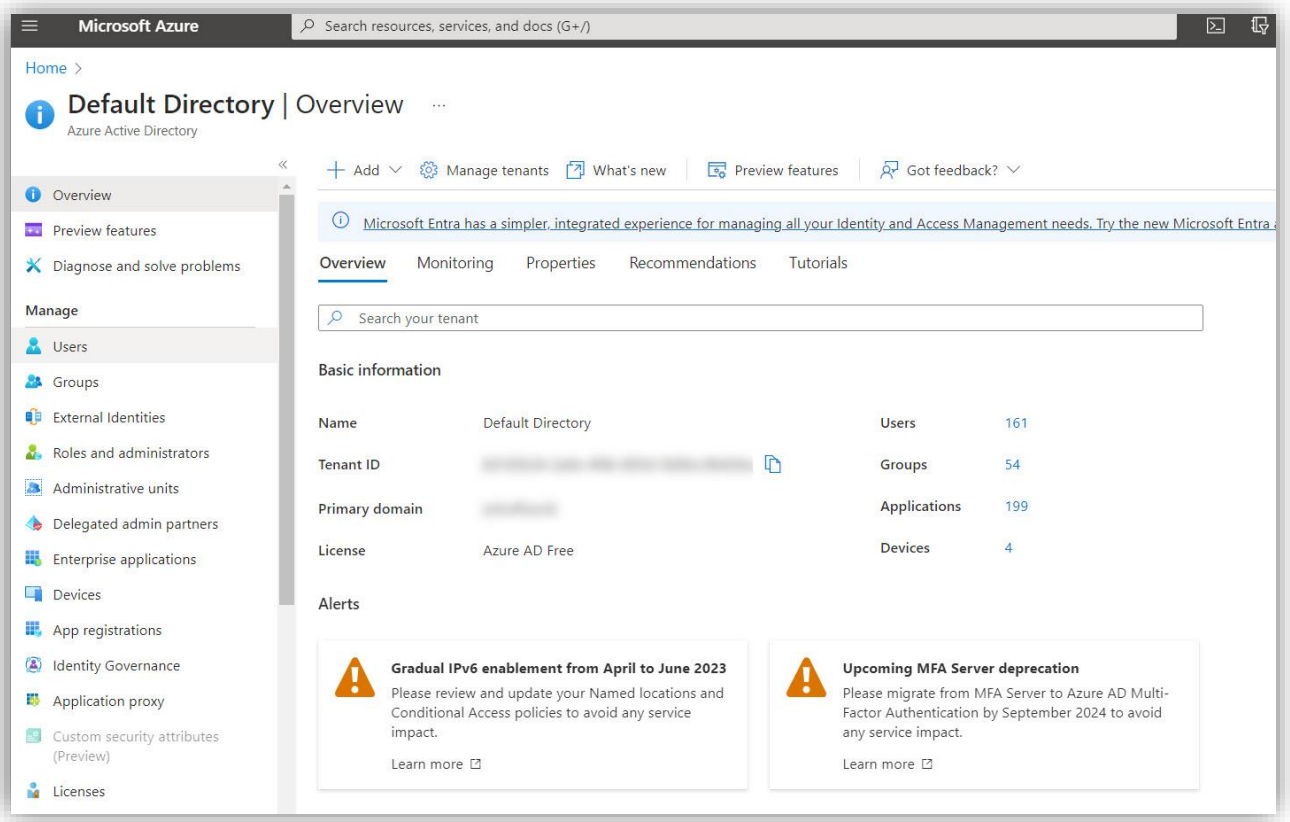
Below are detailed steps to activate MFA for Azure AD users in the Microsoft portal and to set up their first login.

1. Enabling Multi-Factor Authentication for Azure AD Users

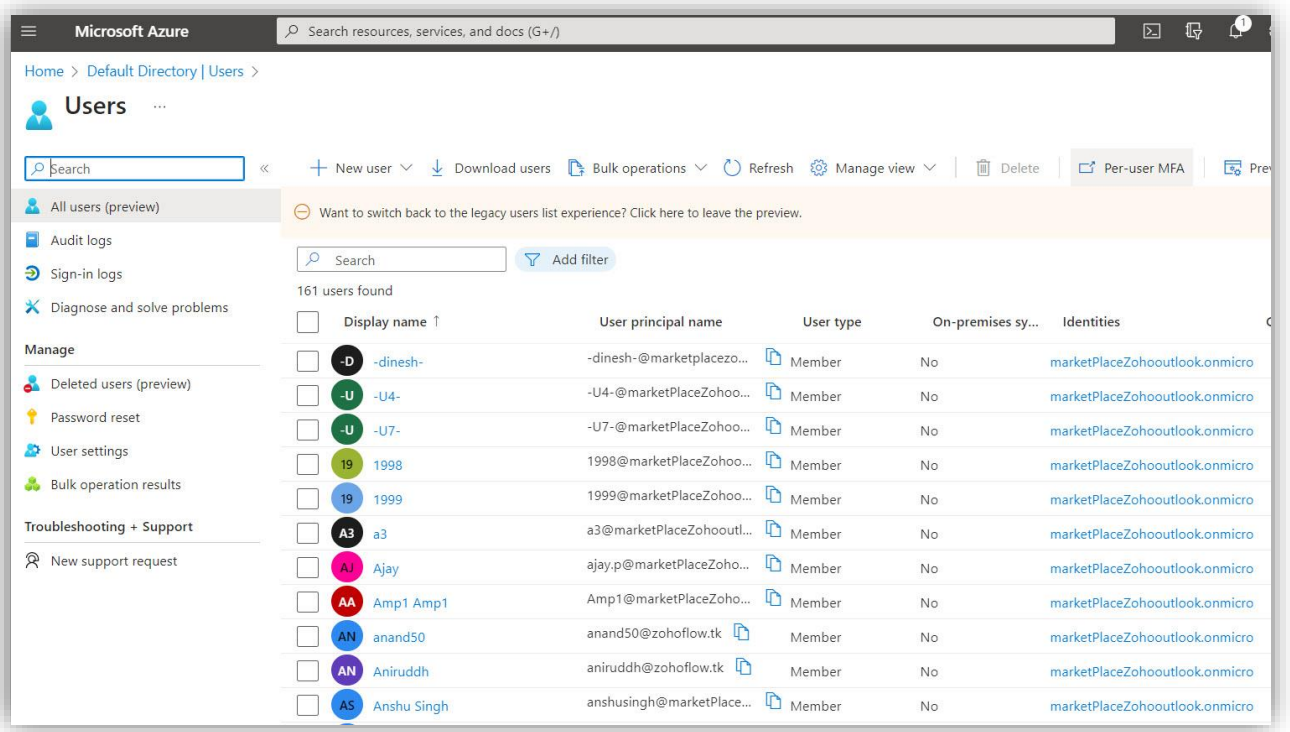
1. Log in to the Microsoft Azure portal through the URL https://portal.azure.com.
2. Select **Azure Active Directory** under Azure services.



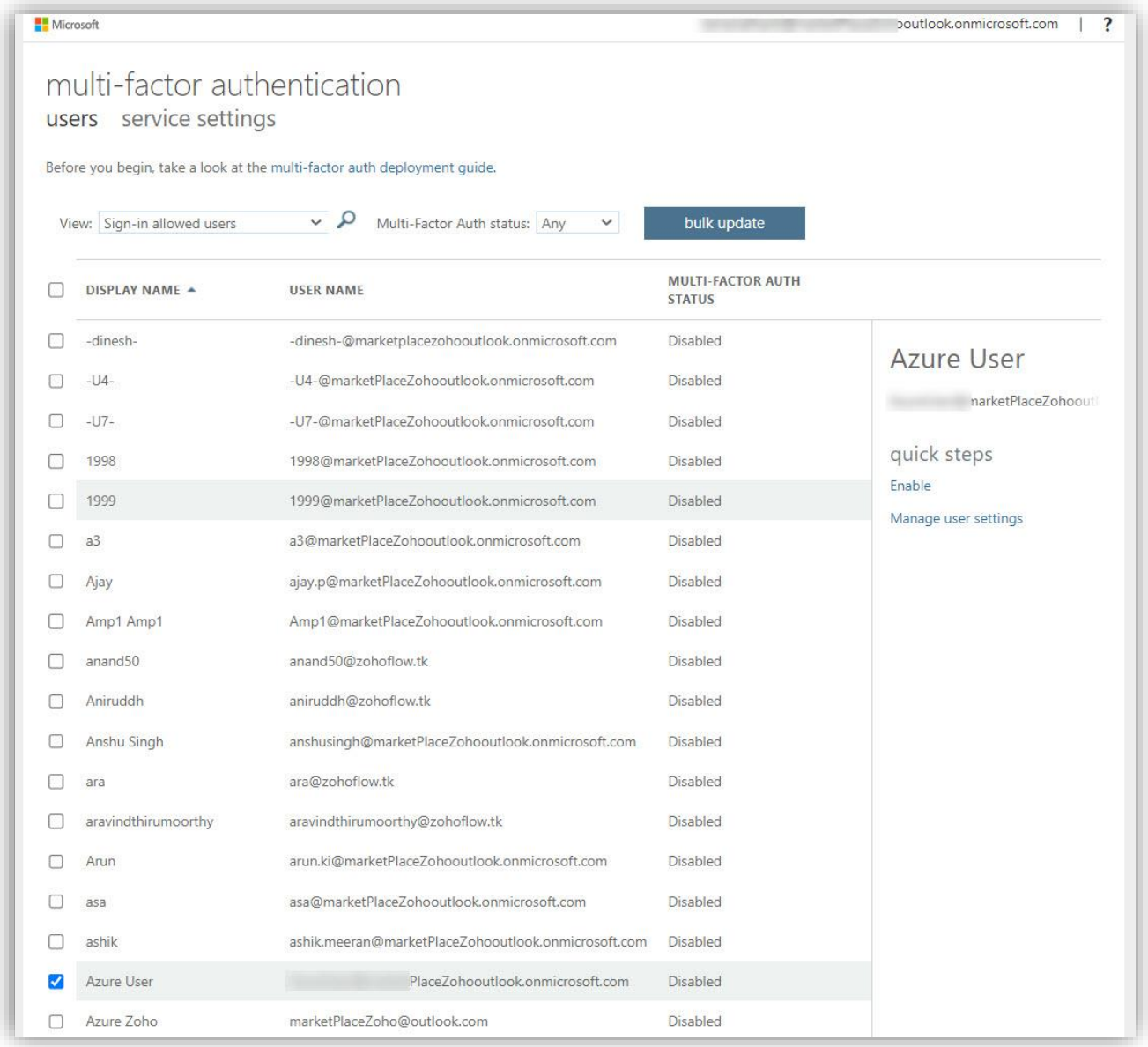
3. Under the **Manage** tab, select **Users**.



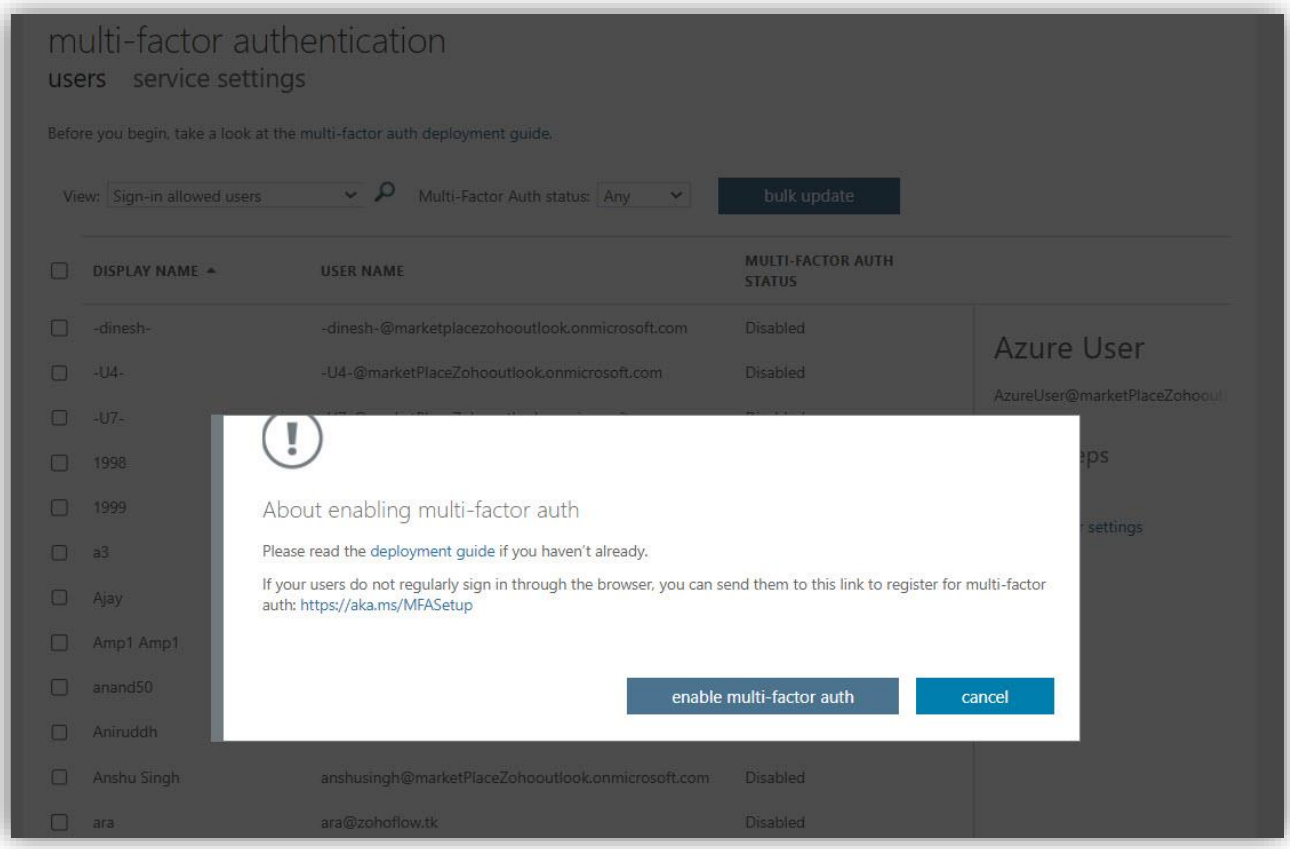
4. Here, click the **Per-user MFA** option at the top. Now you will see the list of users populating in a new browser window.



5. Select the user(s) for whom you want to enable MFA and click the **Enable** option on the right pane.

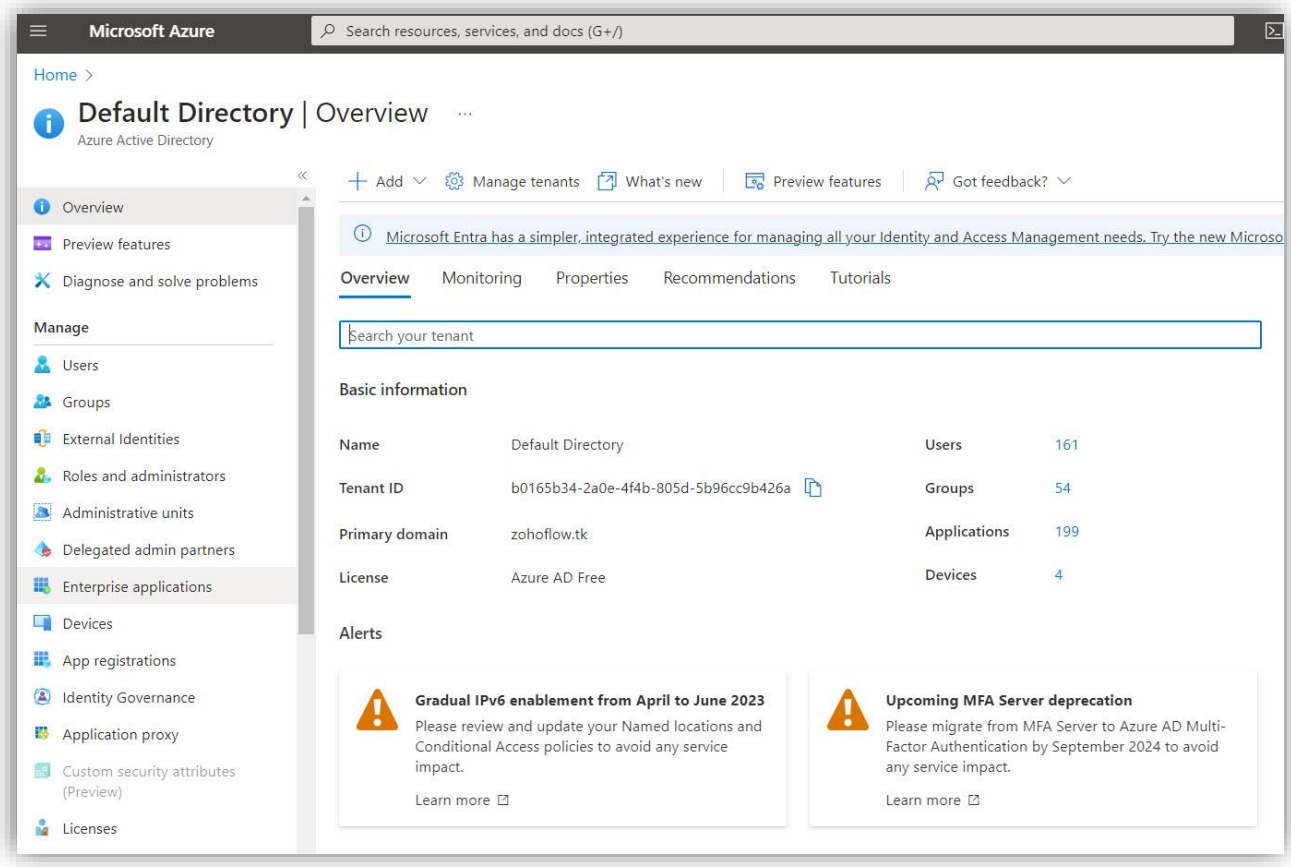


6. In the pop-up box, click the **enable multi-factor auth** button to complete the setup.

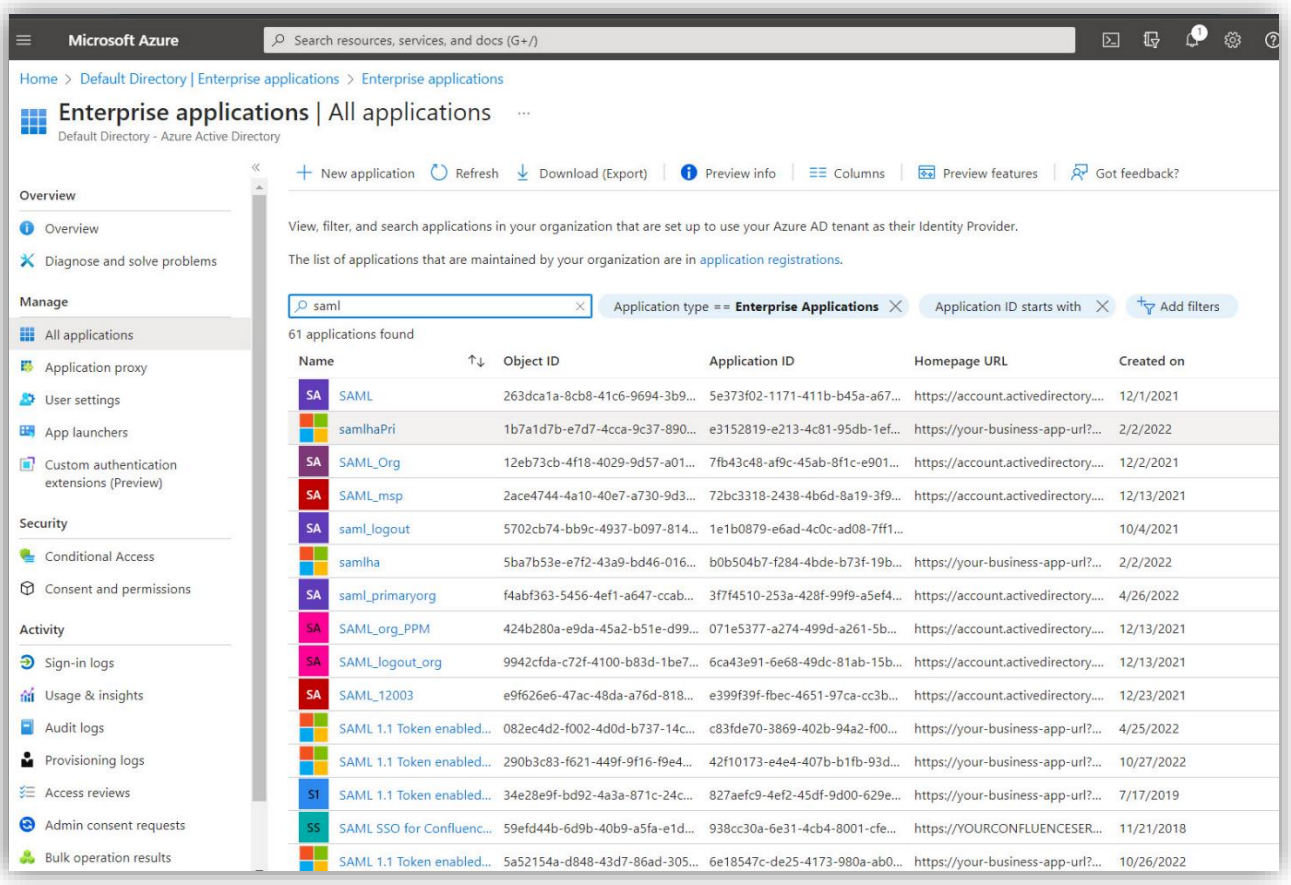


2. Assigning Azure Users to the Enterprise Application

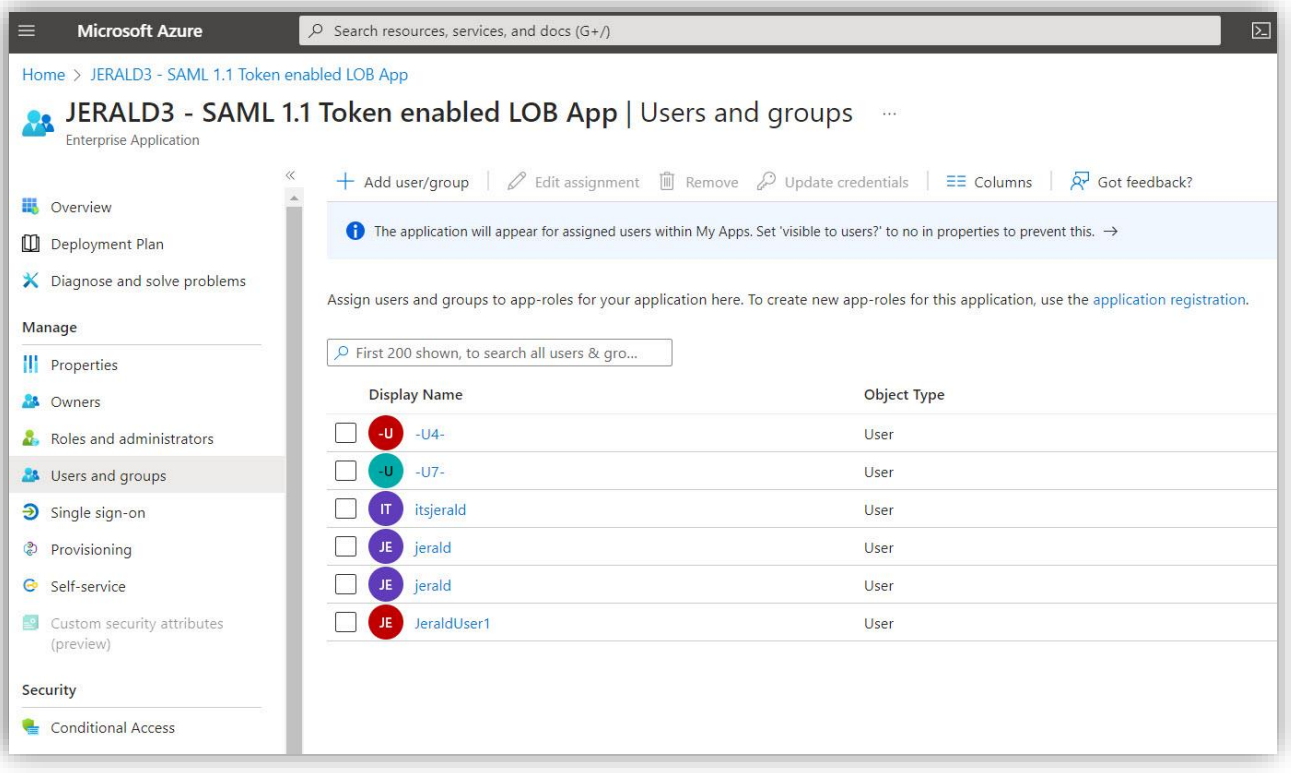
1. Click on **Azure Active Directory** and select **Enterprise applications** under the **Manage** tab.



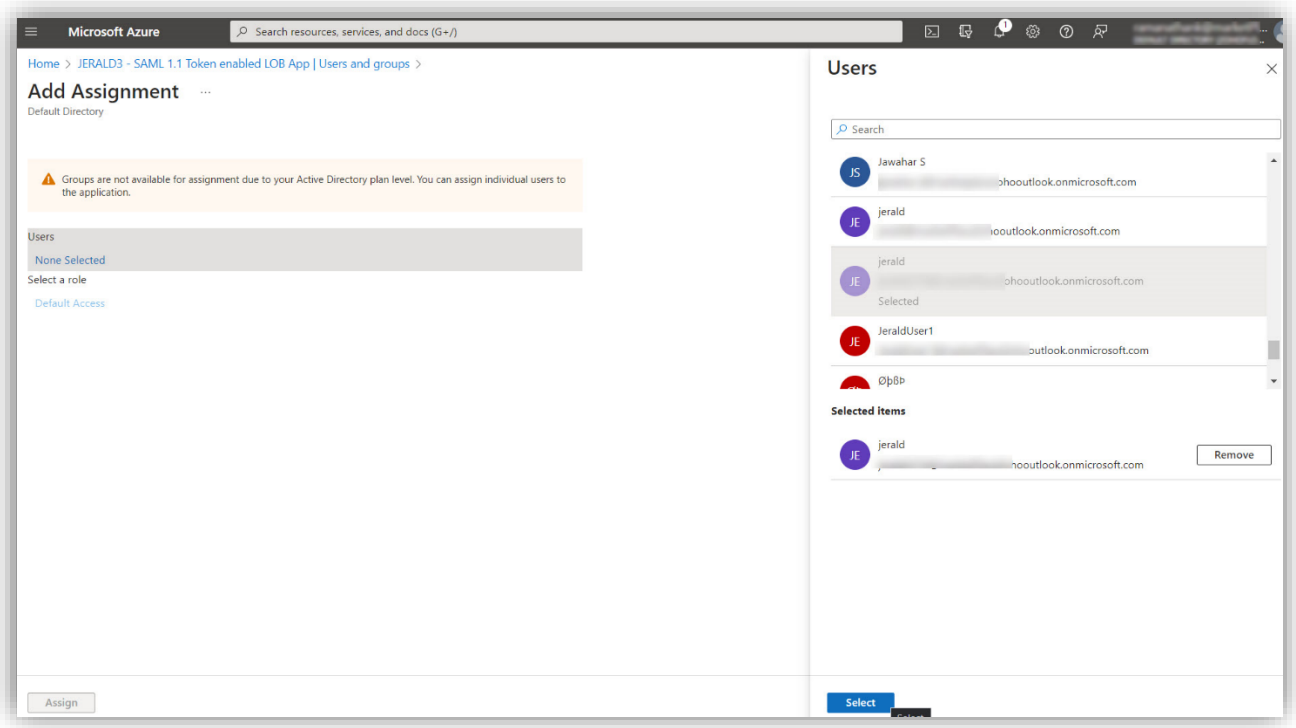
2. Search for your enterprise SAML application and select it.



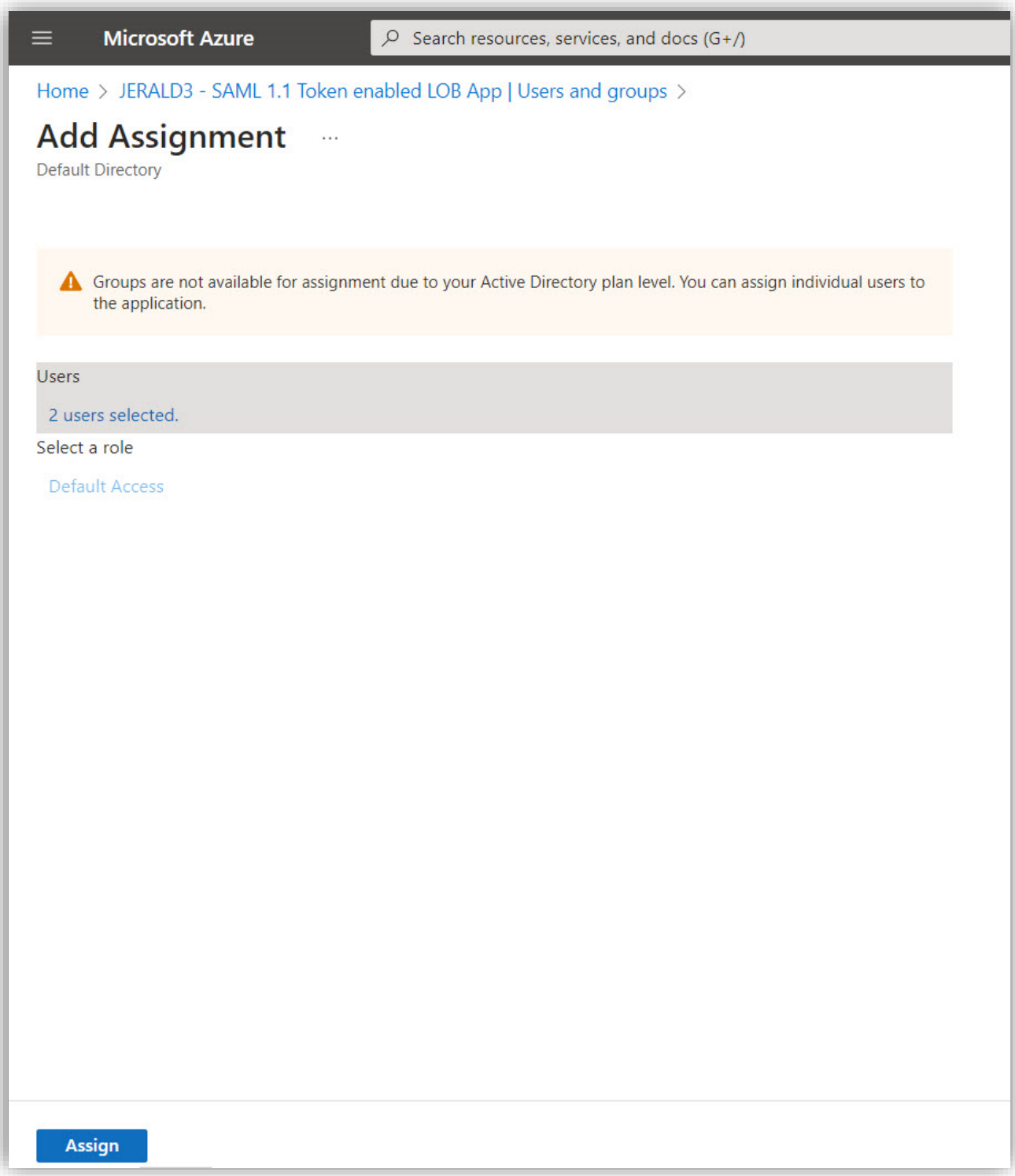
3. Select **Users and groups** from the left pane and click the **Add user/group** option at the top.



4. In the **Add Assignment** pane, click on **None Selected** to open up a list of users. Select the required users and then click the **Select** button at the bottom.



5. After the required users have been selected, click **Assign** at the bottom-left corner to assign them to the enterprise application.



3. Setting Up First Login for the MFA-enabled Azure Users

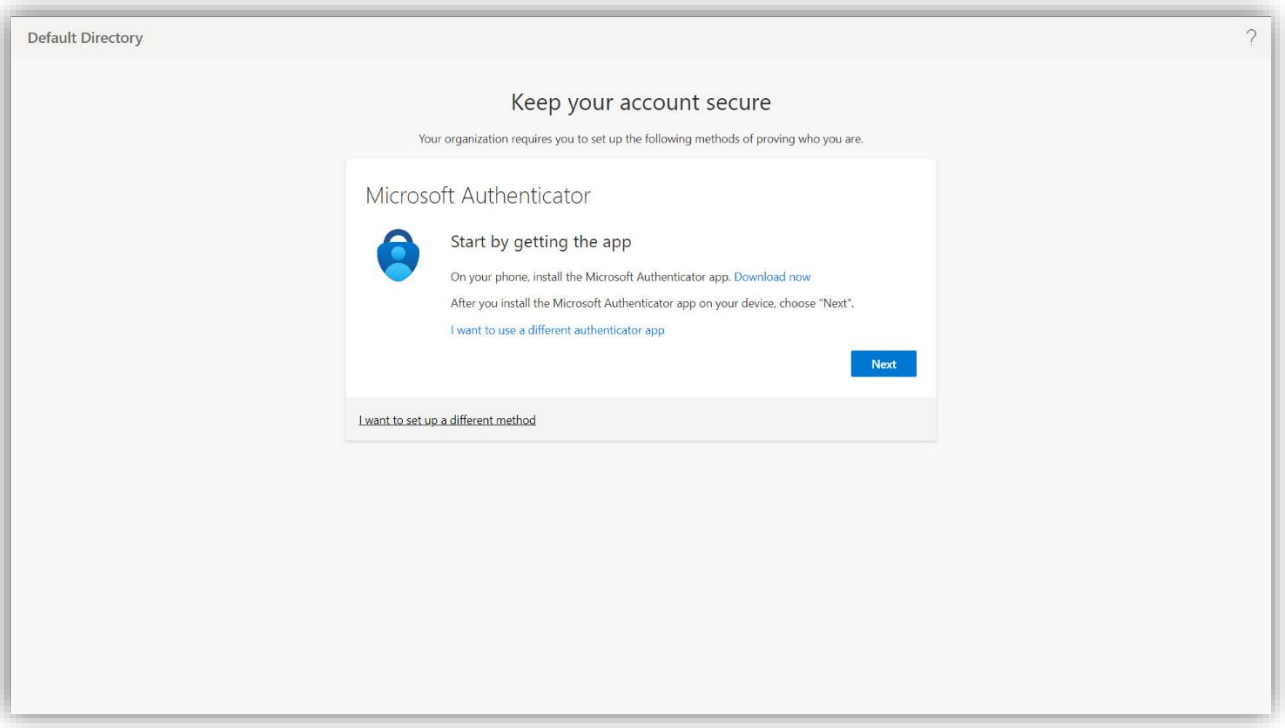
3.1 Prerequisite

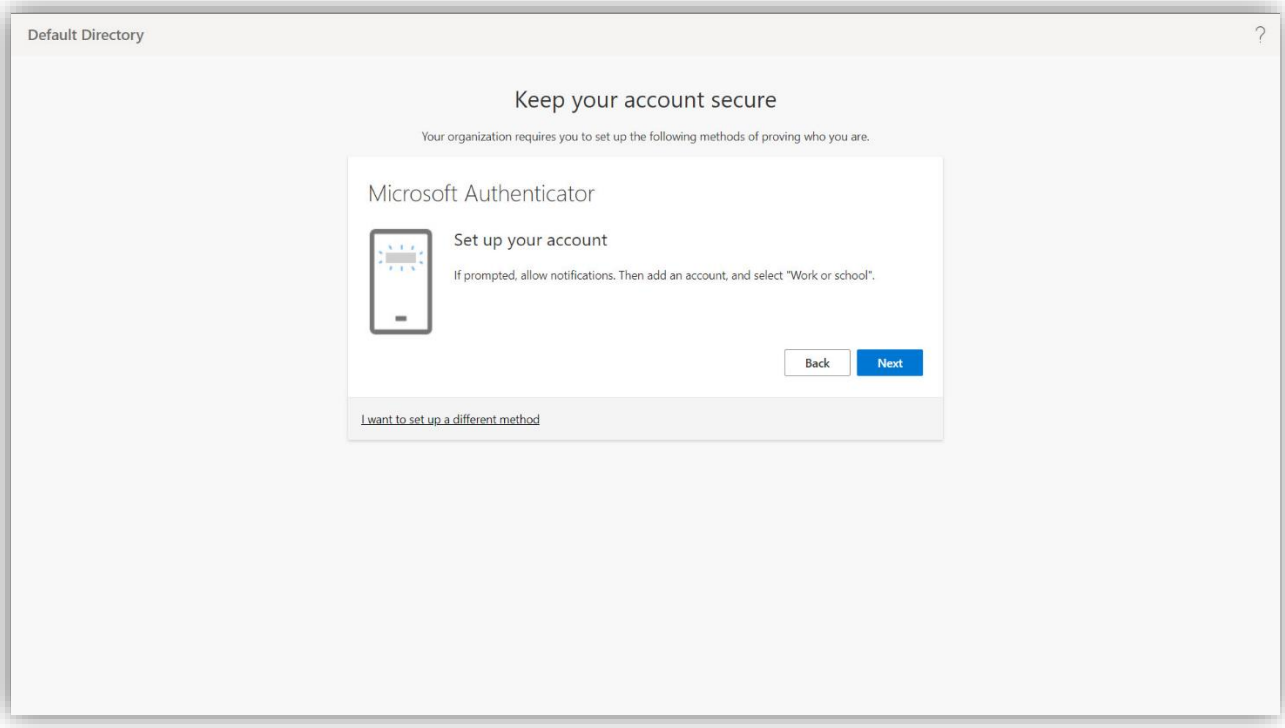
You need to have the Microsoft Authenticator app installed on your phone for additional security verification.

3.2 Steps Required

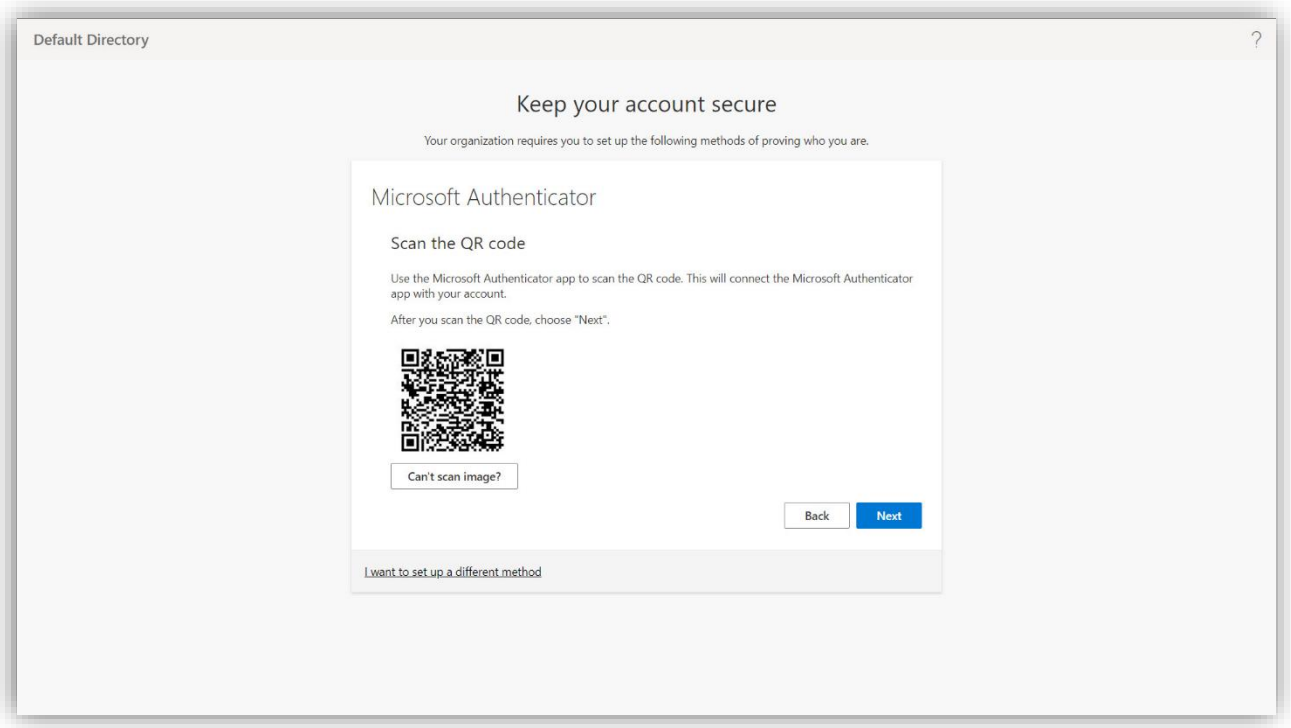
Below steps are for users to set up their first login and multi-factor authentication using the Microsoft Authenticator app.

1. Log in to the Microsoft Azure portal - https://portal.azure.com.
2. Once you login, you will be redirected to the **Keep your account secure** screen. Then, click **Next** until you see a QR code.

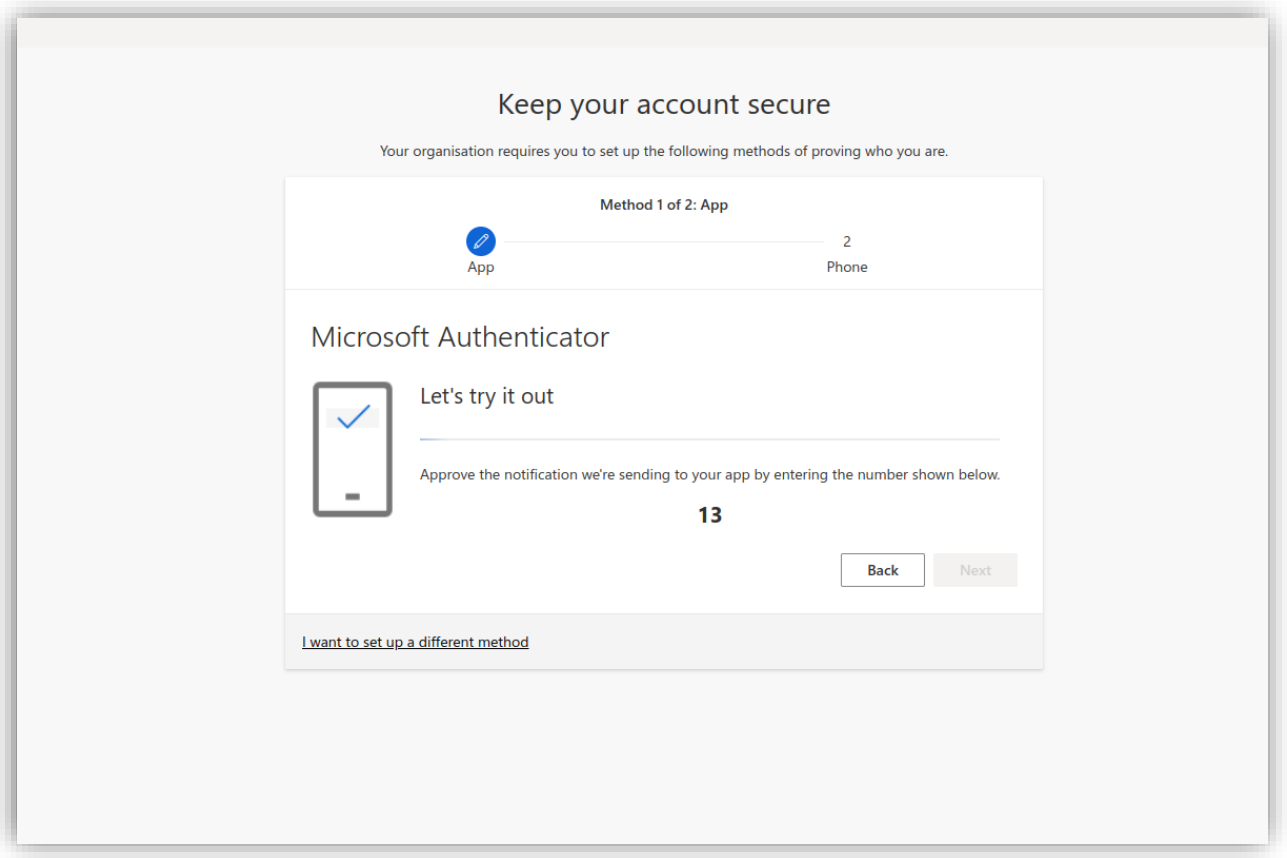


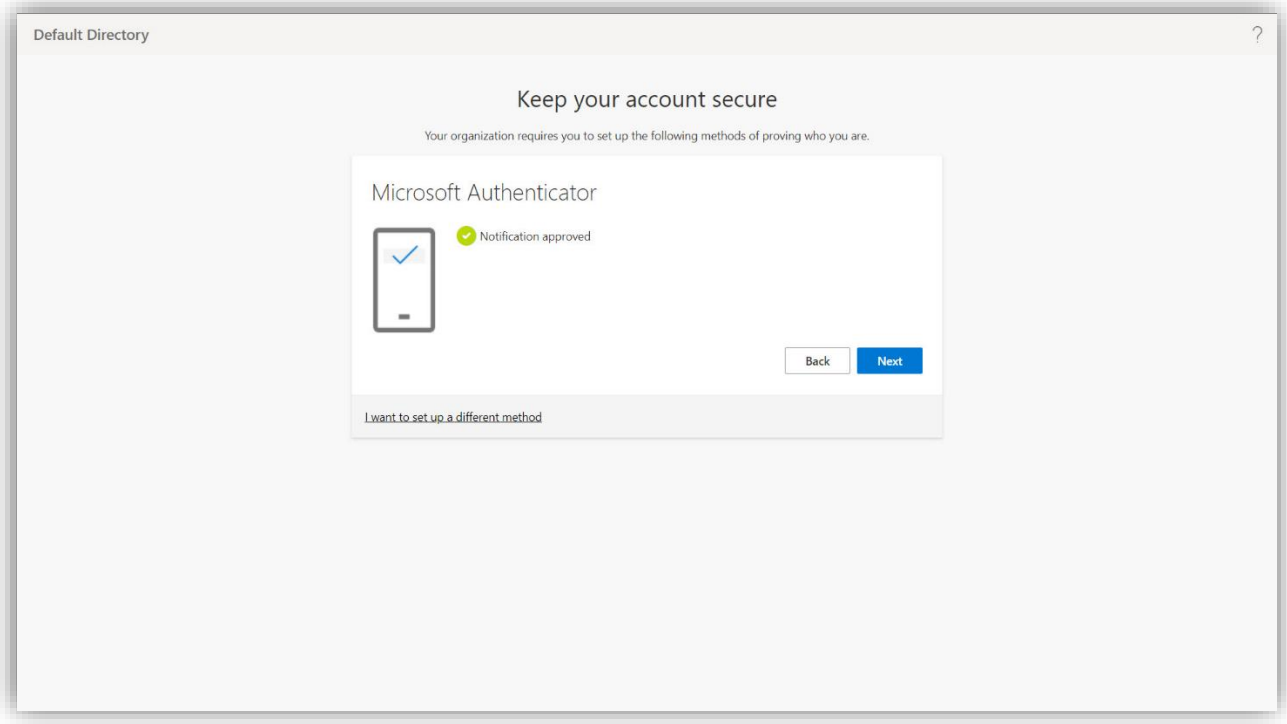


3. Open up the Microsoft Authenticator app on your phone and scan the QR code shown; click **Next**.

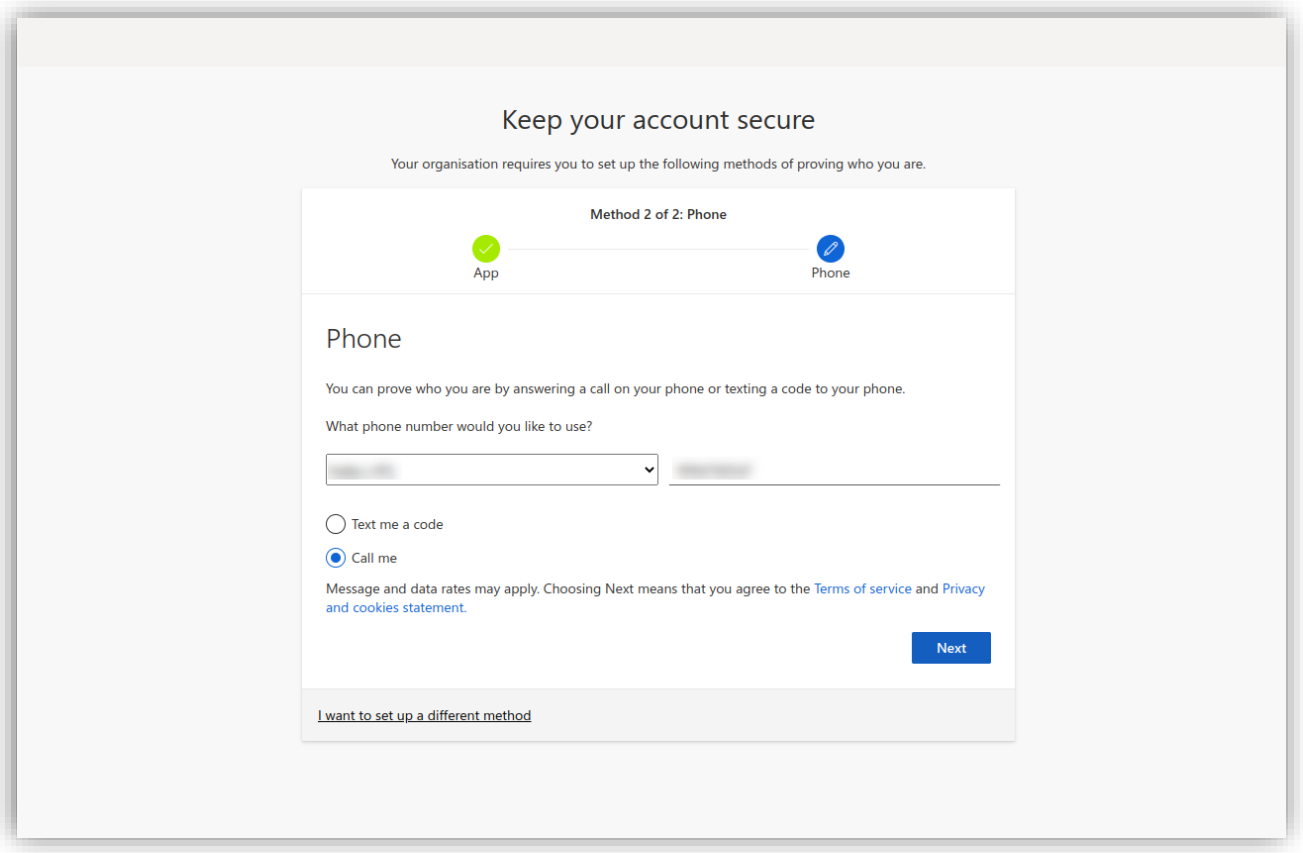


4. Approve the notification that has been sent to the app by entering the number displayed on your computer screen. Once the notification is approved, click **Next**.

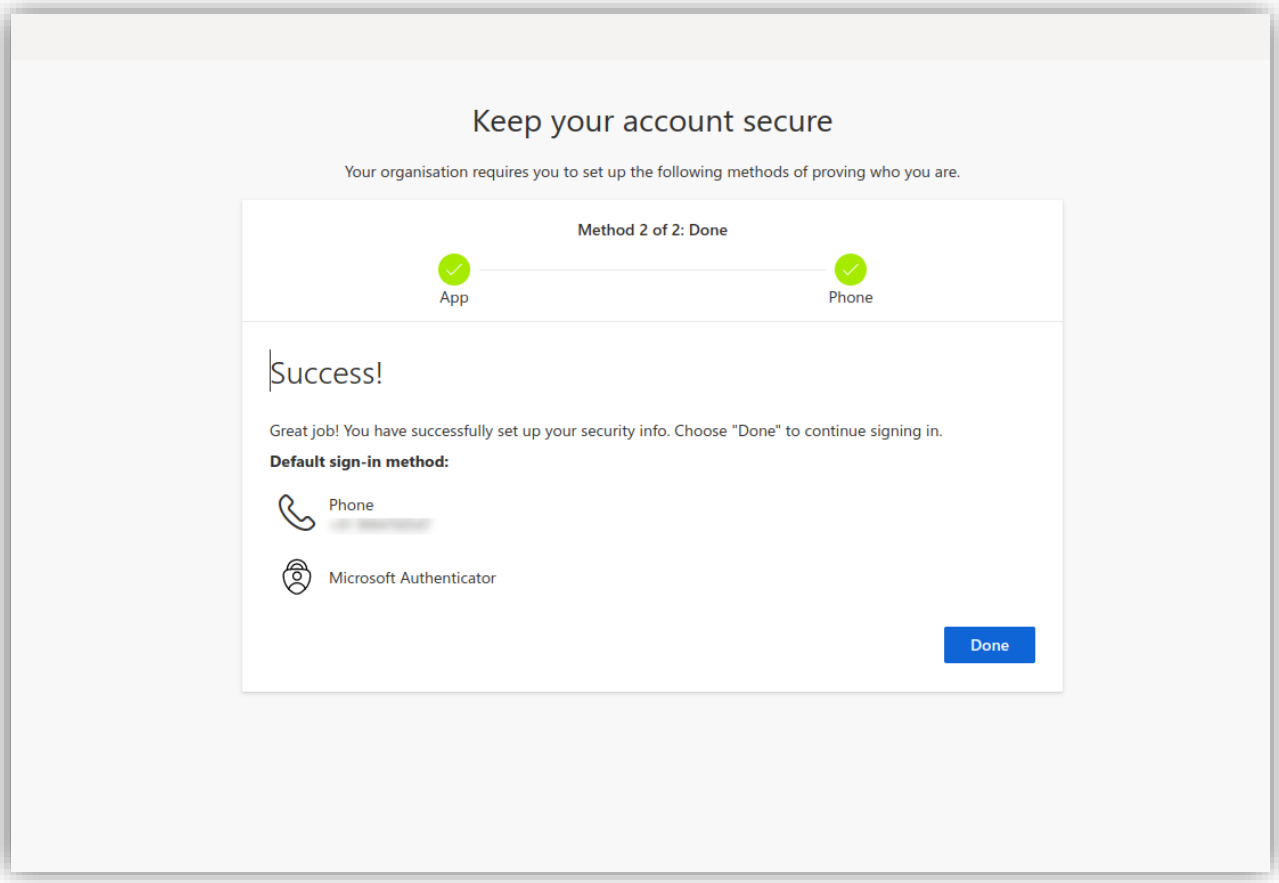


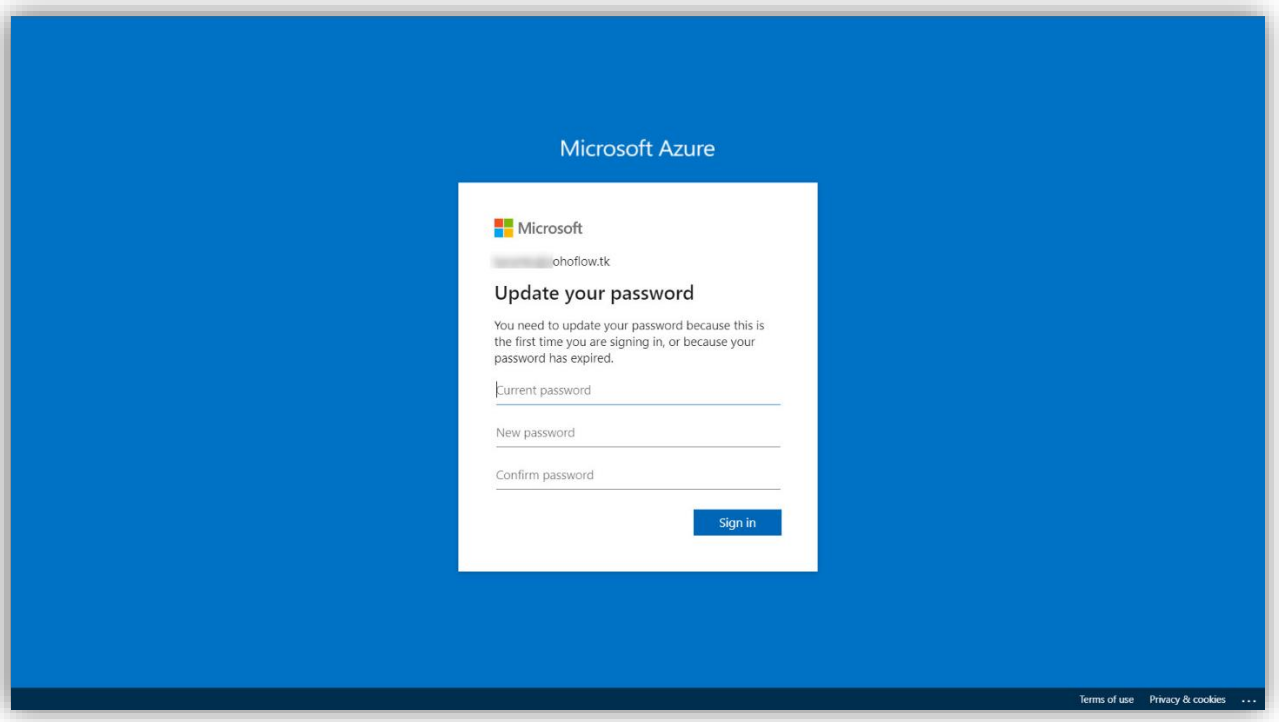


5. Provide your phone number in the text field and choose either **Text me a code** or **Call me**. Click **Next** and complete the verification.

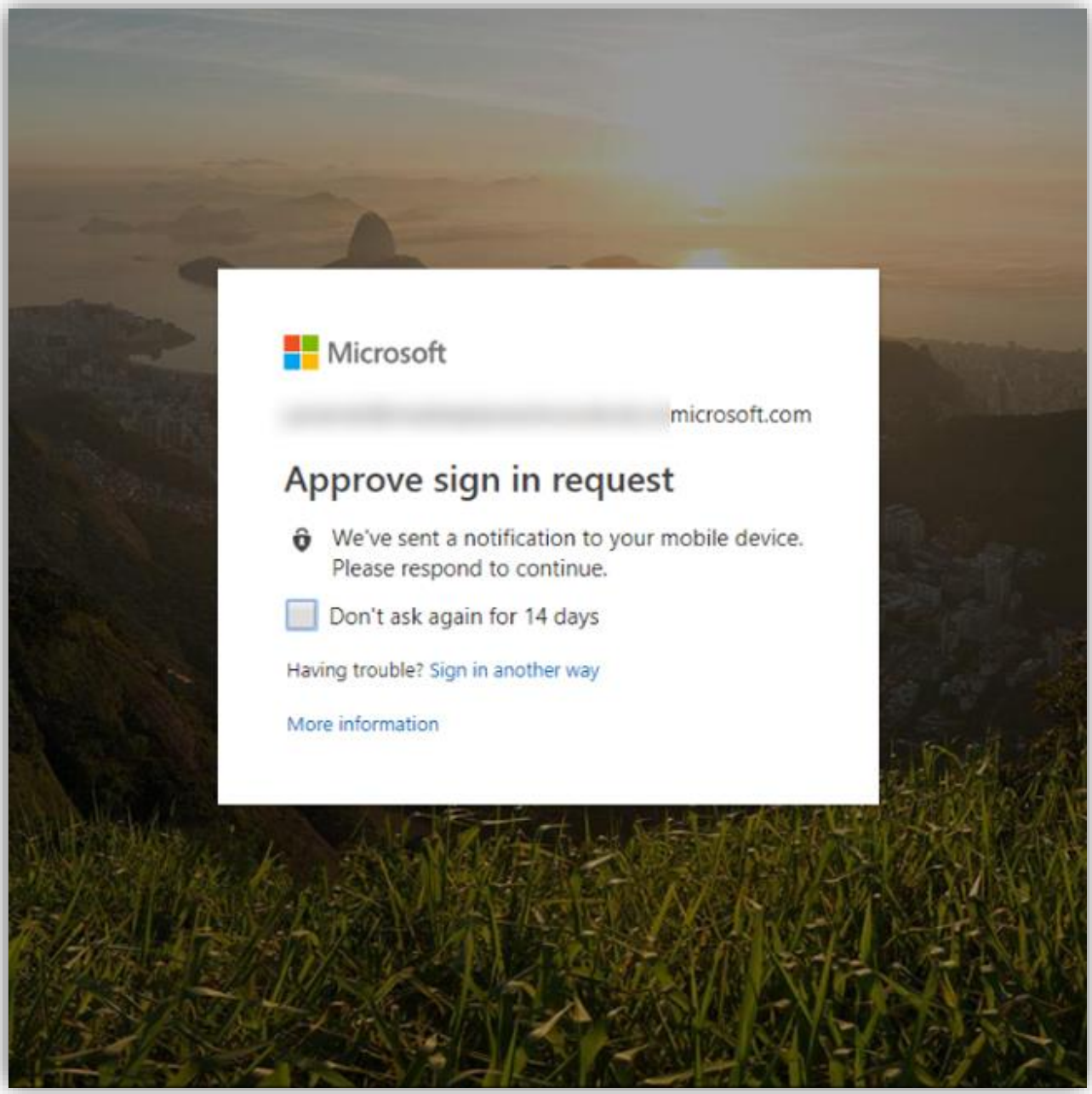


6. You will get a "Success!" message. Click **Done** and you will be asked to reset your password for security reasons.





7. The first login setup is complete. Now, when you try to log in to your Azure account for the first time, you will get a notification on your mobile device to verify the authenticity of your login attempt.



Note: To bypass SAML Single Sign-On and use local authentication to access PAM360, use the following skip URL:

https://hostname:port/PassTrixMain.cc?skipsamlsso=true

where,

"**hostname**" - the host name on which the PAM360 server is running.

"**port**" - the port number used for PAM360.

Configuring Single Sign-On (SSO) using SAML 2.0 for ADFS

Single Sign-On (SSO) is an authentication method that allows users to sign in with a single ID and Password. ManageEngine PAM360 offers support for SSO using SAML 2.0, which facilitates integration with Federated Identity Management Solutions for Single Sign-on (SSO). PAM360 acts as the Service Provider (SP) and it integrates with Identity Providers (IdP) using SAML 2.0. The integration basically involves supplying details about SP to IdP and vice-versa. Once you integrate PAM360 with an IdP, the users have to just login to IdP and then, they can automatically login to PAM360 from the respective identity provider's GUI without having to provide credentials again.

> **Note:** PAM360 allows users to configure SAML SSO for Secondary server as a service provider, which allows users to log in to PAM360 using the Secondary server when Primary is down.

Configuring SSO using SAML is a two-step process involving the following topics:

1. **Steps to Configure ADFS 10.0**
2. **Steps to Configure PAM360 to Enable SSO Services**

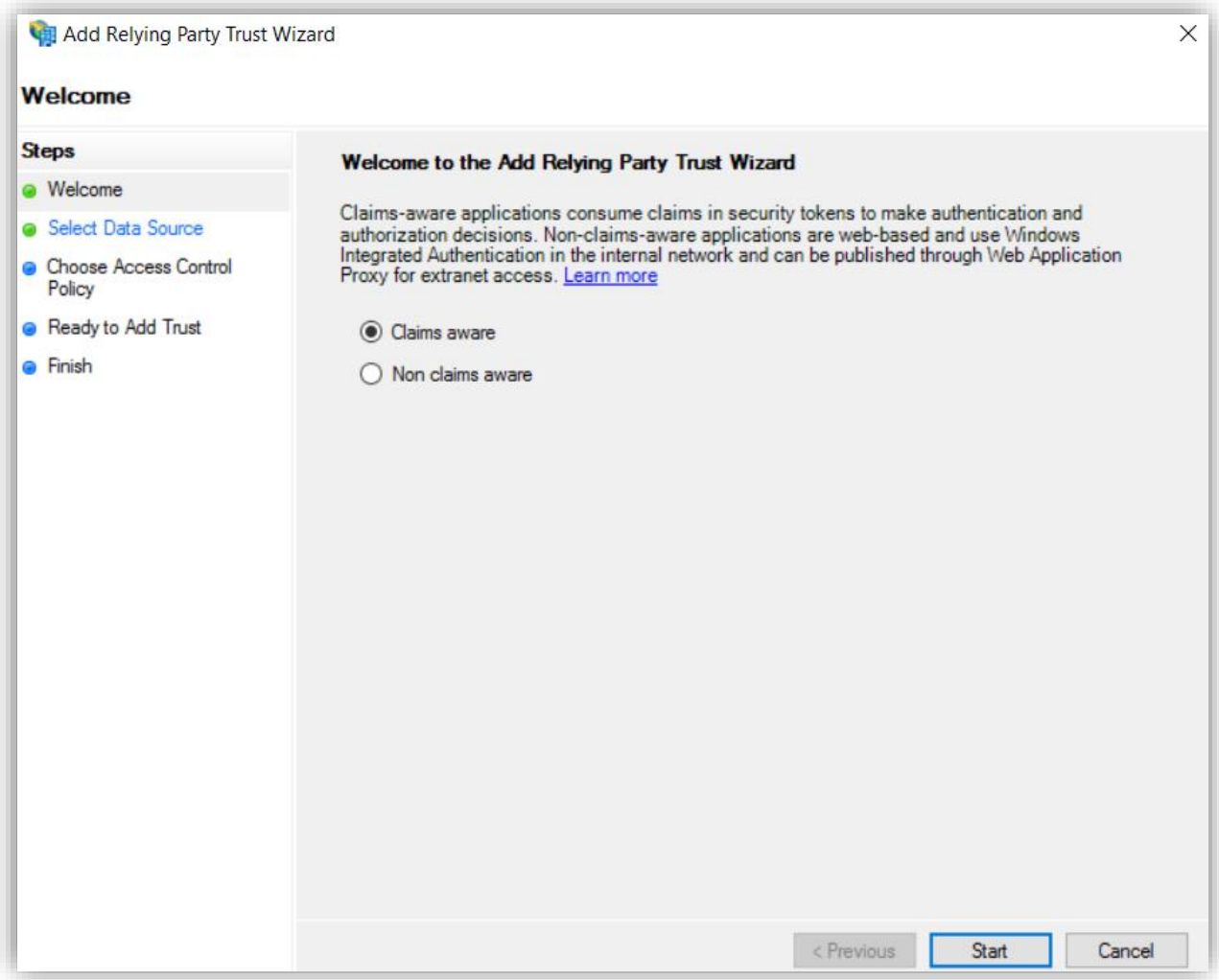
1. Steps to Configure ADFS 10.0

Active Directory Federation Services (ADFS) created by Microsoft runs on Windows and supports SAML integration to provide SSO services to systems and applications throughout the organization. A similar configuration can be achieved in PAM360 as well. For this, you need to first integrate ADFS with PAM360 followed by enabling SSO services.

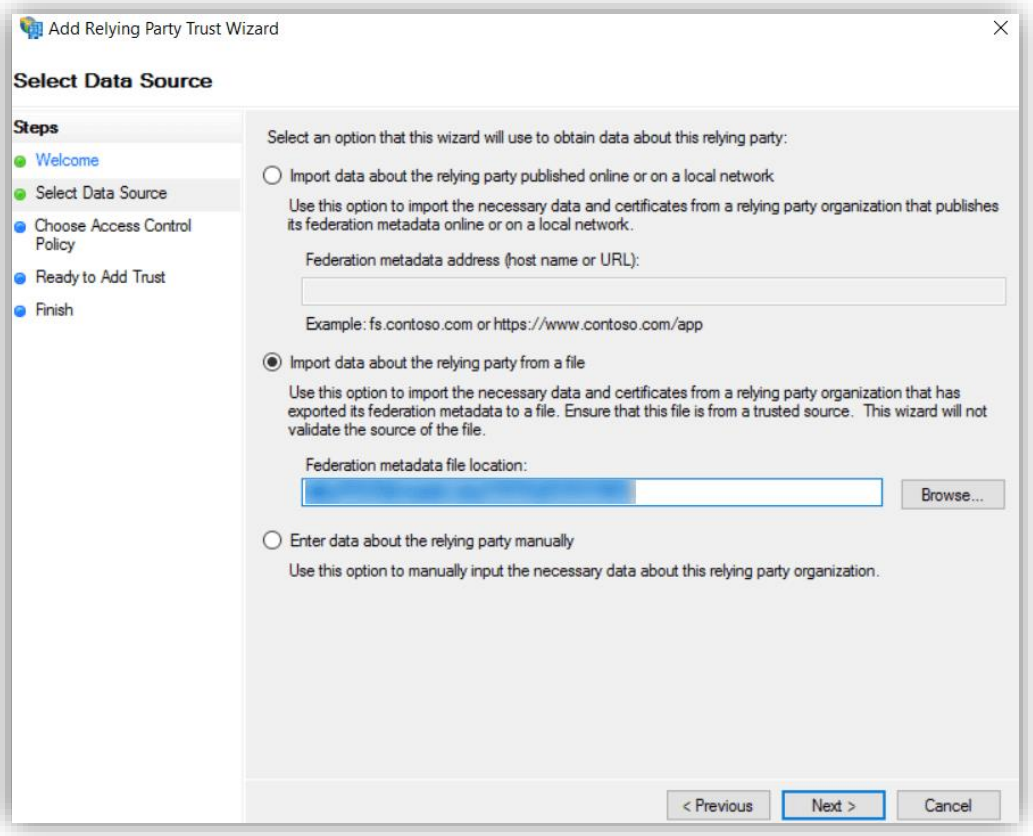
Steps in Detail:

1. Log in to PAM360 and navigate to **Admin >> SAML Single Sign On**. In the SAML SSO configuration page, download the service provider **metadata.xml** file available under step **1**.
2. Navigate to **Start >> All Programs >> Administrative Tools**, and open **ADFS 10.0 Management**.
3. The first step is to add **Trust Relationships** in ADFS 10.0 to add PAM360 details. Under **Trust Relationships**, right-click on **Relying Party Trusts** and select **Add Relying Party Trust**

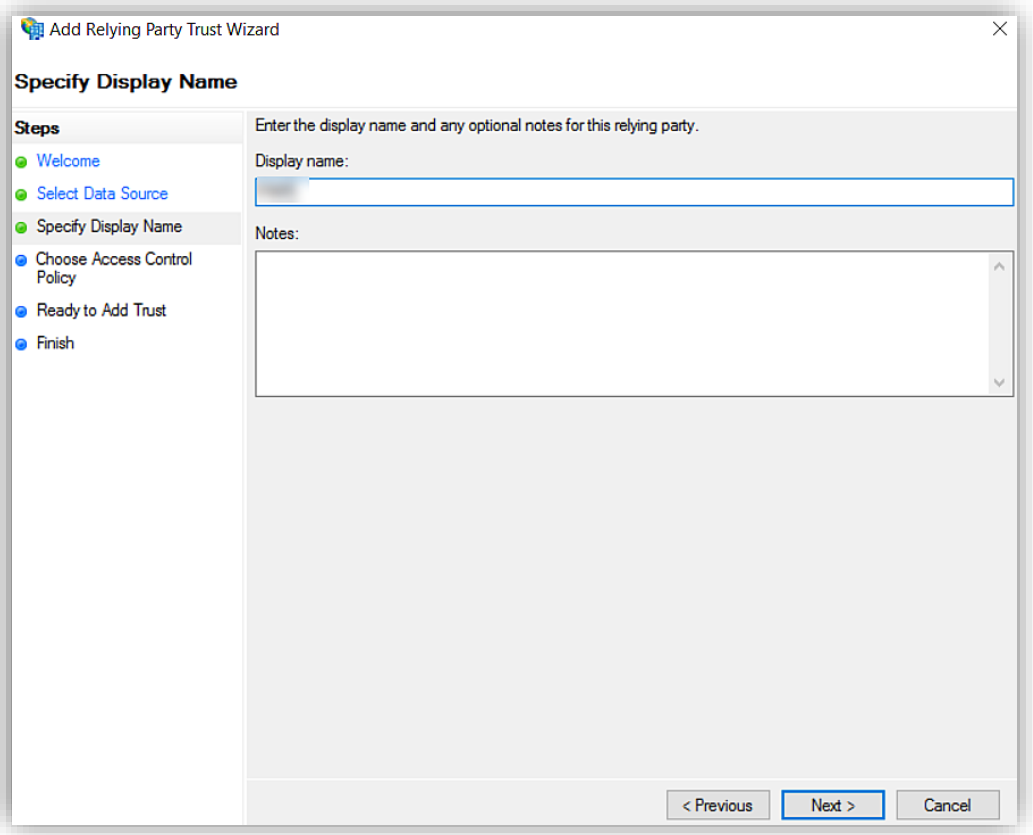
from the drop down menu. A **Add Relying Party Trust Wizard** appears on the screen.



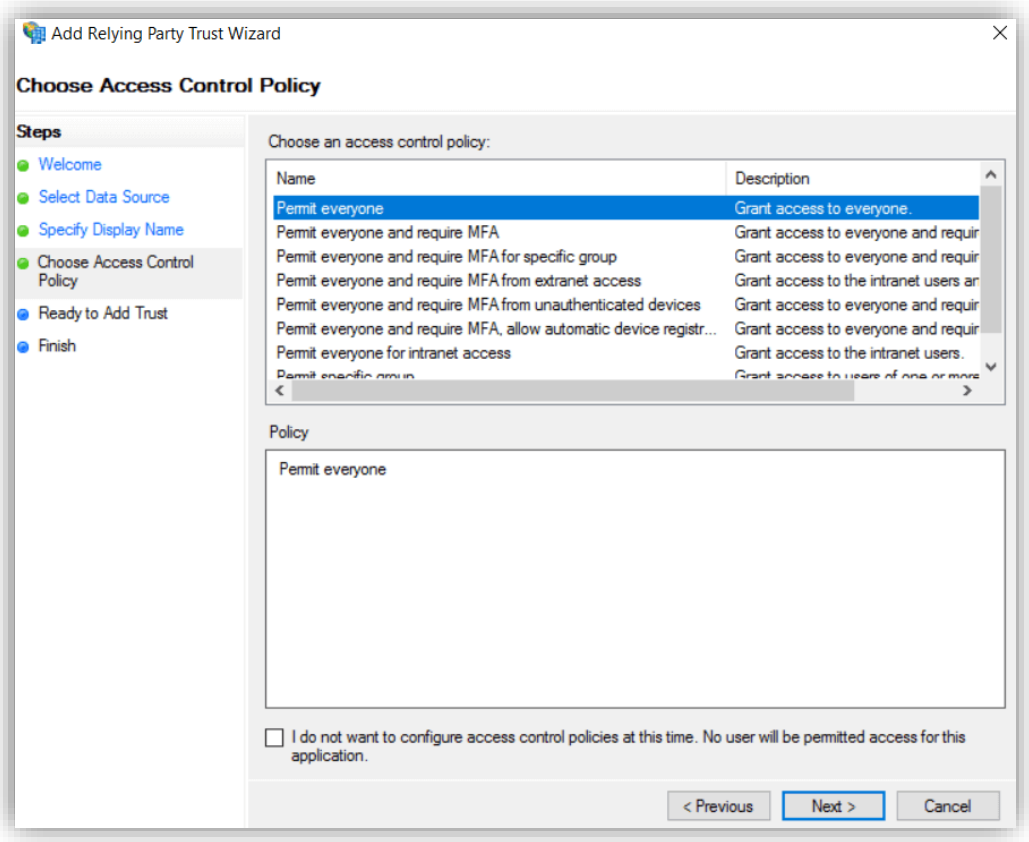
i. Click **Start** and click **Select Data Source** from left pane.
ii. Choose the second option, **Import data about the relying party from a file.**
iii. Click **Browse** to import the **metadata.xml** file downloaded earlier from PAM360, and click **Next**.



iv. Set a **Display name** for the relying party, i.e. PAM360 and click **Next**.

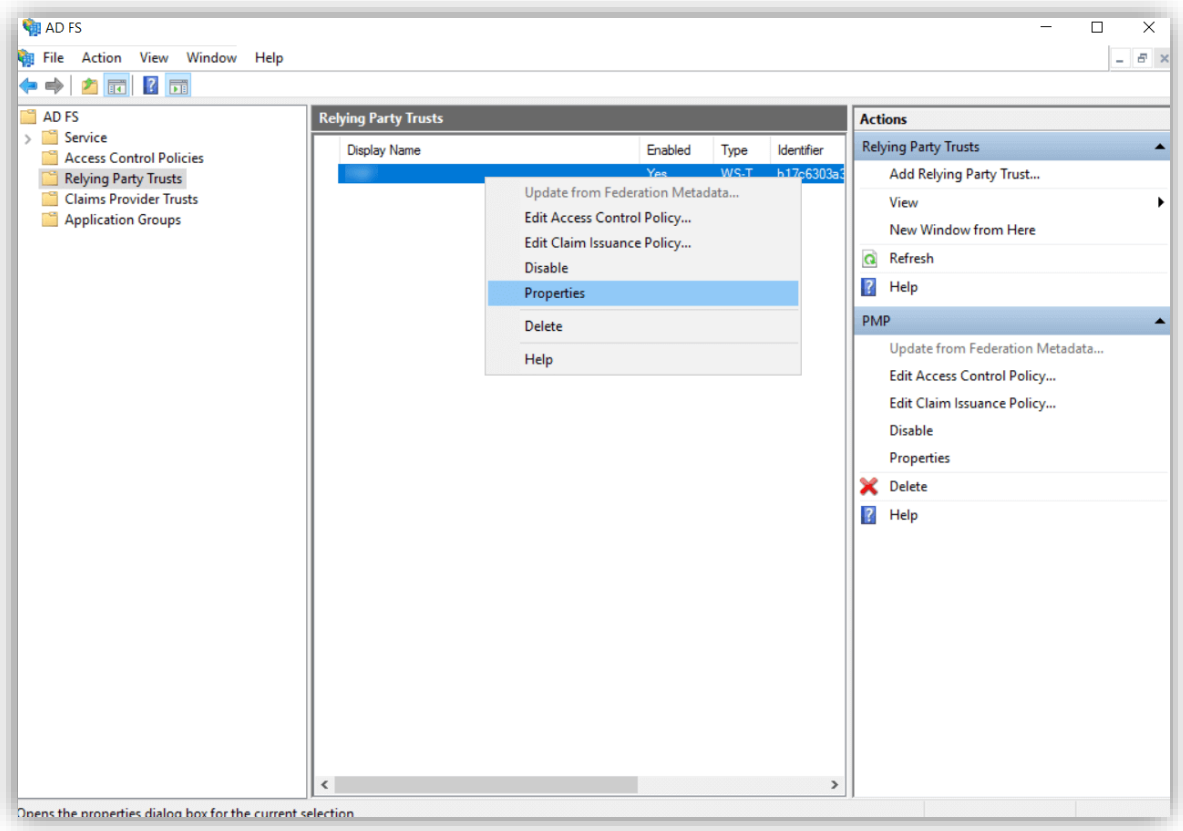


v. **Choose Access Control Policy:** Select **Permit everyone** and click **Next.**

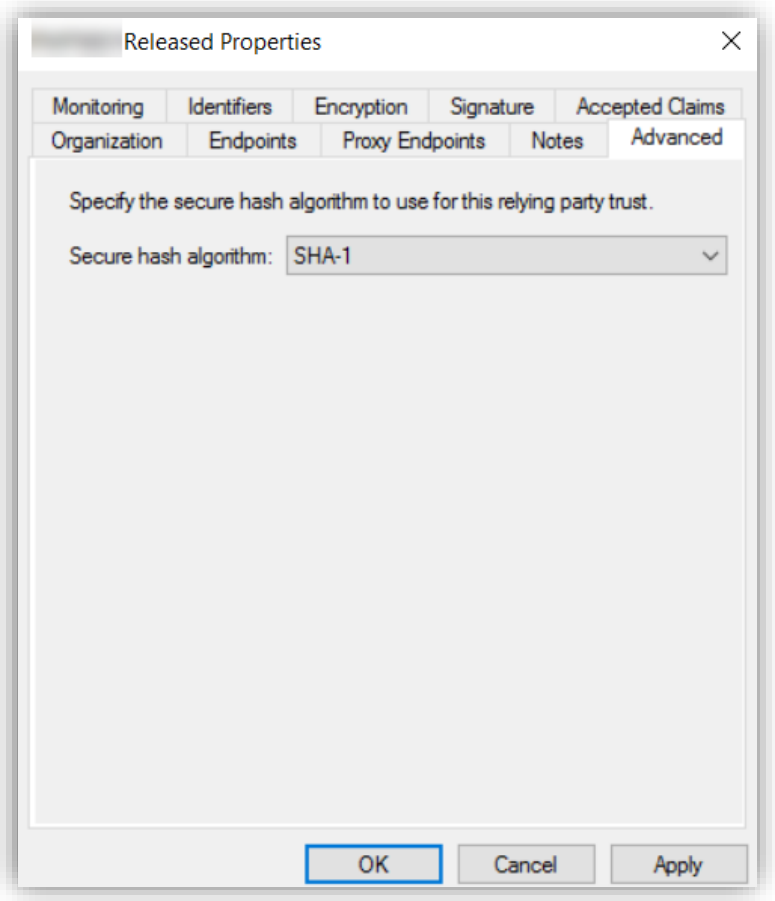


vi. Skip the **Ready to Add Trust** step by clicking **Next** and then click **Close**.

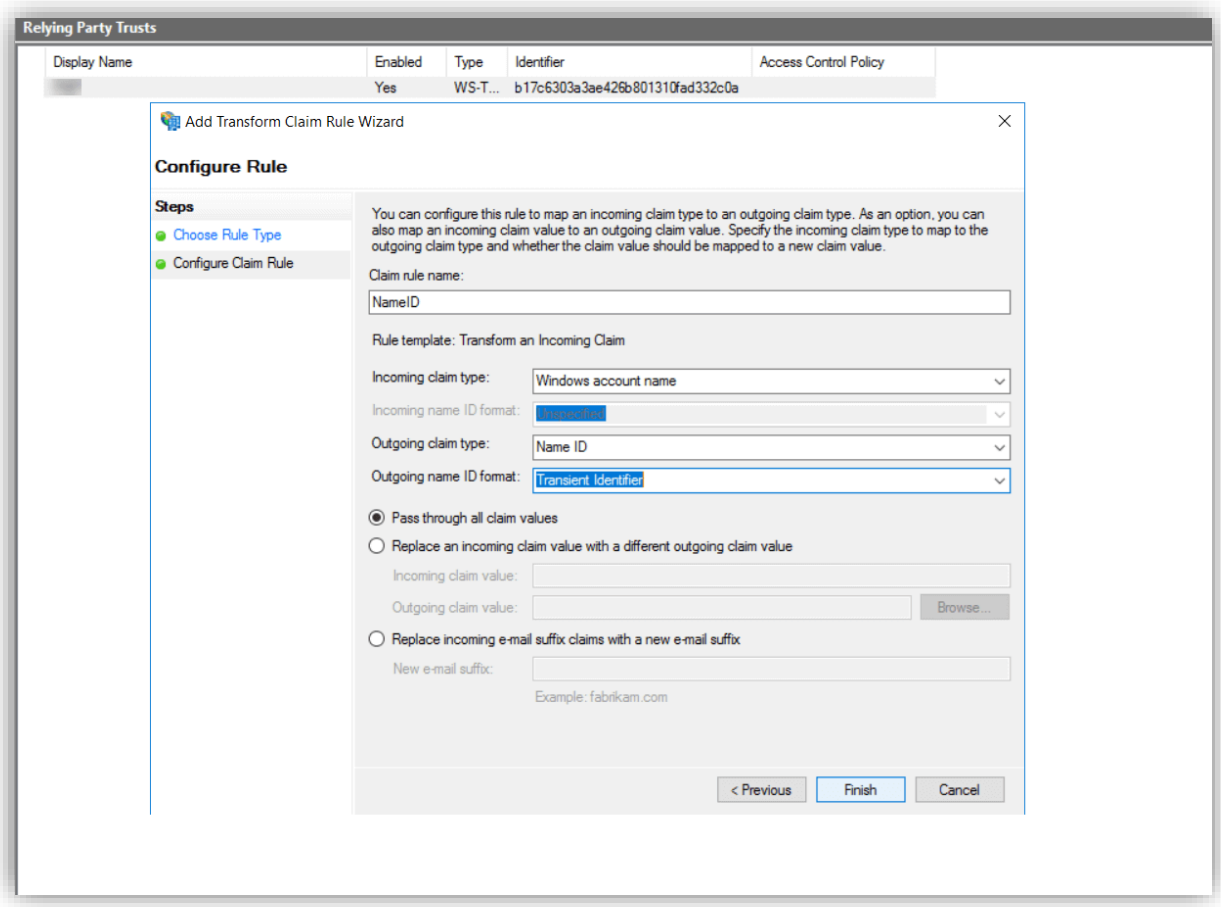
4. PAM360 will now be displayed in the **Relying Party Trusts** list. Right-click on the same and select **Properties** from the drop down menu as shown below.



5. In the dialog box that opens, switch to the **Advanced** tab and select **SHA 1** as the secure hash algorithm. **Apply** changes and click **Ok**.



6. Right-click on PAM360 again and now select **Edit Claim Insurance Policy**.
7. In the dialog box that opens,
    i. Click **Add Rule** under **Issuance Transform Rules.**
    ii. Select **Transform an Incoming Claim** as the **Claim rule template** and click **Next**.
    iii. Under **Configure Claim Rule**,
        a. Enter **NameID** as the **Claim rule name.**
        b. Select **Windows account name** as the **Incoming claim type.**
        c. Select **Name ID** as the **Outgoing claim type.**
        d. Select **Transient Identifier** for **Outgoing name ID format.**
    iv. Click **Finish**.



8. Click **Apply** to save changes and close the **Edit Claim Rules** window by clicking **Ok**.

Now, you have successfully configured ADFS in PAM360. Proceed to step 2 below to know how to enable SSO services in PAM360.

> **Note:** If you have already imported users to PAM360 from AD, then their login names will be stored in the format, **DOMAIN\Loginname**. By default, setting **Windows account name** as the incoming claim type will match this format. However, if you have created PAM360 local accounts for your AD users by importing them via a CSV file, you need to instead select a different claim type that matches the login name format stored in PAM360.

2. Steps to Configure PAM360 to Enable SSO Services

1. Open PAM360 and navigate to **Admin >> Authentication >> SAML Single Sign-On**.
2. Under Step 2 in the page, choose the first option **Upload IdP metadata file** to browse and open ADFS's **Federation.xml** file.

Notes:

1. The XML file can be downloaded from ADFS 10.0 console. In the console's left navigation pane, click on **Endpoints** and scroll down to the Metadata list. Now, locate the URL Path provided for the Federation Metadata type in this list and open the URL in a new browser tab to download the metadata XML file.
2. For SAML SSO authentication, the **Assertion Consumer URL** is the hostname of the server, by default. To update the Assertion URL, follow the below steps:
    a. Go to **Admin >> Settings >> Mail Server Settings.**
    b. Under **Access URL**, update the required URL and click **Save**. Now, the **Assertion Consumer URL** under **Service Provider Details** will be updated.

3. The uploaded XML file will also populate the certificate details required for Step 3. In case the details aren't auto-filled in upon providing the metadata file, try configuring the Identity Provider details manually in Step 2 and 3. Then, click **Save**.
4. To configure SAML Single Logout, navigate to **<PAM360_Installation_Directory\PAM360\conf\system_properties.conf>** and append the following system property under the existing properties.
    - **saml.logout.redirect.slo=true**

Notes:

1. SAML Single Logout is applicable from **PAM360 build 5304** and above only.
2. If you have already configured SAML for PAM360, re-upload the **metadata.xml** file to configure Single Logout.

5. ADFS SSO service is now successfully configured for PAM360. Click on **Enable SAML SSO** to activate the service.
6. Log out and log back in to PAM360 to test the configuration.

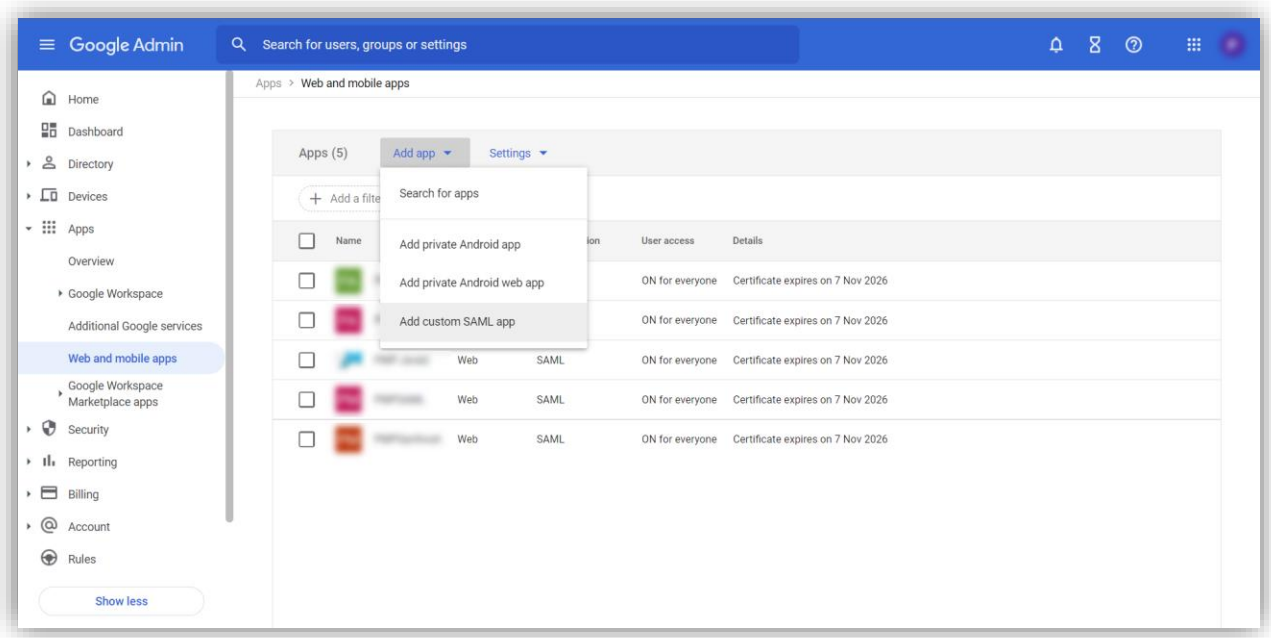
Configuring SAML Single Sign-On (SSO) using G Suite

SAML Single Sign-On (SSO) is an authentication method that allows users to log in to applications using a single credential. ManageEngine PAM360 offers support for SAML 2.0 and allows users to configure SAML using Okta, Azure AD, ADFS, and G Suite/Google Workspace to use SSO.

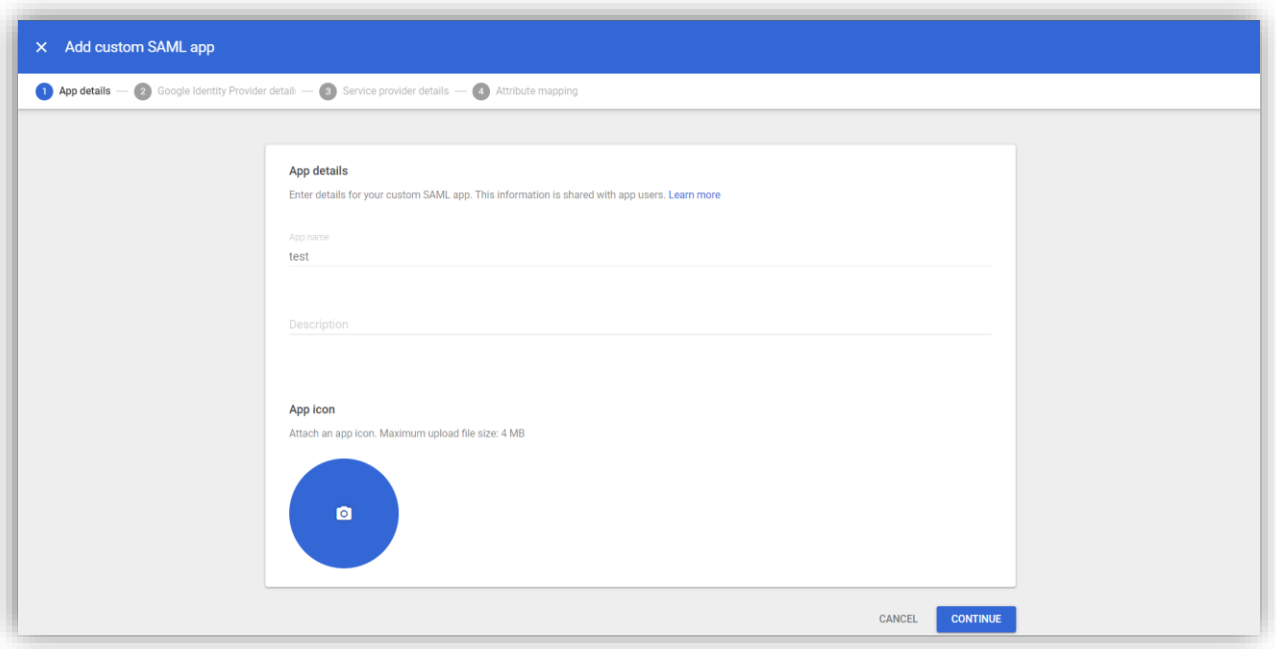
Follow the below steps to configure SAML SSO in G Suite/Google Workspace and enable the same in PAM360.

Steps Required

1. Log in to G Suite/Google Workspace using Super Administrator privileges and navigate to **Apps >> Web and mobile apps.**
2. Click **Add app >> Add custom SAML app.**



3. In the **Add custom SAML app** page,
   i. Enter the **App name, Description** and choose an **App icon.**
   ii. Click **continue.**



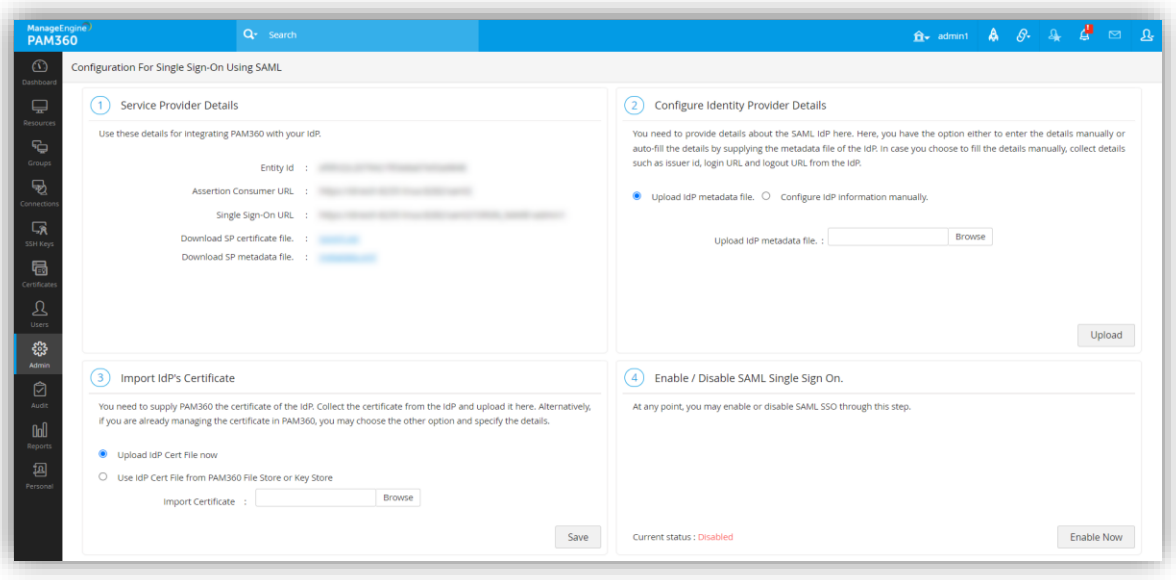
iii. Here, **Download the Metadata file** from G Suite and upload in PAM360.

a. Log in to PAM360 as an administrator and navigate to **Admin >> Authentication >> SAML Single Sign-On.**

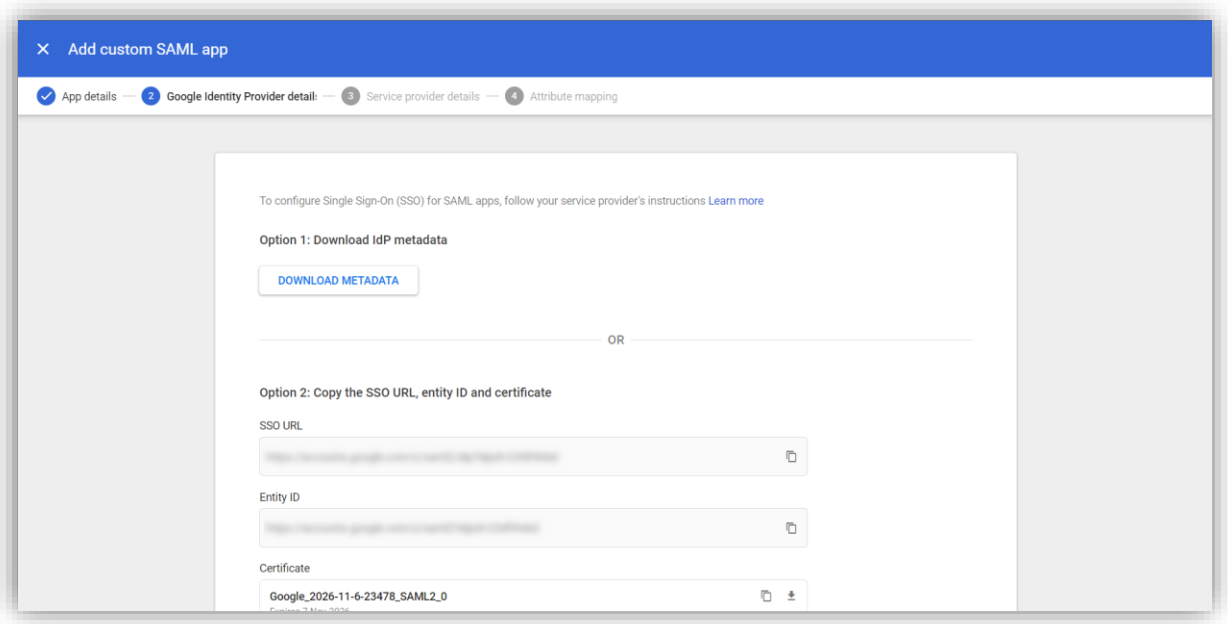
b. Under **Configure Identity Provider Details, Browse** and **Upload IdP metadata file.** [OR]

c. To update the values manually, open PAM360 and navigate to **Admin >> Authentication >> SAML Single Sign On.**

d. Under **2. Configure Identity Provider Details,** mention the **SSO URL** from G Suite as **IdP Login URL** in PAM360 and **Entity ID** from GSuite as **Issuer** in PAM360.



iv. Click **continue.**



v. Now, to configure SAML, mention the service provider details.

A. To access these details, go to PAM360 homepage and select **Admin >> Authentication >> SAML Single Sign On.**

B. Under **1. Service Provider Details,** you will find **Entity Id, Assertion Consumer URL;** copy the values.

> **Note:** By default, the Assertion Consumer URL is the hostname of the server. To update this, follow the below steps:

a. Go to **Admin >> Settings >> Mail Server Settings.**
b. Under **Access URL,** update the required URL and click **Save.**
c. Now, the **Assertion Consumer URL** under **Service Provider Details** will be updated.

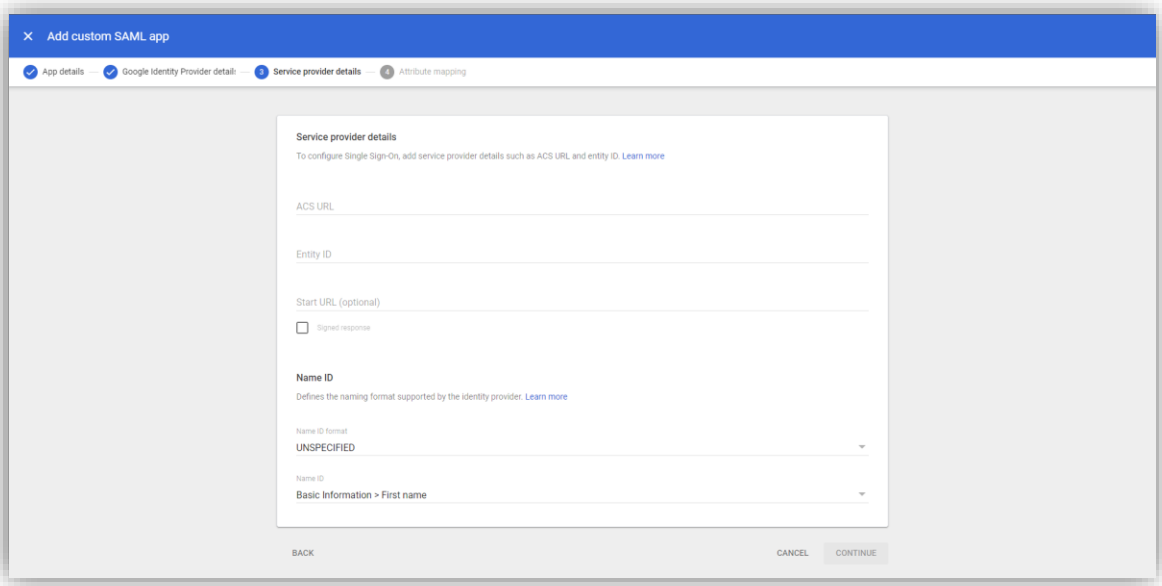
vi. Go back to **Add custom SAML app** page.

a. Enter **Assertion Consumer URL** from PAM360 under **ACS URL** and **Entity ID** from PAM360 under **Entity ID.**

b. You can also mention the **Name ID Format** and **Name ID** here.

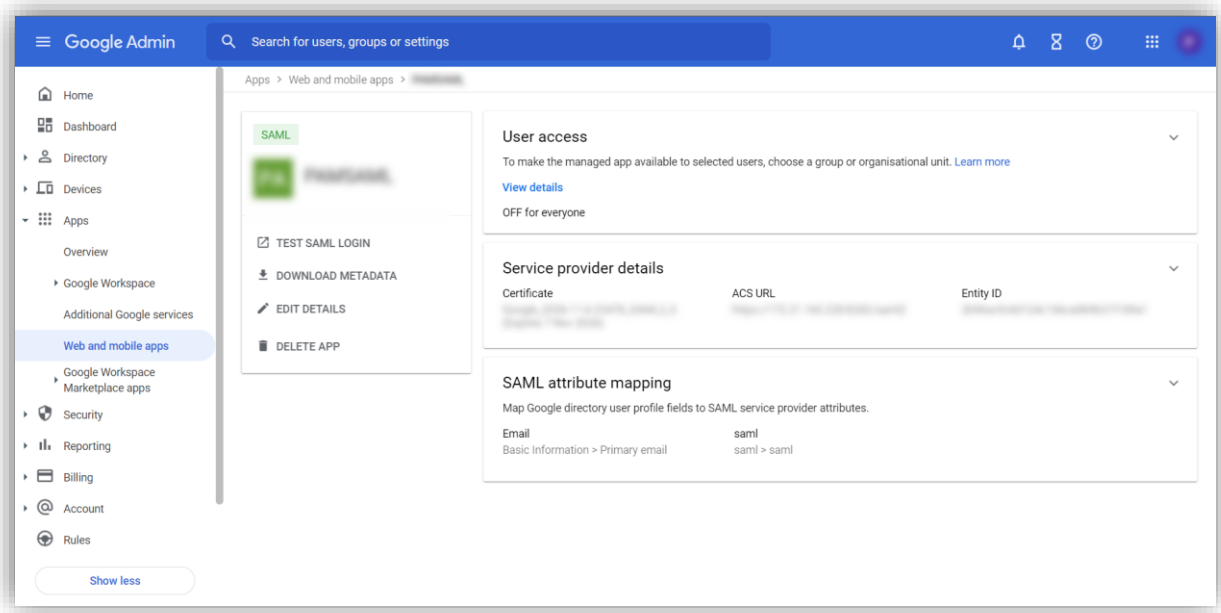
> **Note:** We can update FQDN/IP/SAN name of the PAM360 UI here and not the hostname.

c. Click **Continue.**

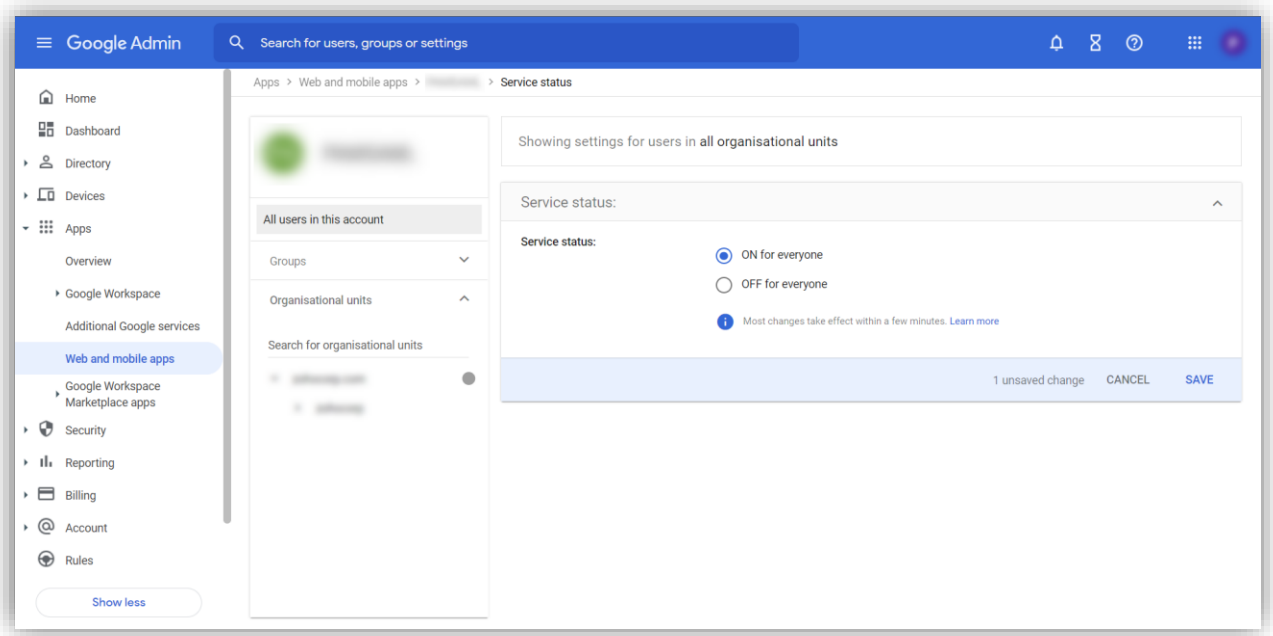


vii. You can update the **Google directory attributes** with PAM360 **App attributes** now or you could choose to update them later.

viii. Click **Finish.** Now, you have successfully set up your custom SAML application in G Suite.



4. The **User access** is turned **OFF for Everyone** by default. To turn it on, click **User access,** select **ON for Everyone** and click **SAVE.**



5. The final step is to enable SAML SSO in PAM360.

   i. Navigate to **Admin >> Authentication >> SAML Single Sign On.**
   ii. Under **4. Enable / Disable SAML Single Sign On,** click **Enable SAML SSO.**

   You have now successfully enabled SAML SSO using G Suite in PAM360.

Configuring SAML Single Sign-On (SSO) for Active Directory Users

Typically, user accounts imported from Active Directory (AD) into PAM360 will have their login names stored in the following format: **Loginname**. Therefore, when you set up SAML Single Sign-on (SSO) for AD users, you can set the Windows account name as the incoming claim type to match the default login format. However, if you have created local PAM360 accounts for your AD users by importing them using a CSV file, you must select a different claim type that matches the login name format stored in PAM360.

This method will work for all types of SAML SSO identity providers. As an example, we have provided the steps to configure this in the Azure AD portal.

Consider the following scenario:
Let's assume you need to configure Azure AD SAML SSO for users imported from Active Directory. In this case, the default login name of the AD users will be in the format Loginname. During an Azure SAML response, PAM360 retrieves a user's email address as their login name. This login name format mismatch creates a conflict during the Azure AD SAML SSO process, preventing the authentication process from being complete. Furthermore, this makes it difficult for administrators to implement Azure AD SAML SSO as a viable SAML authentication method for AD users. To overcome this challenge, create a custom attribute in your AD and add the 'Loginname' value in the custom attribute section to sync it with the Azure AD portal. This can be achieved in three simple steps:

1. **Set up a custom attribute**
2. **Set up a claim in the Azure portal**
3. **Edit the system properties file and complete the configuration**

1. Set up a Custom Attribute

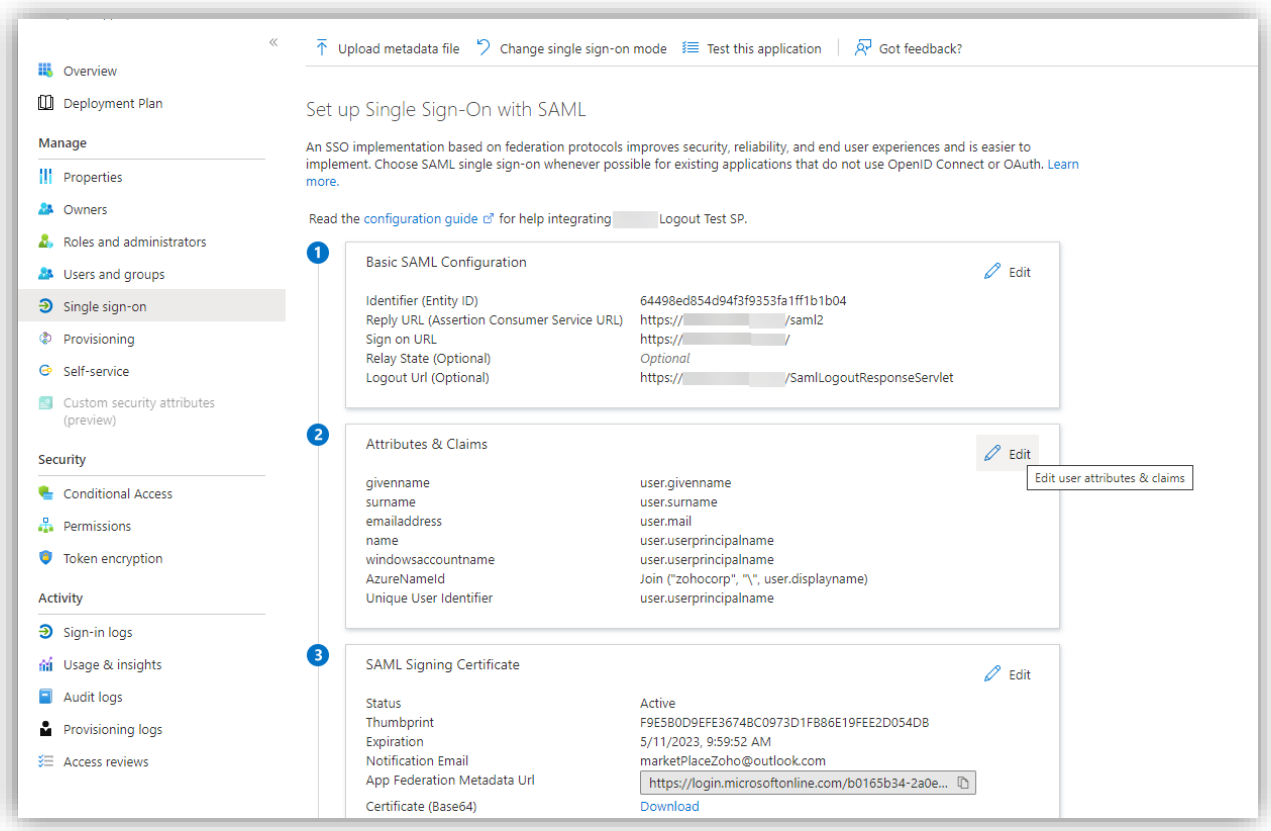
1. In your Active Directory portal, go to the OU which the required users are a part of and go to Properties.
2. Here, under **Attribute Editor,** find the custom attribute that will be in the format: **Loginname**. If it is not already available, then create a new entry. This attribute must be added as a parameter in the Azure portal.
3. Save and apply changes.

2. Set up a Claim in the Azure Portal

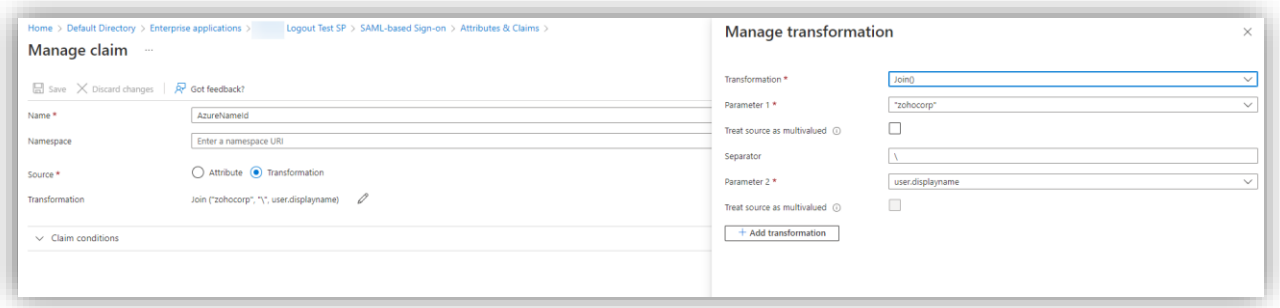
Once you have added the custom attribute, proceed with the below steps to set up a claim for

the NameID in the Azure AD Portal.

1. In the Azure AD portal, go to the PAM360 enterprise application. Here, create a new user attribute to match the username in PAM360.
2. Login to the Azure AD portal and navigate to the **Enterprise Application.**
3. Click the PAM360 SSO APP. Click the edit icon in the **User Attribute & Claims** and create a new user attribute to match the username in PAM360.



4. In the **Manage claim** window, enter the following attributes:
    i. In the Name field, enter the name that needs to be customized - AzureNameId. This same name must be added as the SAML attribute in the system properties in the below step.
    ii. Under **Manage transformation**, enter Transformation value, and enter the domain name as Parameter 1 and the custom attribute you set up in the below step as Parameter 2. Save your changes.



3. Edit the System Properties File and Complete the Configuration

Once you create the new user attribute in the Azure AD portal for the PAM360 Enterprise application, follow the below steps for the custom attribute configuration to be complete:

1. Stop the PAM360 service.
2. Rename the logs file as 'logs.old'.
3. Open system_properties.conf file found in the <PAM360_installation_directory\conf> folder. Scroll down to the bottom and add a new entry **saml.attribute.nameId=AzureNameId**. The nameId mentioned here must be the same as the one added in the Manage claim window. Save the file.

Now, the custom attribute configuration is complete. Start the PAM360 service and configure Azure AD SAML SSO as usual.

Setting up Two-Factor Authentication (TFA)

PAM360 stores sensitive administrative passwords of enterprise resources in encrypted form in the database. Access to the data was earlier restricted by a single level of authentication - local authentication of PAM360 or the authentication of third party identity stores like ActiveDirectory or LDAP.

To introduce an extra level of security, PAM360 provides two-factor authentication. Users will have to authenticate through two successive stages to access the PAM360 web-interface. While the first authentication will be through the usual native authentication or AD / LDAP, the second level of authentication could be one of the following:

- Leveraging PhoneFacotor - a phone-based authentication service
- Leveraging RSA SecurID authentication as the second level of authentication
- A one-time, randomly generated unique password sent by PAM360 to the user by Email
- Google Authenticator
- RADIUS server or Any RADIUS-compliant Authentication
- Duo security
- YubiKey
- Microsoft Authenticator
- Okta Verify Authenticator

This document explains about the following topics:

1. Two-Factor Authentication Options
2. Enable Two-Factor Authentication
3. Reset Two-Factor Authentication

1. Two-Factor Authentication Options

Before enabling the Two-Factor Authentication, decide on the technology you wish to use. At present PAM360 supports TFA through the following options:

1. PhoneFactor Authentication
2. RSA SecurID
3. Google Authenticator
4. Microsoft Authenticator
5. Okta Verify TFA
6. RADIUS server or Any RADIUS-compliant Authentication

7. **Duo security TFA**
8. **YubiKey**
9. **One time password through Email**

Check below the desired help section to know more and proceed setting up the required TFA technology.

2. Enable Two-Factor Authentication

Enabling Two-Factor Authentication in PAM360 consists of two steps:

1. Setting up Two-Factor Authentication.
2. Specifying users for whom the Two-Factor Authentication is to be enforced.

> **Note:** Two-Factor Authentication will take effect only if both the two steps are performed. Also, Two-Factor Authentication will be applicable only for the users for whom it is enforced through Step 2. All other users will be allowed to login to PAM360 through the usual way.

3. Reset Two-Factor Authentication

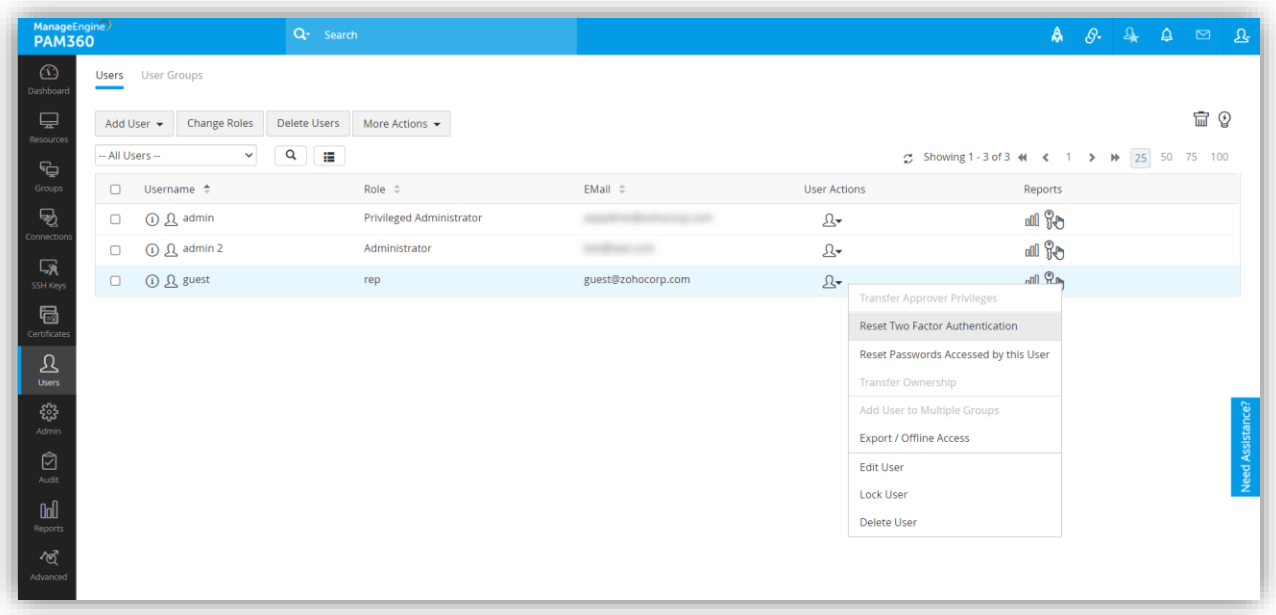
(This feature is applicable from build 5304 and later only)

> **Note:** This feature is available only for **Google Authenticator, Microsoft Authenticator, Yubikey** and **Okta Verify**.

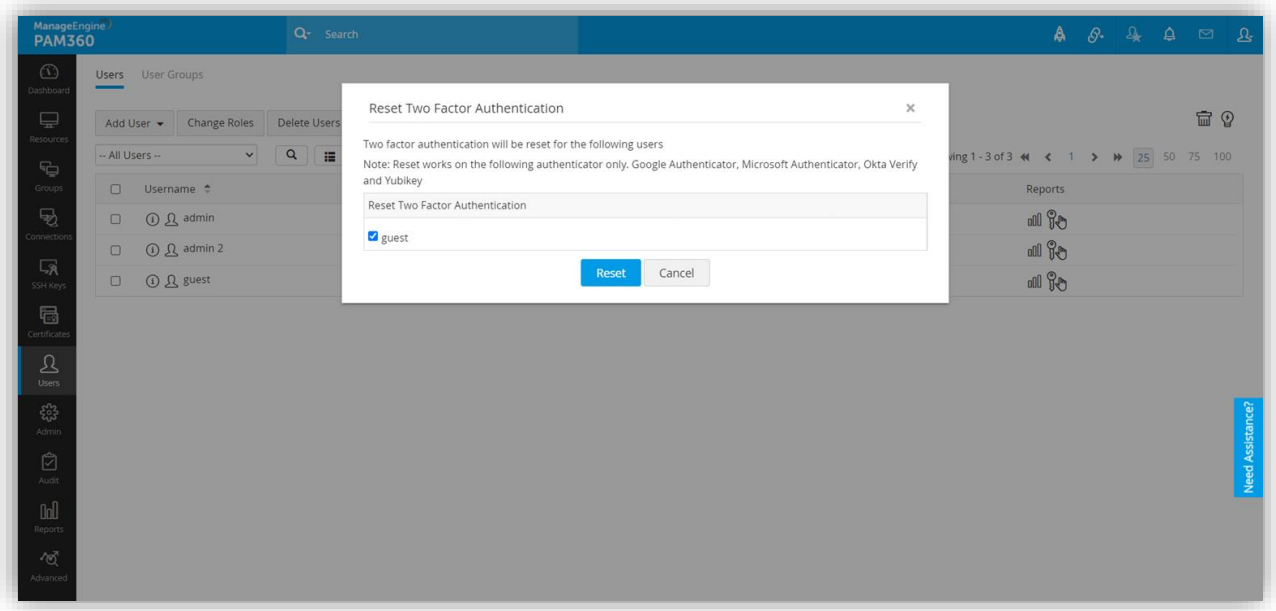
PAM360 now allows administrators and users with appropriate permissions to reset Two-Factor Authentication.

To reset Two-Factor Authentication for a particular user,

1. Log in to PAM360 as an Administrator and navigate to the **Users** tab.
2. Click the **User Actions** icon beside the desired user and click **Reset Two Factor Authentication.**



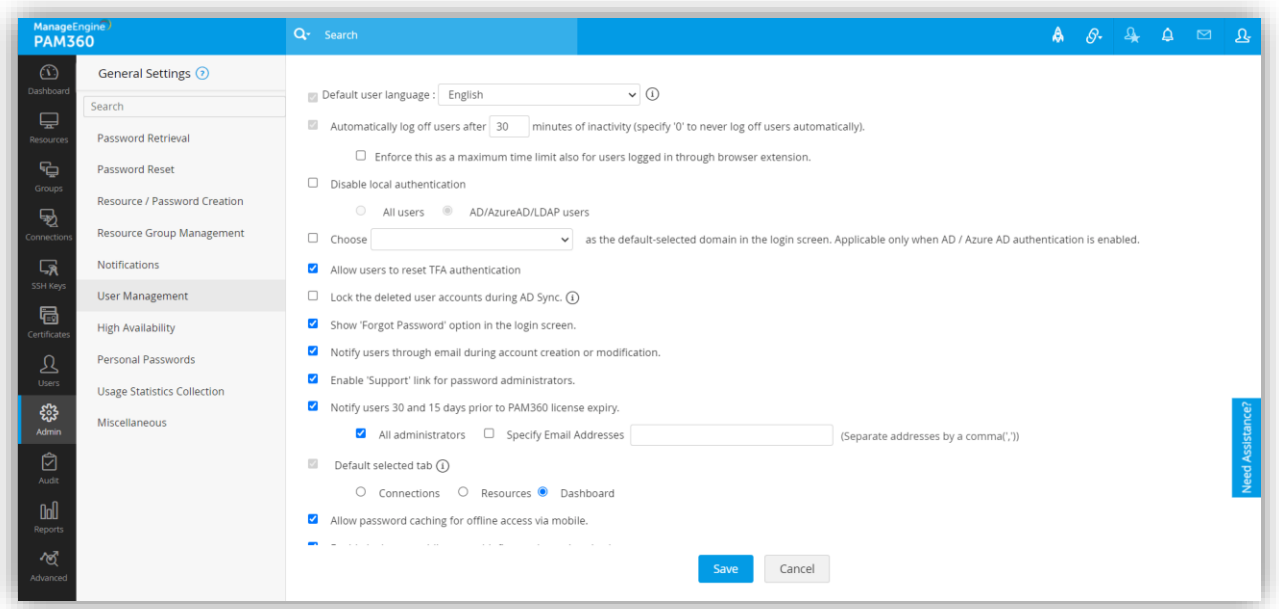
3. Click **Reset** in the pop-up that appears.



Now, the user will be able to reconfigure Two-Factor Authentication while logging in to PAM360.

To allow users to reset Two-Factor Authentication,

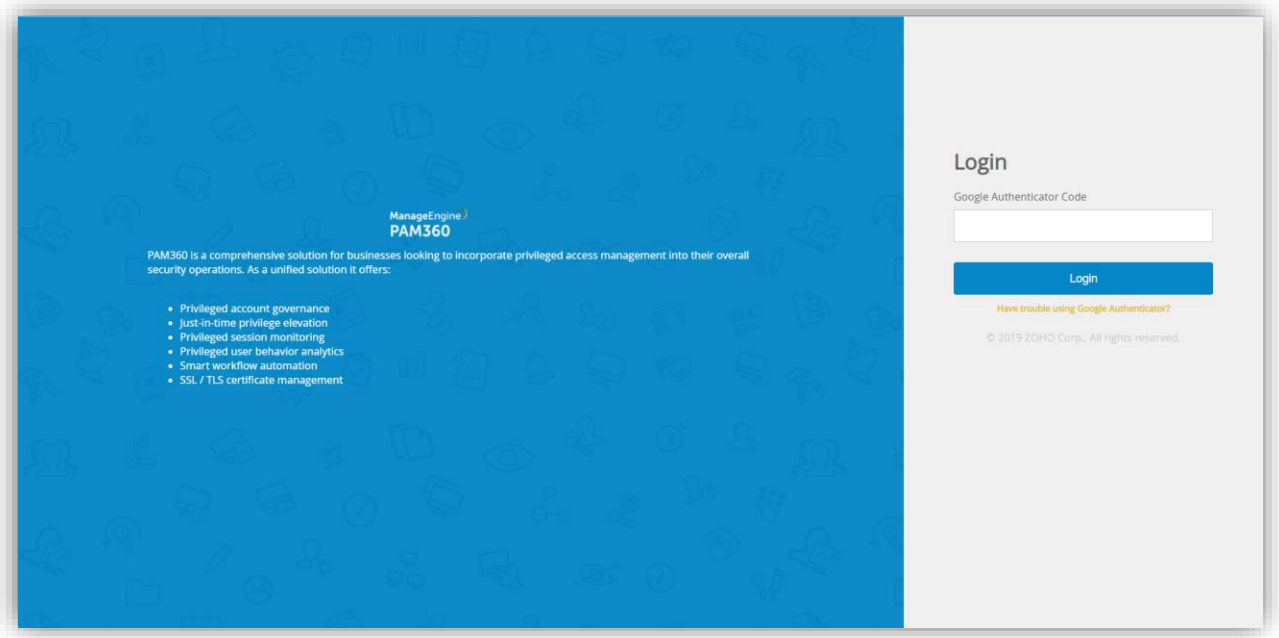
1. Log in to PAM360 as an Administrator and navigate to **Admin >> Settings >> General Settings >> User Management.**
2. Select **Allow Users to reset Two-Factor Authentication** and click **Save.**



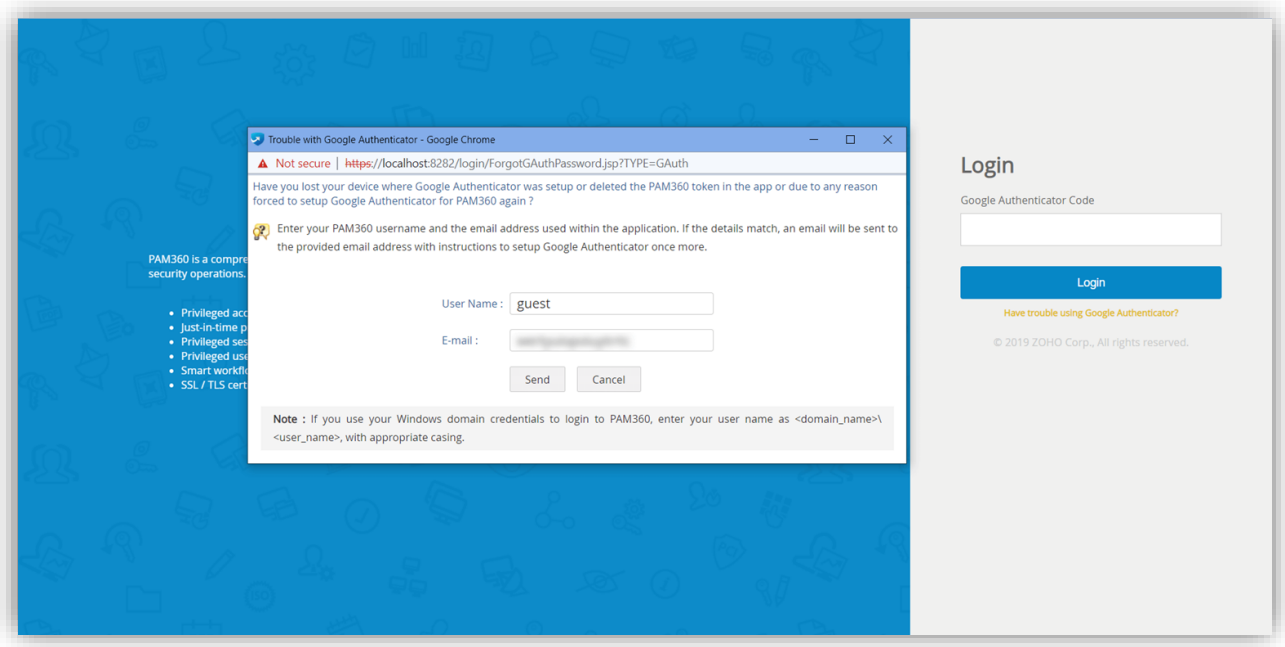
This allows the users to reset and reconfigure Two-Factor Authentication by themselves.

To reset Two-Factor Authentication as a user,

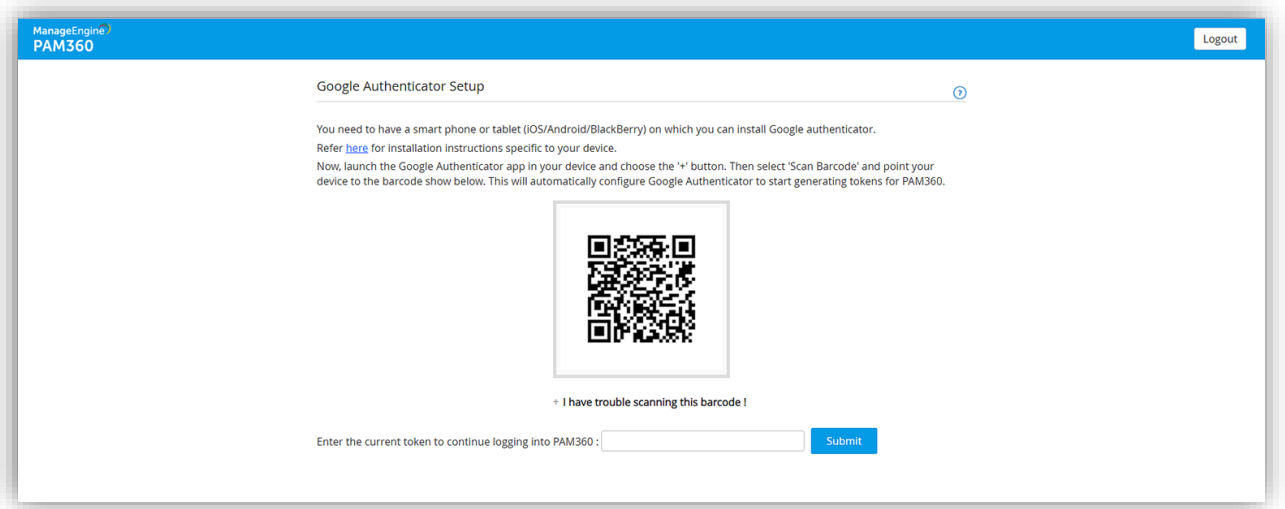
1. Mention the **Username** and **Password** to log in to PAM360.
2. Click **Having trouble using <enabled TFA>?**
   (**Example:** *Having trouble using Google Authenticator?*)



3. In pop-up that appears, mention the **User Name, E-mail** Id and click **Send.**



4. A link to set up Two-Factor Authentication will be sent to the above mentioned **E-mail** Id.
5. Now, open the E-mail and click the link to reset Two Factor Authentication. A success message appears on the screen.
6. Now, log in to PAM30 and you will be able to reconfigure your Two-Factor Authentication.



Setting up Two-Factor Authentication (TFA) - PhoneFactor Authentication

ManageEngine has partnered with PhoneFactor, the leading global provider of phone-based TFA, to enable simple, effective two-factor security for PAM360. ManageEngine is a PhoneFactor Alliance Partner and offers seamless integration with PhoneFactor's authentication services.

PhoneFactor works by placing a confirmation call to your phone during the login process. Upon completing your first authentication through usual means and when you go to the second authentication stage, you simply need to answer your phone and press # (or enter a PIN), which serves as the phone-based authentication.

The following topics are discussed in this document:

1. How does PhoneFactor Work with PAM360?
2. Sequence of Events
3. Enabling PhoneFactor Authentication
    - 3.1 Prerequisite
    - 3.2 Setting up TFA in PAM360
    - 3.3 Deciding the type of PhoneFactor Authentication
        - 3.3.1 Configurations in PhoneFactor Agent
        - 3.3.2 Configurations in PhoneFactor Direct SDK
    - 3.4 Enforcing TFA for the Required Users
4. Connecting to PAM360 Web-Interface when TFA through PhoneFactor is Enabled
5. Workflow

1. How Does PhoneFactor Work with PAM360?

You will be specifying the phone numbers for your users, which results in a mapping between the users and the corresponding phone numbers. In PhoneFactor agent mode, the details about the user, including the phone numbers are maintained at the agent. In Direct SDK mode, the phone numbers are maintained in PAM360 database itself. When a user tries to login to PAM360, PhoneFactor finds out the phone number of the respective user and triggers a call.

2. Sequence of Events

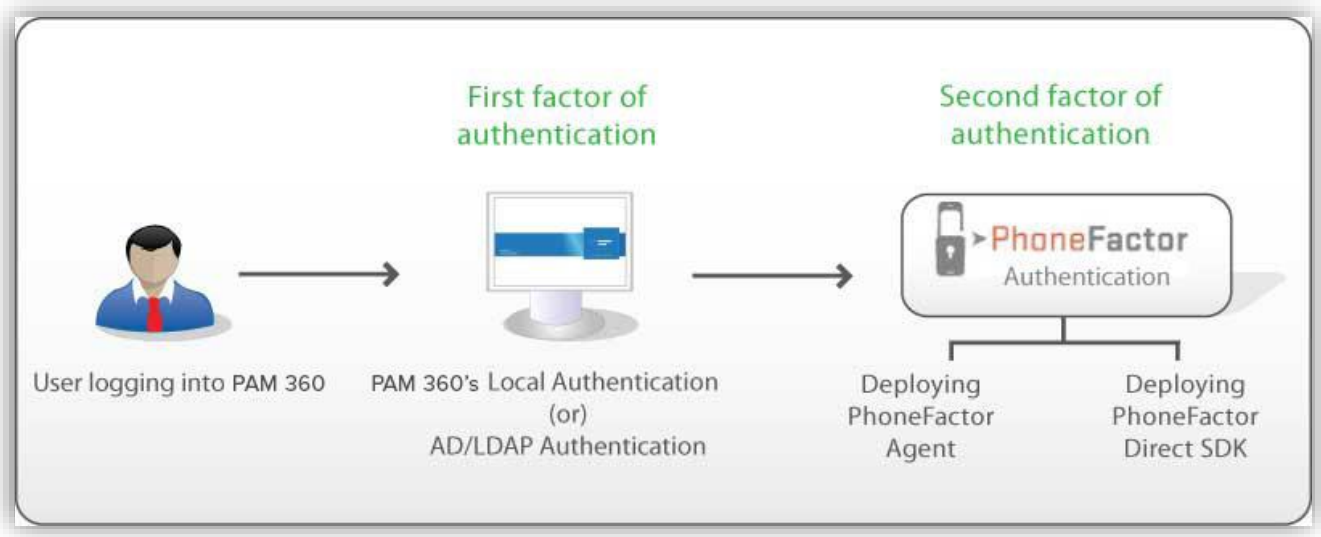
1. A user tries to access PAM360 web-interface.

2. PAM360 authenticates the user through Active Directory or LDAP or locally.
3. PAM360 prompts for the second factor credential through PhoneFactor.
4. PhoneFactor calls you. Answer the call and press # or enter a PIN.
5. PAM360 grants the user access to the web-interface.

3. Enabling PhoneFactor Authentication

3.1 Prerequisite

Prior to enabling PhoneFactor authentication, you need to buy PhoneFactor. Refer to PhoneFactor website for details. After getting PhoneFactor, you need to decide about the specific authentication method - whether you want to install PhoneFactor agent in your environment or deploy PhoneFactor Direct SDK.



3.2 Setting up TFA in PAM360

1. Navigate to **Admin >> Authentication >> Two-factor Authentication**.
2. Choose the option **PhoneFactor**.
3. Click **Save**.

> **Note:** Before proceeding further, ensure that you have entered the phone numbers for all the users for whom you wish to enable TFA through PhoneFactor in PAM360. You can enter a landline number or a mobile number as the primary contact number for PhoneFactor authentication.

Landline numbers should be entered in the following format:

<Country Code> <Phone Number with Area Code> <Extension Number, if any>

Example: 1 9259249500 292

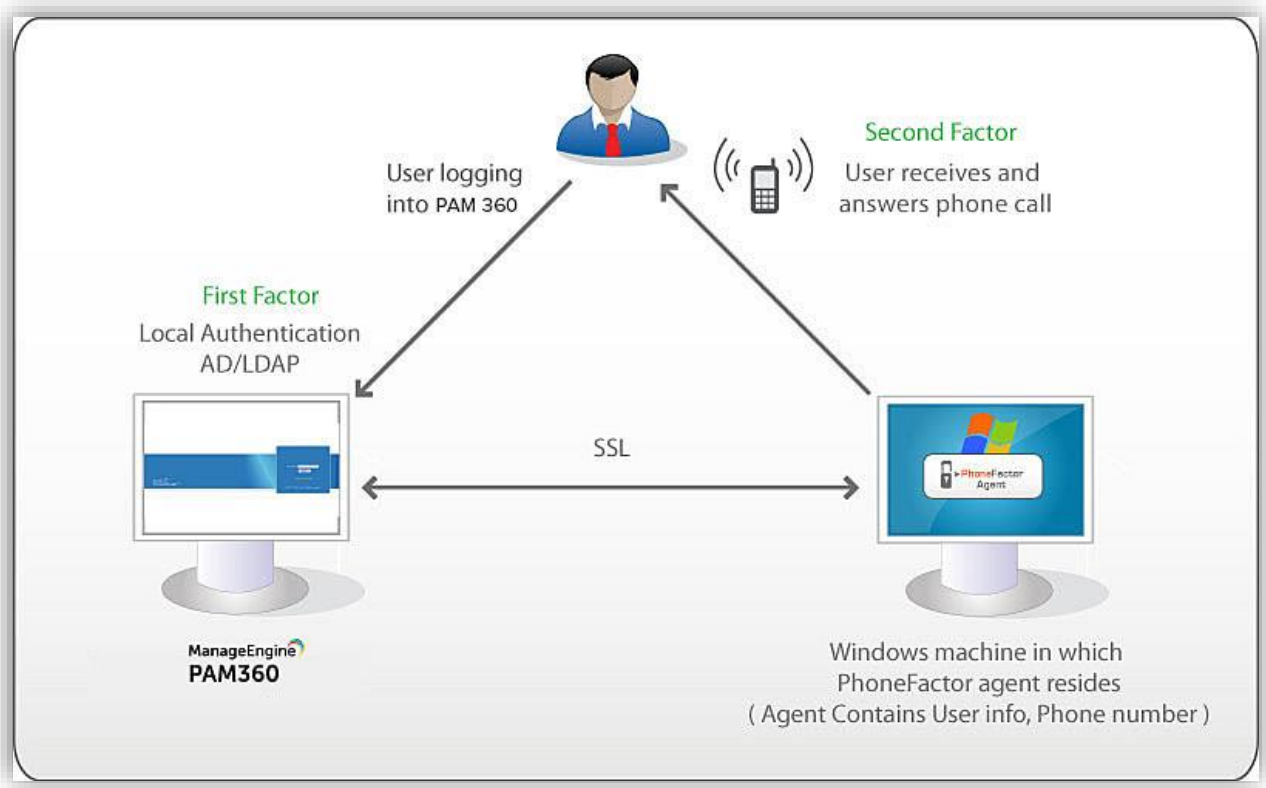
Mobile numbers should be entered in the following format:

<Country Code> <Mobile Number>

3.3 Deciding the type of PhoneFactor Authentication

You can choose to deploy PhoneFactor Agent or PhoneFactor Direct SDK.

Note: Among the two choices, PhoneFactor agent supports entering a PIN for authentication while answering the phone call from PhoneFactor. In Direct SDK mode, users will just be prompted to enter the # key and not a PIN.



3.3.1 Configurations in PhoneFactor Agent

The PhoneFactor agent runs on a Windows server within your network. It includes a configuration wizard that guides you through the setup process for securing PAM360 with PhoneFactor. The PhoneFactor agent can also integrate with your existing Active Directory or LDAP server for centralized user provisioning and management. All user data is stored within the corporate network for additional security. Extensive logging is available for reporting and auditing.

Obtain and install the PhoneFactor Agent and Web Services SDK on a Windows server within your network. The wizard will guide you through the installation process.

1. Configurations in PhoneFactor

> **Note:** If you have already installed PhoneFactor agent, skip this step and directly proceed to Step 2.

i. After installing the agent, make sure you add all the PAM360 users and their phone numbers (maintained in the PhoneFactor agent) to PAM360. You can also integrate Active Directory / LDAP with PhoneFactor agent and automatically import users. If you have users authenticated through PAM360's local authentication, add them to PhoneFactor manually providing details about the phone number.
ii. While adding users in the PhoneFactor agent, take care to provide the same username as available in PAM360. (In PAM360, you would have provided a 'PhoneFactor username' for the users who will be authenticated by PhoneFactor. Take care to enter the same username here in PhoneFactor agent configuration)
iii. After importing users, check if the phone numbers have been entered in the correct format.

> **Important Note:** User information and their phone numbers are maintained in PhoneFactor agent. That means, users will receive the call only at the phone numbers specified in the agent. Whenever, you want to modify the phone number, you need to carry out the change at the agent. Similarly, whenever you add new users to PAM360 and if TFA through PhoneFactor is enabled for them, you need to add the user in PhoneFactor agent too. Otherwise, TFA through PhoneFactor will not work.

2. Configurations in PAM360

i. In the Two-Factor Authentication console in PAM360, select the Authentication Method as **PhoneFactor Agent.**
ii. Enter the credentials to access the PhoneFactor. You need to enter the user name, password and the URL of the host where the PhoneFactor agent is running

iii. Communication between PAM360 and the host where the PhoneFactor agent is running takes place through SSL. So, you need to import (into PAM360) the SSL certificate, which you specified while installing the Web Services SDK.

While installing the PhoneFactor agent/ Web Services SDK, you would have either created a self-signed SSL certificate or you would have used an already available internal certificate (your own certificate). Here, in PAM360, you need import the root of the CA. **If you are using a certificate signed by third-party CA, you may skip this step.**

If you have configured PAM360 High Availability, Configurations in PAM360 Secondary: (PhoneFactor Agent Mode)

If you have configured High Availability in PAM360 and if you chose to deploy PhoneFactor Agent, you need to carry out the following configuration in PAM360 Secondary server. Just as you imported the root of the CA as explained below, you need to do the same in the PAM360 secondary. **If you are using a certificate signed by third-party CA, you may skip this step.**

Steps to Import the Root of the CA:

1. Navigate to **PAM360_Installation_Folder>/bin** directory
2. Execute **importPhoneFactorCert.bat** (in Windows) or**importPhoneFactorCert.sh** (in Linux) **as follows**

   (In Windows)

   In the case of Self-Signed certificates

   importPhoneFactorCert.bat <absolute path of the Self-signed certificate>

   In the case of your own certificates or already available internal CAs

   importPhoneFactorCert.bat <absolute path of the root of the CA>

   (In Linux)

   In the case of Self-Signed certificates

   sh importPhoneFactorCert.sh <absolute path of the Self-signed certificate>

   In the case of your own certificates or already available internal CAs

   sh importPhoneFactorCert.sh <absolute path of the root of the CA>
3. Restart PAM360 server
4. Once you execute the above, the root of the CA will be recorded in PAM360. All the certificates signed by the particular CA will henceforth be automatically taken.
5. Proceed to Step 3 - Enforcing Two-Factor Authentication for required users in PAM360.

Note: If your enterprise network setup requires connecting to the internet via a proxy server, you need to configure the proxy settings to enable PAM360 connect to PhoneFactor website. **(PAM360 console >> Admin >> General >> Proxy Server Settings)**

3.3.2 Configurations in PhoneFactor Direct SDK

Instead of using the Agent, you can also use PhoneFactor Direct SDK, which can be used to integrate with PAM360 and it leverages PAM360's existing user database.

1. Configurations in SDK

PhoneFactor jars have been bundled with PAM360. So, it is enough if you buy PhoneFactor and supply the license details as explained in Step 2 below.

2. Configurations in PAM360

i. Include phone numbers for all the users for whom you wish to enable TFA through PhoneFactor in PAM360. The phone numbers should be entered in proper format. In sharp contrast to PhoneFactor agent where the phone numbers of the users are recorded and maintained at the agent, in the case of Direct SDK, phone numbers are maintained at PAM360 itself.
ii. In the PhoneFactor console, specify the path of PhoneFactor license file, PhoneFactor Certificate and Private Key password. (These files will be present under the PhoneFactor SDK folder.)
iii. Proceed to Step 3 - Enforcing two-factor Authentication for required users in PAM360.

Note: If your enterprise network setup requires connecting to the internet via a proxy server, you need to configure the proxy settings to enable PAM360 connect to PhoneFactor website. **(PAM360 console >> Admin >> General >> Proxy Server Settings)**

If you have configured PAM360 High Availability, Configurations in PAM360 Secondary: (PhoneFactor Direct SDK Mode)

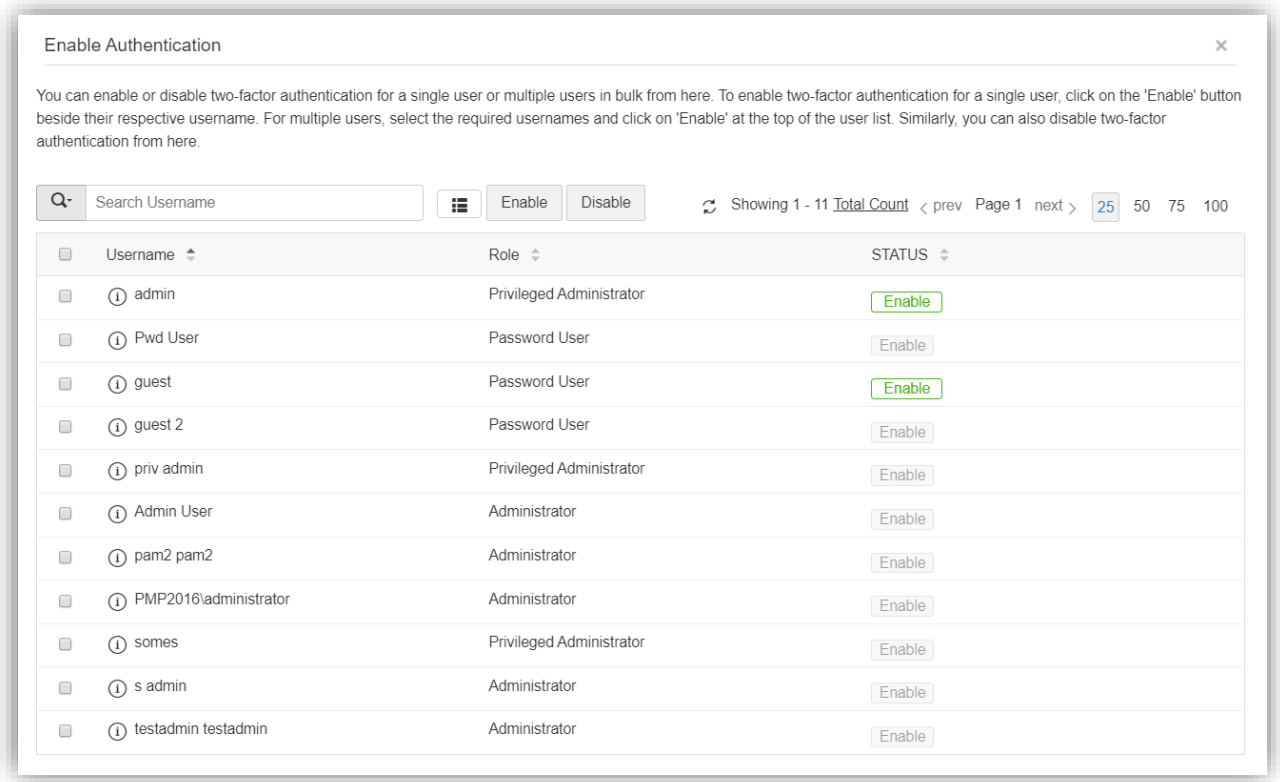
If you have configured High Availability in PAM360 and if you have chosen to PhoneFactor Direct SDK mode, perform the following configurations in the PAM360 Secondary server:

1. Go to **<PAM360-Primary-Installation>/licenses** folder.
2. Copy the files **license.xml** and cert.p12.

3. Now go to **<PAM360-Secondary-Installation>/licenses** folder.
4. Paste the two files.

3.4 Enforcing TFA for the Required Users

1. Once you confirm the PhoneFactor as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom TFA should be enforced.
2. Enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click on the **Enable** button beside their respective username. For multiple users, select the required usernames and click on **Enable** at the top of the user list. Similarly, you can also **Disable** TFA from here.



3. You can also select the users later by navigating to **Users >> More Actions >> Two-Factor Authentication.**

4. Connecting to PAM360 Web-Interface when TFA through PhoneFactor is Enabled

1. The users for whom TFA is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PAM360's local

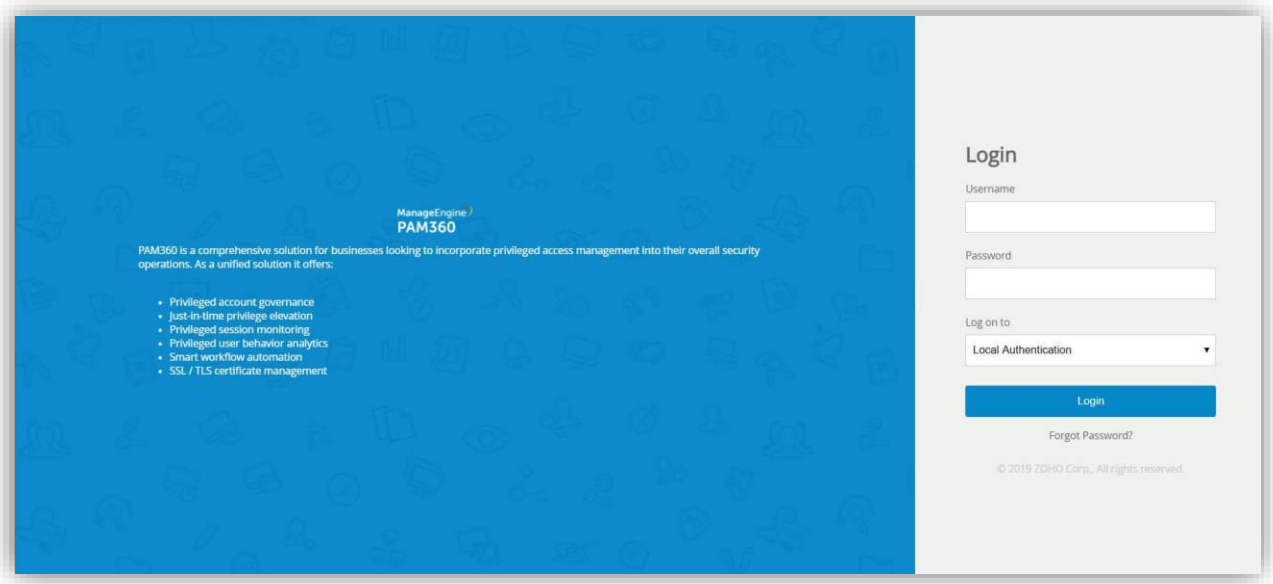
authentication or AD/LDAP authentication.

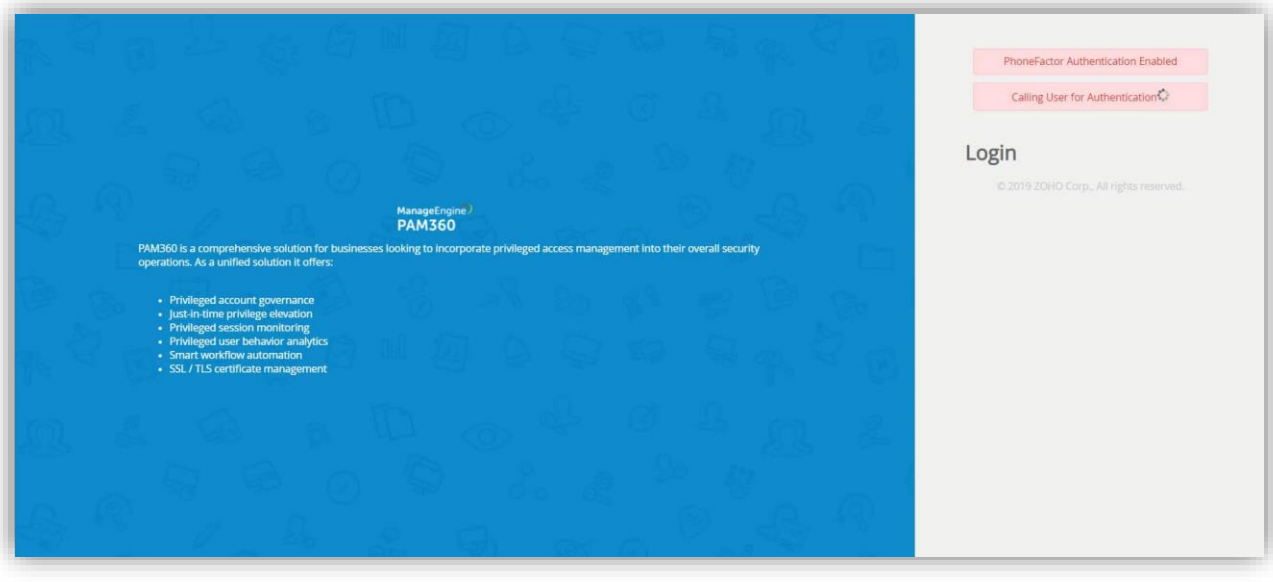
2. When TFA is enabled, the login screen will ask for the username alone in the first UI. The users will be prompted to enter the passwords only in the second step.

5. Workflow (TFA using PhoneFactor)

If the administrator has chosen TFA through PhoneFactor, the TFA will happen as detailed below:

1. Upon launching the PAM360 web-interface, the user has to enter the username to login to PAM360 and click **Login**.
2. Against the text field **Password**, the user has to enter the local authentication password or AD/LDAP password as applicable.





3. Once the authentication through the first factor is successful, you need to await a call to your phone from the PhoneFactor
4. Answer the call and press # key or enter the PIN as instructed. PhoneFactor will take care of authentication.

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) **AND** if you have configured high availability, you need to restart the PAM360 secondary server once.

Setting Up Two-Factor Authentication (TFA) With RSA SecurID

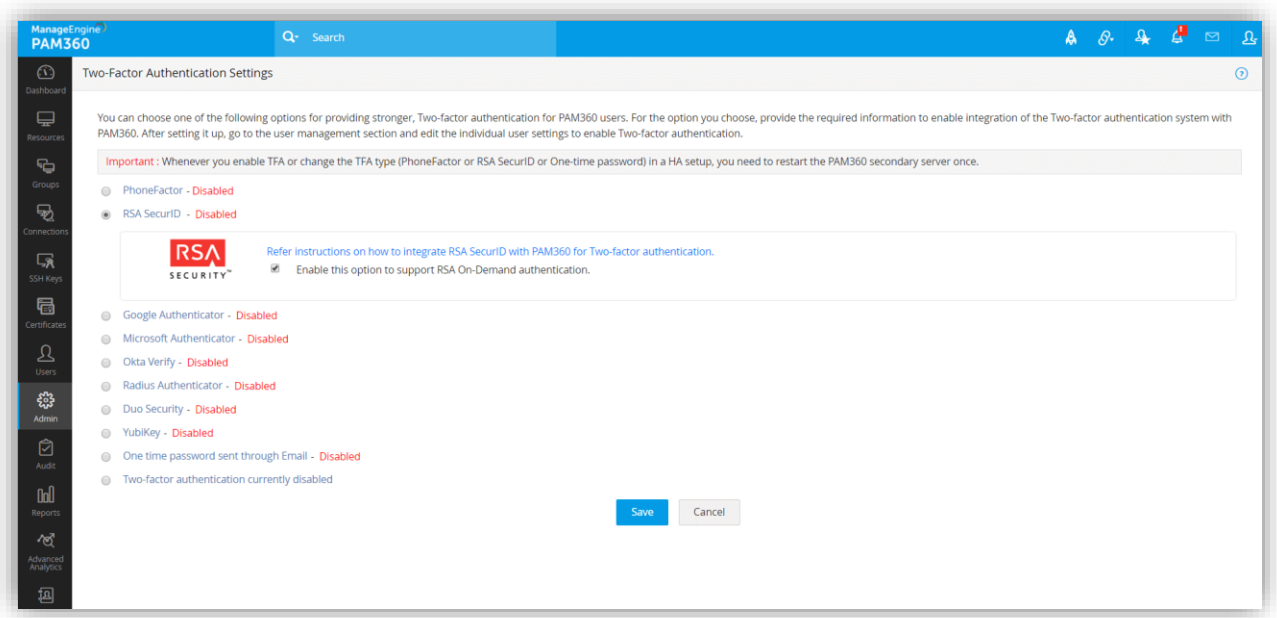
You can set up two-factor authentication (TFA) with RSA SecurID in PAM360 if you have RSA Authentication Manager and RSA SecurID Appliance in your environment. This will help you leverage RSA SecurID's authentication factor as the second layer of security for your login.

Following are the steps to set up TFA with RSA SecurID in PAM360:

1. Configuring TFA in PAM360
2. Integrating RSA SecurID with PAM360
3. Enforcing TFA for required users
4. Connecting to PAM360's web-interface when TFA is enabled

1. Configuring TFA in PAM360

1. Navigate to **Admin >> Authentication >> Two-factor Authentication.**
2. Choose the option **RSA SecurID** and click **Save**. Administrators can also enable RSA On-Demand authentication, by selecting the **On-Demand authentication** check-box.



3. Then, click **Confirm** to enforce RSA SecurID as the second factor of authentication.

2. Integrating RSA SecurID with PAM360

You can integrate RSA SecurID with PAM360 by following the below steps:

1. Register the PAM360 server as an Agent Host in the RSA Authentication Manager.
2. Generate RSA Authentication Manager configuration file, or sdconf.rec in RSA manager. Copy and paste the sdconf.rec to the **<PAM360_SERVER_HOME>\bin** directory. In addition, if a node secret file (securid) exists, copy and paste that as well.
3. In the RSA Authentication API configuration file (rsa_api.properties), edit the "RSA_AGENT_HOST" property value as PAM360's server hostname or IP address. This file will be located in the default application directory (**<PAM360_SERVER_HOME>\bin**).

> **Note:** If you are using PAM360's high availability feature, you need to carry out the above steps in the secondary server installation as well.

Mapping PAM360 users to RSA Authentication Manager:

Before the second factor authentication can take place, use the RSA Security Console to enter all desired PAM360 users into RSA Authentication Manager, assign tokens to them and activate them on the appropriate Agent Host.

Ensure that the user name in RSA Authentication Manager and the corresponding user name in PAM360 are the same. For an already existing RSA user, in case there is a user name mismatch between PAM360 and RSA Authentication Manager, you can map the correct user name in PAM360 by editing the user properties in PAM360.

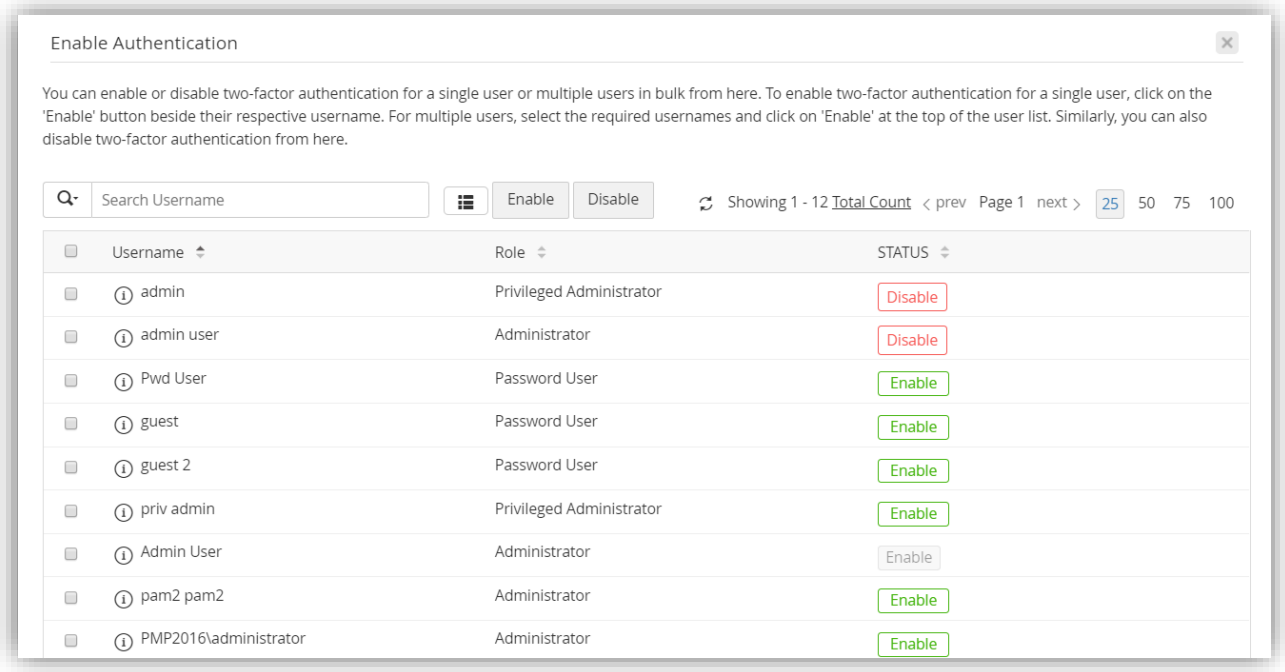
For example, if you have imported a user by the name 'ZYLKER\rob' from Active Directory into PAM360 and in RSA Authentication Manager, the username is recorded as 'rob', there will be a mismatch. To avoid that, you can edit the user name in PAM360 and get the name 'ZYLKER\rob' mapped to 'rob')

The following sequence describes the authentication process between PAM360 and RSA SecurID:

1. When user first tries to access PAM360, authentication is done through ActiveDirectory or LDAP or locally.
2. PAM360 prompts the user for a username and the RSA SecurID passcode, both of which are sent to the RSA Authentication Manager through the RSA Runtime API.
3. RSA Authentication Manager then authenticates the user and returns a message to PAM360.
4. PAM360 grants the user access to the requested resource.

3. Enforcing TFA for Required Users

1. Once you confirm RSA SecurID as the second factor of authentication, in a new pop-up window, you will be prompted to select users for whom TFA should be enforced.
2. You can enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click **Enable** beside the respective username. For multiple users, select the required usernames and click **Enable** at the top of the user list. Similarly, you can also **Disable** TFA from here.



3. You can also select the users later by navigating to **Users >> More Actions >> Two-factor Authentication.**

4. Connecting to PAM360's Web-Interface when TFA is Enabled

The users who have TFA enabled for their accounts will have to authenticate twice successively during login. As mentioned above, the first level of authentication will be through PAM360's local authentication or AD/LDAP authentication. Depending on the type of TFA chosen by the administrator, the second level of authentication will differ as explained below:

1. Upon launching the PAM360 web-interface, the user has to enter the username and local authentication or AD/LDAP password to login to PAM360 and click **Login**.
2. Against the text field **RSA Passcode**, enter the RSA SecurID passcode. The passcode could be a combination of PIN and Tokencode or just the Tokencode alone or the On-Demand PIN depending on the configuration done in RSA Authentication Manager.
3. If you want to leverage the RSA On-Demand authenticator, select **RSA On-Demand** and proceed. In this case, you need to provide the On-Demand Tokencode as specified in

case 3 below.

4.1. Three different scenarios possible while logging into PAM360 using RSA SecurID

Case 1: Entering user generated / system created PIN

As mentioned above, the RSA passcode could be a combination of PIN and tokencode or just tokencode alone or a password depending on the configuration done in RSA Authentication Manager. If the settings in RSA Security Console demands the users to create a PIN on their own or use a system generated PIN, the following options would be shown to the users after step 2 (that is, after entering the first password and RSA tokencode to log in to PAM360).

User Created PIN:

In the case of user created PIN, users will get the option to enter the PIN on their own. The PIN should contain numeric characters - minimum of 4 and a maximum of 8 characters. After entering the PIN, the user will have to wait for a while until the RSA tokencode changes to a new value. Then, in the next screen, enter the new PIN and the RSA tokencode to authenticate.

System Created PIN:

In the case of system created PIN, PAM360 itself will randomly generate a PIN and it will be shown on the screen. Users will have to note down the new PIN and wait for a while until the RSA tokencode changes to a new value. Then, in the next screen, the users will have to enter the new PIN as generated by the system and the RSA tokencode to authenticate.

Case 2: New Tokencode Mode

If a user attempts to log in to PAM360 using a random RSA passcode or by guesswork for a specified number of times, the RSA Authentication Manager will turn the screen to the New Tokencode mode to verify whether the user possesses the token. In that case, PAM360 prompts for next tokencode during the login. That means, the user will have to wait until the RSA device shows a new tokencode and the new code to proceed with logging into PAM360.

> **Note:** If the new tokencode entered by the user is wrong, PAM360 will revert to the initial login screen. Users will have to start again by entering the username.

Case 3: Tokencode Mode

When RSA On-Demand authenticator is configured, you need to supply the Tokencode to log into PAM360. Tokencode will be sent to the registered email id or mobile number as configured in the RSA On-Demand authentication system.

Note: If you have configured High Availability, whenever you enable TFA or when you change the TFA service type, you need to restart the PAM360 secondary server once for it to take effect.

Setting up Two-Factor Authentication (TFA) - Google Authenticator

Google Authenticator is a software-based authentication token developed by Google. The token provides an authenticator, which is a six-digit number users must enter as the second factor of authentication.

You need to install the Google Authenticator app on your smart phone or tablet devices. It generates a six-digit number, which changes every 30 seconds. With the app, you don't have to wait a few seconds to receive a text message. Here's how to set up and use the Google Authenticator app with your Google account, along with a few other well-known sites.

Sequence of Events

Following is the sequence of events involved in using Google Authenticator as the second factor:

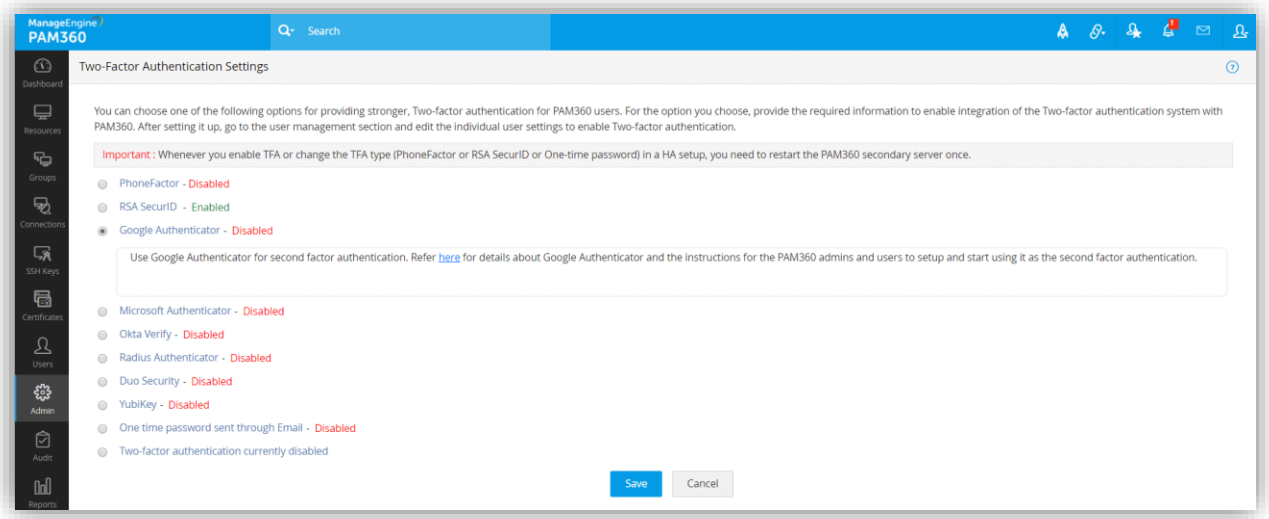
1. A user tries to access PAM360 web-interface.
2. PAM360 authenticates the user through Active Directory or LDAP or locally (first factor).
3. PAM360 prompts for the second factor credential through Google Authenticator.
4. Enter the six-digit token that you see on the Google Authenticator app GUI.
5. PAM360 grants the user access to the web-interface.

Steps Required

1. **Configuring TFA in PAM360**
2. **Enforcing TFA for Required Users**
3. **Connecting to PAM360 Web Interface when TFA via Google Authenticator is Enabled**

1. Configuring TFA in PAM360

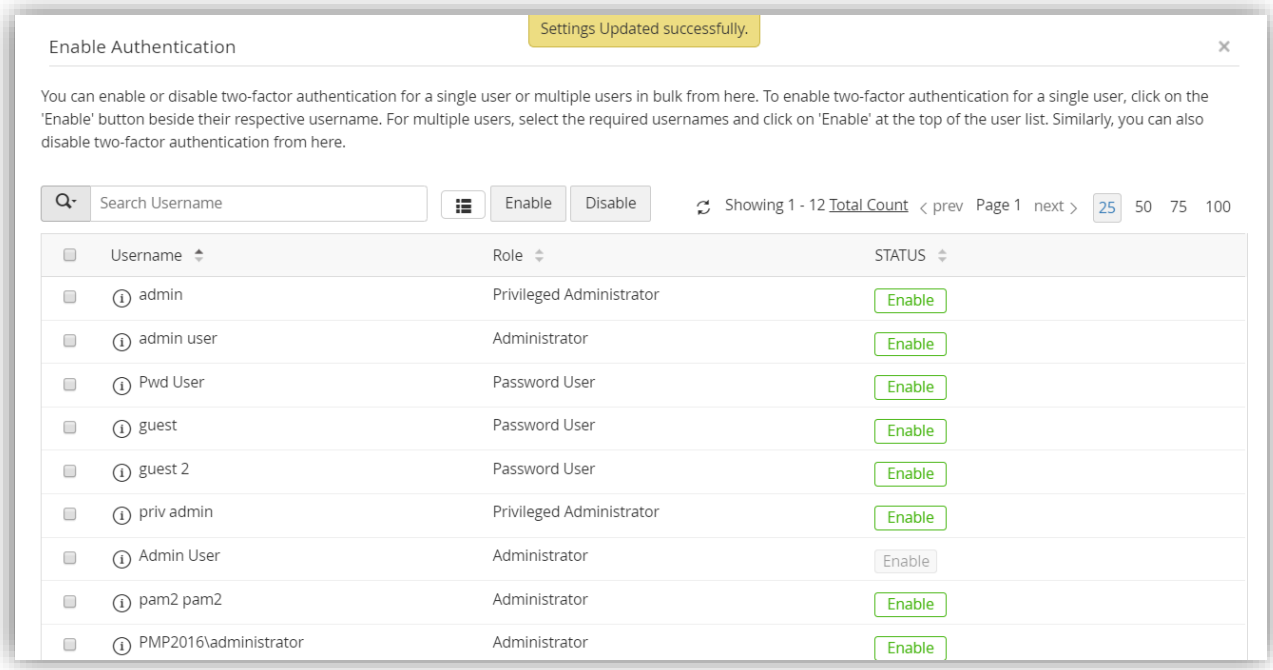
1. Navigate to **Admin >> Authentication >> Two-factor Authentication**.
2. Choose the option **Google Authenticator** and click **Save**.



3. Then, click on **Confirm** to enforce Google Authenticator as the second factor of authentication.

2. Enforcing TFA for Required Users

1. Once you confirm Google Authenticator as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom TFA should be enforced.
2. You can enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click on the '**Enable**' button beside their respective username. For multiple users, select the required usernames and click on 'Enable' at the top of the user list. Similarly, you can also '**Disable**' TFA from here.



3. You can also select the users later by navigating to **Users >> More Actions >> Two-factor Authentication.**

3. Connecting to PAM360 Web Interface when TFA via Google Authenticator is Enabled

Pre-requisite

To make use of google authenticator as the second factor of authentication, you should first install Google Authenticator app in your smart phone or tablet. Google officially supports Android, iPhone, iPad, iPod Touch and BlackBerry devices. Detailed instructions to install the Google Authenticator app is available in Google's website.

Connecting to PAM360 web interface

The users for whom TFA is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PAM360's local authentication or AD/Azure AD/LDAP authentication. If the administrator has chosen the TFA option "Google Authenticator", the TFA will happen as detailed below:

1. Upon launching the PAM360 web-interface, the user has to enter the username and local authentication or Azure AD/AD/LDAP password to log in to PAM360 and click **Login**.
2. **Associating Google Authenticator with your account in PAM360:** When you are logging in for the first time after enabling TFA through Google Authenticator, you will be prompted to associate it with your account in PAM360. You need to first launch the Google Authenticator app in your mobile device/tablet and choose the '+' button. Then, select 'Scan Barcode' and point your device to the barcode shown in the GUI such as the image displayed below. This will automatically configure Google Authenticator to start generating authentication codes for PAM360.
3. After completing this, you can enter the current token for authentication in the text box.

> **Note:** If you had trouble scanning the barcode, the automatic setup will not work. Alternatively, you can carry out the following manual steps in the Google Authenticator app in your device:

4. Choose **Time Based** for your token (this is the default selection in the app).
5. Supply an identifier for your PAM360 account in this format - PAM360: (for ex. PAM360:john@abc.com).
6. Supply the alphanumeric string as the key and select **Done**.

7. Google Authenticator is now setup and it will start generating codes periodically for **<PAM360:user@mailid>**. Enter the current code to continue logging into PAM360.

Troubleshooting Tip

As mentioned earlier, the Google Authenticator is associated with your PAM360 account. If you ever lose your mobile device/tablet OR if you accidentally delete the Google Authenticator app on your device, you will still be able to get tokens to log in to PAM360. In such scenarios, just click the link "Have trouble using Google Authenticator?" in the PAM360 login screen. You will be prompted to enter your PAM360 username and the email address associated with PAM360. You will receive instructions to get Google Authenticator again.

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password or RADIUS or Duo) AND if you have configured high availability, you need to restart the PAM360 secondary server once.

Setting up Two-Factor Authentication (TFA) - Microsoft Authenticator

Microsoft Authenticator is a software-based authentication token developed by Microsoft. The token provides a six-digit number that users must enter as the second factor of authentication. You need to install the Microsoft Authenticator app on your smart phone or tablet devices. It generates a six-digit number, which changes every 30 seconds. With the app, you don't have to wait a few seconds to receive a text message.

Sequence of Events

1. A user tries to access PAM360 web-interface.
2. PAM360 authenticates the user through Active Directory or LDAP or locally (first factor).
3. PAM360 requests for the second factor credential through Microsoft Authenticator.
4. The user has to enter the six-digit token that they see on the Microsoft Authenticator app GUI.
5. PAM360 grants the user access to the web-interface.

This document walks you through the following topics:

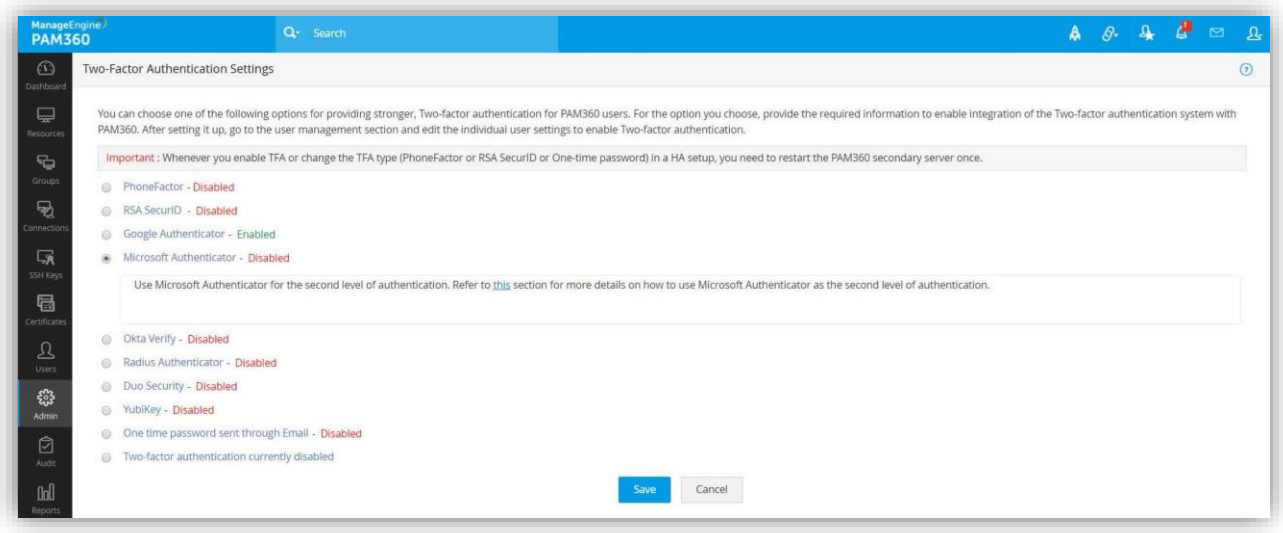
1. **Configuring TFA in PAM360**
2. **Enforcing TFA for the Required Users**
3. **Connecting to PAM360 Web Interface when TFA via Microsoft Authenticator is Enabled**

   3.1 Prerequisite

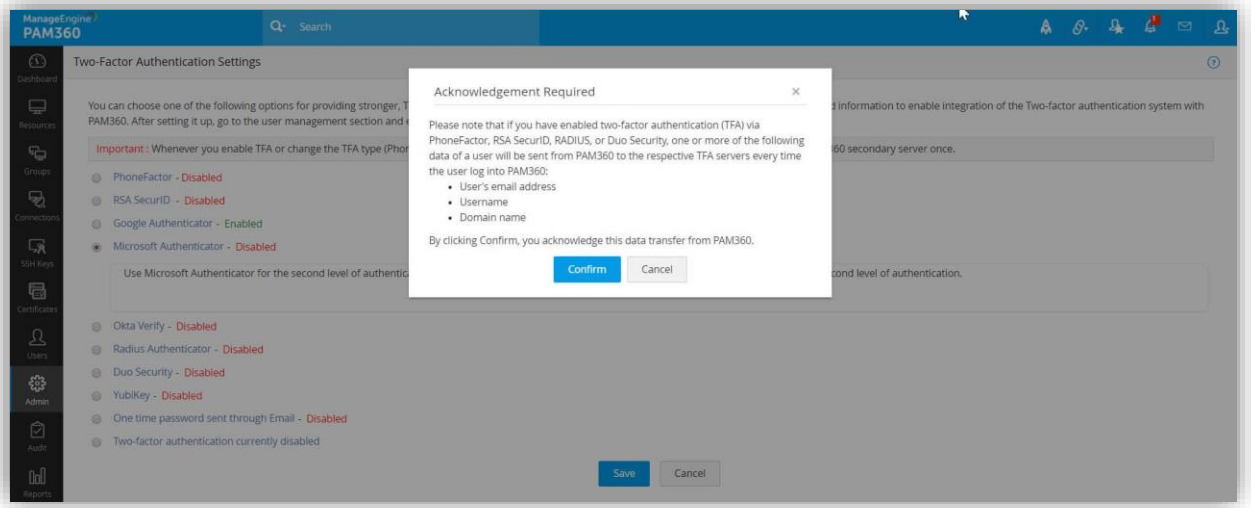
   3.2 Connecting to the PAM360 Web Interface
4. **Troubleshooting Tip**

1. Configuring TFA in PAM360

1. Navigate to **Admin >> Authentication >> TFA.**
2. Choose the option **Microsoft Authenticator**, and click **Save**.

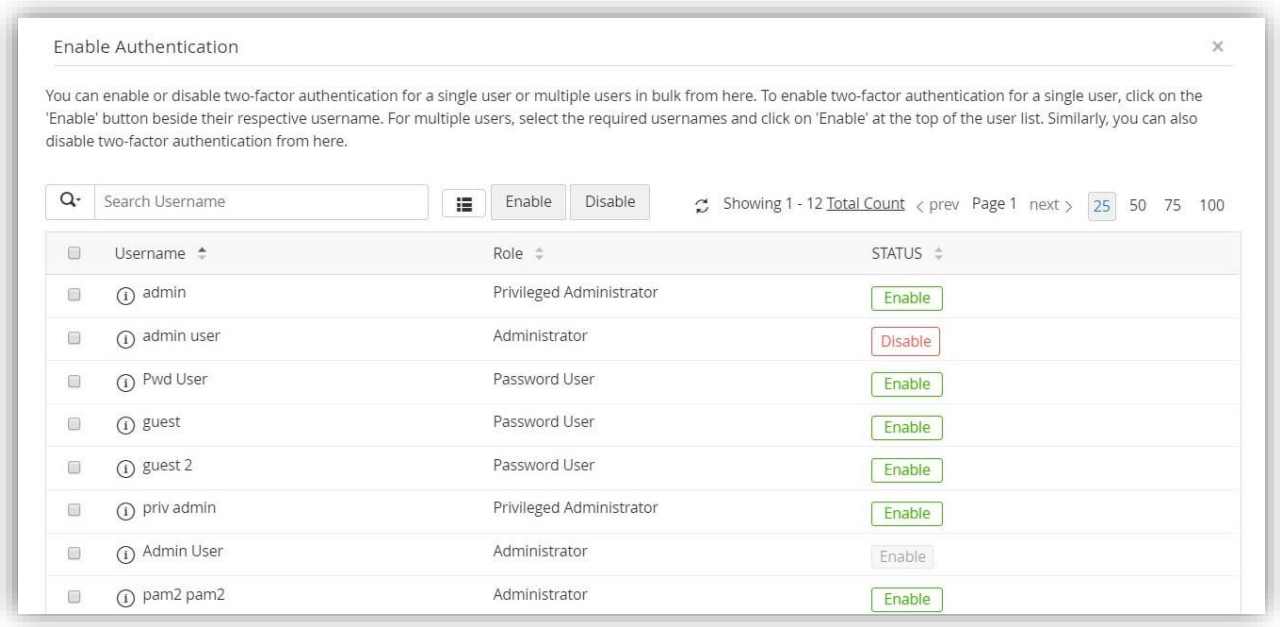


3. Click **Confirm** to enforce Microsoft Authenticator as the second factor of authentication.

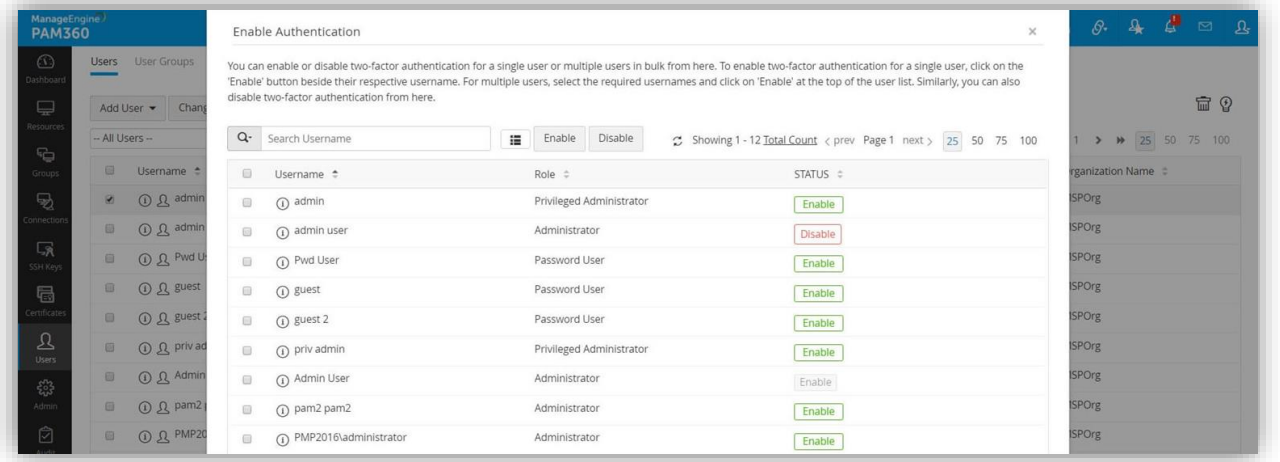


2. Enforcing TFA for the Required Users

1. Once you confirm Microsoft Authenticator as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom TFA should be enforced.



2. You can enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click on the '**Enable**' button beside their respective username. For multiple users, select the required usernames and click on '**Enable**' at the top of the user list. Similarly, you can also '**Disable**' TFA from here.
3. Close the window.
4. You can also select the users later by navigating to **Users >> More Actions >> Two-factor Authentication.**



5. In the window that opens, select the users for whom you want to enforce Microsoft Authenticator TFA.

3. Connecting to PAM360 Web Interface when TFA via Microsoft Authenticator is Enabled

3.1 Pre-requisite

To use Microsoft Authenticator as the second factor of authentication, you should first install the app in your smart phone or tablet.

3.2 Connecting to the PAM360 Web Interface

The users for whom TFA is enabled will have to authenticate twice successively. The first level of authentication will be through the usual authentication, i.e., the users have to authenticate through PAM360's local authentication or AD/LDAP authentication, whichever is enabled.

1. Launch PAM360 web interface, enter the **Username** and **Password** (local authentication or AD/LDAP), and click **Login**.
2. **Associating Microsoft Authenticator with your PAM360 account**:
3. When you are logging in for the first time after enabling TFA through Microsoft Authenticator, you will be prompted to associate it with your account in PAM360. After launching the Microsoft Authenticator app in your mobile device or tablet, click on **Add Account** or the **+** button. Choose **Other (Google, Facebook, etc.)** for the kind of account you're adding, since PAM360 is not a Microsoft extension.
4. Here, you can either **scan the QR code** displayed in your PAM360 website by scanning the barcode shown in the GUI, or **Enter Code Manually.**
5. If you choose to enter the code manually, the GUI will prompt you to enter an account name and a security key.
6. Supply an **Account name** for your PAM360 account in the format– PAM360:account name (for example. PAM360:john@abc.com).
7. Provide an alphanumeric string as your **Secret key**, and then click **Finish**.
8. Microsoft Authenticator will now start generating codes periodically, that changes every 30 seconds.
9. You can enter this code in the text box provided in the PAM360 login page for the second level of authentication.

4. Troubleshooting Tip

As mentioned earlier, the Microsoft Authenticator is associated with your PAM360 account. If you ever lose your mobile device/tablet OR if you accidentally delete the Microsoft Authenticator app on your device, you will still be able to get tokens to log in to PAM360. In such scenarios, just click the link "Have trouble using Microsoft Authenticator?" in the PAM360 login screen. You will be prompted to enter your PAM360 username and the email address associated with PAM360. Once done, you will receive instructions to get Microsoft Authenticator again.

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor, RSA SecurID, One-time password, RADIUS, or Duo) and if you have configured high availability, you need to restart the PAM360 secondary server once.

Setting up Two-Factor Authentication (TFA) – Oracle Authenticator

Oracle Authenticator is a multi-factor authentication application developed by Oracle that acts as an additional layer of security by prompting a second factor of authentication during login. Oracle mobile authenticator is available in iOS 12.0+ and Android 5.0+. You can install Oracle Authenticator on your smartphone or tablet devices. The second level of authentication is a one-time password generated by the Oracle authenticator with a 6-digit number.

How does Oracle Authenticator Work with PAM360?

1. A user tries to access the PAM360 web interface
2. As the first factor of authentication, PAM360 authenticates the user through local authentication/AD/Azure AD/LDAP
3. PAM360 prompts for the second-factor authentication through the configured Oracle Authenticator
4. The user enters the six-digit code from the Oracle Authenticator GUI
5. PAM360 grants access to the user for the PAM360 web interface for further operations

The following sections will help you to configure and use the Oracle Authenticator as the Two-Factor Authentication (TFA):

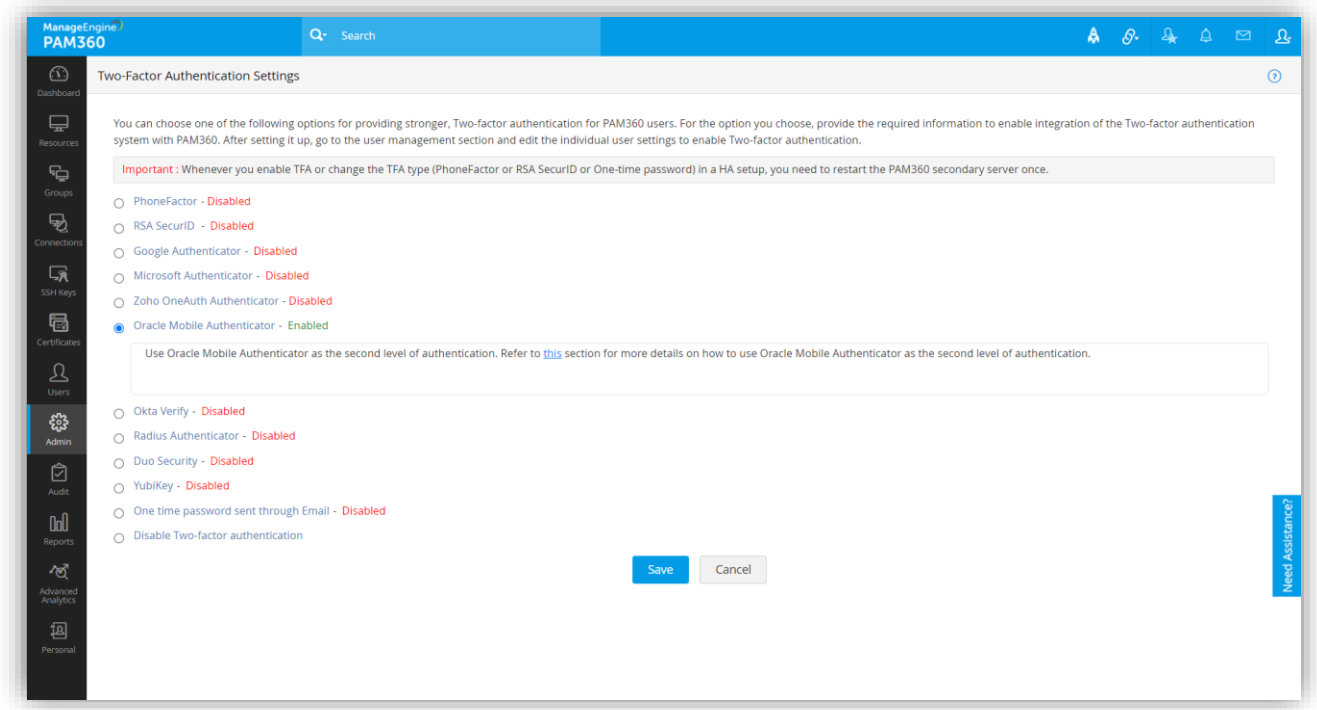
1. **Configuring TFA in PAM360**
2. **Enforcing TFA for Required Users**
3. **Connecting to PAM360 Web Interface when TFA via Oracle Authenticator is Enabled**
4. **Troubleshooting Tip**

1. Configuring TFA in PAM360

a. Navigate to '**Admin >> Authentication >> Two-factor Authentication**'.

b. Enable the option **Oracle Authenticator** and then click **Save**.

c. Click on **Confirm** to enforce Oracle Authenticator as the second factor of authentication to PAM360.



2. Enforcing TFA for Required Users

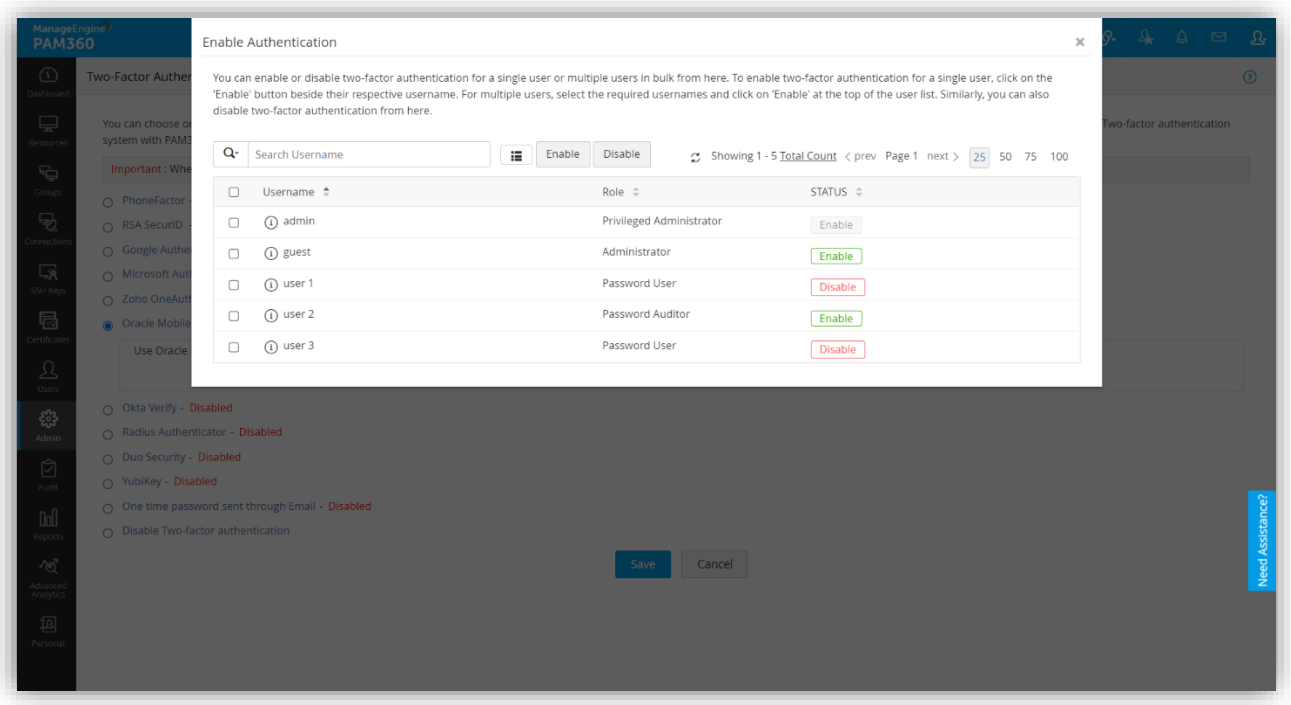
Once you enforce the Oracle - Authenticator as the second factor of authentication, a new window will prompt with the existing PAM360 users details. Select the users for whom the TFA is to be enforced.

a. From here, you can enable or disable the TFA individually or in bulk:

   i. To enable TFA individually, click the **Enable** button beside their respective username.

   ii. To enable TFA in bulk, select the required usernames and click the **Enable** button at the top of the users' list.

   iii. Similarly, follow the above steps with the **Disable** button to disable the TFA for the respective users.



b. You can also enable/disable TFA for the users later by navigating to '**Users >> More Actions >> Two-factor Authentication**'.

3. Connecting to PAM360 Web Interface with Enabled Oracle TFA

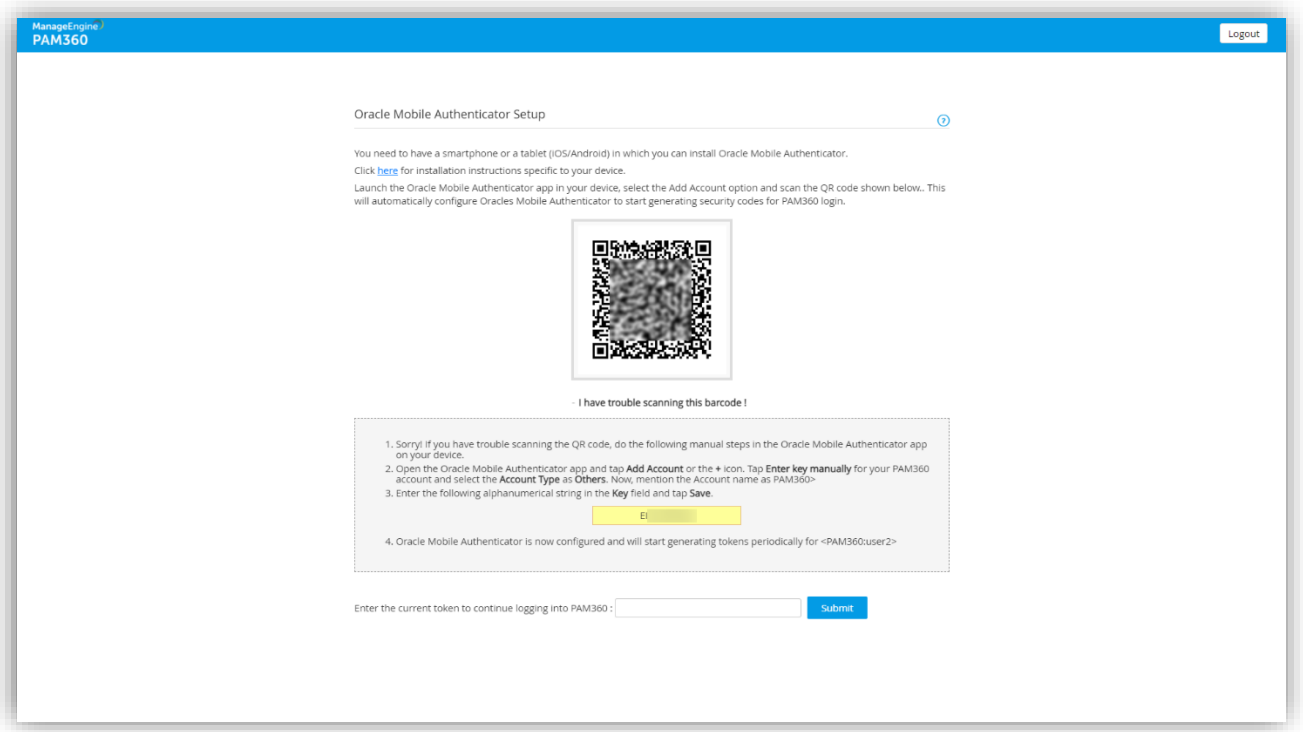
3.1 Prerequisite

Before you log in to PAM360, install the Oracle Authenticator application on your smartphone or tablet. Oracle Authenticator officially supports Android, iPhone, and iPad devices. To install, and to know more about Oracle Authenticator, click here.

3.2 Connecting to the PAM360 Web Interface

As mentioned in the above section, for the TFA-enabled users, the first level of authentication will be through the usual authentication, i.e., the users have to authenticate through PAM360's local authentication or AD/Azure AD/LDAP authentication. Follow the below steps to configure the PAM360 account in the Oracle Authenticator during the initial login for TFA:

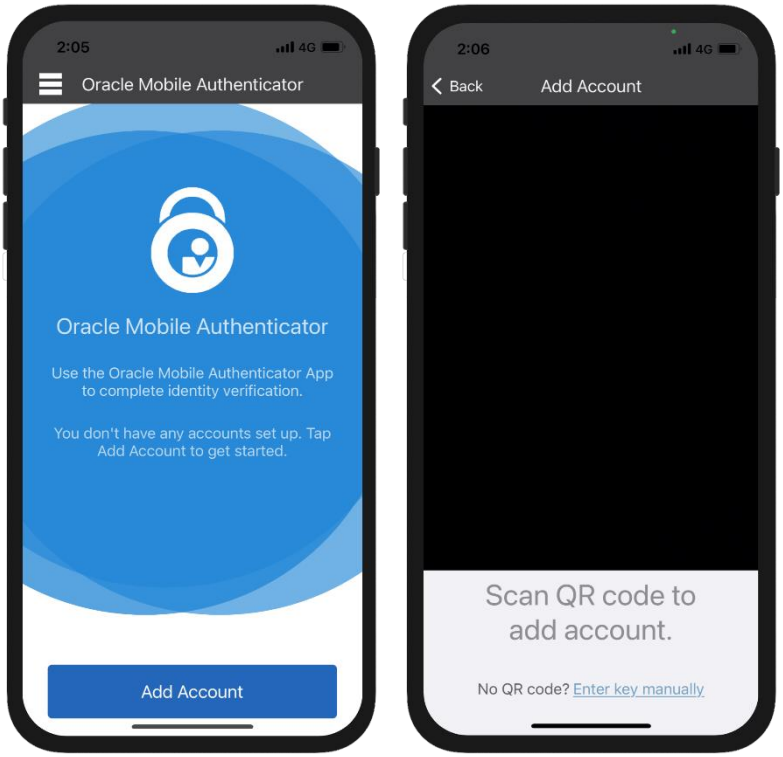
a. Upon launching the PAM360 web interface, the user has to enter the local authentication credentials or Azure AD/AD/LDAP password to log in to PAM360 and click **Login**.



b. If you log in to PAM360 for the first time after enabling TFA through Oracle Authenticator, you will be prompted to associate it with your PAM360 account. Follow the below steps to associate Oracle Authenticator with your PAM360 account:

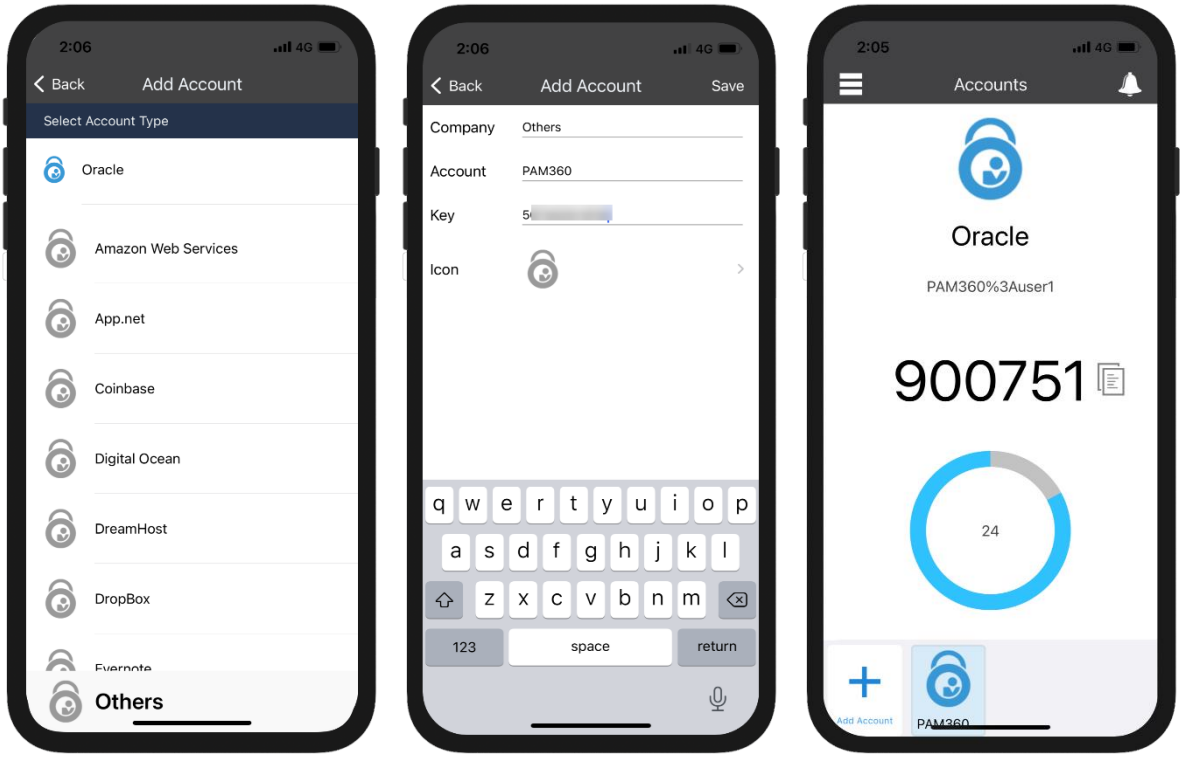
   i. Launch the Oracle Authenticator application on your mobile device/tablet.

   ii. Tap the '**+**' button or click **Add Account**.



iii. Then, point your device to the QR code shown in the PAM360 GUI to scan the QR code to add the account. This will automatically configure Oracle Authenticator and will start generating authentication codes for PAM360.

iv. After completing this, enter the current token for authentication in the text box.



c. If you have trouble scanning the QR code, the automatic setup will not work. Alternatively, you can carry out the following manual steps in the Oracle Authenticator application to complete the configuration process:

i. Click the text '**I have trouble scanning this barcode!**' present below the barcode in the PAM360 GUI.

ii. From the Oracle authenticator application, tap the '**+**' button or click **Add Account**.

iii. Tap the **Enter key manually** and select the **Account Type** as **Others**.

iv. Enter the **Account** name and the **Key** and click **Save**. The Key is the alphanumeric key shown in the PAM360 GUI.

d. Oracle Authenticator is now configured and will start generating the authentication codes periodically. Enter the current generated code to continue logging into PAM360.

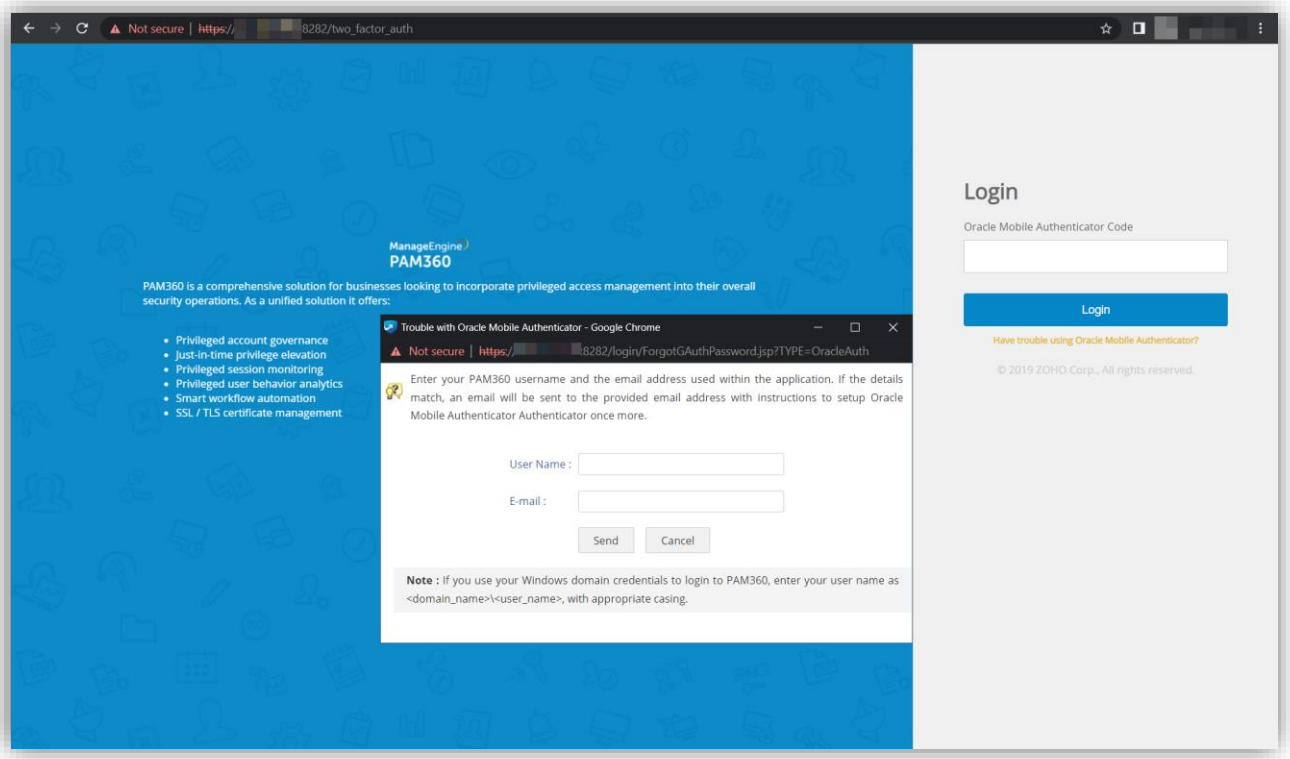
4. Troubleshooting Tip

As you know, the Oracle Authenticator is associated with your PAM360 account. If you lose your mobile device/tablet or accidentally delete the Oracle - Authenticator app from your device, you will still be able to get the generated codes to log in to PAM360. In such scenarios,

a. Click the link "**Have trouble using Oracle Authenticator?**" on the PAM360 login screen.

b. You will be prompted to enter your PAM360 Username and the Email address associated with PAM360.

c. You will receive instructions to get Oracle Authenticator again via the above-mentioned Email.



Setting up Two-Factor Authentication (TFA) – Zoho OneAuth Authenticator

Zoho OneAuth Authenticator, a comprehensive multi-factor authentication application, helps you secure your online accounts, thus improving your business security. It is available for download on multiple devices - iOS, Android, iPad, macOS, watchOS, and Windows platforms and can be installed at your convenience. Once configured, the OTP Authenticator of Zoho OneAuth generates a 6-digit number every 30 seconds that must be entered as the second factor of authentication, following the usual first-factor authentication.

How does Zoho OneAuth Work with PAM360?

1. A user tries to access the PAM360 web interface
2. PAM360 authenticates the user through the first factor of authentication / local authentication - AD/Azure AD/LDAP
3. PAM360 prompts for the second-factor authentication through the configured Zoho OneAuth - Authenticator
4. The user enters the six-digit code from the Zoho OneAuth - Authenticator GUI
5. PAM360 grants access to the user for the PAM360 web interface for further operations

The following sections will help you to configure and use the Zoho OneAuth Authenticator as the Two-Factor Authentication (TFA):

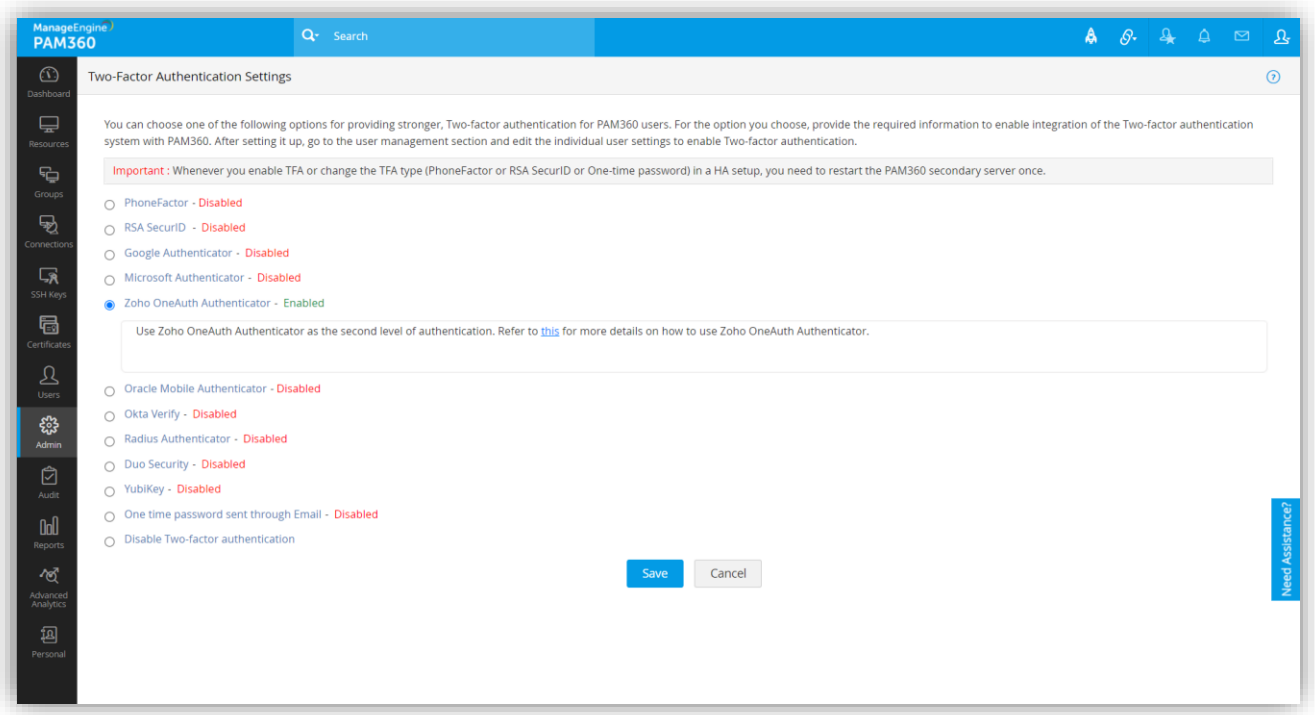
1. **Configuring TFA in PAM360**
2. **Enforcing TFA for Required Users**
3. **Connecting to PAM360 Web Interface when TFA via Zoho OneAuth - Authenticator is Enabled**
4. **Troubleshooting Tip**

1. Configuring TFA in PAM360

a. Navigate to '**Admin >> Authentication >> Two-factor Authentication**'.

b. Enable the option **Zoho OneAuth - Authenticator** and click **Save**.

c. Click on **Confirm** to enforce Zoho OneAuth - Authenticator as the second factor of authentication.



2. Enforcing TFA for Required Users

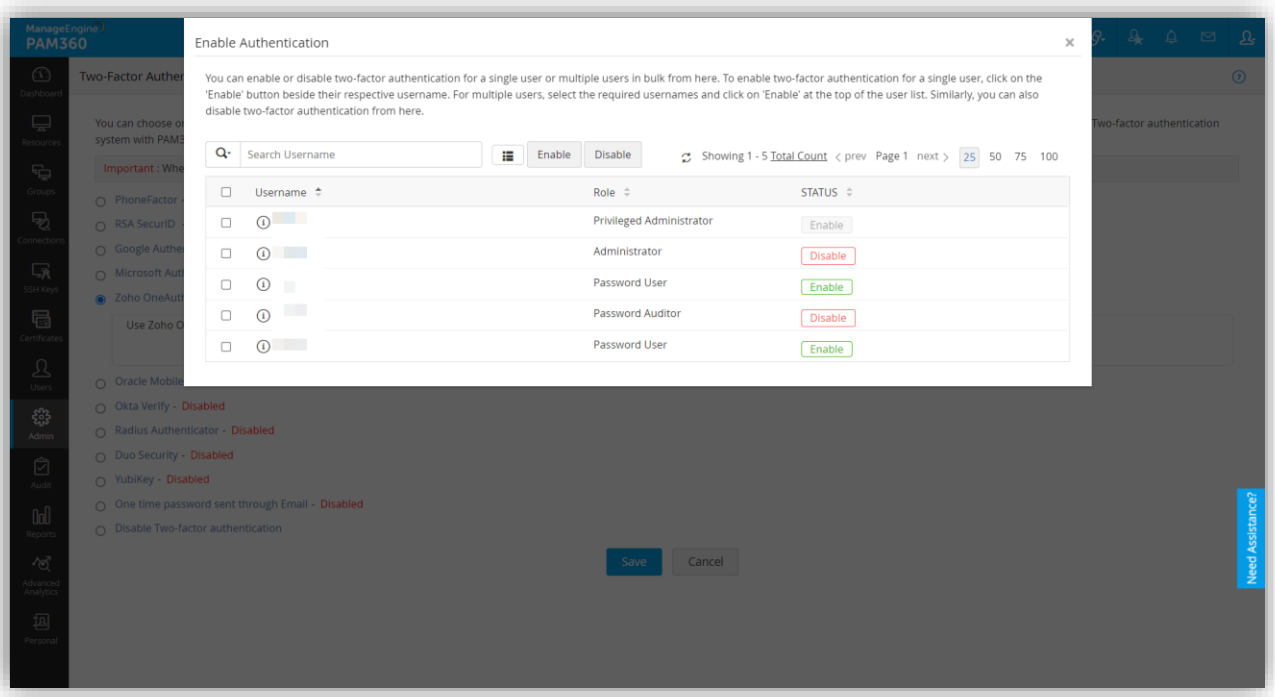
Once you enforce the Zoho OneAuth - Authenticator as the second factor of authentication, a new window will prompt with the existing PAM360 users details. Select the users for whom the TFA is to be enforced.

a. From here, you can enable or disable the TFA individually or in bulk:

   i. To enable TFA individually, click the **Enable** button beside their respective username.

   ii. To enable TFA in bulk, select the required usernames and click the **Enable** button at the top of the users' list.

iii. Similarly, follow the above steps with the **Disable** button to disable the TFA for the respective users.



b. You can also enable/disable TFA for the users later by navigating to '**Users >> More Actions >> Two-factor Authentication**'.

3. Connecting to PAM360 Web Interface with Enabled Zoho OneAuth - Authentication

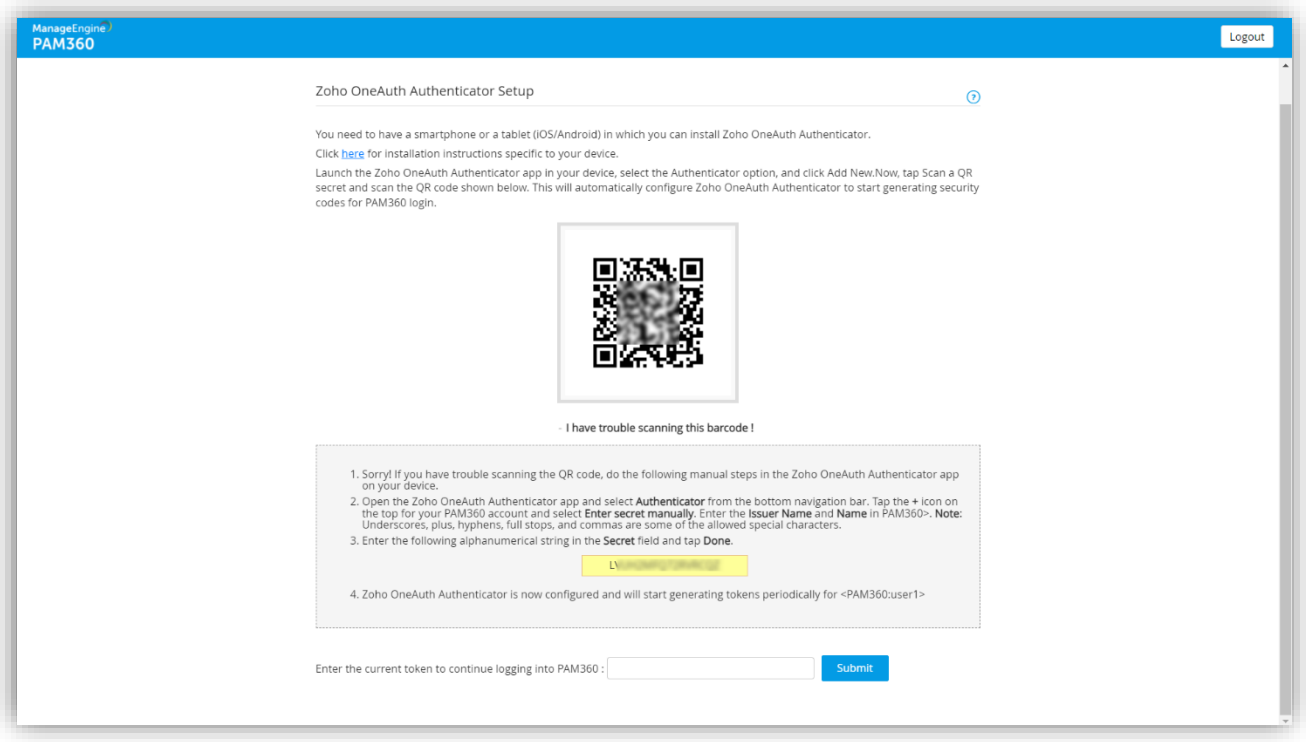
3.1 Prerequisite

Before you log in to PAM360, install Zoho OneAuth - Authenticator application on your smartphone or tablet. To install, and to know more about Zoho OneAuth, click here.

3.2 Connecting to the PAM360 Web Interface

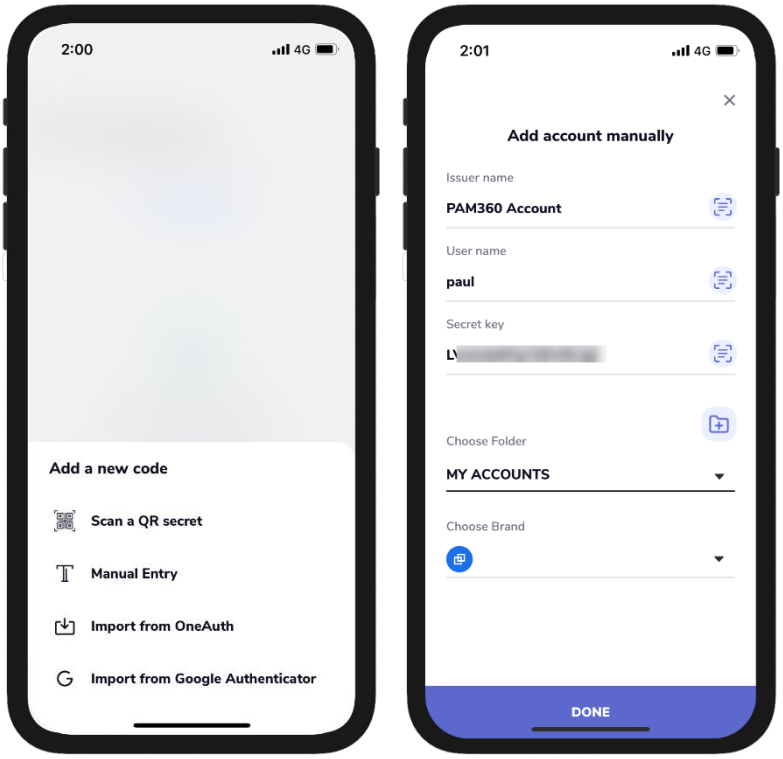
As mentioned in the above section, for the TFA-enabled users, the first level of authentication will be through the usual authentication, i.e., the users have to authenticate through PAM360's local authentication or AD/Azure AD/LDAP authentication. Follow the below steps to configure the PAM360 account in the Zoho OneAuth - Authenticator during the initial login for TFA:

a. Upon launching the PAM360 web interface, the user has to enter the local authentication credentials or Azure AD/AD/LDAP password to log in to PAM360 and click Login.



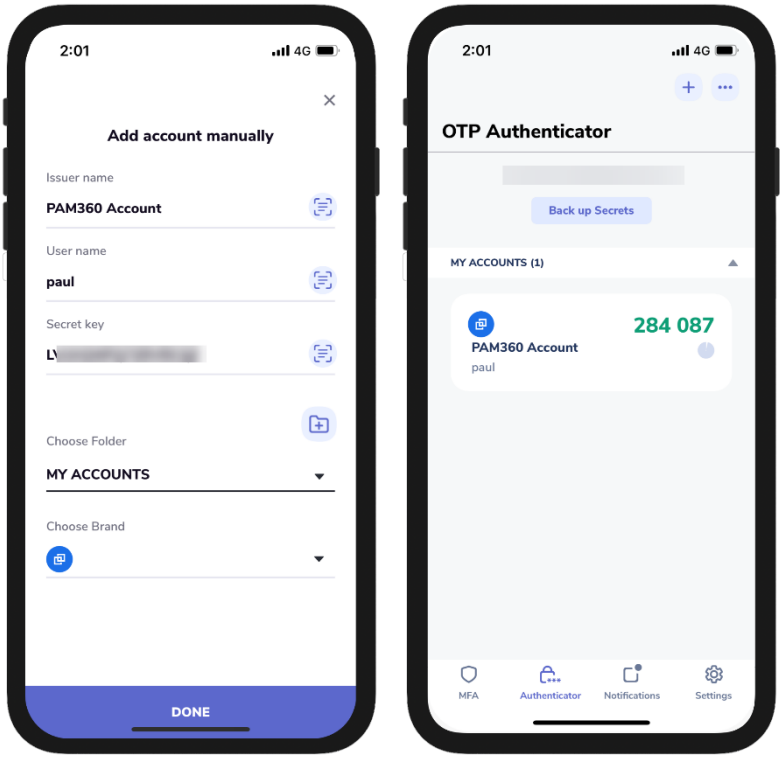
b. If you log in to PAM360 for the first time after enabling TFA through Zoho OneAuth - Authenticator, you will be prompted to associate it with your PAM360 account. Follow the below steps to associate Zoho OneAuth - Authenticator with your PAM360 account:

   i. Launch the Zoho OneAuth application on your mobile device/tablet and tap **Authenticator** from the bottom pane.
   ii. Tap the '**+**' button or click **Add new**.



iii. Click **Scan a QR secret** and point your device to the barcode shown in the PAM360 GUI. This will automatically configure your PAM360 account in the Zoho OneAuth - Authenticator application and will start generating the authentication codes for PAM360.

iv. After the configuration, you can enter the current generated code in Zoho OneAuth - Authenticator for authentication in the PAM360 GUI text box.



c. If you have trouble scanning the barcode, the automatic setup will not work. Alternatively, you can carry out the following manual steps in the Zoho OneAuth - Authenticator application to complete the configuration process:

   i. Click the text '**I have trouble scanning this barcode!**' present below the barcode in the PAM360 GUI.
   ii. From the Zoho OneAuth application, tap the '**+**' button or click **Add new**.
   iii. Select **Manual Entry** and enter the **Issuer name**, **User name**, and the **Secret key**. The Secret Key is the alphanumeric key shown in the PAM360 GUI.
   iv. Select the folder and the account brand icon and click **DONE**.

d. Zoho OneAuth - Authenticator is now configured and will start generating the authentication codes periodically. Enter the current generated code to continue logging in to PAM360.

4. Troubleshooting Tip

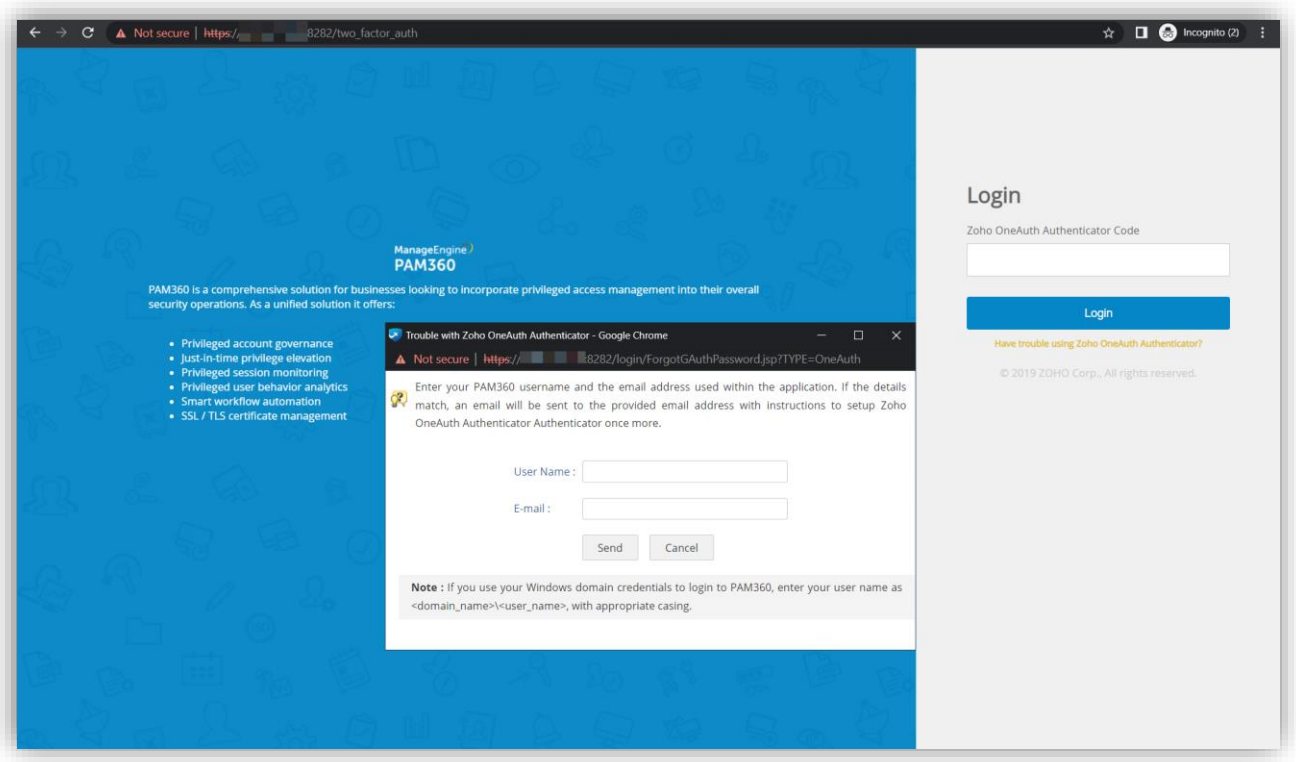
As you know, the Zoho OneAuth Authenticator is associated with your PAM360 account. If you lose your mobile device/tablet or accidentally delete the Zoho OneAuth - Authenticator app

from your device, you will still be able to get the generated codes to log in to PAM360. In such scenarios,

a. Click the link "**Have trouble using Zoho OneAuth - Authenticator?**" on the PAM360 login screen.

b. You will be prompted to enter your PAM360 Username and the Email address associated with PAM360.

c. You will receive instructions to get Zoho OneAuth - Authenticator again via the above-mentioned Email.



Setting up Two-Factor Authentication (TFA) - Okta Verify

Okta Verify is a software-based authentication token that provides a six-digit number that users must enter as the second factor of authentication.

You need to install the Okta Verify app on your smart phone or tablet devices. It generates a six-digit number, which changes every 30 seconds. With the app, you don't have to wait a few seconds to receive a text message.

Sequence of Events

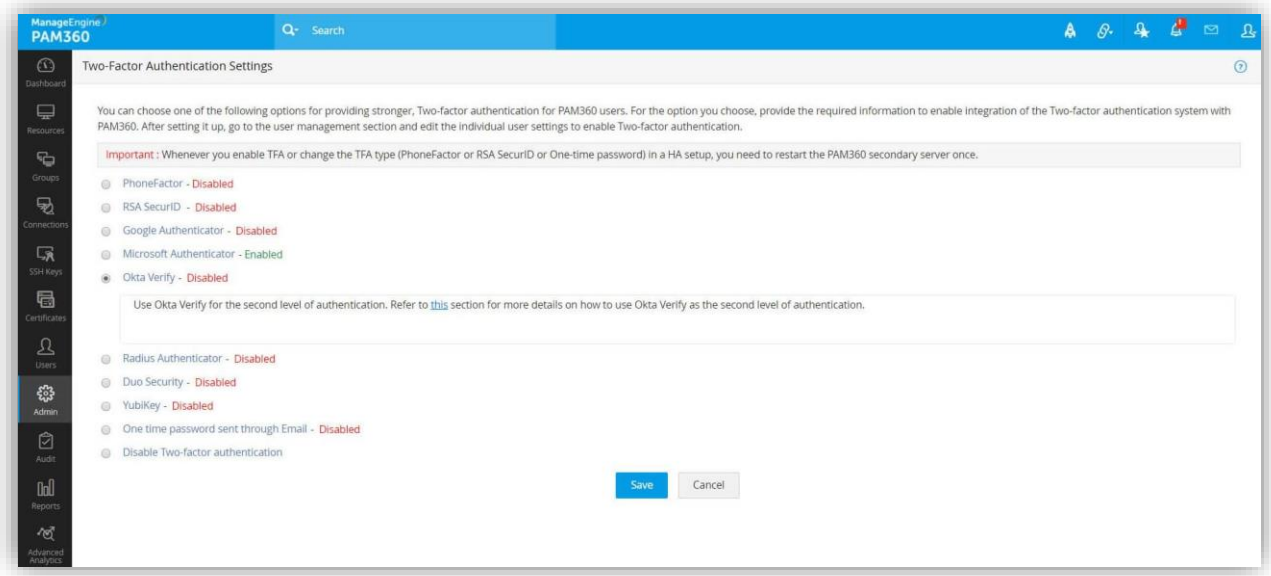
1. A user tries to access PAM360 web-interface.
2. PAM360 authenticates the user through Active Directory or LDAP or locally (first factor).
3. PAM360 requests for the second factor credential through Okta Verify.
4. The user has to enter the six-digit token that they see on the Okta Verify app GUI.
5. PAM360 grants the user access to the web-interface.

This document walks you through the following topics:

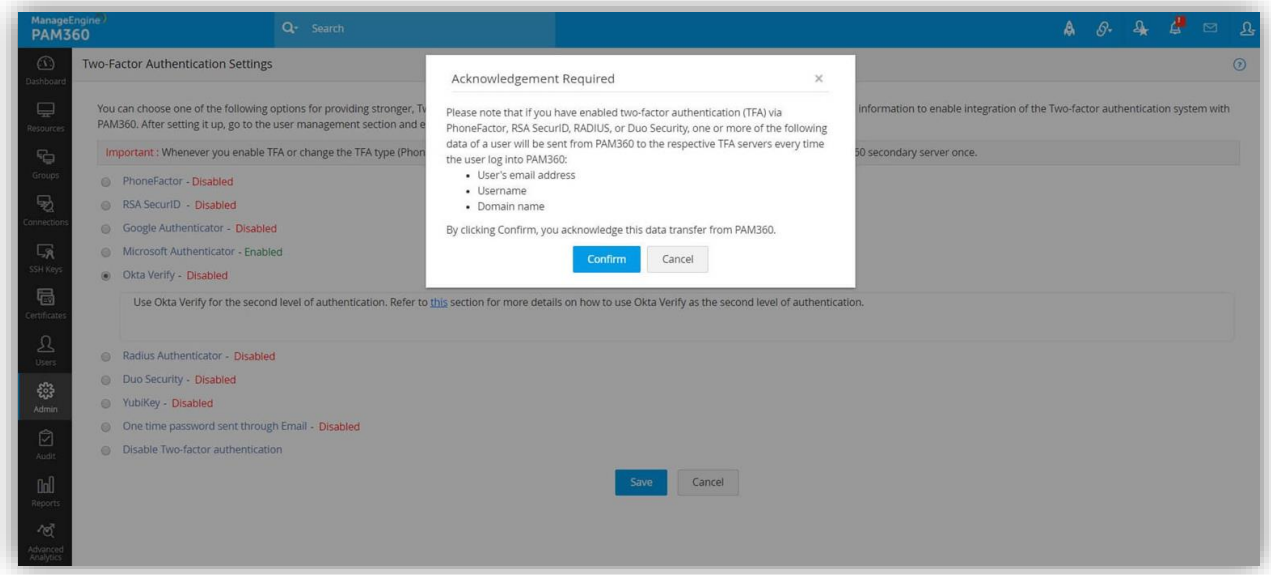
1. Configuring TFA in PAM360
2. Enforcing TFA for Required Users
3. How to Connect to PAM360 Web Interface when TFA via Okta Verify is Enabled?
   3.1 Prerequisite
   3.2 Connecting to PAM360 Web Interface
4. Troubleshooting Tip

1. Configuring TFA in PAM360

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication.**
2. Choose the option **Okta Verify**, and click **Save**.

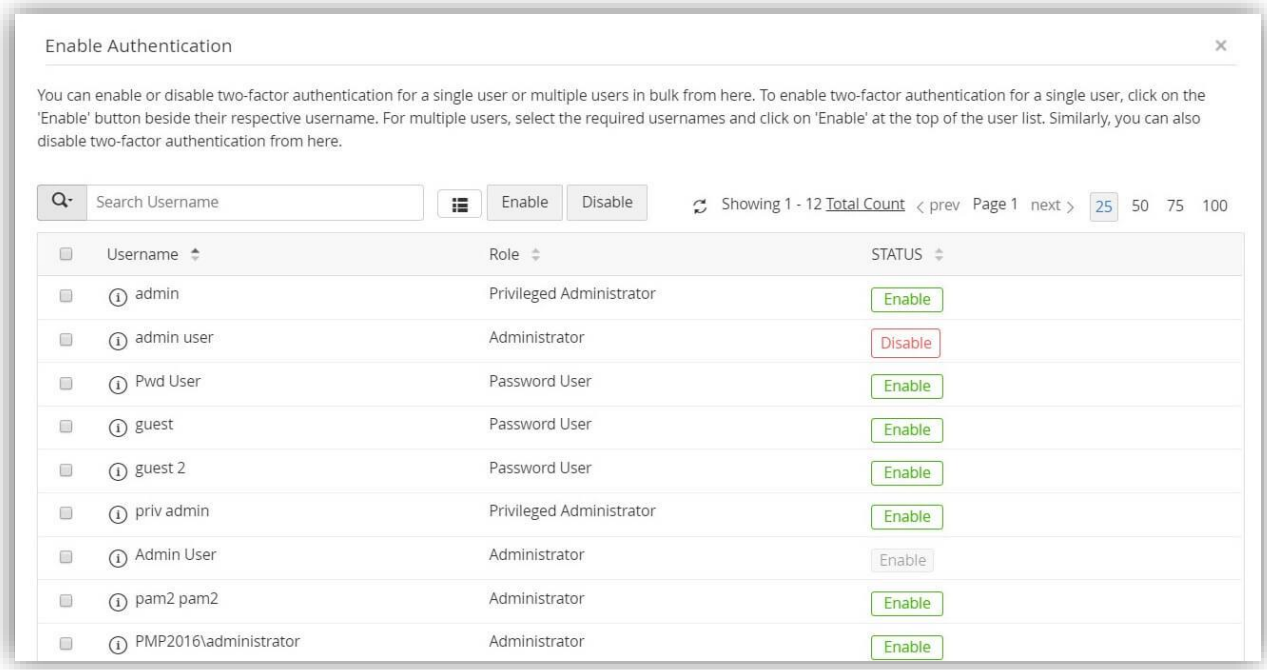


3. Click **Confirm** to enforce Okta Verify as the second factor of authentication.

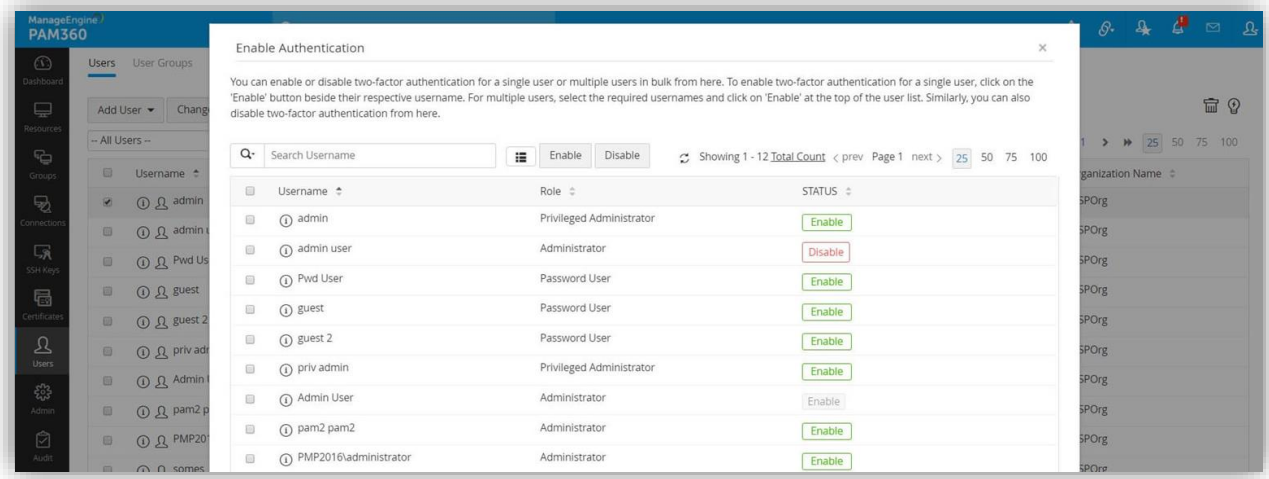


2. Enforcing TFA for Required Users

1. Once you confirm the Okta Verify as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom TFA should be enforced.



2. You can enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click on the **Enable** button beside their respective username. For multiple users, select the required usernames and click on **Enable** at the top of the user list. Similarly, you can also **Disable** TFA from here.
3. Close the window.
4. You can also select the users later by navigating to **Users >> More Actions >> Two-Factor Authentication.**



5. In the window that opens, select the users for whom you want to enforce Okta TFA.

3. Connecting to PAM360 Web Interface when TFA via Okta

Verify is Enabled

3.1 Pre-requisite

To use Okta Verify as the second factor of authentication, you should first install the app in your smart phone or tablet.

3.2 Connecting to PAM360 Web Interface

The users for whom TFA is enabled will have to authenticate twice successively. The first level of authentication will be through the usual authentication, i.e., the users have to authenticate through PAM360's local authentication or AD/LDAP authentication, whichever is enabled.

1. Launch PAM360 web interface, enter the Username and Password (local authentication or AD/LDAP), and click Login.
2. **Associating Okta Verify with your PAM360 account:**
    i. When you are logging in for the first time after enabling TFA through Okta Verify, you will be prompted to associate it with your account in PAM360. After launching the Okta Verify app in your mobile device or tablet, click on **Add Account** or the **+** button.
    ii. Here, you can either scan the QR code displayed in your PAM360 website, or create an account manually by clicking the **No Barcode?** button.
    iii. If you choose to enter the code manually, the GUI will prompt you to enter an account name and a security key.
    iv. Supply an **Account name** for your PAM360 account in the format– PAM360 : account name (for example. PAM360:john@abc.com).
    v. Provide an alphanumeric string as your **Secret key**, and then click **Add Account**.
    vi. Okta Verify will now start generating codes periodically, that changes every 30 seconds.
    vii. You can enter this code in the text box provided in the PAM360 login page for the second level of authentication.

4. Troubleshooting Tip

As mentioned earlier, the Okta Verify is associated with your PAM360 account. If you ever lose your mobile device/tablet OR if you accidentally delete the Okta Verify app on your device, you will still be able to get tokens to log in to PAM360. In such scenarios, just click the link "**Have trouble using Okta Verify?**" in the PAM360 login screen. You will be prompted to enter your PAM360 username and the email address associated with PAM360. Once done, you will receive instructions to get Okta Verify again.

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor, RSA SecurID, One-time password, RADIUS, or Duo) AND if you have configured high availability, you need to restart the PAM360 secondary server once.

Setting up Two-Factor Authentication (TFA) - RADIUS Authenticator

You can integrate RADIUS server or any RADIUS-compliant TFA system (like Vasco Digipass) with PAM360 for the second factor authentication.

Sequence of Events

1. Provide basic details about RADIUS server.
2. Enable the RADIUS-based authentication system as the second factor.

Setting up RADIUS Authenticator involves the following steps:

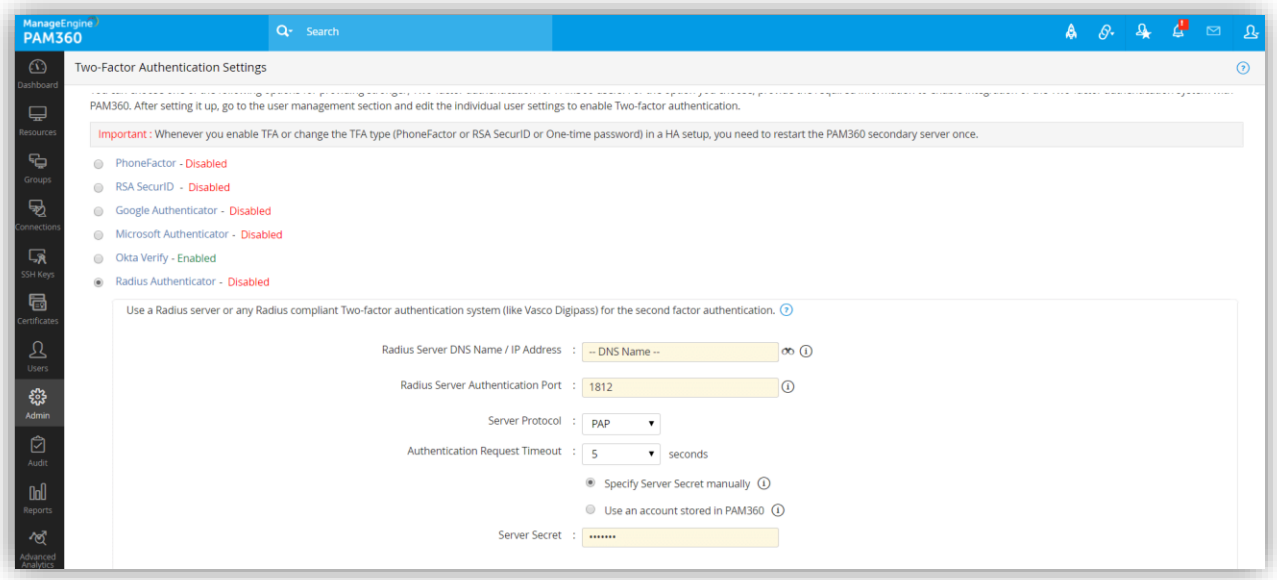
1. **Setting up TFA in PAM360**
2. **Enforcing TFA for Required Users**
3. **Connecting to PAM360 Web Interface when TFA through RADIUS Authenticator is Enabled**

1. Setting up TFA in PAM360

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**.
2. Choose the option **RADIUS Authenticator**.
3. In the new dropdown form that opens, provide the following details:
    i. **Server Name/IP Address** - Enter the host name or IP address of the host where RADIUS server is running.
    ii. **Server Authentication Port** - Enter the port used for RADIUS server authentication. By default, RADIUS has been assigned the UDP port 1812 for RADIUS Authentication.
    iii. **Server Protocol** - Select the protocol that is used to authenticate users. Choose from four protocols - Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MSCHAP), Version 2 of Microsoft Challenge-Handshake Authentication Protocol (MSCHAP2).
    iv. **Server Secret** - You have the option to enter the RADIUS server secret either manually in the text box or you can direct PAM360 to use the secret already stored in the product. In that case, you need to select the resource name and account name from the drop-down. The second option - storing the RADIUS password in PAM360 and selecting it from drop-down is the recommended

approach.

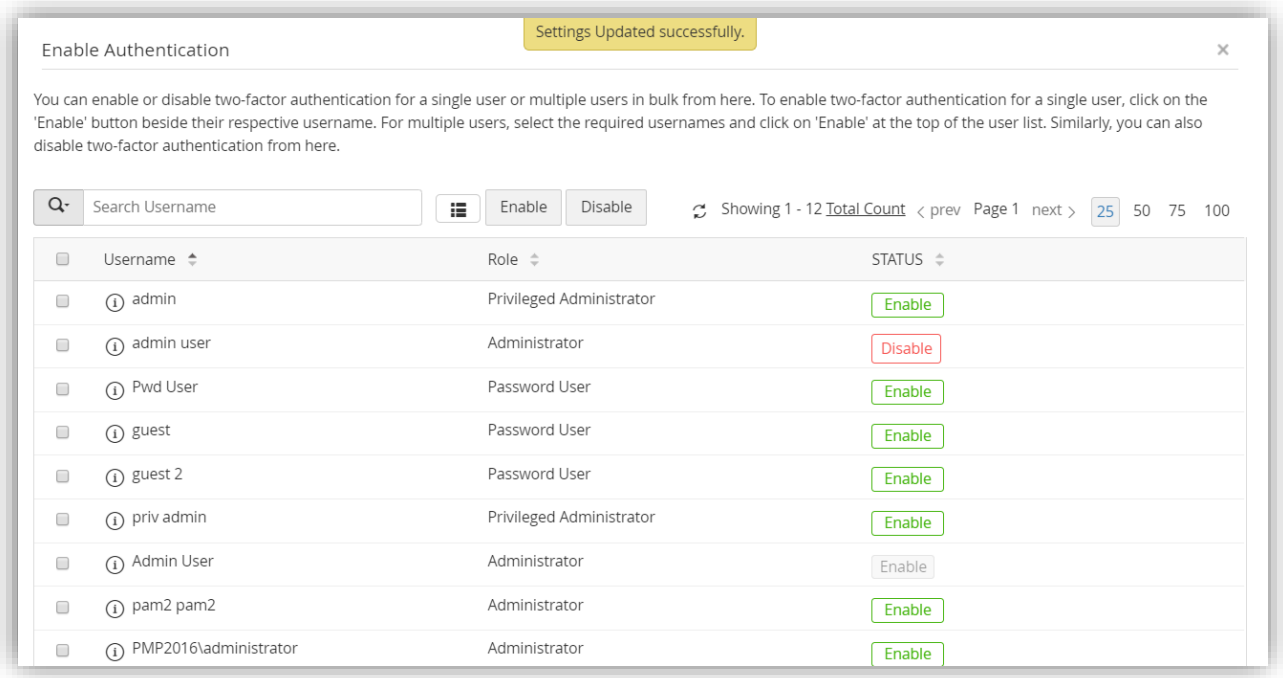
4. Once you have entered the required details, click **Save**.



5. Then, click on **Confirm** to enforce Radius Authenticator as the second factor of authentication.

2. Enforcing TFA for Required Users

1. Once you confirm Radius Authenticator as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom TFA should be enforced.
2. You can enable or disable TFA for a single user or multiple users in bulk from here. To enable TFA for a single user, click on the **Enable** button beside their respective username. For multiple users, select the required usernames and click on **Enable** at the top of the user list. Similarly, you can also **Disable** TFA from here.



3. You can select the users later by navigating to **Users >> More Actions >> Two-Factor Authentication.**

3. Connecting to PAM360 Web Interface when TFA through RADIUS Authenticator is Enabled

The users for whom TFA is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PAM360's local authentication or AD/LDAP authentication. If the administrator has chosen the TFA option **RADIUS Authenticator**, the TFA will happen as detailed below:

1. Upon launching the PAM360 web-interface, the user has to enter the username and local authentication or AD/LDAP password to login to PAM360 and click **Login**.
2. Once the first level of authentication succeeds, you will be prompted to enter the **RADIUS code.**

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password or RADIUS or Duo) AND if you have configured high availability, you need to restart the PAM360, secondary server once.

Setting up Two-Factor Authentication (TFA) - Duo Security

Two-Factor Authentication or Multi-Factor Authentication is an extra layer of security provided to secure your accounts. Duo Security is a cloud based Multi-Factor Authenticator that provides secure access to your account. Duo Security allows you to integrate PAM360 with Two-Factor Authentication.

This document will walk you through the following topics:

1. Configuring PAM360 - Duo Security Integration
2. Configuring TFA in PAM360
3. Enforcing TFA for Required Users
4. Connecting to PAM360 Web Interface when TFA is Enabled
5. Enrolling while Logging in

1. Configuring PAM360 - Duo Security Integration

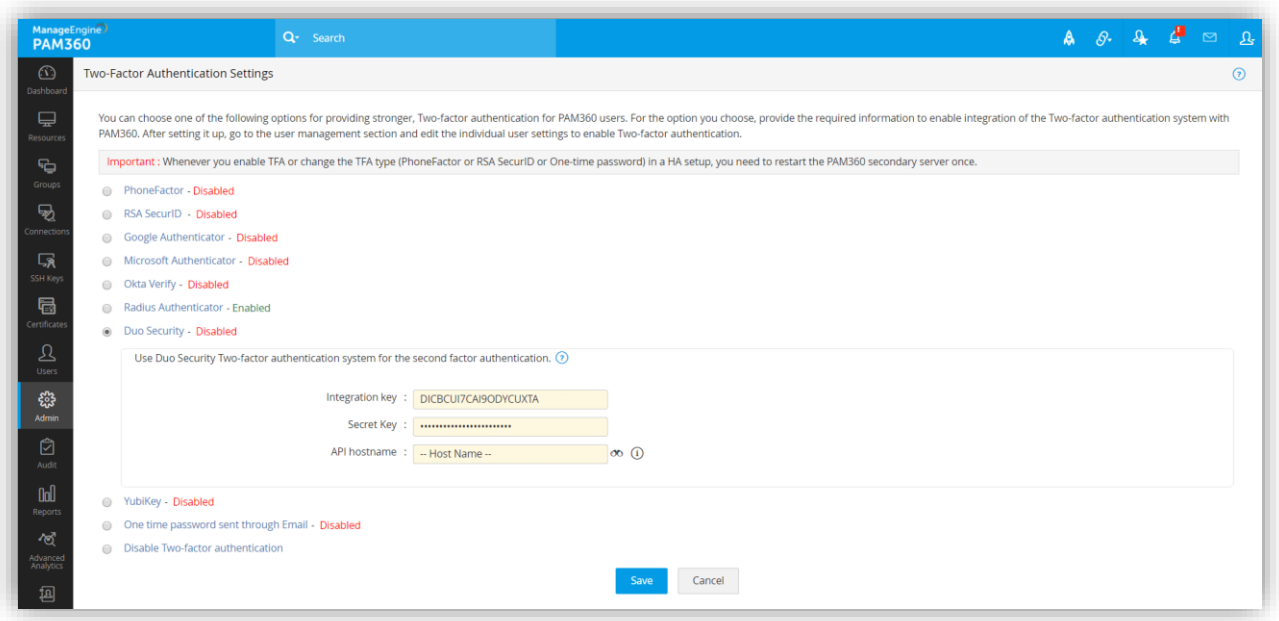
If you have Duo Application in your environment, you can integrate it with PAM360 and leverage the Duo security authentication as the second level of authentication. This section explains the configurations involved:

1. Sign up for a Duo account.
2. Log in to the **Duo Admin Panel** and add a new application.
3. Click the **Protect an application** button. The 'Protect an application' page lists the applications you can protect with Duo.
4. Search for Web SDK and click **Protect This Application** and fill the required field and save it.
5. While saving, take a note of **integration key, secret key** and **API hostname** which must be provided in PAM360 GUI (in step 2 below).
6. Enroll your users with Duo and start authenticating.

2. Configuring TFA in PAM360

1. Go to **Admin >> Authentication >> Two-factor Authentication**.
2. In the UI that opens up, choose the option **Duo Security**.

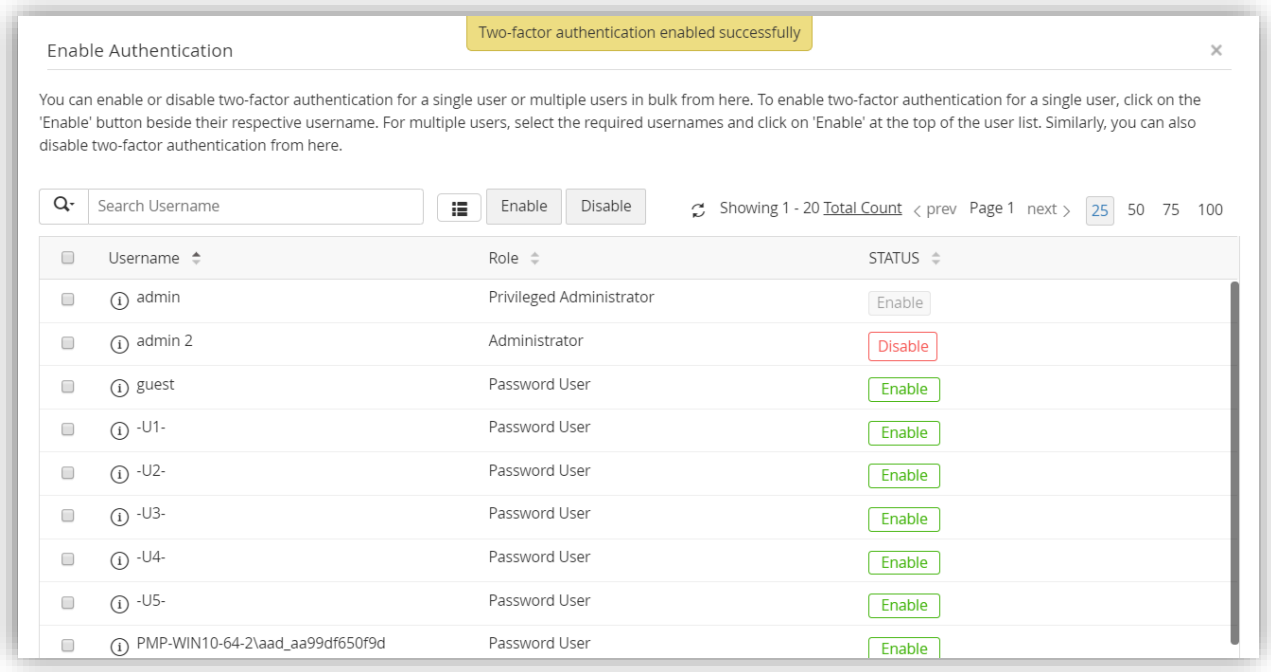
3. Provide the following details that you noted down in step 1,
    i. **Integration key**
    ii. **Secret key**
    iii. **API hostname**
4. Click **Save**.



5. Then, click on **Confirm** to enforce Duo Security as the second factor of authentication.

3. Enforcing TFA for Required Users

1. Once you confirm Duo Security as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom two-factor authentication should be enforced.
2. You can enable or disable Two-Factor Authentication for a single user or multiple users in bulk from here. To enable two-factor authentication for a single user, click on the **Enable** button beside their respective username. For multiple users, select the required usernames and click on **Enable** at the top of the user list. Similarly, you can also **Disable** two-factor authentication from here.

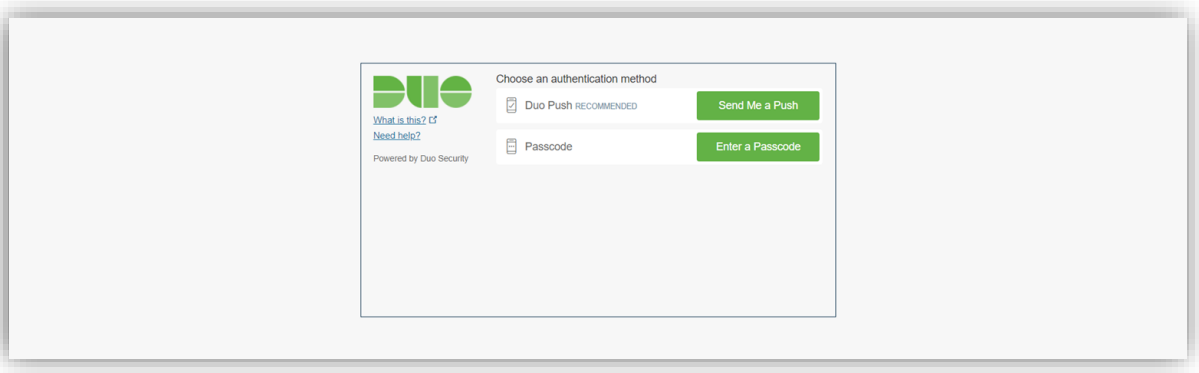


3. You can also select the users later by navigating to **Users >> More Actions >> Two-factor Authentication**.

4. Connecting to PAM360 Web Interface when TFA is Enabled

The users for whom two-factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PAM360's local authentication or AD/LDAP authentication. Depending on the type of TFA chosen by the administrator, the second level of authentication will differ as explained below:

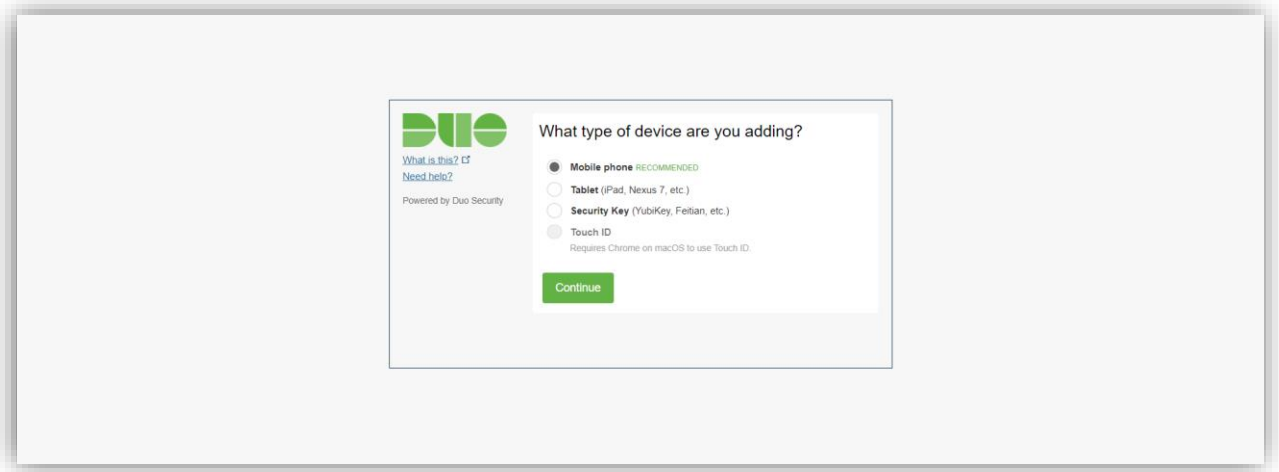
1. Upon launching the PAM360 web-interface, the user has to enter the username and local authentication or AD/LDAP password to log in to PAM360 and click **Login**.
2. Once the first level of authentication succeeds, PAM360 will prompt you to choose an authentication method out of the three options offered by Duo.
3. You can choose **Duo Push** as an authentication method.
    i. Tap **Send me a Push** on the Duo Push request sent to your phone.
    ii. You can also request a '**One Time Passcode**' via SMS on your phone, allowing users to avail two-factor authentication even when there is no internet connectivity.

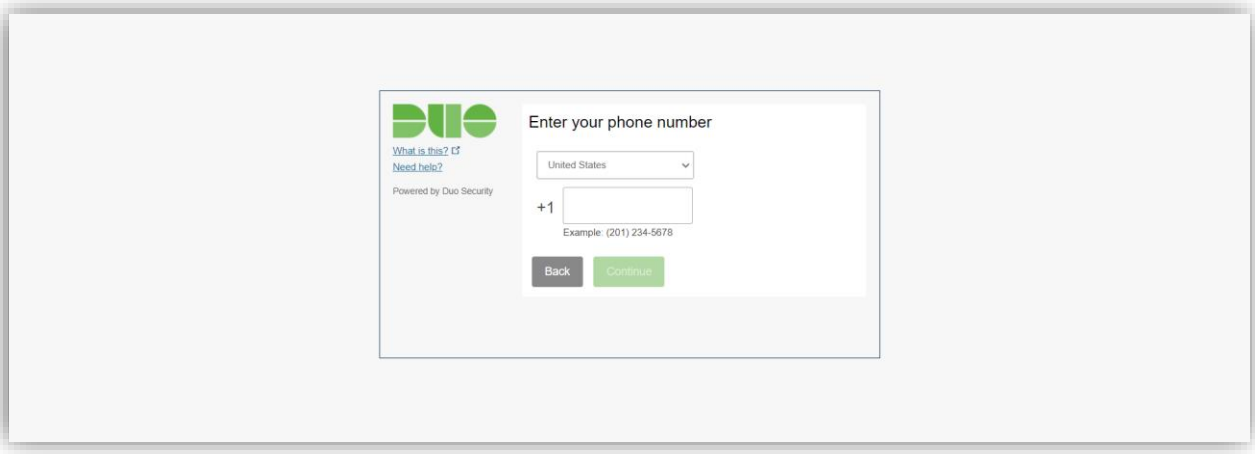


Note: This bulk edit operation will simply overwrite the current password reset configuration, if any, of the chosen resources.

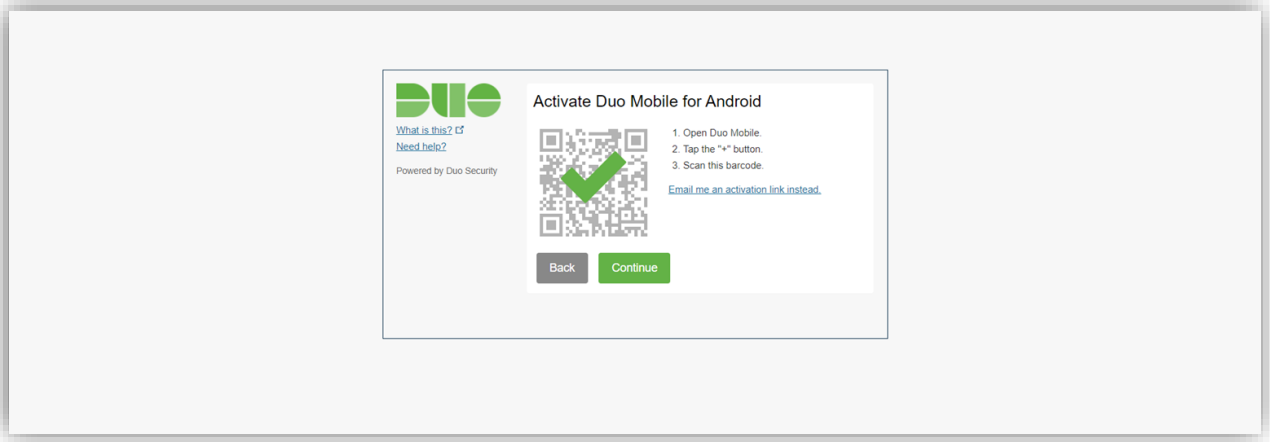
5. Enrolling while Logging in

1. Click **Start Setup** in the login page.
2. Select the type of device you are adding and enter your phone number.





3. Verify your phone number by scanning the QR code sent to your phone.



4. After successful verification, click **Continue.**

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password or RADIUS or Duo) AND if you have configured high availability, you need to restart the PAM360 secondary server once.

Setting up Two-Factor Authentication - YubiKey

YubiKey is a physical key made by **Yubico**, that ensures secure and strong user authentication. You can set up two-factor authentication with YubiKey in PAM360 by following the steps detailed in this document.

You will learn the following topics in this document:

1. YubiKeys Compatible with PAM360
2. Legacy YubiKeys Compatible with PAM360
3. Configuring and Enforcing Two-Factor Authentication using YubiKey
4. Connecting to PAM360 Web Interface after Yubikey TFA is Enabled

1. YubiKeys Compatible with PAM360

- YubiKey 5 NFC
- YubiKey 5C
- YubiKey 5 Nano
- YubiKey 5C Nano

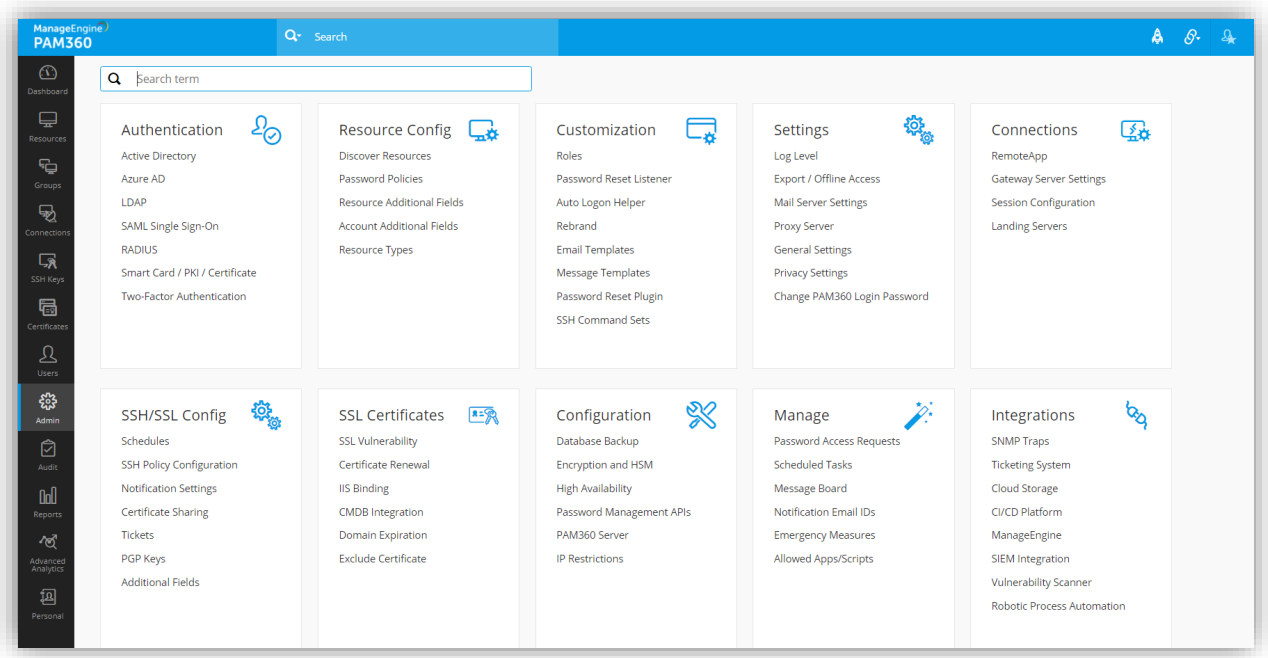
2. Legacy YubiKeys Compatible with PAM360

- YubiKey 4
- YubiKey 4 Nano
- YubiKey 4C
- YubiKey 4C Nano
- YubiKey NEO
- YubiKey Edge
- YubiKey Edge-n
- YubiKey NEO-n

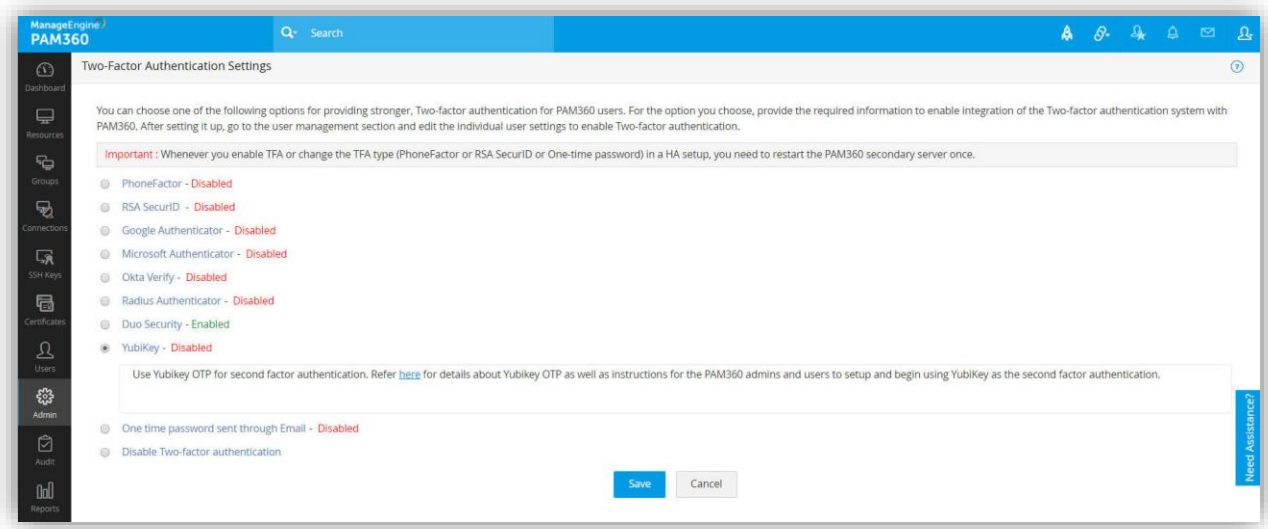
3. Configuring and Enforcing Two-Factor Authentication using YubiKey

3.1 Configuring Two-Factor Authentication using YubiKey

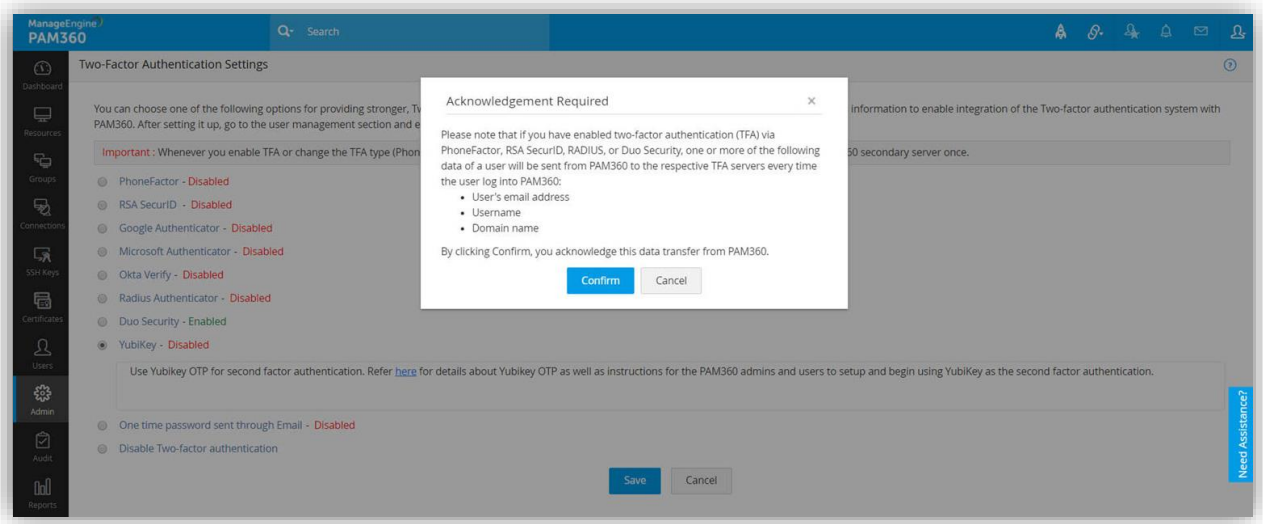
1. Navigate to **Admin >> Authentication >> Two-factor Authentication.**



2. In the window that opens, select **YubiKey** and click **Save.**

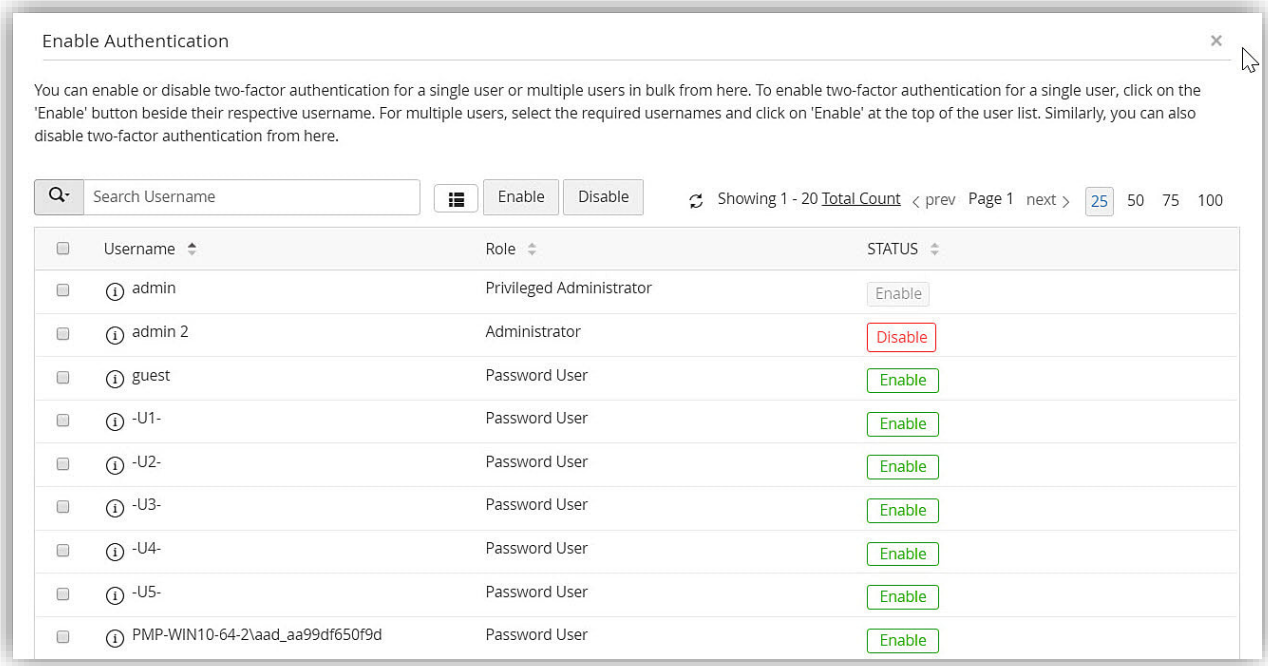


3. Click **Confirm** to enable YubiKey two-factor authentication.

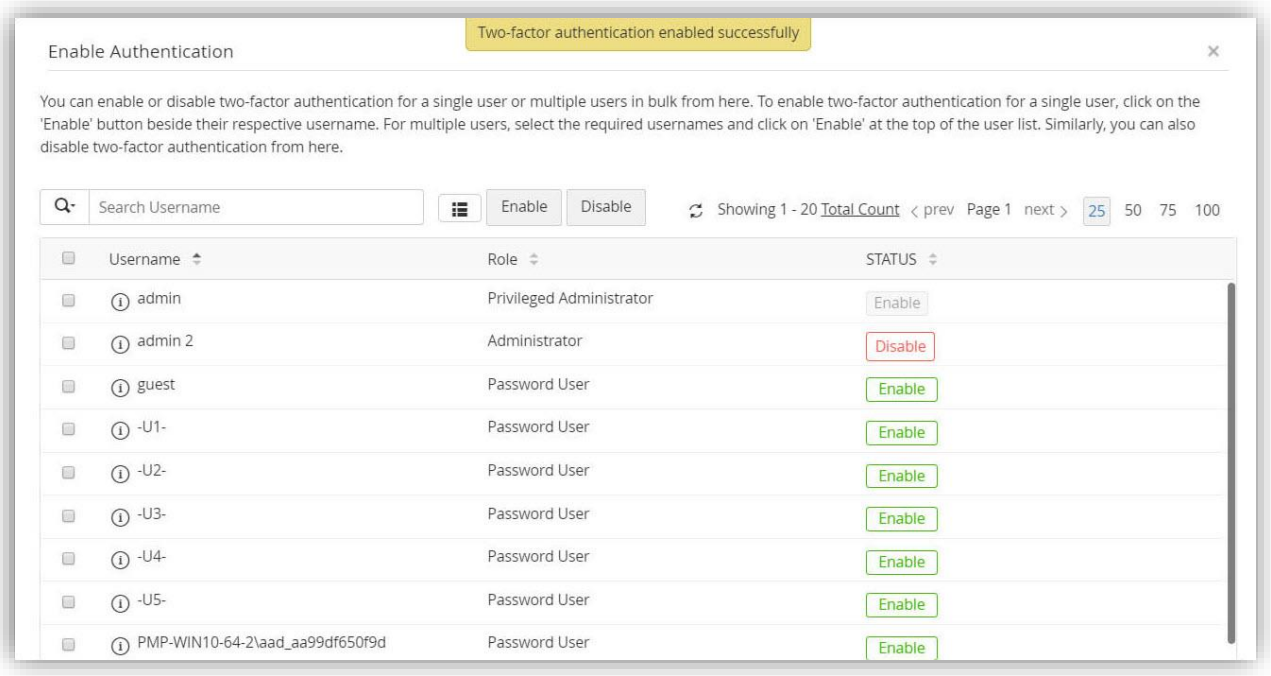


3.2 Enforcing YubiKey Two-Factor Authentication

1. Once you confirm YubiKey two-factor authentication in the previous step, a new window will prompt you to select the users for whom two-factor authentication should be enforced.
2. Click **Enable** to select the required users for whom you want to enforce Yubikey two-factor authentication.



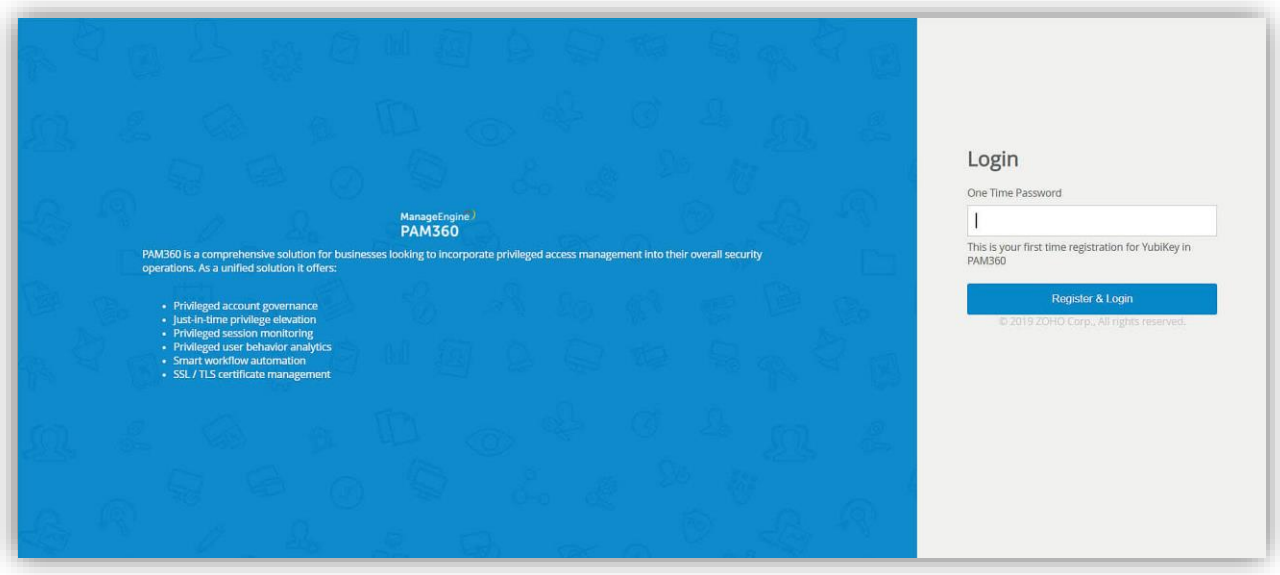
3. You can also select the users later by navigating to **Users >> More Actions >> Two-factor Authentication.**
4. In the pop-up window, select the users for whom you want to enforce YubiKey two-factor authentication by clicking **Enable.**



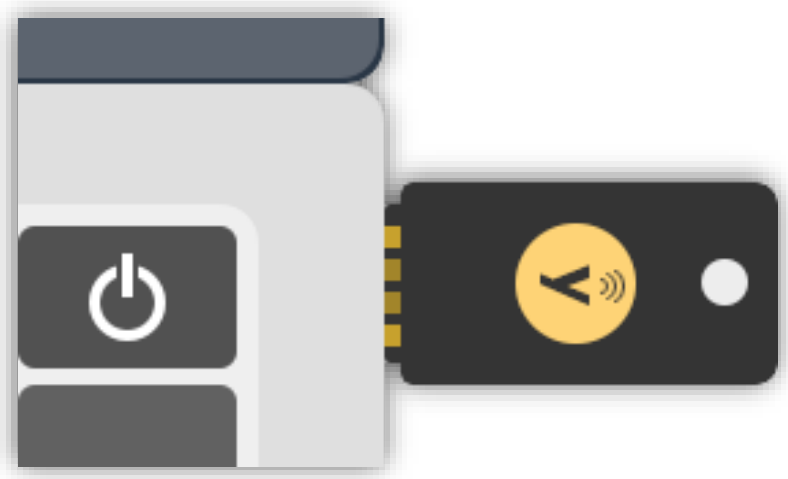
4. Connecting to PAM360's Web Interface after YubiKey TFA is Enabled

While logging into PAM360, the users for whom two-factor authentication is enabled will have to authenticate twice successively. The first level of authentication will be through the usual authentication method i.e., through PAM360's local authentication or AD/LDAP authentication, whichever is enabled for the user.

1. Launch PAM360's web interface, enter the **Username** and **Password** (local authentication or AD/LDAP), and click **Login**.
2. Once the first level of authentication succeeds, PAM360 will prompt you to enter your YubiKey one-time password.



3. Insert the YubiKey into the USB port of your laptop or computer.



4. Before generating a one-time password, you need to decide which slot of the YubiKey (slot 1 or slot 2) you're going to use for authentication throughout.
    - **Slot 1:** If you **tap the YubiKey once,** it generates a 44-character security key whose first 12 characters are unique to this slot. For every subsequent login through this slot, the first 12 characters remain the same and the rest of the 32 characters are randomized.
    - **Slot 2:** If you **tap and hold the YubiKey for 2-5 seconds,** it generates a 44-character security key whose first 12 characters are unique to this slot. For every subsequent login through this slot, the first 12 characters will remain the same and the rest of the 32 characters will be randomized.
    - Here's a sample output from a YubiKey where the button has been pressed three times.

        cccjgjgkhcbbirdrfdnlnghhfgrtnnlgedjlftrbdeut

cccjgjgkhcbbgefdkbbditfjrlniggevfhenublfnrev

cccjgjgkhcbbcvchfkfhiiuunbtnvgihdfiktncvlhck

> **Note:** By default, YubiKey generates slot 1 passcode for NFC configured mobile devices. You can set slot 2 passcode as default by changing the setting from slot 1 to slot 2 using the Yubikey Personalization tool.

5. PAM360 matches the 12-character key against your account in its database and verifies the same for the second level of authentication during future login attempts.
6. After submitting the YubiKey one-time password, click **Register and Login.**

Two-Factor Authentication (TFA) - One-Time Password

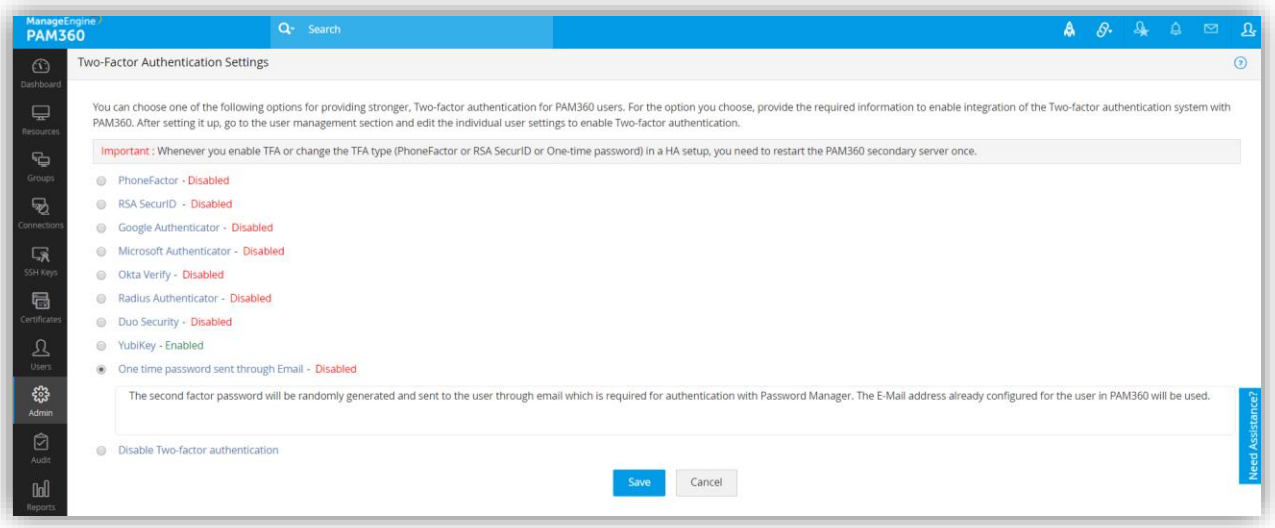
If you choose this option, after the first level of authentication through the usual way, PAM360 will randomly generate a unique password and it will be emailed to the user. The user has to enter the password sent by email to authenticate at the second level. The second level password generated and sent by PAM360 is applicable only for that particular session of the web-interface. If the user logs out and tries to log in again, they will not be allowed to log in with the same password sent by email earlier. The user has to fetch the password sent by email again and enter it for authentication.

Configuring One Time Password in PAM360 involves the following steps:

1. **Configuring TFA in PAM360**
2. **Enforcing TFA for Required Users**
3. **Connecting to PAM360 Web Interface when TFA is Enabled**

1. Configuring TFA in PAM360

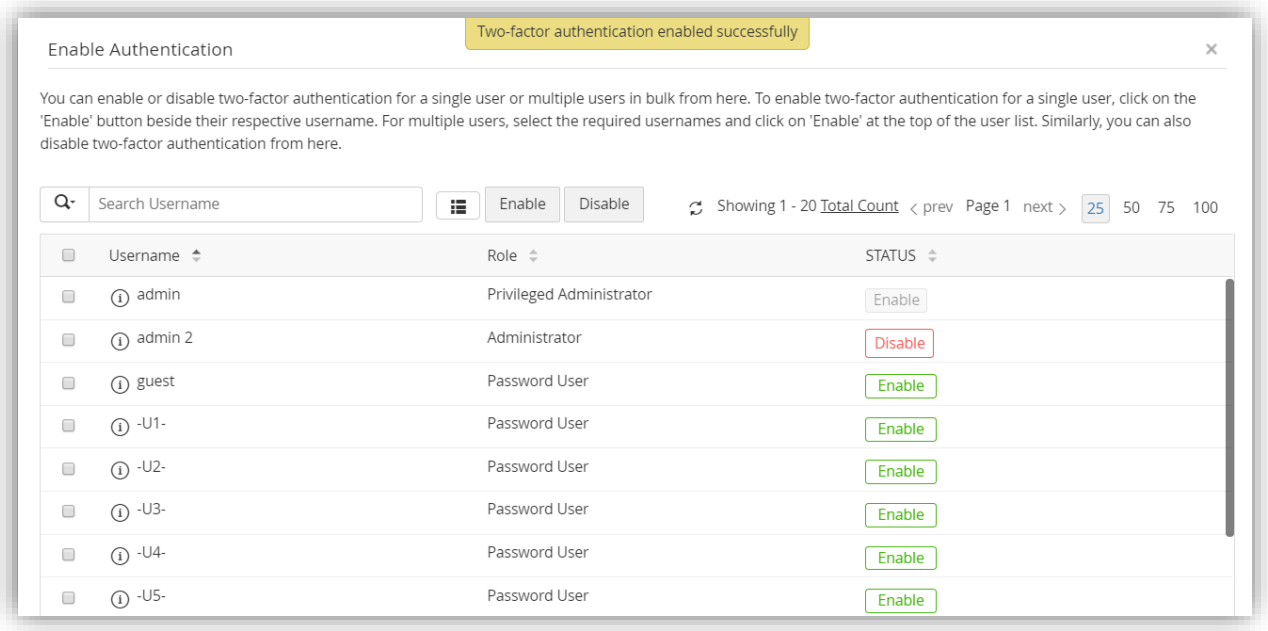
1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**.
2. Choose the option **One-time password sent through email**.
3. Click **Save**.



4. Then, click on **Confirm** to enforce OTP through email as the second factor of authentication.

2. Enforcing TFA for Required Users

1. Once you confirm OTP through email as the second factor of authentication in the previous step, a new window will prompt you to select the users for whom two-factor authentication should be enforced.
2. You can enable or disable Two-Factor Authentication for a single user or multiple users in bulk from here. To enable two-factor authentication for a single user, click on the **Enable** button beside their respective username. For multiple users, select the required usernames and click on **Enable** at the top of the user list. Similarly, you can also **Disable** TFA from here.



3. You can also select the users later by navigating to **Users >> More Actions >> Two-Factor Authentication.**

3. Connecting to PAM360 Web Interface when TFA is Enabled

Users for whom two-factor authentication is enabled, will have to authenticate twice successively. As explained above, the first level of authentication will be through the usual authentication. That is, the users have to authenticate through PAM360's local authentication or AD/LDAP/Azure AD authentication. If the administrator has chosen the TFA option **One time password sent through email**, the two-factor authentication will happen as detailed below:

1. Upon launching the PAM360 web-interface, the user has to enter the username and local authentication or AD/LDAP/Azure AD password to log in to PAM360 and click **Login**.
2. Once the first level of authentication succeeds, PAM360 will generate a random password and email it to the user.

3. The user has to fetch the password from the email and enter it as the second password.
4. If the second authentication succeeds, the user will be allowed to view the PAM360 web interface.

Note: The second level password generated and sent by PAM360 is applicable only for that particular session of the web-interface. If the user logs out and tries to log in again, they will not be allowed to log in with the same password sent by email earlier. When the user logs in again, another new password will be sent to their email which they must use for authentication.

If You have Configured High Availability:

Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password or RADIUS or Duo) AND if you have configured high availability, you need to restart the PAM360 secondary server once.

Resources and Resource Groups

PAM360 allows you to add the critical machines from your environment into the solution to manage them efficiently. PAM360 classifies any critical asset whose user accounts and passwords are to be managed by PAM360 as a '**Resource**'. A 'resource' can be any server, application, network device, or appliance in your environment that carries authentication credentials that need to be secured from external attacks and managed regularly. The term **Account** denotes the 'User Account' & 'Password' that are a part of a '**Resource**'. PAM360 allows you to add all the accounts pertaining to the resources and manage them individually in the product.

A large enterprise organization's IT network typically contains multiple critical machines that have similar needs in terms of management. In this case, it is beneficial to group the machines together based on their individual need or criteria and oversee them together. PAM360 offers the resource group functionality to solve this challenge. A **Resource Group** in PAM360 denotes the group to which a particular resource belongs. For example, if you have some Windows 10 servers among several other Windows servers, you can group all the Windows 10 servers as a single resource group.

Once your PAM360 setup is complete, import users and user groups from your environment into the solution through various means such as manual addition, user addition using API, and via discovery. PAM360 offers multiple authentication methods to choose from, such as Active Directory, Azure AD, LDAP, Radius authentication. In addition, there are several options available for SAML single sign-on and two-factor authentication as well.

The **Resources** tab in PAM360 serves as an expansive space in which you can view and manage all the resources owned by you and/or shared to you by other administrators, along with the related accounts, and their respective passwords. The **Password Explorer** tree in the Resource tab contains a variety of options that consolidate all your resources based on criteria such as the resource groups they are part of, how frequently they are accessed, and so on.

The below sections explore the wide range of operations you can perform from the Resource tab and covers the way in which you can utilize the powerful privileged account management features in PAM360 to their fullest.

1. Exploring the Resources Tab
2. What is the Password Explorer Tree?
3. What Can I Do from the Resources Tab?
4. Resource Groups
5. Possible Actions from the Resources Tab

1. Exploring the Resources Tab

Navigate to the **Resources** tab to get started with adding resources to PAM360. The **Resources** tab is broadly divided into three parts:

i. A list view of all resources and accounts owned by you and/or shared to you.
ii. The Password Explorer on the left pane.
iii. The display area in the middle - The display area in the middle displays the list of resources under the specific category as and when you click from the Password Explorer.

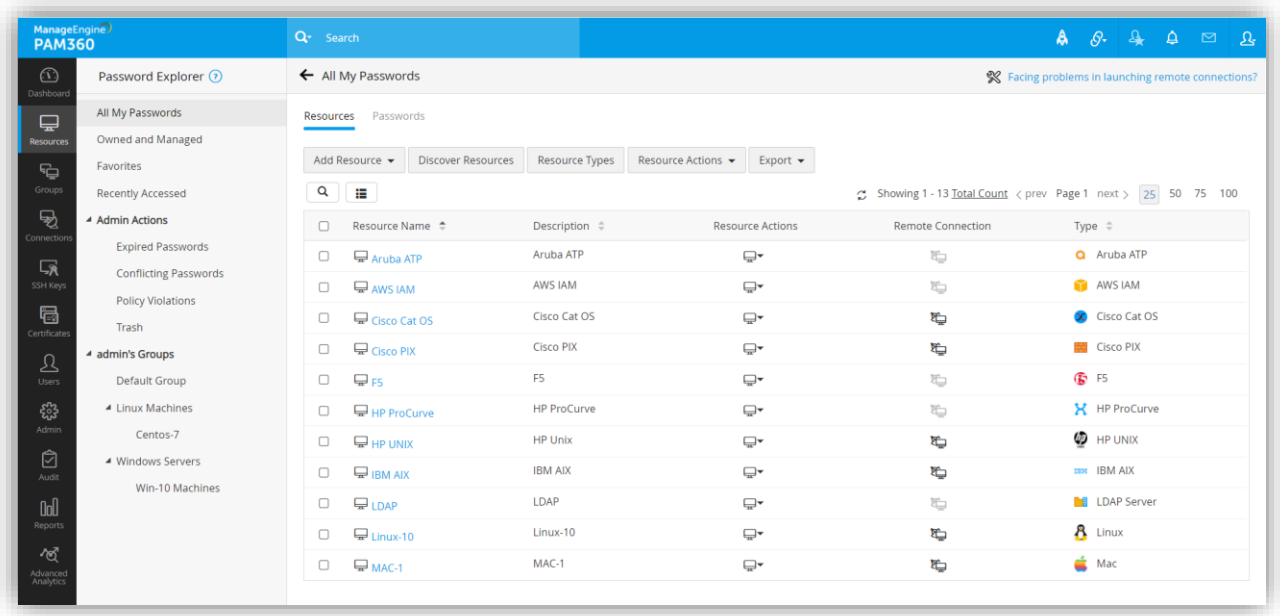
The **Password Explorer** tree on the left pane displays an array of available resources arranged based on categories, such as **All My Passwords, Owned and Managed, Favorites,** and **Recently Accessed**. It also contains two other sections: **Admin Actions** and **Groups.** The section below explains each category in detail.

2. What is the Password Explorer Tree?

The Password Explorer tree organizes all the available resources in PAM360 and displays them under different categories. Click a category name to view the resources that are specific to the selected category. Read further to learn in detail about each category:

1. **All My Passwords** - Click this option to display all the resources that are shared to you and available for your usage. Click the name of a resource to display all accounts corresponding to the selected resource. To search for a resource, click the search icon and enter the resource name, description, or the operating system (OS) type. There is a wide range of operations to be performed on the resources and passwords you have access to. They are explained in detail in the upcoming sections below.
2. **Owned and Managed** - This option is for users with administrator privileges. All resources owned by administrators and shared to them by other users are available here. Click the name of a resource to display all accounts corresponding to the selected resource. To search for a resource, click the search icon and enter the resource name, description, or the operating system (OS) type.
3. **Favorites** - All accounts marked as a 'favorite' are available here. To mark an account as a favorite, go to the **All My Passwords** or **Owned and Managed** section, switch to the **Passwords** tab, and click the star icon (☆) beside an account name. To search for a resource under the **Favorites** section, click the search icon and enter the resource name or the user account name.
4. **Recently Accessed** - All recently accessed resources are listed under this option for a quick reference. To search for a resource, click the search icon, and enter the resource name or the user account name.
5. **Admin Actions** - This section comprises of the following categories: **Expired Password, Conflicting Passwords, Policy Violations, Disabled Resources,** and **Trash.** This section compiles all the accounts whose passwords might require your immediate attention; for example, you may want to perform a bulk password reset on all the expired passwords or restore a resource that was mistakenly deleted, from the trash. All the operations to be performed under Admin Actions are explained below.

6. **Resources groups added by you** - PAM360 allows you to maintain a hierarchical structure for resource groups in, i.e., the tree view. For example, let's assume that your organization contains departments that follow a hierarchy. You can group the resources belonging to the respective levels and create subgroups as required — PAM360 will display them in a tree view in this section to represent the hierarchy they follow in your organization.



3. What Can I do from the Resources Tab?

There is a wide range of actions you can perform over the resources and accounts displayed in the various sections of the **Resource** tab. The below sections explain each of them in detail:

1. **Resource and Account-based operations**
2. **Admin Actions**

3.1 Resource and Account-based Operations

The Resource tab offers exhaustive options for adding and managing resources in PAM360. Each operation is listed below with a link that will explain in detail about how that particular feature works:

i. Add resources into PAM360
ii. Manage resource types
iii. Manage resources
iv. Manage accounts and passwords
v. Share resources and accounts
vi. Additional resource configurations

i. Add Resources into PAM360

Add your privileged resources such as servers and endpoints as resources in PAM360 to start managing their accounts and passwords. There are three ways in which you can add resources and accounts into PAM360: Manual addition, import from file, automatic discovery of resources and accounts. Click the respective links to learn about each topic in detail.

ii. Manage Resource Types

PAM360 supports a wide range of resource types by default. In addition to that, you can add as many custom resource types as you require. Click here to learn in detail about how to manage various resource types in PAM360.

iii. Manage Resources

PAM360 offers extensive options to manage the resources added to the repository. Listed below are the resource-based operations that you can perform in PAM360. You will have learned the following in the

1. Export resources
2. Edit resources
3. Delete resources
4. Copy resources
5. Transfer ownership of resources

iv. Manage Accounts and Passwords

There are different ways in which you can manage the accounts and passwords saved in the PAM360 repository. Some of the operations include viewing, editing, copying, moving accounts, changing passwords, and viewing password history. Click here to learn in detail about each operation.

v. Share Resources and Accounts

PAM360 offers an option to securely share your resources and accounts with other users and/or user groups. Click the links below to learn about each topic in detail.

Share resources and accounts with users and user groups

Share resources and accounts in bulk

vi. Additional Resource Configurations

PAM360 offers several additional resource configurations that you can use to enhance the security of the resources stored in PAM360 and to use them efficiently. Click the below links to learn about each topic in detail:

1. Configure auto logon helper
2. Session recording
3. Remote_Password_Reset

4. Password access control

3.2 Admin Actions

The **Admin Actions** section of the Password Explorer tree provides a consolidated view of expired passwords, passwords that may be violating password policies set by the admin, disabled resources, and Trash. While the PAM360 Dashboard provides a global view of expired/conflicting passwords and policy violations, the Admin Actions section gives a concentrated view of only the passwords owned and managed by you. From this section, you can reset the passwords that are in violation, either selectively or in bulk. Admin Actions section also displays the disabled resources that were imported into PAM360 during an Active Directory/LDAP import. Any resource that was moved to trash during deletion will be visible under the **Trash** category in this section. Each category under **Admin Actions** is explained in detail below:

1. Expired Passwords
2. Conflicting Passwords
3. Policy Violations
4. Disabled Resources
5. Trash

3.2.1 Expired Passwords

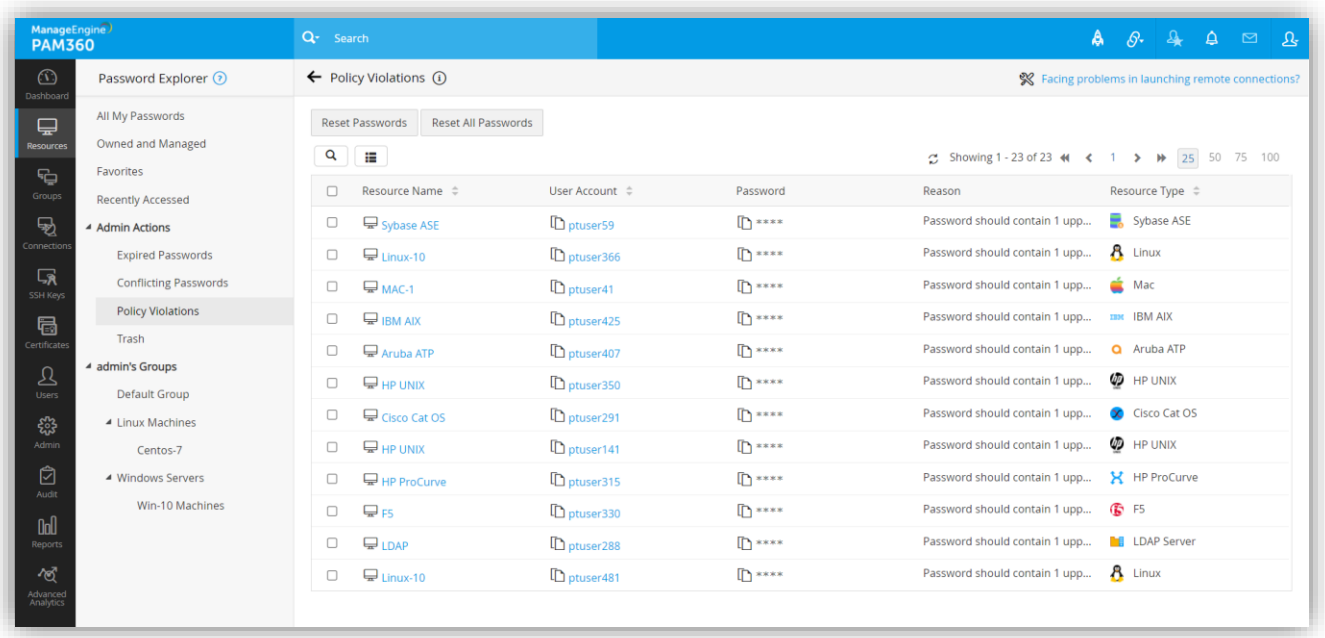
Passwords that are not reset within the maximum number of days specified in the password policy are considered to be expired.
Each password policy comes with a different **Maximum Password Age** in days; PAM360 flags any password that has not been renewed after this time period as expired passwords. This section lists all expired passwords of the accounts that are owned or managed by you.

3.2.2 Conflicting Passwords

Conflicting passwords arise when the password of an account stored in the PAM360 repository is not in sync with the password of the same account in the remote machine. Resetting the password of an account in PAM360 without applying the changes to the remote resource or vice versa leads to conflict in passwords. If left unchecked, out of sync passwords can lead to authentication failure and security issues. As a safety measure, PAM360 runs a periodic password integrity check that ensures that all passwords stored in PAM360 match the ones in the corresponding remote machines. Passwords that are found to be mismatched will be flagged and displayed in this section.

3.2.3 Policy Violations

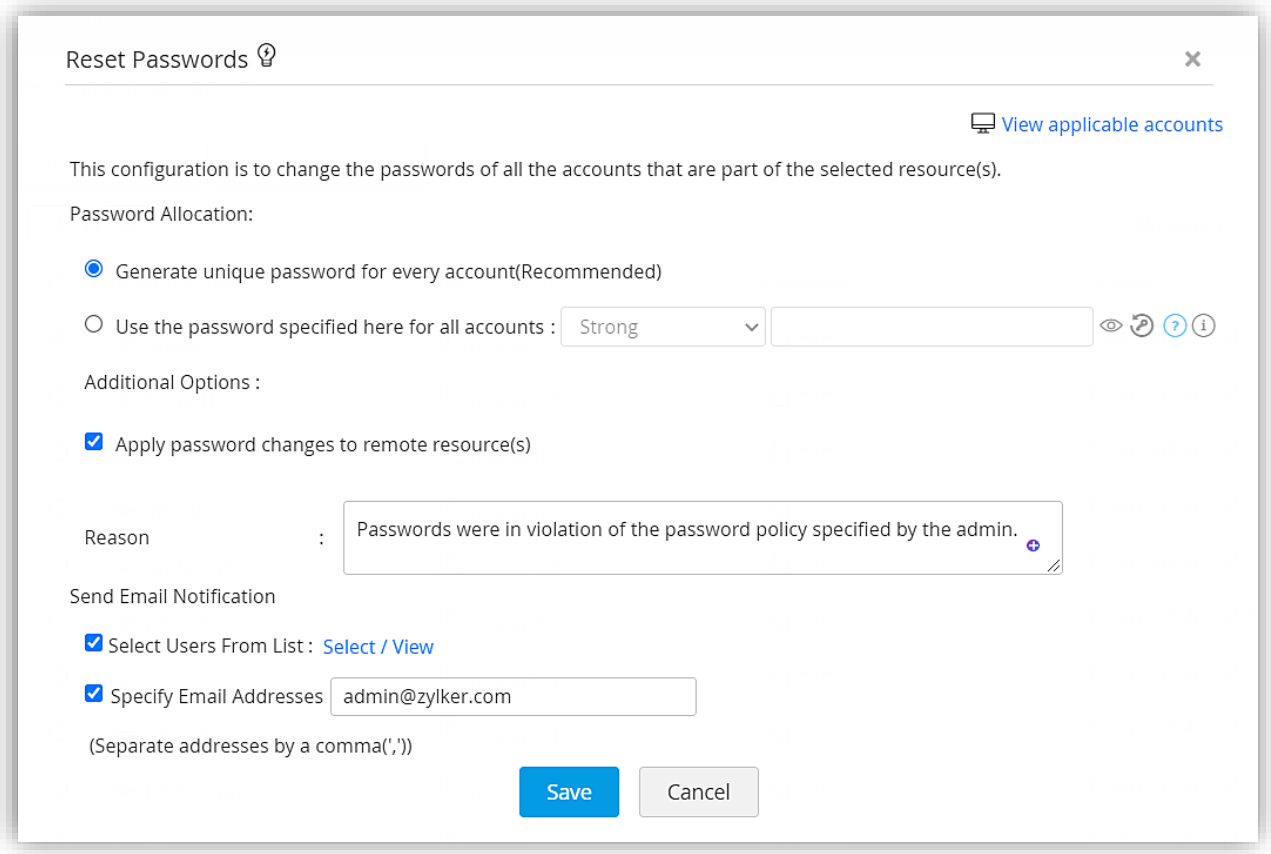
Passwords that violate the password policies applied in PAM360 will be displayed in this section. By default, PAM360 has three password policies: Strong, Medium, Low — they all come with varying levels of complexity. You can also set your own custom password policies and apply that to your passwords. PAM360 runs a periodic check to ensure the complexity of the passwords match the complexity specified in the password policies chosen for them; any password that does not pass the check will be flagged and displayed here.



You can reset the passwords displayed in the above three sections using the password reset configuration settings provided by PAM360.

Password Reset Configuration

1. To reset a selection of passwords, select the required passwords using the checkbox beside each one and click the **Reset Passwords** option at the top.
2. In the pop-up that appears, you can either manually specify a password. This password will be applied to all selected accounts. Or, you can allow PAM360 to generate a unique password for each account.
3. If you select the **Apply password changes to remote resource(s)** option, PAM360 will change the passwords of the remote resources after resetting passwords here. This operation will avoid a mismatch of passwords between the remote machine and the password reflecting in PAM360.
4. There is also a provision to send an email notification about the password reset to others. You can either choose users from PAM360 to notify or specify email addresses to which you wish to send the notification. Click **Save** once you have chosen your preferred configurations.
5. To reset all of the passwords under this category, simply click **Reset All Passwords** without selecting any password from the list below. This action will reset all expired passwords in bulk. The status of the password reset operation will be captured under **Audit >> Resource Audit**.



3.2.4 Disabled Resources

While importing resources from Active Directory/LDAP into PAM360, you can choose to include disabled machines also. After the import is done, all the disabled resources will be consolidated under this section.

3.2.5 Trash

While deleting resources in PAM360, you can choose to delete them permanently or move them to the **Trash**. In this section, you can view all the resources that are moved to trash during deletion.

1. **Restore**: To restore a resource from **Trash**, select the resource, and click **Restore**. The selected resource will be restored to the Resources tab.
2. **Delete**: To delete resources from the Trash selectively, click the checkboxes beside the required resources, and click **Delete**.
3. **Empty Trash**: To delete all resources from the **Trash** section, click the **Empty Trash** option. Please note that this action will only remove trashed resources that are owned by you.

Click here to learn more about deleting resources.

4. Resource Groups

The Resource Groups are accessible from the **Resources** tab. The Password Explorer displays all the resource groups and the corresponding subgroups that you create. Within the resource groups, you can perform all resource and account related operations explained in this section. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type. PAM360 allows you to group Resources of similar attributes for easier management. You can create two types of Resource groups:

- Static resource group
- Dynamic resource group

In the case of a static resource group, you need to mark individual resources that are to be grouped together and create a resource group with a relevant name and description. You can manually add resources to the group at any point in time.

In the case of a dynamic resource group, you need to specify a set of criteria while creating the group. Whenever a new resource is added to PAM360, if it fits the criteria specified for a particular group, the resource is automatically added to the group. For example, let's say you create a group **CV-WinDom-01** for the resource type Windows Domain. In this case, all Windows Domain resources added at any point of time after the creation of this group will automatically be a part of **CV-WinDom-01**.

Similar to how resources and accounts can be shared, resources groups can be shared with other users and user groups as well. However, please note that whenever resources get added or deleted from a group, it affects the password access shared through the group. That is, users with whom a particular resource group has been shared can see passwords of only the resources that are part of the group at that point in time.
To learn more about how to create and manage resource groups in PAM360, click here.

5. Possible Actions from the Resources Tab

The below links take you to the detailed documents that will help you discover, add, and manage various resources types, create resource groups for efficient management of the resources, and gain complete control over the passwords of the resources. Click through each link below to learn about the respective feature.

1. Discovering Resources and Privileged Accounts
2. Adding_Resources_Manually
3. Importing_Resources
4. Storing Files
5. Managing_Resources
6. Sharing_Individual_Resources
7. Sharing Resources in Bulk

8. Managing_Accounts_and_Passwords
9. Managing_Resource_Types
10. Working with Passwords
11. Password_Reset
12. Managing_Resource_Groups
13. Nested_Resource_Groups
14. Exporting_Resource_Groups
15. IIS Web Config. Discovery

Discovering Resources and Privileged Accounts

PAM360 provides the option to automatically discover endpoints in your environment and enumerate the privileged accounts associated with them. This helps enterprises to secure all their privileged identities swiftly and randomize the passwords of the accounts, upon discovery and thereafter at periodic intervals. It is possible to discover a variety of devices such as Windows, Linux, VMware and Network devices, and also the service accounts associated with Windows and Linux (SSH only) domain accounts.

The entire privileged accounts discovery process can be split into the following steps:

1. Discovering Resources
   - 1.1 Prerequisites (common for all resources)
   - 1.2 Steps to Discover Resources
     - 1.2.1 Windows
     - 1.2.2 Linux
     - 1.2.3 Network Devices
     - 1.2.4 VMware
     - 1.2.5 AWS EC2
     - 1.2.6 Amazon WorkSpaces
   - 1.3 Scheduled Resource Discovery
   - 1.4 Track discovery status
2. Adding the discovered Resources into PAM360
   - 2.1 Windows
   - 2.2 Linux
   - 2.3 Network Devices
   - 2.4 VMware
   - 2.5 AWS
3. Discovering Privileged Accounts
   - 3.1 Accounts Discovery: Prerequisite

3.2 Database accounts discovery
3.3 Discover Privileged Accounts of Individual Resources
3.4 Automated periodic discovery of privileged accounts
3.5 PAM360 MSP Edition
3.6 Randomize Passwords Post Discovery

Apart from the above topics, you will also learn how to Randomize Passwords Post Discovery.

1. Discovering Resources

1.1 Prerequisites (common for all resources)

Make sure you have installed the following, before commencing the discovery:

- Microsoft .Net framework 4.5.2 or above.
- Microsoft Visual C++ 2015 redistributable.

1.2 Steps to Discover Resources

The first step to adding resources to PAM360 is the discovery of different endpoints present in your network. The following sections explain how PAM360 goes about discovering different endpoints:

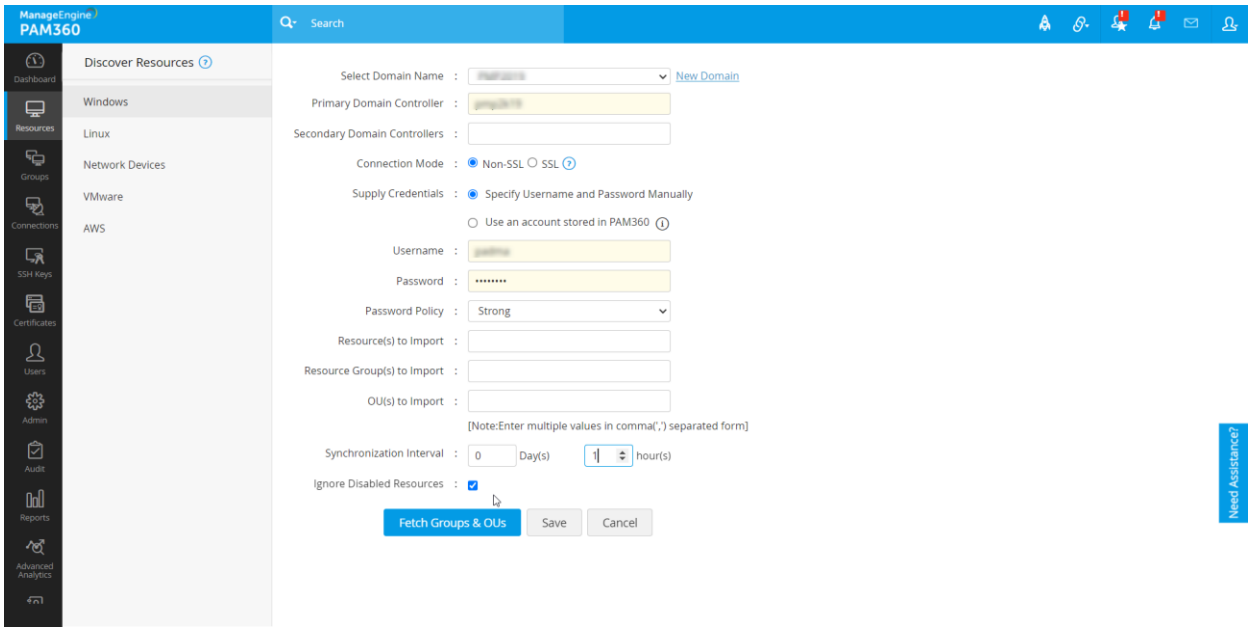
1.2.1 Windows:

PAM360 automatically discovers and lists all the Windows domains from the Windows domain controller, where the PAM360 is running. All you need to do is to select the required domain and provide the domain controller credentials.

Windows servers can be discovered directly from Active Directory. WMI API is used to connect with the domain controller and fetch the list of all the servers/workstations that are part of the selected Group/OU. Then, the WMI connection is established to reach out to each Windows end-point for device discovery.

Steps to Discover Windows Servers:

1. Navigate to **Resources >> Discover Resources >> Windows**. The below wizard is displayed.



2. Fill in the details as mentioned below:

   i. Choose a **Domain Name**, from which the assets are to be imported, from the drop-down list [OR] click **New Domain >> Add** and enter a new domain name.

   ii. Specify the **Primary Domain Controller.**

   iii. Specify one or more **Secondary Domain Controllers**.

> **Note:** Mention the DNS names of the secondary domain controllers as comma-separated values. One of the listed controllers will be used when the primary controller is down. When you use SSL mode, make sure the DNS name specified here matches the CN (common name) specified in the SSL certificate for the domain controller.

   iv. For each domain, you can configure the connection either through **SSL** or **Non SSL**. (PAM360 strongly recommends encrypted communication via SSL for enhanced security).

   v. Supply valid credentials.

      A. **Specify a valid Username/Password manually:**

         a. Specify the DNS name of the domain controller along with a valid user credential (Username/ Password) which has read permission in that domain controller.

         b. If you want to discover users from multiple domains, enter the

username as **<DomainName >\<username>**. For example, if you want to discover users of DOMAIN A users by giving DOMAIN B username/password, you need to enter the username as <DOMAIN B>\username. Any procedure that you normally use to import the SSL certificates to the machine's certificate store can also be followed to import the domain controller's certificate into PAM360's store. Just ensure that the certificate is in the base 64 format and it is stored in the PAM360 bin directory, after which it can be imported to use with PAM360.

c. In the machine where PAM360 is installed, launch Internet Explorer and navigate to **Control Panel >> Internet Options >> Content >> Certificates**.
d. Click **Import. Browse** and locate the root certificate issued by your CA.
e. Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
f. Again click **Import**.
g. Browse and locate the domain controller certificate.
h. Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
i. Apply the changes and close the wizard.
j. Repeat the procedure to install other certificates in the root chain.

B. **Use an Account Stored in PAM360**:
   a. You can use a user account which is already stored in PAM360. This step will help PAM360 gain access and fetch the user accounts present under the specified domain name.

> **Note:** This option allows PAM360 server to communicate with this particular domain controller over SSL. Repeat the following steps for all domain controllers to which you want PAM360 to communicate with over SSL. Note that the DNS name you specify for the domain controller should match the CN (common name) specified in the SSL certificate for the domain controller.

   b. Select the required password policy from the **Password Policy** dropdown. You can also specify password policy for each group or

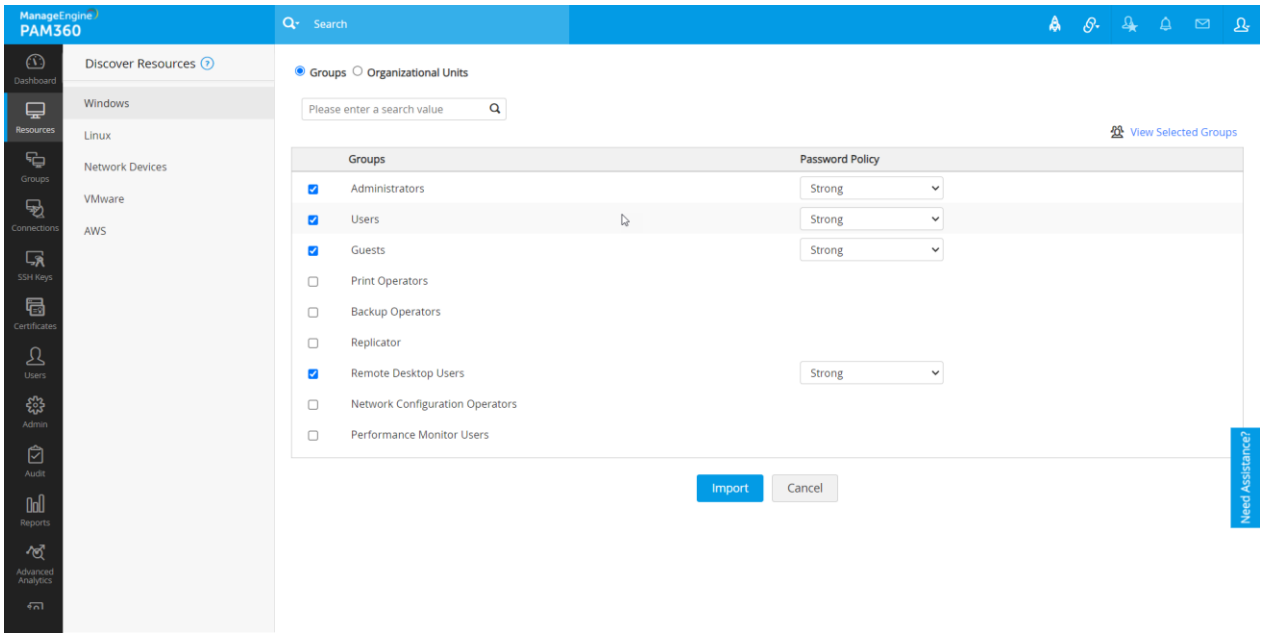
organizational unit while fetching them before the import process.

c. Specify Resources, Resource Groups or OU's by specifying their names as comma-separated values in the respective text fields.

d. If you want to import only a particular resource, enter the required resource name(s) in comma-separated form in the **Resource(s) to Import** field.

e. Similarly, you can choose to import only specific resource groups or OUs from the domain. You can specify the names in the **Resource group(s) to Import** or **OU(s) to Import** fields respectively, in comma-separated form.

3. If you have specified a resource, a resource group, or an OU, click on **Import** to initiate the process. If you have left the fields empty, you can click on **Fetch Groups and OU's** to enumerate all the available resources from which you can choose and import. To view the selected groups before importing, click on **View Selected Groups**.



4. PAM360 periodically queries the AD to keep the resources in sync - new resources added to the AD are automatically added to PAM360 to keep the resources database in sync. All you need to do is enter the time interval for PAM360 to query the AD and ensure to set the sync interval to 3 hours or more based on the number of resource groups and OUs discovered. Click **Save**.

5. Click **Fetch Groups & OUs**.

6. On successful discovery of resources, you can add **All/ Selected Resources** into

PAM360.

1.2.2 Linux:

PAM360 uses **Telnet** and **SSH** as the remote connection modes to discover the devices, where Telnet/SSH are running.

Steps to Discover Linux Servers:

1. Navigate to **Resources >> Discover Resources >> Linux**.
2. Choose to discover using either of the **Telnet** or **SSH**.

    i. **Discover using Telnet:**

        a. Choose the **Connection Mode** as **Telnet**.

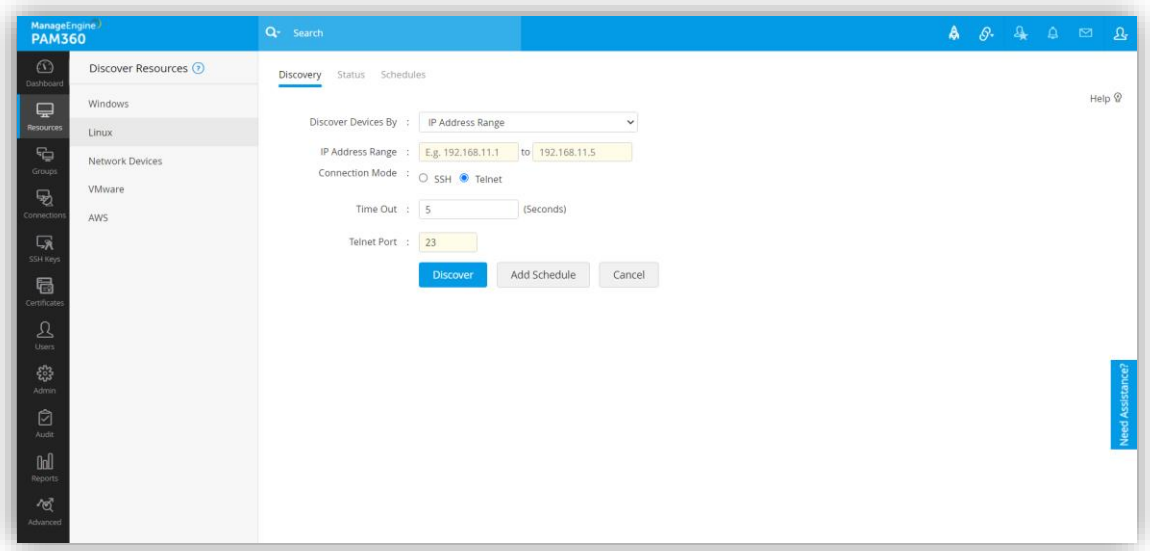
        b. As mentioned in Network Devices discovery part, you can discover a single VM device by specifying the host name or IP address OR multiple devices present in an IP range OR discover multiple devices whose details are available in a flat file.

        c. You can set the maximum **Time Out** period to be up to 999 seconds, within which the devices must be discovered.

        d. Enter the **Telnet Port** number (default port- **23**).

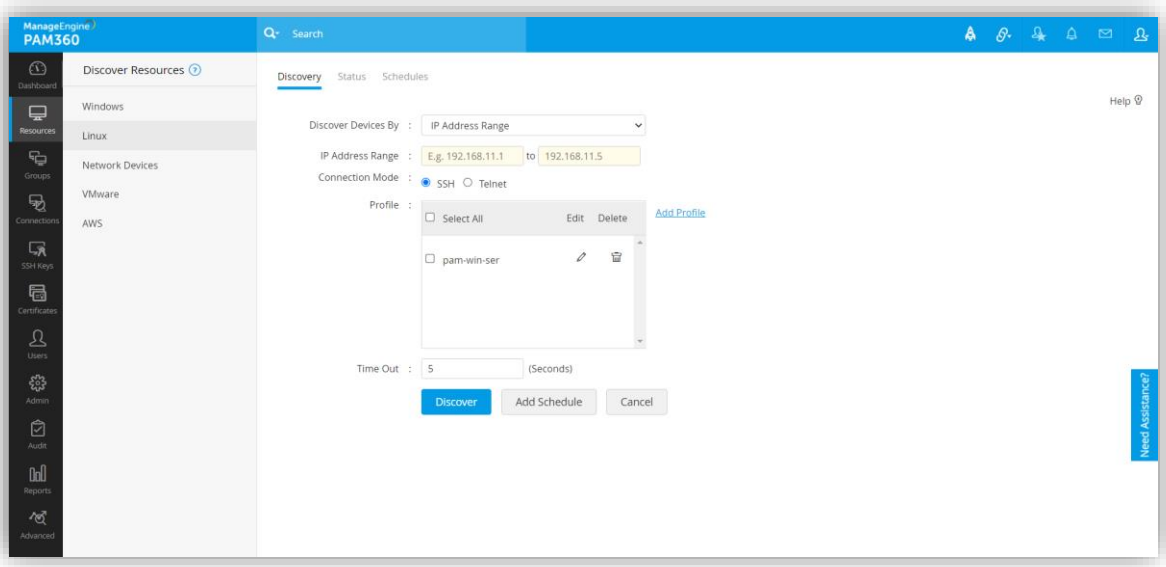
        e. Click **Discover**. A **Discovery Confirmation** window pops up. Choose whether to send notifications to **"All administrators"** or to specific people. If you choose the latter option, specify the email addresses separated by commas. Click **Proceed**. Now, you will see the **Discovery Status** page where the discovered device will be added as a task. You will also see other details such as date/time when the discovery was invoked, completed, etc.

        f. If you want to schedule a periodic resource discovery, click **Add Schedule.** You will see a new window where you can create an automated scheduled task for discovering the newly added accounts during resource discovery. Refer to the Scheduled Resource Discovery scetion to know more in detail.



Note: If the device to be discovered is present on a subnet, different from the host where PAM360 is running, discovery might take longer than the actual timeout specified, due to extended connectivity time. The Telnet option will be disabled soon, and you will have only "SSH" as the dedicated remote connection mode.

ii. **Discover using SSH:**

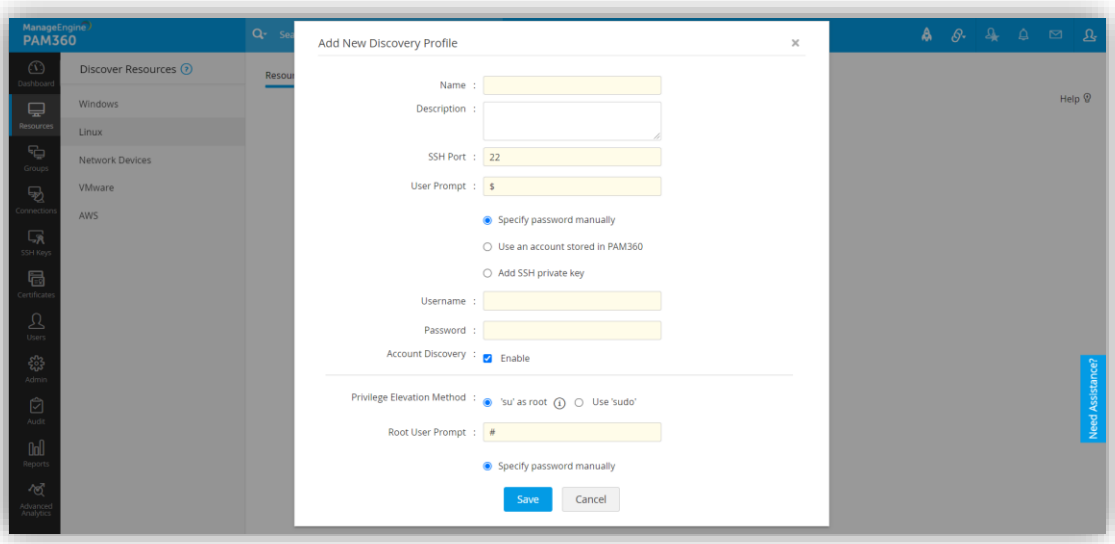


A. Choose the **Connection Mode** as **SSH**.

B. As mentioned in Network Devices discovery part you can discover a single device by specifying the host name or IP address OR multiple devices

present in an IP range OR discover multiple devices whose details are available in a flat file.

C. Initiate the profile configuration process. Choose an existing discovery profile(s) or click **Add Profile**.



D. The **Add New Discovery Profile** wizard is displayed.

a. Fill in details such as **Name**, **Description**, **SSH Port number** and **User Prompt**.

b. Configure credentials in either of the below 3 ways:

i. **Specify the password manually**: If you choose this option, you need to enter a valid **Username** and **Password**.

ii. **Use an Account Stored in PAM360**: If you choose this option, you need to choose a **Resource Name** and an **Account Name** from the respective dropdowns.

iii. **Add SSH private key**: If you choose this option, you need to enter details such as **Username**, **Private Key Name** and the **Private Key Password**. Choose a valid **SSH key file.**

c. **Account Discovery**: Besides resource discovery, SSH connectivity allows discovery of related account(s), as well from the machine. By default, this option will be enabled. Disable, if you don't want any account(s) to be discovered.

d. Choose a **Privilege Elevation Method**: This option appears only if you have enabled account discovery in the previous step.

i. **'su' as root**: If you choose this option, provide the credentials of a **super user only**, in the fields that follow.

ii. **Use 'sudo':** If you choose this option and if the credentials configured in step (ii) is of a "sudo" privileged user, then all the resources(s) and the related account(s) will be discovered. If the credentials configured in step (ii) is of a "normal" user, then only the resource(s) will be discovered.

e. Click **Save.**

E. Set the maximum time limit within which the device discovery is expected to be completed. Specify a **Time Out** value, in **seconds**.

F. Click **Discover**. A **Discovery Confirmation** window pops up. Choose whether to send notifications to **All administrators** or to specific people. If you choose the latter option, specify the email addresses separated by commas. Click **Proceed**. Now, you will see the **Discovery Status** page where the discovered device will be added as a task. You will also see other details such as date/time when the discovery was invoked, completed, etc.

G. If you want to schedule a periodic resource discovery, click **Add Schedule.** You will see a new window where you can create an automated scheduled task for discovering the newly added accounts during resource discovery.

> **Note:** If the device to be discovered is present on a subnet, different from the host where PAM360 is running, discovery might take longer than the actual timeout specified, due to extended connectivity time.

1.2.3 Network Devices:

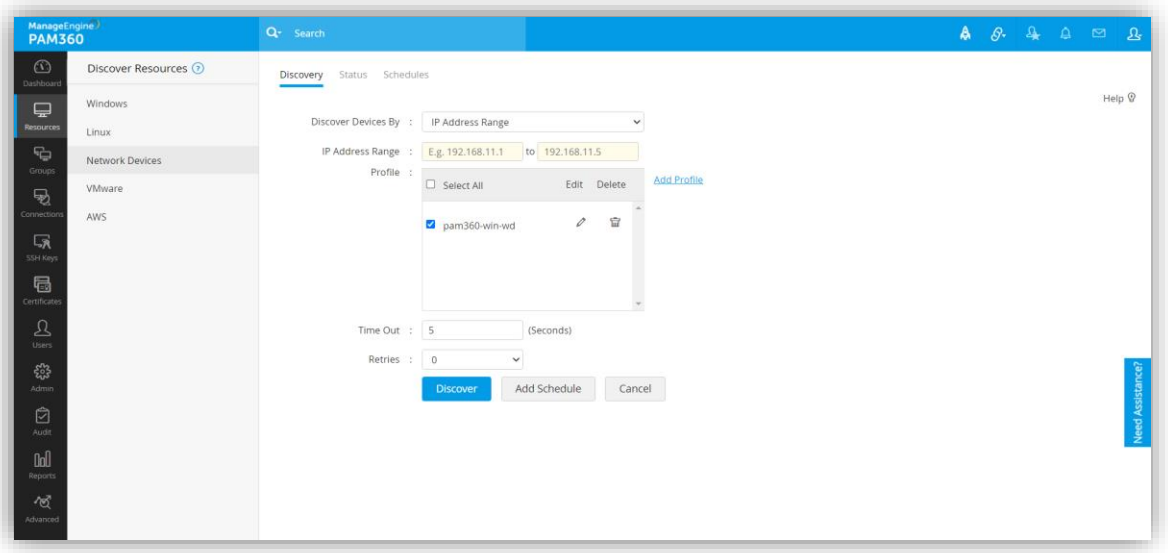
Prerequisite - Create discovery profiles

Before proceeding with discovering the network devices, you should create discovery profiles that help PAM360 to use common details for discovering multiple devices.

Steps to Discover Network Devices:

1. Navigate to **Resources >> Discover Resources >>Network Devices**.
2. There are three different options to discover the devices:
    i. Discover a single device by specifying the **Host Name / IP Address** (Sample values are **192.168.1.1, cisco2611**, etc.).
    ii. Discover multiple devices by entering an **IP Address Range** (e.g. **192.168.11.1** To **192.168.11.5**).
    iii. Discover IT assets in bulk by **importing a file** containing multiple Host Names / IP Addresses. Enter one value per line and specify the IP Address Range as comma-

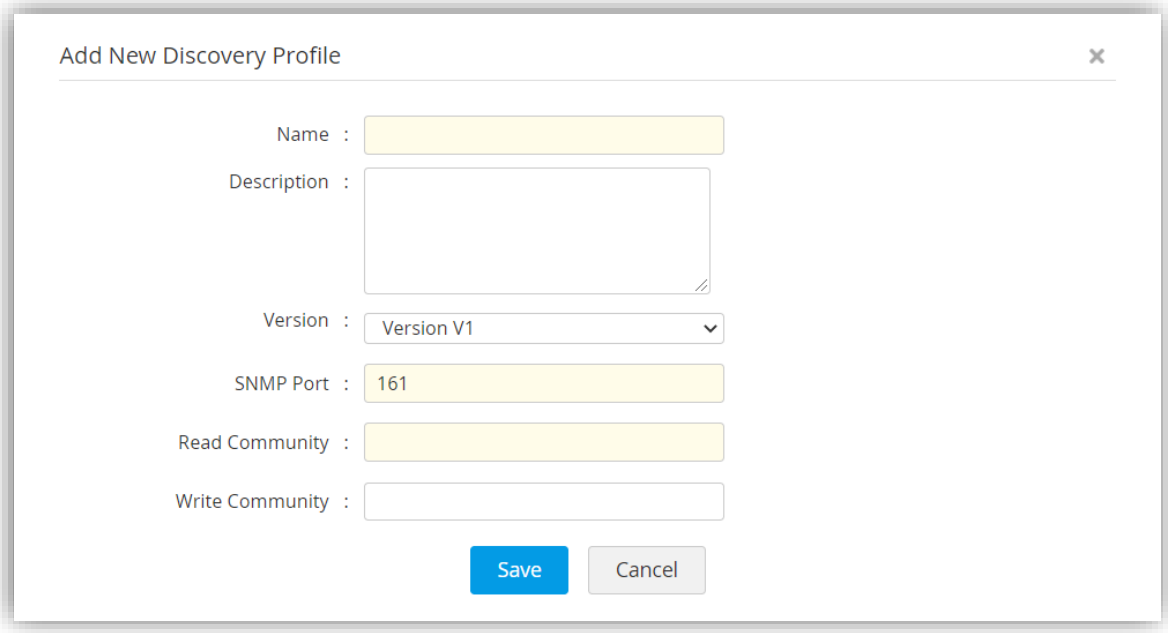
separated or tab-separated values.



Note: At present, PAM360 supports **IPV4** format only.

3. Choose an existing discovery profile(s) [OR] click **Add new profile** beside the Profile field, to initiate the profile configuration process. SNMP versions V1, V2C, V3 are used for performing a GET of sysobject ID for identifying the network device vendor and model information. The profile creation process for each of the protocols has been explained below:

    A. **SNMP - V1, V2c:**



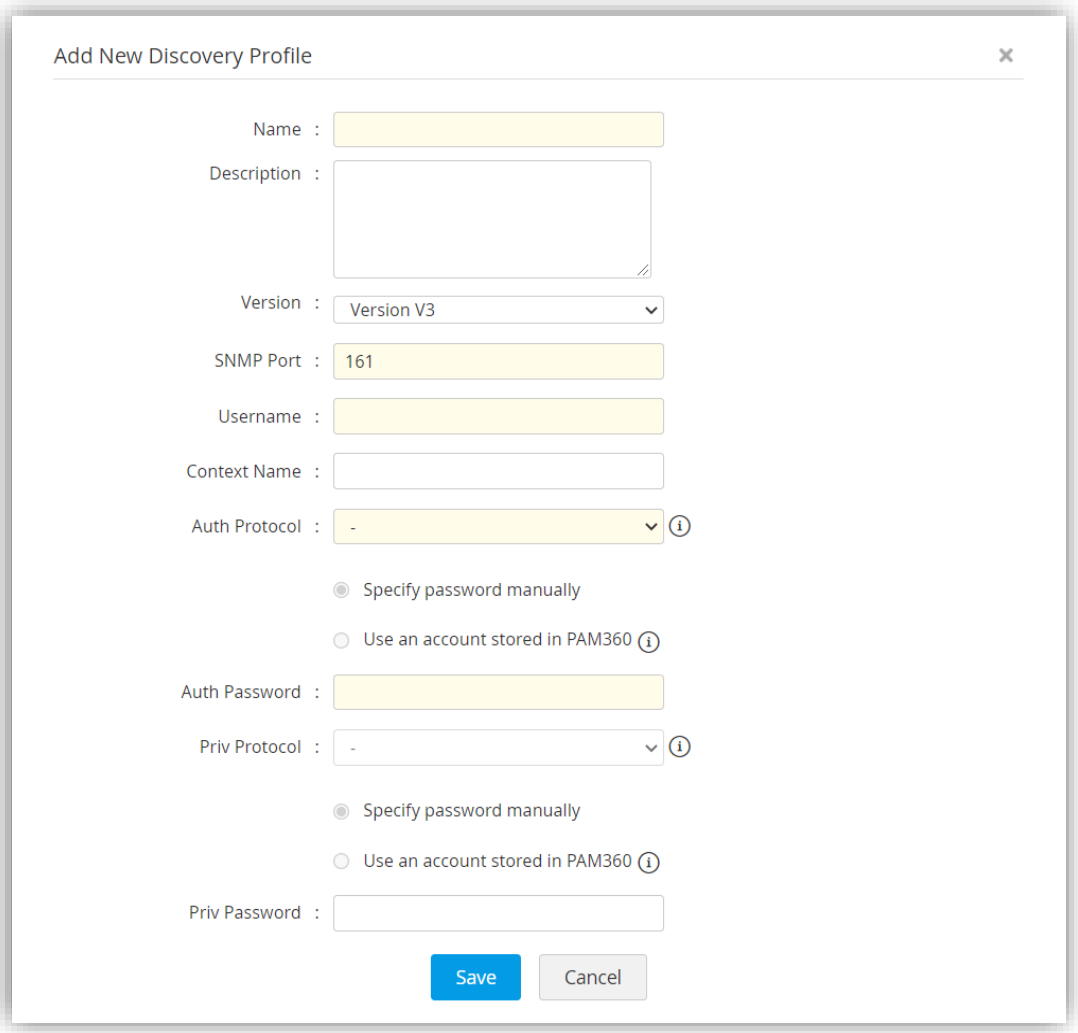
For creating a profile for devices making use of SNMP V1 and V2c:

a. Enter the new profile **Name**. This name uniquely identifies the profile.
b. Enter a **Description** about the profile for your reference.
c. Select the SNMP Version SNMP V1 or V2c in the Version drop-down list.
d. Enter the **SNMP Port** number.
e. Enter the **Read Community (**mandatory). Optionally, you can also specify the Write Community.
f. **Save** the profile.

B. **SNMP V3:**

For creating a profile for devices using SNMP V3:

a. Enter a unique profile **Name**.
b. Enter a **Description** about the profile for your reference.
c. Select the SNMP Version from the Version drop-down list as Version V3.
d. Enter the **SNMP Port** number.



e. **User Name**: Enter the name of the user (principal) on behalf of whom the message is being exchanged.

f. **Context Name**: An SNMP context name or "context" in short, is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context. An SNMP entity potentially has access to many contexts. In other words, if a management information has been defined under a certain context by an SNMP V3 entity, any management application can access that information by giving that context name. The "context name" is an octet string, which has at least one management information.

g. **Authentication** Protocol & Password: Select any of the authentication protocols (MD5 or SHA) and enter the password. MD5 and SHA are processes which are used for generating authentication/privacy keys in SNMPv3 applications.

h. You can either enter the password **manually** or use a **user account** stored in PAM360. **(Follow above steps)**

i. **Priv Protocol:** Select the required privacy protocol and also specify the Priv Password.

j. **Save** the profile.

4. To avoid time-delay, you can set the number of **Retries** (maximum 5) up to which PAM360 should keep attempting to discover the devices.
5. Click **Discover**. A **Discovery Confirmation** window pops up. Choose whether to send notifications to **All administrators** or to specific people. If you choose the latter option, specify the email addresses separated by commas. Click **Proceed**. Now, you will see the **Discovery Status** page where the discovered device will be added as a task. You will also see other details such as date/time when the discovery was invoked, completed, etc.
6. If you want to schedule a periodic resource discovery, click **Add Schedule.** You will see a new window where you can create an automated scheduled task for discovering the newly added accounts during resource discovery. Refer to the Scheduled Resource Discovery section to know more in detail.

1.2.4 VMware:

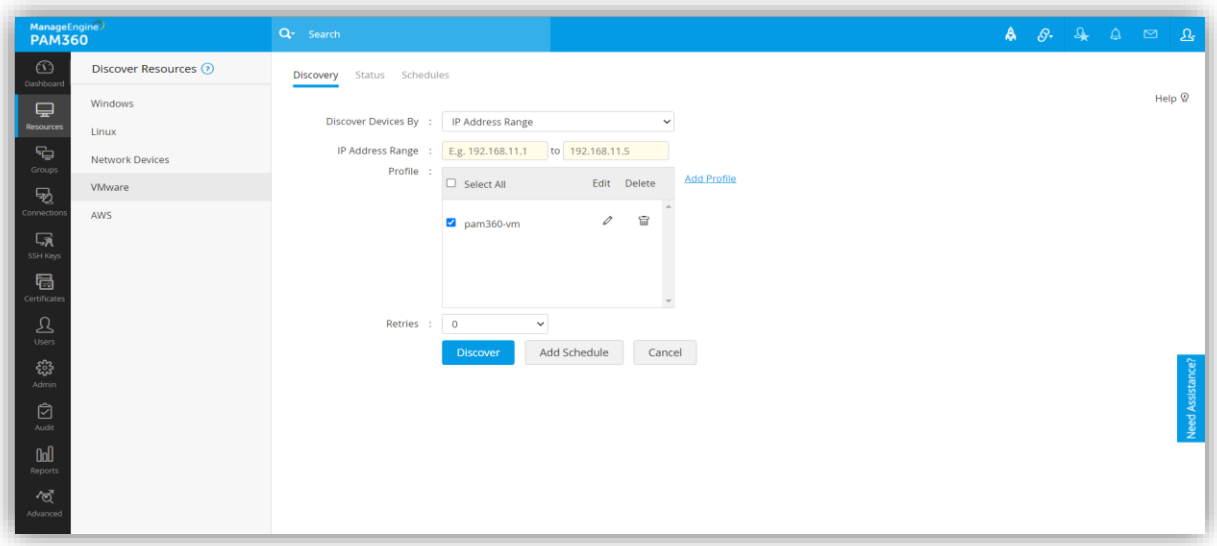
For VMware, VSphere API is used to get the list of all ESXi hosts for device discovery.

Prerequisite - Create Discovery Profiles

Before proceeding with discovering VMware devices, you should create discovery profiles that help PAM360 use common details for discovering multiple devices. You can create the discovery profiles using your vCenter API username and password.

Steps to Discover VMware Devices:

1. Navigate to **Resources >> Discover Resources >> VMware**.



2. As detailed above in the Network Devices discovery section, you can discover a single VM device by specifying the host name or IP address OR multiple devices present in an IP range OR discover multiple devices whose details are available in a flat file.

3. Choose an existing discovery profile(s) [OR] click **Add profile** to initiate the profile configuration process.
    i. In the new window that opens, enter a unique profile **Name**.
    ii. Enter a **Description** about the profile for your reference.
    iii. Enter the **VMware** Port, the vCenter API **Username** and **Password** to establish communication with the virtual device. You can either enter the password **manually** or use a **user account** stored in PAM360. **(Follow above steps)**
    iv. Click **Save**.
4. To avoid time-delay, you can set the number of **Retries** (maximum 5) up to which PAM360 should keep attempting to discover the devices.
5. Click **Discover**. A **Discovery Confirmation** window pops up. Choose whether to send notifications to **"All administrators"** or to specific people. If you choose the latter option, specify the email addresses separated by commas. Click **Proceed**. Now, you will see the **Discovery Status** page where the discovered device will be added as a task. You will also see other details such as date/time when the discovery was invoked, completed, etc.
6. If you want to schedule a periodic resource discovery, click **Add Schedule.** You will see a new window where you can create an automated scheduled task for discovering the newly added accounts during resource discovery. Refer to the Scheduled Resource Discovery section to know more in detail.

1.2.5 AWS EC2:

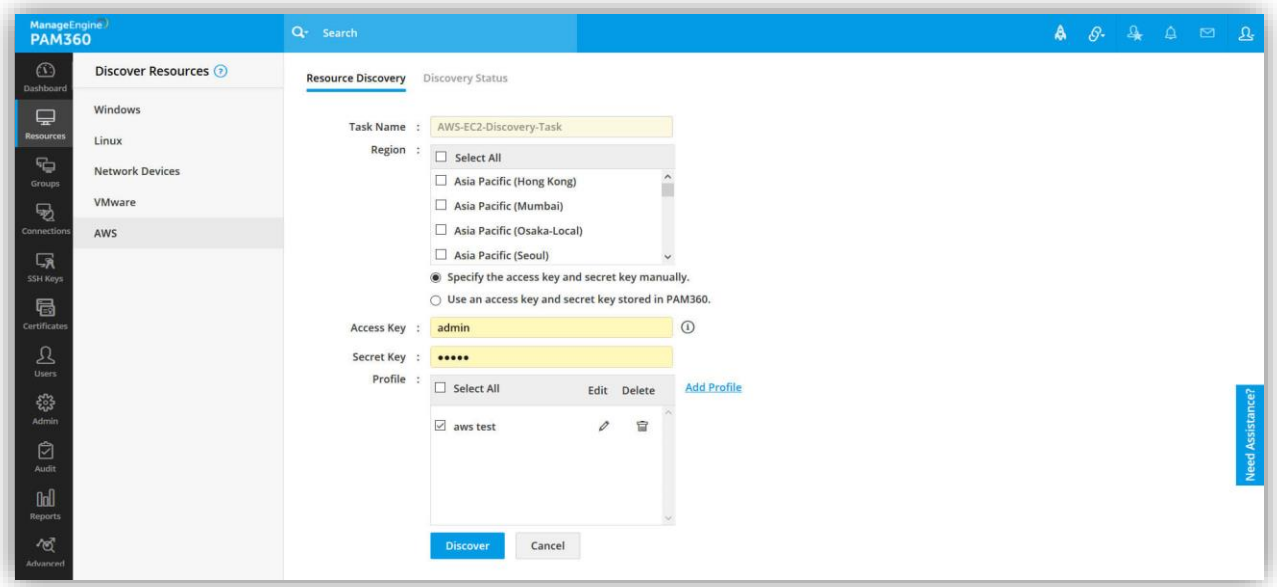
Amazon Web Services(AWS) is an on-demanding, cloud computing platform and Elastic Compute Cloud (EC2) is one of the popular Amazon services. The EC2 platform allows users to rent several virtual instances to run their applications. All these instances can be directly retrieved, imported and managed from PAM360.

Prerequisite

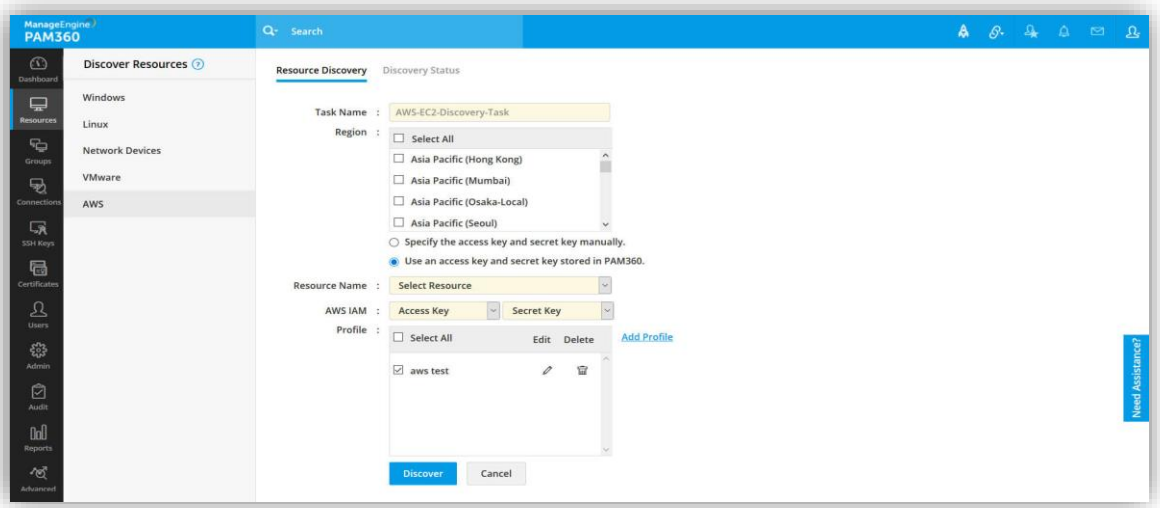
You should have the **Administrator access** and **Amazon EC2 Read-Only Access** to add resources in AWS.

Steps to discover AWS resources:

1. Navigate to **Resources >> Discover Resources >> AWS.**



2. In the **Resource Discovery** page displayed, do the following:
    i. Mention the **Task Name.** Select the **Region** from which the instances should be discovered.
    ii. Either **Specify Access Key Id and Secret Access Key Manually** or **Use an Access Key Id and Secret Access Key stored in PAM360.**
    iii. If you choose to **Specify Access Key Id and Secret Access Key Manually**, enter the **Access Key** and **Secret Key.**
    iv. If you choose to **Use an Access Key Id and Secret Access Key stored in PAM360**, select the **Resource Name** and select the respective **access key** and **secret key** from the **AWS IAM** dropdown.

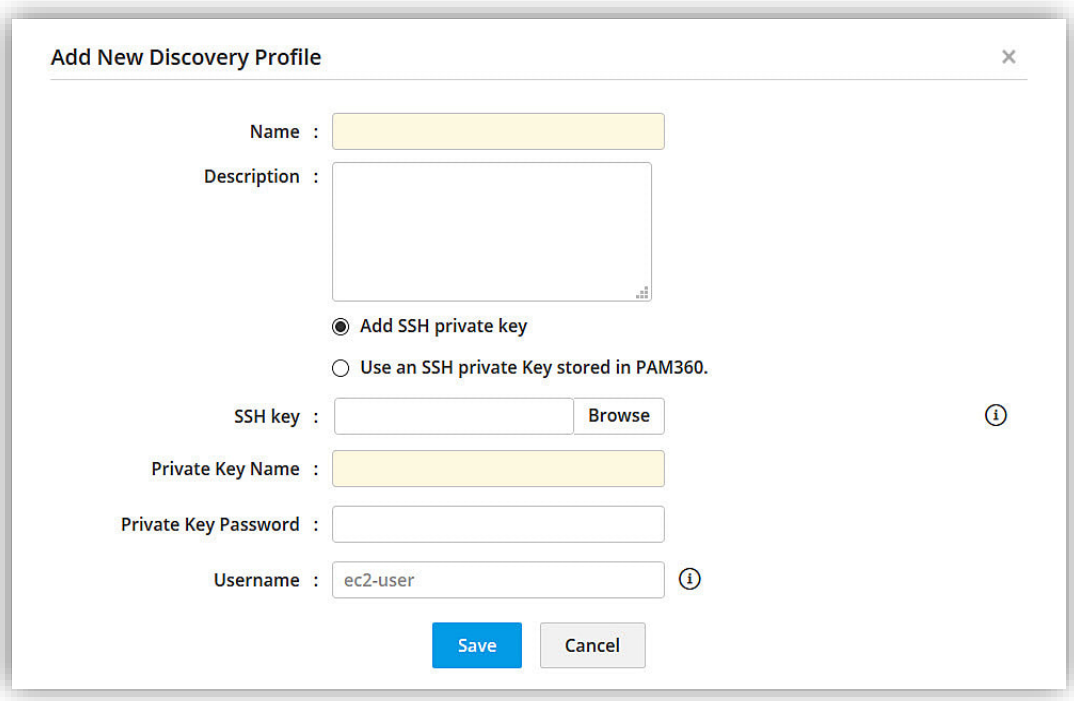


    v. Select **Discovery Profile(s)** or click the **Add Profile** link and specify the following details in the pop-up that appears:

a. Mention the **Name** and **Description**.

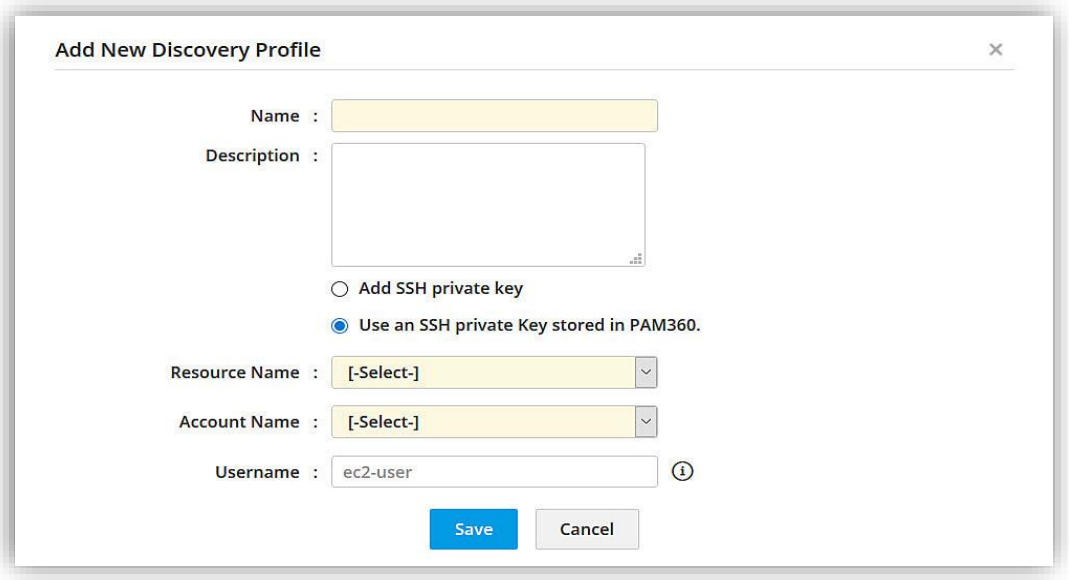
b. Depending on whether you want to **Add a SSH Private Key** or **Use an SSH Private Key stored in PAM360**, select the required one accordingly.

c. If you choose to **Add a SSH private key**, upload the **SSH Key** by clicking **Browse**. Then, mention the **Private Key Name** and **Private Key Password**.



Note: Private key's name should be the same as used in that particular instance.

d. If you choose to **Use a SSH private key stored in PAM360**, select the **Resource Name** and **Account Name**.



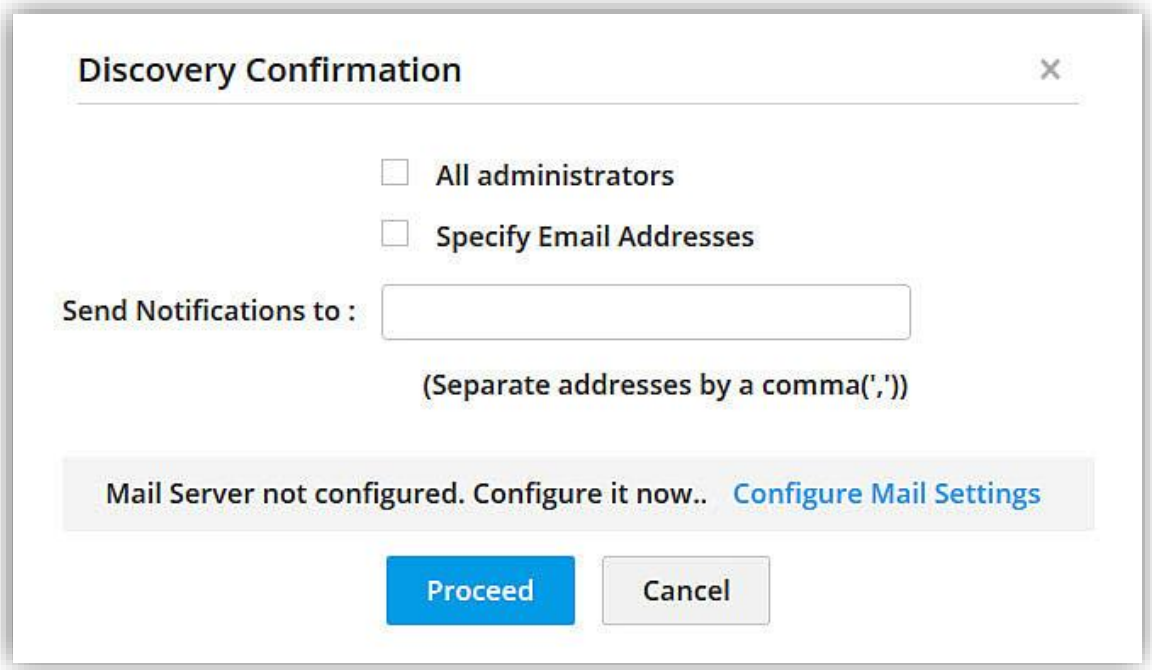
e. Enter the **Username** so that PAM360 checks for a Windows instance and if fails, it checks the credentials for Linux and tries to login. If the **Username** is not mentioned, PAM360 assumes the resource to be a Windows instance and uses the default **administrator** as the username and tries to login.

f. In the event of successful verification, the instances are added in the **Profile** category.

g. Click **Save**. Now, the added profile will be displayed in the **Profile** section. Clicking the ?? and icon against the desired profile lets you modify and delete that profile, respectively.

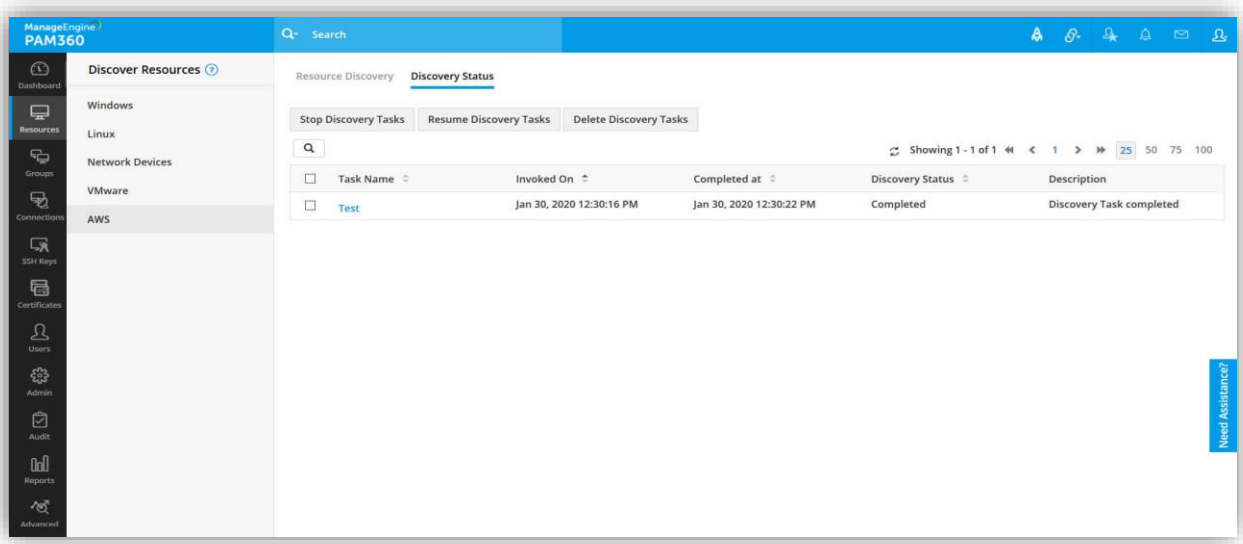
> **Note:** To discover an account from a Windows instance, the Remote Password Reset must be configured manually for that account.

vi. Now, Tap **Discover.** In the pop-up that appears, select to send notifications to **All administrators** or/and **Specific Email Addresses** (me ntion the email id's to whom you want to **Send Notifications** to).



vii. Click **Proceed.** The notification will be sent to the specified email id's.

3. Click the **Discovery Status** tab. You will be able to find the list of discovery operations running in the background.



i. All the tasks discovered will be available in a list view for which you can find its **Task Name, Invoked On, Completed At, Discovery Status** and its **Description.**

ii. Click the task name to view the list of resources that were discovered during that particular task in a pop-up.
   a. Click **Add all discovered resources** to add all the resources that were discovered during this task.
   b. From the list of discovered resources, select only the resource(s) that you wish to add and click **Add selected resources.**

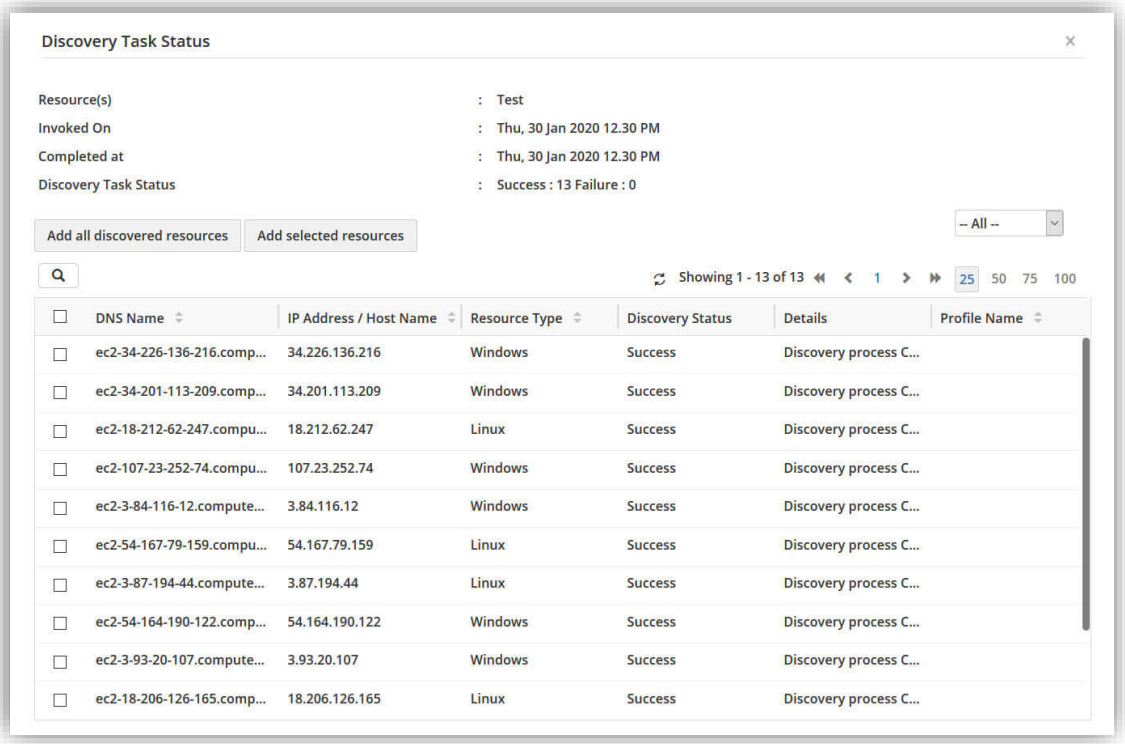
c. Click the **Search** icon to look for a particular resource.
d. You can sort these resources using the drop-down available on the top-right corner of the list view.

iii. To stop or resume a task(s), select the task(s) from the list view and click **Stop Discovery Tasks** or **Resume Discovery Task.**

iv. Select the task(s) you want to delete and hit **Delete Discovery Tasks** button to delete those task(s).

> **Note:** In Windows, if an admin password is rotated, the resource should not be deleted because its password cannot be retrieved by the AWS and the account should be managed by PAM360.

v. Hit the **Search** button to search for a required task.



1.2.6 Amazon WorkSpaces:

In addition to the above-mentioned endpoints, PAM360 also allows you to discover and add virtual desktops from an Amazon WorkSpaces client as resources in the PAM360 repository. You can retrieve, import, and manage all the virtual instances, directly from PAM360. To use PAM360 to discover virtual machines from an Amazon WorkSpaces client, you must first create a directory in the AWS console and establish a virtual desktop. Follow the below steps:

1. Follow the steps detailed in this AWS document to create your Amazon WorkSpaces client.

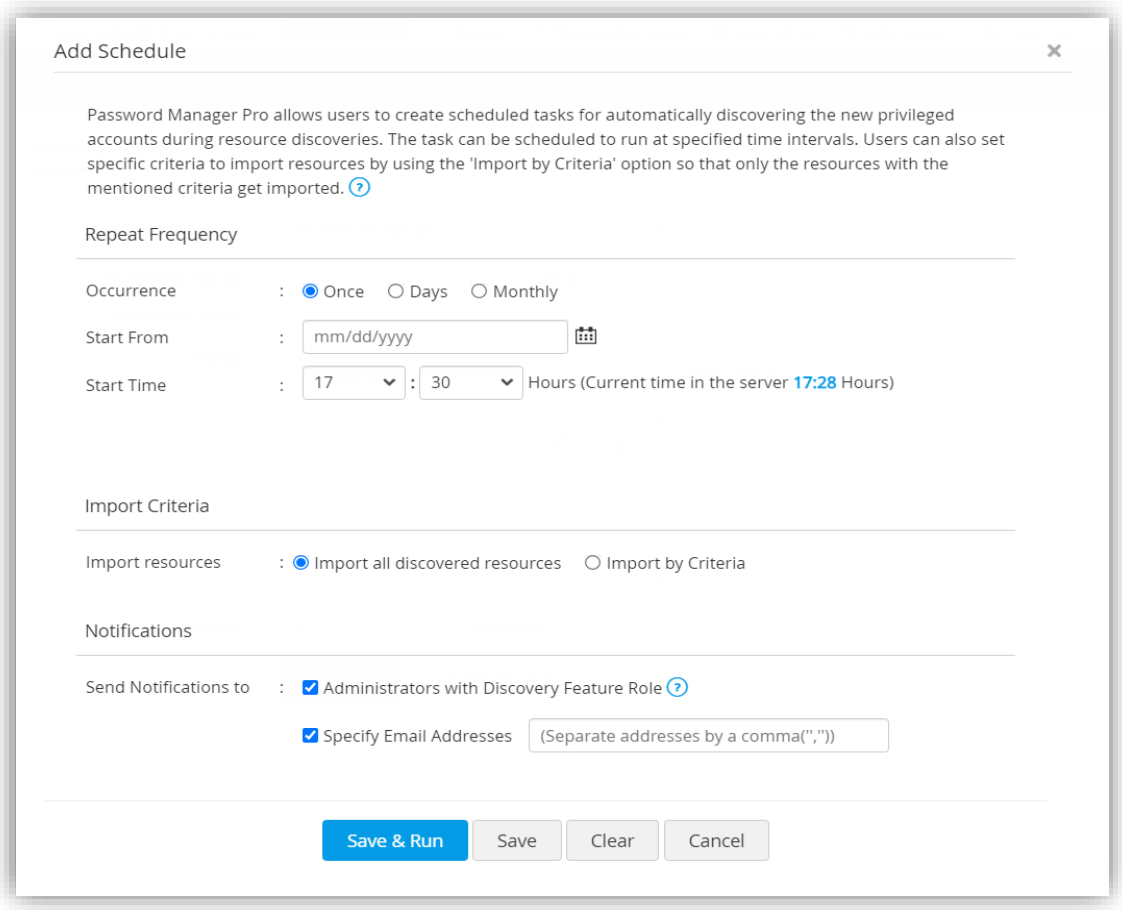
2. Next, launch a virtual desktop using the Amazon WorkSpaces client you created.
3. Once you have set up your virtual desktop, install PAM360 in it.
4. After installing PAM360 in the desktop, proceed with the discovery process by following the steps for **Windows** or **Linux**, based on the operating system the virtual desktop runs on.

1.3 Scheduled Resource Discovery

Add schedules to perform automated periodic resource discovery of Linux, VMware, and Network devices at specified intervals. Set the repeat frequency, set import criteria - filter resources during import based on Resource Name or DNS name using specific criteria. You can also choose to send notifications. Check out the detailed steps below:

> **Note:** Scheduled Resource Discovery is available only for Discover devices using IP Range.

1. After mentioning the required details, click **Add Schedules.**
2. In the pop-up that appears:
    i. Select the occurrence between **Once, Days or Monthly.**
    ii. If you choose the occurrence as **Once,** mention the **Start From** and the **Start Time.** This will allow users to schedule the discovery once on the mentioned **Start Date.**



iii. If you choose the occurrence as **Days,** mention the **Start From, Interval Day(s)** and the **Start Time.**

iv. If you choose the occurrence as **Monthly,** mention the **On** and the **Start Time.**

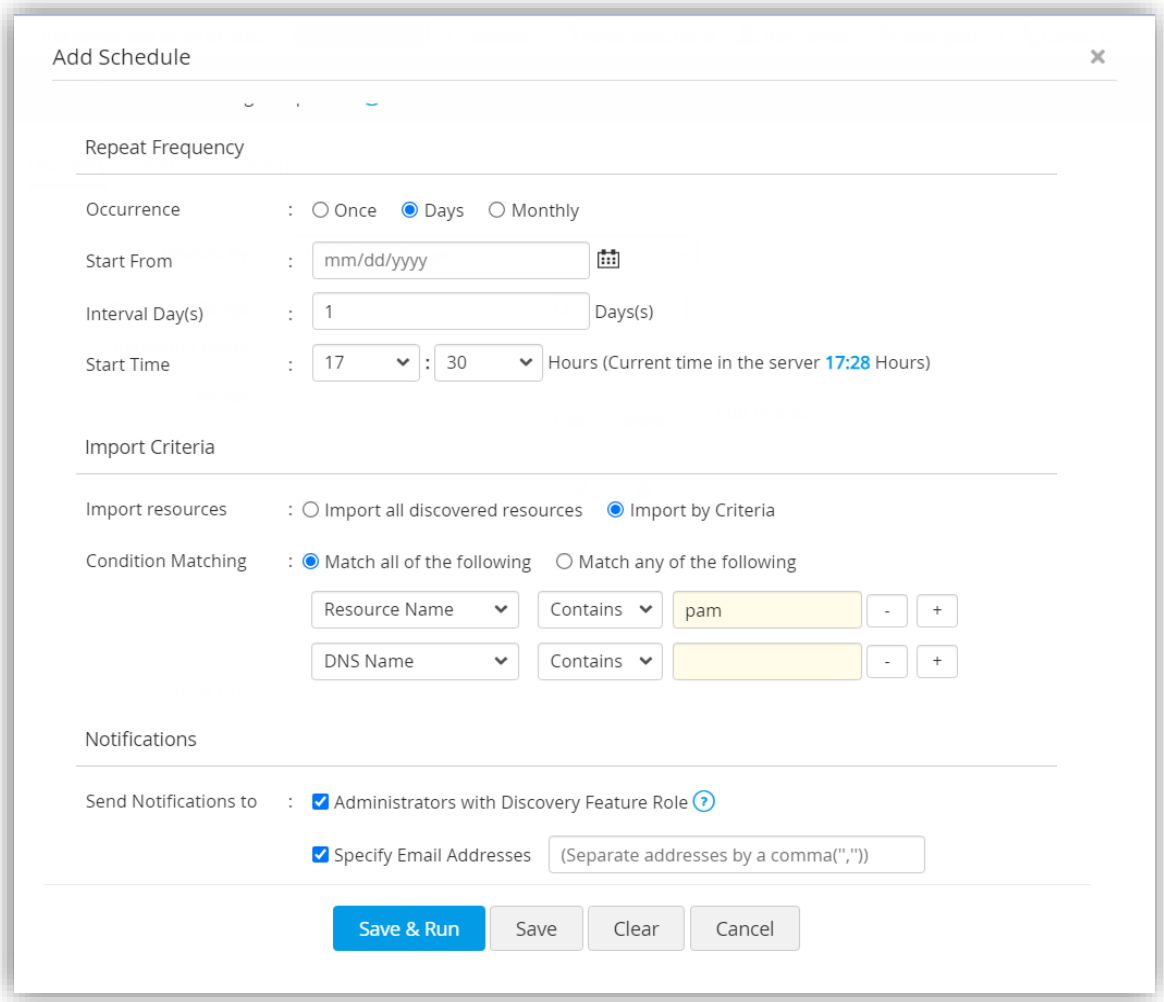
3. Select if you want to **Import all Discovered Resources** or if you want to **Import by Criteria.**

   i. If you choose to **Import by Criteria,** mention the conditions by which you want to import the discovered resources.

   ii. You can choose to **Match all of the following** or **Match any of the following** mentioned criteria.

   iii. Select **Resource Name** or **DNS name.** You can filter the search based on conditions such as **'equals'** or **'does not equal', 'contains'** or **'does not contain', 'starts with'** or **'ends with'.**

4. Select **Administrators with Discovery Feature Role** or **Specify Email Address** and mention the email address separated by comma to notify about the schedule.



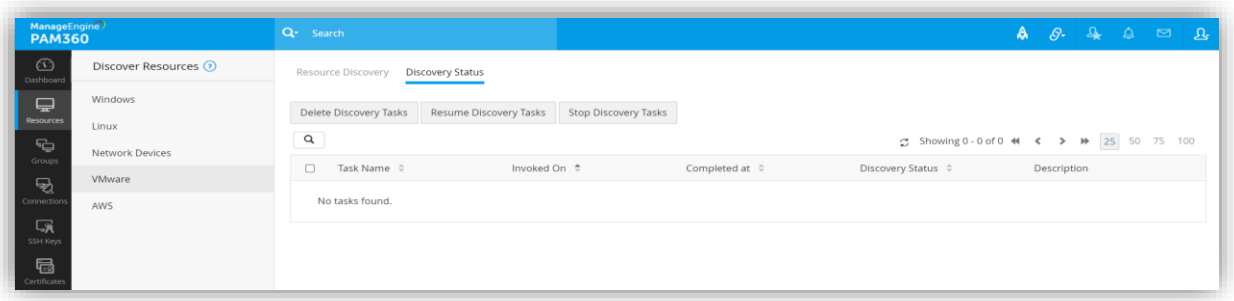
5. Click **Save** to save the schedule.
6. Click **Save and Run** to save and run the schedule (applicable only for Days and Monthly occurrence).

Now, you have successfully added a schedule for Resource Discovery. The added schedule can be viewed from the **Discovery Schedules tab** or from **Admin >> Manage >> Scheduled Task.** From here, you will also be able to **Edit, Disable** and **Delete** the schedule.

1.4 Track Discovery Status

1. After initiating the discovery operation, PAM360 allows you to track the status of the operation in real-time.
2. The list of discovery operations, which are currently running in the background can be found in the **Discovery Status** tab. Using the same tab, you can also track down the history of discovery scans which were performed earlier.
3. For any Discovery operation, you can find its **Task name, Time invoked, Completed At** and **Discovery Status**.
4. PAM360 also provides an option to stop any discovery operation which is currently in progress.

5. Click any Task Name to view the entire list of IT assets discovered during that particular task.



2. Adding the Discovered Resources into PAM360

The following topics explain how each type of discovered resources are added into PAM360:

2.1 Windows

When a Group/OU is imported from AD, the Windows devices that are part of the Group/OU will be automatically listed under the **Resources** tab, from where they can be viewed.

2.2 Linux

For Linux devices, you need to move the discovered resources to the Resource tab manually. In the Discovery Status window under **Discover Resources** option, select the required resources that are discovered and move them to the Resources tab. This operation can also be performed in bulk by selecting multiple resources discovered.

2.3 Network Devices

For network devices, you need to move the discovered resources to the Resource tab manually. In the Discovery Status window under **Discover Resources**, select the required resources that are discovered and move them to the **Resources** tab. This operation can also be performed in bulk by selecting multiple resources discovered.

1. In the **Discovery Status** window, PAM360 provides you an option either to add all discovered resources or add selected resources into the inventory.
2. In the Discovery Status window, upon clicking a task name, the Discovery Task Status will pop up.
3. Click on **Add all discovered resources**, to add the entire set of resources into PAM360 inventory and click **OK** button.
4. If you want to add only particular resources into the PAM360 inventory, select those resources and click on **Add selected resources**.

2.4 VMware

For VMware, you need to move the discovered resources to the **Resources** tab manually. In the Discovery Status window under **Discover Resources** option, select the required resources that are discovered and move them to the Resources tab. This operation can also be performed in bulk by selecting multiple resources discovered.

2.5 AWS

For AWS, you will have to add the resources manually. From the **Discovery Task Status** window, you will be able to import all the resources by clicking on the **Add all discovered resources** button or you can select the required resources and click the **Add selected resources** button.

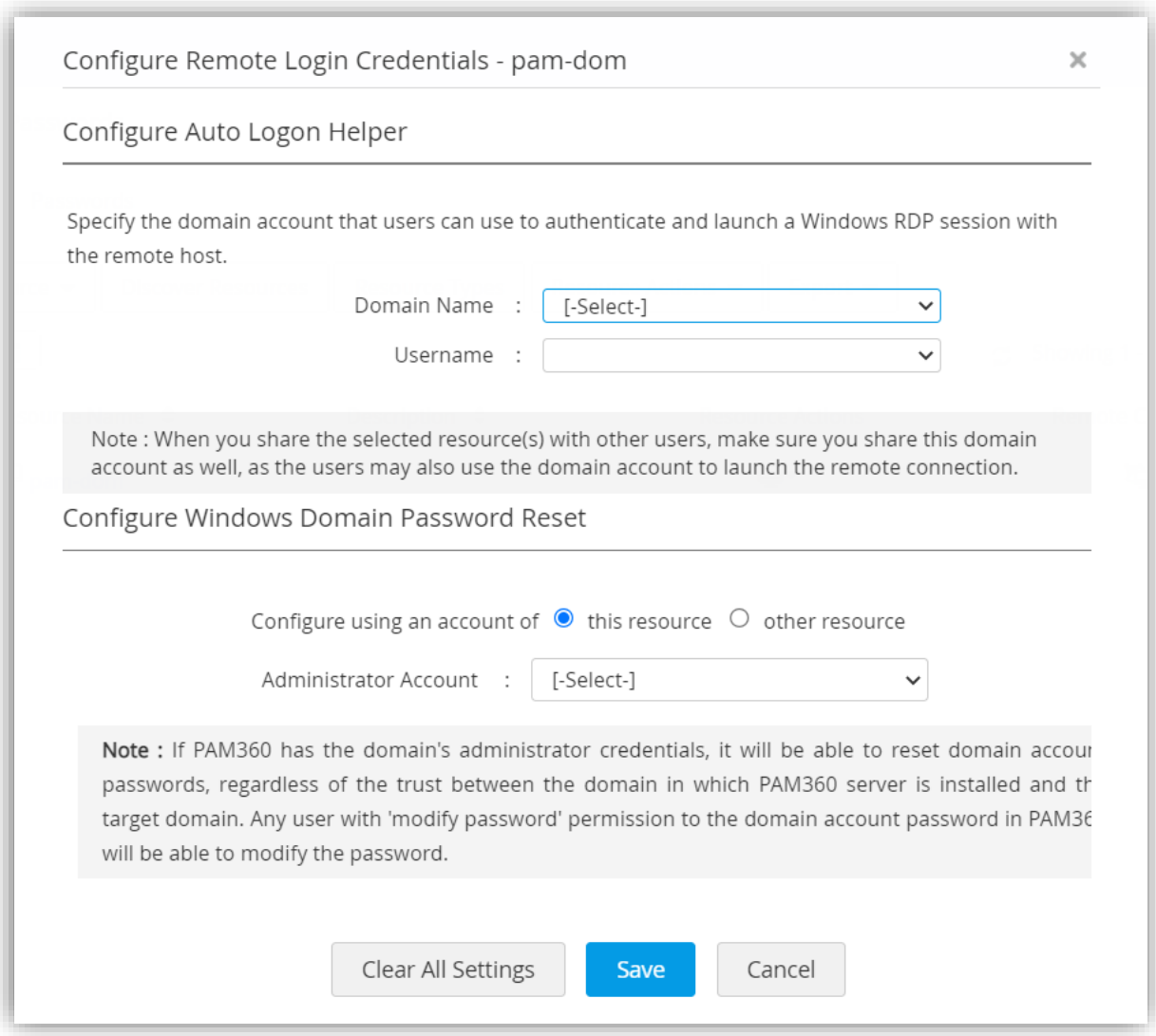
3. Discovering Privileged Accounts

After successfully discovering the IT assets, the next step is to discover the privileged accounts associated with those IT assets. You can discover the privileged accounts associated with each resource individually as well as in bulk.

3.1 Prerequisite (Accounts Discovery)

To discover and enumerate the privileged accounts (including local administrator accounts) from the resources, you need to supply the credentials to enable PAM360 to fetch the accounts. You can do this by clicking the **Edit** button against each resource. This step has to be repeated for all resources whose accounts are to be discovered.

1. Navigate to the **Resources** tab.
2. Click the **Resource Actions** icon against WindowsDomain resource and select **Configure password reset** from the dropdown.
3. In the pop-up form that appears, select the Domain Admin account as the **Administrator Account**.



4. PAM360 supports only specific resource types for privileged accounts discovery. If any of your device is not supported, but is similar to the other supported types, you may select the closest resource type available and try discovering the accounts.
5. When discovering resources, PAM360 fills the resource type field as well. However, check the resource type field and ensure that the correct type is chosen. Otherwise, change the type.
6. Click **Save**.

3.1.1 Discovery of Windows Service Accounts and Local Accounts Associated with the Domain Member Server

When discovering Windows accounts, PAM360 will also automatically fetch the service accounts associated with services present in the domain members. The Windows service accounts discovery and enumeration of the same in the inventory takes place as explained

below:

1. Initially, PAM360 will create a Windows domain resource with the domain name. For example, if the domain name is **PAM360**, then the resource name created will also be **PAM360 - Domain Controller.**
2. Then, PAM360 will try to fetch all the available Windows member servers that are available under the specified OU or groups.
3. After importing the available resources, the corresponding local accounts associated with those resources will also be fetched.

Finally, the service accounts will be fetched for the imported resources. These service accounts will be mapped to the resource group that contains the resources where service accounts are used. The resource group will be created in the form **DomainName_MemberServerGroup.** For example, if the domain name is given as PAM360, the resource group name will be **PAM360_MemberServerGroup**. If the resource group with that name already exists, resource will be added to that resource group.

3.2 Database Accounts Discovery

Similar to the resources listed above, you can also discover database accounts through the discovery feature in PAM360.

As mentioned above, to discover and enumerate the privileged accounts (including local administrator accounts) from database resources, you need to supply the credentials to enable PAM360 to fetch the accounts. You can do this by clicking the Edit button against each resource. This step has to be repeated for all resources whose accounts are to be discovered.

Database Resource Types Supported by PAM360:

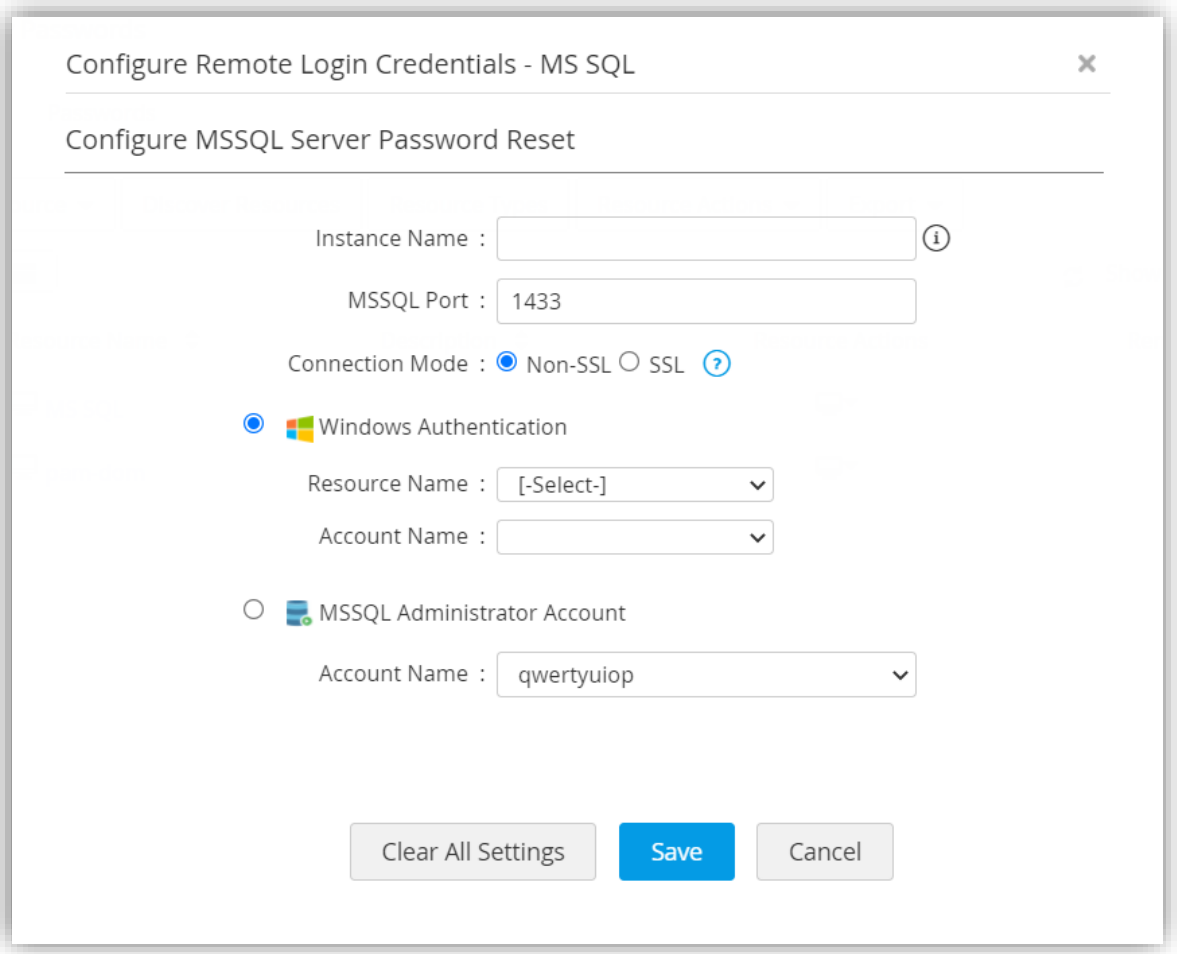
i. MS SQL
ii. MySQL
iii. PostgreSQL
iv. Oracle
v. Sybase

Prerequisites

Supply Credentials for Remote Synchronization

i. MS SQL Server

1. To add an MS SQL resource to PAM360, navigate to **Resources >> Add Resource** and add a resource with the resource type **MS SQL server** and a valid DNS name/IP address.
2. In the **Add Account** window, provide an administrator account's credentials to facilitate the account discovery through this account.
3. To configure remote password reset for this resource, click on the **Resource Actions** drop-down menu beside the resource and select **Configure Remote Password Reset**.
4. For an MSSQL server, the default port in **1433**.Select an administrator account from the **Account Name** drop-down list and **Save** the settings.



5. You can configure the connection either through SSL or Non SSL mode. In case of SSL mode, the SSL certificate must be imported before discovering accounts in PAM360.
6. To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the database server's root certificate into the PAM360 server machine's certificate store.

7. You need to import all the root and intermediate certificates that are present in the respective certificate chain. Before you import the root certificate, stop the PAM360 server.
8. Open the command prompt and navigate to the **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

   For Windows:

   importCert.bat<Absolute Path of certificate>

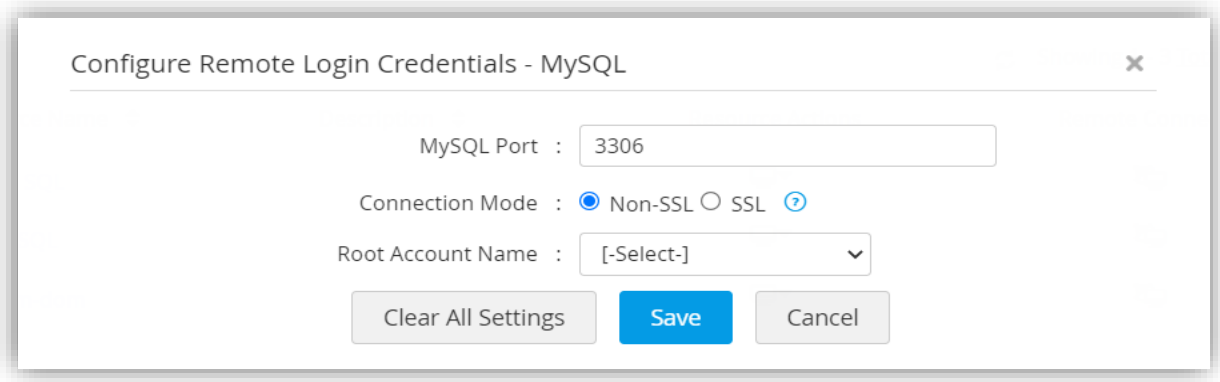
   For Linux:

   importCert.sh<Absolute Path of certificate>

9. Restart PAM360 server.

ii. MySQL server

1. To add a MySQL resource to PAM360, navigate to **Resources >> Add Resource** and add a resource with the resource type MySQL server and a valid DNS name/IP address.
2. In the Add Account window, provide an administrator account's credentials to facilitate the account discovery through this account.
3. To configure remote password reset for this resource, click on the Resource Actions drop-down menu beside the resource and select Configure Remote Password Reset.
4. For a MySQL server, the default port in 3306.Select an administrator account from the **Root Account Name** drop-down list and Save the settings.



5. You can configure the connection either through SSL or Non SSL mode. In case of SSL mode, the SSL certificate must be imported before discovering accounts in PAM360.
6. To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the database server's root certificate into the PAM360 server machine's certificate store.
7. You need to import all the root and intermediate certificates that are present in the respective certificate chain. Before you import the root certificate, stop the PAM360 server. Open a command prompt and navigate to the **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

   For Windows:

   importCert.bat<Absolute Path of certificate>

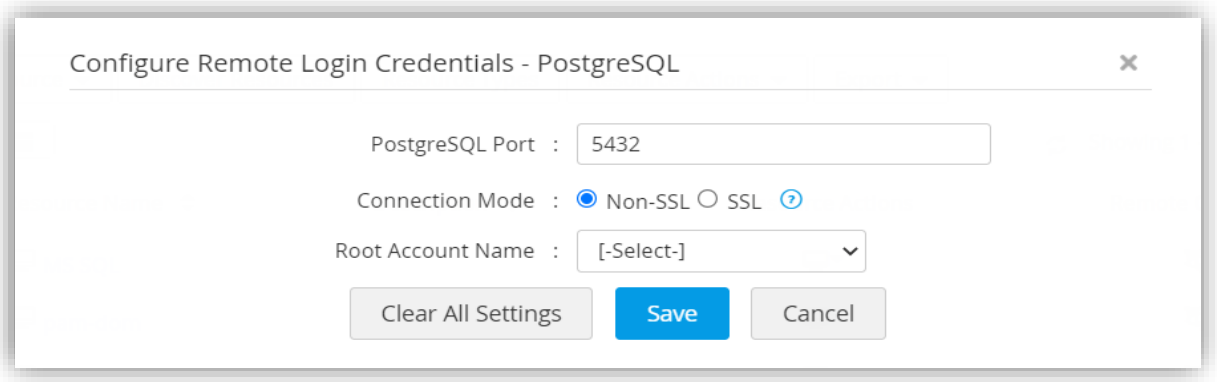
   For Linux:

   importCert.sh<Absolute Path of certificate>

8. Restart PAM360 server.

iii. PostgreSQL Server

1. To add a PostgreSQL resource to PAM360, navigate to **Resources >> Add Resource** and add a resource with the resource type **PostgreSQL server** and a valid DNS name/IP address.
2. In the **Add Account** window, provide an administrator account's credentials to facilitate the account discovery through this account.
3. To configure remote password reset for this resource, click on the **Resource Actions** drop-down menu beside the resource and select **Configure Remote Password Reset**. For a PostgreSQL server, the default port in **5432**.
4. Select an administrator account from the **Root Account Name** drop-down list and **Save** the settings.



5. You can configure the connection either through SSL or Non SSL mode. In case of SSL mode, the SSL certificate must be imported before discovering accounts in PAM360.
6. To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the database server's root certificate into the PAM360 server machine's certificate store.
7. You need to import all the root and intermediate certificates that are present in the respective certificate chain. Before you import the root certificate, stop the PAM360 server. Open a command prompt and navigate to the **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

   For Windows:

   importCert.bat<Absolute Path of certificate>

   For Linux:

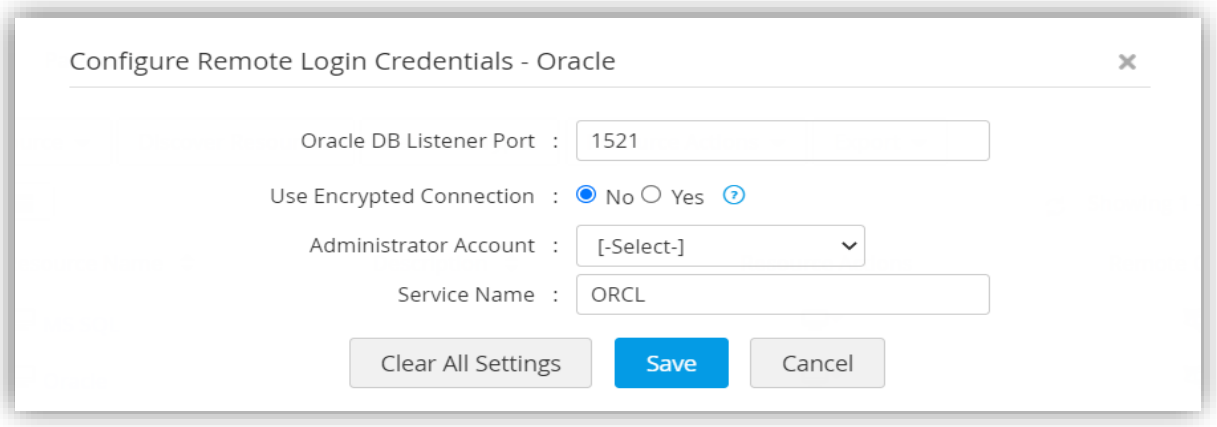
   importCert.sh<Absolute Path of certificate>

8. Restart PAM360 server.

iv. Oracle DB Server

1. To add an Oracle DB resource to PAM360, navigate to **Resources >> Add Resource** and add a resource with the resource type **Oracle DB server** and a valid DNS name/IP address.
2. In the **Add Account** window, provide an administrator account's credentials to facilitate the account discovery through this account.
3. To configure remote password reset for this resource, click on the **Resource Actions** drop-down menu beside the resource and select **Configure Remote Password Reset**.

4. For an Oracle DB server, the default port is **1521**. Select an **Administrator Account** from the drop-down menu and click **Save** to save the settings.



5. You can configure the connection either through SSL or Non SSL. In case of SSL mode, the SSL certificate must be imported before discovering accounts in PAM360.
6. To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the database server's root certificate into the PAM360 server machine's certificate store.
7. You need to import all the root and intermediate certificates that are present in the respective certificate chain.
8. Before you import the root certificate, stop the PAM360 server. Open a command prompt and navigate to the **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

> **For Windows**:
>
> *importCert.bat<Absolute Path of certificate>*
>
> **For Linux**:
>
> *importCert.sh<Absolute Path of certificate>*

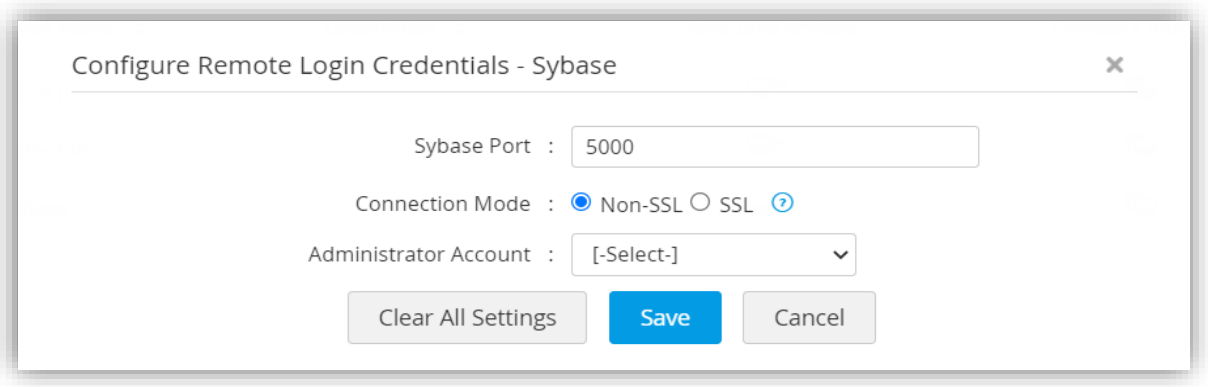
9. Restart PAM360 server.

v. Sybase Server

1. To add a Sybase resource to PAM360, navigate to **Resources >> Add Resource** and add a resource with the resource type **Sybase ASE** and a valid DNS name/IP address.
2. In the **Add Account** window, provide an administrator account's credentials to facilitate the account discovery through this account.
3. To configure remote password reset for this resource, click on the **Resource Actions**

drop-down menu beside the resource and select **Configure Remote Password Reset**.

4. For a Sybase server, the default port in **5000**. Select an **Administrator Account** from the drop-down list and click **Save** to save the settings.



5. You can configure the connection either through SSL or Non SSL. In case of SSL mode, the SSL certificate must be imported before discovering accounts in PAM360.
6. To enable the SSL mode, the MS SQL server should be serving over SSL and you will have to import the database server's root certificate into the PAM360 server machine's certificate store.
7. You need to import all the root and intermediate certificates that are present in the respective certificate chain. Before you import the root certificate, stop the PAM360 server. Open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

   For Windows:

   importCert.bat<Absolute Path of certificate>

   For Linux:

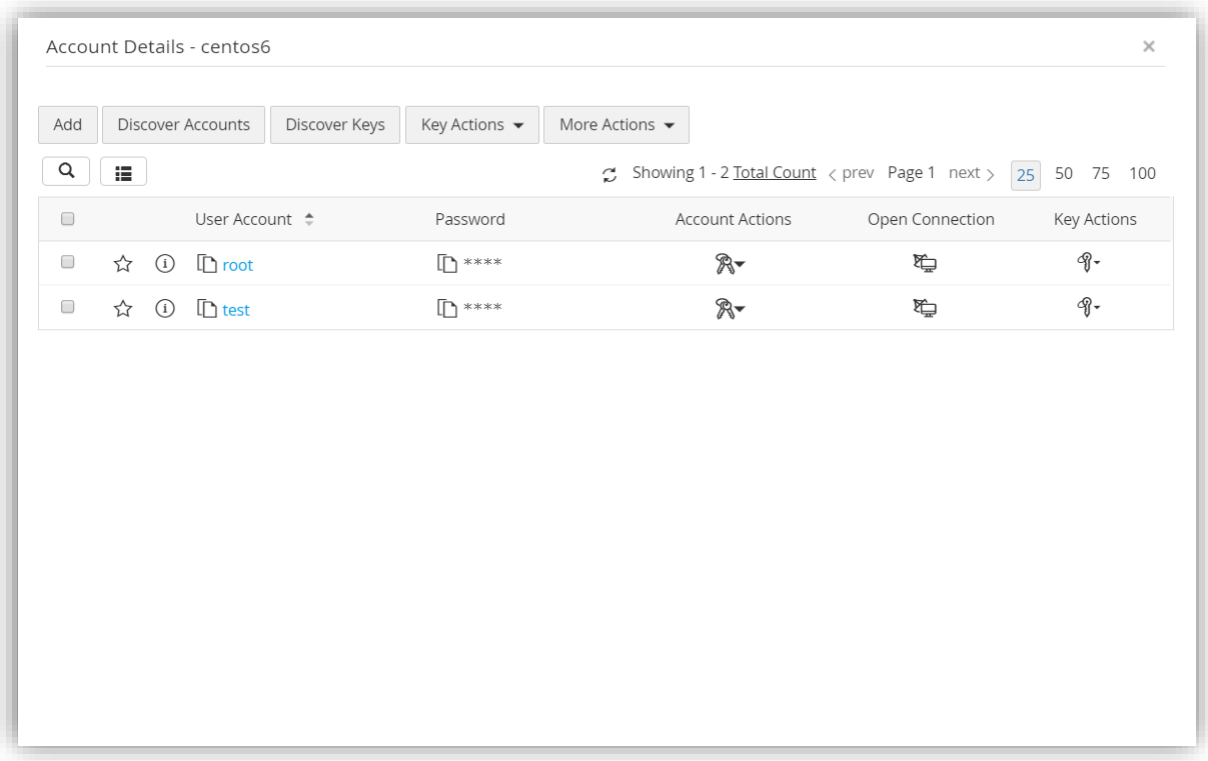
   importCert.sh<Absolute Path of certificate>

8. Restart PAM360 server.

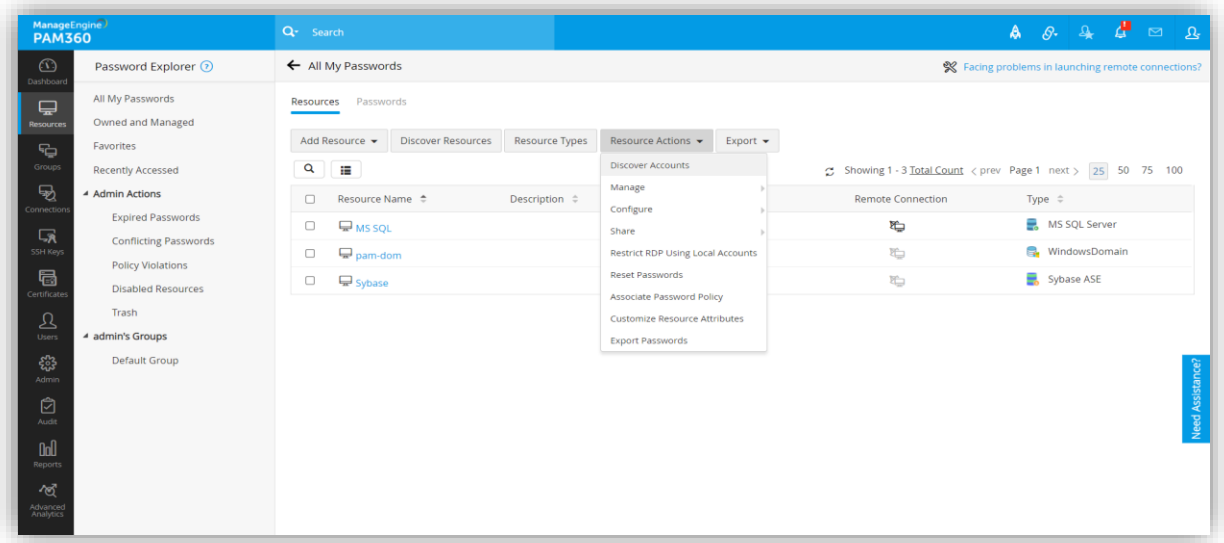
3.3. Discover Privileged Accounts of Individual Resources

Privileged Account Discovery can be initiated from four places in the PAM360 UI:

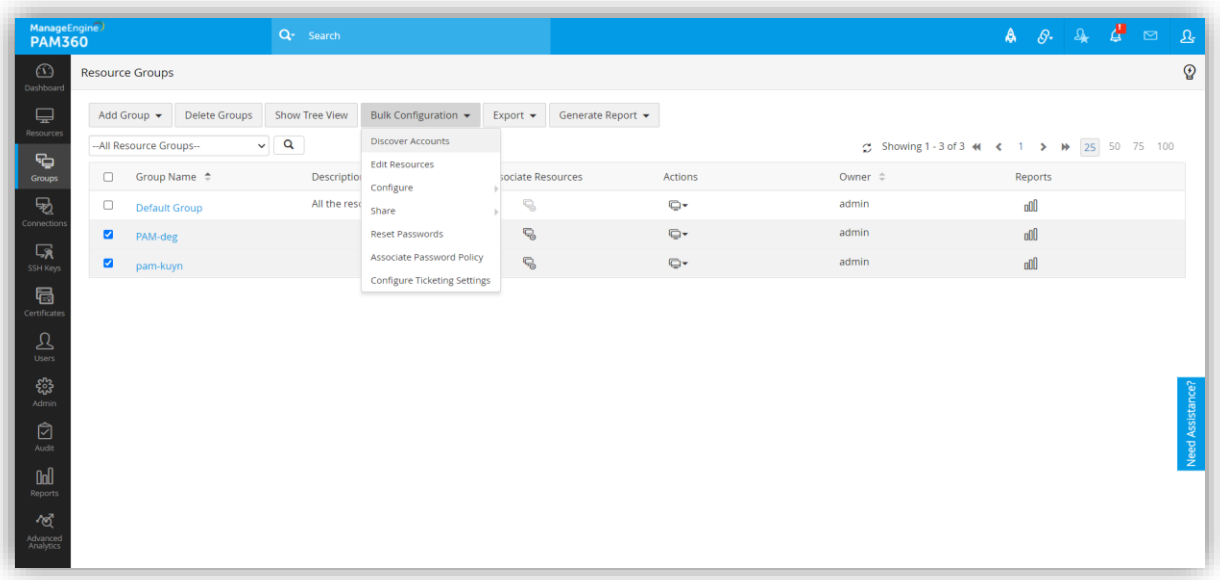
1. In the **Resources** tab, upon clicking a resource, you will see the **Discover Accounts** button. You can use this option whenever you want to discover new accounts added under that particular resource.



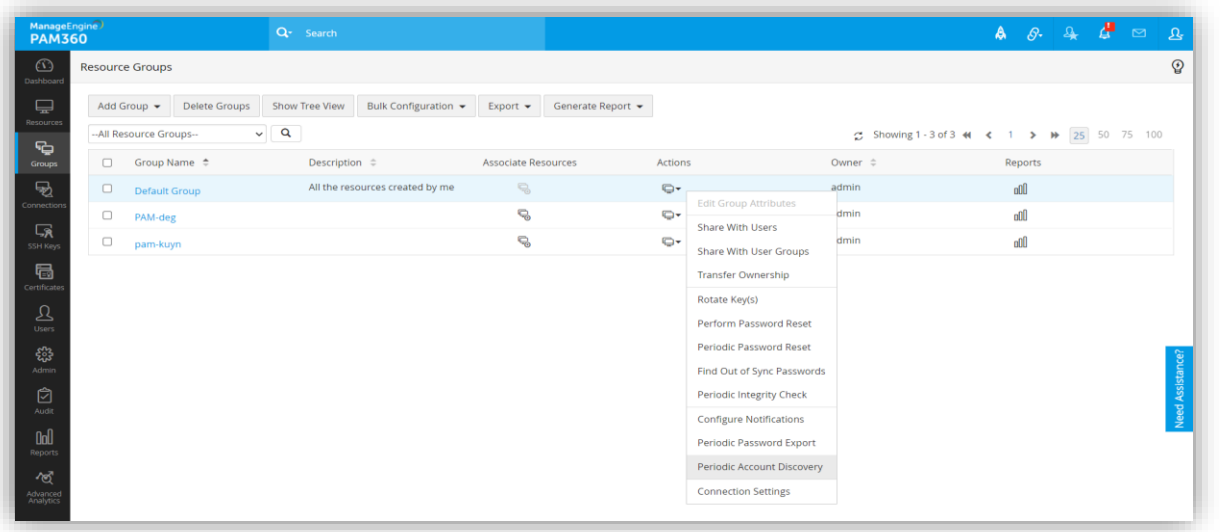
2. You can also use the **Discover Accounts** option to discover accounts that are part of multiple resources. Select multiple resources using the checkboxes and click on this option to discover the accounts that are part of all the selected resources.



3. In the **Groups** tab, select **Discover Accounts** from the **Bulk Configuration** dropdown. You can select multiple resource groups and use this option to discover the accounts that are part of all the selected resource groups.



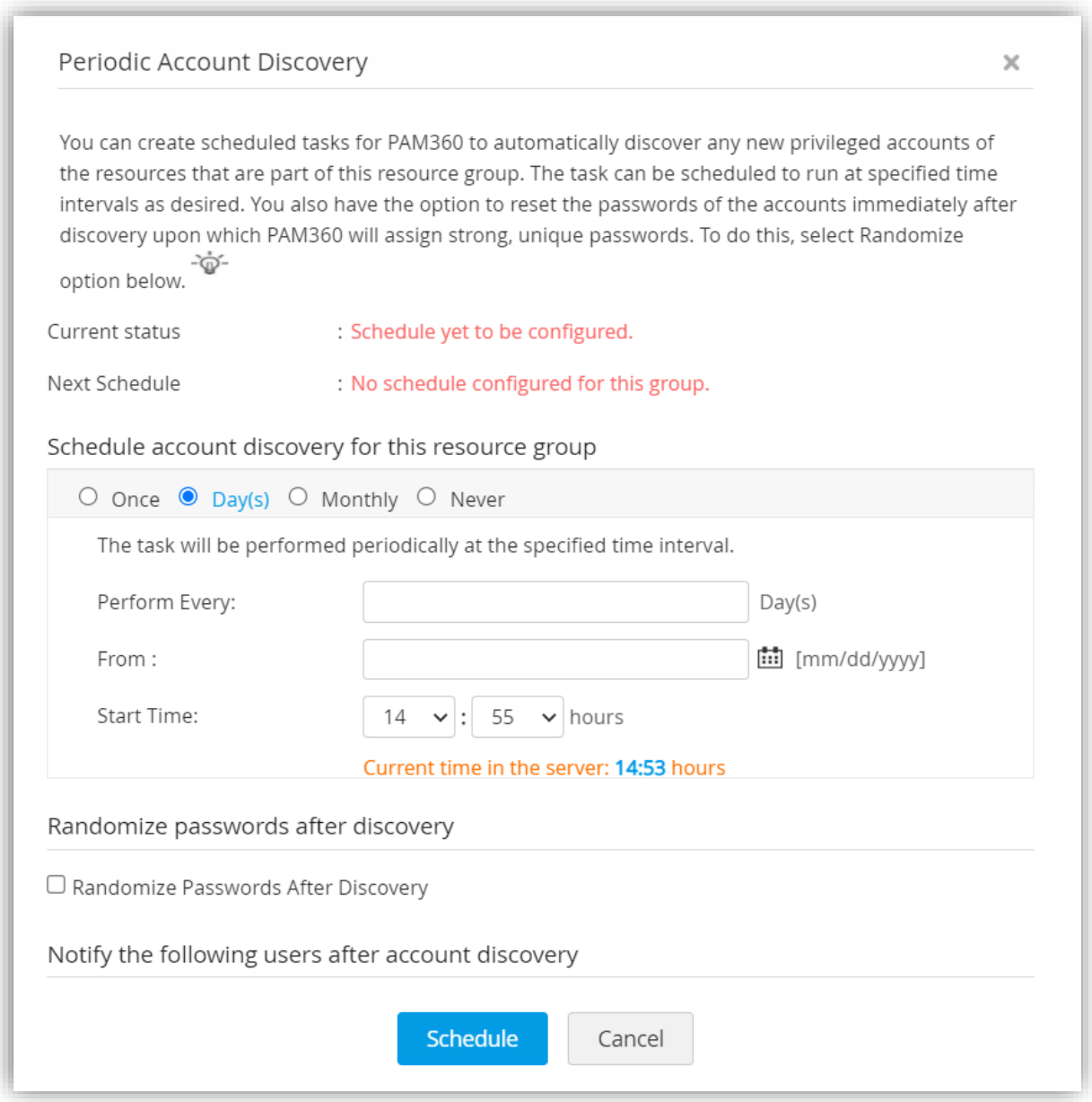
4. In **Resource Groups** tab, select **Periodic Account Discovery** from the **Actions** drop-down list. Using this, you can create a scheduled task to periodically discover the accounts that are part of the resources belonging to the resource group.



3.4 Automated Periodic Discovery of Privileged Accounts

You can automatically discover the privileged accounts of the resources at periodic intervals. This can be configured at the resource group level. The accounts discovered through this method will be added automatically.

1. Navigate to the **Groups** tab.
2. Click the **Actions** icon against the resource group and select **Periodic Account Discovery** from the drop-down list.



Once	Now or Later
Days	Perform on a specific day repeatedly starting from a particular date and time (maximum number of days allowed is 999).
Monthly	On a particular day and time every month.
Never	To stop schedule.

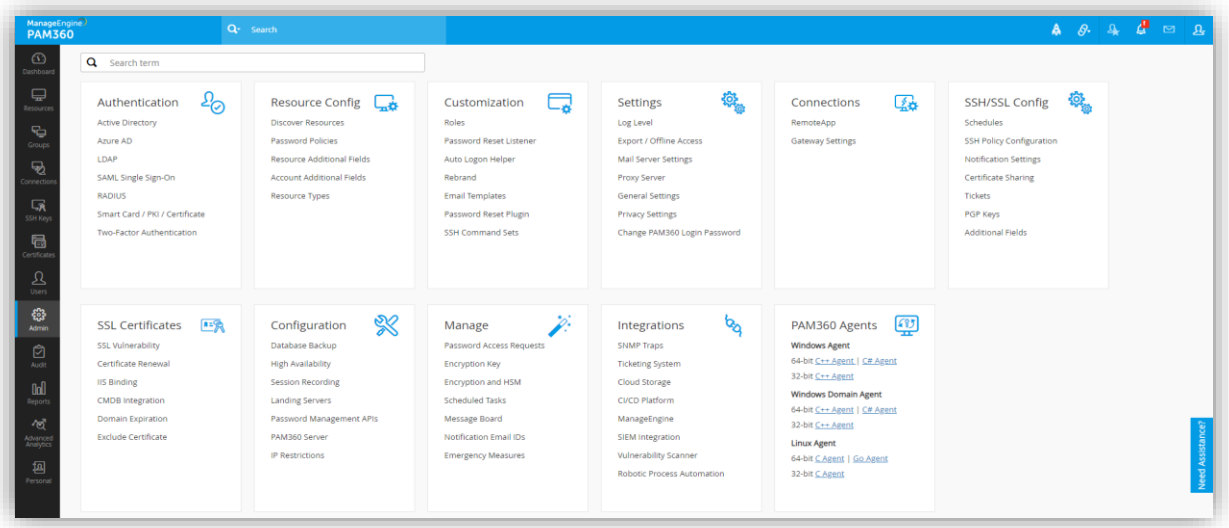
3. PAM360 also provides you with an option to notify the existing PAM360 users or the specified email IDs once the account discovery process is completed.
4. The scheduled account discovery process will be reflected in the audit trails for security purposes.

5. Click on the **Schedule** button.

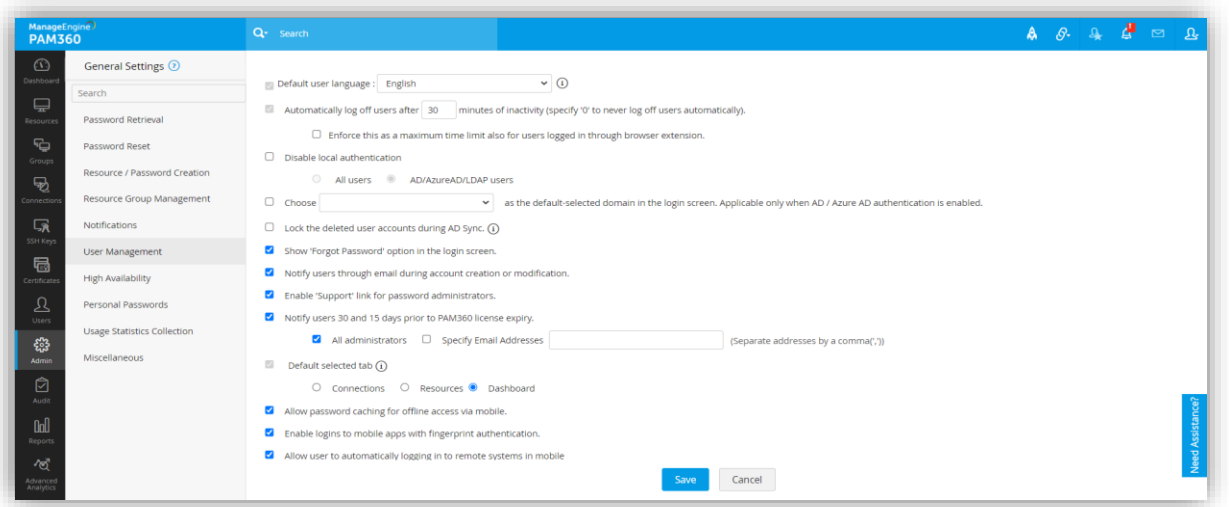
3.5 PAM360 MSP Edition

Discovery option for the client organization can be enabled from the **Admin** tab as follows:

1. Navigate to **Admin >> Settings >> General Settings.**



2. In the UI that opens, select **User Management** from the options on the left-hand side.



3. Select the checkbox **Enable Discovery in client organization**.
4. Click **Save**.

After discovering the accounts, it is recommended to randomize the passwords of the newly discovered accounts.

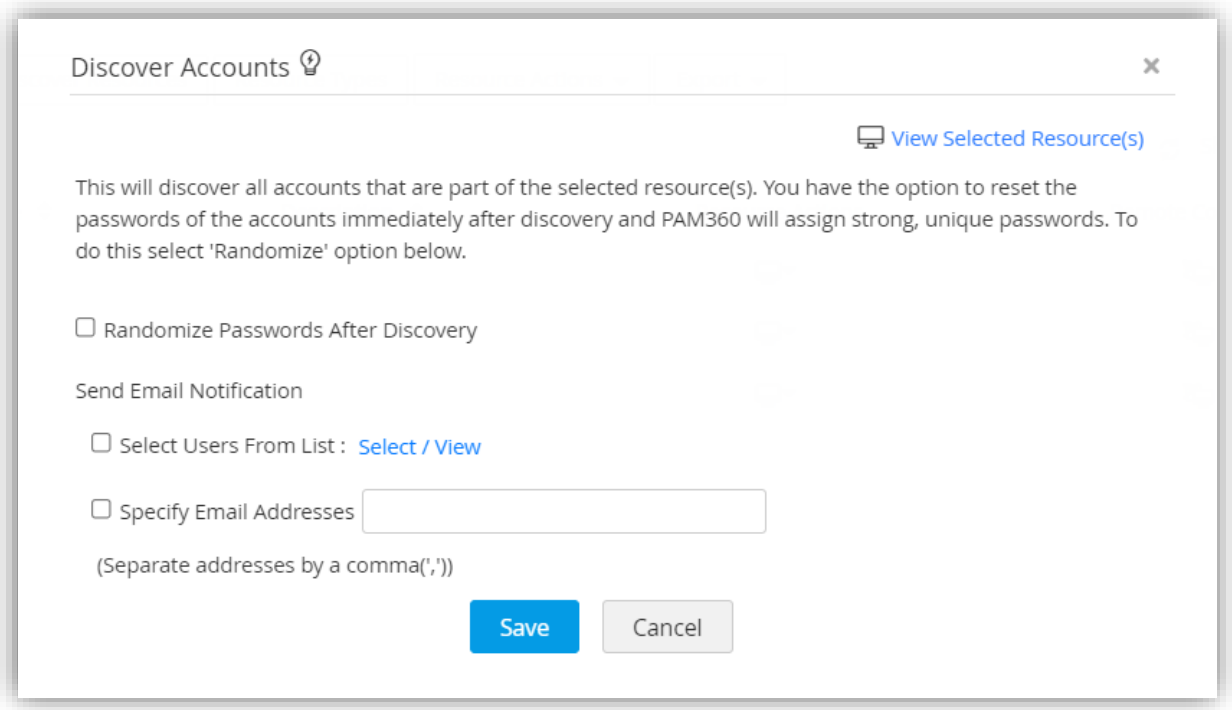
Note: You can also discover the privileged accounts in the agent mode.

3.6 Randomize Passwords Post Discovery

After discovering accounts, it is recommended to reset the passwords of the newly discovered accounts. When accounts are discovered, PAM360 can only fetch the user account name, it cannot fetch the actual password. However, PAM360 is capable of randomizing the passwords upon discovery according to the password policy. The new passwords will then be stored in PAM360.

To randomize passwords after discovery,

1. Navigate to the **Resources** tab.
2. Select the resource(s) whose passwords are to be reset, click the **Resource Actions** button and select **Discover Accounts** from the dropdown.



3. In the dialog box that opens, select the checkbox Randomize passwords after discovery.
4. You can send notification about randomization to password owners. There is also provision to notify other users and specific email IDs.
5. Click **Save**.

Adding Resources Manually

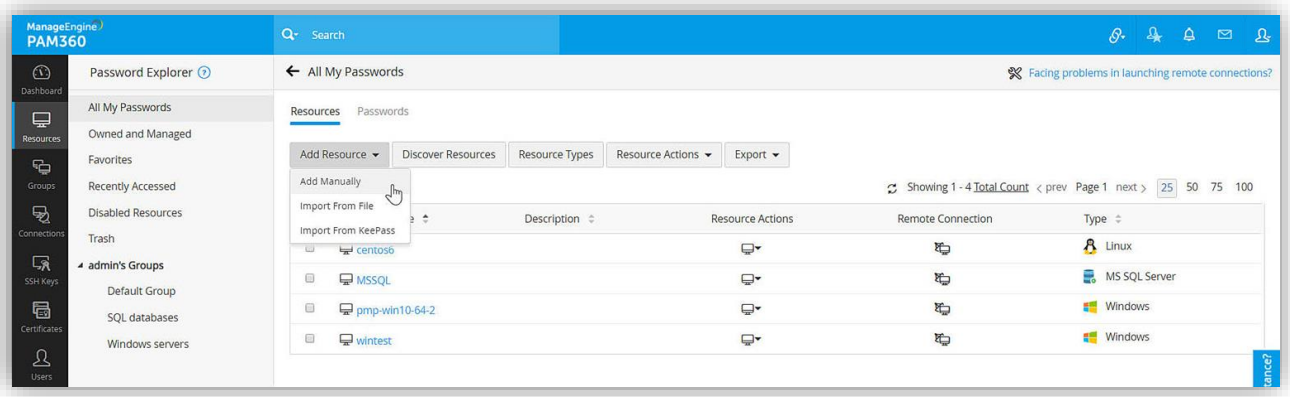
In order to manage the passwords of your privileged accounts, you should add your end-points as resources in PAM360. The term **resource** denotes any server, application, network device or an appliance holding the user accounts and the passwords. There are three different ways of adding resources to PAM360 namely: manual addition of resources, importing resources from a file and discovering resources.

The below sections guide to the step-by-step process of adding the resources in PAM360 from your environment.

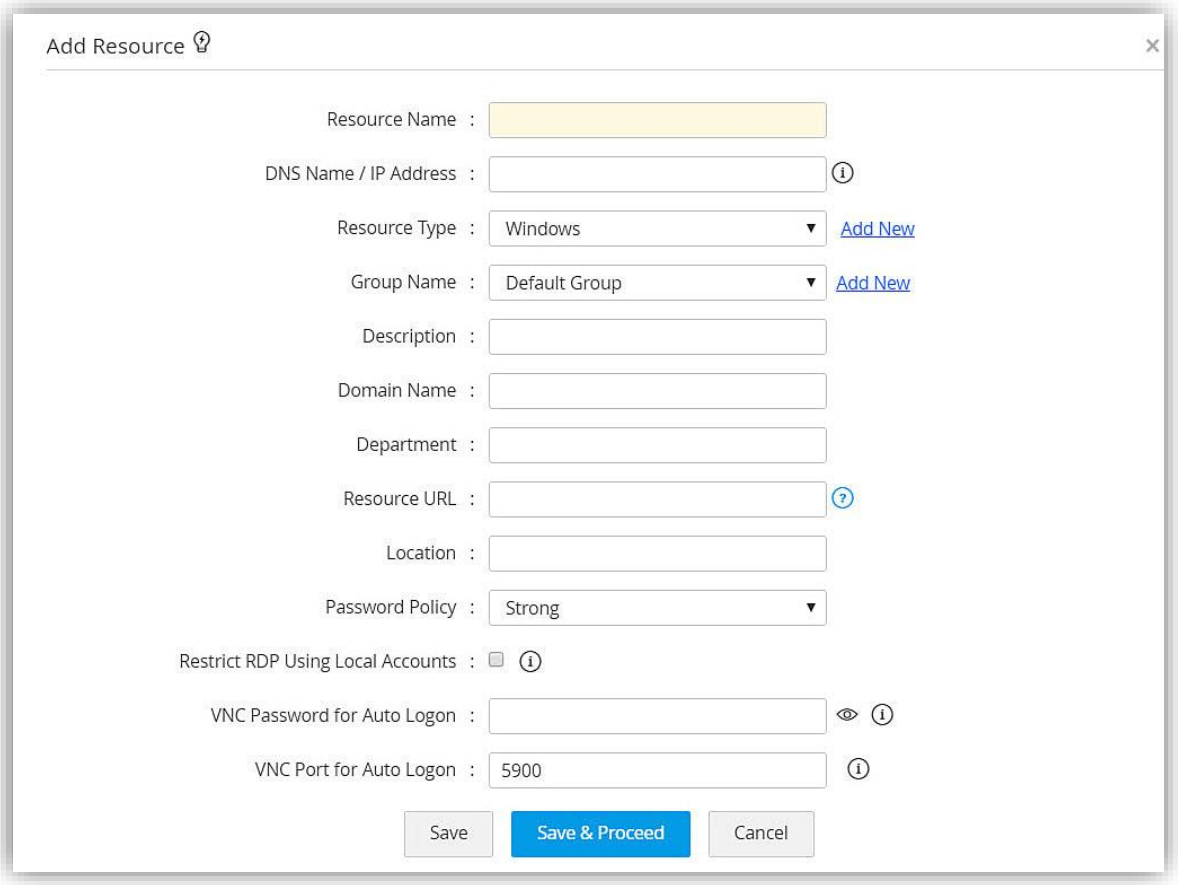
1. Adding a Resource

Follow the below steps to add a resource manually in PAM360:

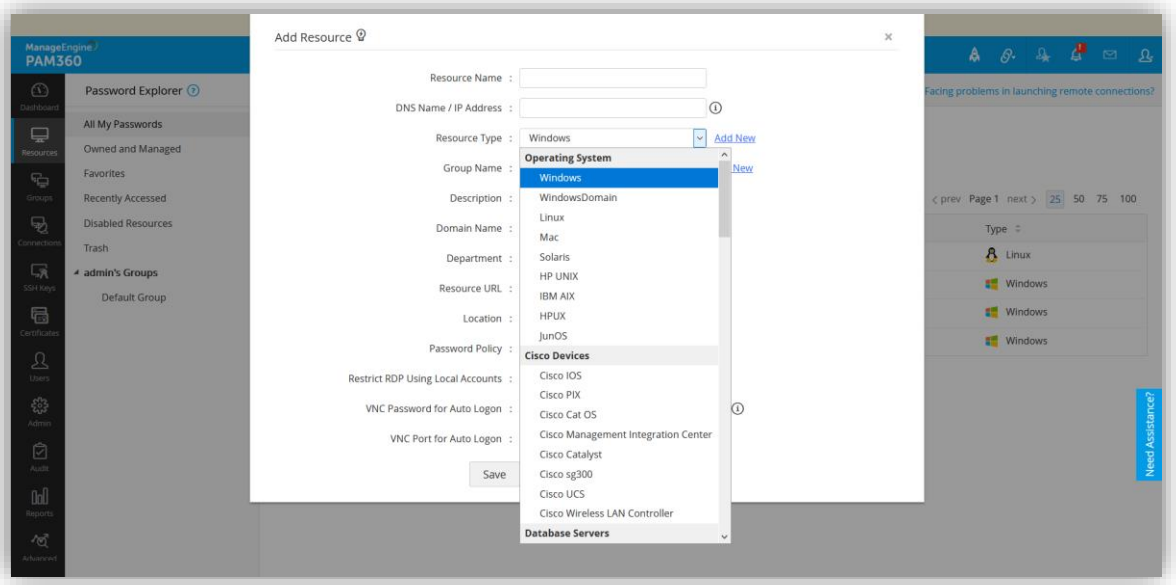
1. Navigate to **Resources** >> **Add Resource >> Add Manually.**

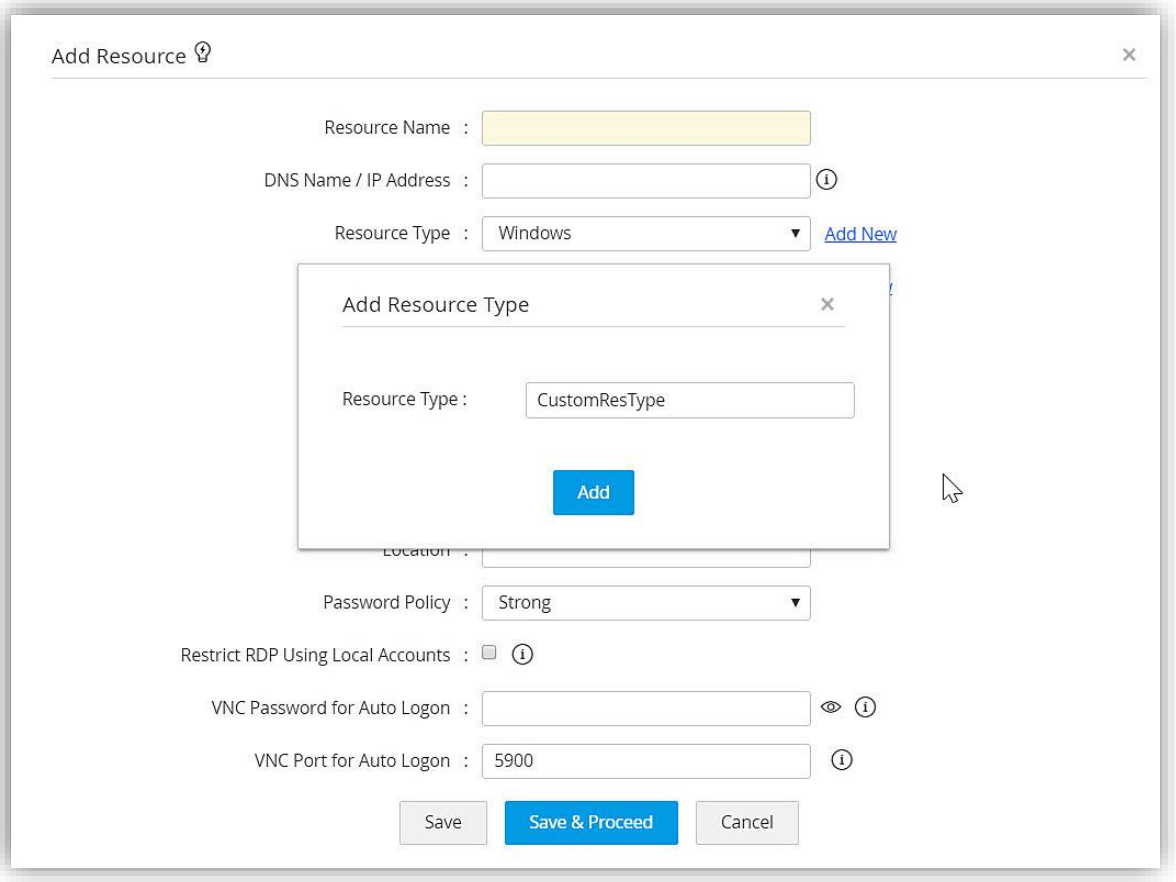


2. In the **Add Resource** window that pops up, fill in the required details:
    i. Specify the **Resource Name** which uniquely identifies the resource in PAM360.
    ii. Enter the **DNS Name or IP Address** of the resource. It is mandatory to provide a valid DNS name or IP address to perform remote operations like remote password reset, account discovery and one-click login.



iii. Choose the Resource Type from the drop-down (the default value will be **Windows**). Based on the resource type, PAM360 uses unique procedures for password resets. For example, the password reset mechanism of Windows is not the same as that of Linux or Mac. This field also helps to organize your resources based on their type. To add a custom resource type, click the **Add New** option beside this field. Enter a custom resource type in the pop up window, such as an App or a printer, click **Add** and then choose the custom resource from the **Resource Type** dropdown. To know more about the types of resources supported by PAM360 and how to manage them, click here.





3. Choose the **Group Name** to add all the common servers, say Windows servers or Linux servers, to a single resource group. To add a new group, click **Add New**, enter a group name, click **Add** and choose the custom group from the **Group Name** drop-down. If a custom group is not created, Default Group will be chosen. Click here for more info on resource groups.

4. When adding a domain controller with the resource type as **WindowsDomain**, enter the domain name as **NETBIOS** in the **Domain Name** field. This is required for the Windows Service Account Reset feature.
5. The fields **Description**, **Department** and **Location** are not mandatory, but having these fields populated with the correct values will be helpful for searching and grouping the resources.
6. When adding a web application or a website as a resource, provide the **Resource URL** and choose the resource type as **Web Site Accounts**. To access any web-based resource, specify the full URL in this field, for example, https://sso.godaddy.com. This value will be used for the auto-fill feature that works with the help of our browser extensions (**Chrome**, **Firefox** and **Edge**).

   Note:

   For the resource types that support URLs, enter the valid URL in the form of HTTPS-based web links. This will be used to establish a connection to the resources using the HTTPS Gateway Connection method if configured by the administrator.

7. Similar to the above types, PAM360 allows you to add virtual machines managed in an Amazon WorkSpaces client, as resources into the PAM360 repository. While adding AWS Active Directory resources, choose the resource type as **WindowsDomain**. Refer to the **Amazon WorkSpaces** in the **Discovering Resources** section to learn how to automatically discover virtual machines in an Amazon WorkSpaces client.
8. Choose the required **Password Policy** from the drop-down. When PAM360 randomly generates passwords for accounts, they will be in compliance with the policy chosen here.
9. Click **Save** to add the resource. Click **Save & Proceed** to add an account to a resource.

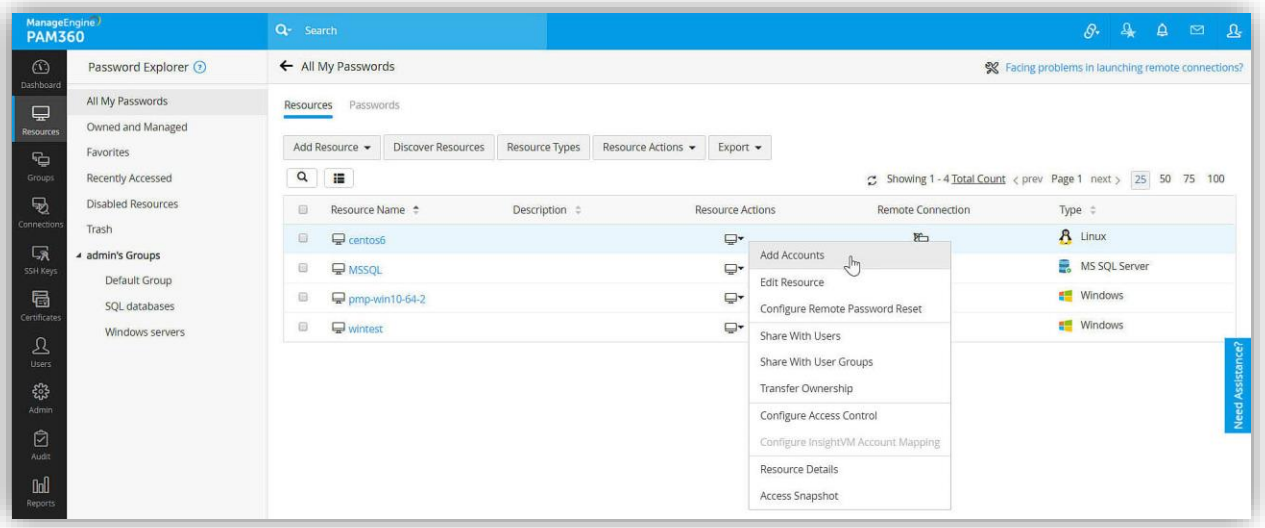
   Notes:

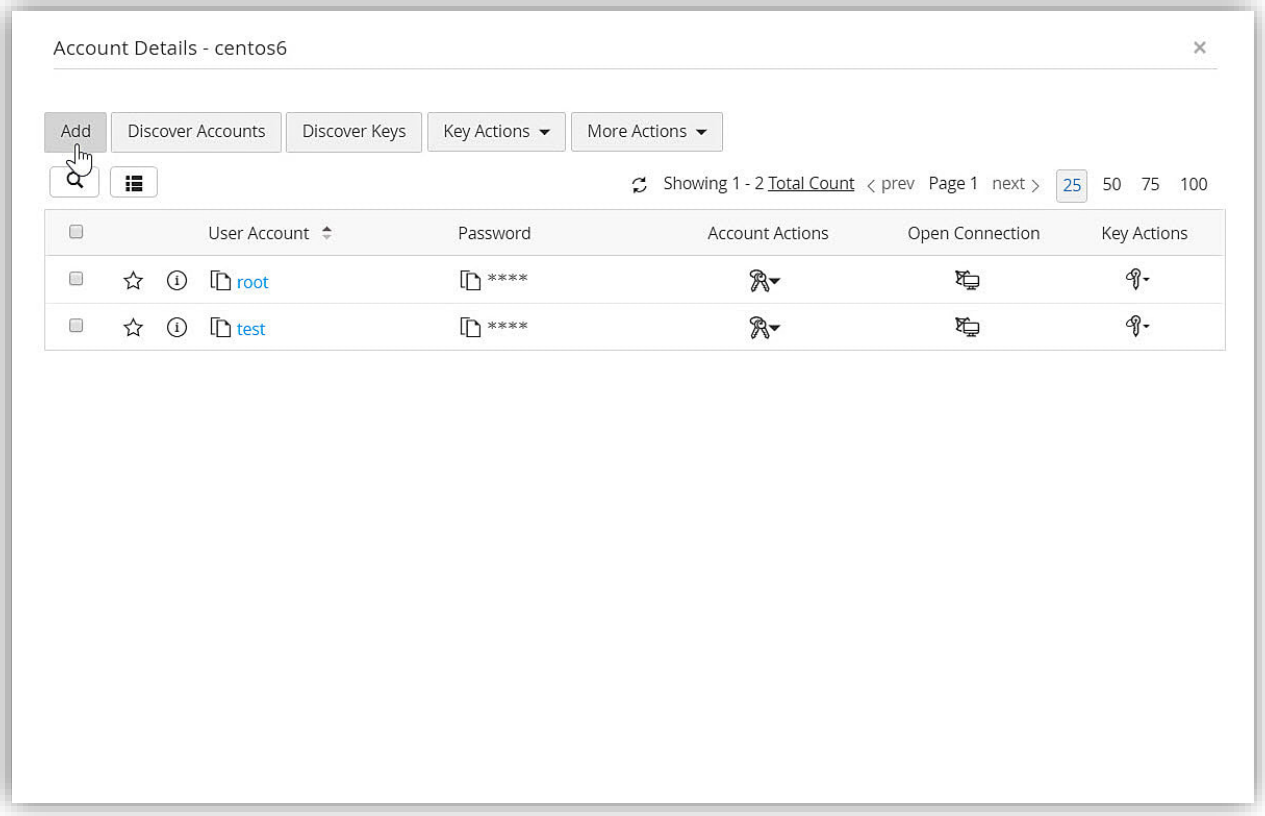
   - Except the Super Administrators (if configured in your PAM360 set up), no one, including the admin users, will be able to see the resources added by you. Click here to know more about resource sharing.
   - Click here to know more about importing resources from Files and KeePass.

2. Adding an Account to a Resource

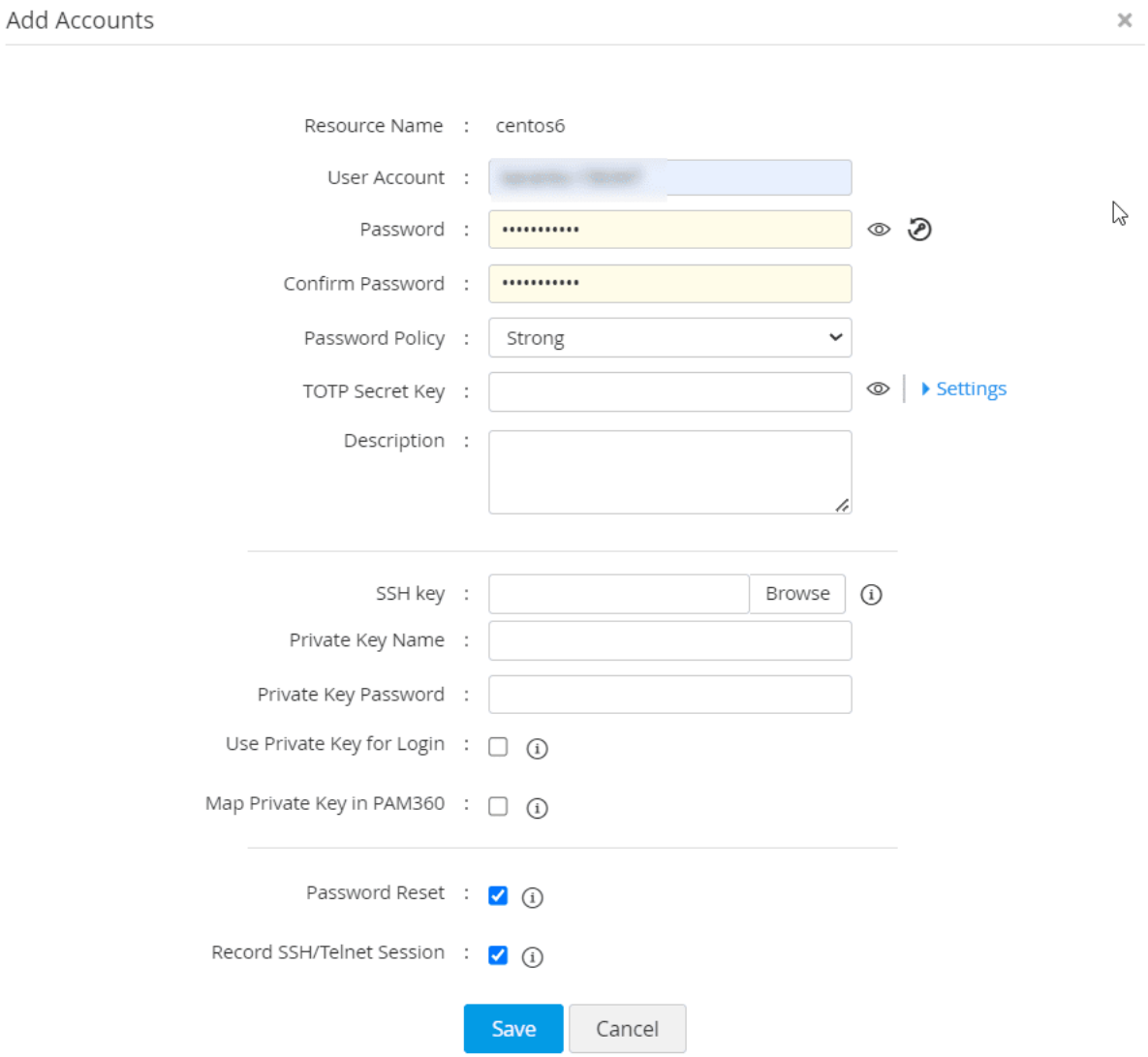
Once resources are added to PAM360, follow the below steps to add user account(s) and passwords to the new resource. You can add an user account to the resource in two ways:

1. Navigate to the **Resources** tab. Click **Resource Actions >> Add Accounts** beside the newly added resource.
   OR
   Click the **Resource Name** of the newly added resource and click **Add** in the **Account Details** window that pops up.





2. Enter the required details in the **Add Accounts** form as explained below:



3. Enter the unique name for the account in the **User Account** field.
4. In the **Password** field, either enter the password of the account manually if you know it, or generate a password using the **Generate Password** tool beside this field. If you are entering the password manually, it should be in compliance with the **Password Policy** you had set for the resource.

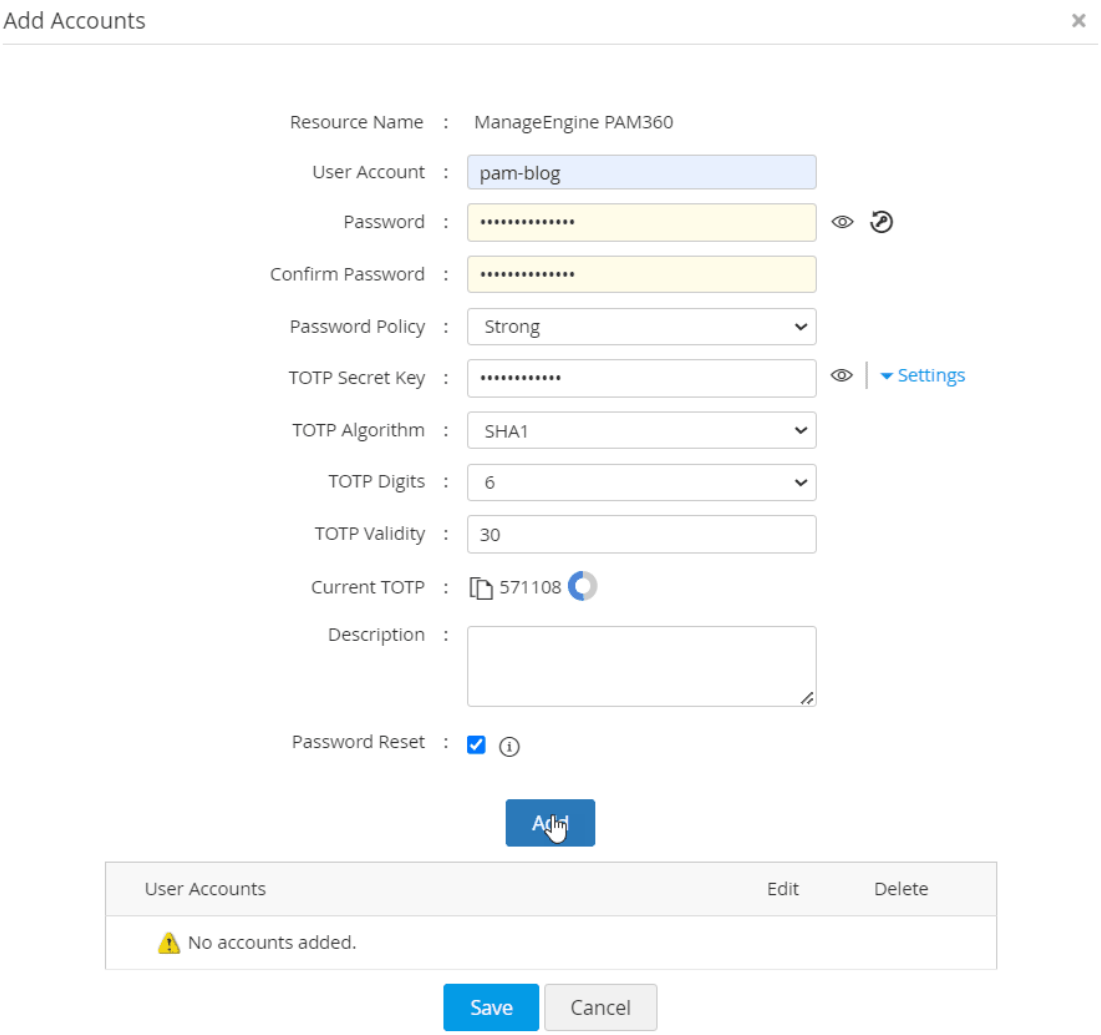
> **Note:** To enable password reset in remote systems, ensure that the passwords you enter in this step and the ones in the actual target systems are the same. PAM360 uses these credentials to log in to the target systems for resetting the password, and if the passwords are wrong, the password reset will not happen.

5. Choose the required **Password Policy** for the account - Strong, Medium or Low. The

password policy is maintained at resource level and account level, and the account level policy can override the value of resource level password policy. Click here to learn more about creating custom password policies apart from the default ones.

6. If the account (particularly website accounts) is enabled with TOTP as the Two-Factor Authentication (2FA), input the **TOTP Secret Key**. This allows the users to directly access the account through the PAM360 interface, streamlining the generation of TOTP one-time codes alongside with shared passwords.
    a. By default, the account configured with TOTP as the 2FA supports the SHA1 Algorithm, 6-digit TOTP codes, and a validity of 30 seconds. If the account supports a different set of parameters for TOTP codes, please select the appropriate **TOTP Algorithm** and **TOTP Digits** and enter the **TOTP Validity** in seconds by clicking upon the Settings dropdown beside the **TOTP Secret Key** field.

    > Note that if the TOTP Algorithm, TOTP Digits, and TOTP validity differ between the account and the values entered here, the authentication mechanism will not work as expected due to the generation of incorrect one-time codes. Also, once configured, the TOTP secret key cannot be retrieved again for the account. Therefore, exercise caution to ensure that the values entered or selected here match those values supported by the account.



7. It is recommended to provide any particular details of the account in the **Description** field as this field will also be searched through when you search for a particular account using PAM360's search tool.
8. To import an SSH key and associate it with this account, click **Browse** and add a .key file. Enter the **Private Key Name** and **Passphrase** for the key.
9. Select the checkbox **Use private key for login** to authorize remote connections using SSH keys instead of account credentials. Refer to the **Remote Connection to SSH-based Devices Using SSH Keys** to know more about remote connection using SSH keys.
10. Select the checkbox **Map private key in PAM360** to force map SSH keys to user accounts, even if the target systems are not reachable.
11. Click **Add** to list this account under **user accounts** column in the same page. You can add any number of accounts under a particular resource by following the above steps; all the accounts will be listed below the **User Accounts** table.

Performing the above steps will add the required user account(s) and password(s) to the resource. Users who are authorized to access the resource will be able to view the information.

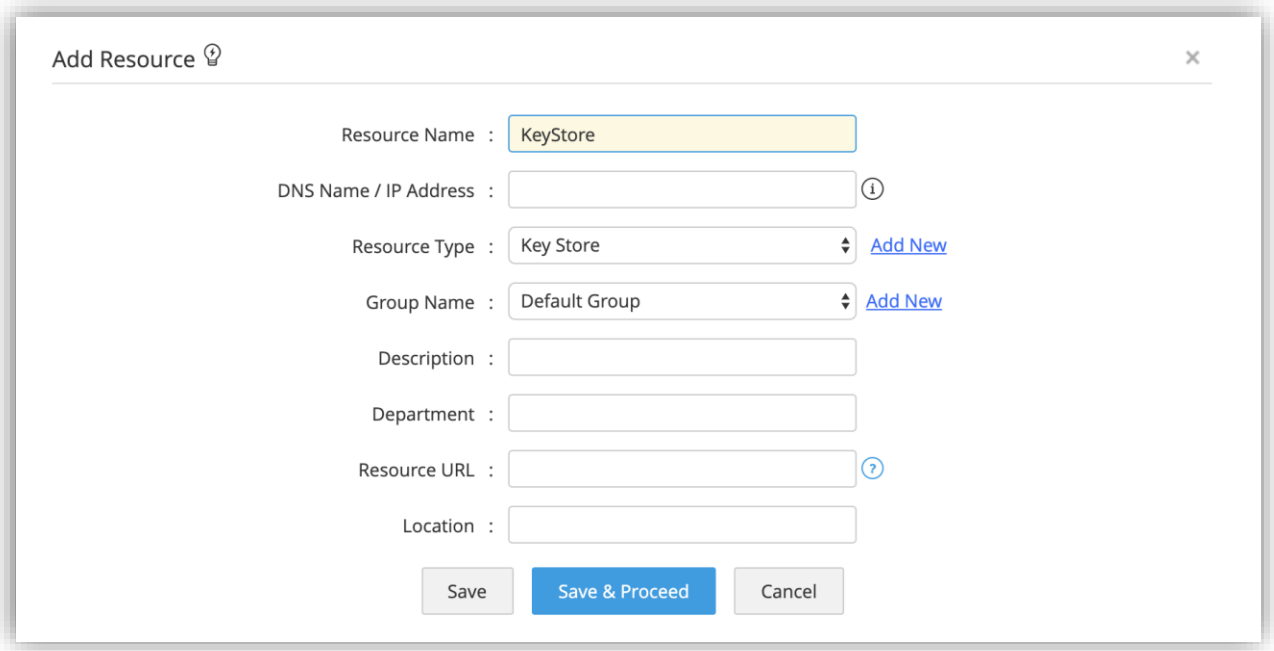
3. Storing Files and Other Sensitive Data

PAM360 allows users to store other types of sensitive data such as:

- **Digital Certificates**
- **License Keys**
- **Files**
- **Documents**
- **Photo Copies**

Different file types can be securely stored in the PAM360 repository along with their passwords. To store a license key, certificate, document, etc., follow the below steps:

1. Navigate to the **Resources >> Add Resource >> Add Manually.**
2. In the **Add Resource** window, fill in the details as required.



i. Specify the **Resource Name** which uniquely identifies the resource in PAM360.
ii. Enter the **DNS Name or IP Address** of the resource. It is mandatory to provide a valid DNS name or IP address to perform remote operations like remote password reset, account discovery and one-click login.

iii. Select the **Resource Type** as any one of the following: (By default, PAM360 supports the following file stores)

- **File Store:** To store digital content (documents, pictures, executables etc).
- **Key Store:** To store software keys.
- **License Store:** To store software license keys.

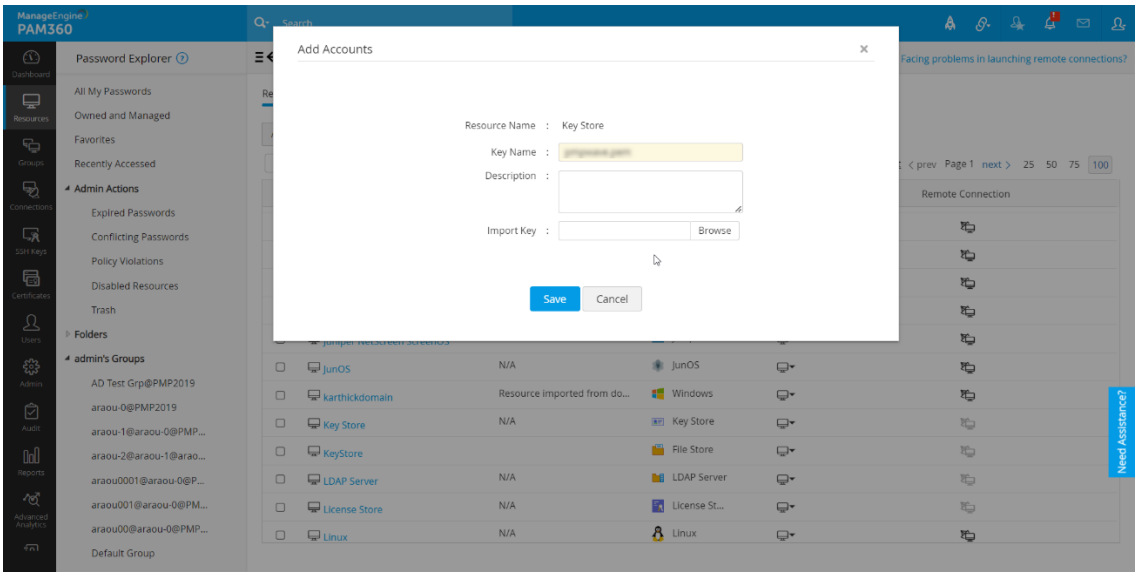
iv. To add a custom resource type, click the **Add New** option beside this field. Enter a custom resource type in the pop up window, such as KeyStore, click **Add** and then choose the custom resource from the **Resource Type** drop-down.

v. The fields **Description**, **Department** and **Location** are not mandatory, but having these fields populated with the correct values will be helpful for searching and grouping the resources.

vi. Click **Save** to save the resource and exit.

vii. Click **Save & Proceed** to import and save the required Key/File/License under the resource.

viii. In the **Add Accounts** window that opens up, the fields will be shown based on the **Resource Name** you chose (**File Store, Key Store, or License Store**). Fill them as required:



a. Specify the **Key Name/File Name/License Name**, to be stored under the resource.

b. Click **Browse** and choose the Key/File/License to be imported.

c. Enter a description in the **Description** field.

d. Click **Save**.

Now, the Key/File/License will be successfully saved under the resource.

> **Note:** Resources of the above types are managed and shared in the same way as other resources. During retrieval, a link to the file is provided for it to be saved locally to the disc.

See also:

- Managing_Resource_Types
- Discovering Resources
- Remote_Password_Reset

Importing Resources

Apart from Adding_Resources_Manually, you can also import them. There are a few ways by which you can import your resources into PAM360:

1. **Importing Resources from a File**
2. **Importing Resources from KeePass**
3. **Importing Resources from Active Directory**

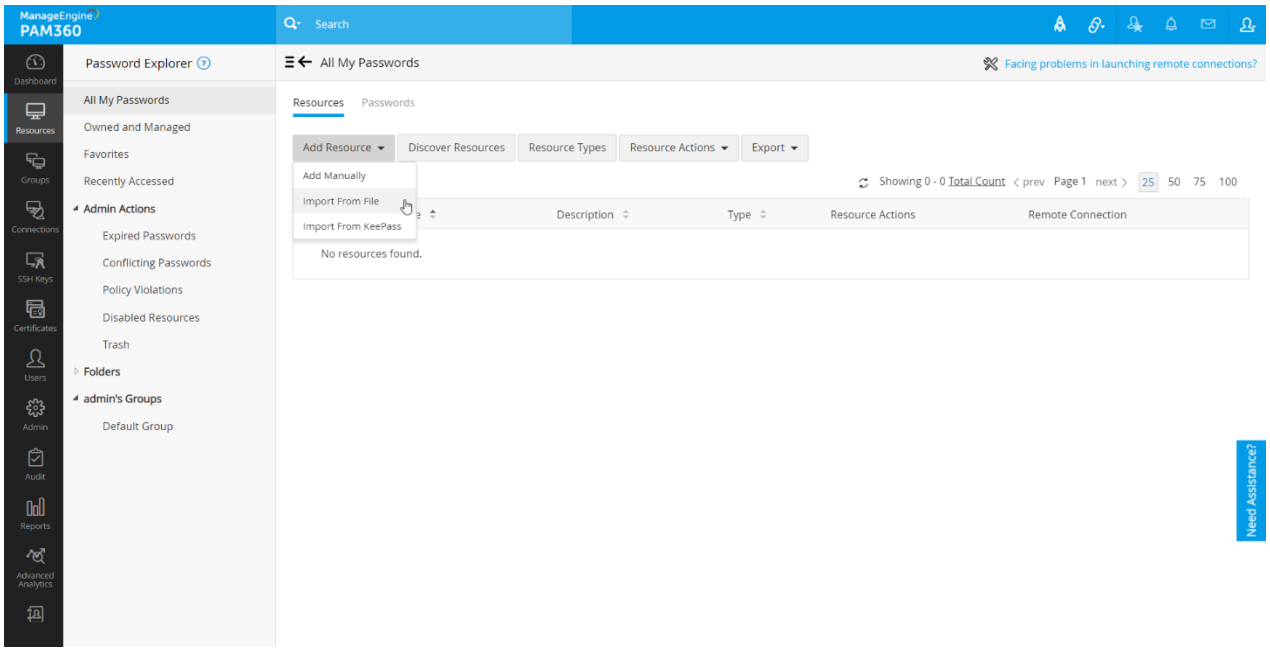
1. Importing Resources from a File

You can import resource details from a CSV/TSV/Excel file using the import wizard. Click here to view sample files and learn more about the file formats supported for importing.

Note: When importing resources, TOTP Secret Keys for accounts with configured TOTP cannot be mapped. You must manually configure TOTP for these accounts after import.

Note: Earlier, it was possible to import a .txt file containing comma-separated data, and in step 2, the data would be listed as expected. However, from build 6400 onwards, if the entries are comma-separated, the file format must be .csv. Files with tab-separated values should be saved as .txt or .tsv for importing.

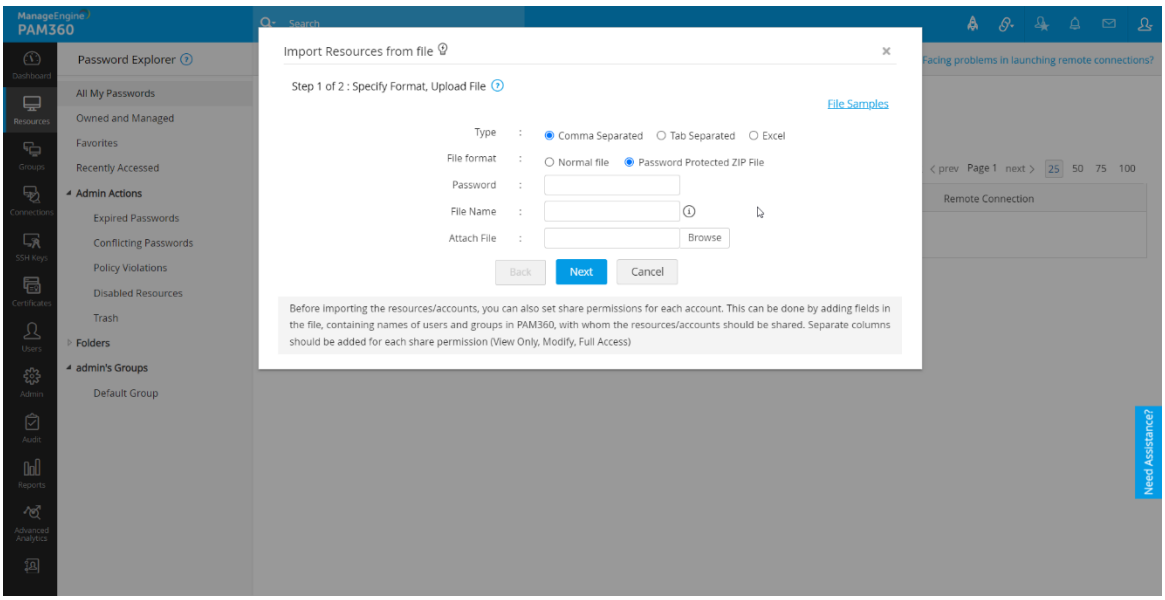
1. Navigate to the **Resources** tab.
2. Click the **Add Resource** button and select **Import from File** from the drop-down list.



3. In the dialog box that opens, select Comma Separated, Tab Separated, or Excel as your file type before you browse and import the file. You can choose from two different file formats:

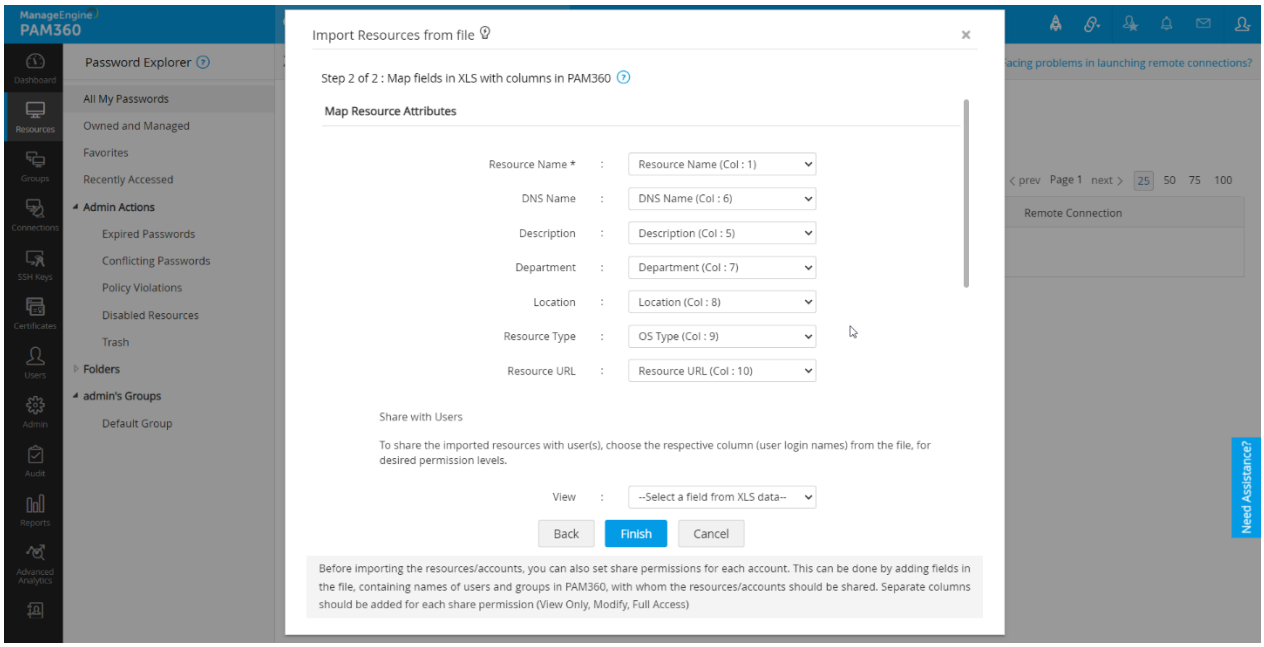
   i. **Normal File:** This option can be used to upload a plain text CSV/TSV file directly.

   ii. **Password Protected ZIP File:** This option can be used if you wish to upload a password protected ZIP folder containing the CSV/TSV/Excel file, for enhanced security. If you choose this file format, you must also provide the password and specify the name of the target file in the 'File Name' field. In case the 'File Name' field is left empty, PAM360 will automatically import information from the first file that it accessed in the unzipped folder.



4. In your CSV/TSV/Excel file, the entries could be present in any order. You can choose which field in the file maps to the corresponding attribute of the PAM360 resource and

account. Both the default and the user defined attributes will be listed in the wizard. The user defined attributes should have been defined before the import operation. If a resource contains multiple user accounts, then the resource fields will have to be repeated for each user account in the file.



5. If you have resources with attributes that cannot be placed in the file (like files for the File Store resource type), you can leave those entries blank in the file and later edit the resource and update the attribute value.
6. If the list of resources imported by you contains any of the already existing resources, they will not be added to PAM360 by default. If you want them to be overwritten, you need to select the option **Overwrite existing resources.**
7. Click **Finish** to complete the resource import process.
8. The successfully/failed import process will be logged as an audit with detailed information. Navigate to the **Resource Audit** sectionin the **Audit** tab for details.

Note: If you are unable to find the reason for import failure from the **Audit** tab, set the log level to **Debug** mode and perform the import operation again. Now, you will get the detailed failure traces from the log file available in the **<PAM360 Installation Folder>\logs\pam0.txt** directory.

Notes: After importing resources, if you want to configure password reset for the target systems, you need to do it by editing the resources.

- **Importing resources takes time**

  When you try to import a large number of resources, it would take a while to import all of them to PAM360 inventory. Once, it is done, you will notice the message "Resources Imported Successfully".

- **My resources have additional fields**

  You can import the additional fields too. But, prior to importing the resources, you need to add those custom fields to PAM360.

- **I do not have some of the fields that are listed as mandatory for PAM360 in my CSV file**

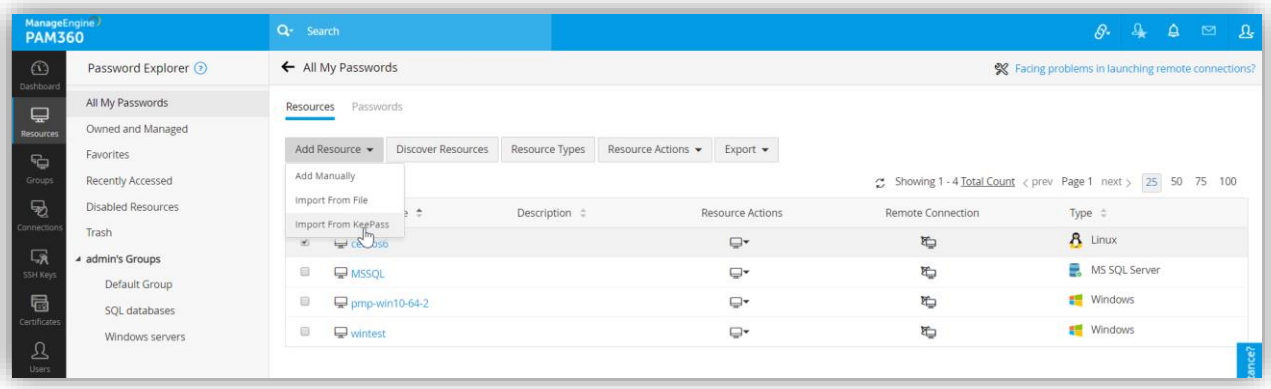
  That is not a problem. Only 'Resource Name' and 'Account Name' fields are mandatory. So, you can import whatever you have.

3. Importing Resources from KeePass

You can also import resource details (IT resources, their accounts, and passwords) directly from KeePass (both 1.x and 2.x) using the import wizard. The import file should be a KeePass database file, either .kdb or .kdbx.

To import resources from KeePass:

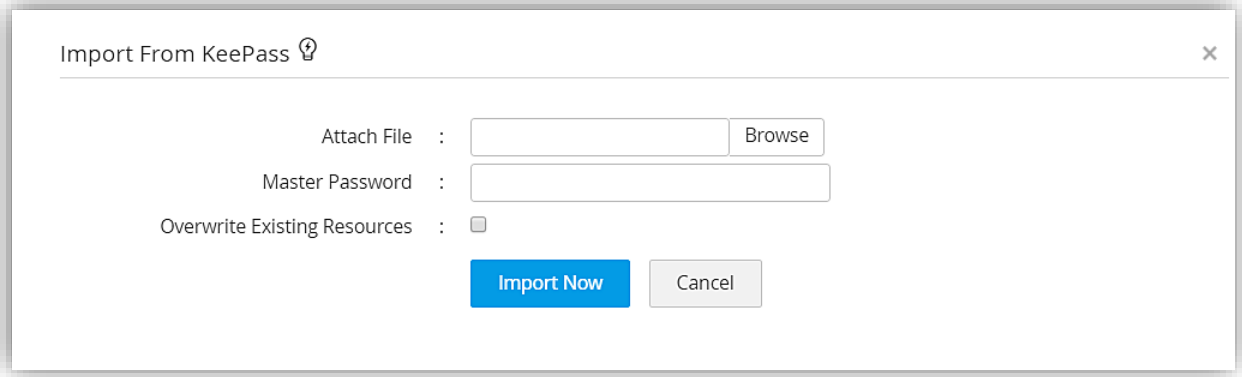
1. Navigate to **Resources** tab.
2. Click the **Add Resource** button and select **Import from KeePass** from the dropdown.



3. In the pop-up form that opens, browse and select the required KeePass Database file for **Import File.** Usually, the file will be available at the location chosen by you while saving the file in KeePass after its creation.
4. After selecting the file, enter the Master Password you have set for the file.

> **Note:** Currently, you can import resources from KeePass only using Master Passwords, and not Key Files. So, ensure the selected file has a Master Password.

5. **Overwrite Existing Resources:** Check this option if you want the import operation to overwrite resources that already exist in PAM360. If this option is off, resources already existing in PAM360 database will not be imported from KeePass.
6. Click **Import Now.** The result of every line imported will be logged as an audit record.



Notes:

1. During the import operation, resource details such as resource URL, user accounts, passwords, and notes will be automatically mapped and imported from KeePass. For DNS Name/IP Address, the details in the file be imported only if they match with the inbuilt regular expressions. Also, if you have stored the resources within different static groups such as Windows, Linux, etc, in the database file, the groups will also be automatically created in PAM360 while importing the resources.
2. Once the resources and groups are imported, the Resource Type of all the resources will, by default, be marked as **Unknown** in PAM360. You can edit the resources and sort them under desired types. In case of web site accounts alone, the resources will be automatically sorted as **Web Site Accounts**, if the site URL is provided in the import file.
3. After importing the resources, if you want to configure remote password reset for the target systems, navigate to **Resources >> Resource Actions >> Configure Password Reset**.

Managing Resources

PAM360's privileged resource and account management solution comes with an all-inclusive spread of features that allows you to manage resources efficiently from the PAM360 interface. You can edit, delete, copy, and export all of your existing resources.

1. Editing Resource Details - The edit operation comes in handy in cases where the resources that you imported in bulk via the discovery operation or through a file are no longer relevant or contain incorrect attributes. The edit operation can avoid the burden of re-importing the said resources.
2. Deleting Resources - The delete option allows you to delete the resources that you no longer need so that you can organize your necessary resources in an orderly fashion. The delete operation gives you an option to either move the selected resources to the Trash or delete them permanently.
3. Copy Resources - Your enterprise's IT network may contain several resources that are identical in properties. Instead of importing all of them into PAM360, you can add one of those resources and make multiple copies of the same. In this process, the attributes of the source resource are applied to all the duplicates. Using the edit operation, you can modify the attributes as per your requirements at any time. Please note that the duplicated resources also inherits the following attributes from the source resource:
    i. The resource-level and account-level share permissions.
    ii. Access control settings configured for the source resource.
    iii. All the accounts that are under the source resource.
    iv. Password history of the accounts that are part of the source resource.
4. Exporting Resources - PAM360 offers several secure options to export the passwords of resources stored in the solution if you wish to have an offline copy for safekeeping. You can either export resource attributes in plain text on a spreadsheet. The file exported in this manner will contain the following options in plain text: resource name, account name, and passwords. A more secure option would be to export the passwords to an encrypted HTML file. In addition to the above, PAM360 provides integration with multiple cloud-storage services such as Dropbox, Box, and Amazon S3 services through integration. Using this, you can synchronize the encrypted HTML file directly to your desired cloud storage service.
5. Transferring Ownership - As a resource owner, the administrator has complete control over the operations they can perform on the owned resources. However, under special circumstances where an administrator who is in charge of managing several resources leaves the organization, PAM360 offers an option to transfer ownership of your existing resources to other available administrators. This one-click operation ensures you don't lose access to those critical assets.

Click through the links listed below to learn about each topic in detail.

Quick Links

1. Exporting Resources
2. Editing Resource Details
3. Copying Resources
4. Deleting Resources
5. Transferring Resource Ownership

Exporting Passwords for Secure Offline Access

PAM360 provides multiple export options for secure offline access and safekeeping of password information.

1. The basic option is to export password information such as resource name, account name, and passwords in plain text to a spreadsheet.
2. The more secure option is to export the passwords to an encrypted HTML file.

> **Note:** In addition, PAM360 allows auto-synchronization of the encrypted HTML file to users' mobile devices through integration with cloud storage services which include **Dropbox, Box, and Amazon S3** services. For more info about how to enable cloud storage option for users.

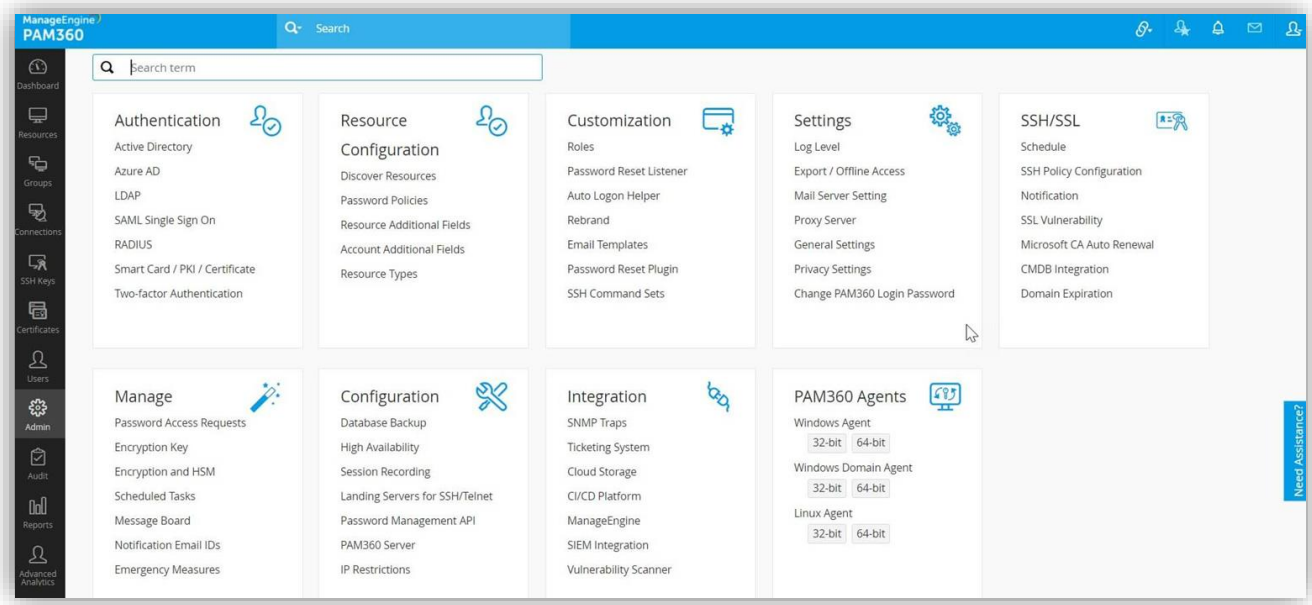
In both the above options, you can export the resources, accounts and passwords for offline access. Administrators can decide which option should be used in their organization. In addition, the export can be enabled or disabled for specific users or user groups based on requirements. However, before configuring user-specific settings for export, the feature should first be enabled globally for all the users.

At the end of this section, you will have learned the following:

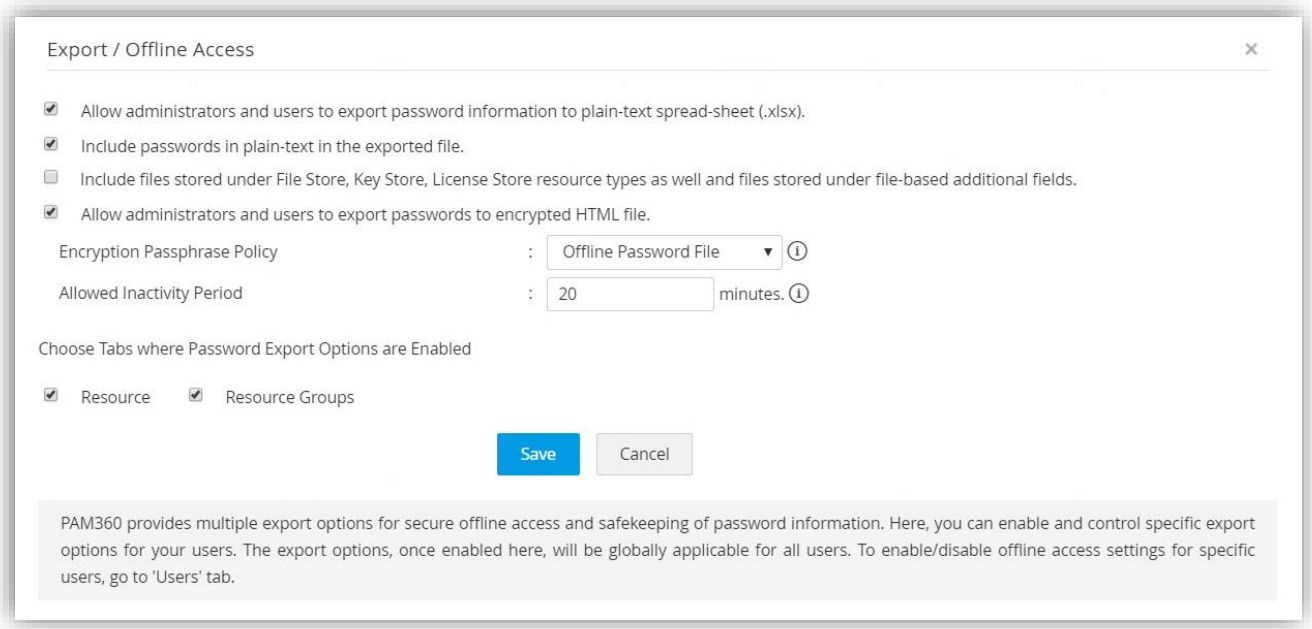
1. **Steps to Configure Settings Globally for Export/Offline Access**
2. **Steps to Export Resources**
3. **User-Specific Settings for Export/Offline Access**

1. Steps to Configure Settings Globally for Export/Offline Access

1. Navigate to **Admin >> Settings >> Export / Offline Access.**



2. In the dialog box that opens, different options related to password export will be displayed.
3. By default, two options - **exporting passwords in plain text to .xls** and **exporting passwords to an encrypted HTML file,** will be enabled to all users and administrators. You can disable these options by deselecting the respective check-boxes.



i. **Exporting resources in plain text to an .xls file**

This option will allow the users and administrators to export resource details in plain text to a spreadsheet. However, in the **Export / Offline Access** UI window, you'll find another option **"Include passwords in plain-text in the exported file".** You can disable this option globally prevent passwords from being printed in plain text in the .xls file. Another option **"Include files stored under FileStore,**

KeyStore, LicenseStore resource types and files stored under file-based additional fields" allows you to choose whether files can be included while exporting in plain text.

> **Note:** If the administrator has enabled encryption for all export operations across PAM360, the XLS file will be exported with password protection. The user has to supply the encryption passphrase everytime that they need access. They can view or copy the passphrase by logging in to PAM360, clicking the **My Profile** icon on the top right corner and selecting **Export Settings** from the drop-down menu.

ii. **Exporting passwords as an encrypted HTML file**

- You can export passwords as an encrypted HTML file so as to view the passwords even when there is no internet connection. This offline option is very secure. The contents of the file will be encrypted using AES-256 bit algorithm with the passphrase that the users will be required to provide prior to exporting the passwords. PAM360 does not store this passphrase anywhere and we recommend you to not store / write it down anywhere either. The HTML file cannot be opened without the passphrase. In case you forget the passphrase, you can export another HTML file. Your passphrase could be up to 32 characters long, including blank spaces.
- To ensure that users set strong passphrases for their HTML file, a complexity policy is set by default if the encrypted HTML option is enabled. The default policy will be **Offline Password File.** To change this policy, you can select any of the other three default password policies of PAM360 or the custom policies created by you, if any. You can select the desired policy in the **Encryption Passphrase Policy** field in the Export Passwords UI window.

4. **Inactivity logout:** You can also specify the inactivity log out time period in minutes, after which the user will be automatically logged out from the offline file while viewing the passwords in the browser. You can specify the timeout period against the text field **Allowed Inactivity Period.**
5. Once you have **enabled/disabled** various export options based on your organization's requirements, click **Save.**

The settings will then take effect globally for all users and administrators in PAM360.

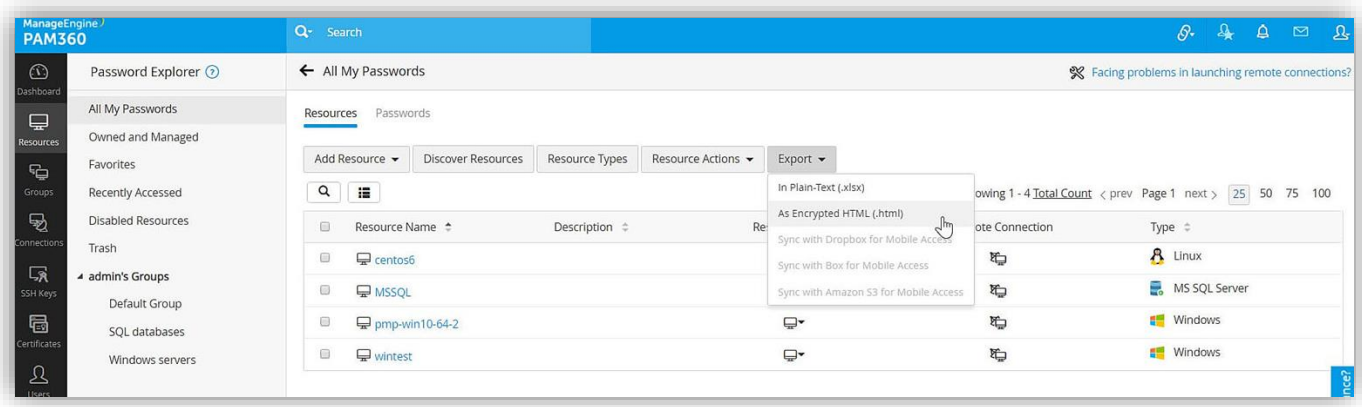
2. Steps to Export Resources

The passwords can be exported by users and administrators as per settings configured by the PAM360 Administrator.

To export resources, navigate to **Resources >> Export**

Option 1 - Exporting resources in plain text to a spreadsheet

To export resources in plain-text, click the button **Export** present in the Resources tab and select **In Plain-Text** from the drop down.

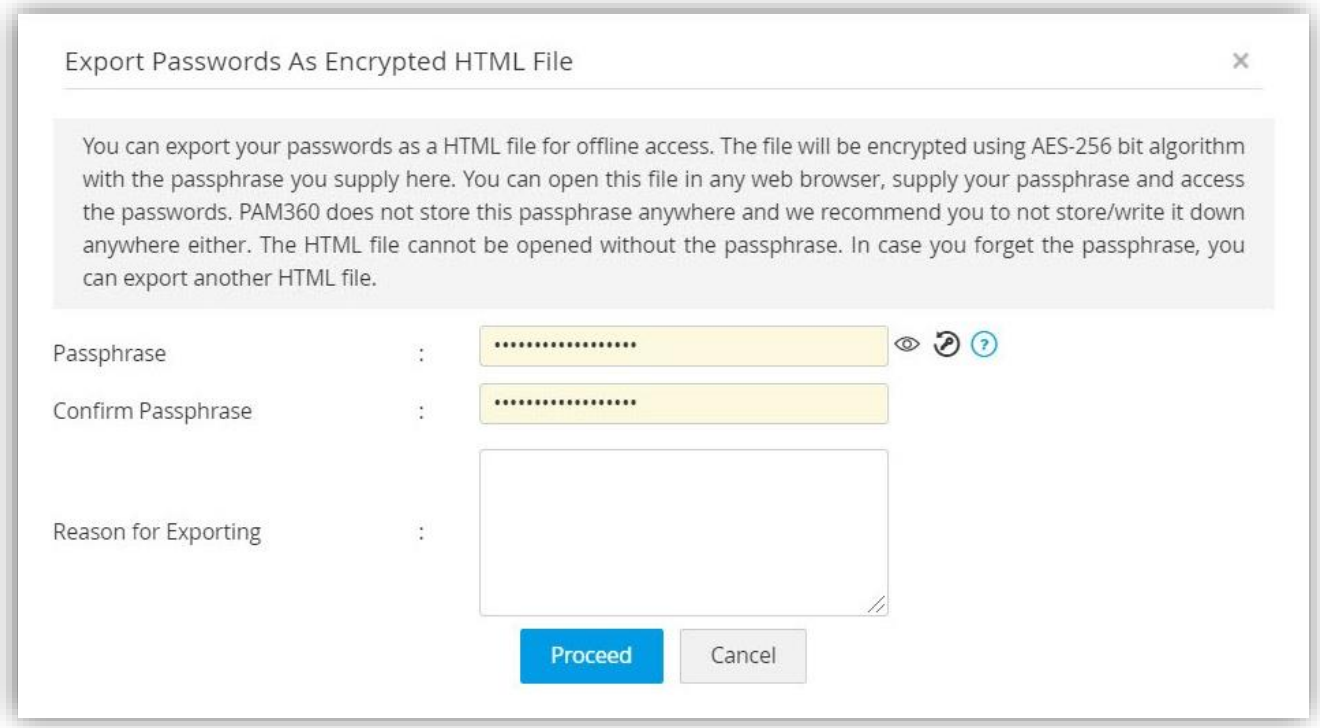


The resources are exported to a file and it is shown as a pop-up. Save the file in a secure location in (.xls) format.

Option 2 - Exporting resources as an encrypted HTML file

To export resources as an encrypted HTML file,

1. Click the button **Export** present in the Resources tab and select **As Encrypted HTML** from the drop down.
2. In the dialog box that opens, specify a passphrase in accordance with the password policy enforced by your administrator. The passphrase will be used for encrypting (AES 256) the HTML file for offline access.

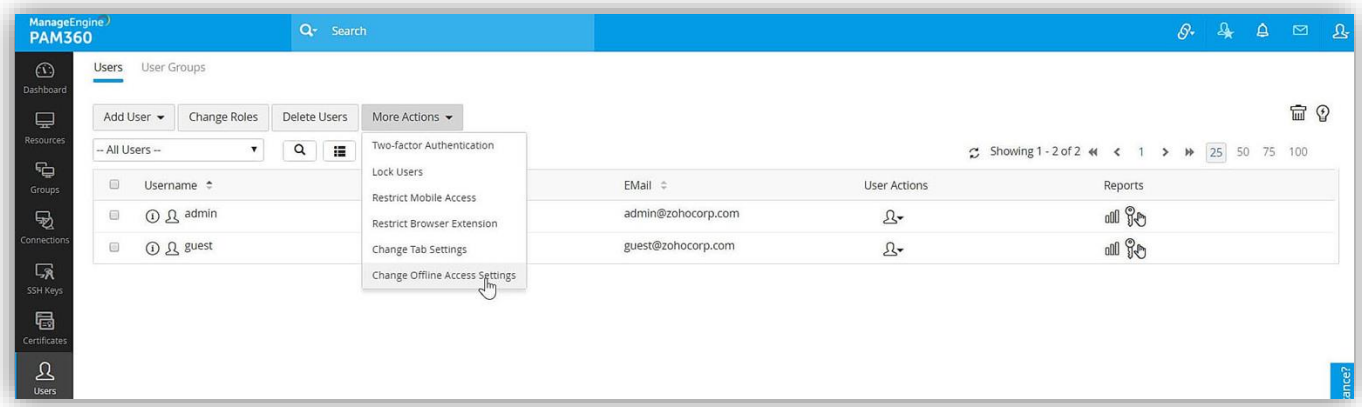


3. You can also open the file in any web browser by simply providing the same passphrase. PAM360 does not store the passphrase anywhere and so if you forget the passphrase, you cannot open the file. And we also recommend you not to store or write down the passphrase anywhere.
4. Confirm the passphrase and enter a reason for exporting the passwords.

The resources are exported to a file and it is shown as a pop-up. Save the file in a secure location in (.html) format.

3. User-Specific Settings for Export/Offline Access

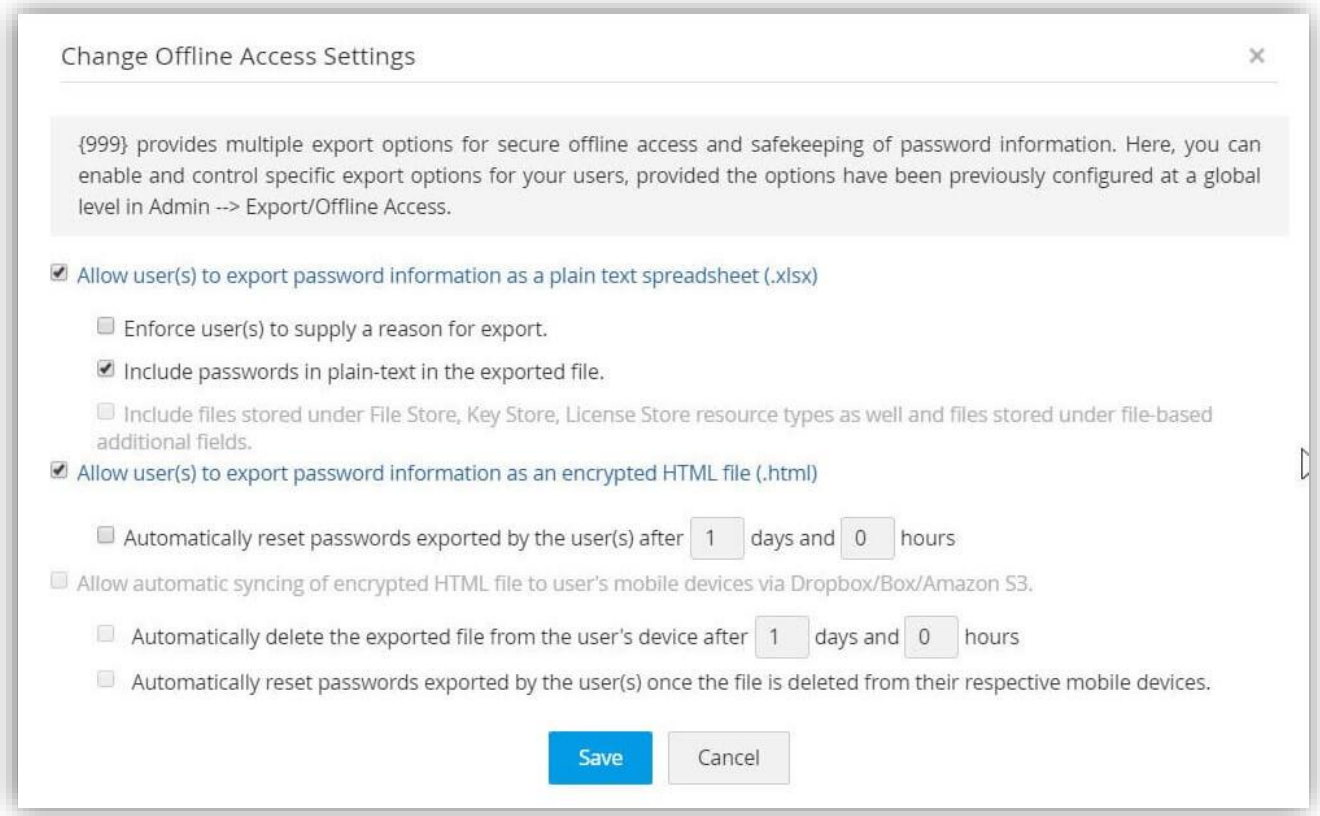
To restrict certain users from having one or all the password export options to allow only specific users to have this permission, user-specific settings can be changed by navigating to Users tab, selecting the desired users for whom settings should be changed, and clicking on **More Actions >> Change Offline Access Settings.** Alternatively, you can also carry out changes for an individual user by clicking on the **User Actions** icon against that specific user and selecting **Export / Offline Access** from the dropdown.



3.1 Imposing restriction for users

You can also impose granular restriction for the users while enabling/disabling export password options.

1. When allowing users to export passwords in plain-text, you can enforce them to specify a reason for exporting. The reason entered here will be recorded as an audit trail. In addition, you can just allow the users to export the resource name and user account details alone, but prevent them from exporting the passwords in plain-text.
2. In the case of exporting passwords as an encrypted HTML, for security reasons, administrators can enforce automatic reset of the exported passwords after a specific time period.
3. In case of auto-synchronization of the encrypted HTML file to users' mobile devices, administrators can enforce automatic deletion of the HTML file from the users' devices after a specific time period. There is also an option to automatically reset the exported passwords immediately after deletion of the HTML file from users' devices.



3.2 Least privilege model for security reasons

For security reasons, PAM360 adopts **Least privilege** model for users. For instance, let's assume that a particular user is part of three user groups and there is group level restrictions for one of the groups - the members of the group are not allowed to export passwords in plain text. In the above scenario even if the user has permission to export passwords in plain text at individual level, the restriction imposed on one of the groups in which the user is part of, will take precedence. This rule applies for all type of restrictions as explained above.

Managing Resources

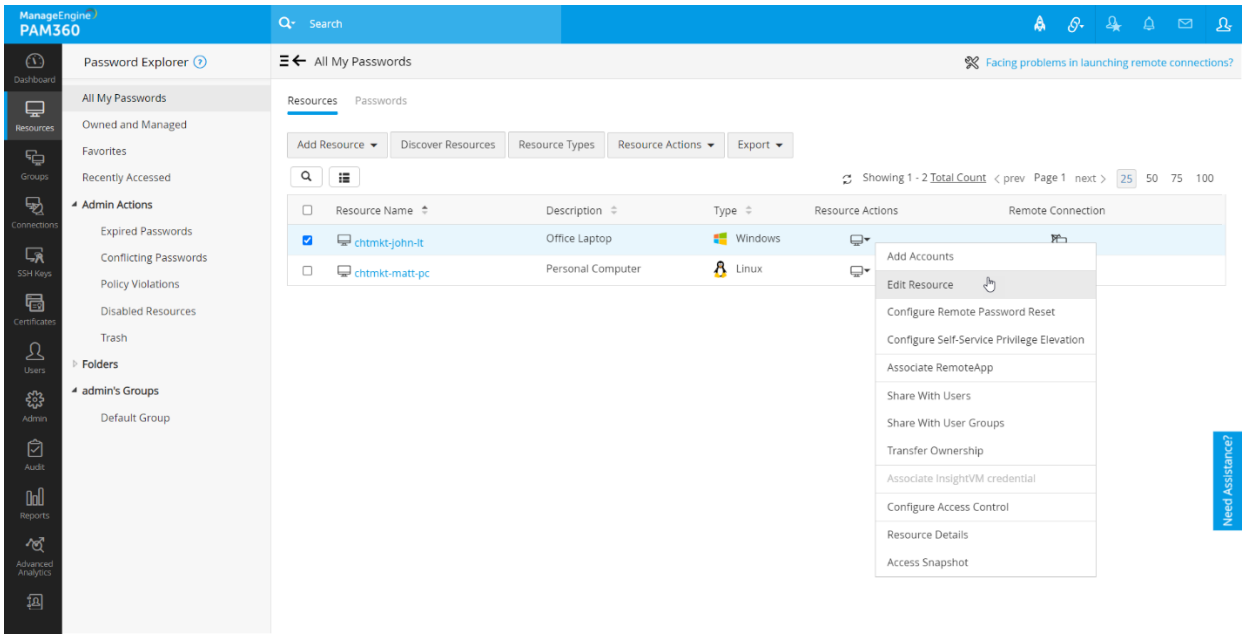
You can manage all the resources added by you from the 'Resources' tab. Edit any of the attributes of the resources and the associated accounts, such as Resource URL, Password Policy, Domain Name, etc., anytime as required. It is also possible to temporarily move the resources to trash or permanently remove them if no longer needed.

The following are the possible actions on the existing resources:

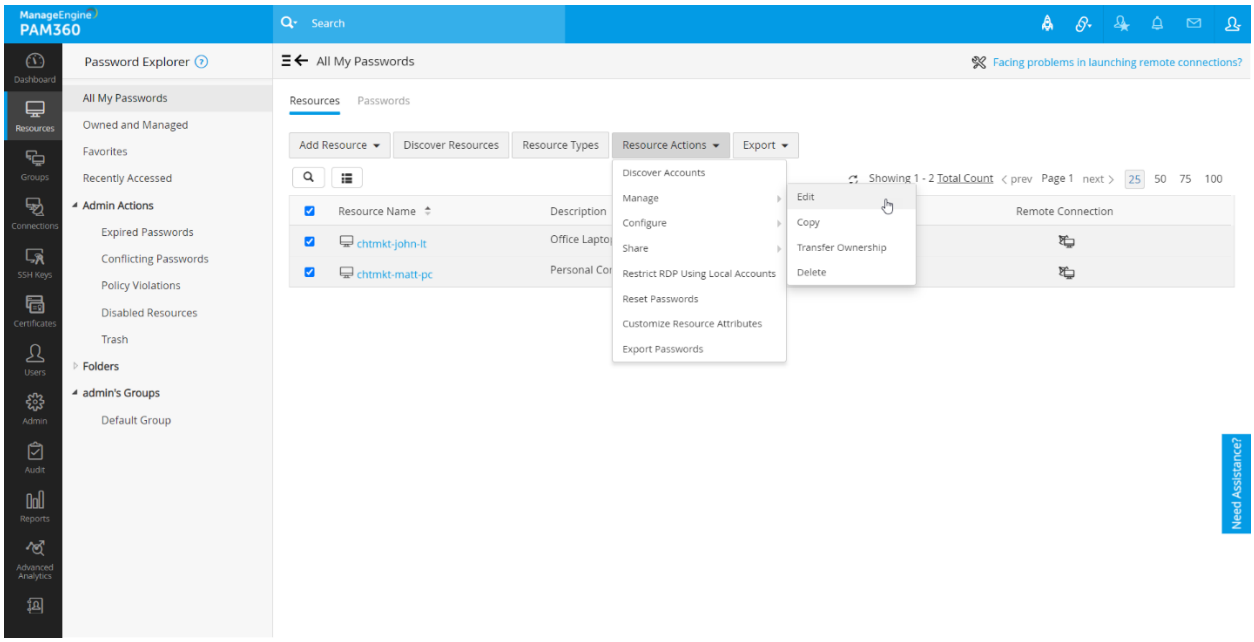
1. **Editing a Resource**
2. **Adding Accounts to an Existing Resource**
3. **Deleting a Resource**
4. **Restoring Resources from Trash**

1. Editing a Resource

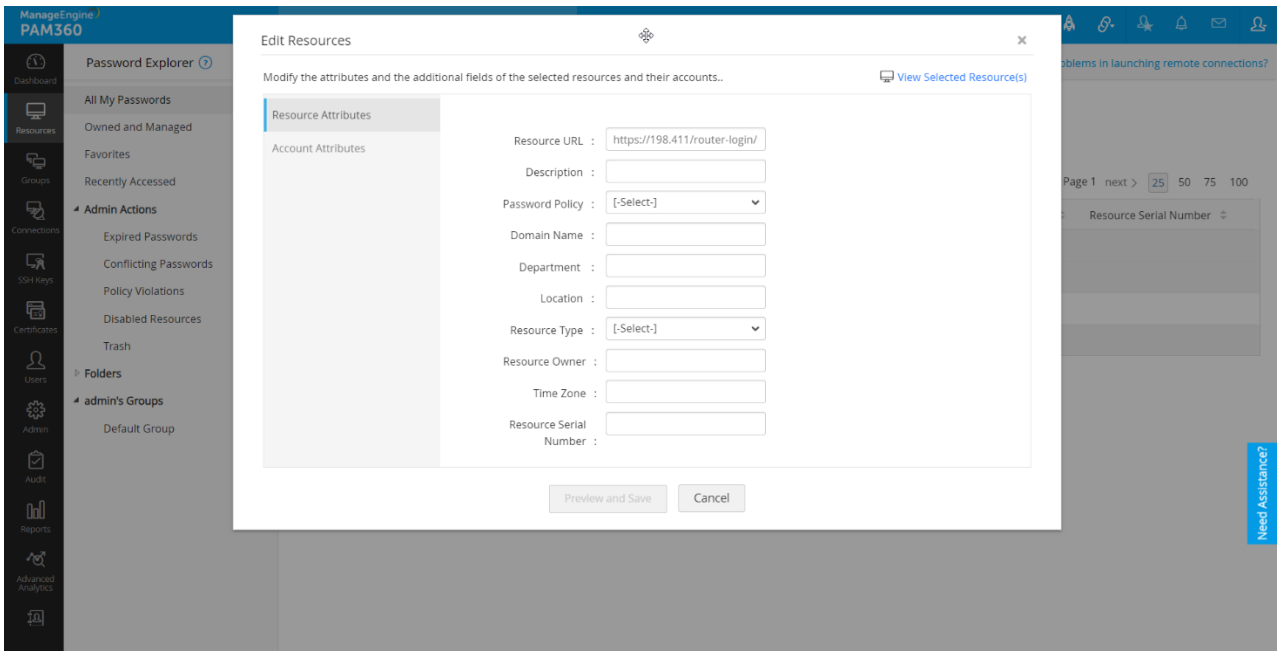
1. Navigate to the **Resources** tab.
2. Click the **Resource Actions** icon against the resource you wish to edit and select **Edit Resource** from the drop-down list.



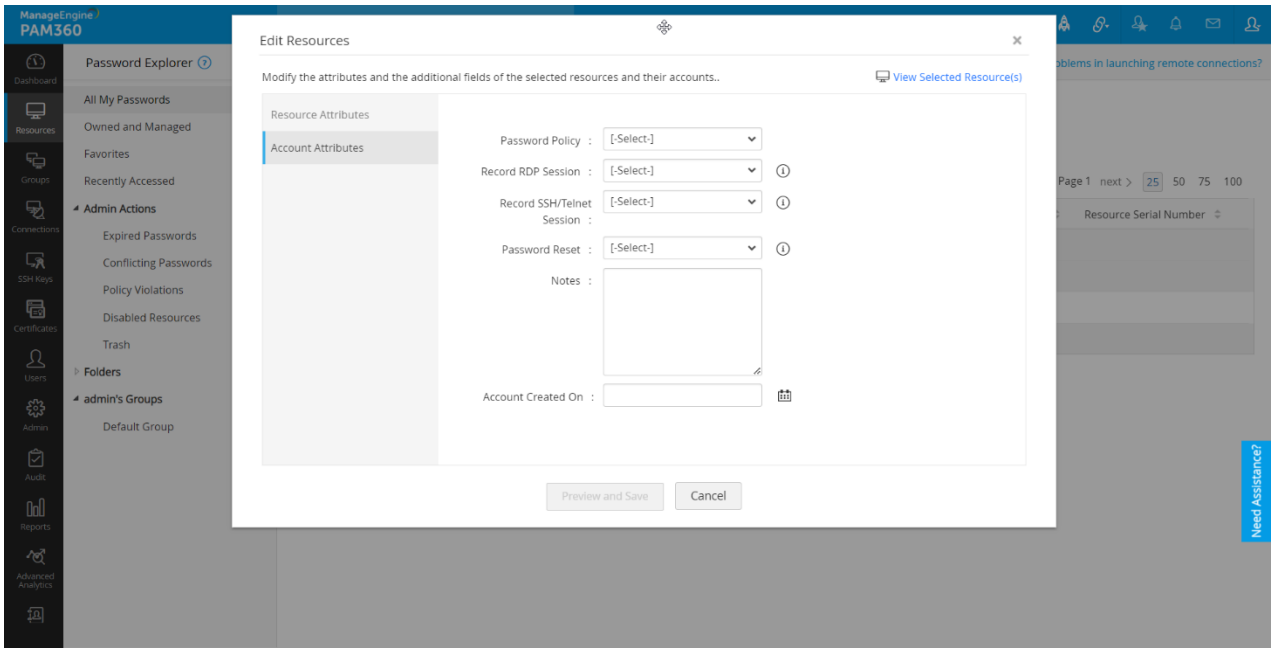
3. To edit resources in bulk, select the required resources, click **Resource Actions >> Manage >> Edit** at the top. This will open the **Edit Resources** window. Here you can modify the attributes and the additional fields of the selected resources and their accounts.



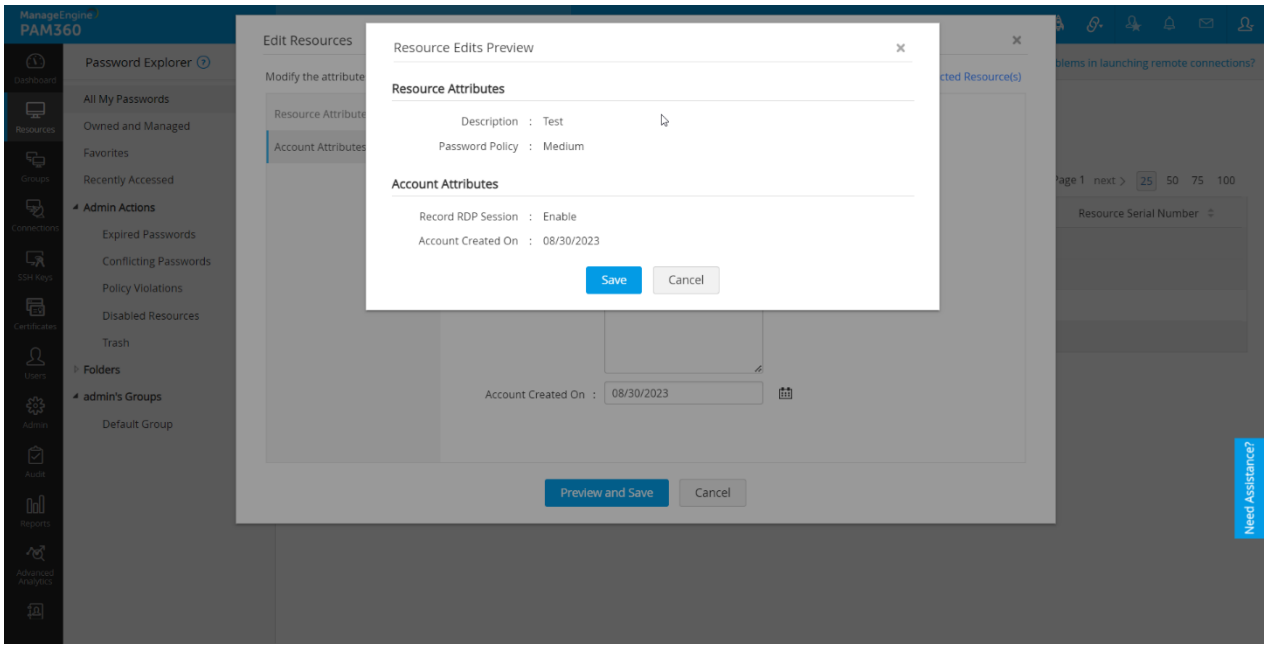
4. From the **Resource Attributes** tab, you can edit the following attributes: **Resource URL, Description, Password Policy, Domain Name, Department, Location,** and **Resource Type**.



5. From the **Account Attributes** tab, you can edit the following attributes: **Password Policy, Record RDP Session, Record SSH/Telnet Session, Password Reset,** and **Notes**.



6. If you have already configured additional fields, they will appear under the default attributes on both **Resource Attributes** and **Account Attributes** windows. To learn how to create additional fields, refer to the **Additional Fields** section.
7. After editing the attributes, click **Preview and Save**.
8. In the **Resource Edits Preview** window that appears, review the edits you have made and click Save.



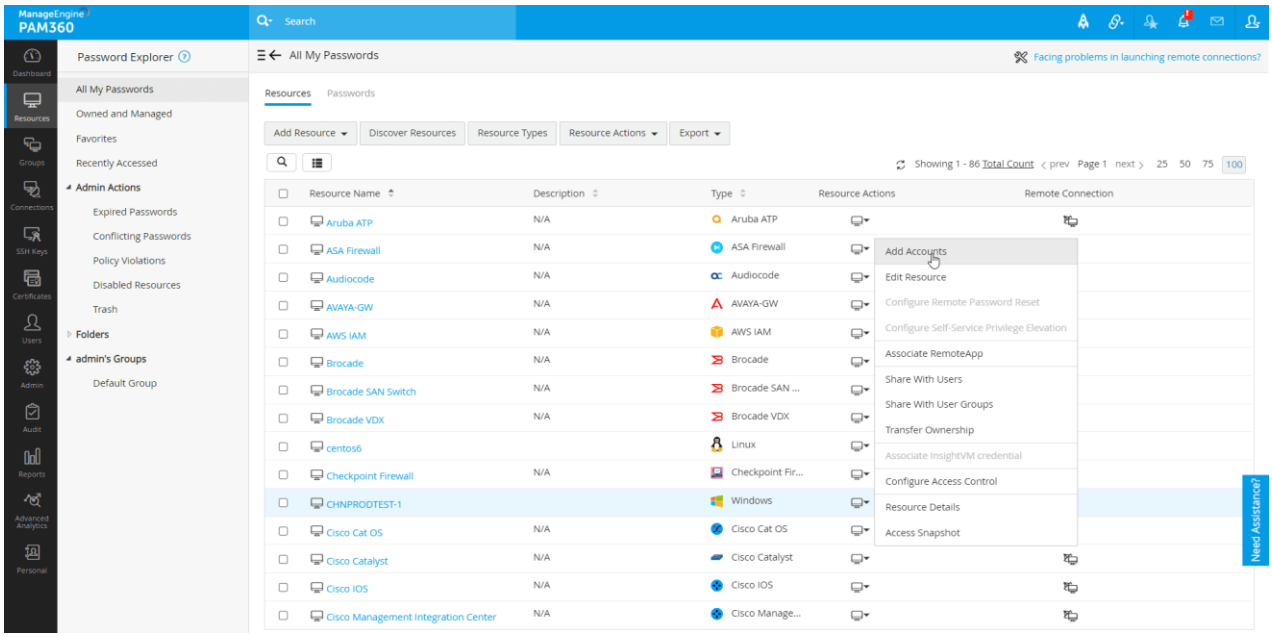
The changes you made will be applied to the selected resources with respect to the resource types. For example, if the selected resources include both Windows and Linux resource types and both RDP session recording and SSH/Telnet session recording are enabled in the **Account**

Attributes tab, you can take RDP session recording only for the Windows resources and SSH/Telnet session recording only for the Linux resources. You can also review the changes made in bulk edit from the **Audit** tab.

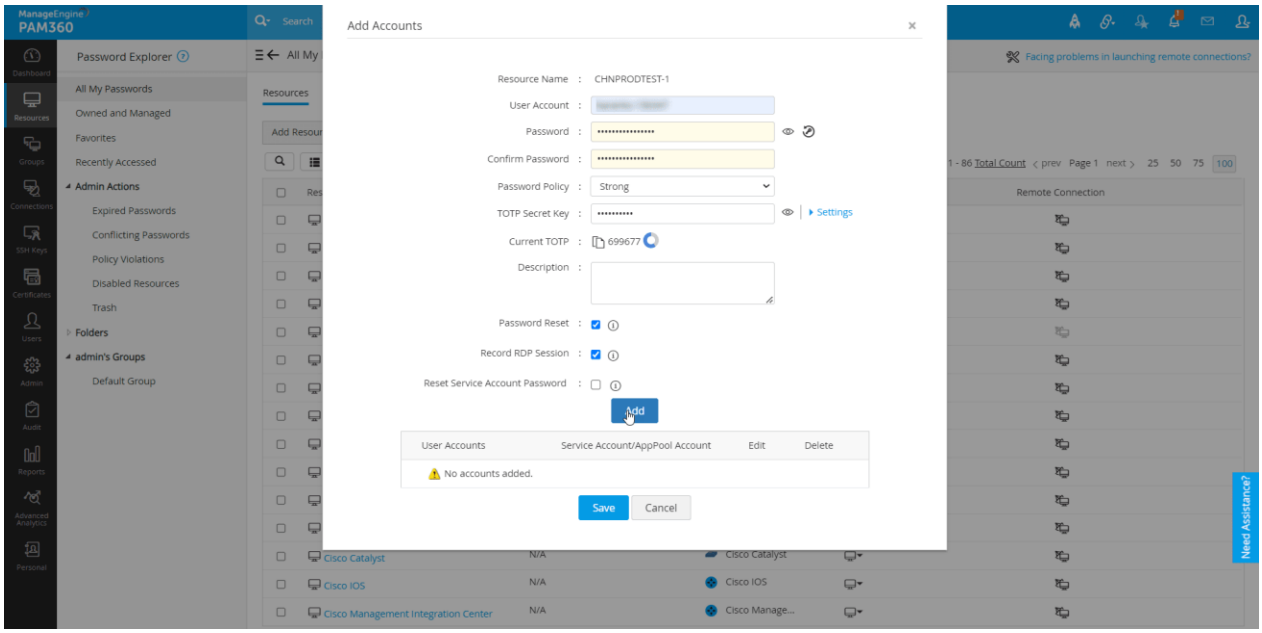
2. Adding Accounts to an Existing Resource

You can add any number of user accounts to an already existing resource. To add an account,

1. Navigate to the **Resources** tab.
2. Click the **Resource Actions** icon against the resource you wish to add an account and select **Add Accounts** from the drop-down list.



3. In the pop-up form that appears, enter the details about the account to be added.
4. Click **Add**. If you want to add more accounts, add them too by repeating the steps given here.
5. Click **Save**.

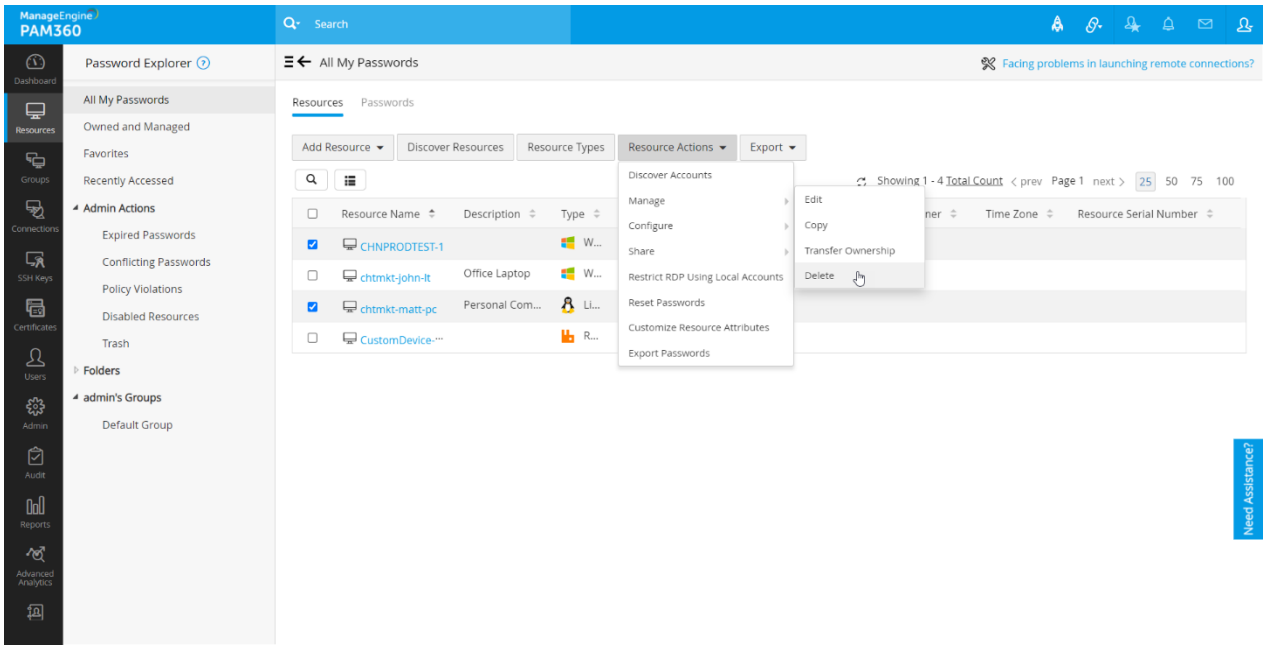


3. Deleting a Resource

You can delete those resources that are no longer required from the PAM360's Resources list. If you delete a resource, all the accounts and passwords that were part of that resource would also be deleted permanently. Alternatively, you can choose to move a resource to Trash from which it can be restored at a later point of time.

To delete a resource:

1. Navigate to **Resources** tab.
2. Select the particular resource that is to be deleted.
3. Click **Resource Actions** and select **Delete Resources** from the drop down.
4. To delete resources in bulk, select the required resources and click to **Resource Actions >> Manage >> Delete** at the top.



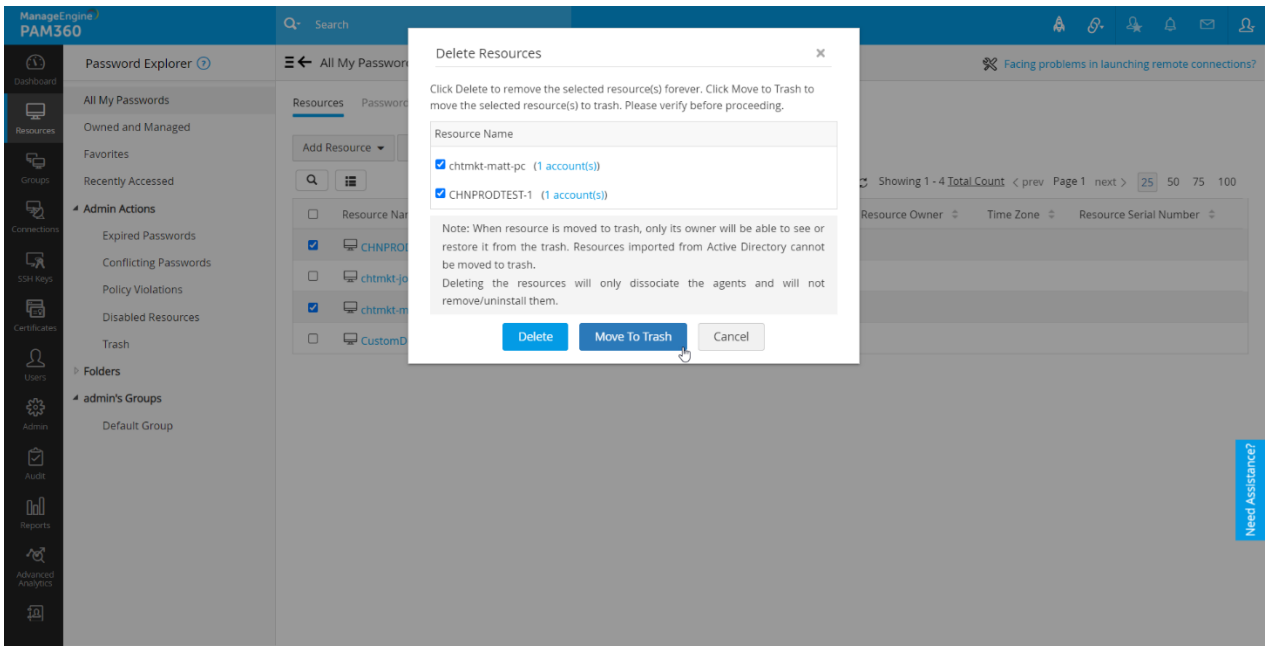
5. In the pop-up window that opens, you will have two options:

   i. **Delete:**

      ➢ To delete intended resources permanently, select the resource name and click **Delete.**

   ii. **Move To Trash:**

      ➢ This option can be used to move the resources to **Trash** without deleting them permanently.



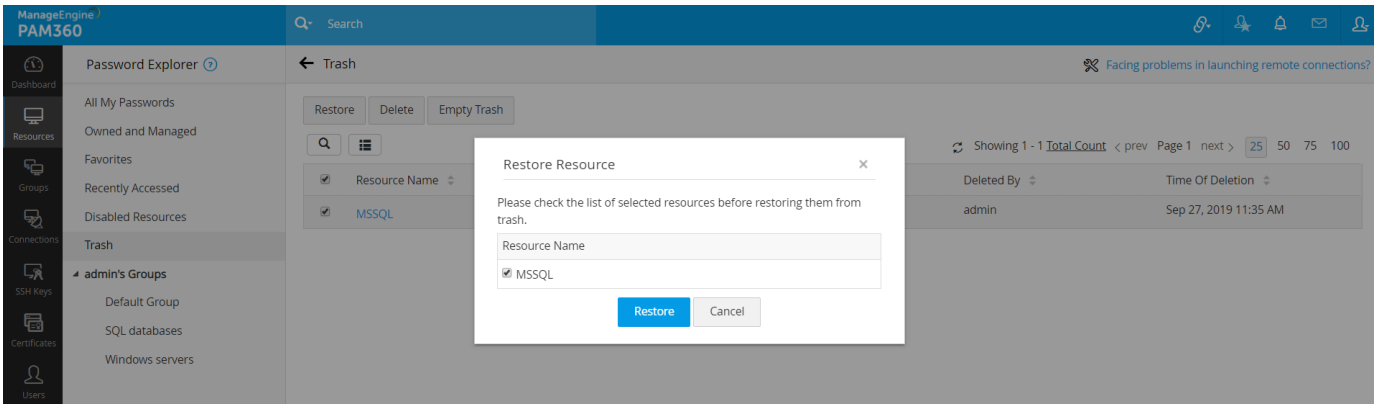
6. When a resource is moved to trash, only the resource owner will be able to view it under the **Trash** tab.

7. Resources moved to the **Trash** will not be removed from PAM360 and can be restored at any time until the PAM360 encryption keys have been rotated.
8. However, once the key rotation is done, the resources in Trash and all their associated privileged accounts will be removed from PAM360.

> **Note:** Resources imported from AD, Azure AD, and LDAP directories cannot be moved to **Trash**.

4. Restoring Resources from Trash

To restore a resource that has been moved to Trash, navigate to **Resources >> Trash** and click **Restore**. A list of resources in the **Trash** will open in a pop-up box from which the intended resource(s) can be restored.



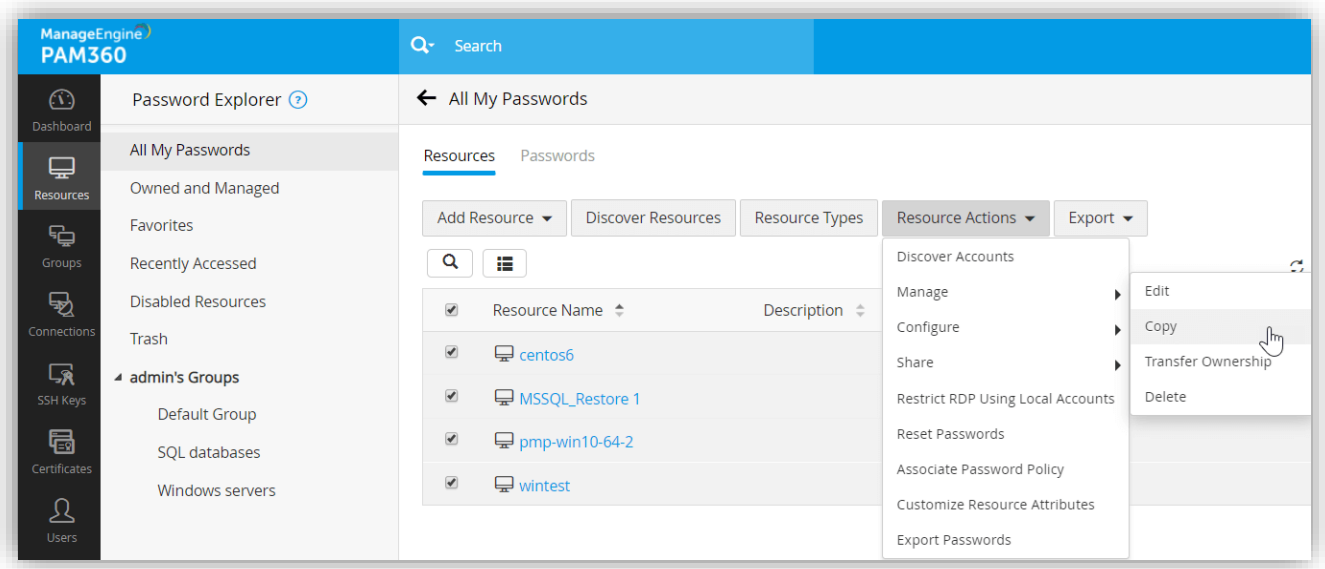
Copying Resources

If you have many resources with identical properties, you can add one resource and make multiple copies of the it in PAM360. This simplifies the bulk resource addition process.

You can copy a single resource or multiple resources and duplicate them as separate resources in PAM360. The attributes of the duplicated resources can be edited to suit your requirements.

Steps Required

1. Navigate to the **Resources** tab and select the specific resource(s) to be copied.
2. Go to **Resource Actions >> Manage >> Copy.**



3. In the pop-up that opens, you need to select the specific properties which you want the copied resources to inherit.

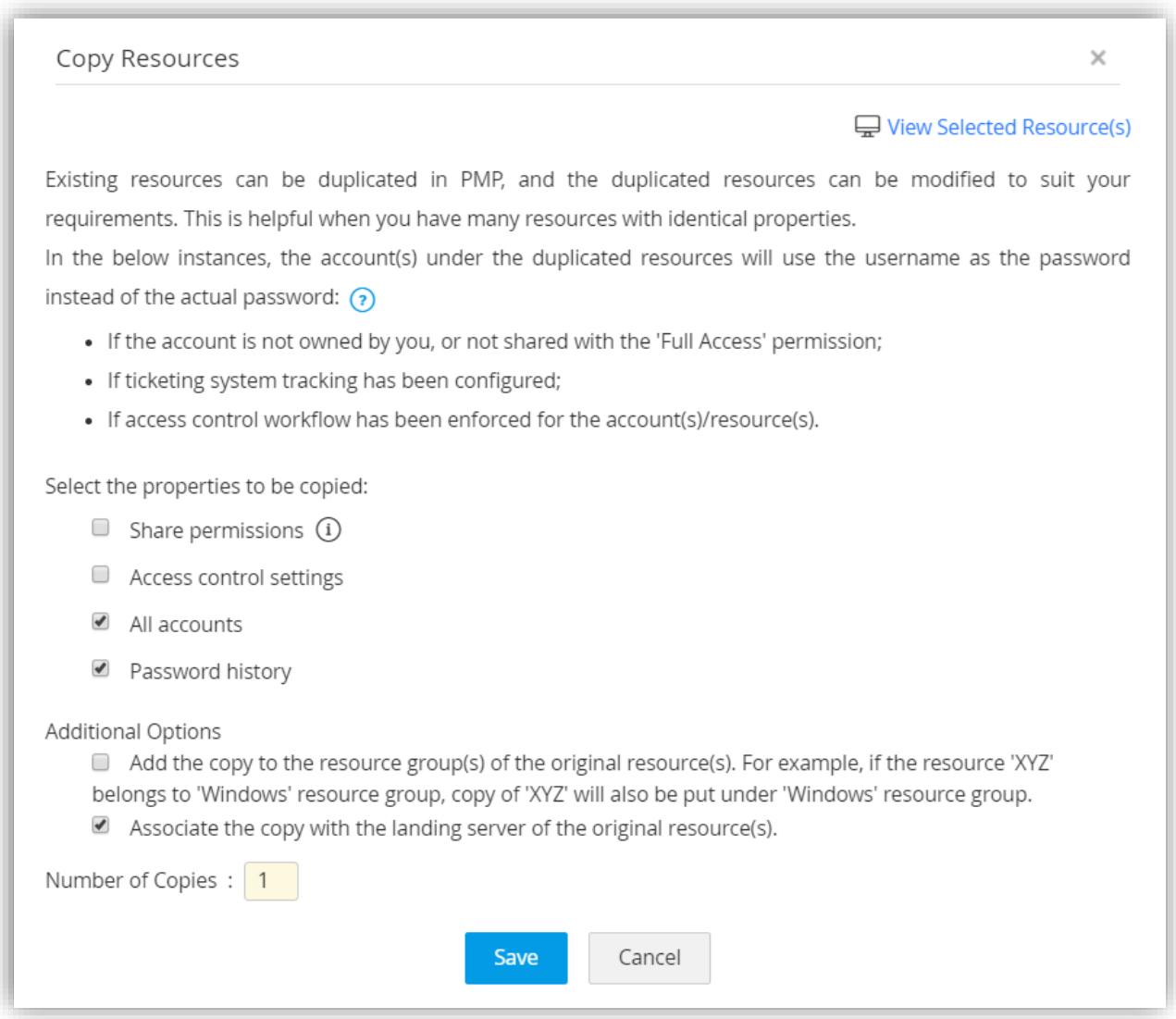
    i. **Select the properties to be copied:**

    - **Sharing permissions** - Resource(s) level and account(s) level sharing can be inherited. When you select this, all the sharing permissions of the original resource will be inherited by the copy or copies.
    - **Access control settings** - If you select this option, the access control setting configured for the original resource, will be inherited by the copy or copies.
    - **All acounts** - This will copy all the accounts that are part of the resource(s) being copied.
    - **Password history** - Password history of account(s) that are part of the resource(s) being copied.

ii. **Additional Options:**

- You also have the option to add the resultant copy resource to all the resource group(s) to which the original resource(s) belong(s).
- You can also associate this copy automatically with the landing server of the original resource. This option is applicable only to the resources that can be connected over SSH/Telnet.
- Specify the **Number of Copies** you want.

iii. Click **Save**.



4. You will now see the required copy or copies in the **Resources** tab.

Note: The copying operation does not affect the original resource in any way.

Transferring Resource Ownership at Different Levels

You can transfer the resources that you own to other administrators. With a transfer, you will no longer have access to the transferred resource unless the new owner shares it with you again. However, the shares that you enabled earlier for other users will remain intact.

Note:

Transferring resource ownership to a new user in the PAM360 server will not provide access to the remote resources added via an agent by another administrator. The 'conf' file in the agent installation directory should be updated with the new user name (in the attribute 'UserName=admin') to manage those resources.

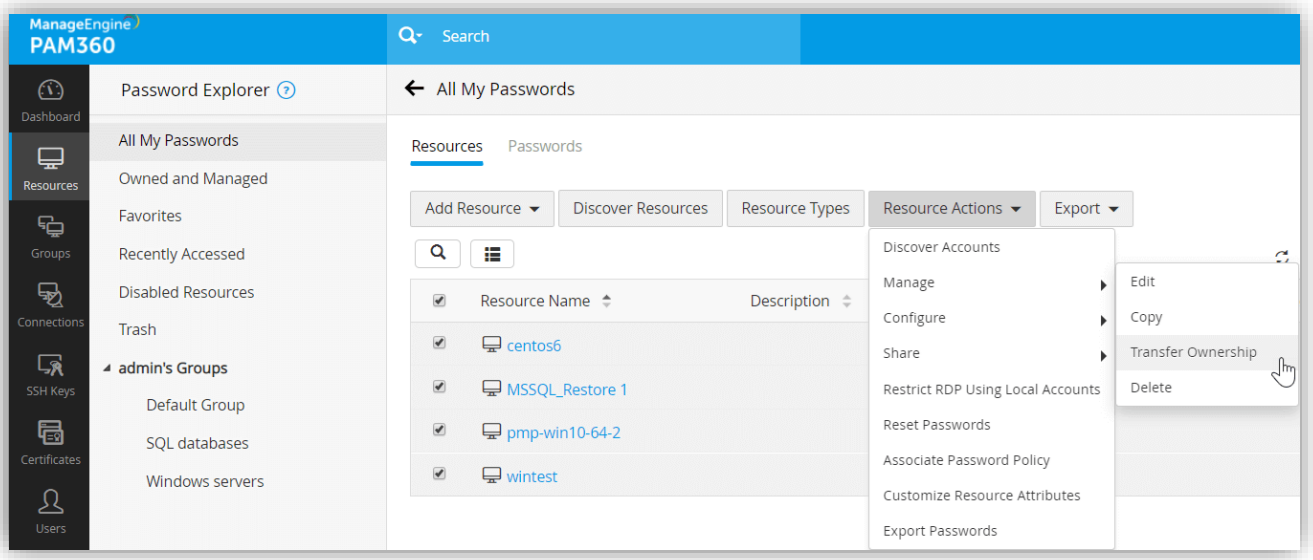
At the end of this section, you will have learned the following:

1. Transferring the Ownership of the Resource(s)
2. Transferring the Ownership of Resource Group(s)
3. Transferring the Ownership of Resource Group(s) in Bulk

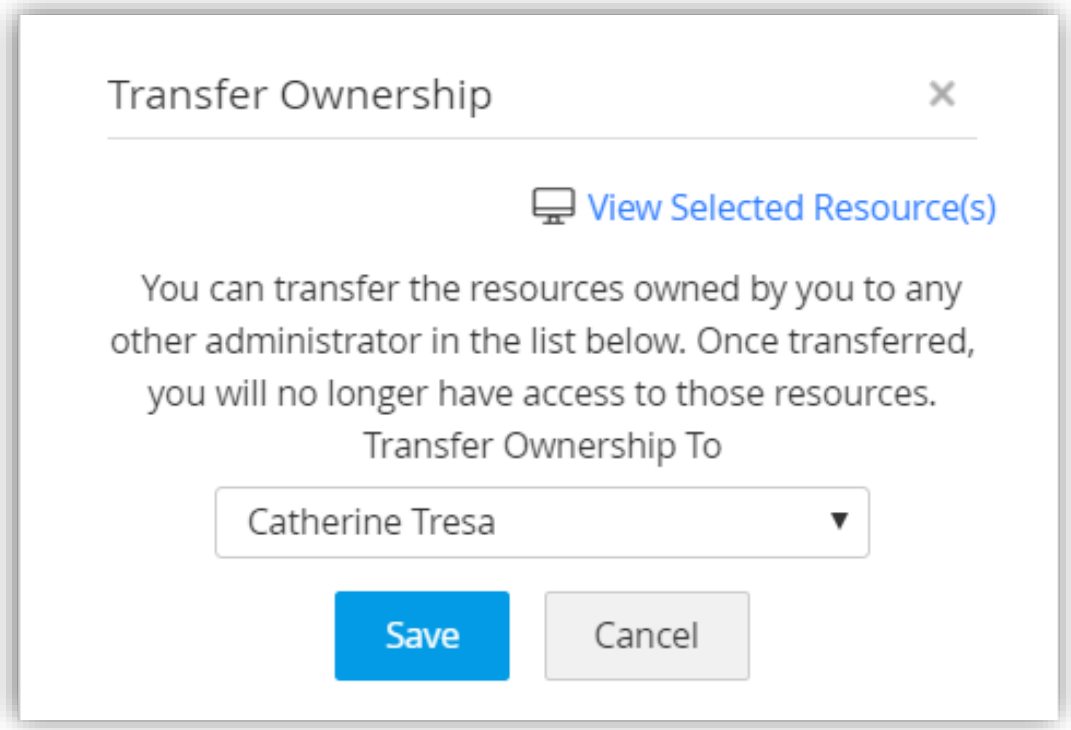
1. Transferring the Ownership of the Resource(s)

To transfer the ownership of a particular resource or a selective number of resources, do the steps that follow:

1. Navigate to ' **Resources >> Owned and Managed**'.
2. Click **Transfer Ownership** from the **Resource Actions** drop-down beside the particular resource to transfer ownership of a single resource to another admin.
3. Select the required resources and click '**Resource Actions >> Manage >> Transfer Ownership**' at the top of the resources list to transfer ownership of a set of resources in bulk to another admin.

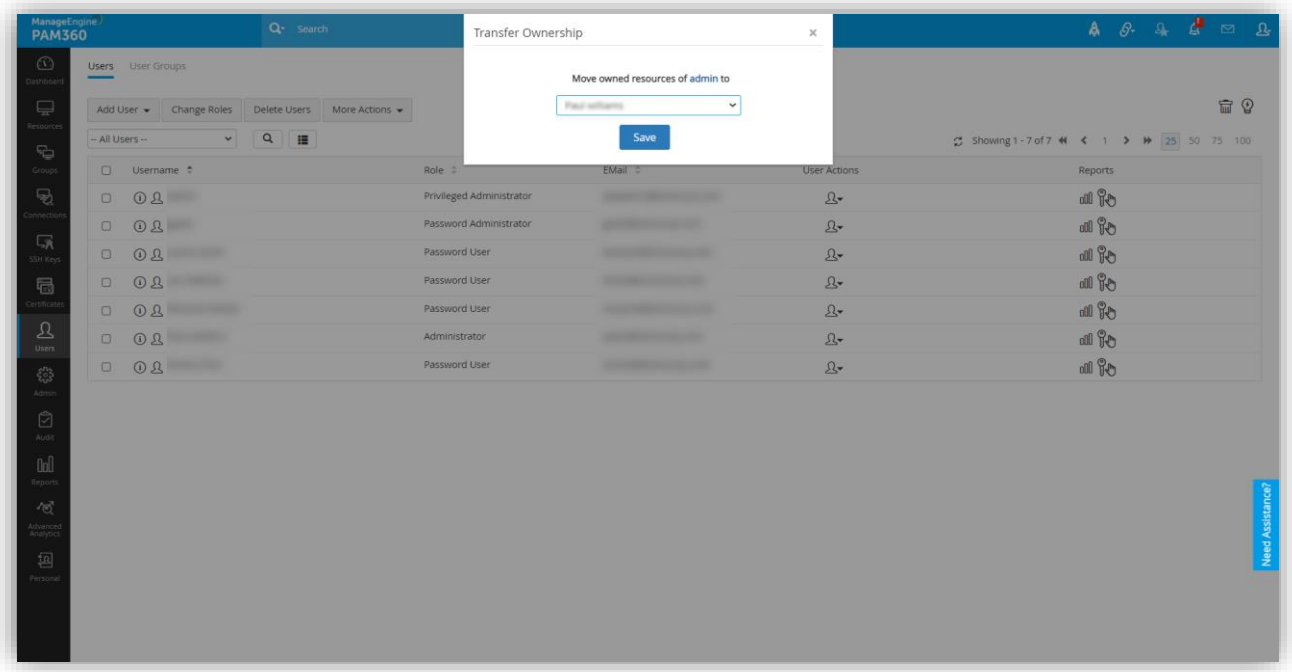


4. In the pop-up form that appears, select the user to whom the ownership has to be transferred and click **Save** to transfer the ownership.



To transfer the entire resources managed by you to a new admin, do the steps that follow:

1. Navigate to '**Users >> Users**'.
2. Select the **Transfer Ownership** option from the **User Actions** drop-down menu beside the user to whom you want to transfer the entire resource ownership.
3. Select the respective admin and click **Save** to transfer your entire resources ownership.



2. Transferring the Ownership of Resource Group(s)

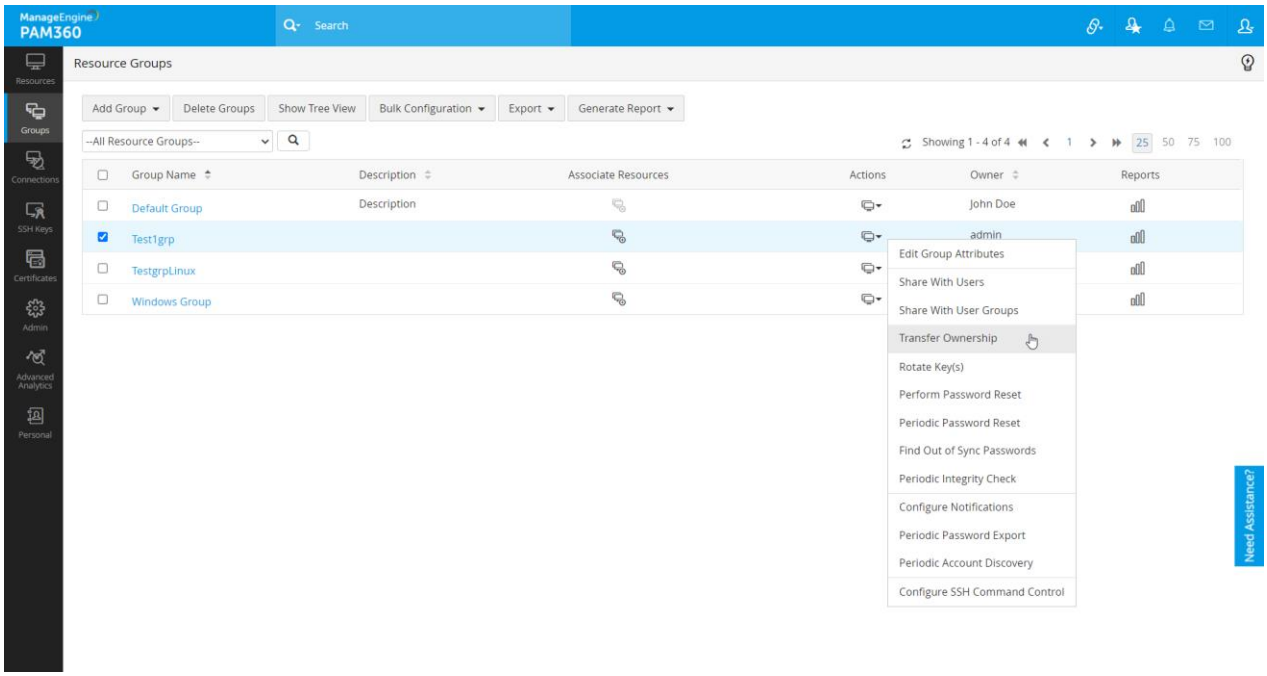
Prerequisites:

For transferring dynamic resource groups individually, you must enable Dynamic Group Share permission using the steps given below.

1. Navigate to **Users >> User Groups**.
2. Click the **User Group Actions** button beside the required user group and select **User Group Privileges**.
3. Now, select the checkbox **Permit group members to share the Dynamic Resource Groups owned by them with others granting 'Full Access' permission** from the list and click **Save**.

To transfer the ownership of a resource group, do the steps that follow:

1. Navigate to the **Groups** tab.
2. Click the **Actions** icon beside the particular resource group whose ownership you want to transfer to another admin and select **Transfer ownership** from the drop-down list.

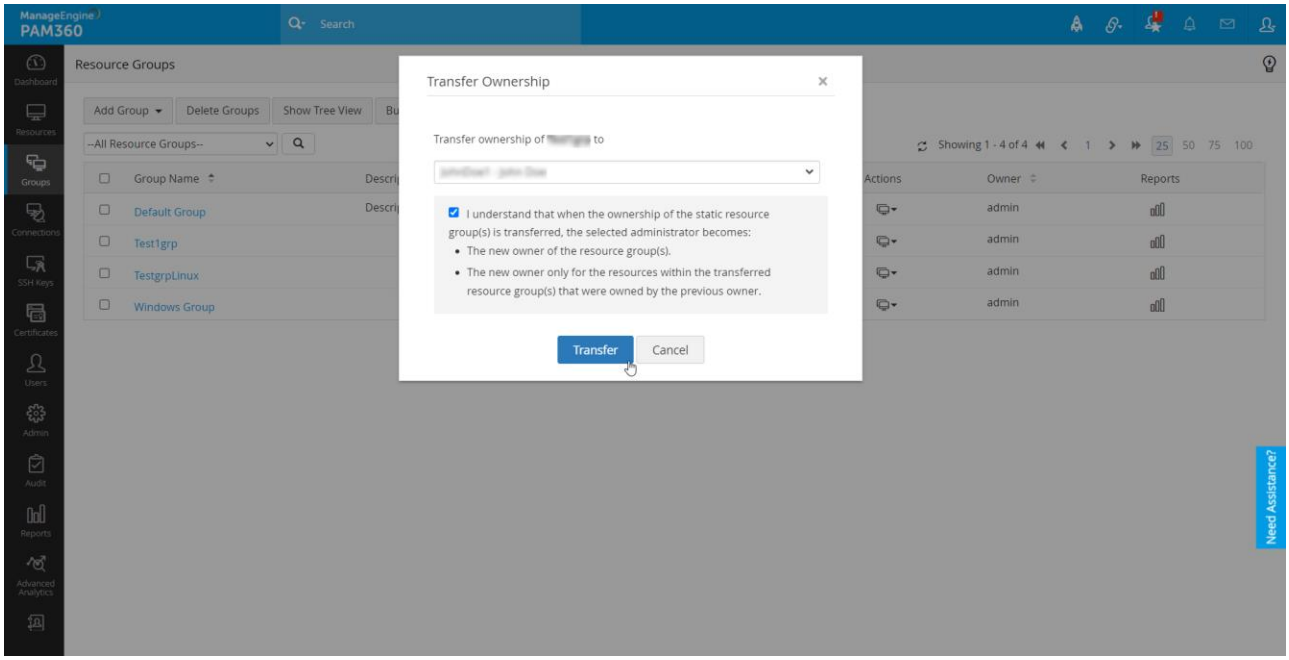


i. When you transfer a static resource group, the selected administrator becomes
   - The new owner of the resource group.
   - The new owner only for the resources within the transferred resource group that were owned by the previous owner.

ii. When you transfer a dynamic resource group,
   - The selected administrator becomes the new owner of the resource group, but not the resources within.
   - The previous owner gains Full Access to the resource group, but not the resources within.

3. In the pop-up form that appears, select the administrator to whom the ownership has to be transferred.

4. After selecting the new administrator, read and enable the consent checkbox , and click Transfer to transfer the ownership of the selected resource groups.



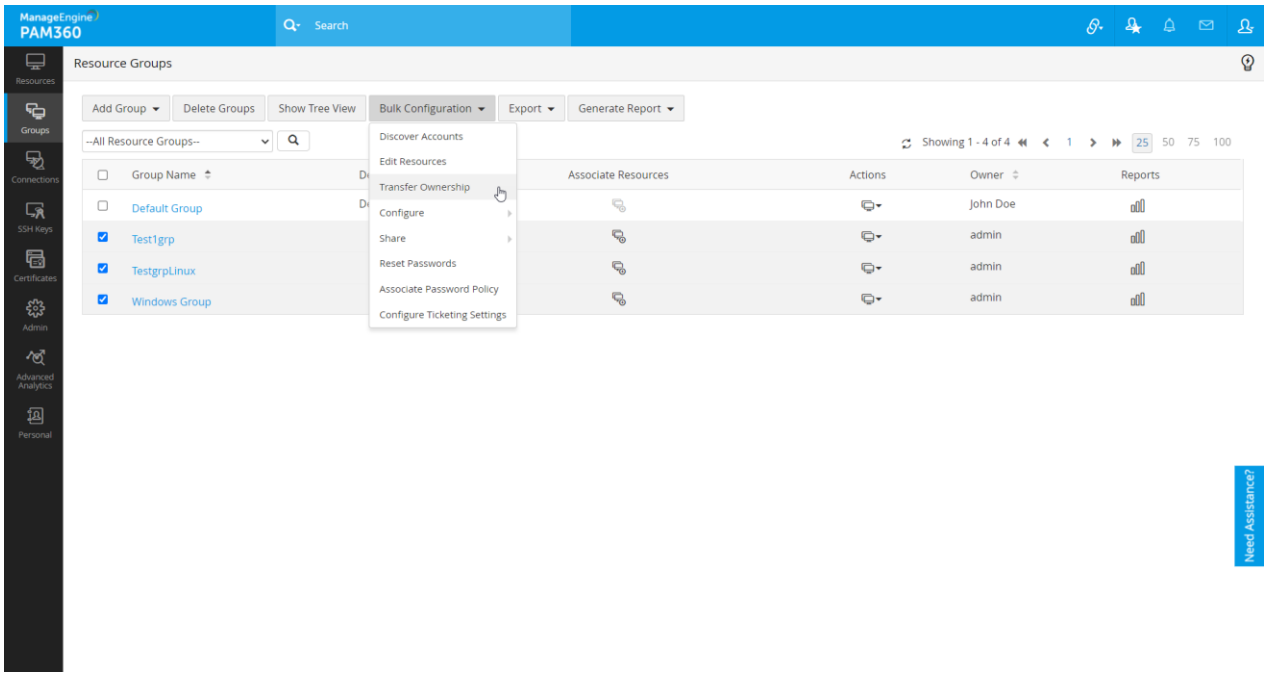
Notes:

1. The ownership of the default resource group cannot be transferred.
2. The ownership of resources within the dynamic resource groups can be transferred in bulk from the **Resources** tab.

3. Transferring the Ownership of Resource Group(s) in Bulk

To transfer the ownership of resource groups in bulk, do the steps that follow:

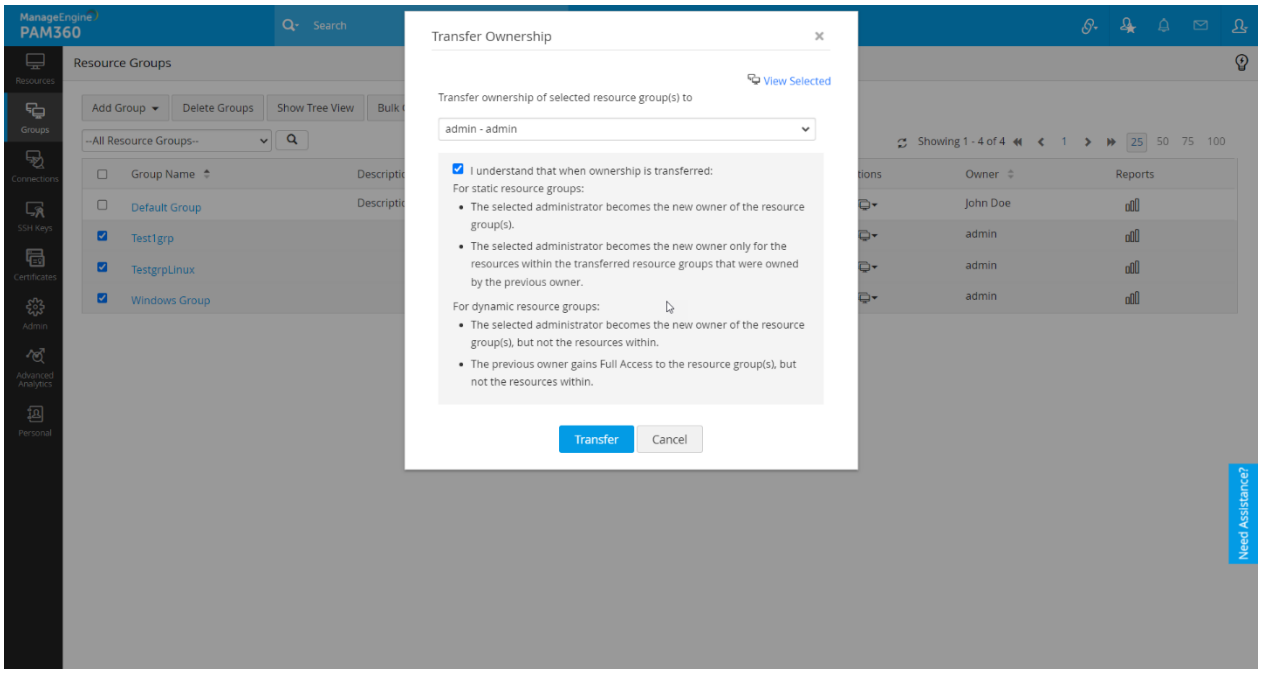
1. Navigate to the **Groups** tab and select the resource groups.
2. Click **Bulk Configuration >> Transfer Ownership**.



3. To view the selected resource groups, click on **View Selected** at the top-right corner of the dialog box.

> **Note:** You should log in as a super administrator to avail the option to transfer ownership of resource groups in bulk. Click here to learn how to promote an administrator to a super administrator.

4. Select the administrator to whom you want to transfer ownership from the drop-down menu.
5. Read and enable the consent checkbox. click **Transfer** to transfer the ownership of the selected resource groups.


ManageEngine
PAM360
Search
Resource Groups
Add Group
Delete Groups
Show Tree View
--All Resource Groups--
Group Name
Default Group
Test1grp
TestgrpLinux
Windows Group
Owner
John Doe
admin
admin
admin
Reports
Showing 1 - 4 of 4
25 50 75 100
Transfer Ownership
View Selected
Transfer ownership of selected resource group(s) to
admin - admin
I understand that when ownership is transferred:
For static resource groups:
The selected administrator becomes the new owner of the resource group(s).
The selected administrator becomes the new owner only for the resources within the transferred resource groups that were owned by the previous owner.
For dynamic resource groups:
The selected administrator becomes the new owner of the resource group(s), but not the resources within.
The previous owner gains Full Access to the resource group(s), but not the resources within.
Transfer
Cancel
Need Assistance?

Sharing Individual Resources

PAM360 allows you to share your individual resources/resource groups with other users and user groups. When you share a resource, all the passwords of that particular resource will also be shared. You can grant varying permissions to users and user groups for password usage by choosing one of the following levels.

Share Permission Levels

Remote App Only	View Passwords	Modify Passwords	Full Access
Users and User groups can access and use the Remote Apps associated with the resources.	Users and User groups can access and use the passwords of the shared resources/ resource groups.	Users and User groups can both access and modify the passwords of the shared resources/resource groups. However, this privilege does not allow the users/user groups to change any other attribute of the resource.	Users and User groups can have the complete management of the shared resources/resource groups. They can even re-share the resources and the related account passwords with other users. **Note**: The Default Group cannot be granted with **Full Access** permission.

How Precedence Works for Permission Levels?

For password sharing permissions (**View/Modify/Full Access**), the lowest level of permission takes the highest precedence as explained below:

1. Permissions set for individual accounts override the permissions set for a resource which the account is a part of.
    - For example, if a user account is granted with **View** permission for a password and the resource it is a part of gets **Modify** permission, this particular user account will still have only **View** permission to that password.
2. Permissions set for a resource overrides the permissions set for a resource group which the resource is a part of.
    - For example, if a resource is granted with **Modify** permission for a password and the resource group it is a part of gets **Full Access**, then this particular resource will still have only **Modify** access to that password.

3. Similarly, the share permission set for a user overrides that of a user group the user is a part of.
    - For example, if a particular user is granted with **View** only permission for a password and the user group it is a part of gets **Full Access**, then this particular user will still have only **View** access to that password.

Types of Sharing

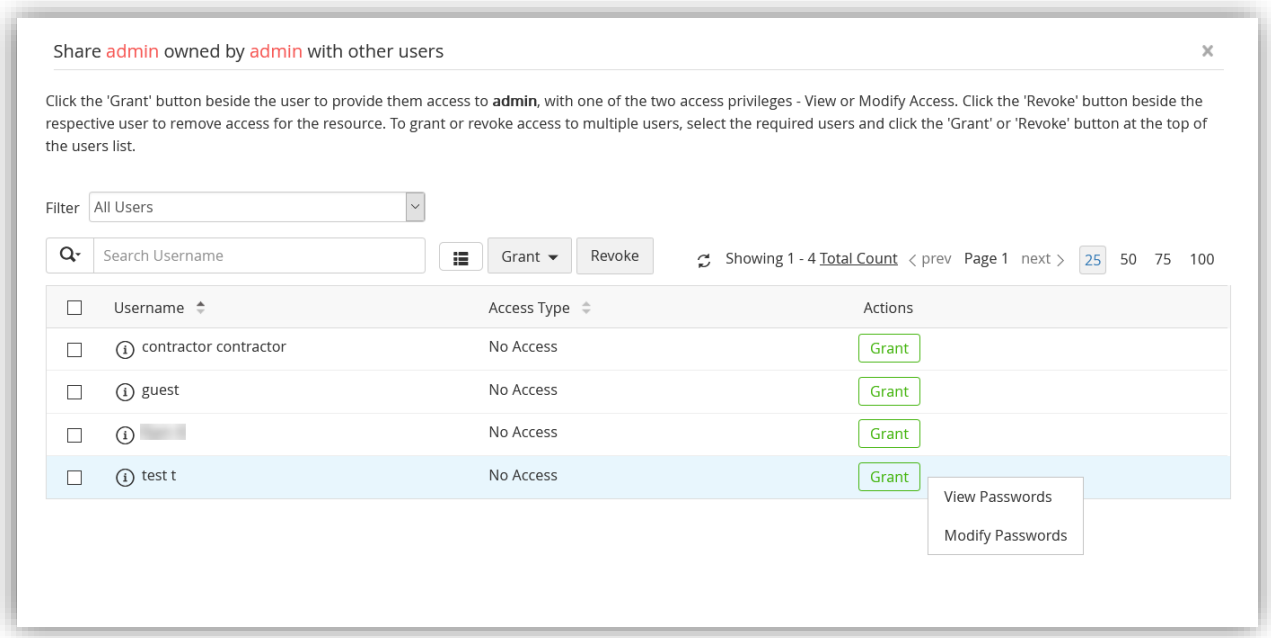
1. **Sharing Individual Accounts with Users/User Groups**
    1.1 **Sharing Individual Accounts of a Particular Resource with Users/User Groups**
2. **Sharing Resources with Users/User Groups**
3. **Sharing Resource Groups with User/User Groups**

1. Sharing Individual Accounts with Users/User Groups

Follow the below steps to share a particular account with user(s) or user group(s), with **View** or **Modify** permissions.

> **Note:** Only two permission levels will be available while sharing individual accounts, as the **Full Access** permission is meant only for resources and resource groups

1. Navigate to **Resources >> Passwords.**
2. Select the particular account of the resource that you want to share and click **Account Actions** beside it.
3. From the **Account Actions** drop down, click either **Share With Users** or **Share With User Groups** depending on whether you want to share the account with users or user groups.
4. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the account is to be shared. Choose either **View Passwords** or **Modify Passwords** as the permission level and click **Save**.

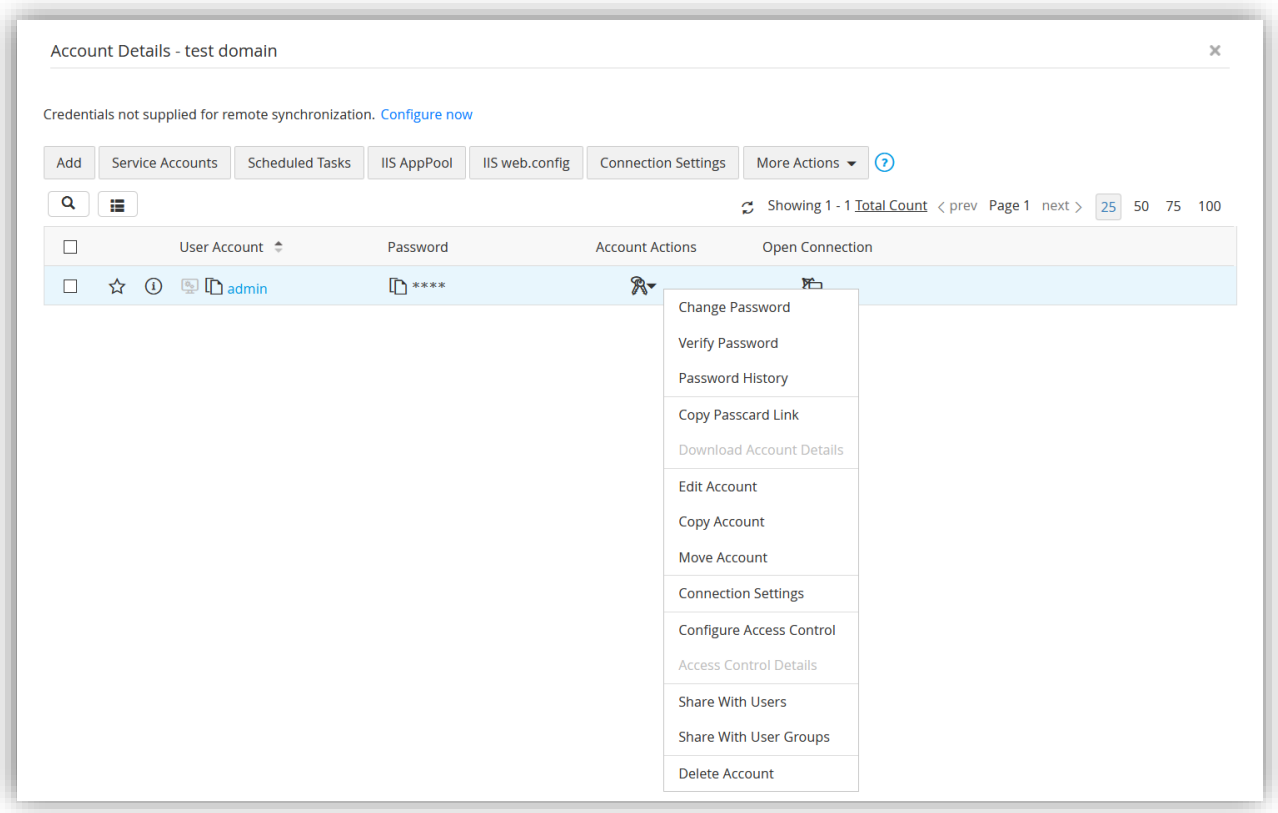


Now, you have successfully shared the account with the required user(s) or user group(s).

1.1 Sharing Individual Accounts of a Particular Resource with Users/User groups

Follow the below steps to share accounts of a particular resource with user(s) or user group(s), with **View** or **Modify** permissions.

1. Navigate to the **Resources** tab.
2. Click on the particular resource whose accounts you want to share.
3. Under **Account Details**, click the **Account Actions** icon beside a particular account.
4. Click **Share with Users** or **Share with User Groups.**



5. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the account is to be shared. Choose either **View Passwords** or **Modify Passwords** as the permission level.
6. Click **RemoteApp Only** to share the associated remote app to a particular user. To know more about configuring remote app, click here.
7. Click **Save.**

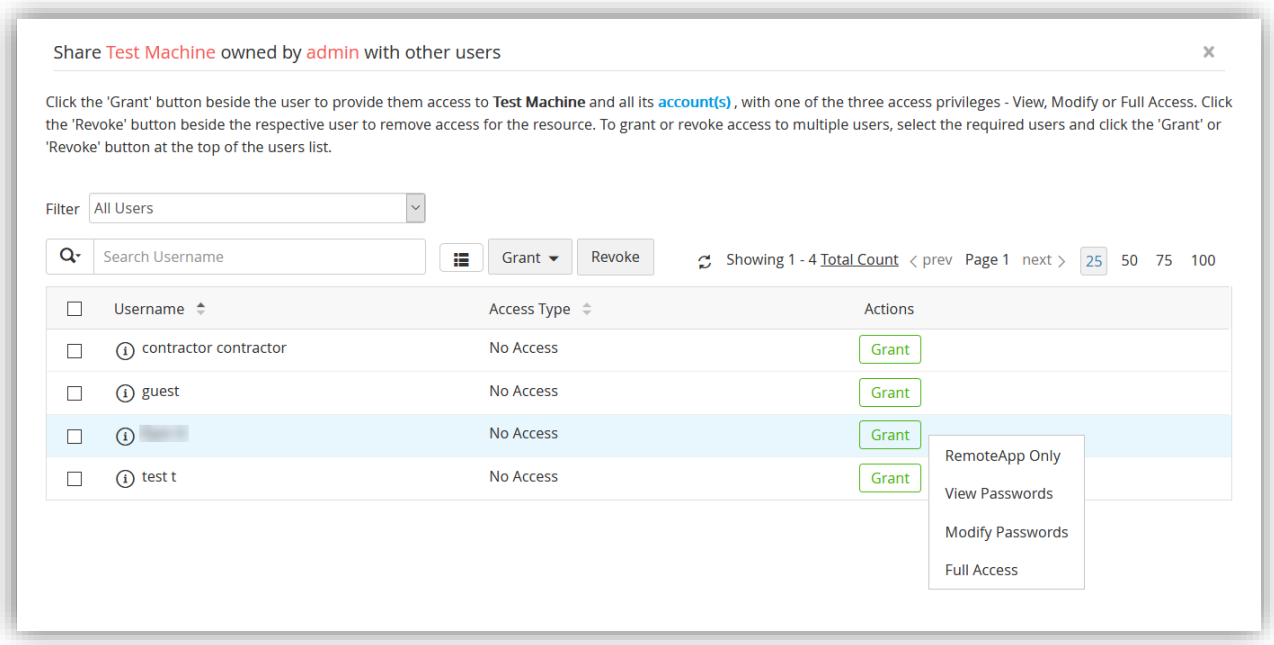
> **Note:** PAM360 supports RemoteApp only for Windows and Windows Domain resources. Only Connection Users and Users with Remote app permission will be able to access Remote apps. To know more about user roles and permissions, click here.

2. Sharing Resources with Users/User groups

Follow the below steps to share a resource with user(s) or user group(s) with any of the three permission levels - **View**, **Modify**, or **Full Access**.

1. Navigate to the **Resources** tab.
2. Select the particular resource to be shared and click **Resource Actions** beside it.
3. From the **Resource Actions** drop down, click either **Share With Users** or **Share With User Groups** depending on whether you want to share the account with users or user groups.

4. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the account is to be shared. Choose from the permission levels: **View Passwords**, **Modify Passwords**, or **Full Access**,
5. Click **RemoteApp Only** to share the associated remote app to a particular user. To know more about configuring remote app, refer to the **Working with Remote Apps** help section.
6. Click **Save**.



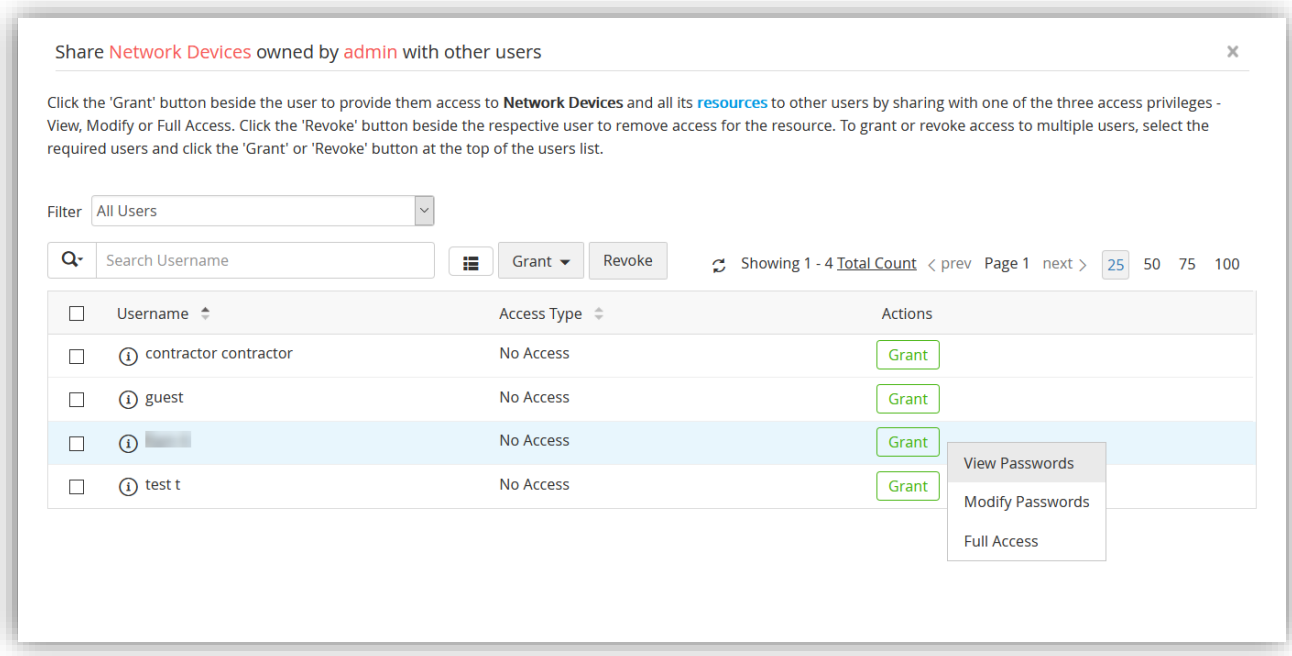
Now, you have successfully shared the resources to the required user(s) or user group(s).

3. Sharing Resource Groups with Users/User Groups

Follow the below steps to share a resource group with user(s) or user group(s), with any of the three permission levels - **View, Modify,** or **Full Access.**

1. Navigate to the **Groups** tab.
2. Select the particular resource group to be shared and click the **Actions** drop down beside it.
3. From the **Actions** drop down, click either **Share With Users** or **Share With User Groups** depending on whether you want to share the account with users or user groups.
4. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the account is to be shared. Choose from the permission levels: **View Passwords, Modify Passwords,** or **Full Access**, and click **Save**.

Now, you have successfully shared a resource group with the necessary user(s) or user group(s).



Note: When you share a particular resource group with a user group, the resource group will be visible to all members of that user group. That means, all the resources and the accounts that are part of that resource group will be visible to all members of the user group. Also, the permissions granted to the user group **(View, Modify or Full Access)** will be applicable to all the members.

Sharing Resources in Bulk

PAM360 allows you to share your resources/resource groups in bulk with other users and user groups. When you share a selection of resources, all the passwords of all of the resources will also be shared. You can grant varying permissions to users and user groups for password usage by choosing one of the following levels.

Sharing Permissions Levels

View Passwords	Modify Passwords	Full Access
Users and User groups can access and use the passwords of the shared resources/ resource groups.	Users and User groups can both access and modify the passwords of the shared resources/resource groups. However, this privilege does not allow the users/user groups to change any other attribute of the resource.	Users and User groups can have the complete management of the shared resources/resource groups. They can even re-share the resources and the related account passwords with other users. Note: The Default Group cannot be granted with Full Access permission.

How Precedence Works for Permission Levels

For password sharing permissions (**View/Modify/Full Access**), the lowest level of permission takes the highest precedence as explained below:

1. Permissions set for individual accounts override the permissions set for a resource which the account is a part of.
    - **For example,** if a user account is granted with **View** permission for a password and the resource it is a part of gets **Modify** permission, this particular user account will still have only **View** permission to that password.
2. Permissions set for a resource overrides the permissions set for a resource group which the resource is a part of.
    - **For example,** if a resource is granted with **Modify** permission for a password and the resource group it is a part of gets **Full Access**, then this particular resource will still have only **Modify** access to that password.
3. Similarly, the share permission set for a user overrides that of a user group the user is a part of.
    - **For example,** if a particular user is granted with **View** only permission for a password and the user group it is a part of gets **Full Access**, then this particular user will still have only **View** access to that password

Types of Sharing

1. Sharing Accounts in Bulk with Users/User Groups

   1.1 Sharing Accounts of a Particular Resource in Bulk with Users/User Groups

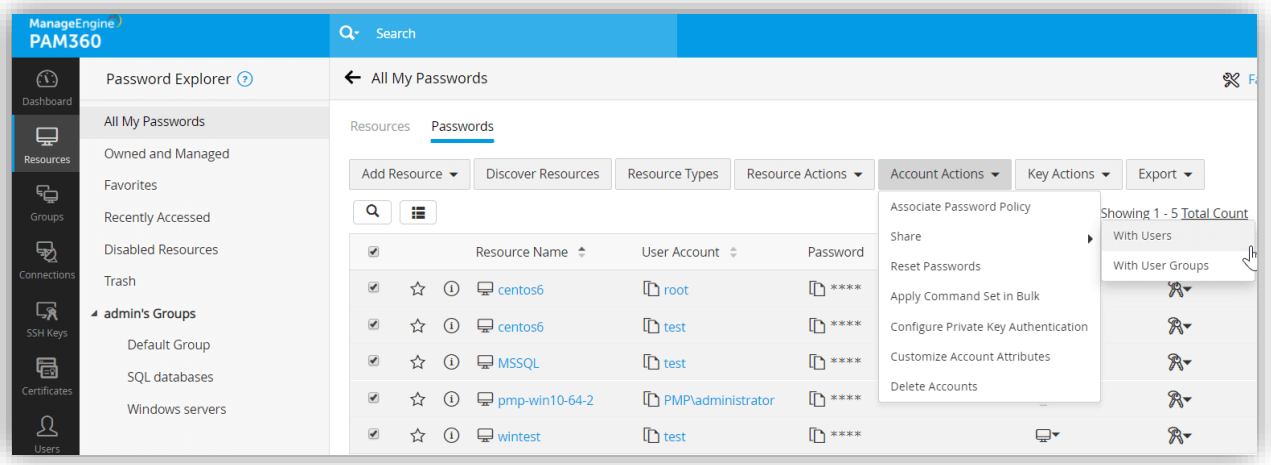
2. Sharing Resources in Bulk with Users/User Groups
3. Sharing Resource Groups in Bulk with User/User Groups

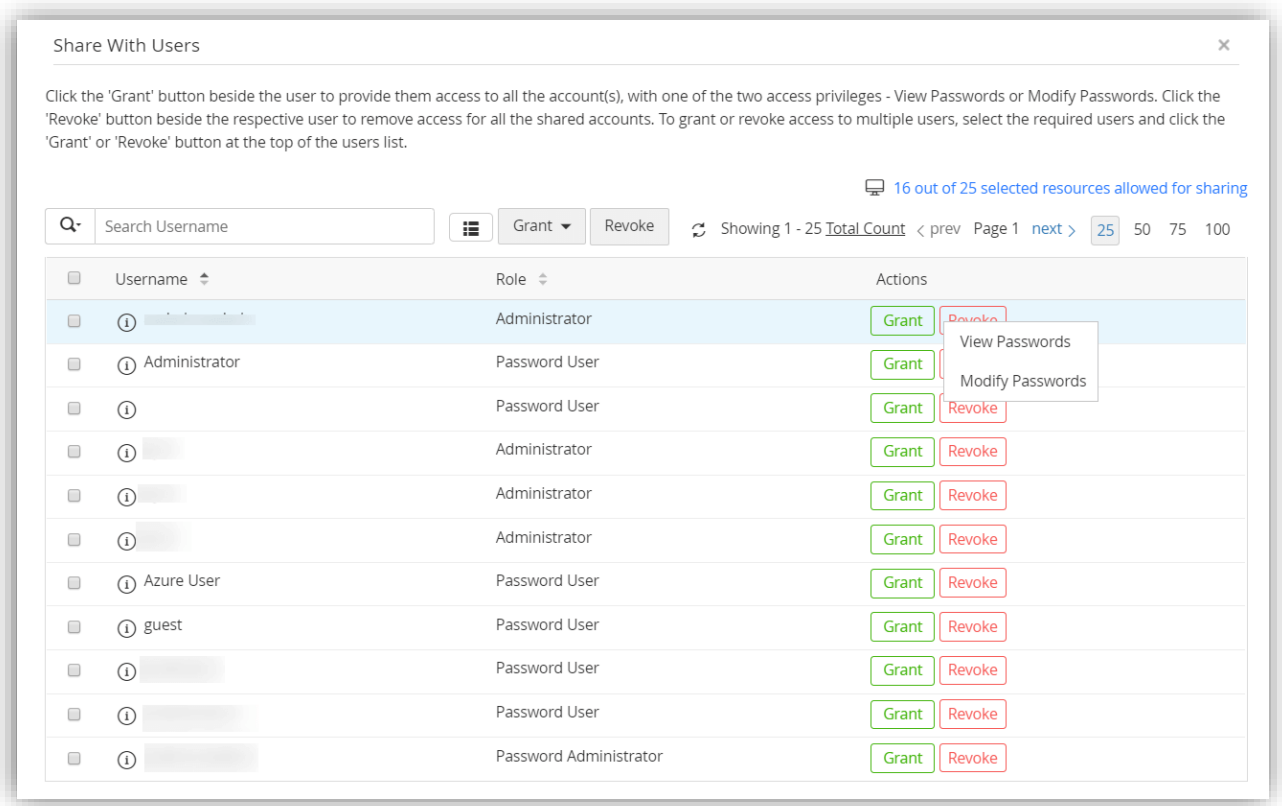
1. Sharing Accounts in Bulk with Users/User Groups

Follow the below steps to share a set of accounts in bulk with user(s) or user group(s), with **View** or **Modify** permissions.

> **Note:** Only two permission levels will be available while sharing accounts, as the **Full Access** permission is meant only for resources and resource groups.

1. Navigate to **Resources >> Passwords** and select the accounts that you want to share.
2. Click the **Account Actions** drop down at the top and go to **Share >> With Users** or **With User Groups** depending on whether you want to share the accounts with users or user groups.
3. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the account is to be shared. Choose either **View Passwords** or **Modify Passwords** as the permission level and click **Save**.

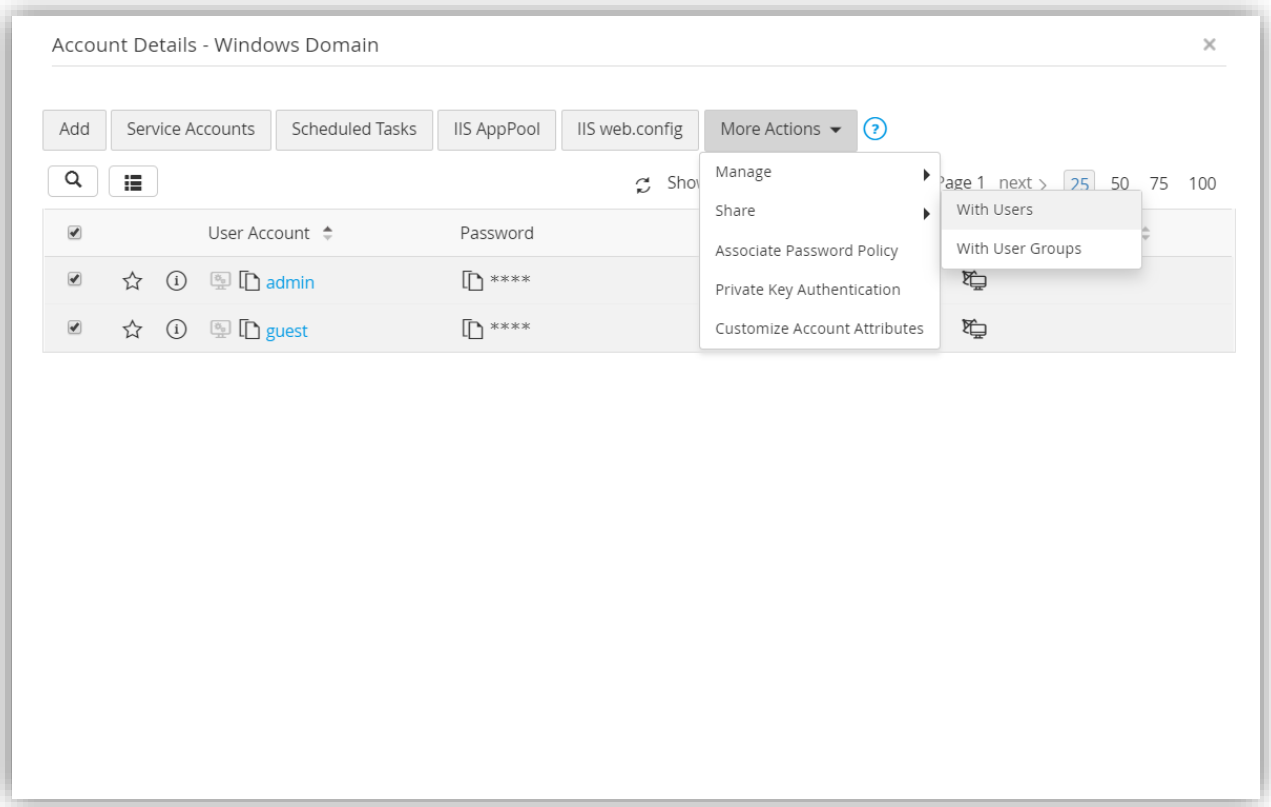


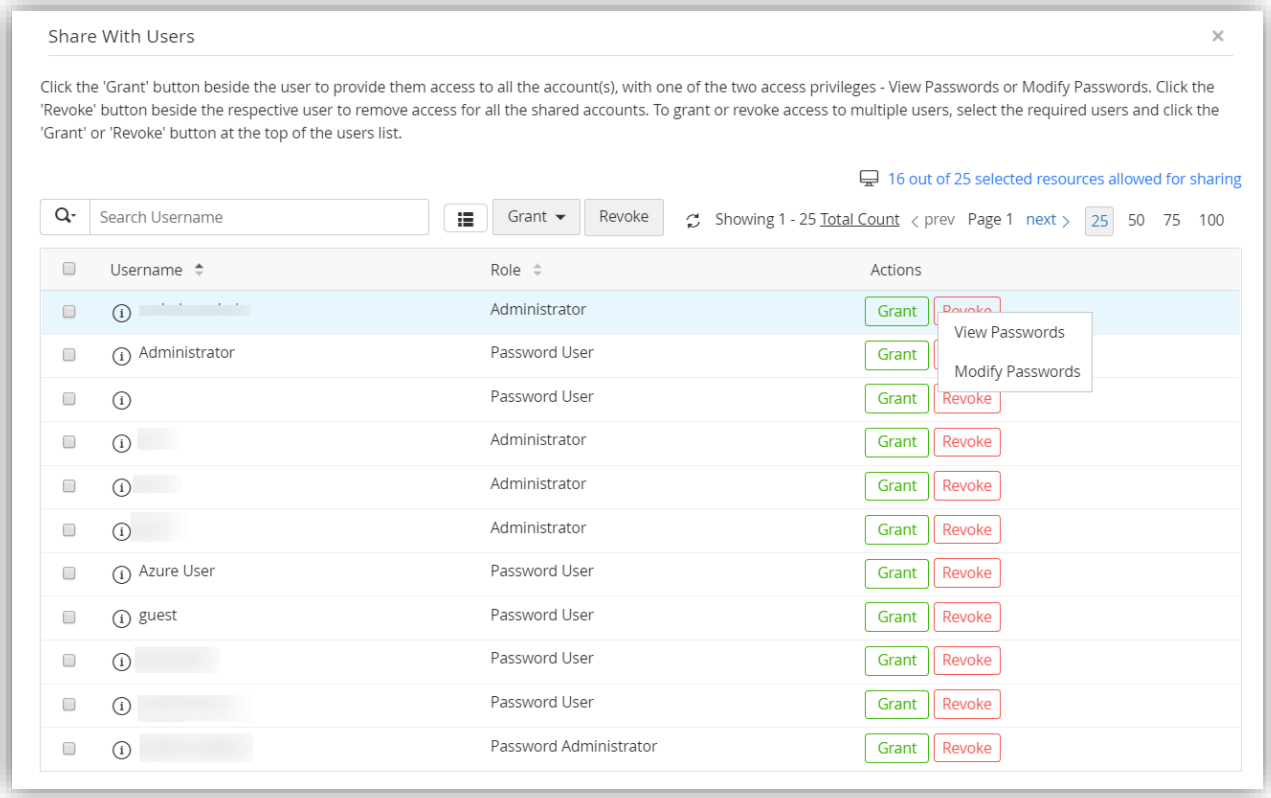


1.1 Sharing Accounts of a Particular Resource in Bulk with Users/User groups

Follow the below steps to share accounts of a particular resource in bulk with user(s) or user group(s), with **View** or **Modify** permissions.

1. Navigate to the **Resources** tab and click on the particular resource whose accounts you want to share in bulk.
2. Under **Account Details**, select the accounts to be shared and go to **More Actions >> Share >> With Users** or **With User Groups** depending on whether you want to share the accounts with users or user groups.



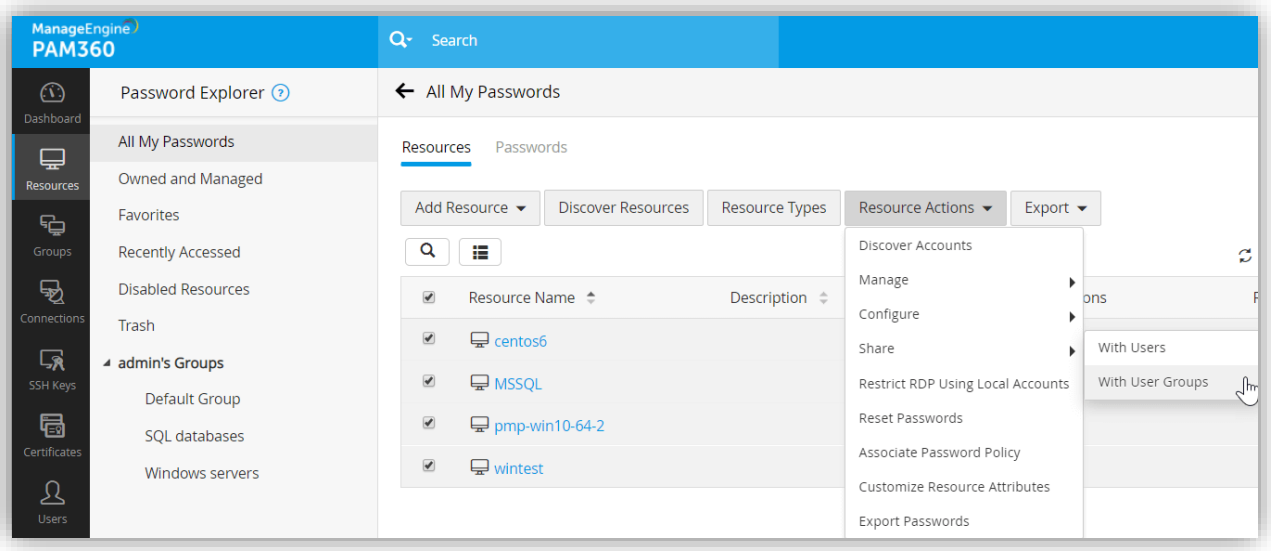


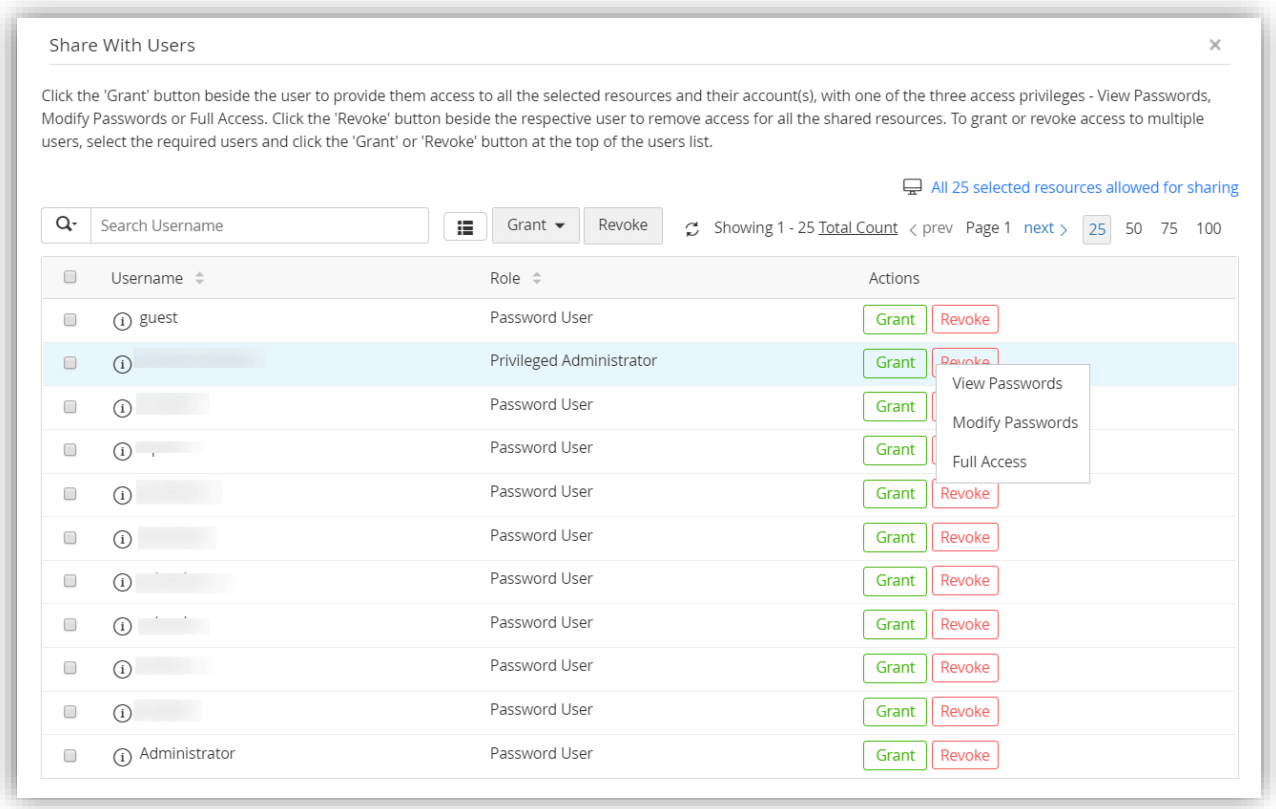
3. In the pop-up box that appears, click the **Grant** option against that user/user group with whom the selected accounts are to be shared. Choose either **View Passwords** or **Modify Passwords** as the permission level and click **Save**.

2. Sharing Resources in Bulk with Users/User groups

Follow the below steps to share a set of resources in bulk with user(s) or user group(s) with any of the three permission levels - **View**, **Modify**, or **Full Access**.

1. Navigate to the **Resources** tab and select the particular resources to be shared.
2. Click the **Resource Actions** drop down at the top and go to **Share >> With Users** or **With User Groups** depending on whether you want to share the resources with users or user groups.
3. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the resources are to be shared. Choose from the permission levels: **View Passwords**, **Modify Passwords**, or **Full Access**, and click **Save**.

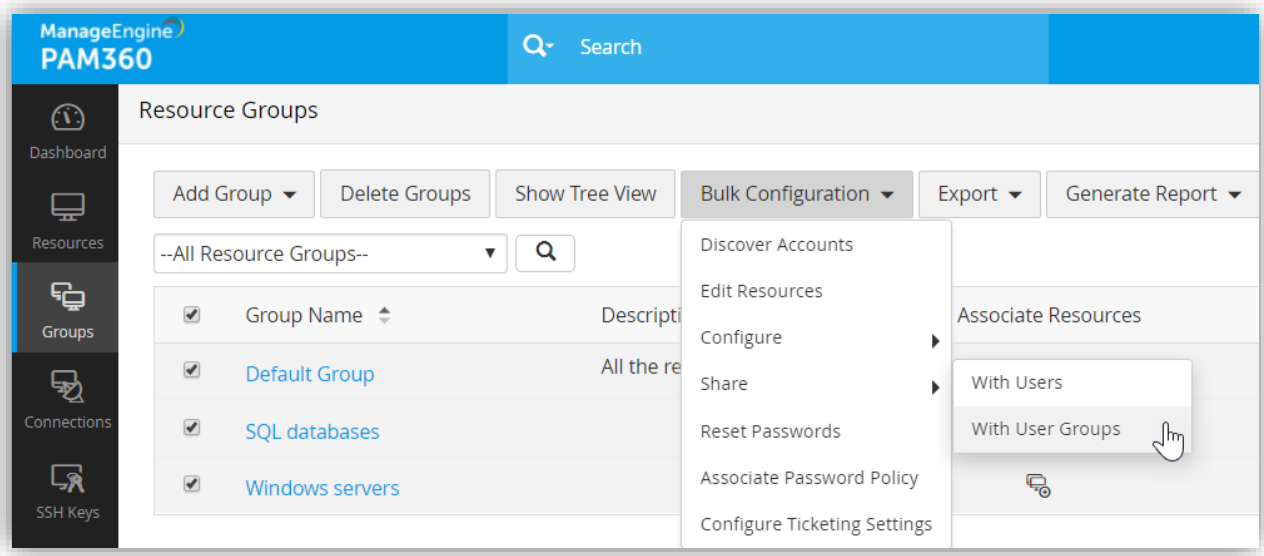


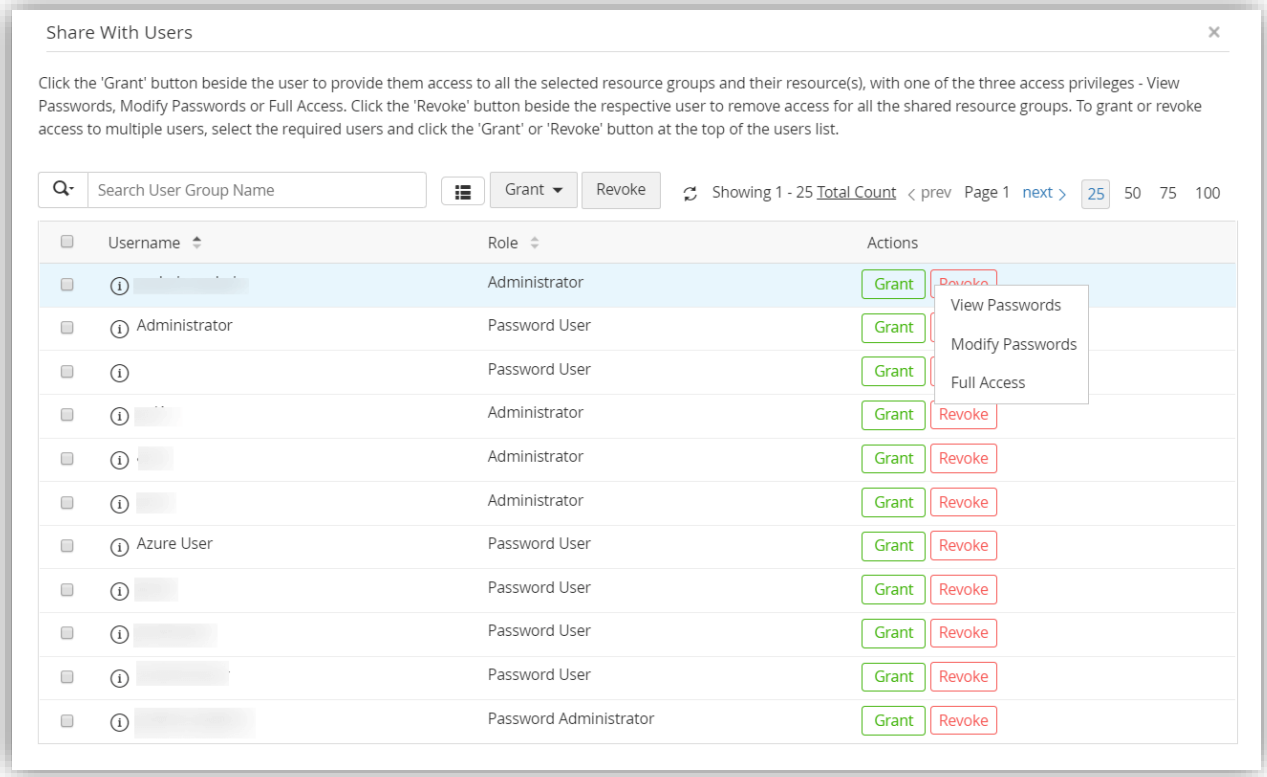


3. Sharing Resource Groups in Bulk with Users/User Groups

Follow the below steps to share a set of resource groups with user(s) or user group(s), with any of the three permission levels - **View, Modify,** or **Full Access.**

1. Navigate to the **Groups** tab and select the resource groups to be shared.
2. Click the **Bulk Configuration** drop down at the top and go to **Share >> With Users** or **With User Groups** depending on whether you want to share the account with users or user groups.
3. In the pop-up box that appears, click the **Grant** option beside that user/user group with whom the resource groups are to be shared. Choose from the permission levels: **View Passwords, Modify Passwords,** or **Full Access,** and click **Save**.





Note: When you share a particular set of resource groups with a user group, the resource groups will be visible to all members of that user group. That means, all the resources and the accounts that are part of those resource groups will be visible to all members of the user group. Also, the permissions granted to the user group **(View, Modify or Full Access)** will be applicable to all the members.

Managing Accounts and Passwords

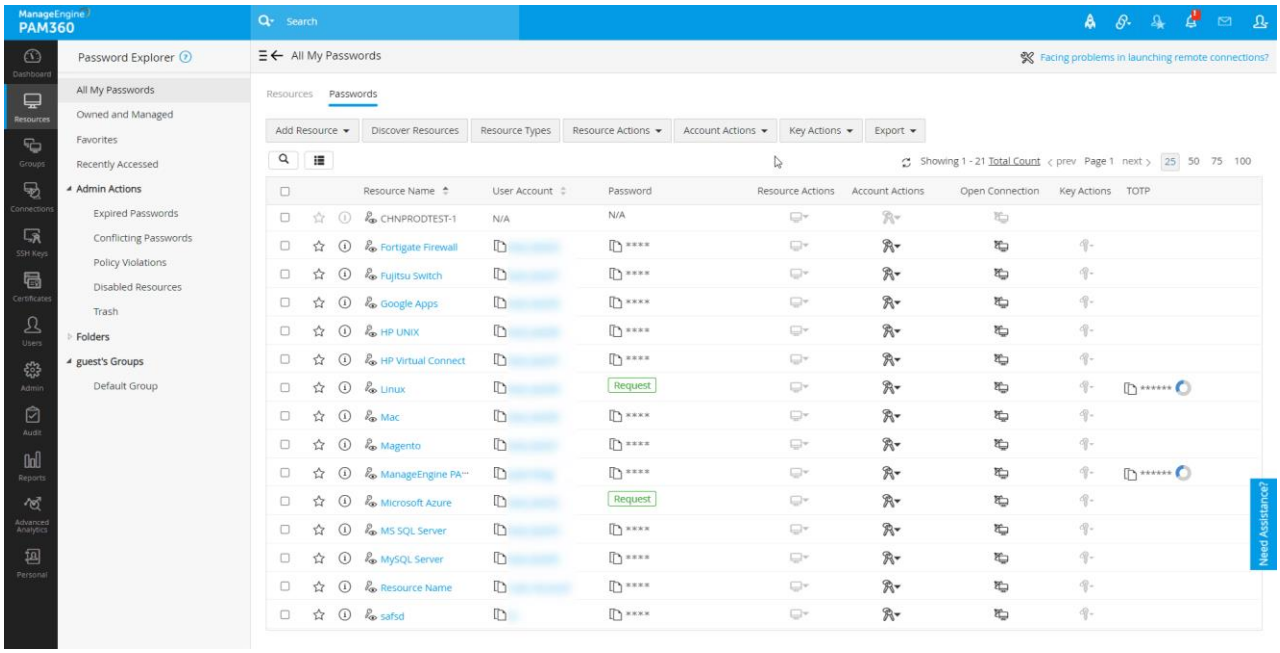
This document discusses the different ways in which users can manage accounts in PAM360 such as viewing, editing, copying, moving accounts and also to change password, view password history and check integrity of passwords stored in PAM360.

1. Viewing Accounts
2. Copying Passwords
3. Changing Passwords
4. Verifying Passwords Stored in PAM360
5. Viewing Password History
6. Copying Passcard Link
7. Editing Accounts
8. Copying Accounts
9. Moving Accounts

1. Viewing Accounts

Follow the below steps to view an account that is part of a resource.

1. Navigate to **Resources** tab.
2. Click on the particular resource name whose account details you want to view.
3. The accounts of the respective resource would be displayed in a new dialog box.
4. By default, passwords are shown in hidden form behind asterisks; to view the passwords in plain text, just click on the respective asterisks. The passwords will be shown for 10 seconds only. After that, they will be automatically hidden. You can also view the passwords by clicking the asterisks again.

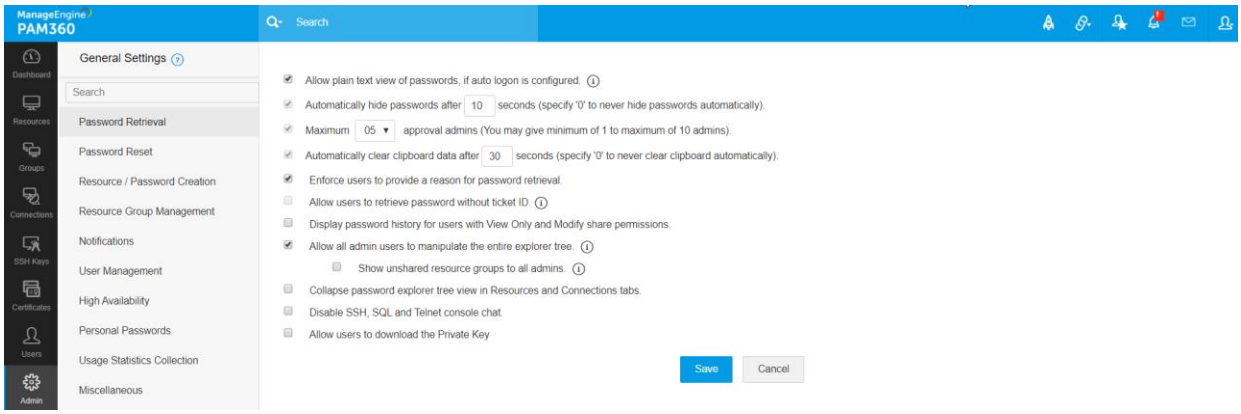


You can modify the default 10 seconds from the **General Settings** page.

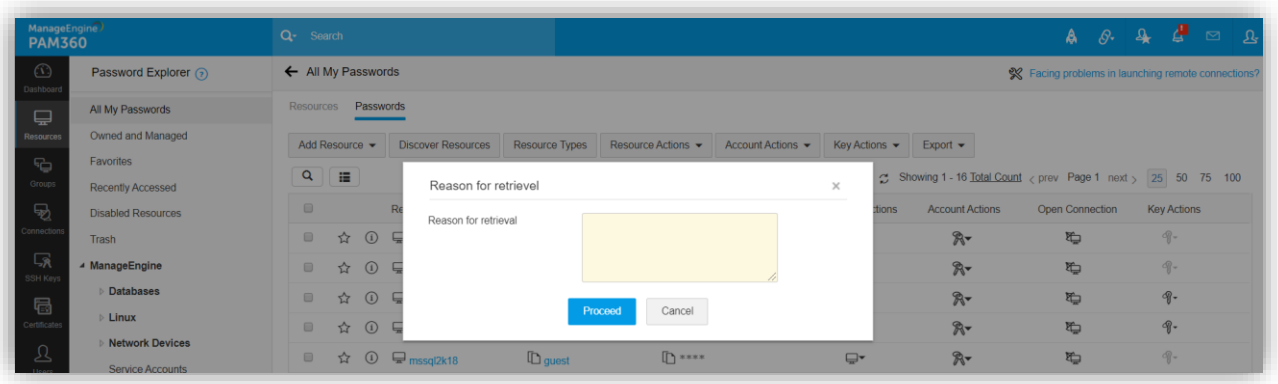
1.1 Enforcing Users to Provide a Reason for Viewing Passwords

By default, when a user tries to retrieve the password of a resource, on clicking the asterisks, the passwords appear in plain text. If you want to force your users to provide a reason why access to the password was needed, you can enable the option **Enforce users to provide reason when retrieving the passwords** in General Settings. Follow the below steps:

1. Navigate to **Admin >> Settings >> General Settings**.
2. In the UI that opens with a list of options, select **Password Retrieval**.
3. Click the checkbox **Enforce users to provide reason when retrieving the passwords**.
4. Click **Save**.



5. After enabling this option, when you click on the asterisks, a pop-up window will open. In that pop-up window, provide a reason for retrieval and click **Proceed**.

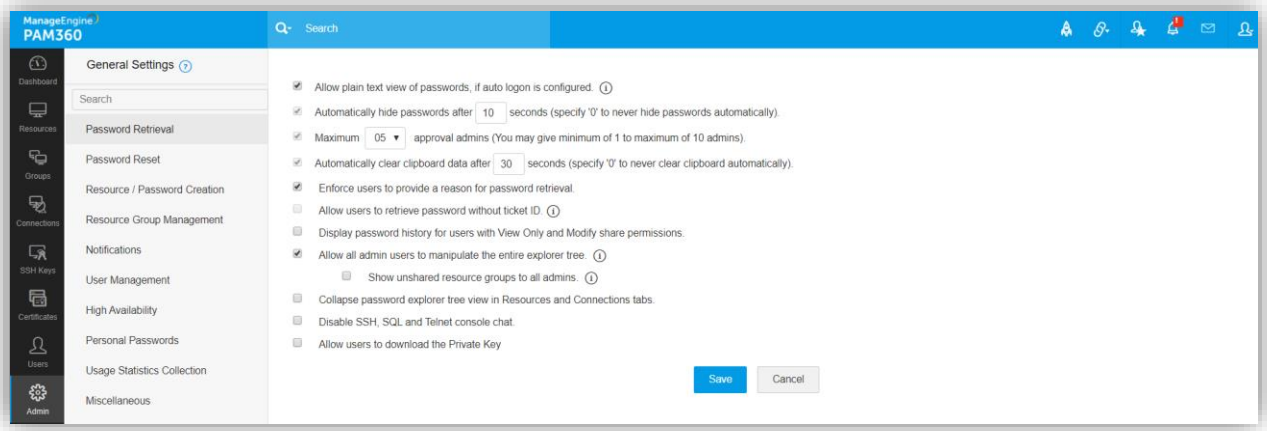


1.2 Allowing password users and auditors to retrieve passwords for which auto logon is configured

Through the auto logon feature, PAM360 provides the option to establish direct connection to the resource eliminating the need for copy-paste of passwords. By default, password users and auditors will be able to retrieve the passwords that are shared with them. However, if auto logon is configured, they might not need access to the passwords. In such cases, you can take a decision to either allow or restrict access to passwords and implement the same through the option **"Allow password users and auditors to retrieve passwords for which auto logon is configured"** in General Settings.

To enable this option,

1. Navigate to **Admin >> Settings >> General Settings**.
2. In the UI that opens with a list of options, select **Password Retrieval.**
3. Click the checkbox **Enforce users to provide reason when retrieving the passwords**.
4. Click **Save**.

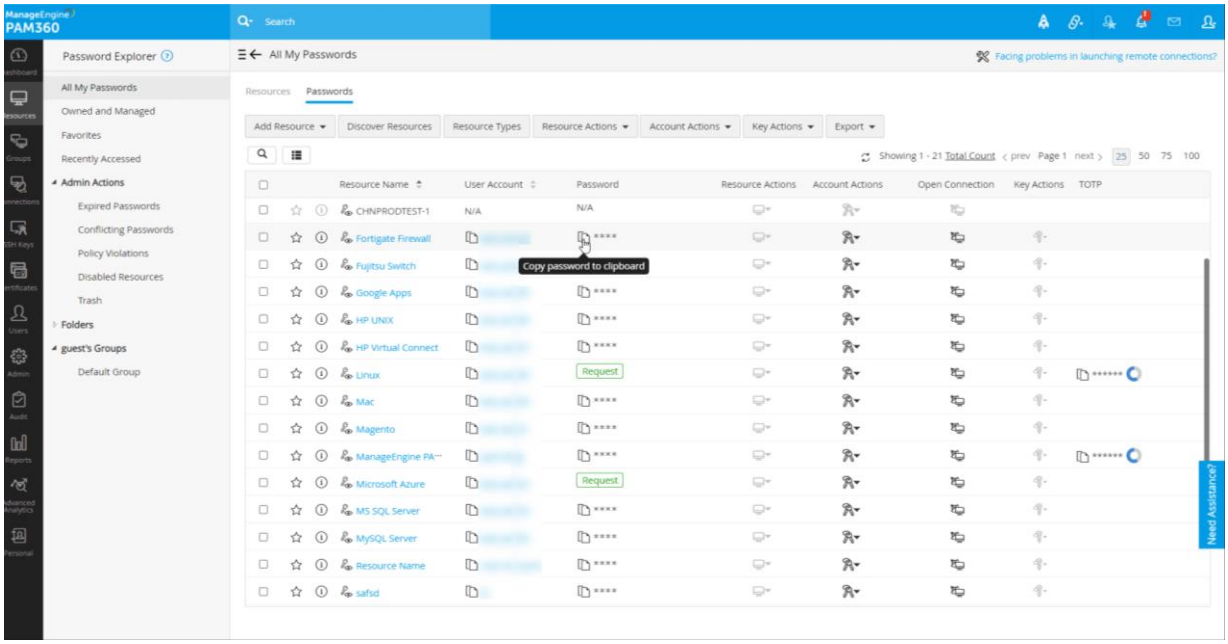


2. Copying Passwords

PAM360 leverages clipboard utility of browsers to copy passwords when you intend to copy and paste passwords.

Follow the below steps to copy passwords:

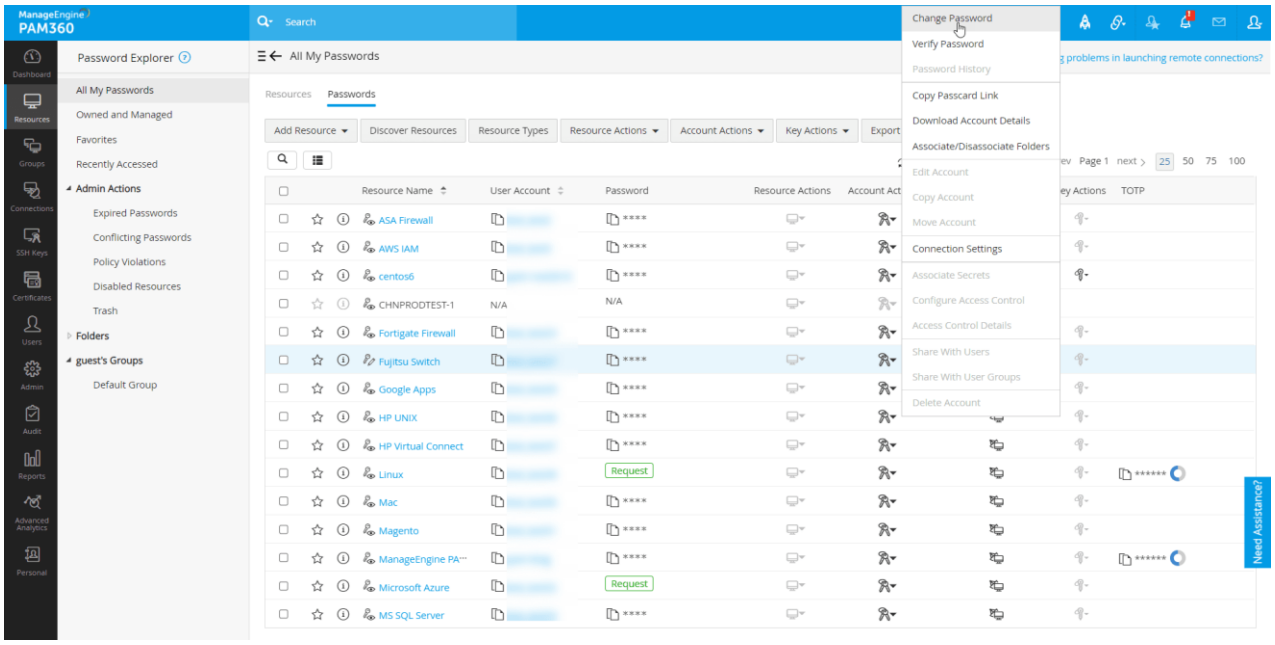
1. Navigate to the **Resources** tab.
2. Switch to **Passwords** link and click the copy icon present against the desired passwords to copy.
3. The copied passwords will be available to paste for 30 seconds.



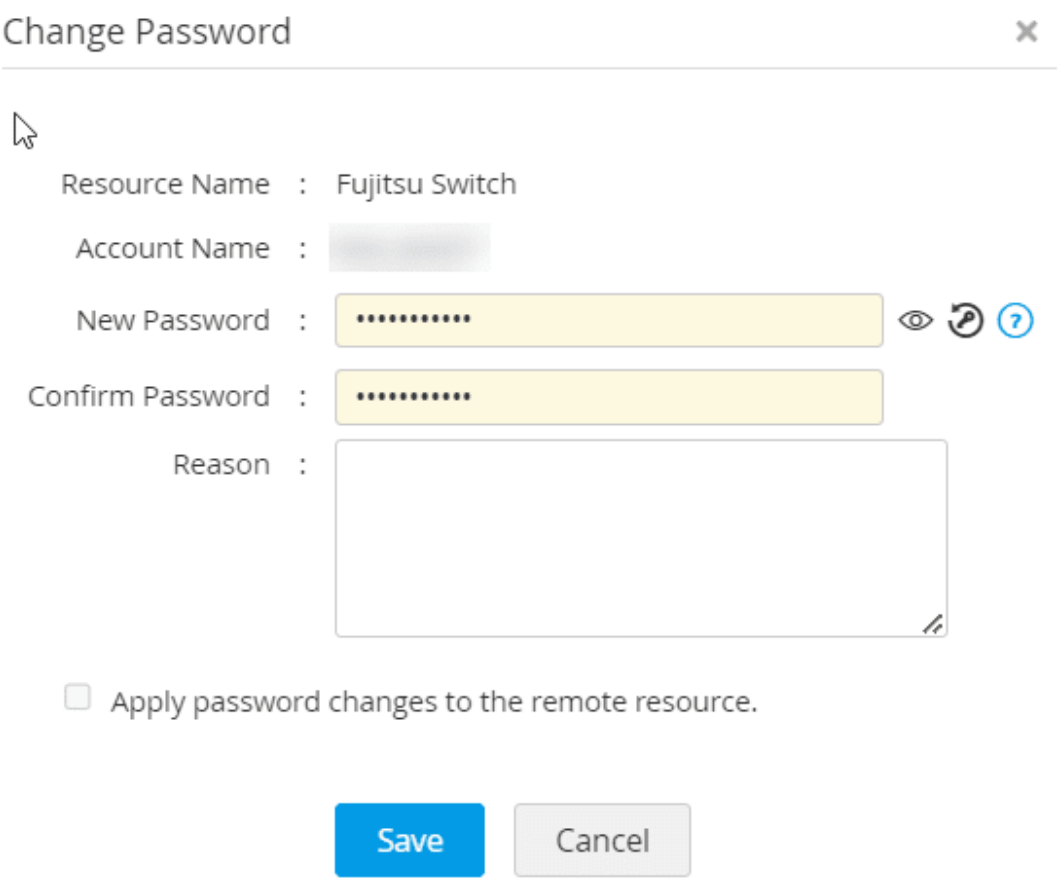
3. Changing Passwords

To change the passwords of user accounts,

1. Navigate to the **Resources** tab, switch to the **Passwords** tab or from the **Resources** tab, click a required resource name to open the **Account Details** dialog box.
2. Click the **Account Actions** icon against the resource whose password you want to change and select **Change Password** from the drop-down list.



3. In the pop-up form that appears, enter the new password and confirm the same.
4. Click **Save**.



Notes:

- While entering the new password, the password policy set by the administrator for this resource will get enforced, if any.
- If your account belongs to any of the types - Windows, Windows Domain, Linux, IBM AIX, HP UNIX, Solaris, Mac OS, MS SQL server and Cisco Devices (IOS, CatOS, PIX), you have the option to synchronize the new password in the remote resource too. In such cases of remote synchronization, if there is a failure in updating the password in the resource, password changes will not be saved locally as well.

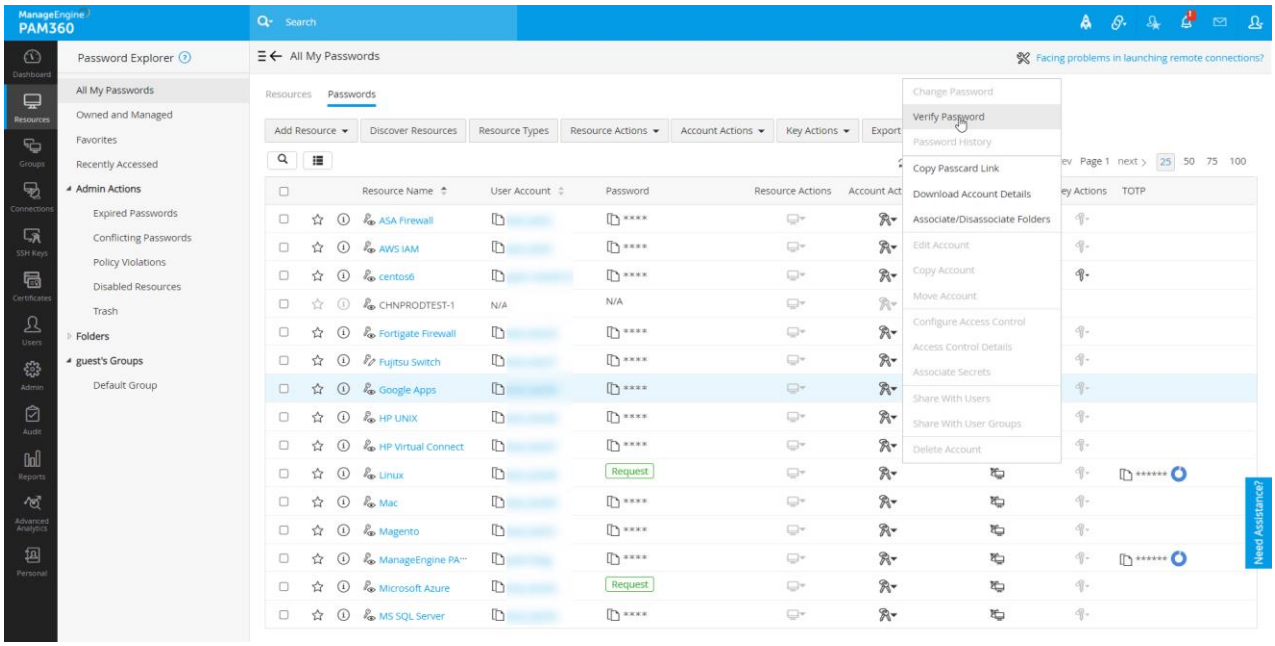
4. Verifying Passwords Stored in PAM60

Passwords of resources such as servers, databases, network devices and other applications are stored in PAM360. It is possible that someone who has administrative access to these resources could access the resource directly and change the password of the administrative account. In such cases, the password stored in PAM360 will be outdated and not be of any use to the users who access PAM360 for the password. To deal with such possibilities, PAM360 provides an option for checking the validity of passwords at any point of time, both on demand and also at periodic intervals. On demand verification for password validity can be performed for a single account or for all the resources/accounts stored in the PAM360 application.

4.1 Verifying Individual Passwords

Follow the below steps to verify the integrity of the password of a single account:

1. Navigate to **Resources** tab, switch to the **Passwords** tab or from the **Resources** tab, click a required resource name to open the **Account Details** dialog box.
2. Click the **Account Actions** against the resource whose password you want to verify for synchronization and select **Verify Password** from the drop-down list.



3. PAM360 will try to establish connection with the target system. Once the connection is established, it tries to log in with the credentials stored in PAM360. If login does not succeed, PAM360 concludes that the password is out of sync.

Notes:

1. Password Verification will work only for the accounts for which **Remote password reset** has been enabled.
2. If PAM360 cannot establish a connection with the system due to some network problem, it will not be considered that the password is out of sync.

4.2 Verifying Passwords in Bulk

Check if the passwords stored in PAM360 are in synchronization with the actual passwords of the resources by running this check.

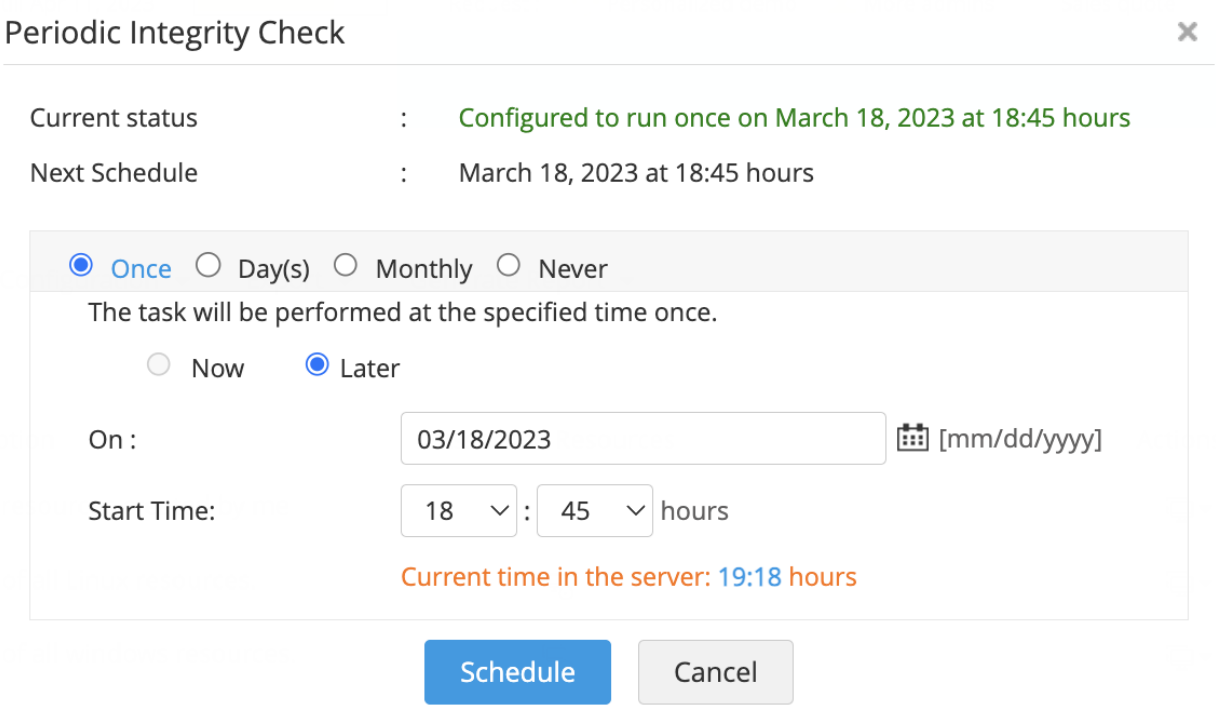
Follow the below steps to verify the integrity of the passwords in bulk:

1. Navigate to Groups >> Group Actions >> Find Out of Sync Passwords. A window shows up.
2. Click Start Now. A success message 'Integrity check scheduled successfully' will be displayed. Now, all the passwords of the selected group will be checked and email notification will be sent to the administrator.

4.3 Scheduled Verification of Passwords in Bulk

You can schedule to check the integrity of the passwords stored in PAM360. Follow the steps below:

1. Navigate to **Groups >> Group Actions >> Periodic Integrity Check**. A window shows up with the current and upcoming status of the schedule of the selected group.



2. Schedule the integrity check or modify the existing schedule by choosing any of the below options:
    i. Once, on a specific day and time
    ii. On an interval based on the specified days, from a specific day and time
    iii. Monthy, on a specific day and time
    iv. Never
3. Click **Schedule**.

Now, the integrity check will be run based on the schedule configured, and PAM360 will try to establish connection with the target systems for all the accounts in the selected group for which remote password reset has been enabled. Once the connection is established, it tries to login with the credentials stores in PAM360. If login does not succeed, PAM360 concludes that the passwords are out of sync. A consolidated notification will be emailed to all the administrators and auditors.

Note: If PAM360 cannot establish a connection with the system due to some network problem, it will not be considered that the password is out of sync.

4.4 Verifying All the Passwords Stored in PAM360

1. Navigate to **Reports >> Password Out of Sync**
2. Under that report, click the link **Find Out of Sync passwords**. In the dialog box that opens, click **Start Now.**
3. Once you schedule the check, PAM360 will try to establish connection with the target systems for all the accounts for which remote password reset has been enabled. Once the connection is established, it tries to log in to each resource with the credentials stored in PAM360 respectively. If login does not succeed, PAM360 concludes that the password is out of sync. In case, PAM360 is not even able to establish connection with the system due to some network problem, it will not be taken as password out of sync. A consolidated notification would be emailed to all the administrators and auditors.

5. Viewing Password History

The history of changes done to the passwords are captured in the form of password history. Information such as the old password, modified by whom, from which machine and the time at which it was modified are all captured in history.

To view password history of an account,

1. Navigate to **Resources** tab, switch to the **Passwords** tab or from the **Resources** tab, click a required resource name to open the **Account Details** dialog box.
2. Click the **Account Actions** icon against the resource whose password history you want to view and select **Password History** from the drop down list.
3. In the pop-up for that appears, password history will be displayed.

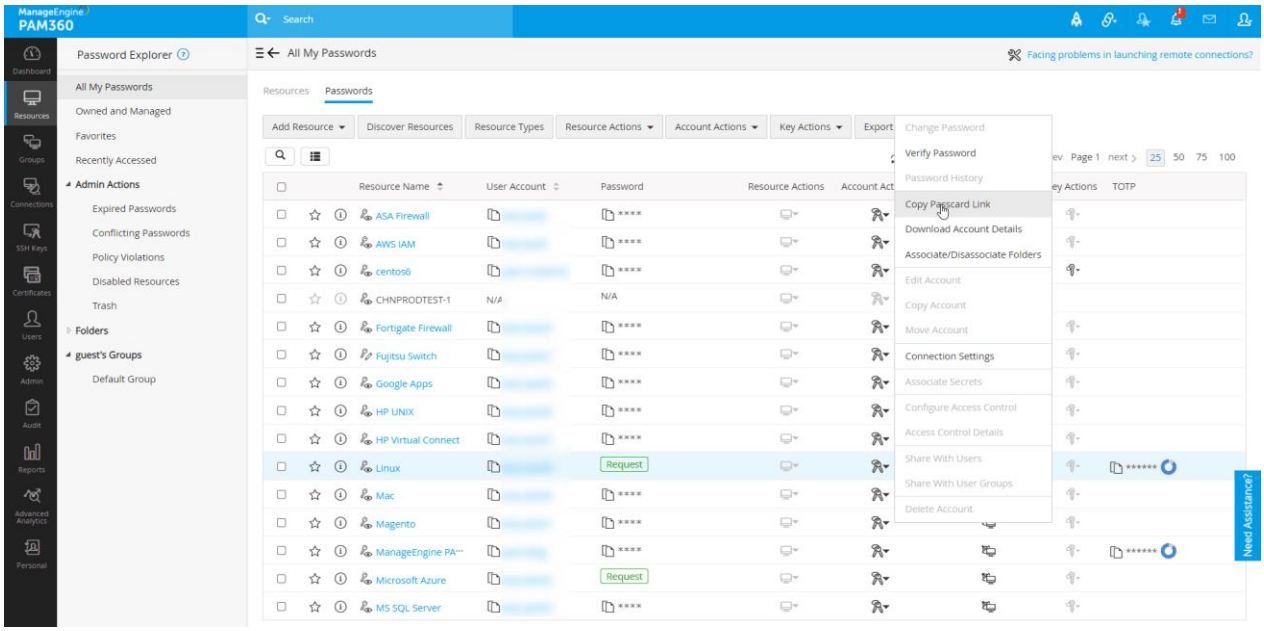
6. Copying Passcard Link

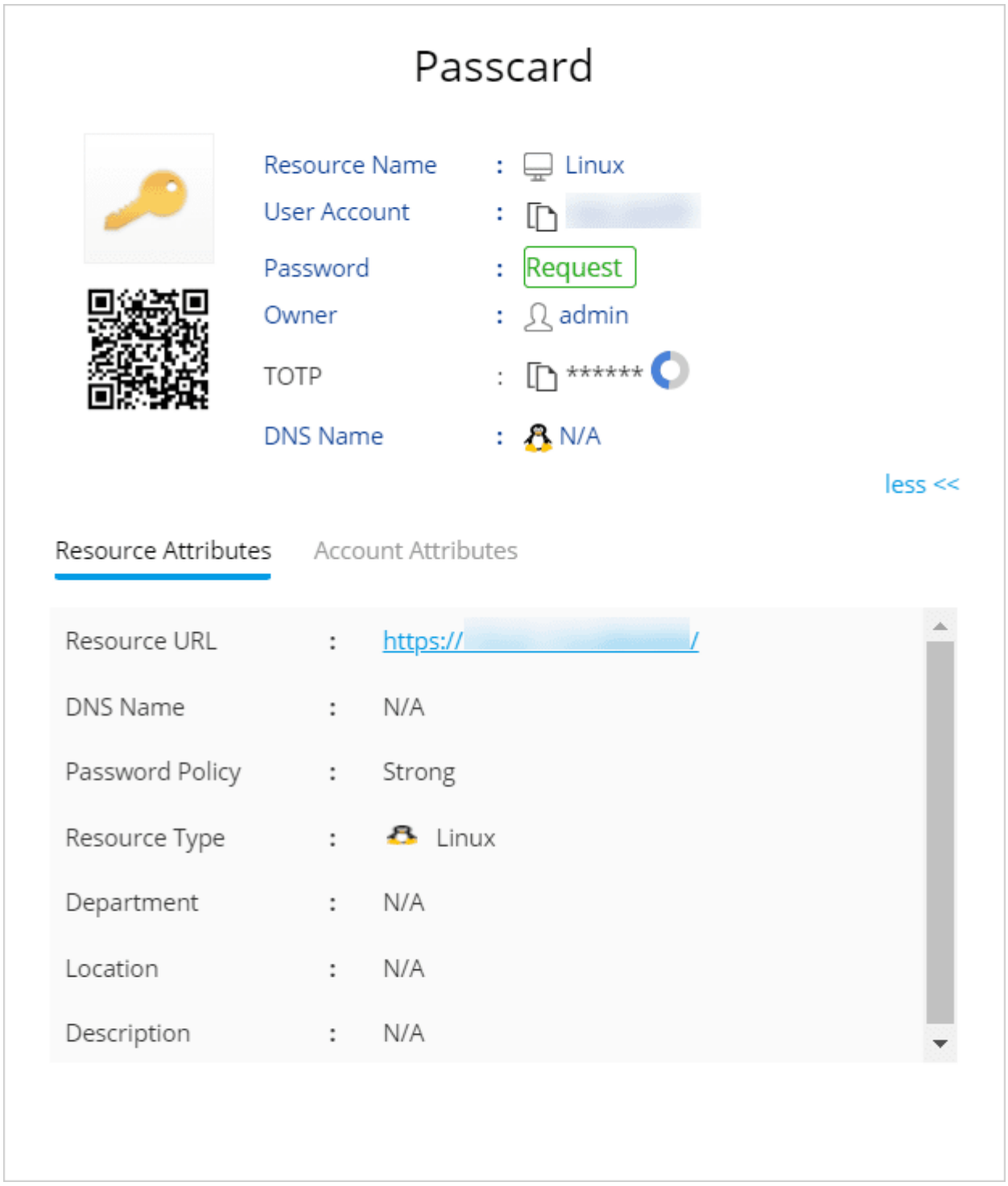
A passcard typically contains details such as Resource Name, Account Name, Password of the account, Owner of the resource and the DNS name, along with any additional resource or account attributes that might be added to it. To view the passcard of an account, you must be logged into PAM360 and the corresponding resource must be owned by you or shared to you.

The Passcard link provides consolidated details of an individual account in PAM360 as a shareable link. The link can be accessed by only those to whom the passcard is shared with the relevant privilege (read-only, read-write, or manage).

Follow the below steps to copy the Passcard of an account:

1. Navigate to **Resources** tab, switch to the **Passwords** tab or from the **Resources** tab, click a required resource name to open the **Account Details** dialog box.
2. Click the **Account Actions** icon beside the required account name and choose **Copy Passcard Link** from the dropdown.
3. The Passcard link will be copied to the clipboard and will remain there until you click the **Click Here to Clear Clipboard** option to erase it. The **Click Here to Clear Clipboard** option will appear in the top right corner of the page as soon as you copy the Passcard link.
4. Paste the copied Passcard URL in a new browser window to view its contents. The Passcard will also contain a QR code from which the URL can be scanned and extracted.





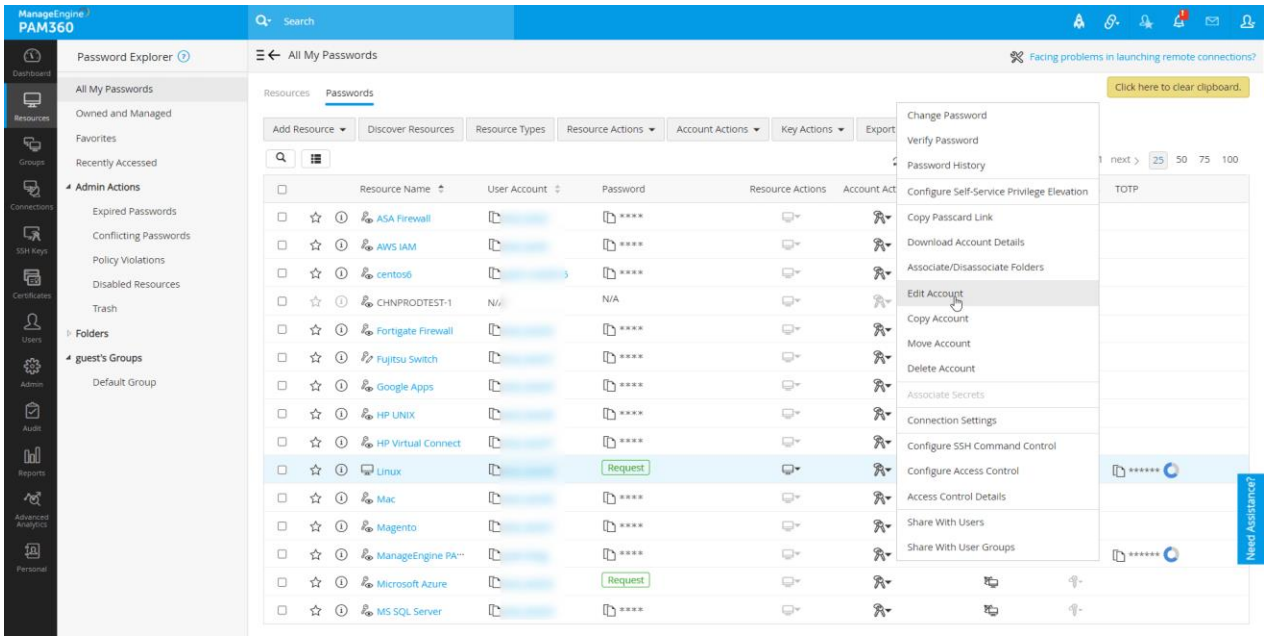
7. Editing Accounts

At any point of time, you can edit the details of any of the accounts.

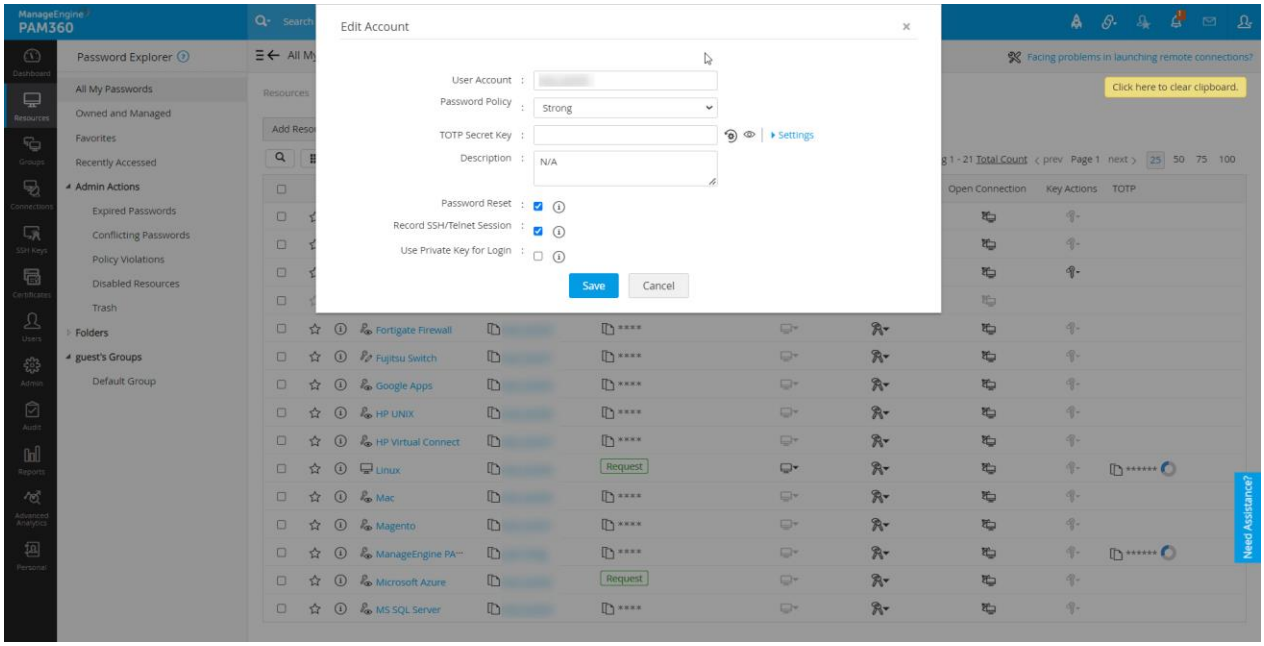
To edit an account,

1. Navigate to the **Resources** tab, switch to the **Passwords** tab or from the **Resources** tab, click a required resource name to open the **Account Details** dialog box.
2. Click the **Account Actions** icon beside the resource whose password you want to edit

and choose **Edit Account** from the dropdown.



3. In the pop-up form that appears, edit the required property of the account.
4. Select the checkbox **Use private key to login to this account instead of password** to authorize remote connections using SSH keys instead of account credentials. Click here to know more about remote connection using SSH keys.
5. Once you're done, click **Save**. The required change will get reflected in the view.

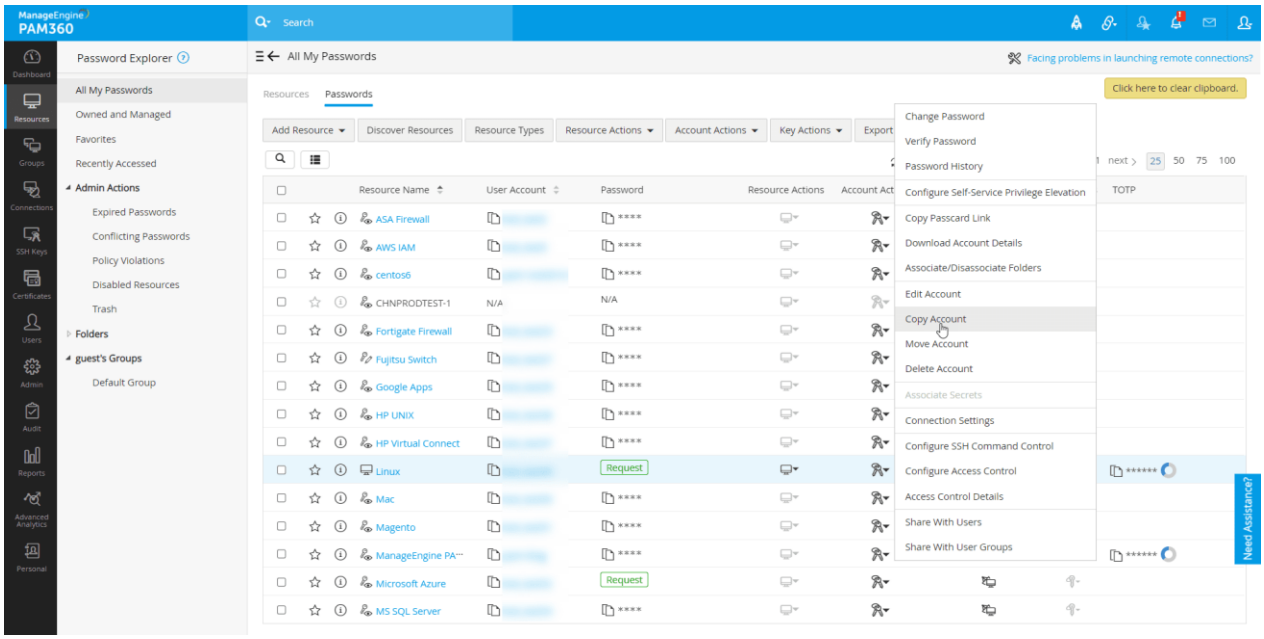


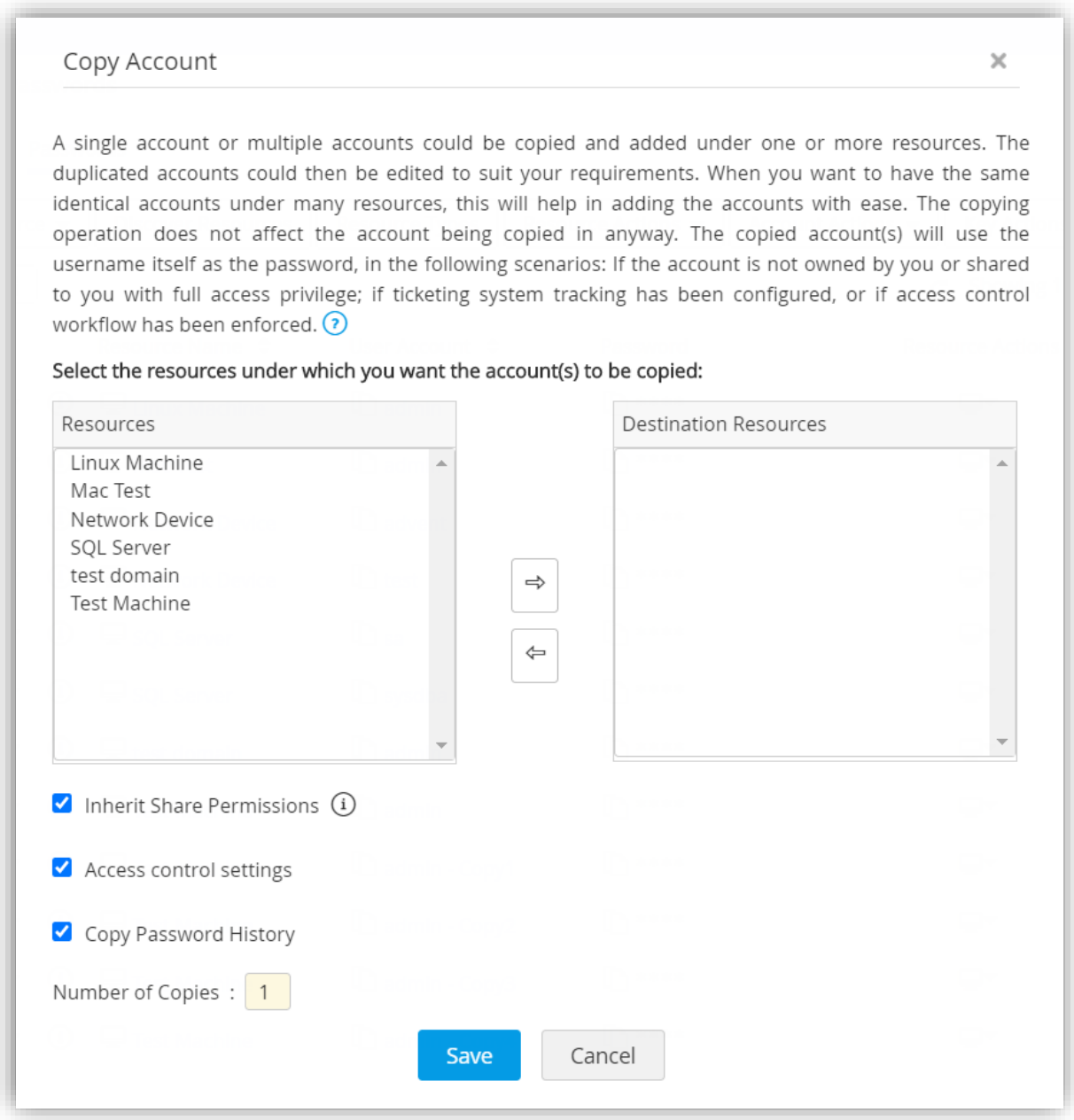
8. Copying Accounts

Copy and add accounts under one or more resources. You can then edit the replicated accounts to suit your requirements. The Copy Account feature will come handy when you handle identical accounts of different resources. Remember, the copy action will not create any changes to the account(s) copied.

Follow the below steps to copy one or more accounts:

1. Navigate to **Resources** tab and switch to **Passwords** tab. Select the account(s) to be copied.
2. To copy a single account, go to **Resources** tab, click a required resource name to open the **Account Details** dialog box.
3. Then, click the **Account Actions** icon beside the required account and select **Copy Account** from the drop-down list.
4. In the **Copy Account** dialog box, select the resources under which you want the accounts to be copied. Move the required resources to the **Destination Resources** pane using the arrows.
5. Select the **Inherit Share Permissions** option for the new copies inherit the selected account's share permissions i.e., the new account will also be shared with all those who had permission to view the parent account.
6. Select the **Access Control Settings** option to retain the access control configuration done for the selected account, during the copy operation. Please note that this copy operation will retain only the Account-level access control configuration. If this option is unchecked during the copy operation (OR) if the selected account does not have any individual access control settings configured, then the resource level access control settings of the destination resource will be applied to this account as well.
7. Select the **Copy Password History** option to retain the selected account's password history. Refer to the help section **Viewing Password History** for more information on password history.
8. You can also specify the number of copies required. Click **Save**. The account(s) will appear under the selected resource(s).


ManageEngine
PAM360
Search
Password Explorer
All My Passwords
Owned and Managed
Favorites
Recently Accessed
Admin Actions
Expired Passwords
Conflicting Passwords
Policy Violations
Disabled Resources
Trash
Folders
guest's Groups
Default Group
All My Passwords
Facing problems in launching remote connections?
Resources
Passwords
Click here to clear clipboard.
Add Resource
Discover Resources
Resource Types
Resource Actions
Account Actions
Key Actions
Export
Resource Name
User Account
Password
Resource Actions
Account Act
TOTP
ASA Firewall
AWS IAM
centos6
CHNPRODTEST-1
Fortigate Firewall
Fujitsu Switch
Google Apps
HP UNIX
HP Virtual Connect
Linux
Mac
Magento
ManageEngine PA···
Microsoft Azure
MS SQL Server
Request
Change Password
Verify Password
Password History
Configure Self-Service Privilege Elevation
Copy Passcard Link
Download Account Details
Associate/Disassociate Folders
Edit Account
Copy Account
Move Account
Delete Account
Associate Secrets
Connection Settings
Configure SSH Command Control
Configure Access Control
Access Control Details
Share With Users
Share With User Groups
Need Assistance?



9. Moving Accounts

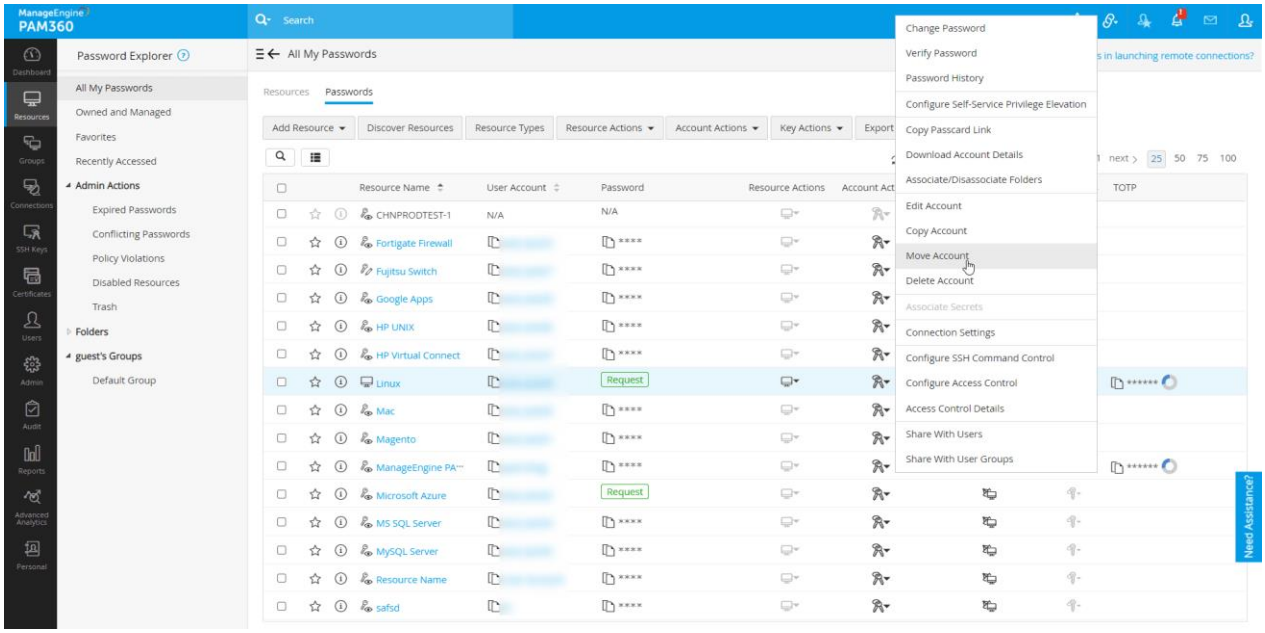
Move one or more accounts that are part of one resource to another resource. When you do so, the selected account(s) will be removed from the present resource.

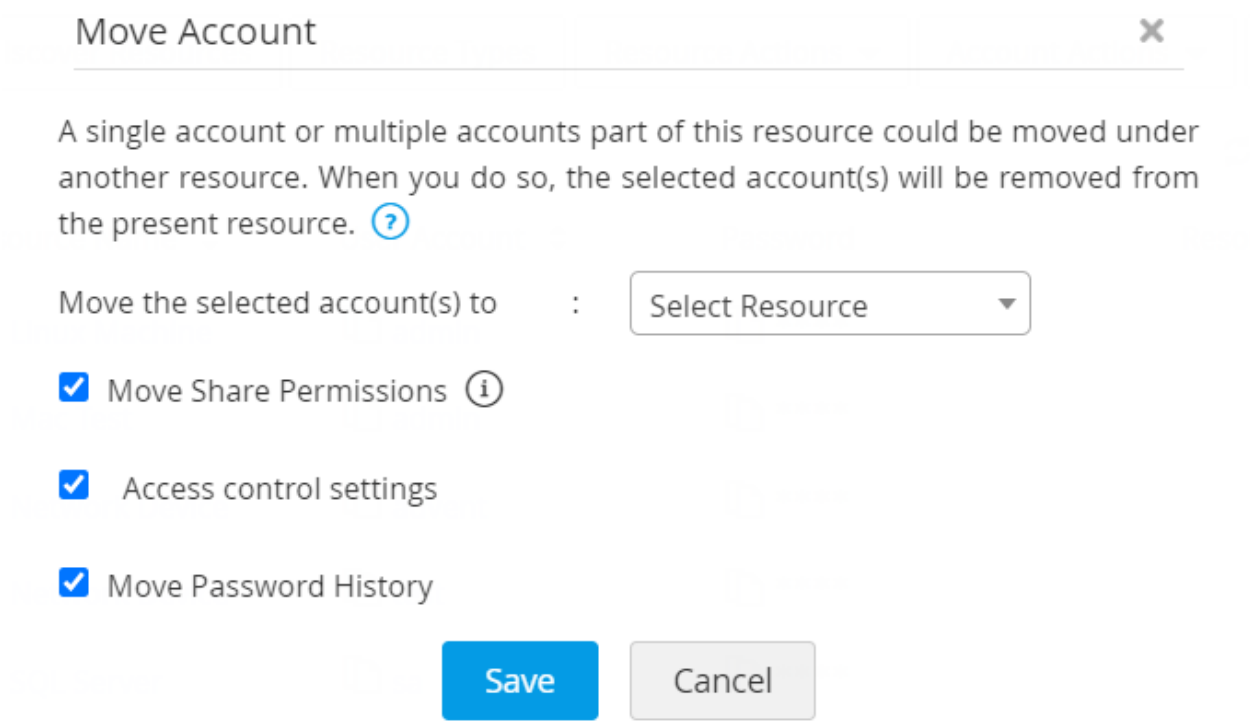
Follow the below steps to move one or more accounts:

1. Navigate to the **Resources** tab and switch to **Passwords** tab. Select the account(s) to be moved.
2. To move a single account, go to **Resources** tab, click a required resource name to open the **Account Details** dialog box.
3. Then, click the **Account Actions** icon and choose **Move Account** from the drop-down

list.

4. In the **Move Account** dialog box, choose a resource from the **Move the Selected Account(s)** to dropdown.
5. Select the **Inherit Share Permissions** option to move the selected account's share permissions i.e., the new account will also be shared with all those who had permission to view the parent account.
6. Select the **Access Control Settings** option to retain the access control configuration done for the selected account, during the move operation. Please note that this move operation will retain only the Account-level access control configuration. If this option is unchecked during the move operation (OR) if the selected account does not have any individual access control settings configured, then the resource level access control settings of the destination resource will be applied to this account as well.
7. Select the **Move Password History** option to retain the selected account's password history. Refer to the help section **Viewing Password History** for more information on password history.
8. Click **Save**. The account(s) will be removed from the present resource and it will appear under the selected resource(s).




Move Account
A single account or multiple accounts part of this resource could be moved under another resource. When you do so, the selected account(s) will be removed from the present resource.
Move the selected account(s) to :
Select Resource
Move Share Permissions
Access control settings
Move Password History
Save
Cancel

Managing Resource Types

PAM360 supports certain resource types by default. In addition, you can add as many custom resource types as you require. Manage the resource types in PAM360 from both the **Resources** tab and the **Admin** console. Add, edit, delete and customize the resource types based on your requirements. You can also add custom icons for the resource types. The various categories of resource types supported by PAM360 and the operations that can be performed on them are discussed in this document.

> **Note:** You cannot delete the default resource types, but can edit their attributes to fit your requirements.

1. Resource Type Categories
2. Adding a Resource Type
3. Editing a Resource Type
4. Bulk Editing Resource Types
5. Enabling Resource Filters
6. Deleting a Resource Types

1. Resource Type Categories

Classify the resources added into PAM360 into any of the following resource type categories. You will see these resource types listed under the Resource Type drop-down while adding or editing the resources.

Operating Systems

- HPUX
- Windows
- Windows Domain
- Linux
- Mac
- Solaris
- HP Unix
- IBM Aix

Cisco Devices

- Cisco Management Integration Center
- Cisco Catalyst
- Cisco SG300
- Cisco UCS
- Cisco Wireless LAN Controller
- Cisco IOS

- Cisco Pix
- Cisco Cat OS
- Cisco Nexus OS

Database Servers

- MS SQL
- Sybase ASE
- Oracle DB server
- PostgreSQL

Network Devices

- ASA Firewall
- Audiocode
- Brocade
- Brocade VDX
- Brocade SAN Switch
- Checkpoint Firewall
- Extreme Networks
- F5
- Fortinet
- Fortigate Firewall
- Fortimail
- Fujitsu Switch
- Gigamon
- H3C
- HMC
- HP Printer
- HP Onboard Administrator
- HP Virtual Connect
- Huawei
- HP Procurve
- Juniper
- Juniper Netscreen ScreenOS
- HP iLO
- Mikrotik
- Opengear
- Orange Firewall
- Palo Alto Networks
- Pfsense
- Routerboard
- Ruijie
- Sonicwall
- TPLINK
- VMWare VCenter
- Citrix Netscaler SDX

- Citrix Netscaler VPX
- Magento
- Netapp 7Mode
- Netapp CDot

File Stores

- HPE StoreOnce
- File Store
- Key Store
- Certificate Store
- Nimble Storage
- License Store

Cloud Services

- WebLogic
- AWS IAM
- Google apps
- Rackspace
- Microsoft Azure
- Salesforce
- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL
- Azure App

MQ Applications

- RabbitMQ

Others

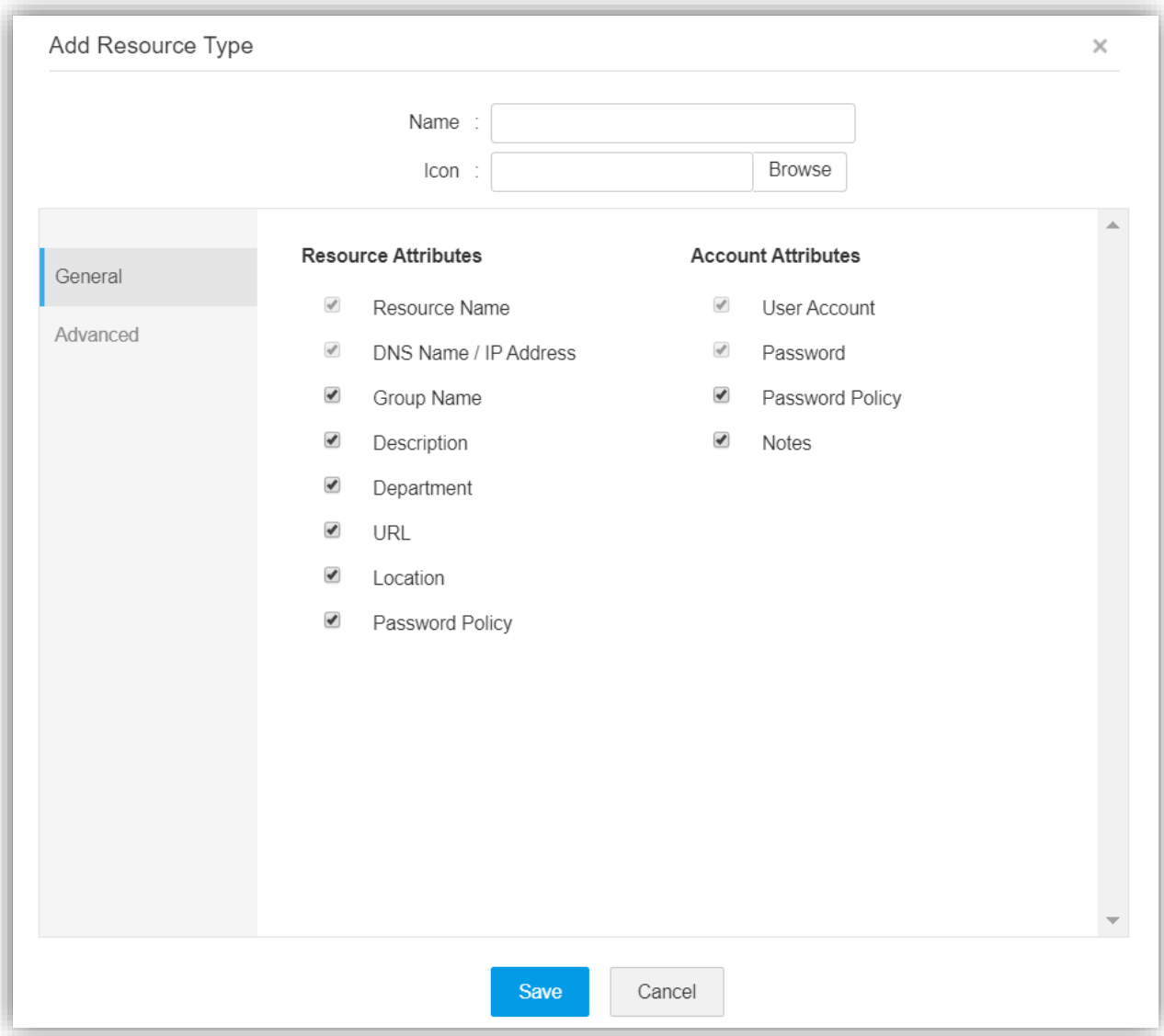
- Website accounts
- LDAP Server
- VMWare ESXi
- IBM AS400
- Oracle XSCF
- Oracle ALOM
- Oracle ILOM
- Aruba ATP
- AVAYA-GW
- FortiManager-FortiAnalyzer
- Nortel

2. Adding a Resource Type

1. Navigate to **Admin >> Resource Config >> Resource Types** or **Resources >> Resource**

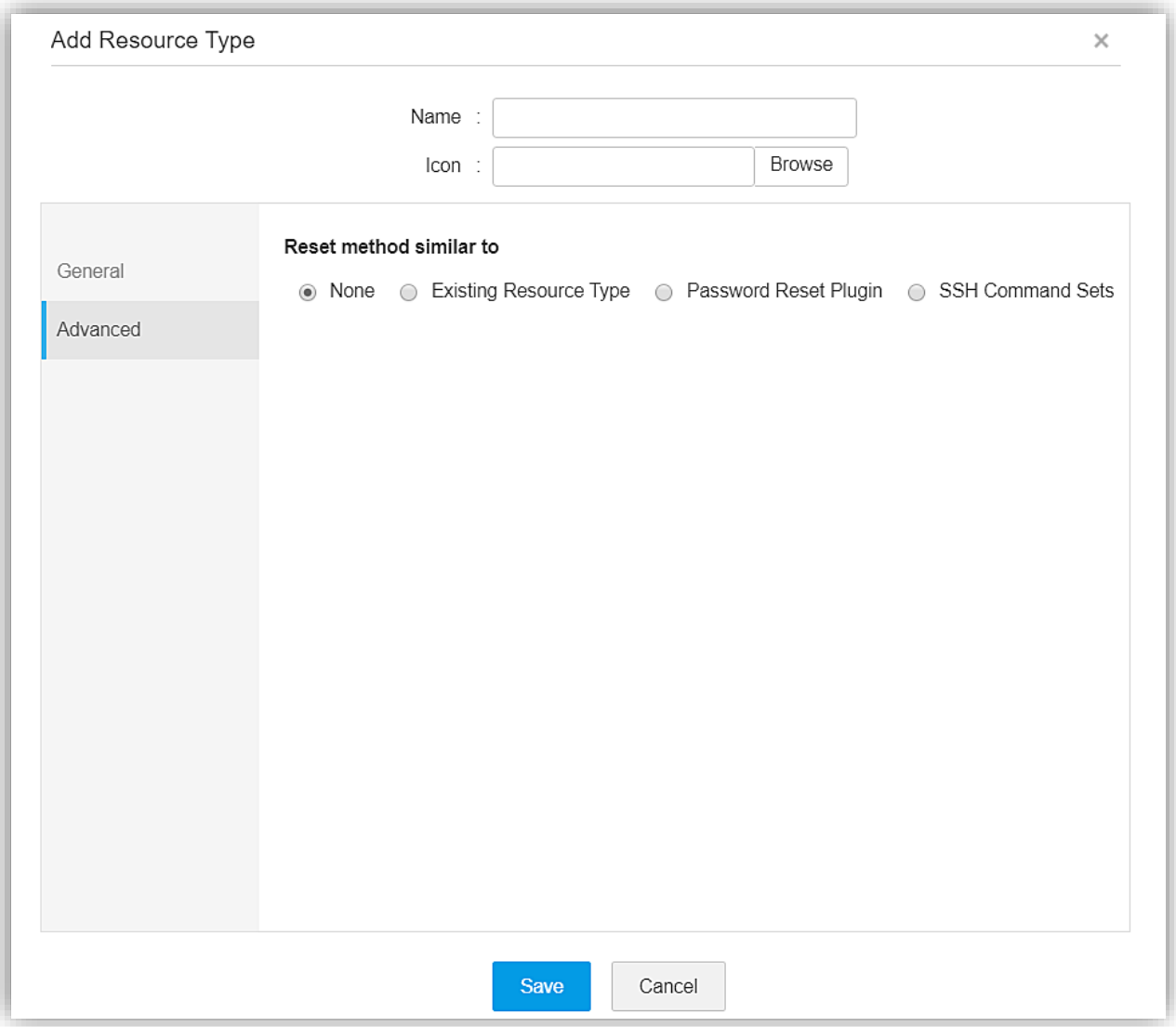
types.

2. In the **Resource Types** window that pops up, click **Add** to open up the **Add Resource Type** pop-up box.
3. Here, enter a **Name** for the new resource type.
4. Enter a name for the new resource type. Click **Browse** to choose your own icon for the new resource type you are adding. If you do not add a custom icon, then a default icon will be set by PAM360.
5. Use the **General** tab to choose **Resource** and **Account** attributes based on the requirements of your new resource type.



6. Use the **Advanced** tab to choose the type of password reset method you want to set for your resource type. You have the below options to choose from:
    i. Existing Resource Type
    ii. Password Reset Plugin

iii. SSH Command Sets

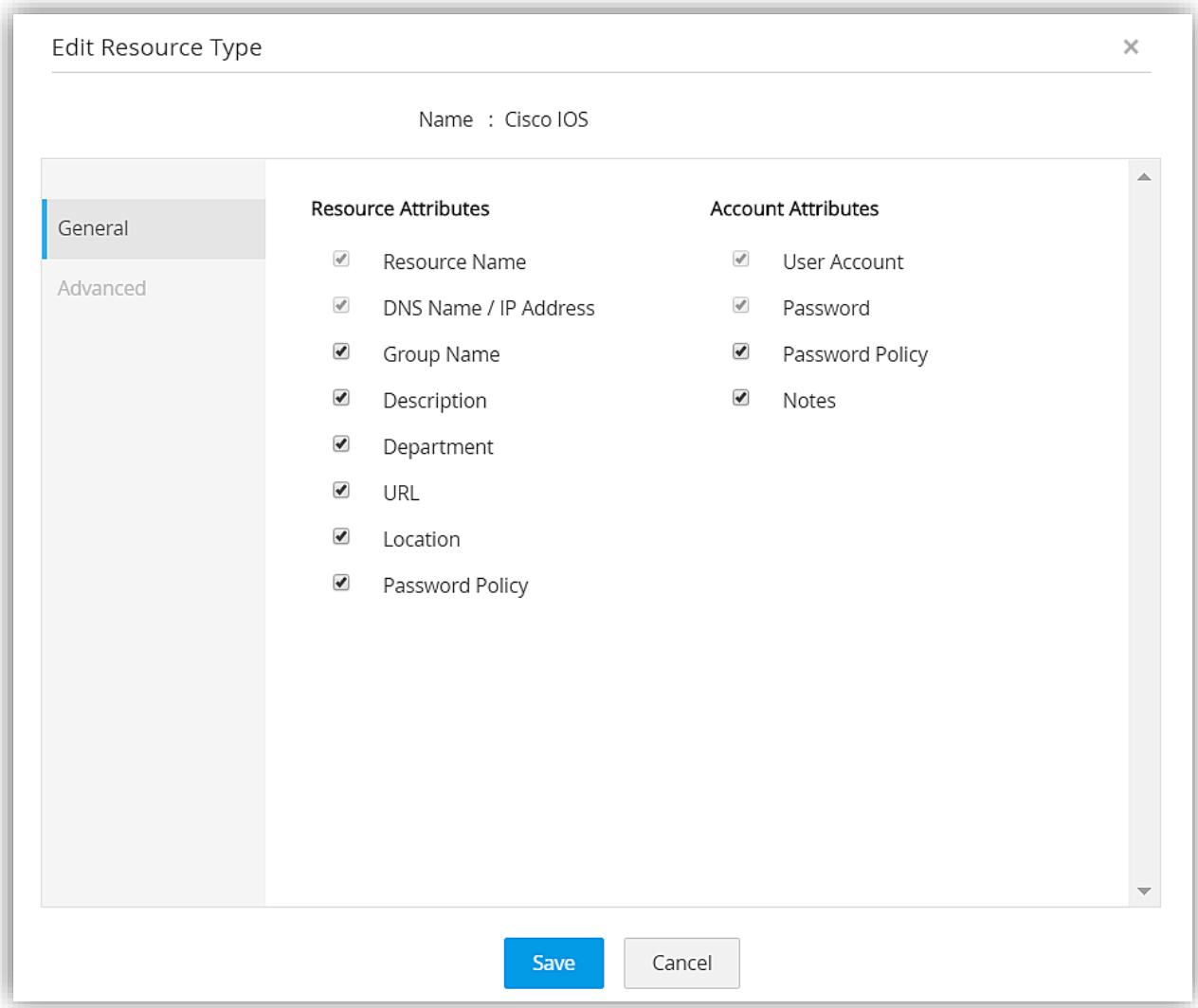


7. You may choose the **Existing Resource Type** option if the resource type you are adding is similar to an existing resource type, such as a variation of a network device like Cisco or HP. This will enable PAM360 to associate similar actions with your custom resource type.
8. Choose the **Password Reset Plugin** option if you have already created a plugin from the **Admin** console. Click here for more information on the password reset plugins.
9. Choose the **SSH Command Sets** option for network devices that need a custom set of commands to perform password reset. Click here for more information on SSH Command Sets.
10. Click **Save** to save your changes.

Now, you have successfully created a new resource type which will be listed under the **Resource Type** drop-down.

3. Editing a Resource Type

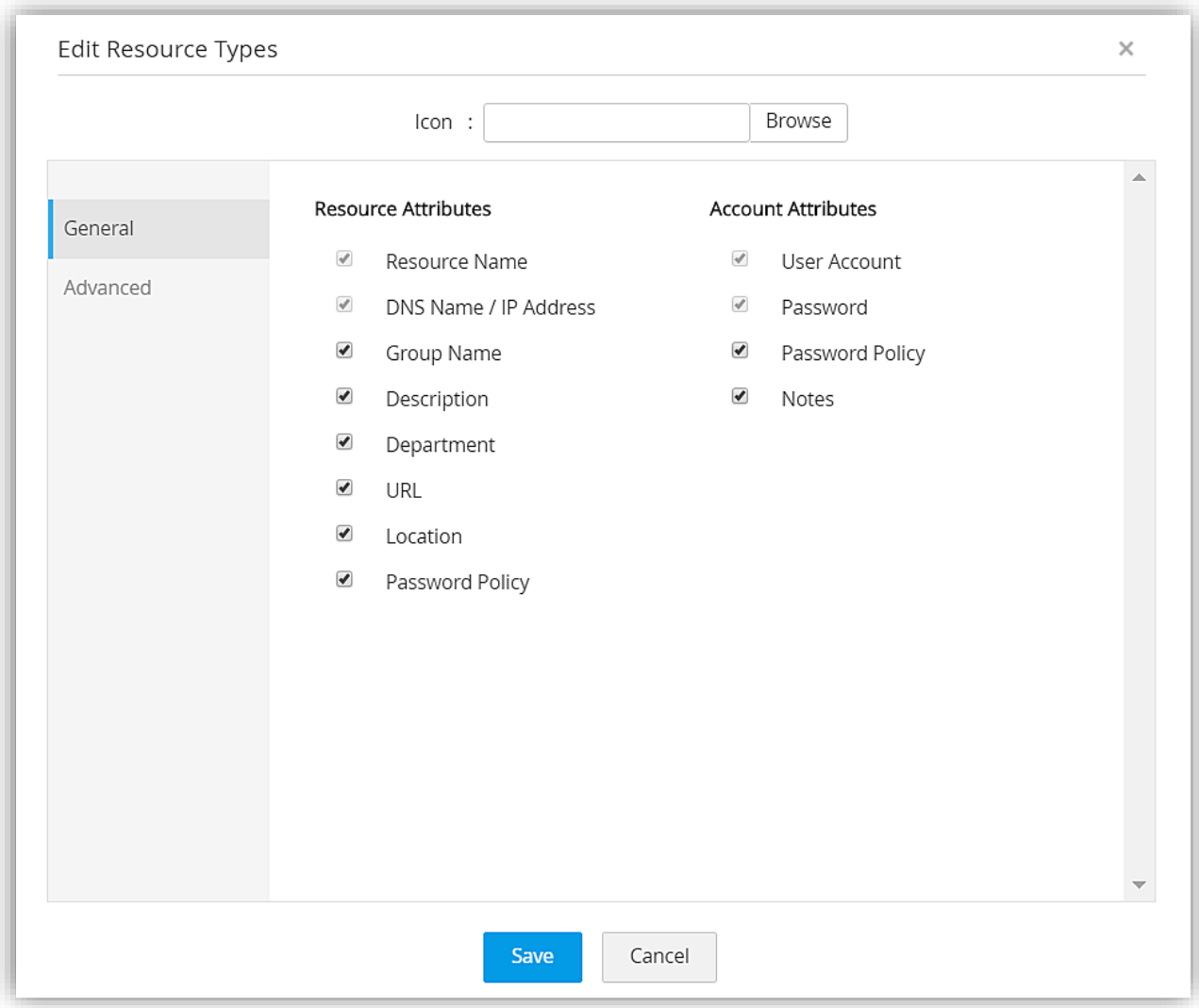
1. Navigate to **Admin >> Resource Config >> Resource Types**.
2. To edit attributes of a single resource type, click the **Edit** icon against the said resource type.



3. In the pop-up box, select or deselect the basic resource and account attributes as per your requirement. The **Advanced** tab will be disabled for edits. Click **Save** to save the changes.

4. Editing Resource Types in Bulk

1. Navigate to **Admin >> Resource Config >> Resource Types.**



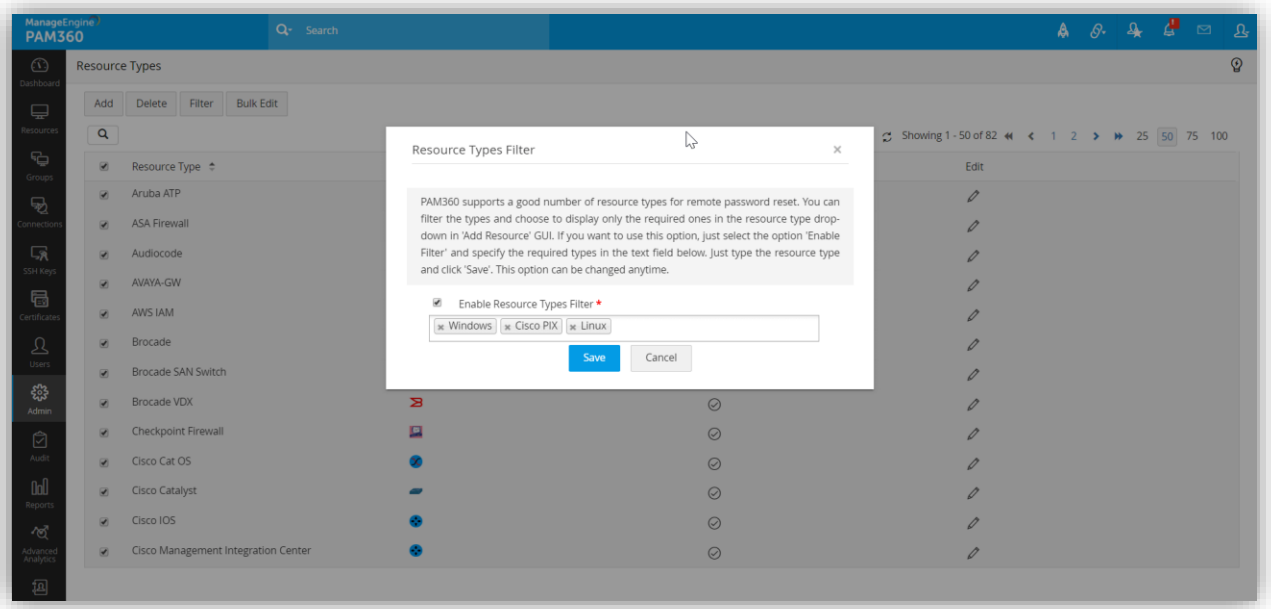
2. Select one or more resources and then click **Bulk Edit**.
3. In the pop-up box, choose the resource and account attributes based on the resource type by checking the boxes based on your requirement. Here, you can also upload a new icon of your choice for the selected resource types and **Save** the changes.

> **Note:** Default resource types cannot be customized.

5. Enabling Resource Types Filter

Enable the **Filter** option to help you filter the various types listed in the Resource Types window and display only the required ones in the **Add Resource** dropdown list.

1. Navigate to **Admin >> Resource Config >> Resource Types.**
2. To enable resource types filter, click the **Filter** option.



3. In the pop-up box, select the checkbox **Enable Resource Types Filter**, then in the text field below, specify the resource types that you want to be displayed and **Save** changes.

6. Deleting a Resource Type

1. Navigate to **Admin >> Resource Config >> Resource Types.**
2. Select the resource type that is to be deleted and then click **Delete;** confirm delete by clicking **Ok** in the pop-up dialog box.

See also:

- Adding Resources
- Discovering Resources
- Remote Password Reset

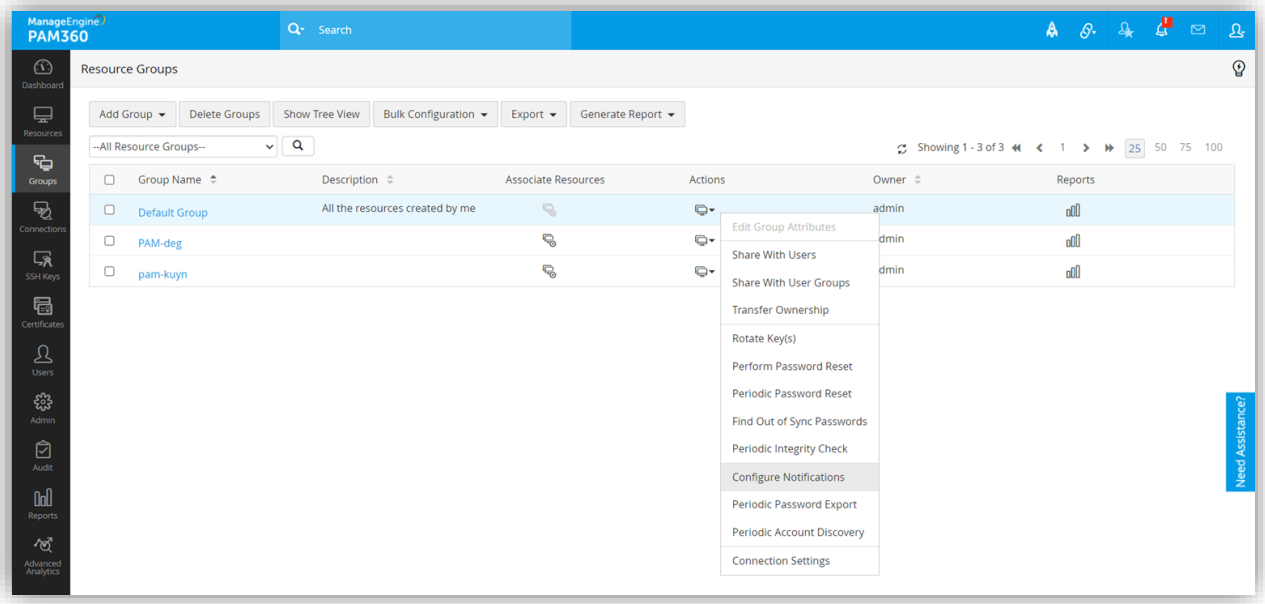
Password Action Notification

With the help of Password Action Notification feature, notifications can be sent out to resource users and/or other users as desired by administrators, whenever any action is performed on a password. For instance, when a password is accessed or altered, password share is changed, password has expired, password policy is violated or passwords are out of sync. You can configure email notifications to be sent out on the occurrence of specific events as mentioned above.

In addition to notifications, especially when password shares are changed or when passwords expire, you can also configure password reset actions to be performed automatically by PAM360. Password Action Notifications can be configured only at a resource-group level.

1. Configuring Password Action Notifications for a Resource Group

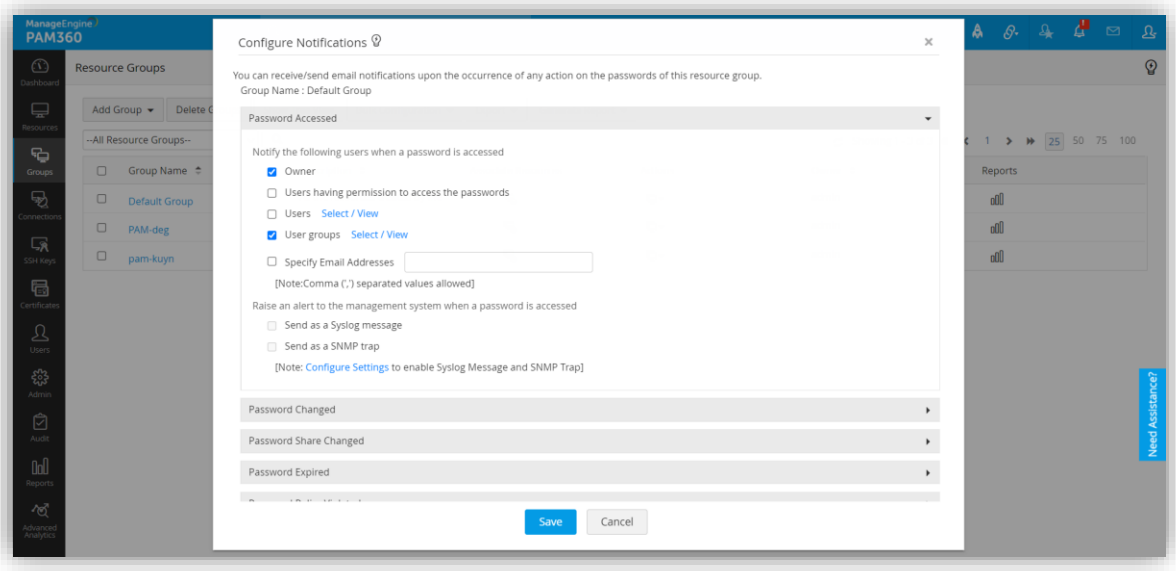
1. Go to Groups tab and click the **Actions** icon against the group for which you need to enable action notifications and select **Configure Notifications** from the dropdown list.



2. A pop-up form will open. Click on the action for which you wish to send notifications. The various password actions are:
    i. **Password Accessed** - When a user views the password.
    ii. **Password Changed** - When a password is changed.
    iii. **Password Share Changed** - When a password share permission is changed.
    iv. **Password Expired** - When the validity of a password ends.

v. **Password Policy Violated** - When a password is in violation to the password policy defined.

vi. **Password Out of Sync** - When passwords stored in PAM360 differ with those of the resources.



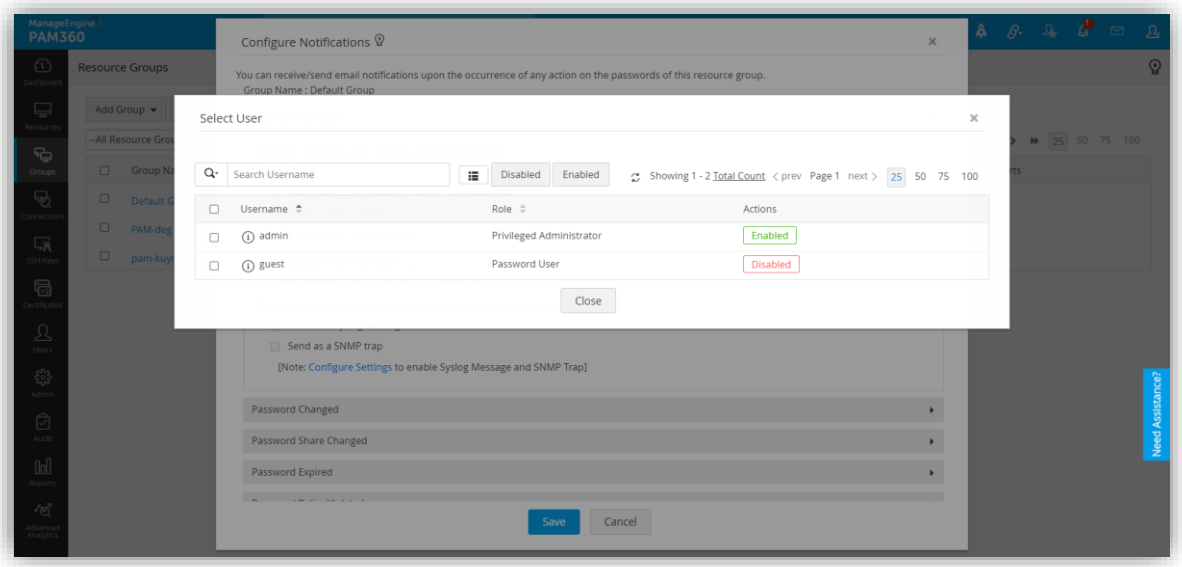
vii. In order to enable notifications for desired password actions, you have to specify the list of recipients for each action as explained below:

viii. **Owner** - owner of the password.

ix. **Users having access to passwords** - users with whom the password has been shared by the owner, with any of the access permissions (View Only / Modify / Full Access). This will apply only to the users who possess access to the password right at the time when this notification is generated.

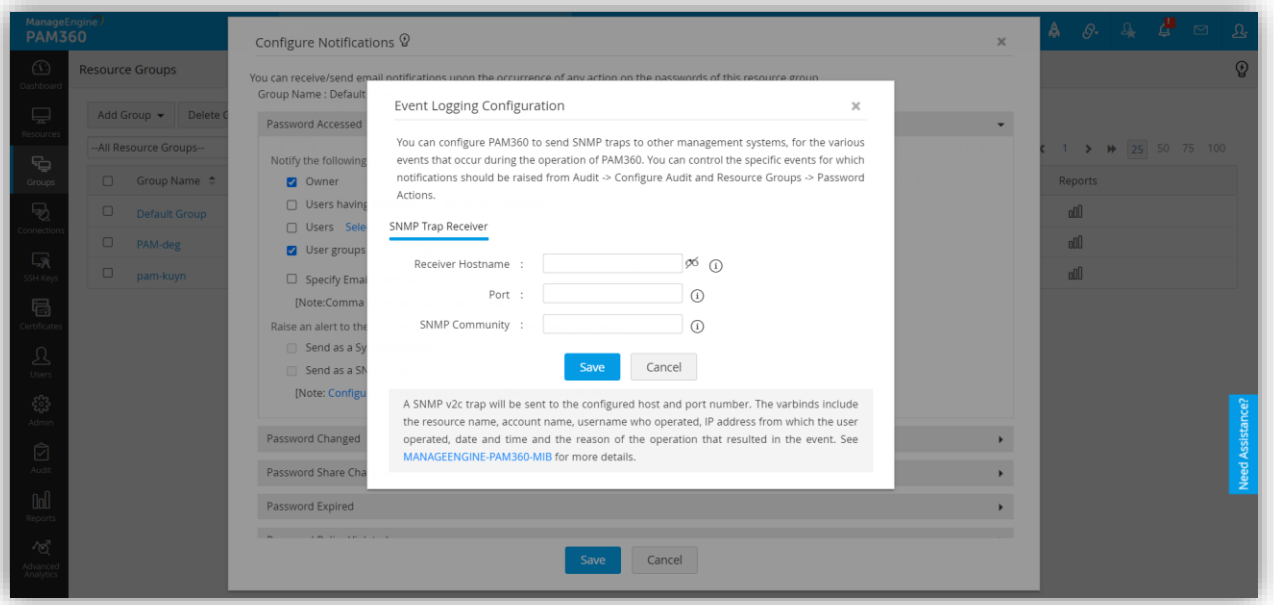
x. **Users -** any other specific user(s) apart from the above two recipients. Desired users can be selected by clicking on the link against this option.

xi. **User Groups -** users from a specific user group(s). Desired user groups can be selected by clicking on the link against this option.



xii. **Specify E-mail Address** - to generate notifications to specified list of email aliases or email addresses. For multiple email IDs, separate the entries with a comma.

3. Apart from the above, you can also generate SNMP Traps to your network management system. Before selecting these options in the Configure Password Actions window, make sure you have globally configured these settings under **Admin >> SNMP Trap**. Refer to related help document section **SNMP Traps**.

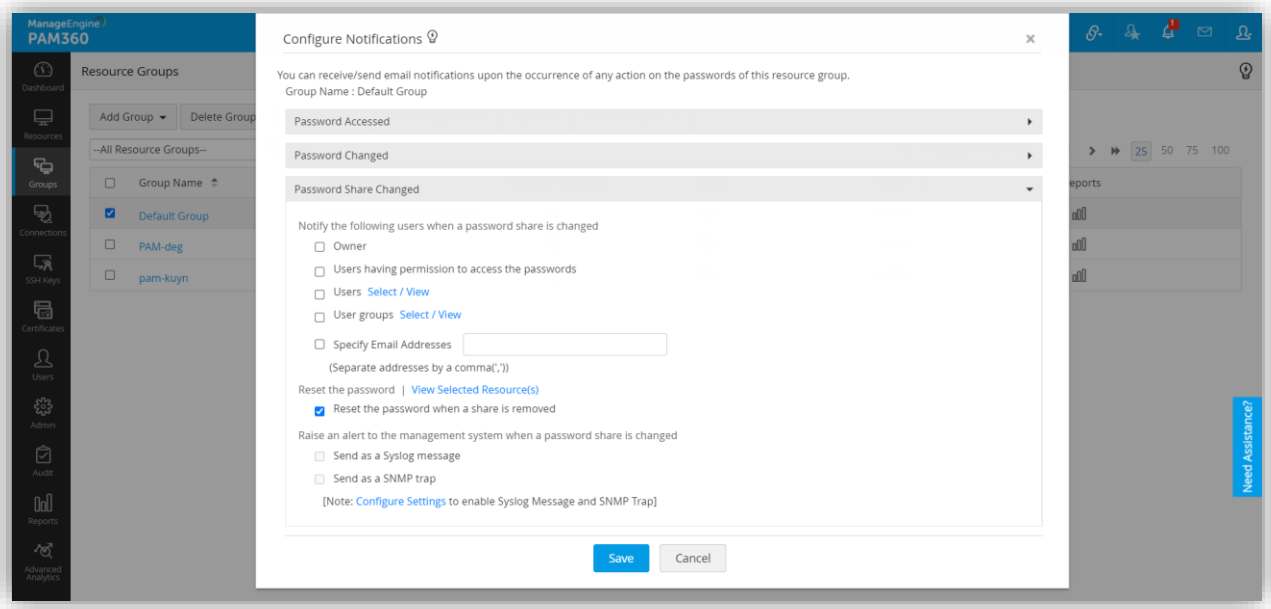


2. Configuring Password Reset Actions along with Notifications

1. In addition to sending notifications, you also have the option to effect automatic

password resets for the actions **Password Share Changed, Password Expired** and **Password Policy Violated.**

2. **For example,**
    - When the share for a password is removed, if you wish to automatically reset the password, you may do so by selecting the checkbox **Reset the password when a share is removed.**
    - When a password expires - in case validity period has been set earlier while defining password policies, you can enable **Reset passwords upon expiry**.
    - When passwords are in violation of their associated policy, enable **Reset passwords upon violation** under **Password Policy Violated.**
3. Once you have enabled desired notification and reset options, click **Save**.



Notes:

1. In all the above actions, email notifications are sent to the specified recipients. You have the option to customize the email content. Refer to **Email Templates** help section for complete details.
2. Password reset action is applicable and performed only for passwords for those that are currently supported and/or correctly configured, using either agent-based or agentless modes.

Password Reset Plugin

PAM360 primarily provides out-of-the-box support to enforce automatic remote password reset for a wide range of commonly used resource types such as Windows local accounts, Windows domain accounts, Linux root accounts, etc. In addition to this, the **Password Reset Plugin** feature enables you to add your own implementation class and enforce automatic password resets for resources that are not supported by PAM360 out-of-the-box such as legacy resource types, in-house applications, etc.

With the plugin, you can also leverage access control for legacy accounts and enable automatic reset of passwords instantly upon usage. This way, the passwords of these accounts will serve as one-time passwords that are reset after every use via the associated plugin.

How does a Password Reset Plugin Work?

Password Reset Plugin is primarily an implementation class that an administrator has to manually add in PAM360. The plugin can be invoked from PAM360 server to connect to a remote resource and carry out a password reset. Password reset plugins can be configured individually for resources that are of user-defined resource types.

When you trigger a password reset for a resource belonging to a custom resource type for which a password reset plugin has been associated, then PAM360 will invoke the interface methods of that plugin. Once invoked, the plugin will first connect to the remote resource and try to reset the password of the resource. If the remote password reset is successfully completed by the plugin, PAM360 will subsequently update the new password it its repository. In addition to this, the plugin helps you verify whether the password of a remote resource is in sync with the one saved locally in PAM360's repository.

Who can Add Password Reset Plugins?

Password Reset Plugins can be added only by users with either the default administrator roles or custom roles that are provisioned with the "Manage Password Reset Plugin" scope under the operation category, "Custom Settings." Besides, all plugins added should also be approved by a second administrator to guard against potential risks associated with invoking arbitrary plugins.

Approving a recently added password reset listener:

If you are an administrator, and another administrator requests you to approve the addition of a password reset plugin, you need to:

1. Navigate to **Admin >> Customization >> Password Reset Plugin.**
2. Click the link under **Approval Status** column, beside the plugin which has to be approved.

The plugin creation, edition, deletion, and approval events are all audited for future reference.

How to Add a Password Reset Plugin?

Summary of Steps

1. Create your Implementation Class
2. Compilation
3. Implementation Tips
4. Configurations in PAM360 Installation

1. Create your Implementation Class

Write a java class by implementing the RemotePasswordReset interface:

```
public interface RemotePasswordReset

 {

   public boolean changeRemotePassword(Properties resetPropsprop) throws Exception;

   public String getErrorMessage() throws Exception;

   public boolean verifyRemotePassword(Properties verifyProps) throws Exception;

   public boolean isDeviceAvailable(Properties verifyProps) throws Exception;

 }
```

Implementation description:

```
// This class provides the methods to implement password reset plugin. You need to
implement the interface

public interface RemotePasswordReset

{

/**

* Used to display the error message while doing the password reset and verification
operations. The output gets reflected in audit trails.

* @return Error message, if password reset is successful, return null. Otherwise, return a
```

proper error message.

*/

public boolean changeRemotePassword(Properties resetProps) throws Exception;

/** Actual function that will be called whenever "change remote password" functionality is triggered

*@param resetProps will contain all the details regarding the account for which password reset is triggered.

* @return Final output that will be sent to PAM360 server.

* {@value true} Success case - Allows the operation to proceed.

* {@value false} Failure case - Denies the operation to proceed.

**/

public String getErrorMessage() throws Exception;

/*** Used to display the error message while doing the remote password reset and verification operations. The output gets reflected in audit trails.

* Return a proper error message.

*/

public boolean verifyRemotePassword(Properties verifyProps) throws Exception;

/** This function will be called whenever "verify remote password" functionality is triggered.

*@param verifyProps will contain all the details regarding the account for which "verify remote password" was triggered.

*@return Final output that will be sent to PAM360 server.

*{@value true} Success case - Allows the operation to proceed.

*{@value false} Failure case - Denies the operation to proceed.

**/

public boolean isDeviceAvailable(Properties verifyProps) throws Exception; }

/** This function will be called before "verify remote password" function to check the accessibility of the device for which verify password was triggered.

*@param verifyProps will contain all the details regarding the account for which verify remote password was triggered.

*@return Final output that will be sent to PAM360 server.

*{@value true} Success case - Allows the operation to proceed.

*{@value false} Failure case - Denies the operation to proceed.

**/

2. Compilation

<PAM360_HOME>\lib folder.

AdventNetPassTrix.jar;

json_simple-1.1.jar;

For Example,

javac -d . -cp AdventNetPassTrix.jar;json_simple-1.1.jar; JiraServerResetImplementation.java - (For Windows)

javac -d . -cp AdventNetPassTrix.jar:json_simple-1.1.jar; JiraServerResetImplementation.java - (For Linux)

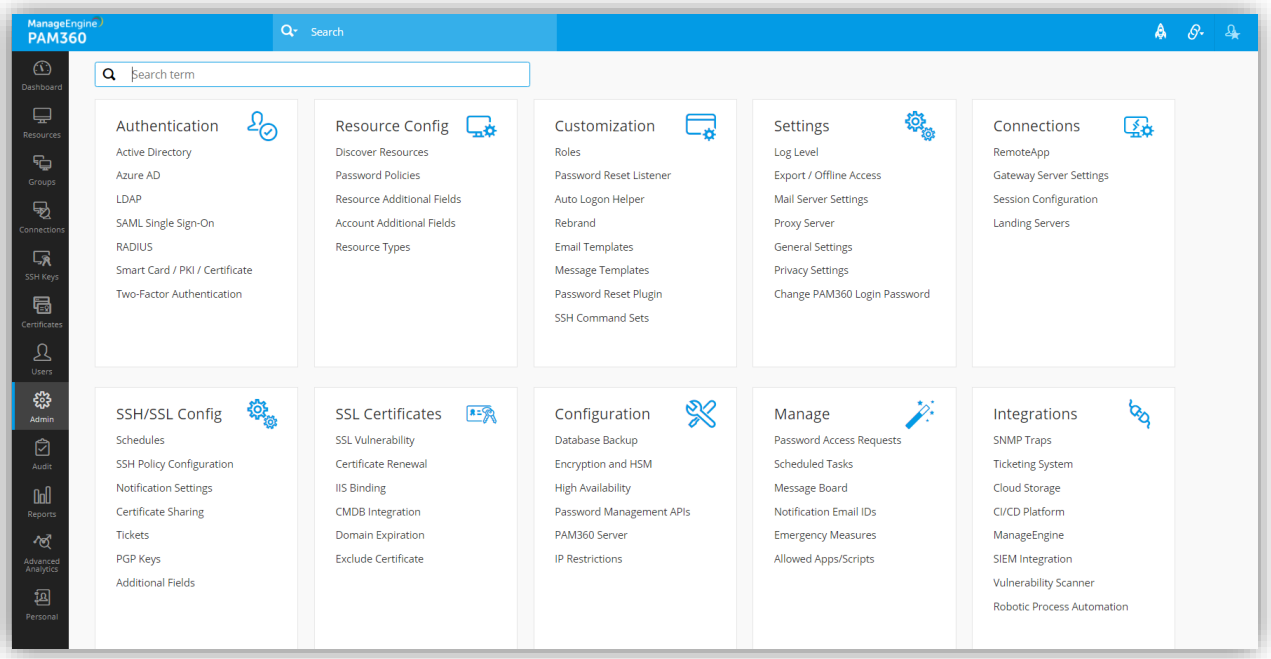
3. Implementation Tips

You can implement your class in such a way that properties of resources (resources and accounts in PAM360) are obtained as arguments. You may obtain the value of any property from the list of keys listed below.

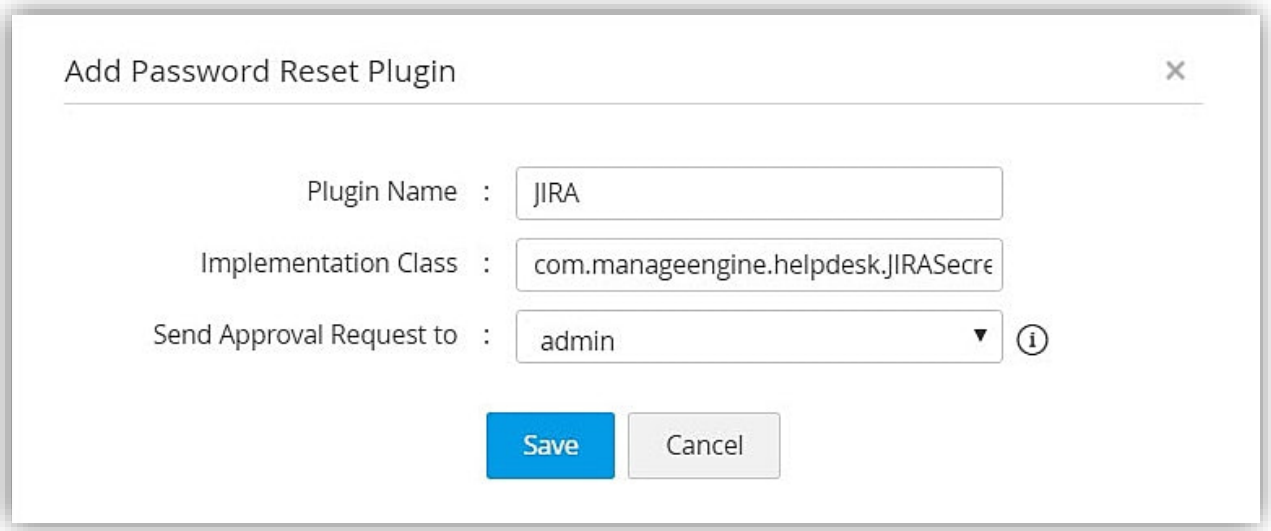
resetProps.get("RESOURCEID");	Returns a Long object of the resource ID.
resetProps.get("ACCOUNTID");	Returns a Long object of the account ID.
resetProps.get("OLDPASSWORD");	Returns a String object of the account's old password.
resetProps.get("NEWPASSWORD");	Returns a String object of the account's new password that has been set.
resetProps.get("RESOURCENAME");	Returns a String object of the resource name.
resetProps.get("DNSNAME");	Returns a String object of the resource's DNS name.
resetProps.get("ACCOUNTNAME");	Returns a String object of the account name.
resetProps.get("OSTYPE");	Returns a String object of the resource's OS type.
resetProps.get("NOTES");	Returns a String object of the notes present under the account details.
resetProps.get("LOGINNAME");	Returns a String object of the login name of the user who initiated the password reset.
resetProps.get("IPADDRESS");	Returns a String object of the IP address of the resource.
resetpresetPropsrops.get("RESOURCEDETAILS");	Returns a ResourceDetails object that contains all other details of the resource.

4. Configurations in PAM360 Installation

1. The first step is adding the password reset plugin to PAM360. Navigate to **Admin >> Customization >> Password Reset Plugin.**



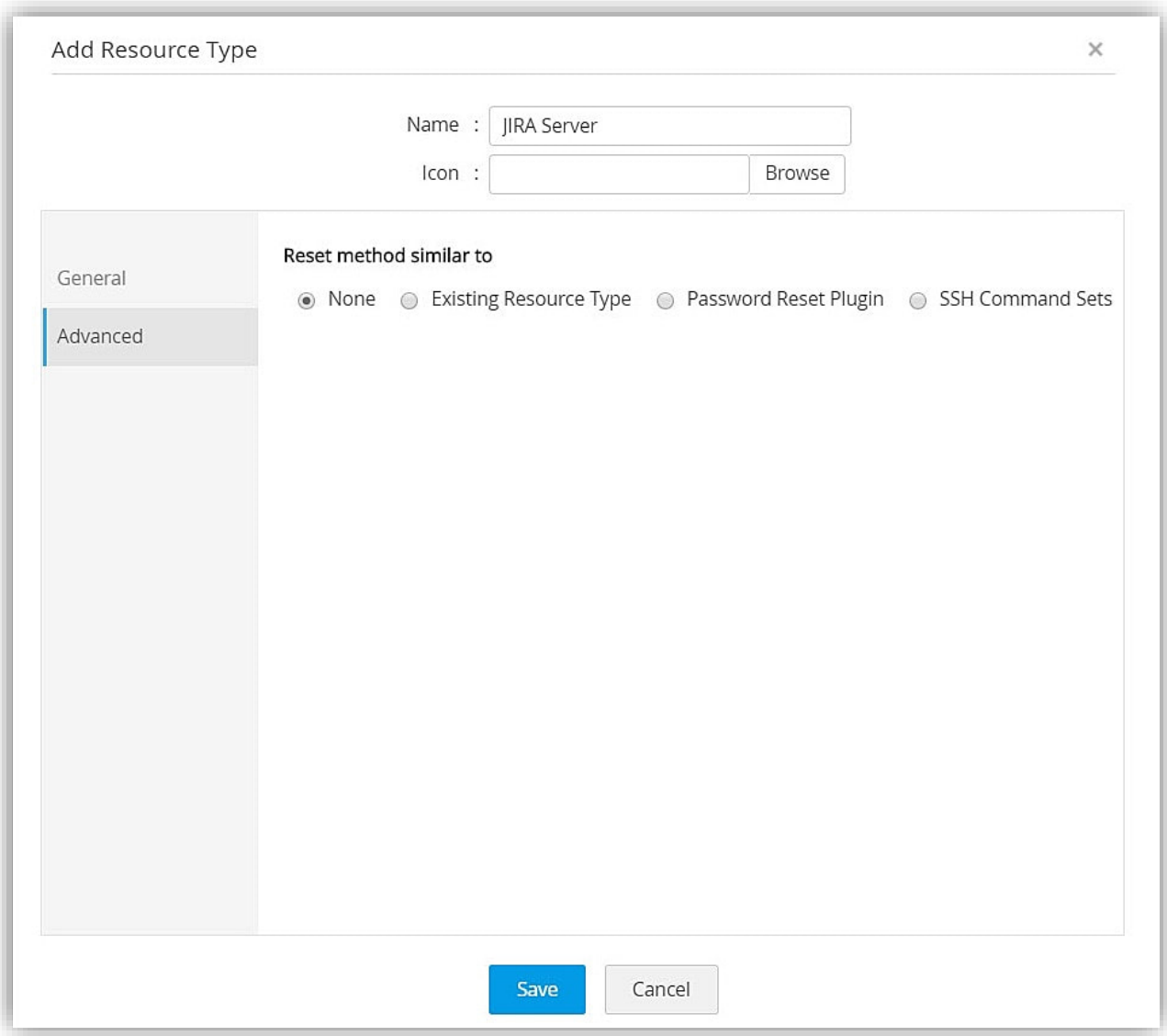
2. Here, click on the **Add Password Reset Plugin** tab.
3. In the dialog box that opens, give a suitable name to your plugin, and specify the name of the implementation class, for example, ''com.manageengine.helpdesk.JIRASecretResetPlugin''.



4. After adding the plugin details, choose an administrator from the drop down list to send the approval request to, and click **Save**.

Note: When you click **'Save'** in the above step, an email will be sent to the chosen administrator regarding the request. In addition to this, all the administrators apart from you will be notified of the request; any of them can approve it by either clicking on the notification or navigating to **Admin >> Customization >> Password Reset Plugin,** and approving it under the **'Approval Status'** column beside the plugin.

5. Once the plugin is approved, you can add the resource type for which you want to use the plugin to reset such resources' passwords. To do so, navigate to the **Resources** tab and click on the **Resource Types** button at the top. Alternatively, you can also add a new resource type by navigating to **Admin >> Customization >> Resource Types.**
6. In the **Resource Types** page, click on **Add** and switch to the **Advanced** tab in the dialog box that opens.



7. Give a suitable name and set an icon (optional) for the custom resource type. Next,

choose the **Password Reset Plugin** radio button.

8. All the approved plugins will be available under the **Reset method similar to**: drop down menu. Choose the required plugin, and click **Save**.
9. This plugin will now be invoked whenever you create a resource of this custom type, configure remote password reset for the resource's privileged accounts, and trigger the reset action.

For further information, refer to this sample implementation class created to reset the user account passwords of Jira Service Desk. You can implement this code in the password reset plugin and reset the passwords of Jira Service Desk.

Password Reset Listener

Password reset is one of the most important functions performed by PAM360 in order to protect the sensitive resources from unauthorized access. PAM360 allows you to carry out similar tasks by invoking scripts or executables, referred to as Password Reset Listeners.

This document walks you through the following topics:

1. What are the Follow up Actions you can do using Password Reset Listeners?
2. How does a Password Reset Listener Work?
3. Who can Add Password Reset Listeners?
4. Custom Listener
5. Reference Implementation
6. Frequently Asked Questions

1. What are the Follow up Actions you can do using Password Reset Listeners?

1. Restart the dependent services immediately after password reset.
2. In case of a Windows service that makes use of an account whose password is reset locally in PAM360 database, the reset listener helps change the respective **stored credentials** (i.e the credentials specified in the **Logon** property) of the windows service.
3. Reset the passwords of Windows scheduled tasks and other associated processes.
4. Carry out password resets for network devices. For instance, if you have added the accounts of network devices as resources, you can first reset the passwords of such accounts locally and then invoke a custom script to connect to the devices and execute the changes in the device as well.

2. How does a Password Reset Listener Work?

Notes:

1. After updating to **build 5570,** the existing password reset listeners will be called as the **Agentless Post Password Reset Listeners.**
2. The **Execution Order** and **Execution mode** for the Password Reset Listener will only be available after **build 5710.**

Password Reset Listener is a script or executable that can be invoked by you whenever the password of an account is being changed or reset in the PAM360 repository. This password reset listener can be invoked even for local password changes and also for resources for which remote password reset is not supported out-of-the-box by PAM360. You can configure listener scripts individually for each resource type including the user defined resource types.

- The password reset listener script will be invoked in a similar fashion as it will be from the command prompt of the operating system from which it is invoked.
- In case, the script needs another program to invoke it from the command prompt, it could be provided as the 'Pre-Command' for that script (for example 'cscript c:\scripts\changepassword.vbs old_password new_password).
- By default, the parameters resource name, dns name, account name, old password, and new password are passed as arguments to the script.
- You can also add additional arguments by specifying them against the text field "Additional Parameters" at the time of invoking the script, in the order specified.

The script runs with the same privilege as the user account running the PAM360 server. For Security reasons, dual control mechanism is implemented, which will ensure that two administrators will see and approve the script before it is invoked by PAM360. PAM360 will not invoke the script unless it has been approved by both the administrators. For example, when an administrator adds or edits the password reset listener, PAM360 will not invoke the scripts unless it has been approved by the other administrator. Thus, the add / edit / delete operations related to password reset listeners can be successfully executed only with the approval of two administrators in PAM360. The actions are also audited for future references.

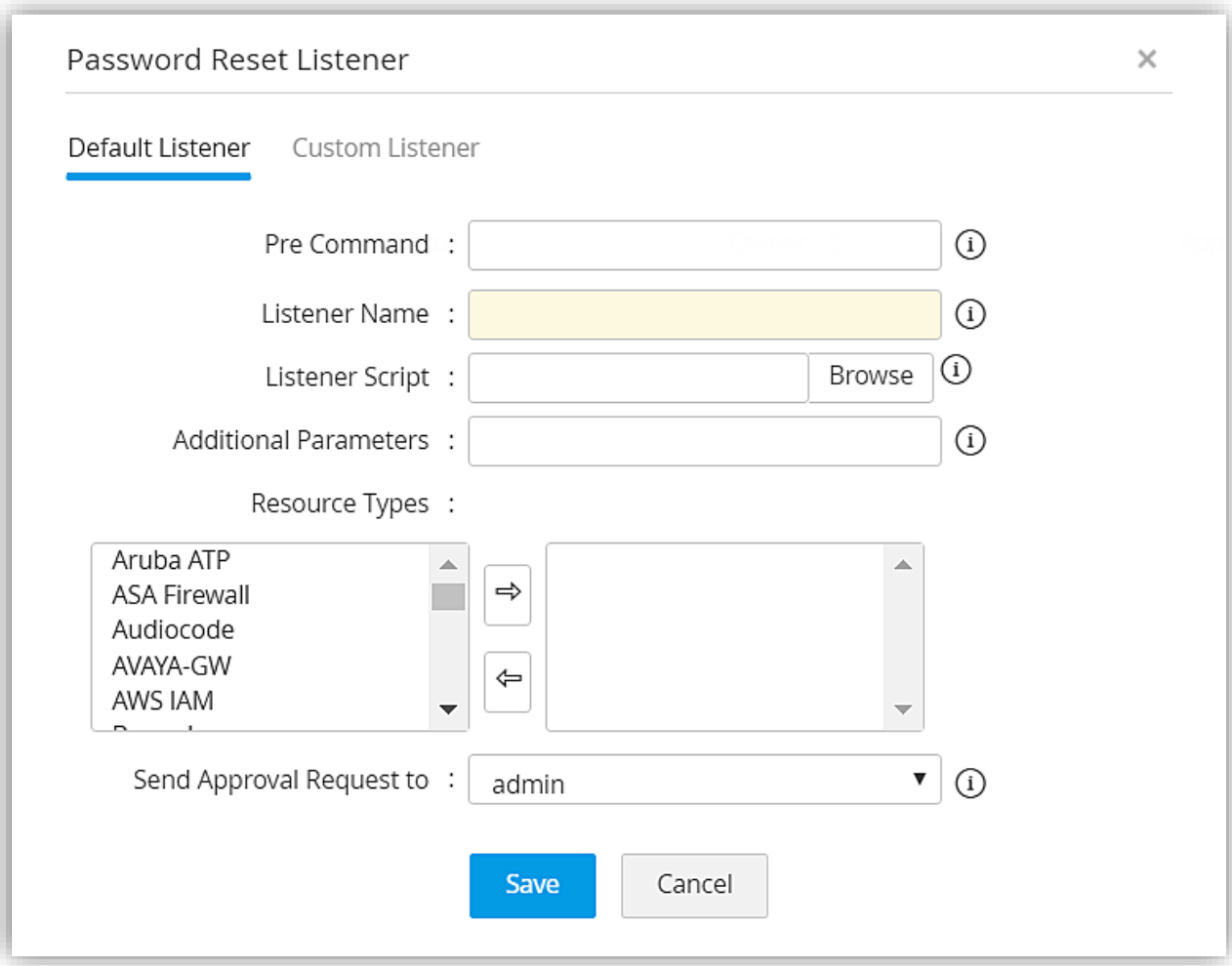
The password reset listener is invoked from a separate thread, so it does not impact the password reset process of PAM360. The listener scripts added will be stored in the same database as the other information. This provides security and also backup, if it is configured for PAM360 database

To set up password reset listener,

1. Navigate to **Admin >> Customization >> Password Reset Listener**.
2. The Password Reset Listener window will open. Click **Add Listener**.
3. As mentioned above, the password reset listener script will be invoked in a similar fashion as it will be from the command prompt of the operating system from which it is invoked. In case, the script needs another program to invoke it from the command prompt, it could be provided as the **Pre-Command** for that script **(for example 'cscript c:\scripts\changepassword.vbs old_password new_password)**.
4. Enter a name for the listener. Next, browse and add the listener script.
5. By default, parameters such as resource name, dns name, account name, old password, and new password are passed as arguments to the script. In case you require to pass additional arguments, add additional arguments by specifying them against the text

field **Additional Parameters**. The additional parameters supplied will be passed to the script in the order given, at the time of invoking the script.

6. You can also specify the resource types for which the changes to be applied and send approval request to the other administrator.
7. After adding necessary details, select an administrator from the drop down for sending an approval request. A mail will be sent to the selected administrator intimating the approval request.
8. Click **Save.**



3. Who can Add Password Reset Listeners?

The listeners can be added only by PAM360 administrators. In addition, all listeners added should also be approved by a second administrator to guard against potential risks associated with invoking arbitrary scripts. So, once a listener is created and saved by an admin, the same will be sent to another administrator for their approval. A mail will be sent to the second administrator intimating the approval request.

To approve a recently added password reset listener,

If you are an administrator, and another administrator requests you to approve a listener, then you need to;

1. Navigate to **Admin >> Customization >> Password Reset Listener.**
2. Click the link under **Approval Status** column, beside the listener which has to be approved.
3. Once you approve, the listener will take effect.

The listener creation, edition, deletion, and approval events are all audited.

4. Custom Listener

In addition to reset listeners, PAM360 allows you to provide your own implementation through "custom listeners". The custom listener basically lets you provide your own listener implementation class, which offers you complete flexibility to execute any post password reset follow-up action, instead of just letting PAM360 execute the listener script provided by you. It offers you complete flexibility to execute any post password reset follow-up action.

How to create a custom listener?

Summary of steps involved in custom Listener creation:

Step 1: Write your own implementation class

Implement PAM360ListenerInterface (more details in the reference implementation below).

Step 2: Configuration in PAM360 GUI

Add entries for the implementation class in PAM360 GUI.

Step 3: Archive your implementation class as .jar and put it into PAM360

Step 4: Restart PAM360

5. Reference Implementation

To explain how you can have your own implementation for listener in PAM360, we are providing a reference implementation below. This implementation is for executing PowerShell scripts with reset listener.

Step 1 - To write your own implementation class:

You need to write your own class implementing **PAM360ListenerInterface.java** as explained below.

```
public interface PAM360ListenerInterface {
static final Logger LOG =
Logger.getLogger(PAM360ListenerInterface.class.getName());
public String executeListener(Properties resourceProps, Properties
accountProps, String listenerFilePath, String oldPassword) throws
Exception;}
```

You can implement your class in such a way that properties of resources (resources and accounts in PAM360) are obtained as arguments. For example, if you need 'Resource Name', you may have to do it as below:

```
resourceProps.get("RESOURCENAME")
```

You may obtain the value of any propery from the list of keys listed below.

Resource Properties (resourceProps)

- **RESOURCENAME -** Name of the Resource added in PAM360
- **IPADDRESS -** DNSName or IPAddress of the Resource
- **RESOURCEURL -** Resource URL configured for the resource
- **DOMAINNAME -** Domain Name if the Resource is of type WindowsDomain
- **SSHPORT -** SSH Port if the device can be connected over SSH
- **RESOURCEDESC -** Description of the resource
- **LOCATION -** Location of the Resource
- **DEPARTMENT -** Department to which the resource belongs to
- ALL RESOURCE CUSTOM COLUMN NAMES (Label name will be the key)

Account Properties (accountProps)

- **DESCRIPTION -** Account's description
- **LOGINNAME -** Login Name of the userAccount added into PAM360
- **PASSWORD -** Password for this user account
- **DOMAINNAME -** Domain Name if the account added is a domain account
- **COMPLIANTSTATUS -** Provides a status whether the password is in compliant with the Password Policy configured in PAM360
- **COMPLIANTREASON -** Reason, if the password is not compliant with the Password Policy
- **EXPIRYSTATUS -** Status of expiry of the account's password
- **PASSWRDSYNCSTATUS -** Provides information if the password is in sync with the

password that is set on the remote resource

- ALL ACCOUNT CUSTOM COLUMN NAMES (Label name will be the key)

Other Arguments

- **listenerFilePath** - The path of the script/file that you want to invoke as listener. You also have the option to provide the script/file while configuring the listener in PAM360 in Step 5.
- **oldPassword** - Passing the old password to the implementation class to carry out password reset

Sample implementation to execute PowerShell script

```
public class PowerShellListener implements PAM360ListenerInterface {
public String executeListener(Properties resourceProps, Properties
accountProps, String listenerFilePath, String oldPassword) throws Exception {
String message = "Executed Successfully";// used for audit reason
// got the properties
// call the powershell script}}
```

Step 2: Configuration in PAM360 GUI

Add entries for your implementation class in PAM360 GUI. To do this, navigate to **Admin >> Password Reset Listener >> Add Listener** and in the GUI that opens, click the tab **Custom Listener** and then click the link **Add New**. Enter the following details:

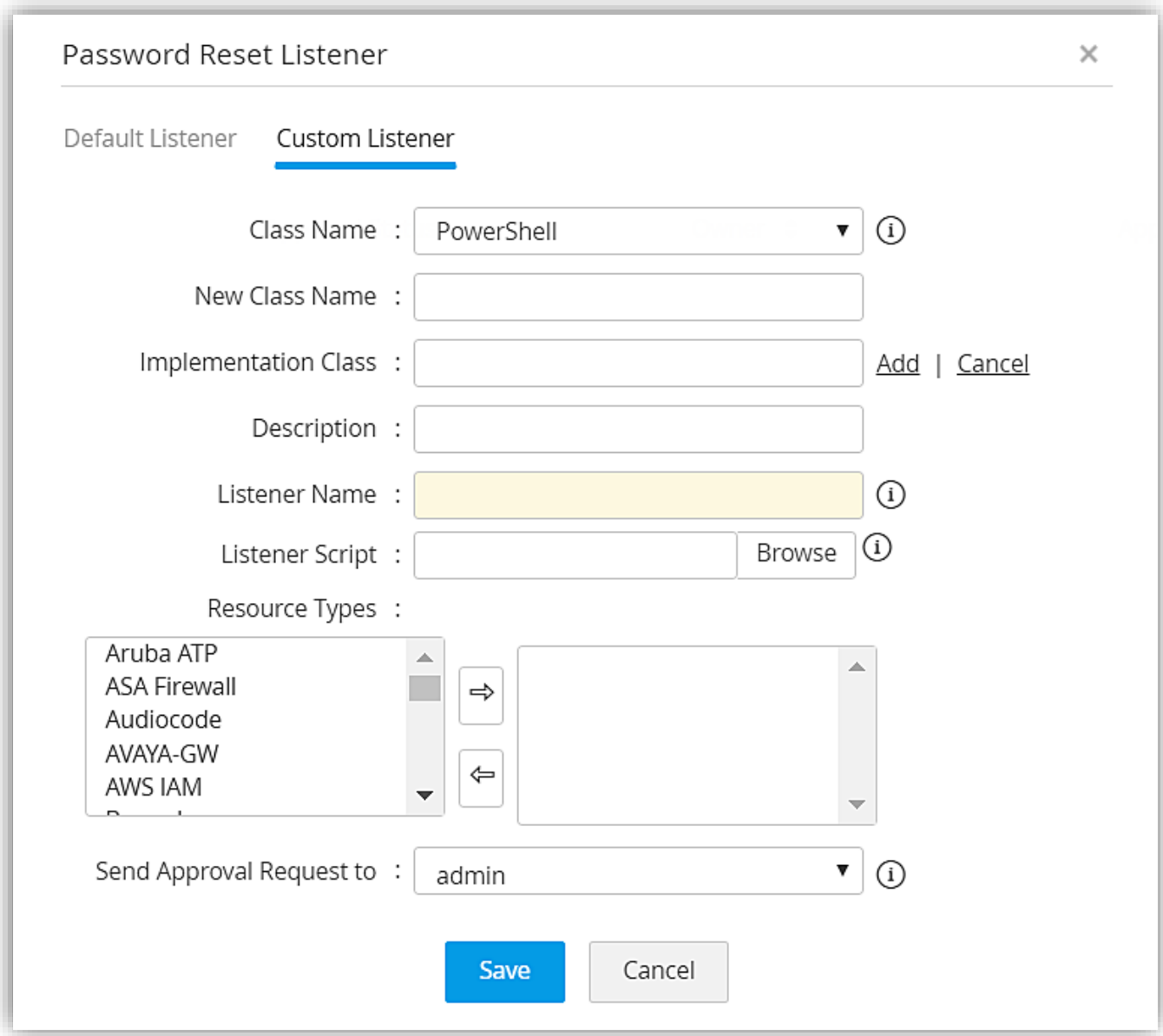
1. Navigate to **Admin >> Customization >> Password Reset Listener.**
2. Click **Add Listener.**
3. In the pop-up form that opens, click on **Add new** under **Custom Listener** tab and enter the details.
4. Enter the name of the new implementation class and add your own implementation class.
5. Add entries for your implementation class and also give information about your implementation class in description.
6. Enter a name for the listener script with appropriate extension and then browse and locate the listener script.
7. You can also specify the resource types for which the changes to be applied and send approval request to the other administrator.
8. Select an administrator from the drop down for sending approval request. A mail will be sent to the administrator intimating approval request.
9. Click **Save.**

Step 3: Archive your implementation class as .jar and put it into PAM360

You need to convert your implementation class as **.jar** and put it into **<PAM360-Installation Folder>/lib** directory.

Step 4: Restart PAM360

After completing the above steps, you need to restart PAM360 to give effect to this implementation.



Password Policies

Password policies help you define the structure and complexity of passwords to be used. You can either make use of the predefined policies or create new policies to suit the needs of your organization. Once you define the policy, PAM360 enforces that policy and reports on violations. The inbuilt password generator will generate passwords based on the policy defined.

This document walks you through the following topics:

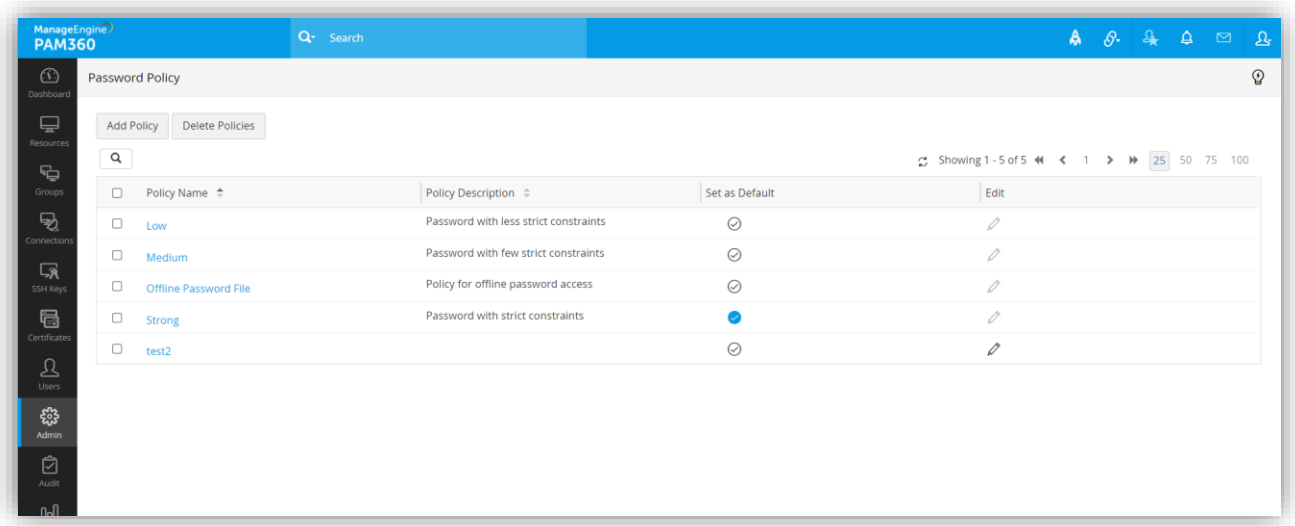
1. Default Password Policies
2. Customizing Password Policies
3. Creating your Own Password Policy
4. Applying Password Policy to Resources in Bulk
5. Enforcing Password Policy during Resource/Account Creation
6. Enforcing Password Policy from General Settings

1. Defult Password Policies

Password policy for PAM360 can be centrally managed from the **Admin** tab, **Admin >> Resource Config >> Password policies**. By default, PAM360 lists four policies and these policies cannot be edited or deleted. The default policies are:

- **Low -** Password with less strict constraints.
- **Medium -** Password with few strict constraints.
- **Strong -** Password with strict constraints.
- **Offline password file -** Policy for offline password access.

Apart from the default policies, you can also create your own password policy based on your requirements.

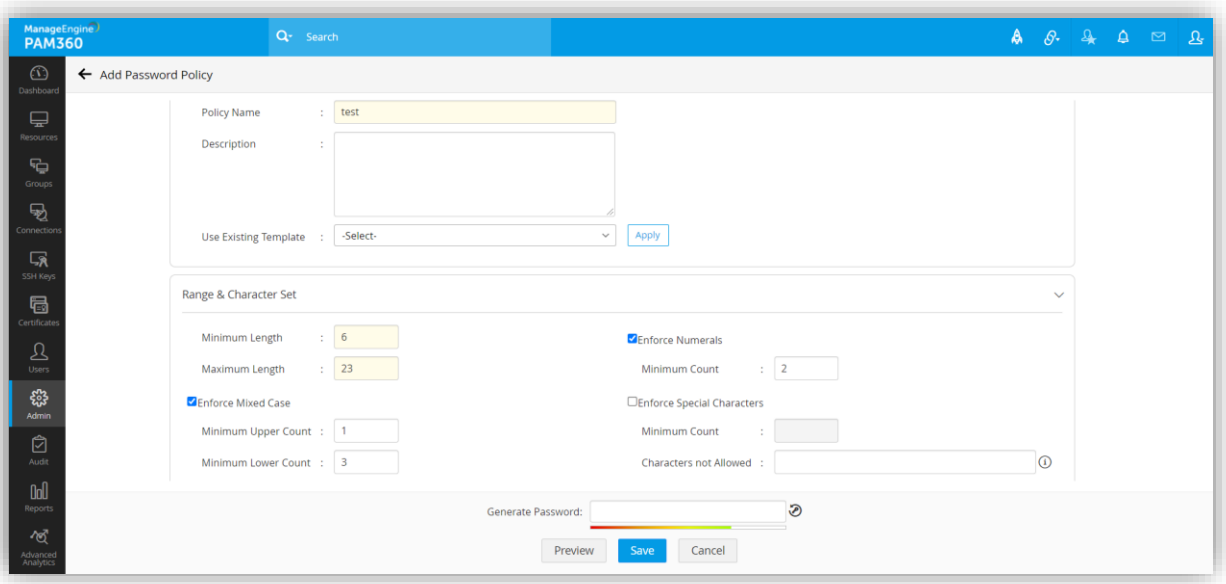


2. Customizing Password Policies

1. Navigate to **Admin >> Resource Config >> Password policies.**
2. You can select any of the policy as default policy by selecting the **set as default** icon against the desired policy.
3. After setting default policy, if a user tries to change the password, the default policy will be enforced and the user will be forced to enter a password as per the policy.

3. Creating your Own Password Policy

1. Navigate to **Admin >> Resource Config >> Password policies.**
2. Click **Add** policy.
3. Enter the **Policy Name** and **Description.** You can also select from the existing templates and **apply** them here.
4. Under **Range & Character Set:**
    i. Mention the **Minimum** (4) and **Maximum** (255) **Length** of the password.
    ii. Select **Enforce Numerals** and mention the **Minimum Count** of numerals to be used in the password.
    iii. Select **Enforce Mixed Case** and mention the **Minimum Upper Case** and **Minimum Lower Case** letters to be used in the password.
    iv. Select **Enforce Special Characters** and mention the **Minimum Count** of characters to be used in the password. You can also mention the **Characters not Allowed** in the password.



5. Under **Words Usage:**

   i. Select the checkbox, **Password should not contain dictionary words** to not allow dictionary words as the password. **Example:** *apple, ranger, etc.*

   ii. You can also **choose** from the existing dictionaries. Click **Manage** to manage the dictionary files.

      a. In the pop-up that appears, mention **Dictionary name**, select the dictionary **file** (.txt) to be imported and click **Add.** You can add upto 5 dictionaries. Click here to download some of the recommended dictionaries.

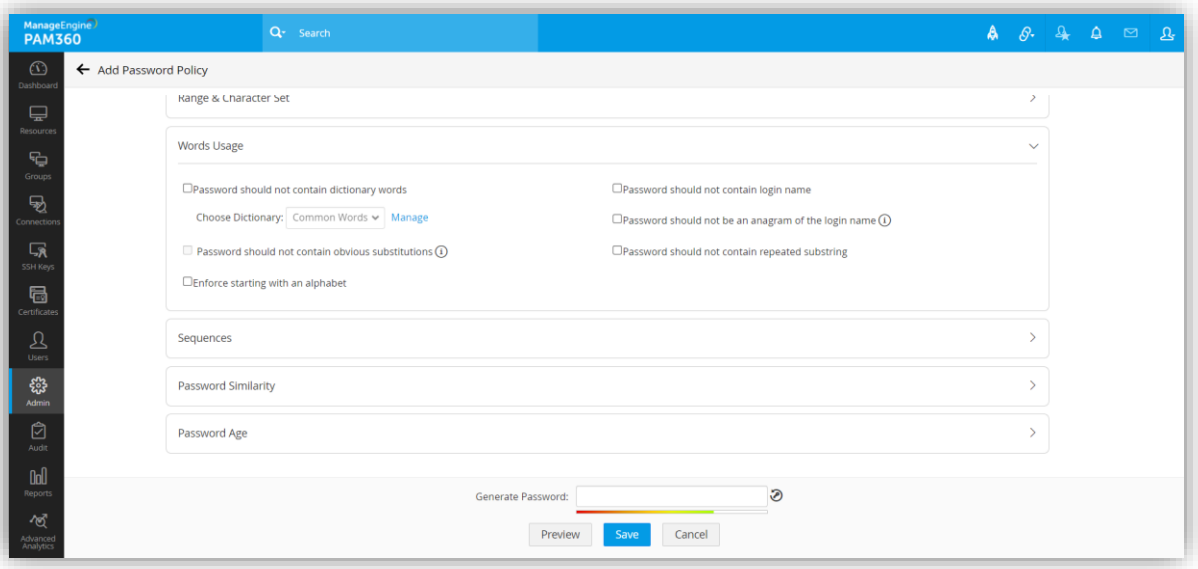
      b. Select the checkbox **Password should not contain obvious substitutions** to not allow obvious substitutions. **Example:** *@pple, r4nger, etc.*

   iii. Select the checkbox **Enforce starting with an alphabet** to allow only the passwords that begins with an alphabet. **Example:** *Awed28.*

   iv. Select the checkbox **Password should not contain login name** to not allow username as password.

   v. Select the checkbox **Password should not be an anagram of the login name** to not allow password that is an anagram of username. **Example:** *username: admin; password: dmain.*

   vi. Select the checkbox **Password should not contain repeated substring** to not allow password with repeated substrings. **Example:** *testtest.*



6. Under **Sequences:**

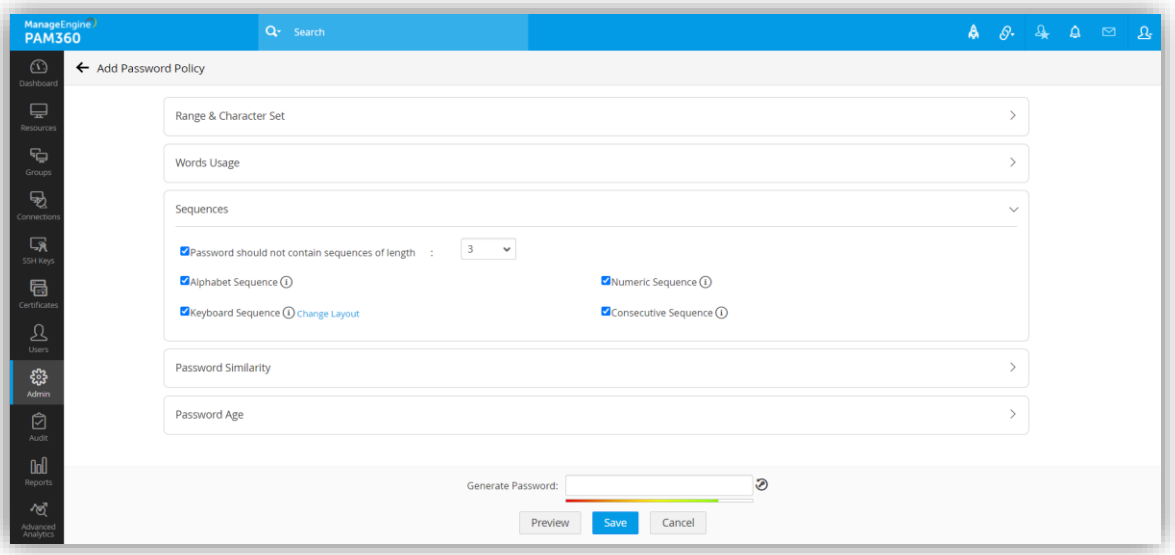
   i. Select **Password should not contain sequences of length** to not allow a password with sequences and mention the **sequence length.**

   ii. Select the checkbox to not allow **Alphabet Sequence** and their reverse as the password. **Example:** *abcd, hgfe, etc.*

   iii. Select the checkbox to not allow **Keyboard Sequence** as the password. Click **Change Layout** to choose the layout of the keyboard. **Example:** *qwerty, asdfg etc.*

   iv. Select the checkbox to not allow **Numeric Sequence** and their reverse as the password. **Example:** *1234,8765, etc.*

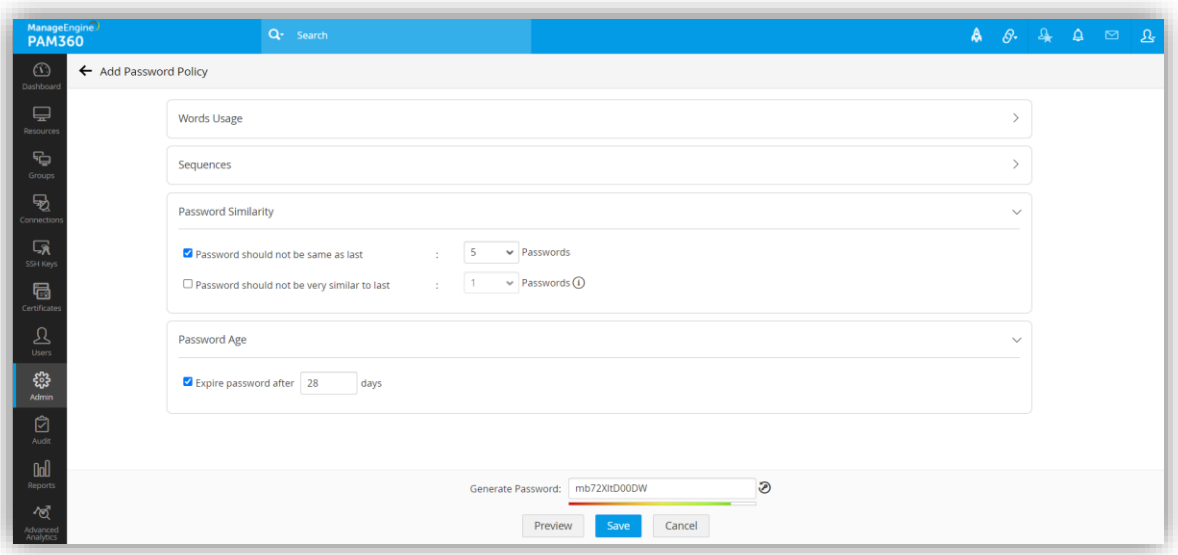
   v. Select the checkbox to not allow **Consecutive Sequence** of letters, numbers or symbols as the password. **Example:** *aaa, 111, &&&, etc.*



7. Under **Password Similarity:**

    i. Select **Password should not be same as last** to not allow previously used passwords. You can restrict upto ten (10) previous passwords.

    ii. Select **Password should not be very similar to last** to not allow password similar to previously used passwords. You can check with upto ten (10) previous passwords. **Example:** *anem28, bnem28*.

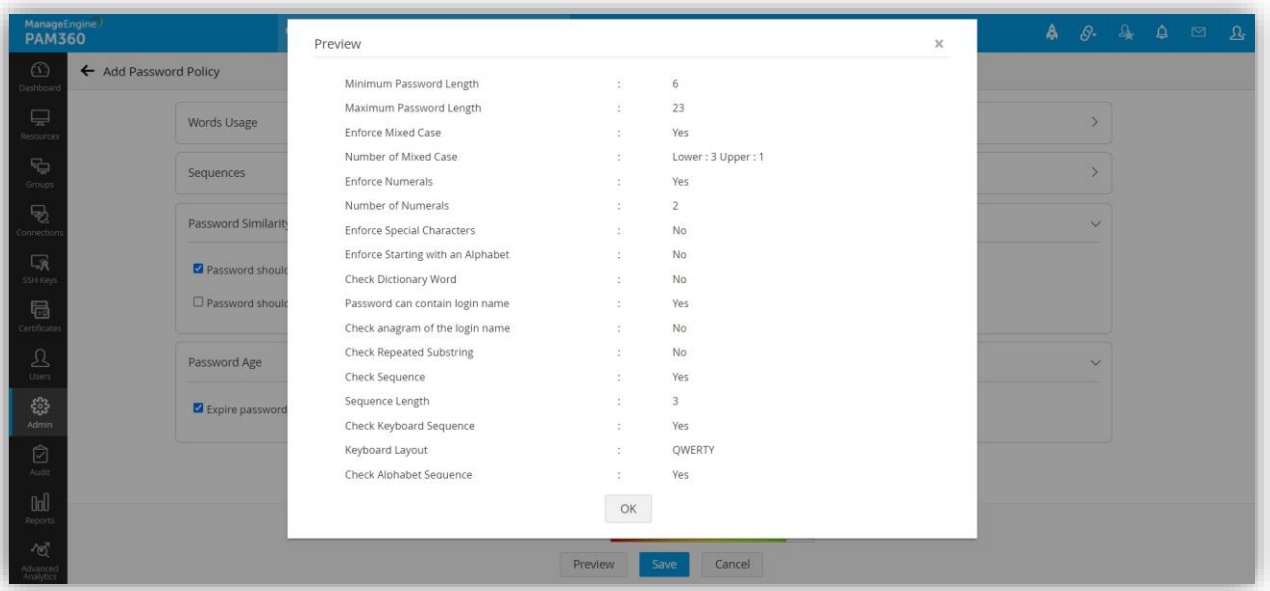


8. Under **Password Age:**

    i. Select **Expire password after** and mention the number of **days** after which the password should expire.

9. Click **Generate Password** icon to generate a sample password with the selected constraints.

10. Click **Preview**. A pop-up appears displaying the selected password constraints.

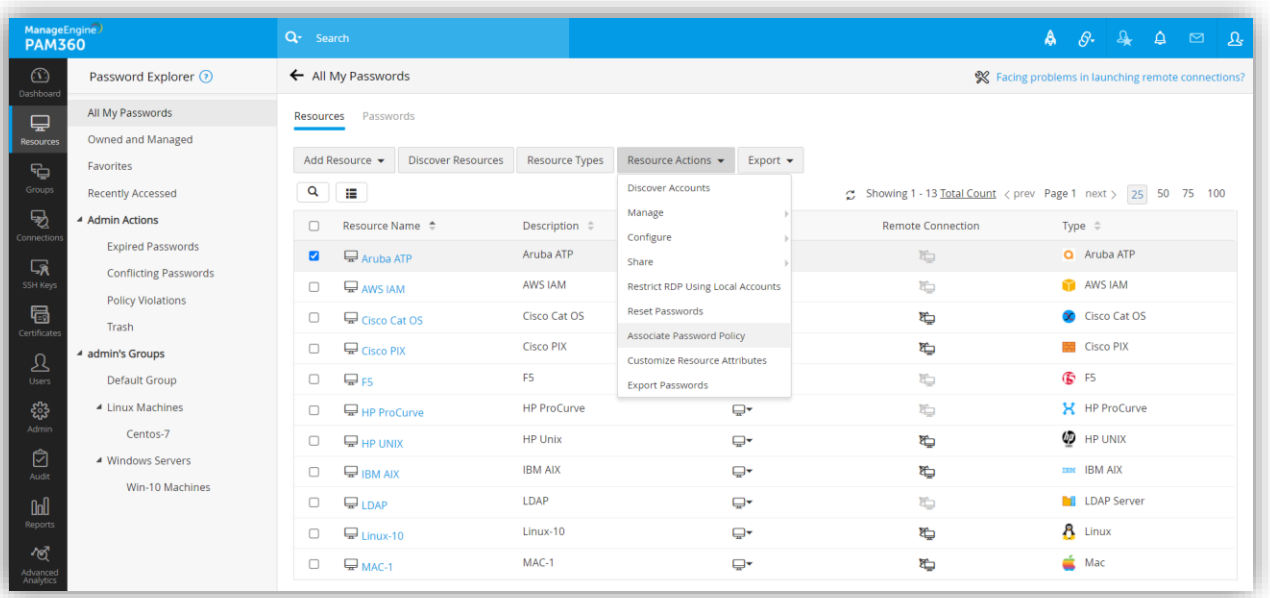


11. Click **Save.**

Now, you have successfully created your own password policy based on your requirement.

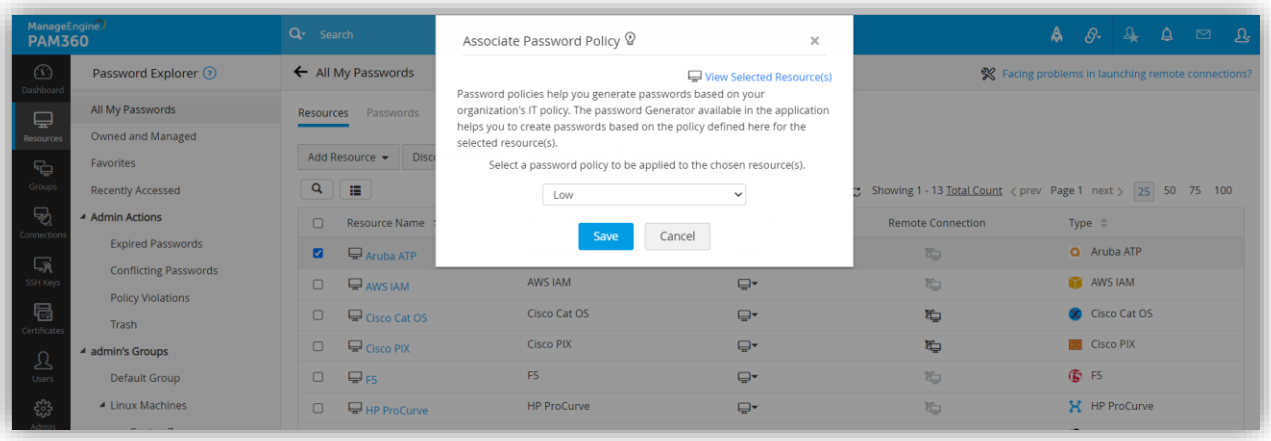
4. Applying Password Policy to Resources in Bulk

1. Navigate to **Resources** tab.
2. Select the resources for which you wish to apply the same password policy.



3. Click **Resource Actions** and select Associate Password Policy from the dropdown.
4. In the pop-up form that appears, select the **Password policy to be applied to the chosen**

resource(s) from the drop down and Click **Save**.



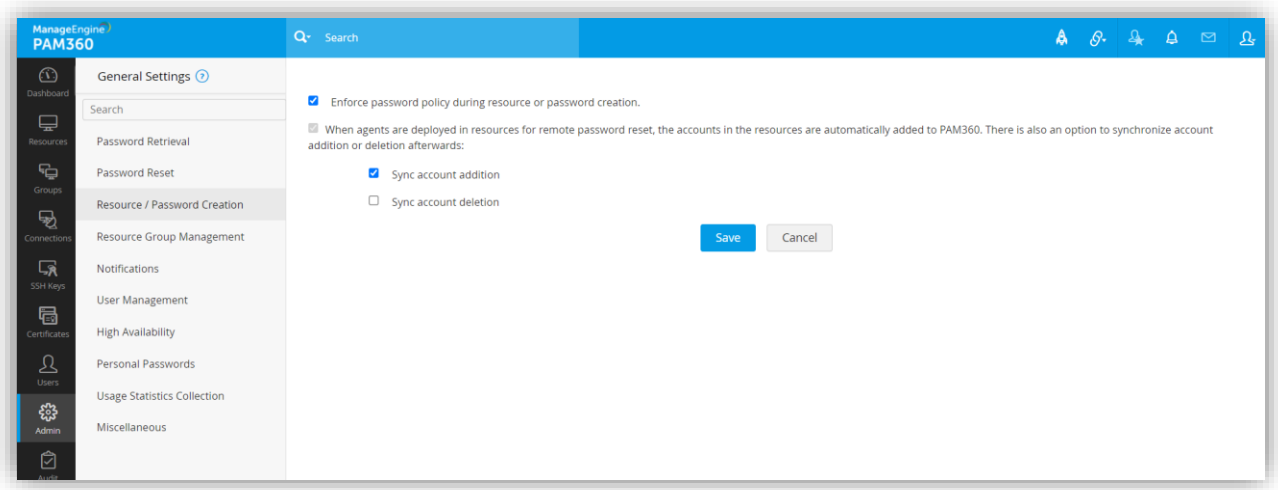
After the completion of selection of password policy, the chosen password policy will be applied to all the selected resources in bulk. In case, any of the chosen resources had already been with a password policy, this action would simply overwrite the previous policy.

5. Enforcing Password Policy during Resource/Account Creation

In normal scenarios, PAM360 can check the passwords stored in the repository for compliance to the policy specified and report violations. If you want to enforce the password policy at the time of creation itself, you need to switch on a configuration in **General Settings**. To know more about general settings, click here.

6. Enforcing Password Policy from General Settings

1. Navigate to **Admin >> Settings >> General settings.**
2. In the UI that opens with a list of options, select **Resource / Password creation** from the left pane.
3. By default, password policy gets enforced only at the time of password change. If you wish to enforce policy compliance at the time of resource or account addition itself, then click the checkbox **Enforce password policy during resource or password creation.**
4. Once you click this, you will be permitted to add your resource or account only if the password is in accordance with the policy defined.


ManageEngine
PAM360
Search
Dashboard
Resources
Groups
Connections
SSH Keys
Certificates
Users
Admin
Audit
General Settings
Search
Password Retrieval
Password Reset
Resource / Password Creation
Resource Group Management
Notifications
User Management
High Availability
Personal Passwords
Usage Statistics Collection
Miscellaneous
Enforce password policy during resource or password creation.
When agents are deployed in resources for remote password reset, the accounts in the resources are automatically added to PAM360. There is also an option to synchronize account addition or deletion afterwards:
Sync account addition
Sync account deletion
Save
Cancel

Password Access Control Workflow

Access control is a strategy that verifies the authenticity of users and ensures that they have suitable privileges to perform a task or access data. To put it simply, access control is a way of selectively restricting access to sensitive data. An effective access control strategy comprises of two major components: authentication and authorization. Through authentication, one can verify if a person is who they claim to be. However, authentication alone is not sufficient to protect data, and an additional layer called authorization, which determines whether a user is permitted to access the data or perform an action they are attempting, is mandatory. Authentication and authorization are the two key components that are essential to strengthen data security in an organization.

Password Access Control in PAM360

PAM360 provides an access control mechanism that allows administrators to grant password access to users for a specific period. Admins can start granting exclusive privileges once a password is ready to share, and only one user is allowed to use a particular password at a single point of time. Additionally, administrators can provide just-in-time (JIT) privilege elevation to local user accounts in a Windows resource. For example, assume, "**dbuser**" is a local account in a Windows resource added to PAM360, and this account does not have any admin privileges. Using the JIT privilege elevation feature, admin can elevate **dbuser**'s privileges equal to that of an admin or any other privileged user.

You will learn the following topics concerning Password Access Control workflow in this document:

1. The Password Access Control workflow
2. Precedence in Password Access Control
3. Executing the Password Access Control workflow
   - 3.1 Access Control at Resource level
   - 3.2 Access Control at Account level
     - 3.2.i Approval Administrators
     - 3.2.ii Excluded Users
     - 3.2.iii Miscellaneous Settings
     - 3.2.iv Auto Approval
     - 3.2.v JIT Privilege Elevation
   - 3.3 Viewing Access Control Details
4. Use case scenarios
5. Message Templates
6. Glossary of Terminologies

1. The Password Access Control Workflow

Once the password access control is enforced for a resource or an account, the following workflow is invoked for password access attempt by the users:

1. A user needs access to a password that is shared with them.
2. The user makes a request to access the password.
3. The request is sent to the designated administrator(s) for approval. If more users require access to the same password, all the requests will be queued up for approval.
4. If the administrator does not approve the request within the stipulated time, the request becomes void. In case the user has specified a particular time frame for password access, then the request becomes void after the user-specified stipulated time.
5. If the request is rejected by even one of the designated administrators, it becomes void.
6. If the administrator approves the request, the user will be allowed to check out the password only during the stipulated time, or at the time set by the administrator during approval. In case more than one administrators have to approve a password request, the user will be allowed to check out the password only after all of the designated administrators have approved the request.
7. Once the user checks out the password, it will be available exclusively for their use till the stipulated time.
8. If any other user requires access to the same password concurrently, they will be provided access only after the previous user checks in the password. This rule applies to all types of user roles in PAM360, including administrators, password administrators and owner of the password.
9. Administrator can also revoke password access for the user any time. The password will be forcefully checked-in during such circumstances, denying access to the user. Once the user finishes their work, the password will be reset.
10. While granting a temporary exclusive access to a user, you can enable administrators to view the password concurrently by selecting the option **Enforce users to provide reason for password retrieval** under **Admin >> Settings >> General Settings.**

> **Note:** The access control workflow does not override the password ownership and sharing mechanism of PAM360. Rather it is only an enhanced access control mechanism. Normally, when a password is shared with a user, the user will be able to view the password directly. Now, with the password access control mechanism, the user will have to request access to a password, even if they have access to it.

2. Precedence in Password Access Control

Account level access control configuration takes higher precedence over Resource level access control configuration as explained below in detail:

1. When Access Control settings are enforced on a resource, the settings are automatically applied to all the accounts within the resource. However, when Account level access control settings are applied to an individual account within the resource, it overrides the resource level access control settings that were previously applied for the selected account.
    i. Let's assume, **PAM360-win10** is a resource with several accounts under it. When access control mechanism is enforced for the resource PAM360-win10, the settings are applied to all accounts under PAM360-win10 automatically. In case, if Account Level access control is applied for a user account, say **Administrator**, within the resource PAM360-win10, that action will override the resource level access control that was earlier applied for the user account **Administrator**. However, the access control settings for the rest of the accounts within the resource will remain unchanged.
2. If resource level access control settings are deactivated, it will not affect the account level access control configurations within the same resource.
3. If account level access control settings are deactivated for an account, then the resource level access control, if configured, will be applied to the account automatically.
4. Account level access control settings come in handy when certain accounts within a resource require a higher level of security.
    i. Let's assume **CentOS-1** is a resource with several accounts under it. Access control mechanism is enforced for CentOS-1 and settings are customized in a way that it requires the approval of one authorized administrator to access the resource; the same settings will be applied to all accounts under the resource. However, the user account **Root** under the resource requires better security. In this case, account level access control configuration can be applied to **Root** so that it requires approval of at least five authorized administrators to gain access to its password. Modifying access control configuration for Root will not affect the configuration done for CentOS-1 and the other accounts under the resource.

3. Executing the Password Access Control Workflow

Follow the below steps to implement password access control for a resource or an account:

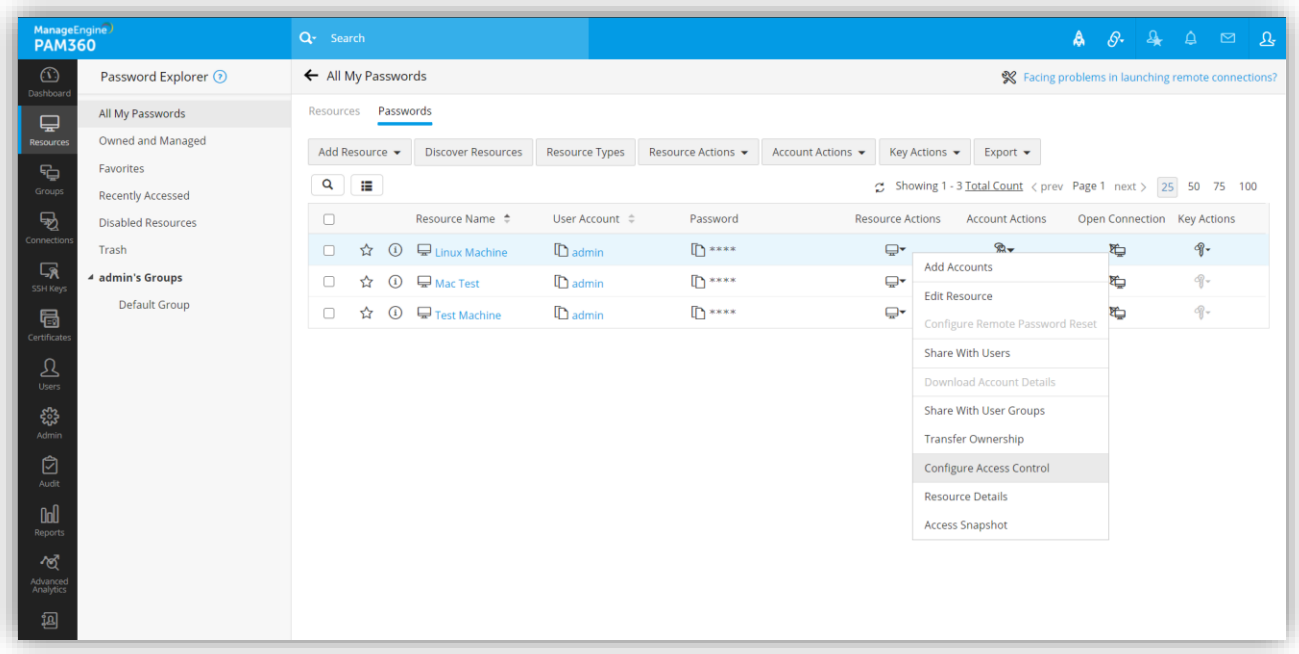
3.1 Access Control at Resource Level

3.2 Access Control at Account Level

3.3 Viewing Access Control Details

3.1 Access Control at Resource Level

1. To implement access control for multiple resources, navigate to the **Resources** tab and select the resources for which you wish to enforce access control, click the bulk **Resource Actions** menu and choose **Configure >> Access Control**.
2. To implement access control for a single resource, in the **Resources** tab, click the **Resource Actions** drop-down beside the required resource and choose **Configure Access Control.**

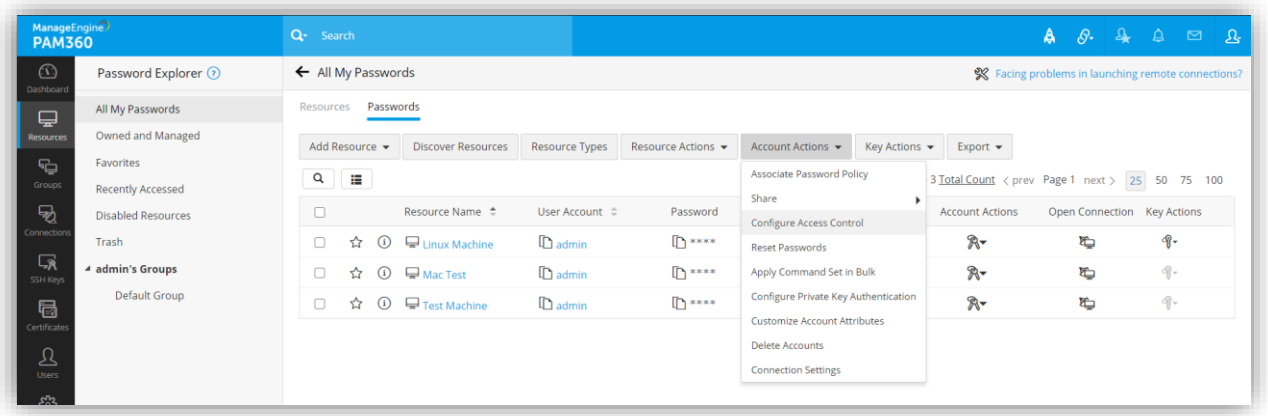


3.2 Access Control at Account Level

With Access Control at account level, it is possible to set password access control independently for each account under a resource, without affecting the access control configurations of other accounts in the resource. This ability to set unique configurations for each account helps users maintain unparalleled security levels for each account, based on requirements.

Follow the below steps to implement access control for accounts:

1. To implement access control for multiple accounts, navigate to **Resources** and switch to the **Passwords** tab. Select all accounts for which you wish to enforce access control in bulk, click the bulk **Account Actions** menu and choose **Configure Access Control.**
2. To implement access control for a single account, switch to the **Passwords** tab, click the **Account Actions** drop-down beside the required account and choose **Configure Access Control.** Alternatively, to implement access control for one or more accounts belonging to the same resource, click the resource name in the **Resources** tab. In the **Account Details** dialog box that opens up, select the required accounts and click **More Actions >> Configure Access Control** or click **Account Actions >> Configure Access Control** beside the required account.

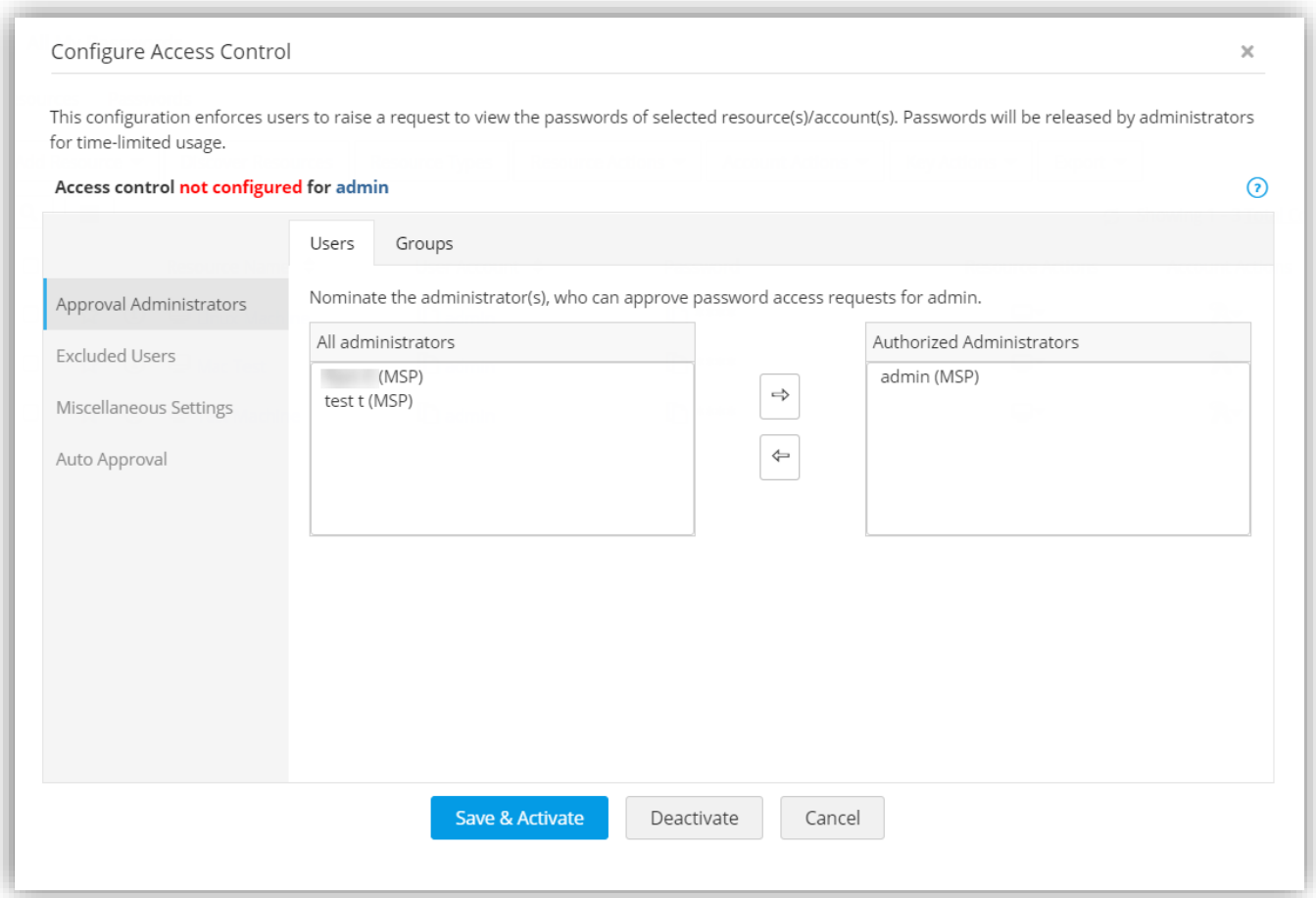


3. In the **Configure Access Control** window, you will see five tabs. Customize the settings as required.

    i. **Approval Administrators**
    ii. **Excluded Users**
    iii. **Miscellaneous Settings**
    iv. **Auto Approval**
    v. **Privilege Elevation**

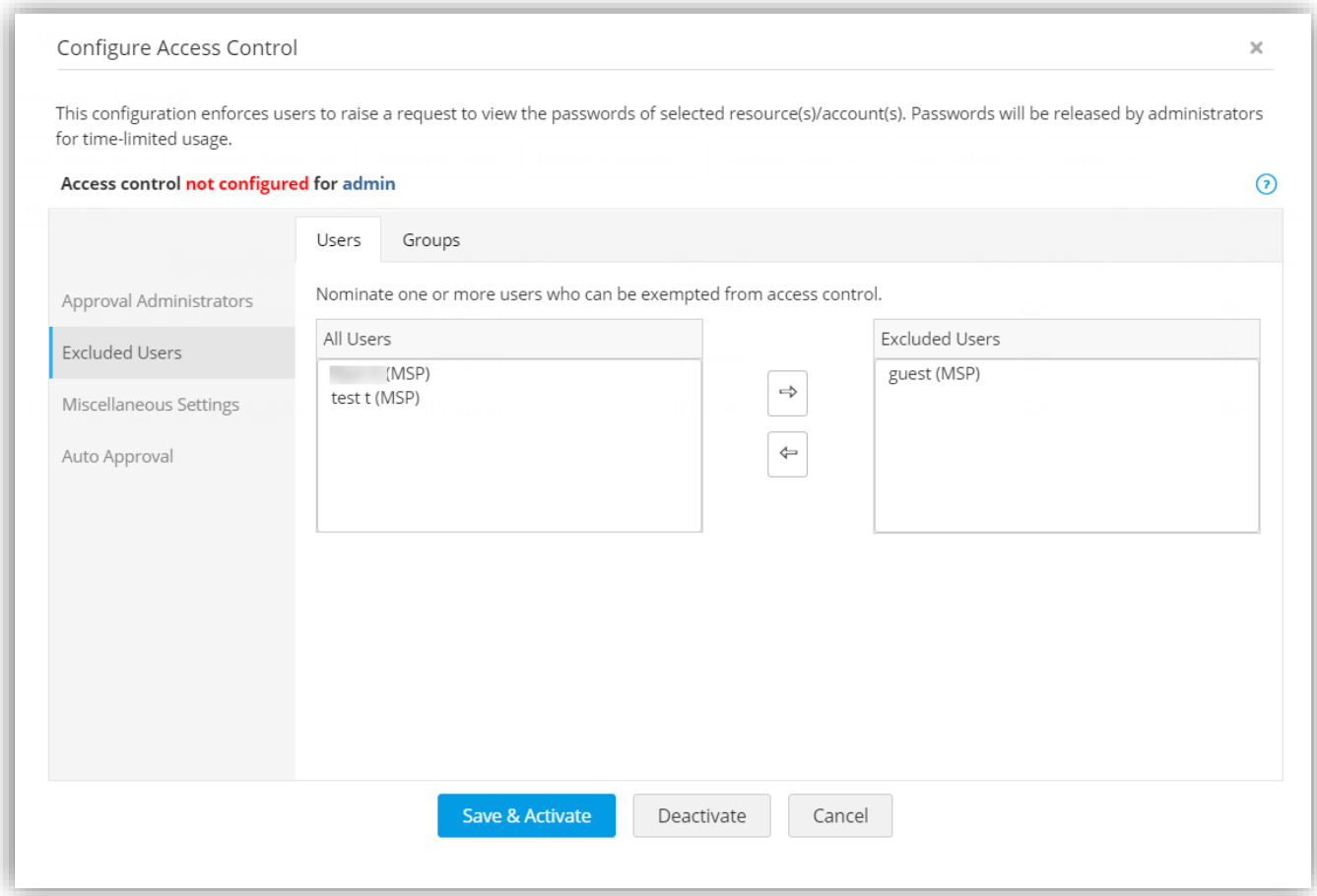
3.2.i Approval Administrators

Designate the administrator(s) as the approvers of password release requests. The list of all administrators, password administrators, and privileged administrators in the system are listed in the left pane. You can designate as many administrators as you wish for a particular resource or an account. Anyone from the list of **Authorized Administrators** could approve the requests raised by users.



3.2.ii Excluded Users

Exclude a set of users from the access control workflow using this option. The excluded users will be able to access passwords directly without raising requests



3.2.iii Miscellaneous Settings

1. **Enforce approval by at least __ administrators:** Select this option to enforce approval by a specific number of administrators for all password requests. This number can vary from 1 to 10 administrators and you can customize this by choosing the number of admins under **Admin >> Settings >> General Settings >> Maximum X approval admins (You may give minimum of 1 to maximum of 10 admins).** If you wish to enforce approval by at least 10 admins, then you must designate 10 admins as the authorized administrators under the **Approval Administrators** section.

   Note: You can also designate user group(s) as approvers for password release requests. When a user group is designated as an approver, all the users with admin rights within that group (the administrators, password administrators, privileged administrators and admin users with the custom role) are given access rights. If you have enforced approval by a particular number of administrators, say 5, then the authorized user group must have at least 5 valid administrators.

2. **Enforce users to provide a reason for password retrieval:** Use this option to mandate users to provide a reason when they try to retrieve a password in plain text by clicking

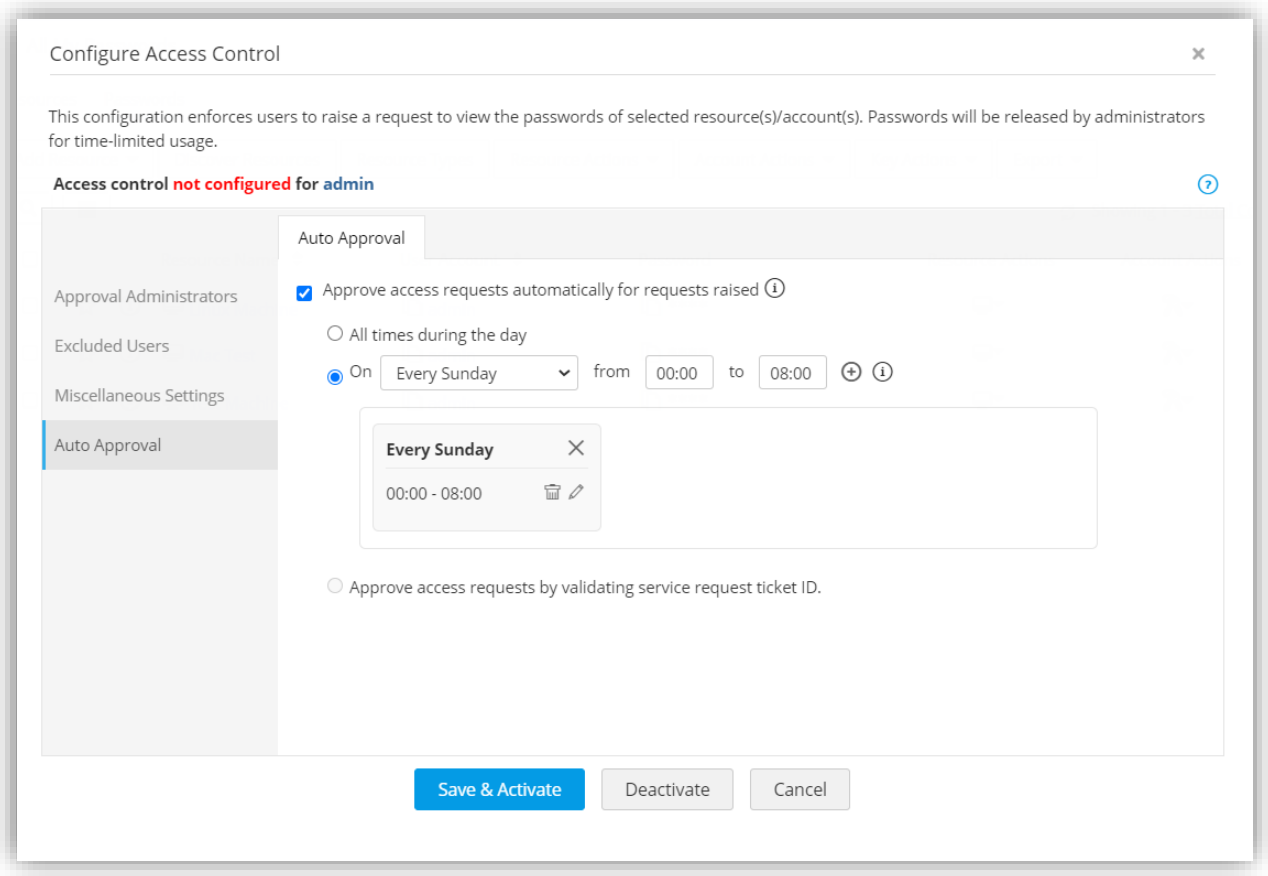
the asterisks. This is useful for auditing purposes.

3. **Send a reminder mail to the administrators to process the password access request before X minutes of the stipulated time:** Use this option to set a time at which a reminder email will be sent to the administrator about the password request that is yet to be approved. PAM360 will send the reminder email at the specified number of minutes before the void time.
4. **Once the access time ends, provide grace time of X minutes to the user**: Enable this option to provide a grace time of up to **60 minutes** to the user, after the password access time ends.
5. **The password will be checked in automatically after X hours of approval time:** Use this option to specify the exact time after which the password will be checked in automatically and will no longer be available for use.
6. **Requests are void after X hours, if not approved:** Use this option to specify the maximum time, in hours, after which a pending password request will become void if the administrators do not approve. If even one administrator approves the password request, then the approval status will be sent as notification to the other authorized administrators.
7. **Password access can remain exclusive for a maximum of X minutes:** Select this option to enforce concurrency controls for password access. During this specified time, the password is made available for the exclusive use of a particular user and no one else, including the resource owner, is allowed to view the password. By default, the password will remain exclusive for **30 minutes**. However, you can modify it to a desired value. For example, if you specify the time period as two hours, the password will be made available exclusively for that user for two hours. Others cannot view the password during that time. After the specified time, the password access will be void and will not be available to the user and other users will be able to view the passwords. If you specify the value as '0' hours, the password will remain exclusive for unlimited hours.
8. **Reset password / key after exclusive use (password / key checked-in by the user):** Select this option to enforce automatic reset of password once the user checks in the password thereby giving up access. For automatic password reset to take effect, you need to ensure that all required credentials have been supplied to the resource for remote password reset or you should have installed PAM360 agents in the resource. Otherwise, the automatic password reset will not take effect. For instructions on remote password reset, click here and for details on password reset via PAM360 agents, click here.

3.2.iv Auto Approval

1. PAM360 provides the option to set automatic approval of password access requests. This auto-approval feature will be handy during the times when an administrator may not be available to approve access requests for users. To implement this, administrators can set an approval time for every day or specific times on specific days of the week. All password access requests that are raised in this time frame will be auto-approved and

the authorized administrators will be notified. For example, you can set auto-approval for all requests raised between 2 p.m to 3 p.m on Saturday. You can set up to 3 approval time frames for a single day. Except for the automatic nature of approval, all other aspects of this feature will follow the access control workflow.



2. Once you have configured the necessary options for setting up the access control workflow for a resource or an account, click **Save & Activate**.

3.2.v JIT Privilege Elevation

Administrators can provide just-in-time (JIT) privilege elevation to local accounts in PAM360. For this, the administrator has to access the **Privilege Elevation** tab. Then, select the required groups out of the available local groups in the Windows resource and save them locally in the PAM360 database. Now, the privilege elevation configuration is ready for the local user account(s) under the selected resource.

Later, during the password check-out by any of the local accounts under the resource, their access privileges will be elevated as that of the local groups they were added to, and they will be able to operate with the same group privileges, for a stipulated time, as set by the administrator under **Miscellaneous Settings.**

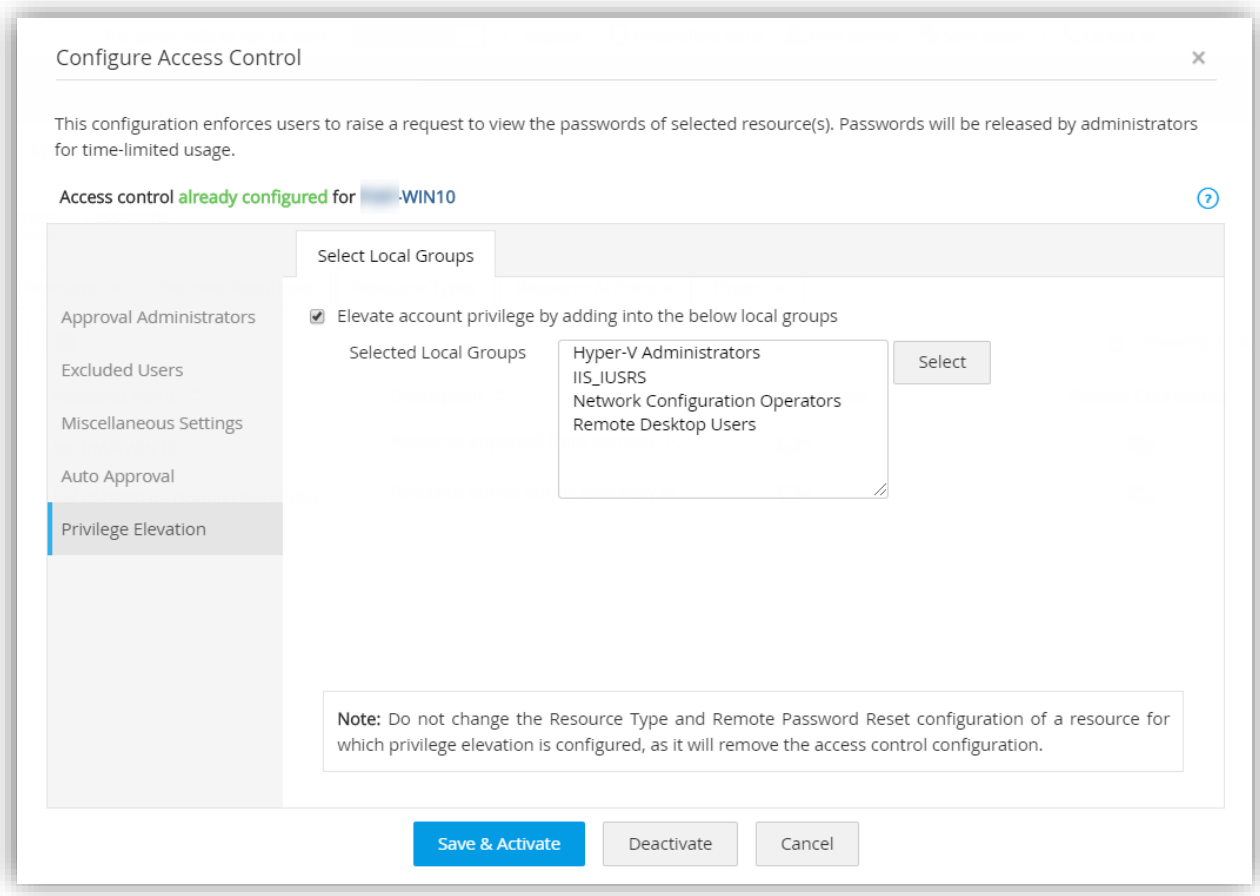
Benefits

The JIT privilege elevation feature comes in handy in situations where a local account may not have the access privileges to use certain applications or services in a system. Using the JIT privilege elevation feature, administrators can provide timely and controlled access to accounts to operate applications or systems for a specified period. This feature gives administrators the ability to control who can access what and for how long, thereby eliminating the need to provide unnecessary blanket access for all accounts. This is based on the principle of least privileged access, which is one of the core philosophies of zero trust networks.

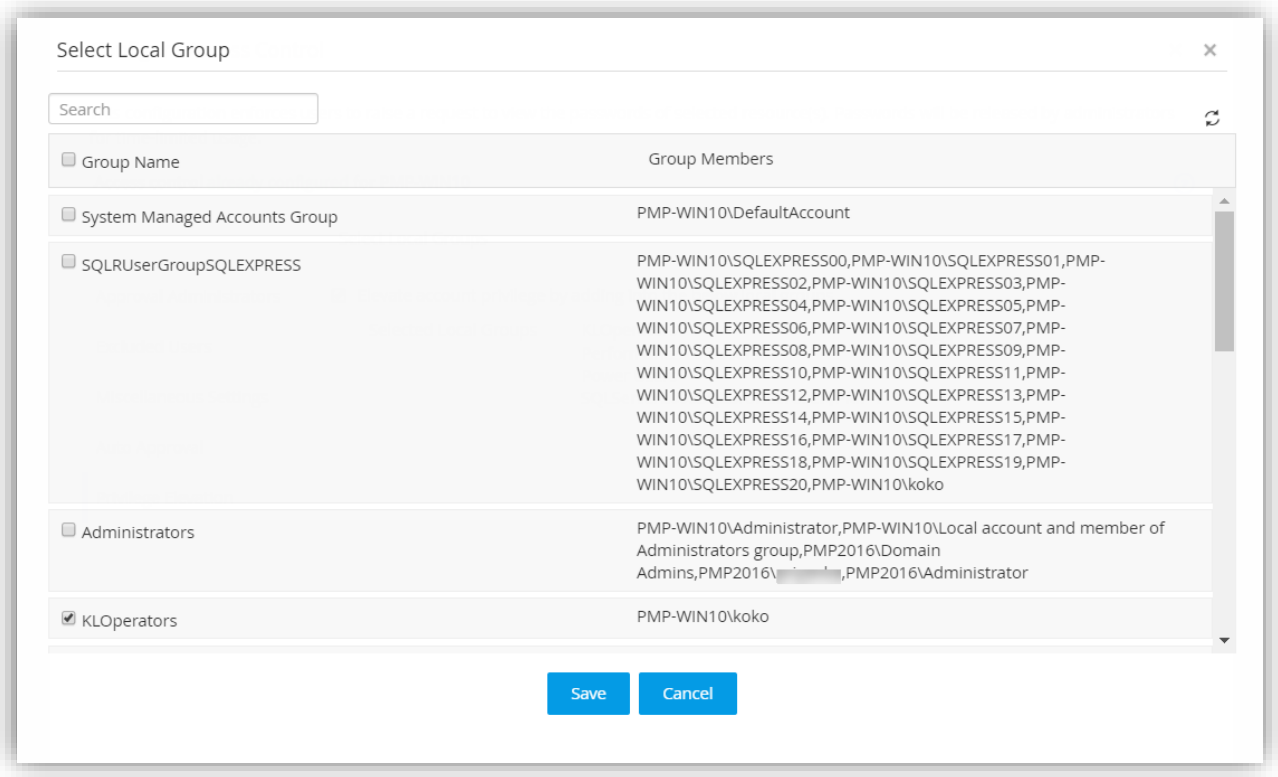
Steps Required

Follow the below steps to fetch and save local groups from a Windows resource to facilitate JIT privilege elevation:

1. Access the **Privilege Elevation** tab and enable the **Elevate account privilege by adding into the below local groups** option.



2. Click **Select** and all the local groups available in the Windows resource will be fetched and displayed in the **Select Local Group** dialog box. Choose the required groups and click **Save**. To update this list of local groups saved in the database, click the **Refresh** icon at the top right corner of the window.



3. The selected groups will be listed in the **Selected Local Groups** box shown above.

Once you have configured the necessary options for setting up password access control, click **Save & Activate.** To remove previously configured access control for the selected resource, click the **Deactivate** button.

Now, when the resource is shared to a user with Password User/Password Auditor capabilities, they can request for password access or elevation. This request can be approved/rejected by any admin in the **Authorized Administrators** list.

Notes:

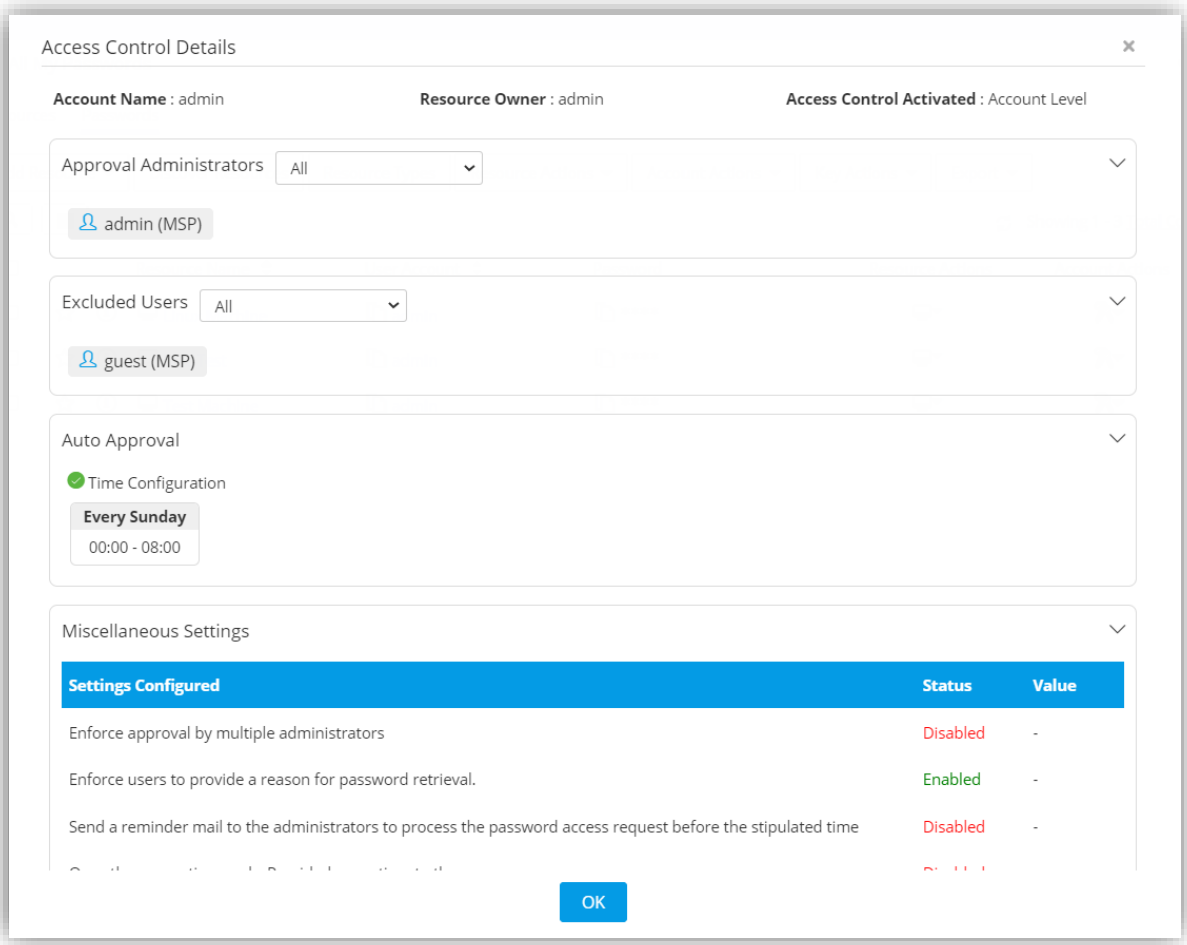
- Privilege elevation for local accounts using the above procedure can be done only for **Windows** resources. To apply privilege elevation in Windows Domain resources, integrate PAM360 with ManageEngine ADManager Plus. Refer to the **ManageEngine ADManager Plus** help section to more details on the integration.
- Privilege elevation happens only at the time of password check-out i.e., PAM360 will add the local account to the selected local groups only when the password of the local account is checked out from the PAM360 vault.
- If privilege elevation fails for a local user account when PAM360 adds it to the selected local groups, then the password of the account cannot be requested by users who have access to it. For more details on the reasons of failure, check audit logs in the **Audit** tab.
- Password access control cannot be deactivated for a resource when the password is checked out and is currently in use.
- It is recommended that resource owners do not change the **Resource Type** or **Remote Password Reset** settings of a resource for which access control is configured and whose password is currently in use. Doing so will remove the access control configuration. To check if the status of a password is In Use, go to **Admin >> Manage >> Password Access Requests** and check the status under **Action**. Refer to the below use case scenarion 2 for more details.

3.3 Viewing Access Control Details

Once Access Control is activated for an account or a resource, the **Access Control Details** option consolidates all the settings applied and provides it in a single window for easy perusal. Please note that the **Access Control Details** window can be accessed from the **Account Actions** menu only. Follow the below steps to view the access control details:

1. Navigate to the **Resources** tab and switch to the **Passwords** tab.
2. Click the **Account Actions** icon beside the required account and choose **Access Control Details** from the drop-down. Alternatively, click a resource name in the **Resources** tab. In the **Account Details** dialog box that opens, click **Account Actions >> Access Control Details** beside the required account.
3. The **Access Control Details** dialog box will display the following details:

i. Account Name.
ii. Resource Owner.
iii. Type of Access Control activated: **Resource Level** or **Account Level.**
iv. List of **Approval Administrators** (users and/or groups).
v. List of **Excluded Users** (users and/or groups).
vi. **Auto Approval** time frame set for this particular account or resource.
vii. Any **Miscellaneous Settings** configured such as, enforcing approval by multiple administrators, enforcing users to provide a reason for password retrieval etc.



4. Use Case Scenarios

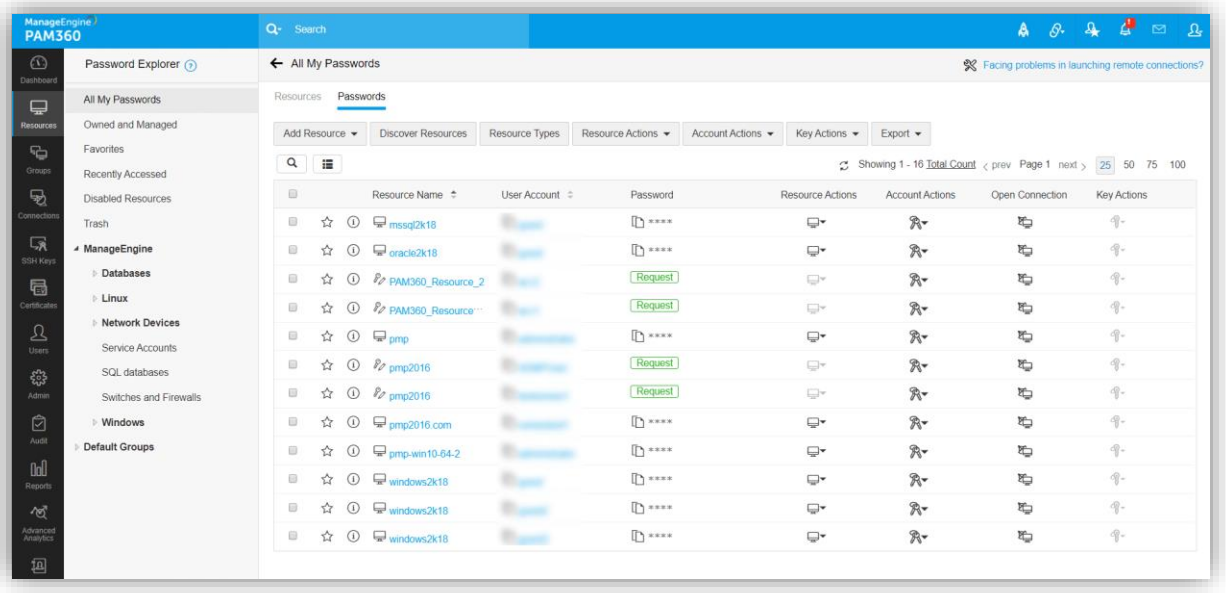
The following are some of the use case scenarios in which access control workflow will be useful in an organization.

Case 1: User Requesting Access to View a Password

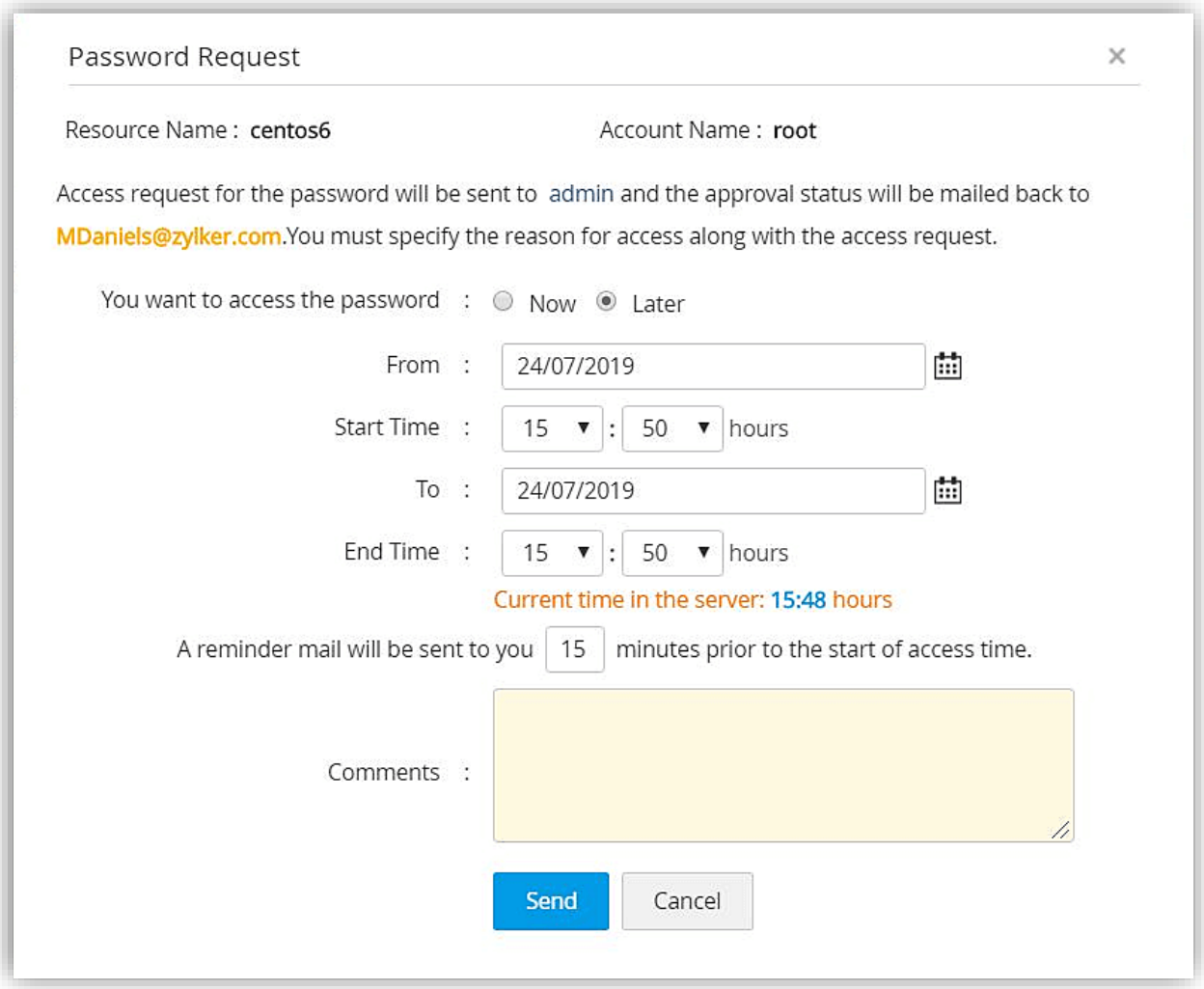
To access a password protected by the access control workflow, a user will have to request the administrator to grant permission to view the password.

Steps To Make a Request:

1. Click the **Resources** tab from the left pane and click the **Passwords** tab.
2. All the passwords will be listed in the table below. Click **Request** beside the desired passwords to request the administrator to grant permission to view the passwords.



3. In the new pop-up form that opens, you will be able to:
    - Specify when you want to access the password - now or later.
    - Enter a reason to view the password.
    - Specify the time before which a reminder email is to be sent.



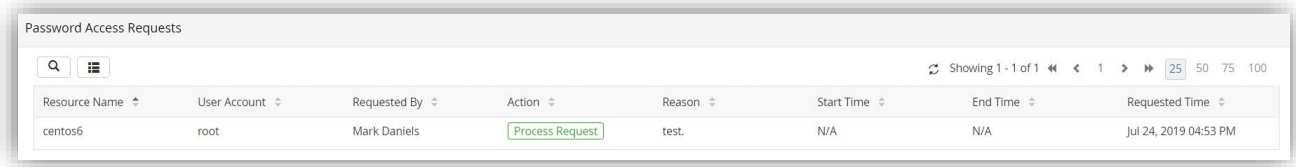
4. Once the administrator approves your request, you will be allowed to view the password. Till then, the status will be Waiting for approval.
5. Once the administrator approves the request, the status will change to **Check Out**. To view the password, click **Check Out.** Please note that the **Check Out** button will be enabled only during the approved access time.
6. Click **Save**. Now, you will be allowed to view the password.

Case 2: Administrator Approving a Password Request

If you're an administrator and a user has requested your approval to view a password, you will receive an email notification about the request. You can view all the requests pending your approval from the **Admin** tab.

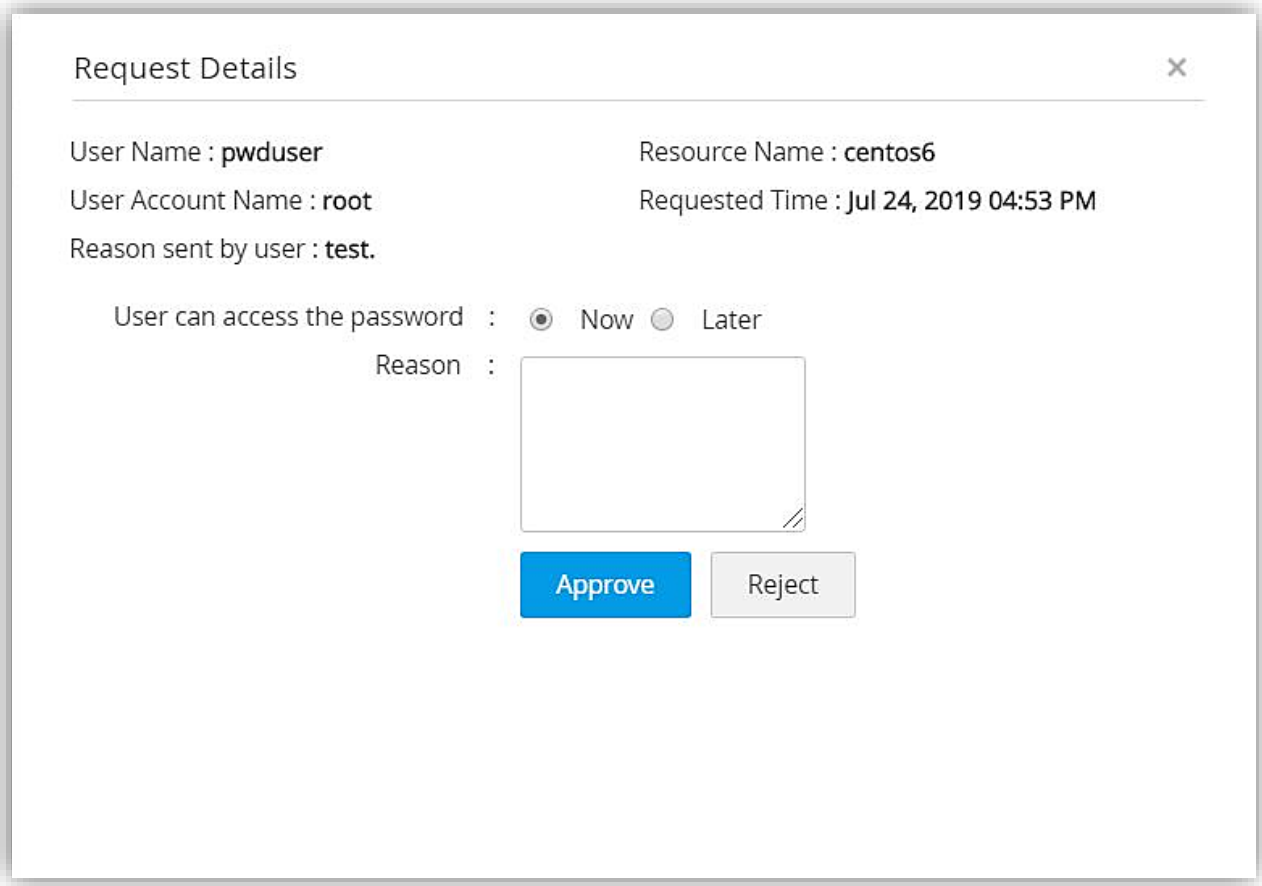
To Approve a Request,

1. Navigate to **Admin >> Manage >> Password Access Requests**.

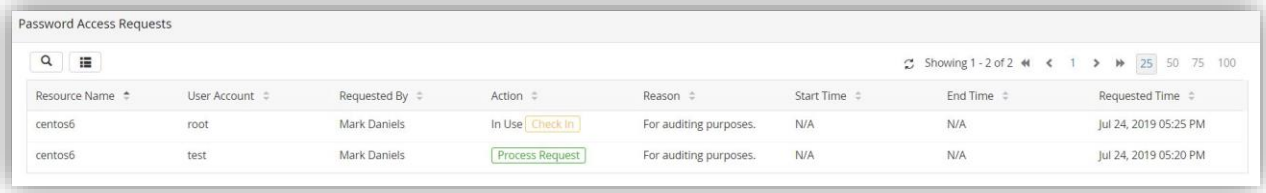


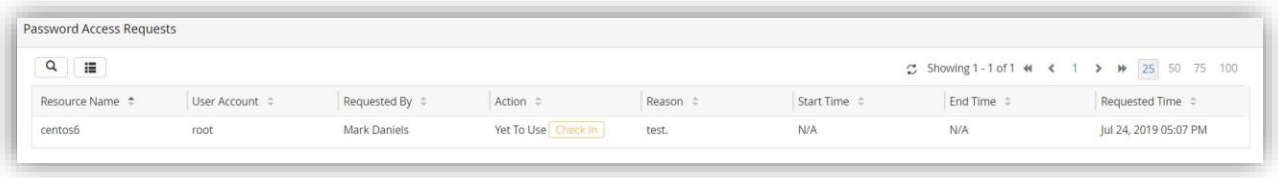
2. Click **Process Request** beside a request to allow the user to view the password. Once you do this, a new window will open where the administrator can do any of the following things:

    - Approve or reject the password access request.
    - Specify when the user can access the password - **Now** or **Later**.
    - Specify the reason for approval / rejection of the request.



3. Immediately after you approve the request, the status of the link will change to **Yet to Use**, indicating that the user is yet to check out the password.





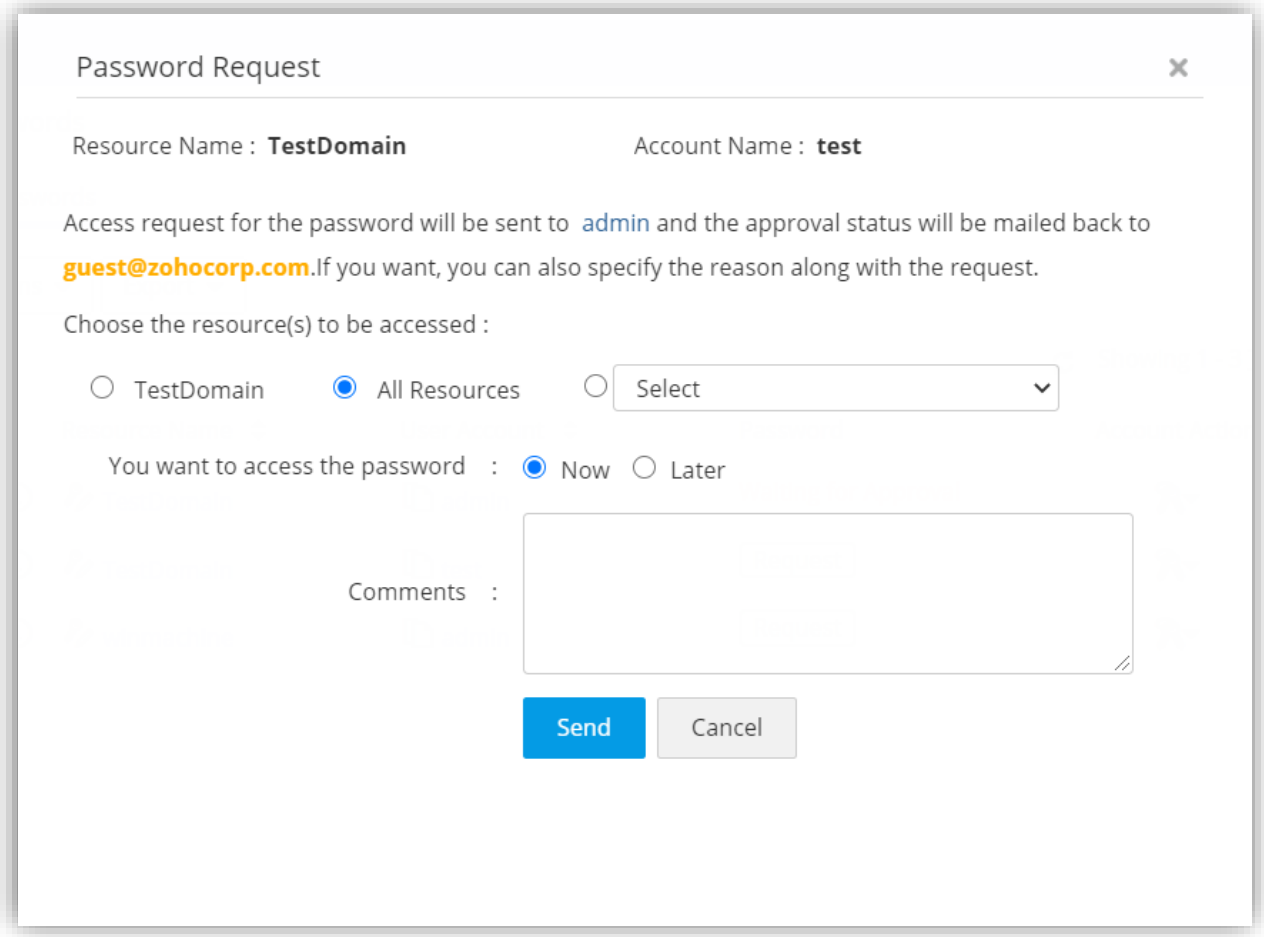
4. Once the user has viewed the password, the status will change to **In Use**.

> **Note:** If a password access request is rejected by an admin in the above scenario, the request will be removed from the queue.

Case 3: User Requesting Access and Administrator Approving a Password Request for Windows Domain Account

Steps to request a password:

1. Click the **Resources** tab from the left pane and click the **Passwords** tab.
2. All the passwords will be listed in the table below. Click **Request** beside the desired passwords to request the administrator to grant permission to view the passwords.
3. In the new pop-up form that opens, you will be able to:
    - Choose the resource(s) to be accessed - **Current Windows Domain Machine, All Resources** or **select** the required resource(s) from the drop-down.
    - Specify when you want to access the password - **now** or **later.**
    - Enter a reason to view the password.
4. Click **Send.**



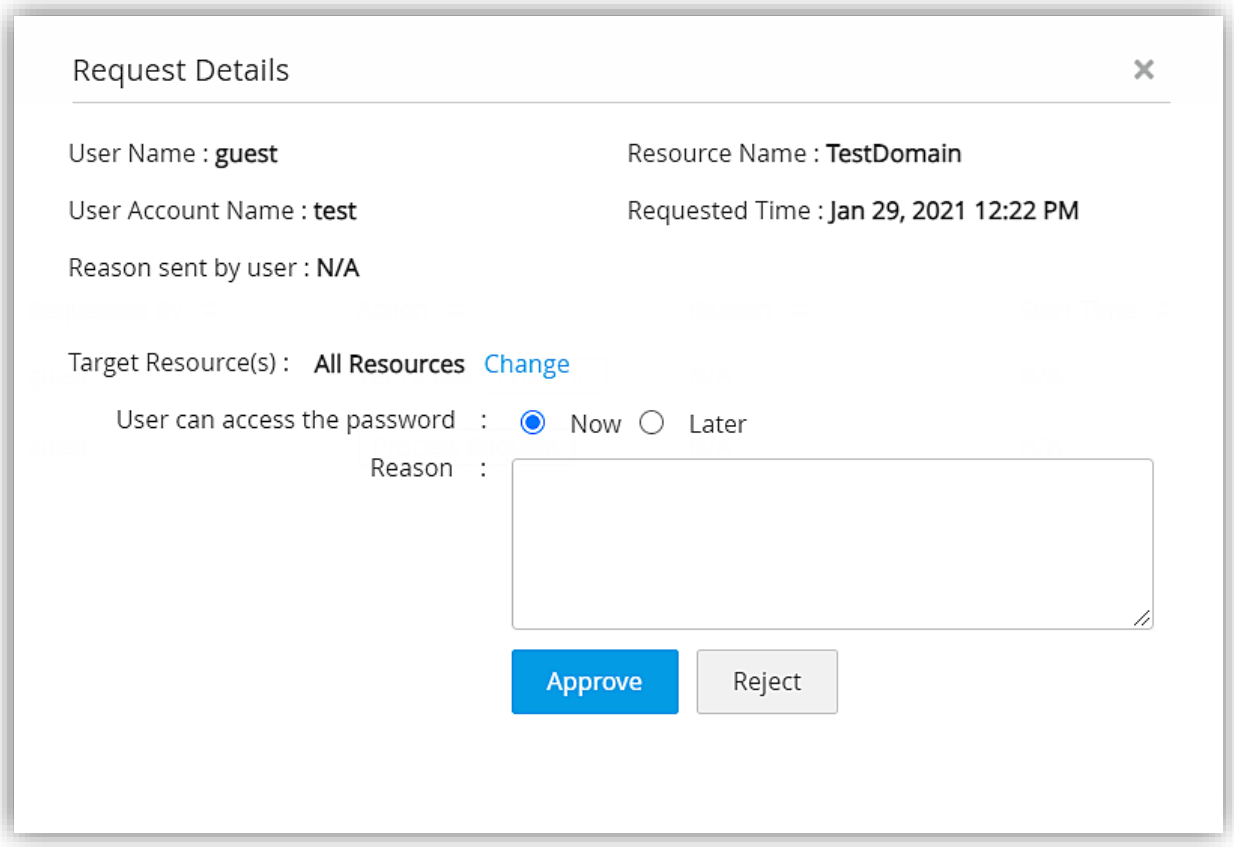
5. Once the administrator approves your request, you will be allowed to view the password. Till then, the status will be **Waiting for approval.**
6. Once the administrator approves the request, the status will change to **Check Out.** To view the password, click **Check Out.** Please note that the **Check Out** button will be enabled only during the approved access time.
7. Click **Save.** Now, you will be allowed to view the password.

> **Note:** Users can choose the required resources in the domain account and request permission to access them. Users will be able to access only the approved resources using that domain account.

To Approve a Request:

1. Navigate to **Admin >> Manage >> Password Access Requests.**
2. Click **Process Request** beside a request to allow the user to view the password. Once you do this, a new window will open where the administrator can do any of the following things:
    - Change the Target Resource(s).

- Specify when the **User can access the password - Now** or **Later**.
- Specify the reason for approval / rejection of the request.
- **Approve** or **Reject** the password access request.



3. Immediately after you approve the request, the status of the link will change to **Yet to Use,** indicating that the user is yet to check out the password.
4. Once the user has viewed the password, the status will change to **In Use.**

Case 4: User Completes their Password Usage

The crux of the access control mechanism is that the user will be allowed only temporary access to passwords. So, once the user finishes their work, they can give up the password.

To Give Up Access to the Password:

1. Click the **Check In** button beside the password. Now the password will be checked back into the system and the status will change as **Request** again.
2. You will no longer be able to view the password. In case, you require access again, you will have to go through the Request-Release process again.

Case 5: Administrator Forcefully Checks In the Password

Access control mechanism allows exclusive access privilege to a user for a specified time period. During this period, no one else will be allowed to view the password, including the owner. In case an emergency arises to revoke the exclusive permission to the user, administrator can forcefully check in the password at any point of time.

To Forcefully Check In a Password:

1. Go to **Admin >> Password Access Requests.**
2. Click **Check in** beside the specific request to revoke the user's access permission. Once you do this, user will not be allowed to view the password. The password access request will also vanish from the list.

Case 6: What Happens if the Automatic Scheduled Password Reset Fails During Password Check In

Once a password is checked out by a user, it will be checked in due to any of the following three reasons:

1. User checks in the password on their own after password usage is complete.
2. System automatically revokes the password after the stipulated time.
3. Administrator forcefully checks in the password.

When password is checked in, if the admin settings require automatic password reset, PAM360 will try to reset the password. In case PAM360 is not able to reset the password in the actual resource, PAM360 will immediately trigger email notifications to the administrators who approved the password access request of the use so that they can troubleshoot and set things right. The password reset failure will also reflect on the audit trails.

Case 7: What Happens if a Scheduled Password Reset Scheduled Task Runs When a Password is Checked Out?

PAM360 provides an option to create scheduled tasks for automatic and periodic password resets. It is possible that a scheduled task starts executing the reset of a password that is currently checked out by a user. If that reset task is allowed to execute successfully, the user will be working with an outdated password. To avoid such password mismatch issues, PAM360 will prevent the reset of that password alone while all other passwords of other resources that are part of the scheduled task will be reset. The failure to reset the exempted password during the password reset schedule will reflect on the audit trails.

Case 8: Disabling Access Control

As an administrator, if you want to disable access control for any resource or an account, you may do so at any time as explained below.

i. Deactivating Access Control for Resources

1. Go to the **Resources** tab and select the resources for which you wish to disable access control.
2. Go to the bulk **Resource Actions** menu, choose **Configure >> Access Control** and click **Deactivate** in the **Configure Access Control** dialog box.
3. To deactivate access control for a single resource, click the **Resource Actions** icon beside the required resource and choose **Configure Access Control** from the drop-down. Click **Deactivate** in the **Configure Access Control** dialog box.

> **Note:** Deactivating the Resource level access control will not affect any Account level access control configuration enforced on the accounts belonging to that resource.

ii. Deactivating Access Control for Accounts

1. Go to the **Resources** tab, switch to the **Passwords** tab and select the accounts for which you wish to disable access control.
2. Go to the bulk **Account Actions** menu, choose **Configure Access Control** and click **Deactivate**.
3. To deactivate access control for a single account, click the **Account Actions** icon beside the required account and choose **Configure Access Control** from the drop-down. Click **Deactivate** in the **Configure Access Control** dialog box.

Now, the Access Control for the selected resources or accounts is deactivated. So, any user who has permission to view a password (owned/shared) can directly view the password without going through the access control process.

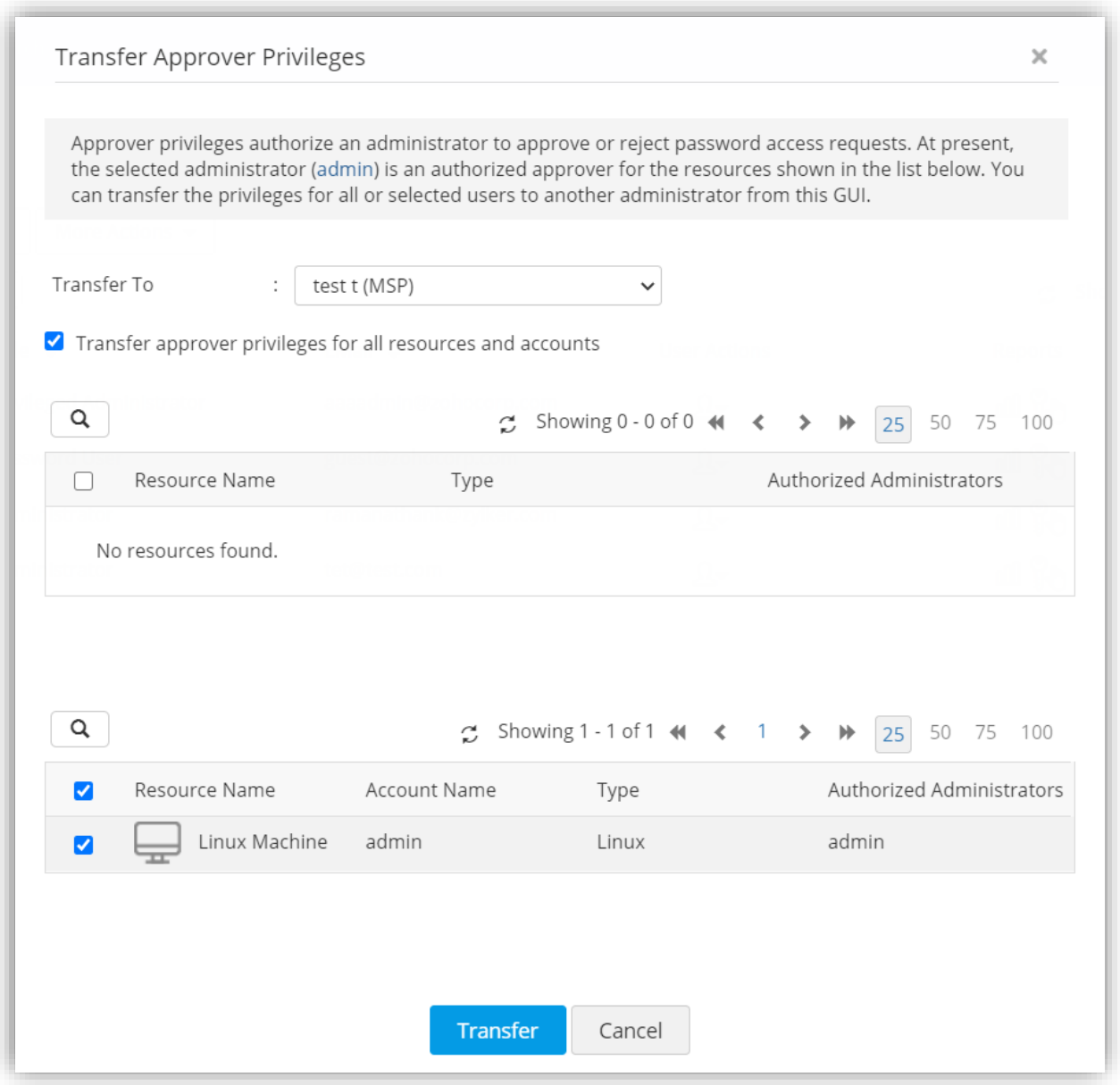
> **Note:** If Account level access control is deactivated and there is a Resource level access control already in place for the resource, then the Resource level access control will be automatically applied to the account as well. Check the **Precedence in Password Access Control** section to more about how precedence works for access control settings.

Case 9: Transferring Approver Privileges to Other Administrators

When an administrator leaves the organization or moves to a different department, resources/ accounts owned by that administrator are transferred to some other administrator. If the departing administrator had acted as the approver for password release requests, the approval privileges should also be transferred. All the resources and accounts that were earlier controlled by one admin can be easily transferred in bulk to another admin. Follow the below steps to learn how to transfer approver privileges from one administrator to another.

To Transfer Approver Privileges:

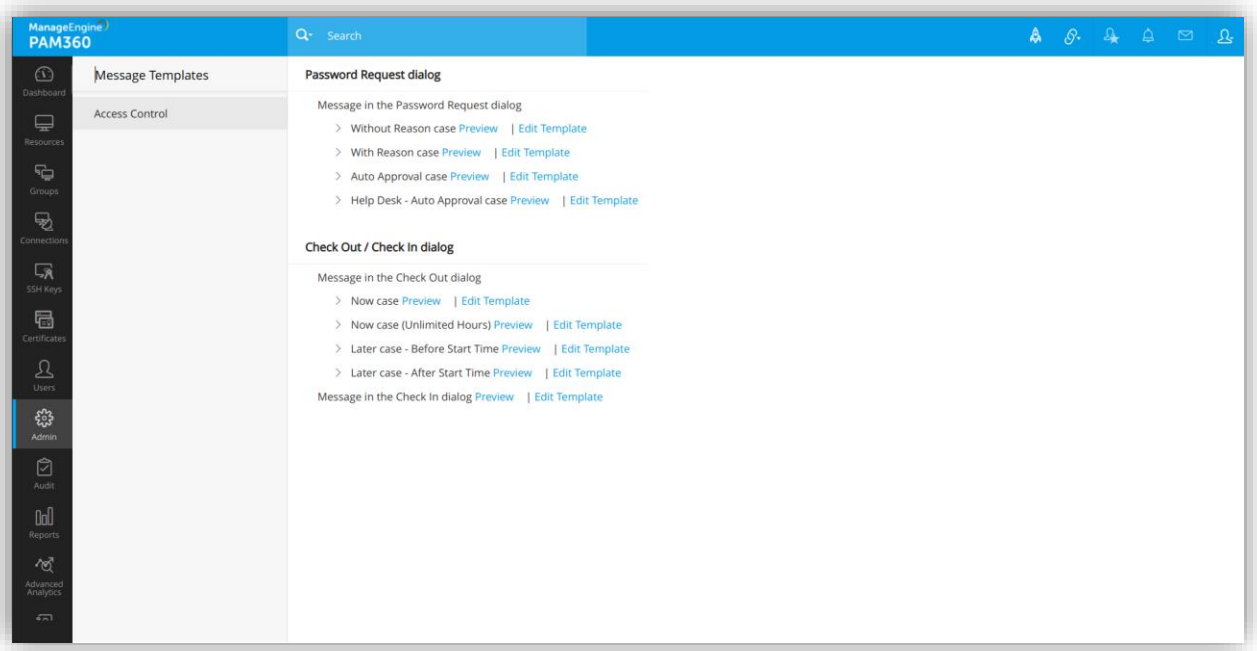
1. Navigate to the **Users** tab and select or search for the user whose approver privileges you would like to transfer to another admin.
2. Click the **User Actions** icon beside that user and select **Transfer Approver Privileges** from the drop down list.
3. In the **Transfer Approver Privileges** window that opens, all the resources and accounts for which the selected admin is an authorized administrator will be displayed. Choose the desired resources.
4. From the **Transfer To** drop down, select the admin to whom you would like to transfer the approver privileges to and click **Transfer**. The approver privileges will be transferred and the authorized administrator will be subsequently changed.



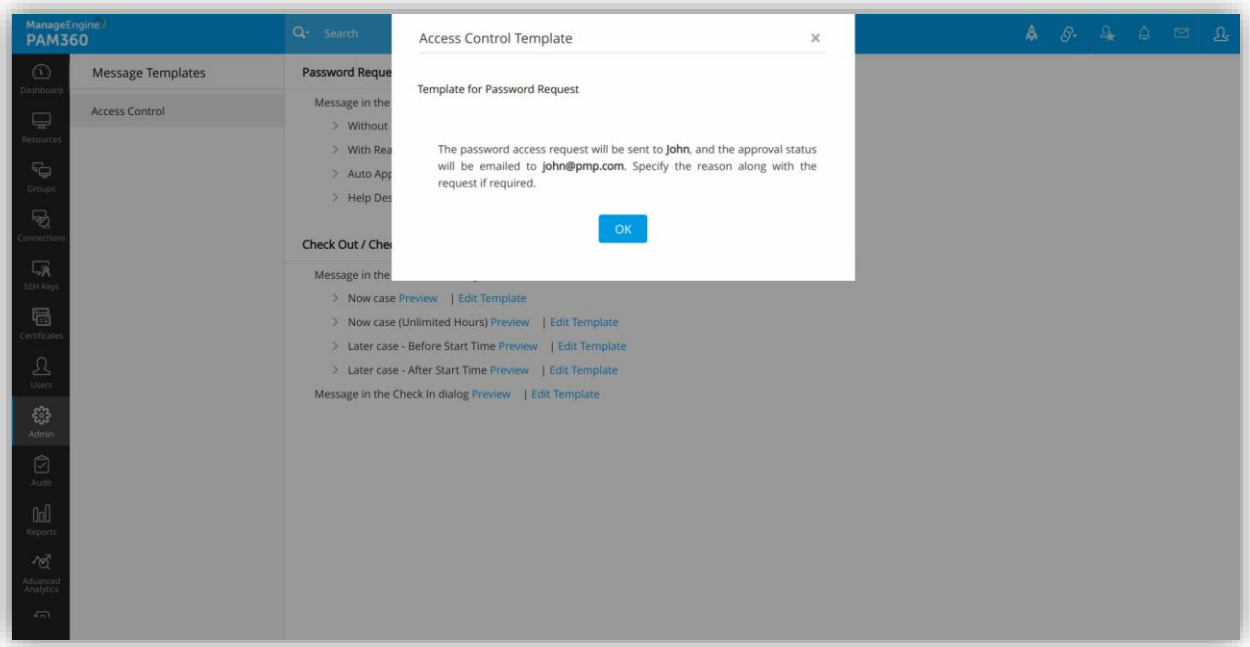
5. Message Templates

By default, PAM360 has predefined templates for access control dialog boxes such as Password Request, Password Check In, Password Check Out. Using message templates, the administrators will be able to alter the messages in access control workflow dialog. To customize the messages in access control dialog:

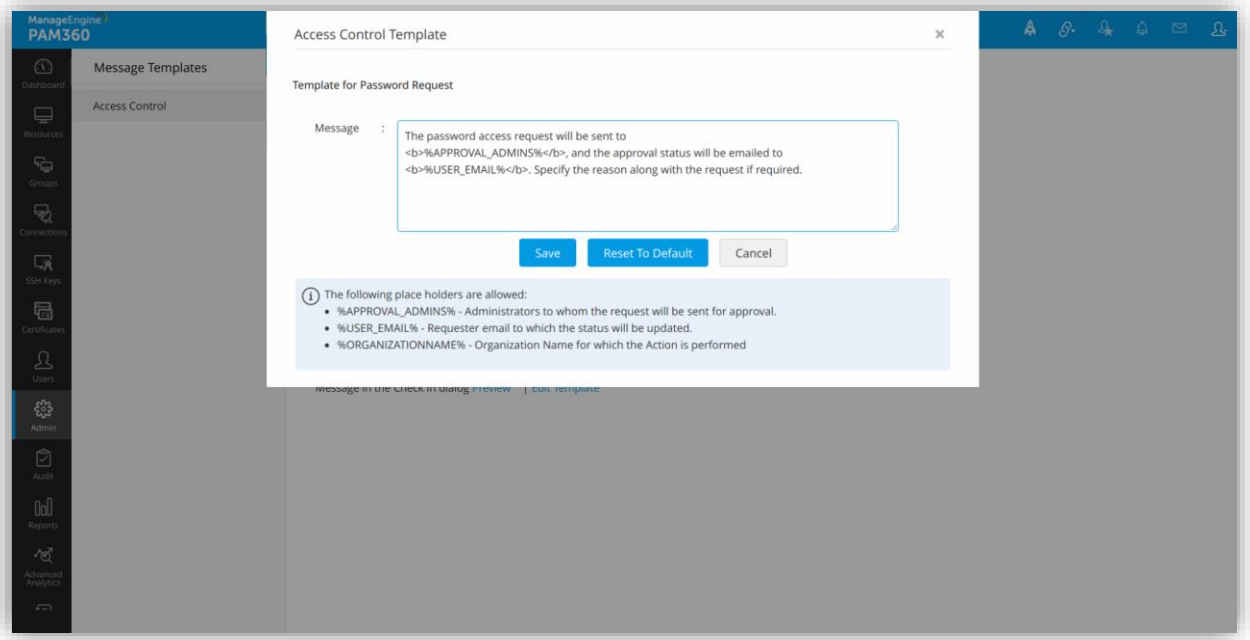
1. Navigate to **Admin >> Customization >> Message Templates.**
2. For each category, you will find a number of sub-categories with a dedicated message template.



3. Preview the existing content for each template by clicking the respective **Preview** link.



4. Click **Edit Template** against the desired template to edit the content.
    i. In the Access Control Template window, enter a customized **Message.**
    ii. While entering the **Message**, you can specify place holders for certain values like ORG name or user email, etc. The exact ORG name will be replaced with the place holders at runtime. The allowed place holders for each template can be found at the bottom of its respective Access Control Template window.
    iii. Click **Save** to save the message template.
    iv. Click **Reset to Default** to reset the message template to the default message.
    v. Click **Cancel** to cancel and exit the Access Control Template window.



5. The Access control dialog box of the respective categories will now have the new

content.

6. Glossary of Terminologies

Term	Description
Request	The user has to make a request to view the password.
Waiting for Approval	User's password release request is pending with administrator(s) for approval.
Check Out	Administrator has approved the request and the user can view the password.
Approve/Reject	Administrator can either approve or reject the password request.
Yet to Use	Indicates that the user is yet to view the password released by the administrator.
In Use	Password is being used exclusively by a user.
Check In	Giving up/revoking password access.

Password Reset

Here in this guide, you will find all the related links to password reset. It includes several methods to reset passwords remotely, steps to secure your passwords, reset all your passwords individually or in bulk, ways to gain further control over who accesses your passwords, etc.

Quick Links

1. Remote_Password_Reset
2. Password Reset using Agents
3. Configuring Password Reset in Bulk
4. Periodic_Password_Reset
5. Windows Service Account Reset
6. IIS AppPool Account Reset
7. Windows Scheduled Task Reset
8. SSH based Password Reset

Remote Password Reset

1. Overview
2. Remote Password Reset via Agent-less Mode
    2.1 Configuring Remote Password Reset for Individual Resource Types
        2.1.1 Windows
        2.1.2 Windows Domain
        2.1.3 Linux/IBM AIX/HP UX/Solaris/Mac OS/VMWare ESXi
        2.1.4 IBM AS400/Sun Oracle ALOM/ILOM/XSCF Sun Oracle ALOM/ILOM/XSCF
        2.1.5 Cisco Devices(IOS, CatOS, PIX)
        2.1.6 MS SQL Server
        2.1.7 MySQL/Postgre SQL
        2.1.8 Sybase ASE
        2.1.9 Oracle DB Server
        2.1.10 HP ProCurve
        2.1.11 Juniper Netscreen
        2.1.12 HP iLO
        2.1.13 Oracle WebLogic server
        2.1.14 AWS IAM
        2.1.15 Google Apps
        2.1.16 Microsoft Azure
        2.1.17 Rackspace
        2.1.18 Salesforce
        2.1.19 Amazon Aurora PostgreSQL
        2.1.20 Amazon Aurora MySQL
        2.1.21 RabbitMQ
        2.1.22 LDAP Server
    2.2 Configuring Remote Password Reset for Resource Types in Bulk
3. Remote Password Reset via Agent Mode

1. Overview

PAM360 provides the option to remotely change the passwords of certain resource types. In general, you can configure remote password reset in PAM360 for any device that can be reached via command-line interface (CLI) and accept commands for managing passwords. Read further to know more about configuring remote password reset for resources.

PAM360 allows you to change the password of a remote resource through two modes; agent-less mode and agent mode.

2. Remote Password Reset via Agent-less Mode

If you're configuring remote password reset via agent-less mode, specify the account which will be used to log in remotely to the target resource and reset the password.

2.1 Configuring Remote Password Reset for Individual Resource Types

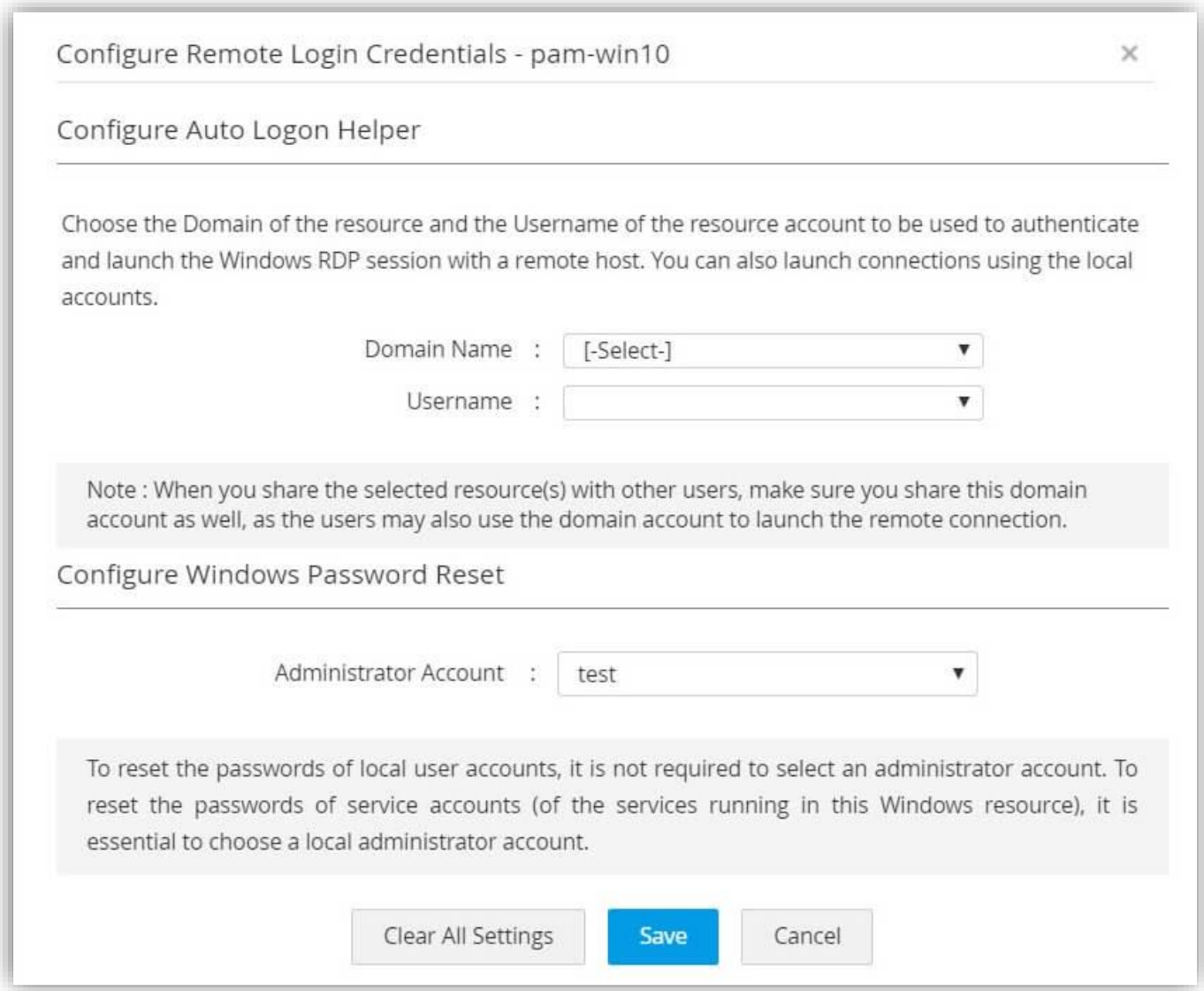
Operating Systems

2.1.1 Windows

1. PAM360 is designed to perform password reset for all Windows local accounts using the service account with which it is running.

   > **Note:** The aforementioned service account should have either domain admin rights or local admin rights in the PAM360 server and in the target systems that you would like to manage.

2. Log in to the PAM360 server and open the Services console (services.msc) to update the service account of PAM360 service.
3. However, if you'd like to override this and use a local account for the password reset, then navigate to **Resources >> Resource Actions >> Configure Remote Password Reset** and choose an admin account.
4. If the PAM360 service is running with a privileged service account (Domain admin or Local admin on all member servers), then it can forcefully reset Windows passwords without the need for the old password to be present inside.

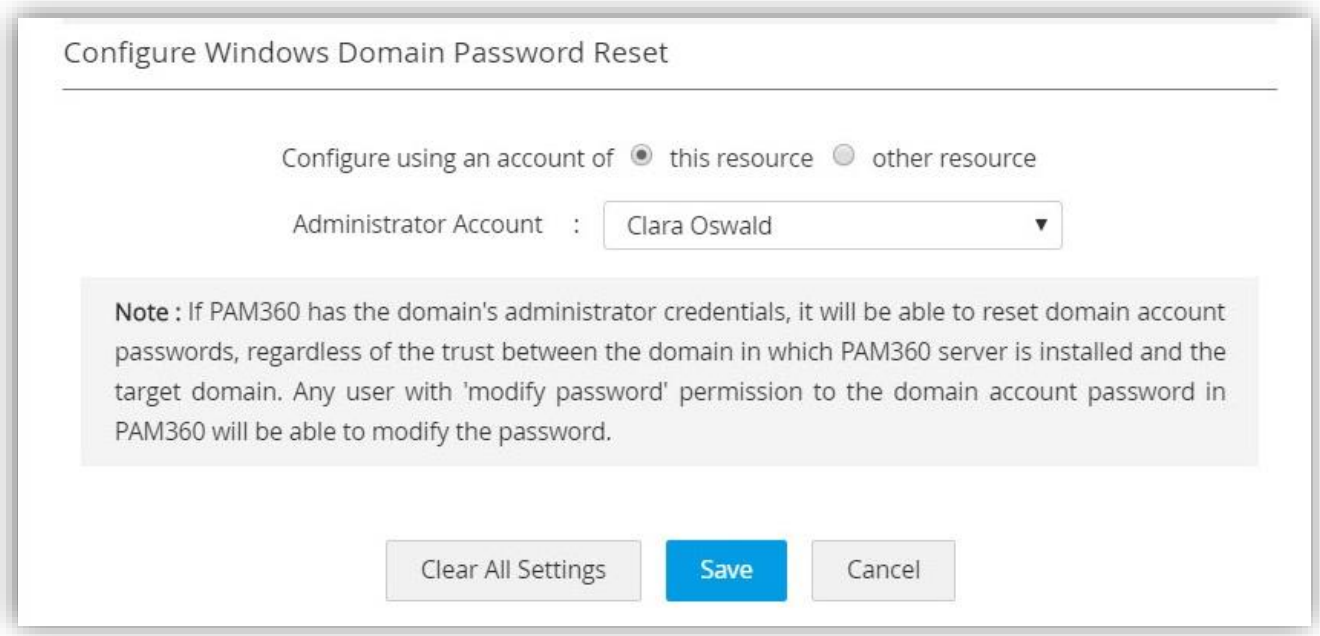


2.1.2 Windows Domain

If you are using the **Privileged Accounts Discovery** feature to import Windows resources from Active Directory, then PAM360 will automatically add your domain controller as a resource with Resource Type as **Windows Domain.**

To reset domain account passwords that are present in your Windows Domain resource, specify an admin account to be used for remote login as well as password reset. Follow the below steps to configure remote password reset.

1. Navigate to the **Resources** tab and click **Resource Actions >> Configure Remote Password Reset.**
2. Select the domain account as the administrator account and **Save.**
3. It is recommended to use the same PAM360 Service Account here so that it will be helpful for AD Audit purposes.



Note: If PAM360 has the domain administrator credentials, it can reset domain account passwords regardless of the trust between the domain in which PAM360 server is installed and the target domain. Any user with 'modify password' permission for the domain account password in PAM360 will be able to modify the password.

2.1.3 Linux/IBM AIX/HP UX/Solaris/Mac OS/VMWare ESXi

For remote password reset of Unix resources, PAM360 first uses the remote login account to log in to the target system. Then, to carry out password reset, privilege elevation is needed. If the target system supports execution of password reset commands through Sudo, PAM360 can either use the two options available here: 'su' as root or use 'sudo' to execute the remote password reset commands.

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset** and then do the following:
    i. **Selecting the Protocol**
        a. Select the protocol for remote login method - SSH or Telnet. Next, specify your remote login account. For remote login, PAM360 allows you to either choose an account of the resource type for which you're setting up the password reset or specify an account of any Windows Domain resource stored in PAM360. To use a Windows Domain account as the remote login account, select the option 'other resource' while setting up the remote login account. Then, specify the Resource Name as well as the Remote Login Account of the desired account.
        b. Specify the authentication method. If you have chosen Telnet or SSH with

Windows Domain account for remote login, you can skip this step go to setting the privilege escalation method.

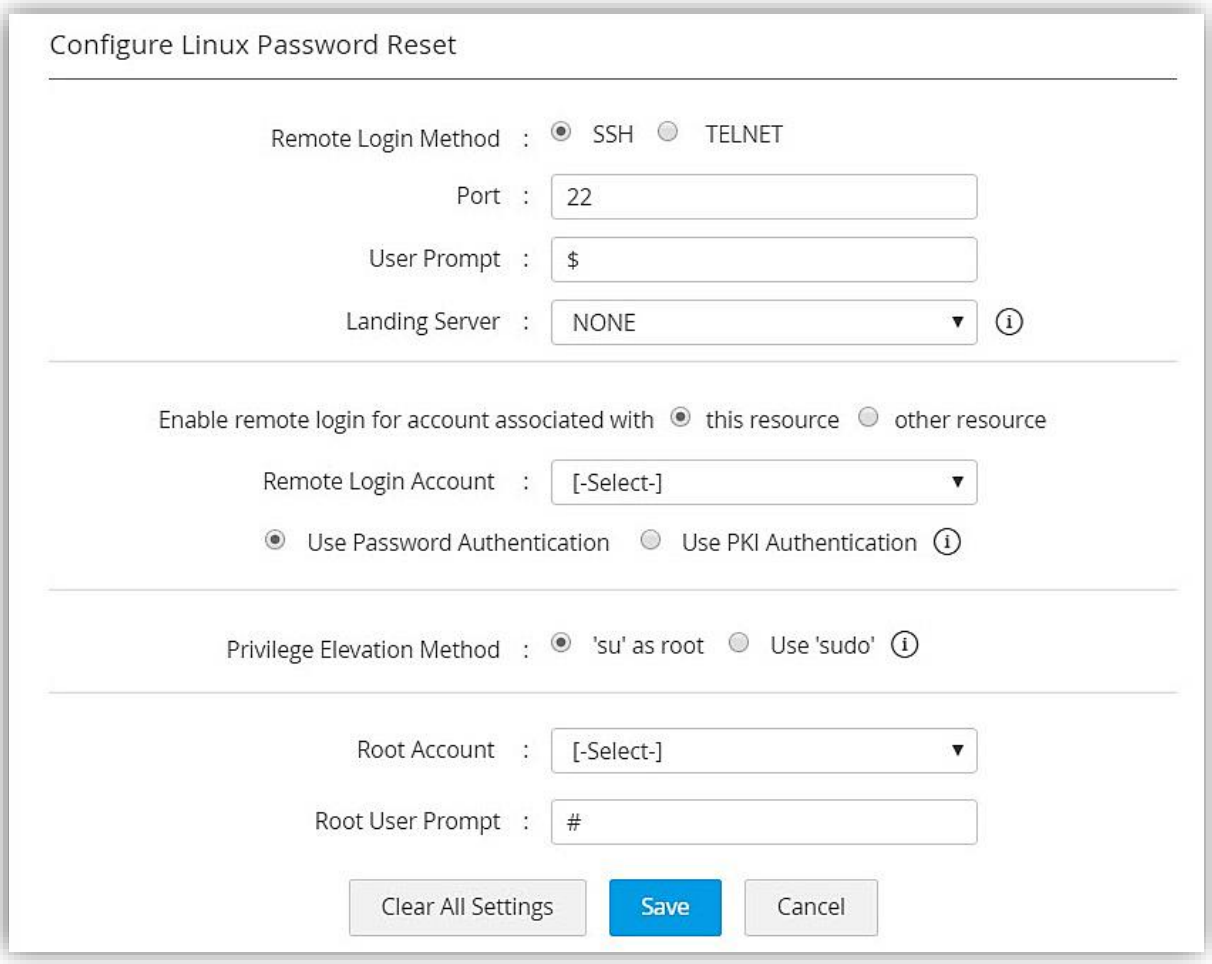
ii. **If you opt for SSH, specify the authentication method**

a. If you choose SSH as the Remote Login Method and the remote Unix resource's account as the remote login account, there are two authentication methods you can choose from: **Password Authentication** or **Public Key Infrastructure(PKI)** Authentication.
b. For PKI authentication, the public key would be present in the remote system under a specific remote login account. Typically, it would be available under $Home/.ssh folder. Select the remote login account for which the public key is present; browse and supply the corresponding Private Key.

> **Note:** PAM360 supports SSH2 and above only.

iii. **Specifying the root account/selecting 'sudo'**

a. As mentioned above, for executing remote password reset commands, PAM360 can use either 'su' as root or 'sudo', which allows the user to run the command with root privileges without having to switch to the root account.
b. If you use the option, 'su' as root, select the root account.
c. If the target system allows execution of password reset commands through 'sudo', then select that option.
d. Click **Save.**



Note: You can also use SSH Command sets to configure remote password reset for the types Linux, IBM AIX, HP UX, Solaris, Mac OS, VMWare ESXi and any other Linux or Unix-based resource types.

2.1.4 IBM AS400/Sun Oracle ALOM/ILOM/XSCF Sun Oracle ALOM/ILOM/XSCF

No specific password reset configuration required for these resources as PAM360 will use the accounts added to the resources to perform the password reset.

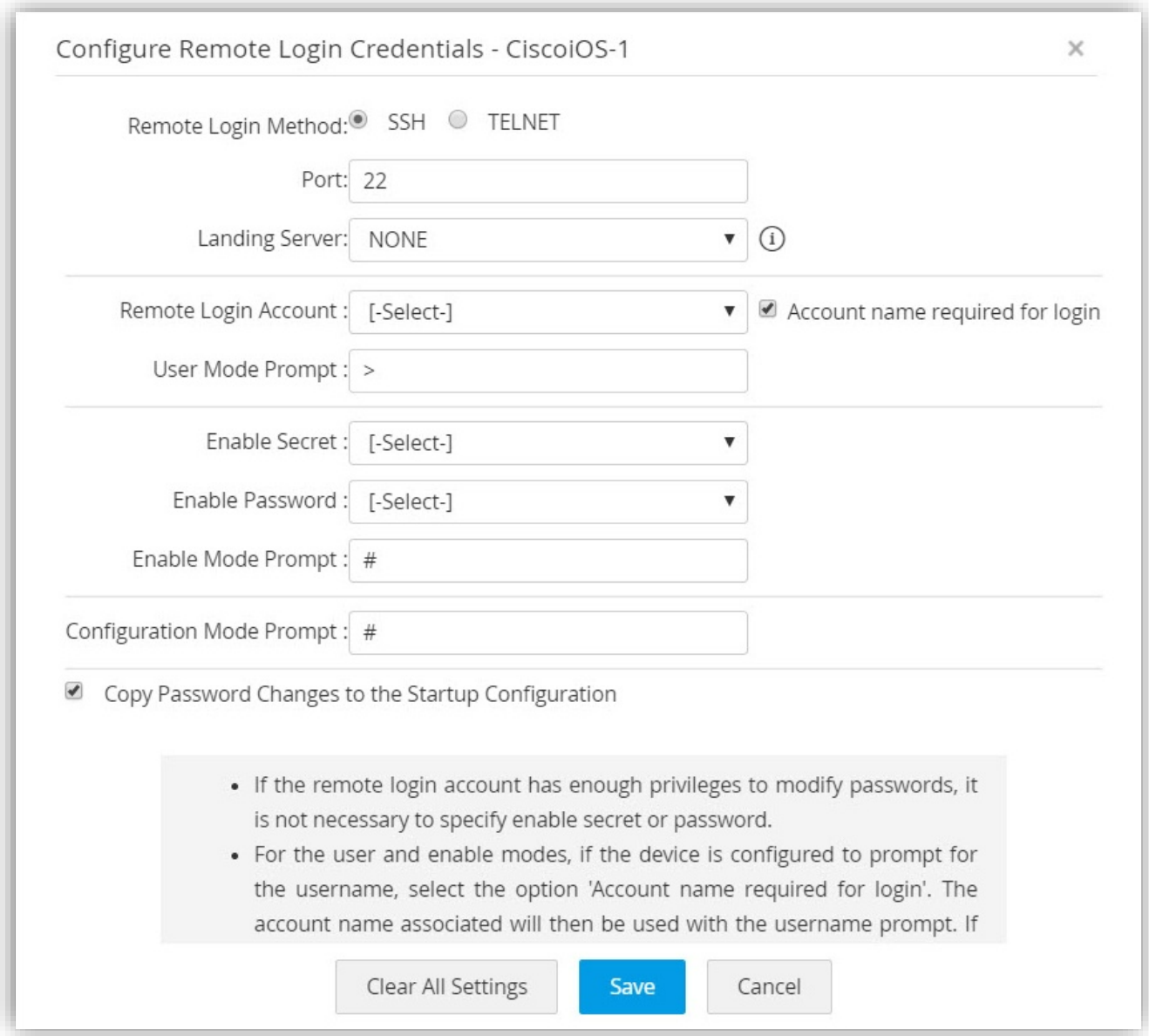
Cisco Devices

2.1.5 Cisco Devices (IOS/CatOS/PIX)

PAM360 requires Telnet or SSH service to be running in the resource. Passwords of the enable mode and a user account are required for PAM360 to log into the resource. PAM360 will use the configuration terminal mode to reset the passwords. Follow the below steps to enable remote password reset for Cisco devices:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset** and specify the following details.
    i. **Remote Login Method:** PAM360 supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol.
    ii. **Remote Login Account:** Login account for establishing connection with the device.
    iii. **Account name required for login:** For the user and enable modes, if the device is configured to prompt for the user name, then check on the option **Account name required for login.** The account name associated will then be used with the user name prompt. If this option is unchecked, PAM360 will expect only the password prompt.
    iv. **User Mode Prompt:** The prompt that appears after successful login.
    v. **Enable Secret:** This is for entering into privileged mode to perform password reset. If the remote login account has enough privileges to modify passwords, it is not necessary to specify Enable Secret.
    vi. **Enable Password:** This is for entering into privileged mode to perform password reset. If the remote login account has enough privileges to modify passwords, it is not necessary to specify Enable Password.
    vii. **Enable Mode Prompt:** This is the prompt that will appear after going into enable mode. For example, #.
    viii. **Configuration Mode Prompt:** To carry out any change to any feature/configuration of the device, you need to enter configuration mode. The prompt that will appear while going into configuration mode has to be entered here. For example, # "Primary Credentials".
    ix. **Copy Password Changes to the Startup Configuration:** Select this option to apply the password changes made to the running configuration in PAM360 to the startup configuration.

> **Note:** Enabling the option to copy the running configuration to the startup configuration will cause the current configuration content, including those made outside of PAM360, to be copied immediately.



Database Servers

2.1.6 MS SQL Server

As Password reset for MS SQL server is done over JDBC, it is required to provide either the MS SQL Administrator credentials or a domain account credentials with enough privileges to modify SQL server passwords. Follow the below steps to enable remote reset of the password of MS SQL server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the instance name of MS SQL server. If the instance name is specified, PAM360 will try to establish connection with specified instance. If not, PAM360 will try to establish connection with the specified port.
3. Specify the port where the MS SQL server is running. By default, MS SQL occupies the port 1433.

4. Specify the connection mode - you can configure the connection between MS SQL Server and PAM360 to be over an encrypted channel (SSL) or Non-SSL. If you choose **SSL mode,** do the following:

SSL Mode:

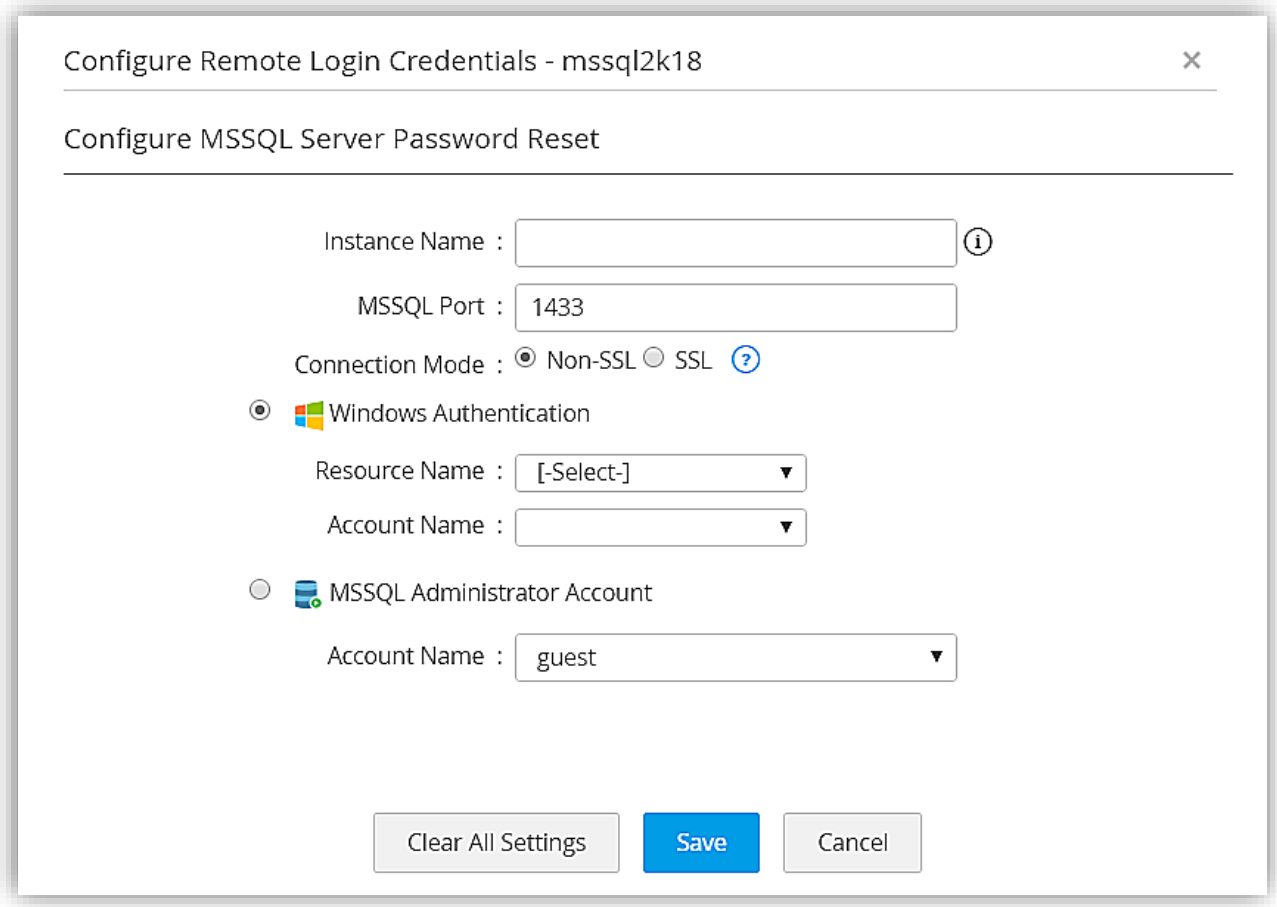
i. To enable the SSL mode, the MS SQL server should be serving over SSL and you have to import the MS SQL server's root certificate into the PAM360 server machine's certificate store. Import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.

ii. To import root certificate, open a command prompt and navigate to **<pam360_server_home>\bin** directory and execute the following command:

For Windows
importCert.bat **<Absolute Path of certificate>**

For Linux
importCert.sh **<Absolute Path of certificate>**

5. Restart PAM360 server. Then, continue with the following steps:



6. To enable PAM360 to access the MS SQL server, provide any one of the following details: **Windows Authentication** (OR) **MS SQL Administrator Account**. Select the domain name the MS SQL server is a part of and select any account present in the domain.
7. Click **Save.**

2.1.7 MySQL/PostgreSQL Server

As password reset for a MySQL/PostgreSQL server is done over JDBC, the MySQL/PostgreSQL administrator credentials are required. Follow the below steps to enable remote reset of the password of MySQL/PostgreSQL server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the port where the MySQL/PostgreSQL server is running. By default, MySQL/PostgreSQL occupies the port 3306.
3. Specify the connection mode: Connection between MySQL/PostegreSQL Server and PAM360 can be configured to be over an encrypted channel such as SSL or Non-SSL. If you choose **SSL mode,** do the following:

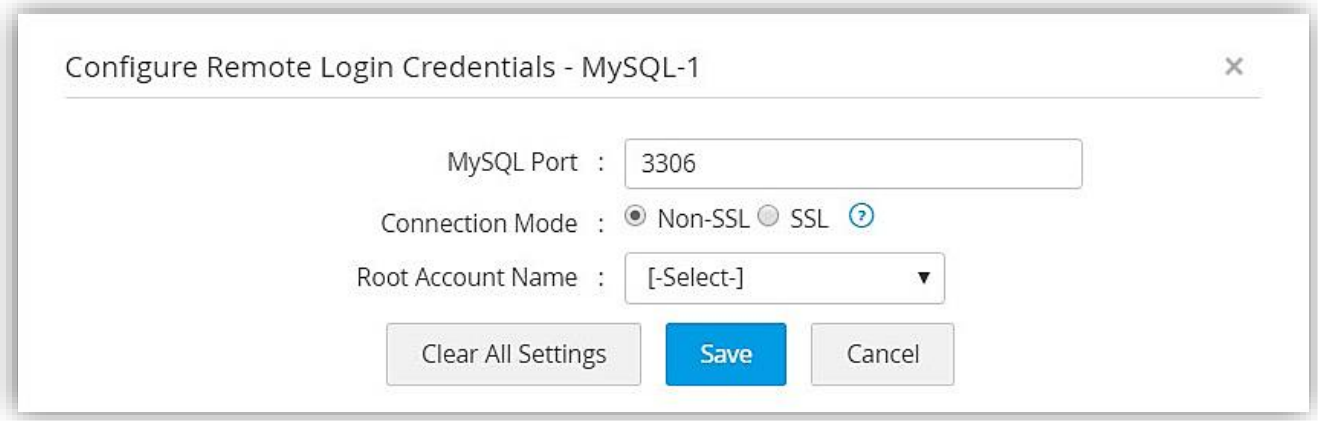
   SSL Mode:

   i. To enable the SSL mode, the MySQL/PostgreSQL server should be serving over SSL and you have to import the MySQL/PostgreSQL server's root certificate into the PAM360 server machine's certificate store. Import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.
   ii. To import root certificate, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin directory** and execute the following command:

```
For Windows
importCert.bat   <Absolute Path of certificate>

For Linux
importCert.sh   <Absolute Path of certificate>
```

4. Restart PAM360 server. Then, continue with the below steps.
5. To enable access to the MySQL server for PAM360, provide MySQL **Root Account Name.**
6. Click **Save.**


Configure Remote Login Credentials - MySQL-1
MySQL Port :
3306
Connection Mode :
Non-SSL
SSL
Root Account Name :
[-Select-]
Clear All Settings
Save
Cancel

2.1.8 Sybase ASE

Prerequisites

1. To perform remote password reset in Sybase ASE, jConnect 6.0 JDBC driver is required. The JDBC driver is a file named **jconn3.jar** which will be available under the path **<sybase_install_directory>\jConnect_6_0\classes** in Sybase ASE 15.0.
2. Copy the **jconn3.jar** file and save it under **<pam360_install_directory>\lib** folder in the machine running the PAM360 server.

Steps to Configure Remote Password Reset for Sybase ASE

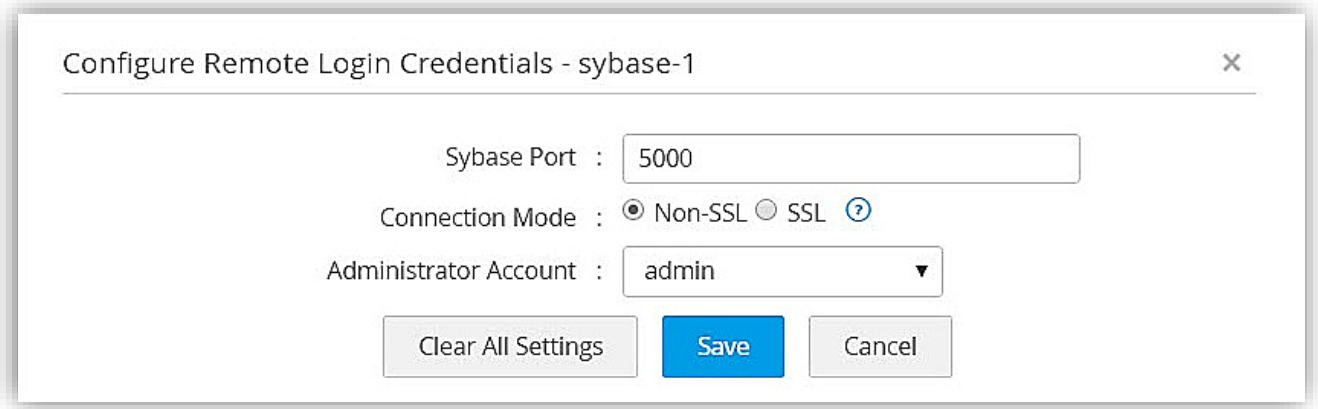
As administrative privileges are required to carry out password reset for Sybase ASE, specify an administrator account. Follow the below steps to enable remote password reset for Sybase ASE:

1. Specify the Sybase ASE Port. By default, it occupies the port 5000 (in SSL mode, default port is 2748).
2. Specify the connection mode - you can configure the connection between Sybase ASE and PAM360 to be over an encrypted channel (SSL) or Non-SSL. If you choose **SSL mode,** do the following:

   SSL Mode:

   i. Copy and save the trust root certificate of the Sybase server present under **<sybase_home>\ASE-15_0\certificates** (in sybase ASE 15.0) to **<pam360_install_directoty>\conf** folder.
   ii. Run this command to import the certificate in PAM360: **'<pam360_home>\jre\bin\keytool.exe -import -v -alias sybase -file <rootcert.txt> -keystore server.keystore -keypass passtrix -storepass passtrix -noprompt'.**
   iii. **<rootcert.txt>** is the root certificate of the Sybase ASE and usually named as **<hostname>.txt.**

3. Restart PAM360 server.
4. Specify an administrator account of Sybase ASE.
5. Click **Save**.

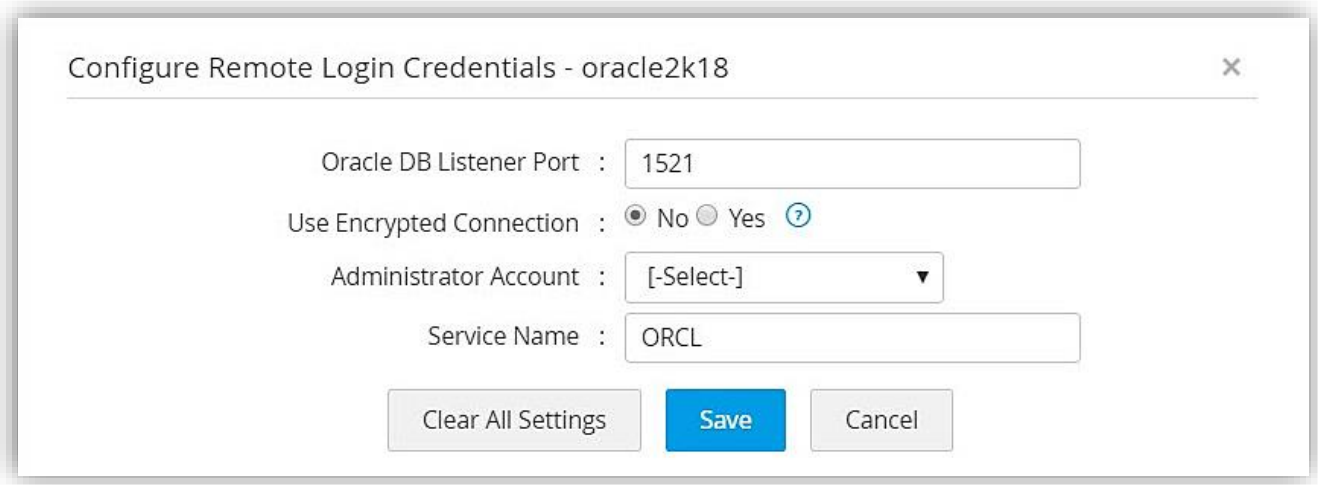


2.1.9 Oracle DB Server

Important Note: As of August 2022, Oracle extends support to the following versions of the Oracle database only: 18c, 19c, and 21c. Therefore, PAM360 will also support only these three versions of Oracle DB in the product. Refer to the Oracle Lifetime Support Policy Guide for more information.

To carry out password reset for Oracle DB server, administrative privileges are required, so specify an administrator account. Follow the below steps to enable remote reset of the password of Oracle DB server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the Oracle DB Listener Port. By default, the Oracle DB server listens to the port 1521.
3. Specify the connection mode - you can configure the connection between Oracle DB Server and PAM360 to be over an encrypted channel (AES 256). If you choose the option **YES** (encrypted mode), do the following:
    i. Start **Oracle Net Manager.**
    ii. In the Navigator window, select **Oracle Net Configuration.**
    iii. Expand the option **Local >> Profile.**
    iv. From the list in the right side pane, select the option **Oracle Advanced Security.**
    v. In the tabbed window that appears thereafter, click the tab **Encryption.**
    vi. In the drop-down list for Encryption, select the option **Server.**
    vii. For **Encryption Type** list, select the option **Accepted.**
    viii. The text field for **Encryption Seed** can be left blank or enter random characters ranging between 10 and 70.
    ix. Select the algorithm **AES 256.**
    x. Specify an Oracle administrator account.
4. Specify the Oracle Service Name. By default, the service name is taken as ORCL.
5. Click **Save.**



Network Devices

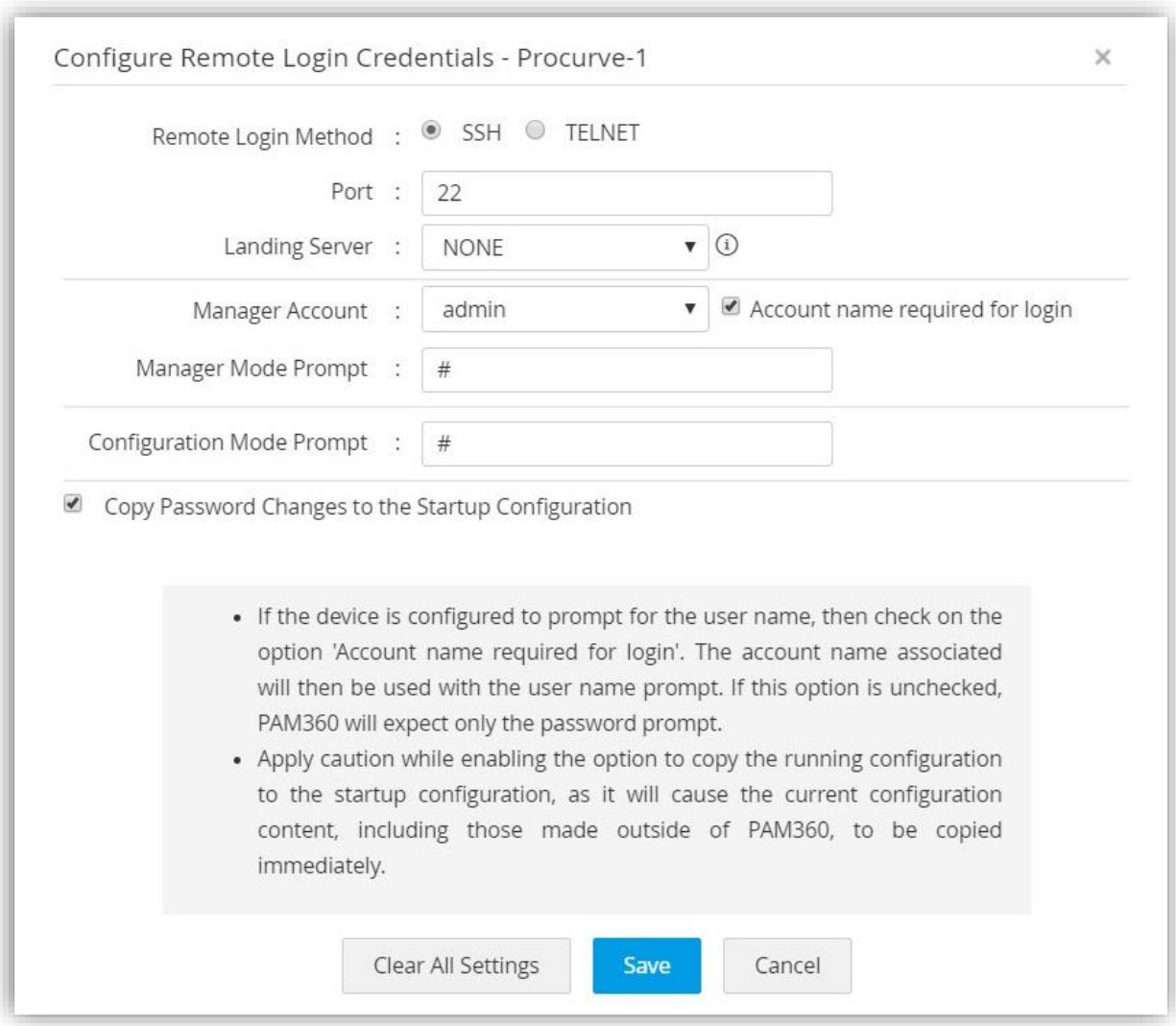
2.1.10 HP ProCurve Devices

For HP ProCurve Devices, PAM360 requires Telnet or SSH service to be running in the resource. Specify the **Manager Account** and **Manager Mode Prompt** and **Configuration Mode Prompt** details for PAM360 to login to the resource. PAM360 will use the configuration mode to reset the passwords.

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Provide the following details:

    i. **Remote Login Method:** PAM360 supports SSH and TELNET protocols through which connection could be established with the device for password reset. Select the required protocol.
    ii. **Manager Account:** Login account for establishing connection with the device. If the device is configured to prompt for the user name, then select the option **Account name required for login**. The account name associated will then be used with the user name prompt. If this option is unchecked, PAM360 will expect only the password prompt.
    iii. **Manager Mode Prompt:** The prompt that appears after successful login.
    iv. **Configuration Mode Prompt:** This is for entering into privileged mode to perform password reset.
    v. **Copy Password Changes to the Startup Configuration:** Select this option to apply the password changes made to the running configuration in PAM360 to the startup configuration.

Note: Enabling the option to copy the running configuration to the startup configuration will cause the current configuration content, including those made outside of PAM360, to be copied immediately.

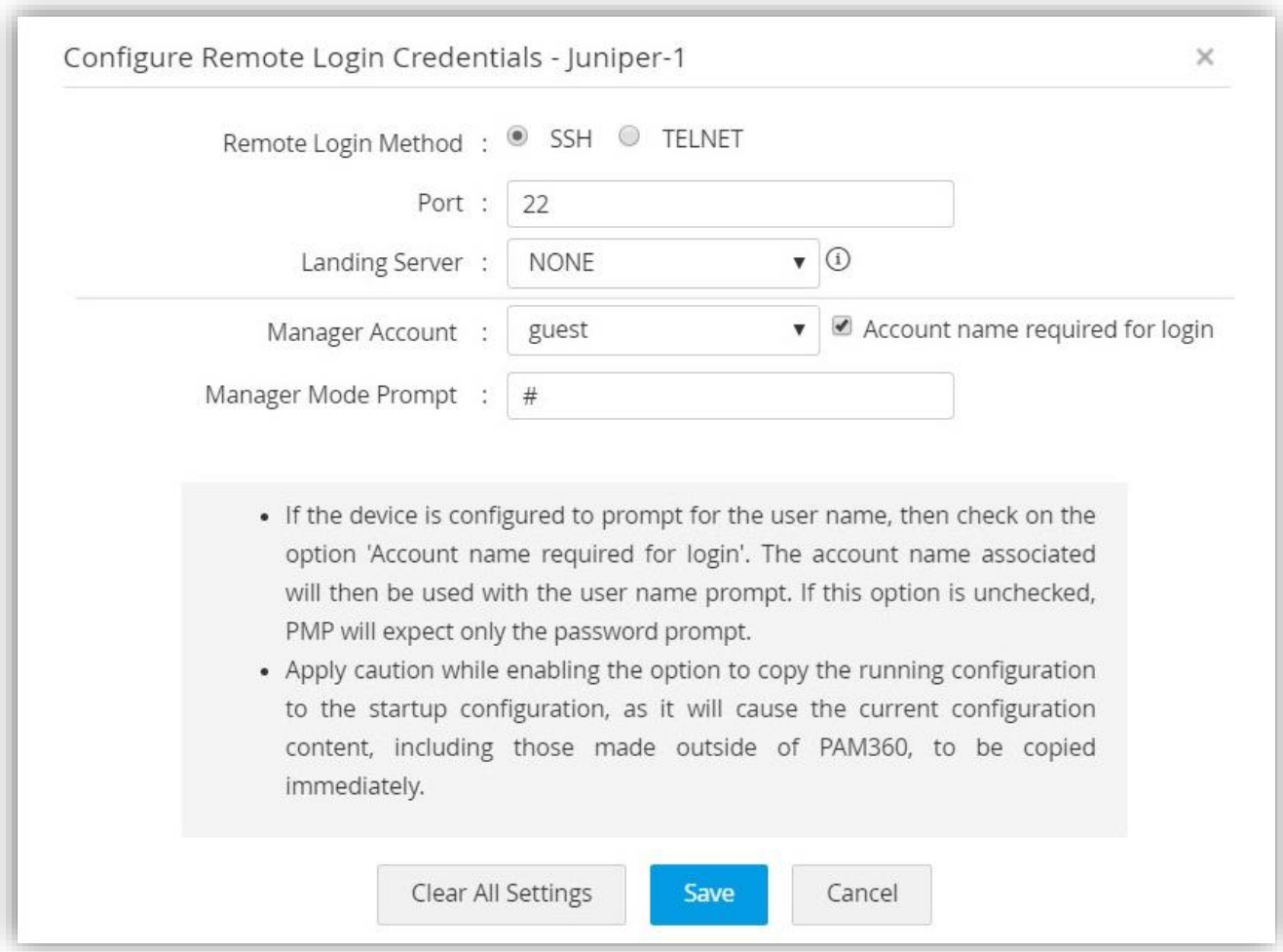


2.1.11 Juniper Netscreen Firewall Devices

PAM360 requires Telnet or SSH service to be running in the resource. Admin Account and Prompt of Admin Account are required for PAM360 to login to the resource. Follow the below steps to enable remote reset of passwords for Netscreen devices:

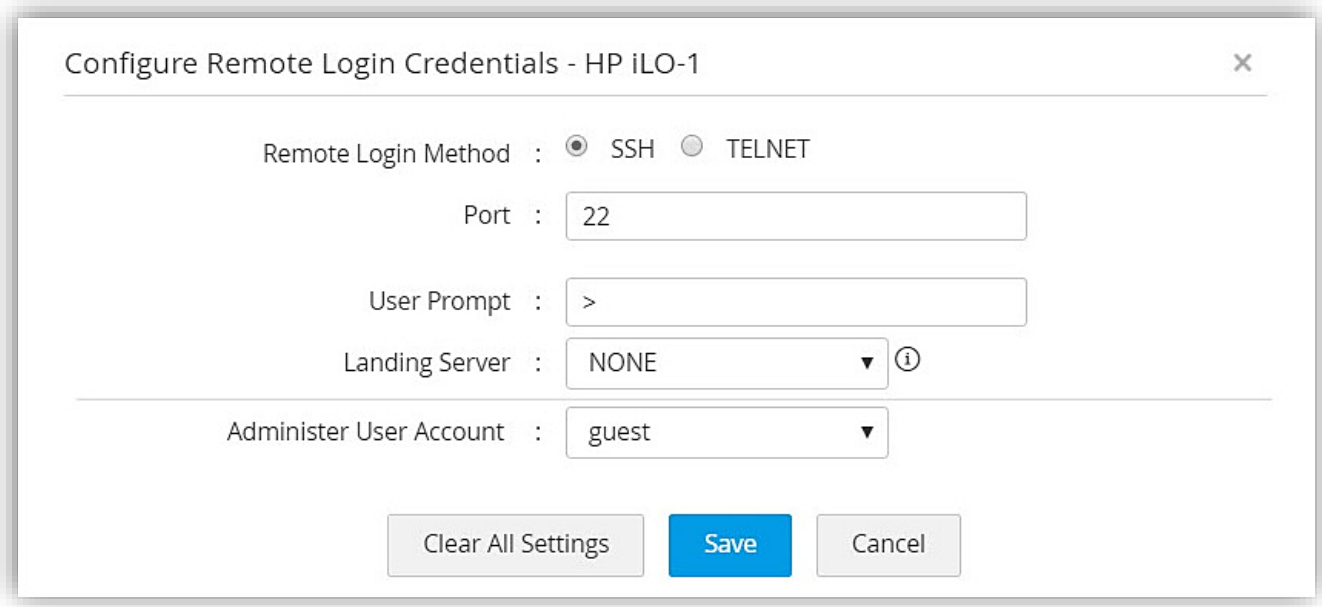
1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset** and specify the following details.

    i. **Remote Login Method**: PAM360 supports SSH and TELNET protocols by which connection could be established with the device for password reset. Select the required protocol.
    ii. **Manager Account**: Login account for establishing connection with the device. If the device is configured to prompt for the user name, then check on the option **Account name required for login.** The corresponding account name will then be used with the user name prompt. If this option is unchecked, PAM360 will expect only the password prompt.
    iii. **Manager Mode Prompt**: The prompt that appears after successful login.



2.1.12 HP iLO

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset** and enter the following details:
    i. **Remote Login Method:** PAM360 supports SSH and TELNET protocols by which connection could be established with the device for password reset. For this to work, Telnet or SSH service must be running in the resource.
    ii. **Enter the port:** By default, SSH occupies the port 22.
    iii. **Specify the prompt**: Enter the prompt that appears upon successful user login and also the user account with administrator privileges.



Cloud Services

2.1.13 Oracle WebLogic Server

As Password reset for a WebLogic server is done over JMX, the administrator credentials must be specified before proceeding with the below steps.

Prerequisites

1. The following JAR files **wljmxclient.jar, wlclient.jar, rmic.jar, weblogic.jar** will be available under the path **<weblogic_install_directory>\wlserver\server\lib>** in the WebLogic server.
2. Copy the JAR files and save them in the **\lib** folder in the machine running the PAM360 server.

Steps to Configure Remote Password Reset for Oracle WebLogic Server

Follow the below steps to enable remote reset of the password of the WebLogic server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the port where the WebLogic server is running. By default, WebLogic server occupies the port 7001. Specify the connection mode - connection between WebLogic Server and PAM360 can be configured to be over an encrypted channel such as SSL or Non-SSL. **If you choose SSL mode, do the following.**

   SSL Mode:

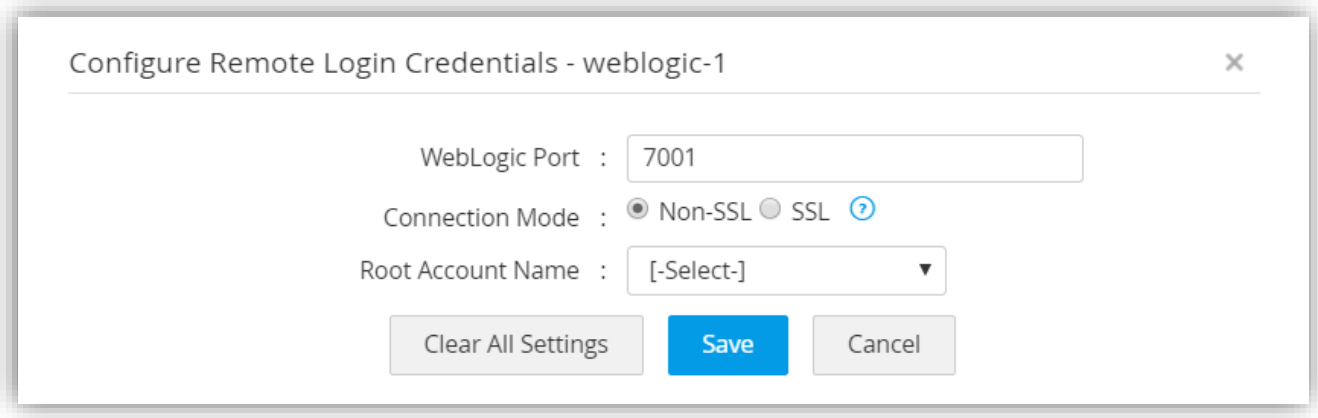
   i. To enable the SSL mode, the WebLogic server should be serving over SSL and you have to import the WebLogic server's root certificate into the PAM360 server machine's certificate store. Import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.

   ii. To import root certificate, open a command prompt, navigate to **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

```
For Windows
importCert.bat   <Absolute Path of certificate>

For Linux
importCert.sh   <Absolute Path of certificate>
```

3. Restart the PAM360 server. Then, continue with the following steps.
4. To enable PAM360 access the WebLogic server, provide the WebLogic **Root Account Name.**
5. Click **Save.**

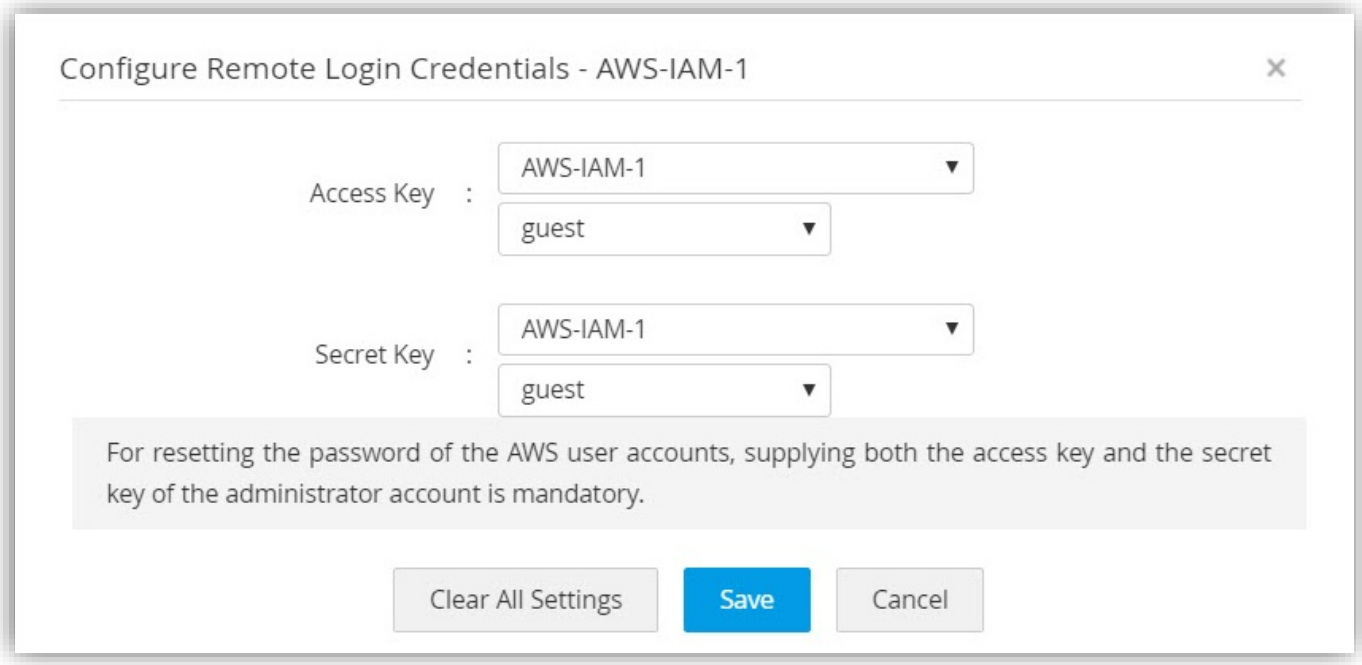


2.1.14 AWS IAM

1. Password reset for AWS IAM user accounts is done using AWS SDK.
2. Navigate to the **Resources tab >> Resource Actions >> Configure Remote Password Reset.**

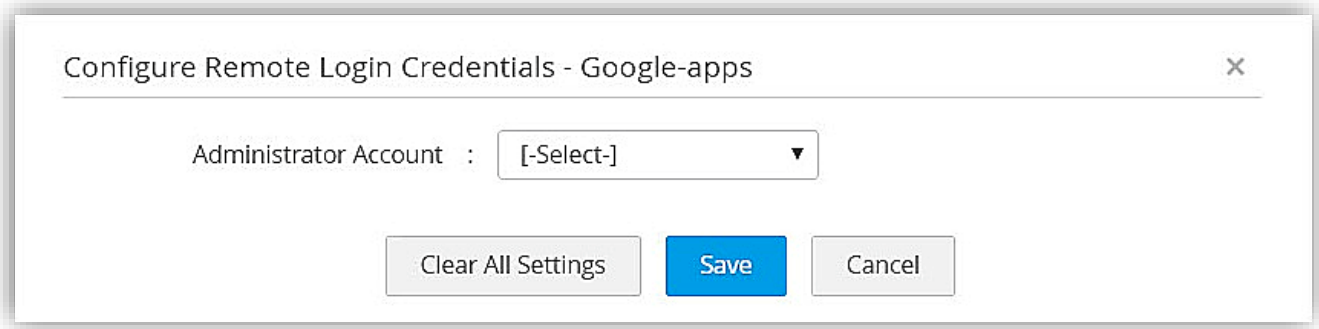
The administrator account's access key and secret key are required.

3. The access key and secret key should have been added as passwords in PAM360. These passwords can be associated with an account of any resource type, which can be used for the remote synchronization.



2.1.15 Google Apps

1. Password reset for Google Apps is done using Google Data APIs.
2. To enable the Password reset option for GApps, select an administrator account has so that it can be used to reset the passwords of other admin/user accounts.



2.1.16 Microsoft Azure

Remote Password Reset using MS Online Module:

(This reset procedure is applicable prior to build 6000)

Prerequisites

Password Reset for Microsoft Azure accounts is done using Powershell so works only if Powershell 2.0 and above. Also, the MSOnline module of Powershell needs to be installed.

Installing Windows Azure AD Module for Powershell:

Before configuring Microsoft Azure with PAM360, install the appropriate version of the Windows Azure AD Module for Windows PowerShell for your OS.

For 64-bit Systems

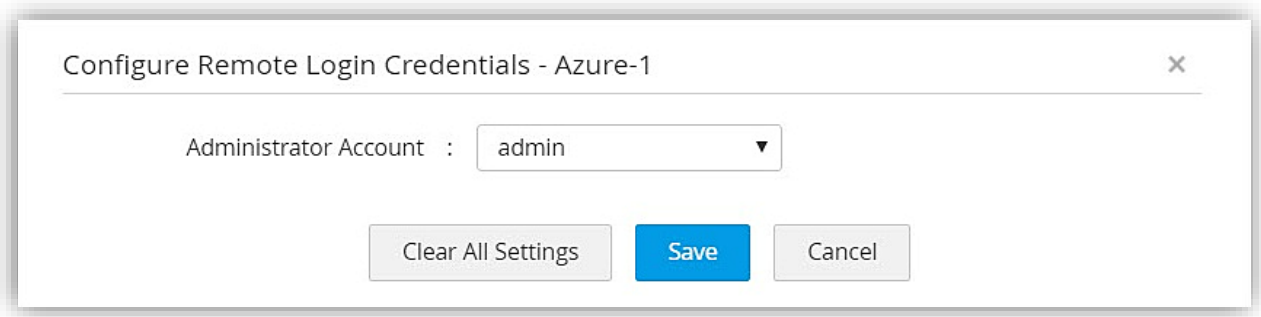
1. Open **Powershell** (run as Administrator).
2. Execute the following command to install **MSOnline** module:
   - *Install-Module MSOnline*
3. After installing the module, move **MSOnline** folder from the path **C:\Program Files\WindowsPowerShell\Modules** to **C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules.**

> **Note:** If you are unable to locate the **MSOnline** folder, execute the following command to find the path where the module is installed:
>
> - *$env:PSModulePath -split ";"*

Configuring Remote Password Reset for Microsoft Azure:

For resetting the passwords of user accounts, select an administrator account to enable remote login.

1. Navigate to the **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Select an **Administrator Account** and click **Save**.



Remote Password Reset using Azure Application:

(This reset procedure is applicable from build 6000)

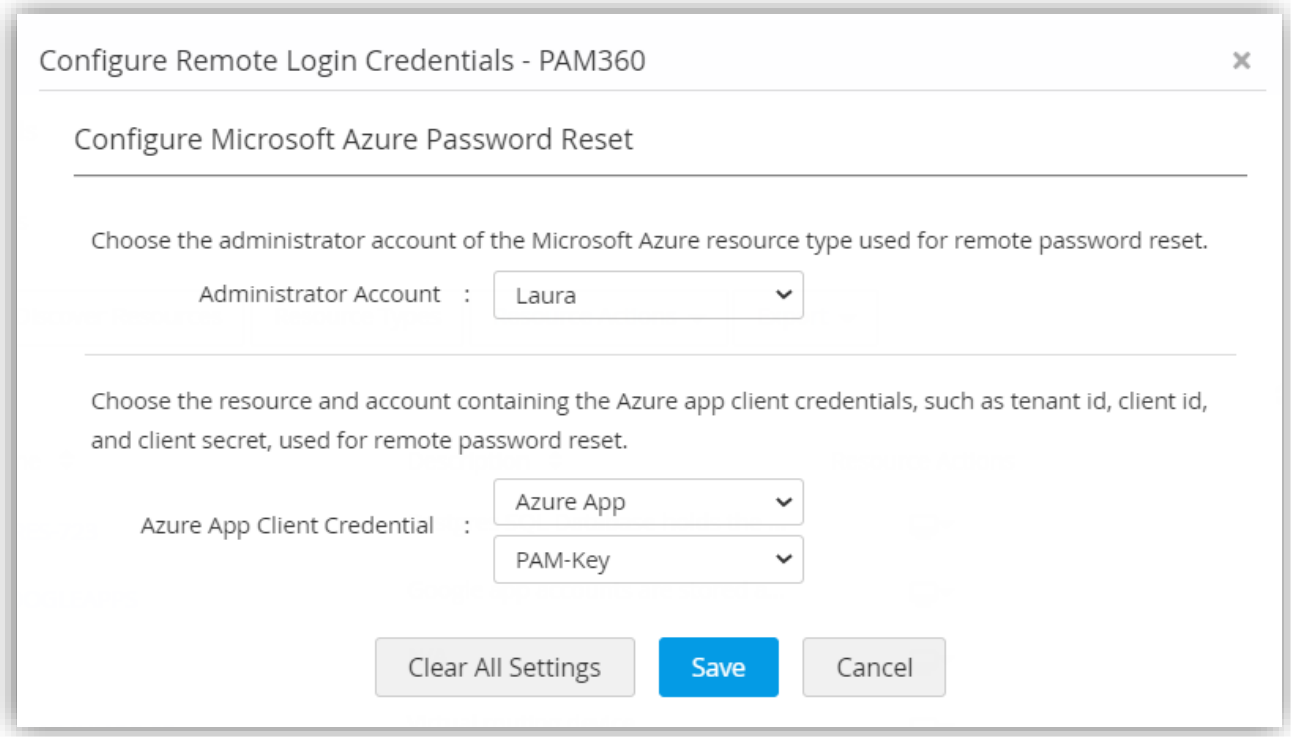
Prerequisites:

An Azure app and a privileged account are required to reset passwords for Microsoft Azure resources. The Azure App should be created in Microsoft Azure with the appropriate permission and imported as a resource in the PAM360 interface before performing the remote password reset.

Configuring Remote Password Reset for Microsoft Azure:

Do the steps that follow to perform the remote password reset from the PAM360 interface:

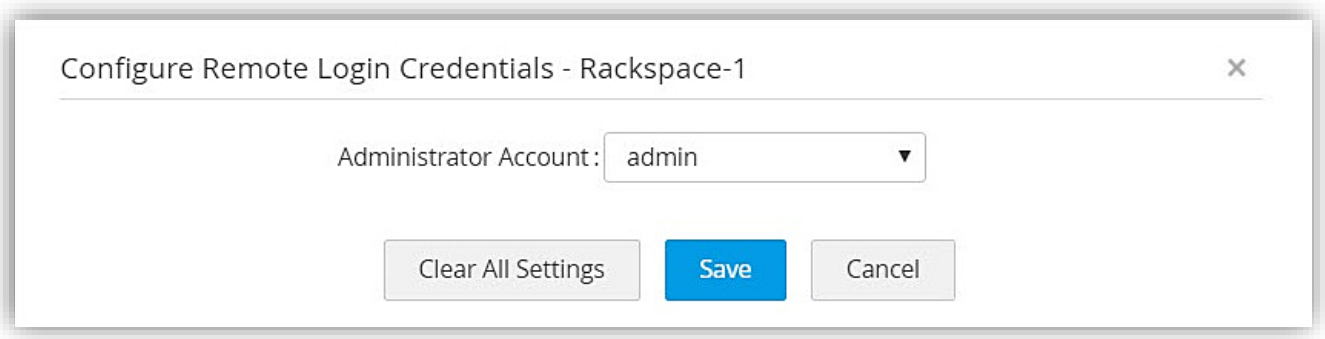
1. Click the **Resource Actions** drop-down menu beside the Microsoft Azure resource and Select **Configure Remote Password Reset.**
2. In the pop-up that opens, select an **Administrator Account** and an **Azure App Client Credentials** stored as a resource in PAM360.
3. Click **Save** to perform the reset.



2.1.17 Rackspace

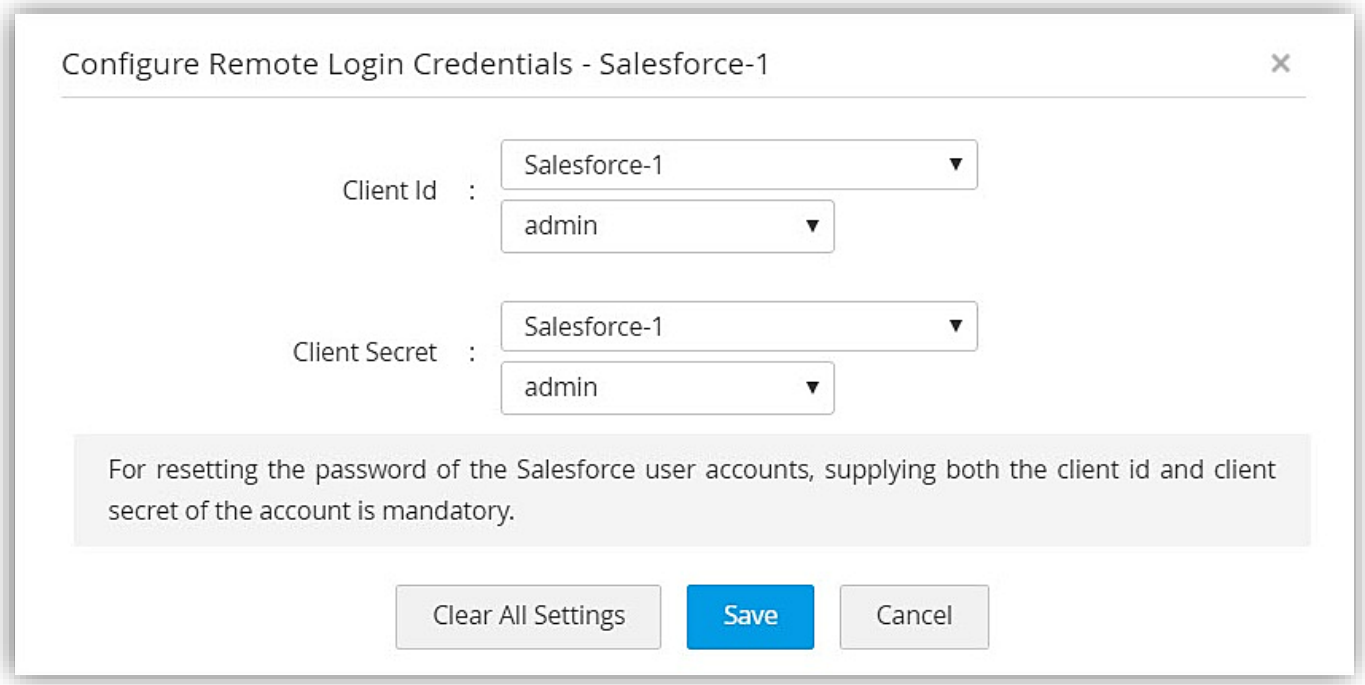
1. Password Reset for Rackspace user accounts is done using Rackspace REST APIs.
2. To carry out password resets, navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.** Here, a Rackspace administrative credential is required which has to be selected as the admin account.

> **Note:** The following are the location-based Authentication End Points available for connection to the server.
>
> **US-based end point:** https://identity.api.rackspacecloud.com/v2.0
>
> **UK-based end point:** https://lon.identity.api.rackspacecloud.com/v2.0



2.1.18 Salesforce

1. Password reset for Salesforce user accounts is done using Force.com REST API.
2. In order to proceed with the configuration, navigate to **Resources** >> **Resource Actions >> Configure Remote Password Reset.** The administrator account's **Client ID** and **Client Secret** are required.
3. The **Client ID** and **Client Secret** should have been added as passwords in PAM360. These passwords can be associated with an account of any resource type, which can be used for remote synchronization.



2.1.19 Amazon Aurora PostgreSQL

Follow the below steps to enable remote reset of the password of Aurora PostgreSQL server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the **Port** where the PostgreSQL server is running.
3. Specify the connection mode: Connection between PostegreSQL Server and PAM360 can be configured to be over an encrypted channel such as SSL or Non-SSL. **If you choose SSL mode, do the following:**

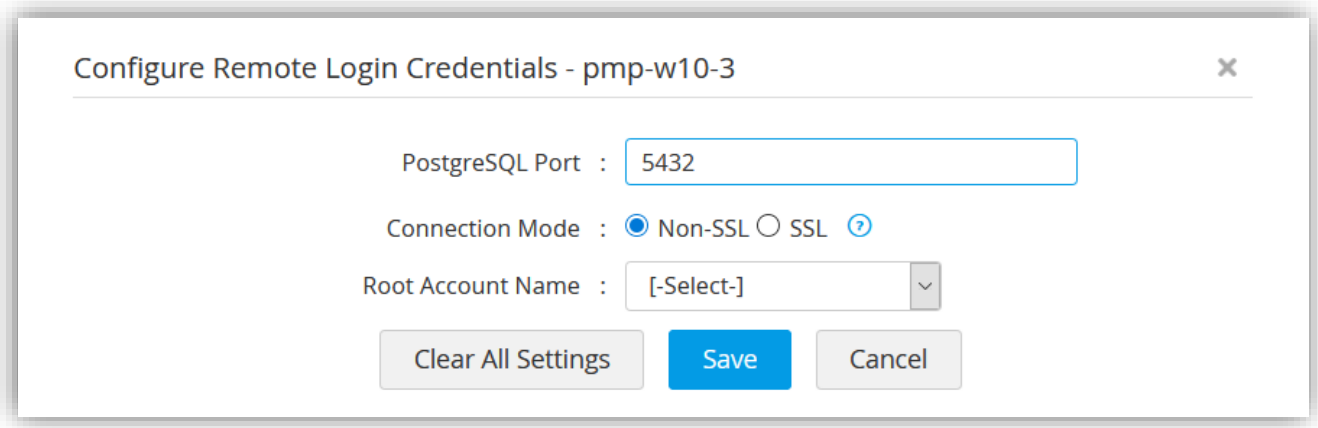
   SSL Mode:

   i. To enable the SSL mode, the PostgreSQL server should be serving over SSL and you have to import the PostgreSQL server's root certificate into the PAM360 server machine's certificate store. Import the rds-ca-2019-root.pem certificate.
   ii. To import root certificate, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin directory** and execute the following command:

For Windows
importCert.bat <Absolute Path of certificate>

For Linux
importCert.sh <Absolute Path of certificate>

4. Restart PAM360 server and reset the password for your account. To know more about changing password for your account, click here.



2.1.20 Amazon Aurora MySQL

Follow the below steps to enable remote reset of the password of Aurora MySQL server:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the **Port** where the MySQL server is running.
3. Specify the connection mode: Connection between MySQL Server and PAM360 can be configured to be over an encrypted channel such as **SSL** or **Non-SSL.** If you choose **SSL mode**, do the following:

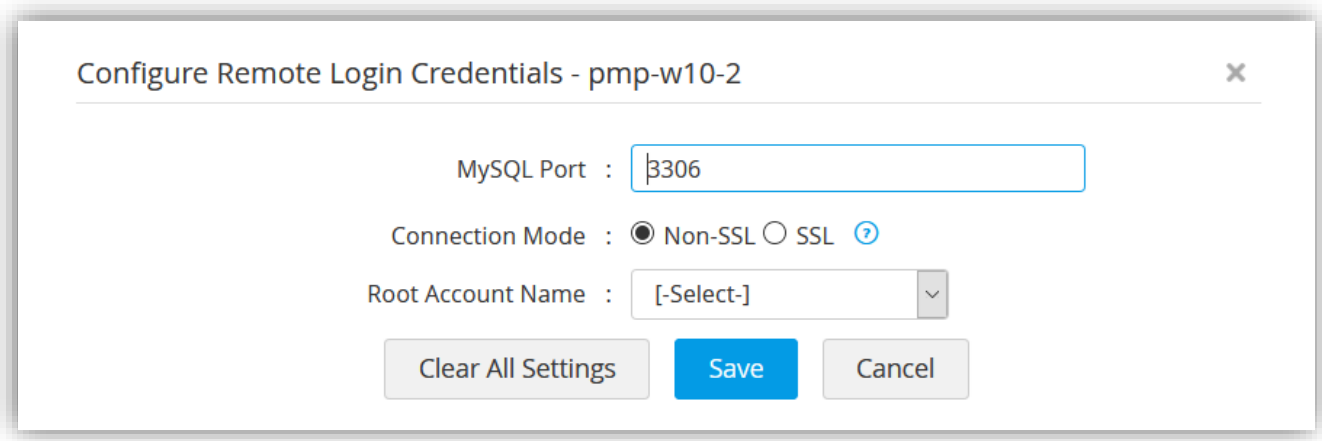
   SSL Mode:

   i. To enable the SSL mode, the MySQL server should be serving over SSL and you have to import the MySQL server's root certificate into the PAM360 server machine's certificate store. Import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.
   ii. To import root certificate, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin directory** and execute the following command:

For Windows
importCert.bat <Absolute Path of certificate>

For Linux
importCert.sh <Absolute Path of certificate>

4. Place the MySQL Connector jar in the **PAM360\lib** folder.
5. Restart PAM360 server and reset the password for your account. To know more about changing password for your account, click here.



RabbitMQ

2.1.21 RabbitMQ

Prerequisite

To perform remote password reset for a RabbitMQ resource from PAM360, you need a RabbitMQ administrator account.

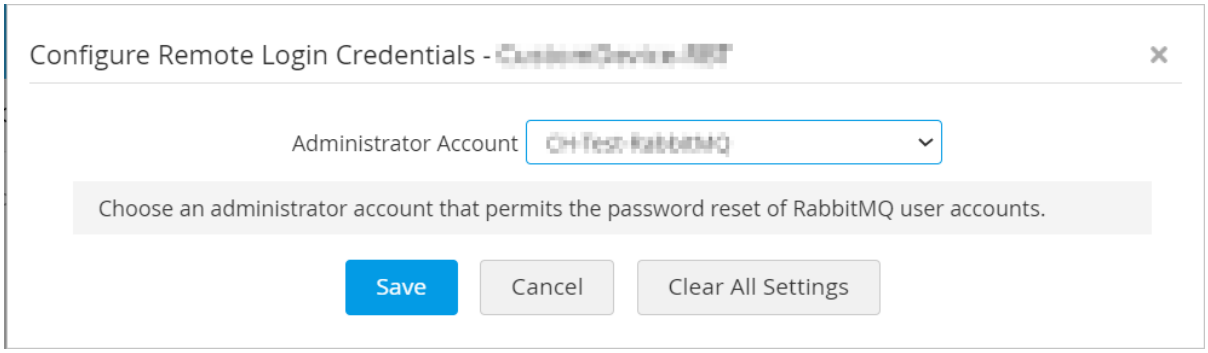
Steps to add a RabbitMQ resource and an administrator account:

1. Navigate to **Resources** and click **Add Resource >> Add Manually**.
2. Specify the resource name, DNS name/IP address, Resource URL, and select **RabbitMQ** as your resource type.
3. Click **Save & Proceed**.
4. In the Add Accounts window, add an administrator account and the other required accounts for the RabbitMQ resource. Click **Save & Proceed**.

Note: When adding a RabbitMQ resource, entering a valid HTTPS URL in the Resource URL field is mandatory.

Steps to configure remote password reset for RabbitMQ:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset**.
2. From the **Administrator Account** dropdown, select the required RabbitMQ administrator account that permits the password reset of RabbitMQ user accounts.
3. Click **Save**.



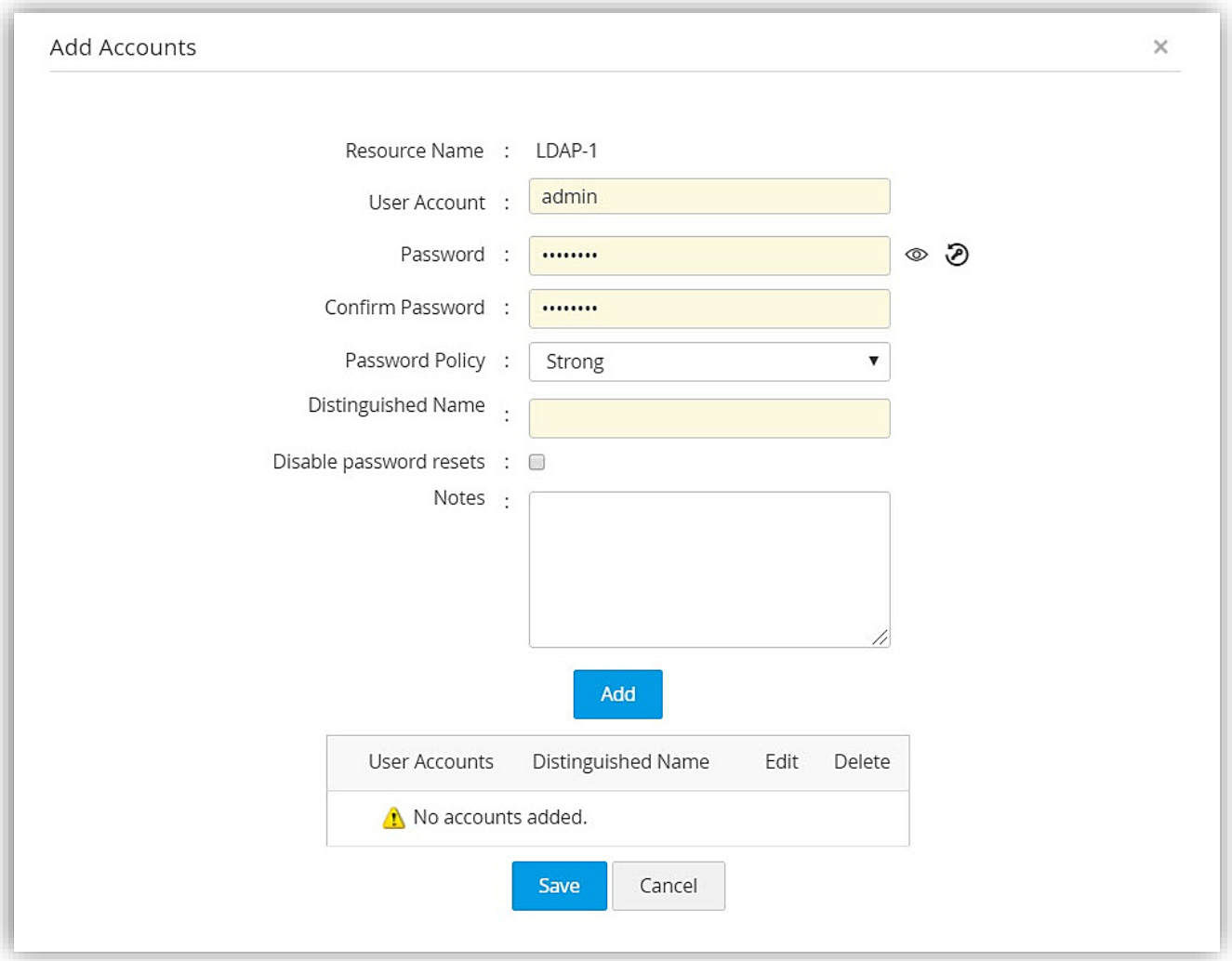
Others

2.1.22 LDAP Server

Prerequisite

At the time of adding a new LDAP resource to PAM360, you must specify a **Distinguished Name** for the LDAP server account.

Example: c=administrator, cn=people, dc=test, dc=com.



Steps to Configure Remote Password Reset for LDAP Server

As administrative privileges are required to carry out password reset for LDAP server, an administrator account has to be specified.

For remote reset, PAM360 supports the following types of LDAP servers:

- **Microsoft Active Directory**
- **OpenLDAP**
- **Oracle Internet Directory**
- **Novell eDirectory.**

Follow the below steps to enable remote password reset for the aforementioned types of LDAP servers:

1. Navigate to **Resources >> Resource Actions >> Configure Remote Password Reset.**
2. Specify the type of the LDAP Server being added.
3. Specify the LDAP server Port. By default, it occupies the port 389 (in SSL mode, default port is 636).

4. Specify the connection mode - you can configure the connection between the LDAP server and PAM360 to be over an encrypted channel (SSL) or Non-SSL. Except Microsoft Active Directory, for other LDAP servers, choose SSL or Non-SSL. If you choose SSL mode, do the following.

> **Note:** If the selected LDAP server is Microsoft Active Directory, the connection has to be through SSL only.

SSL Mode:

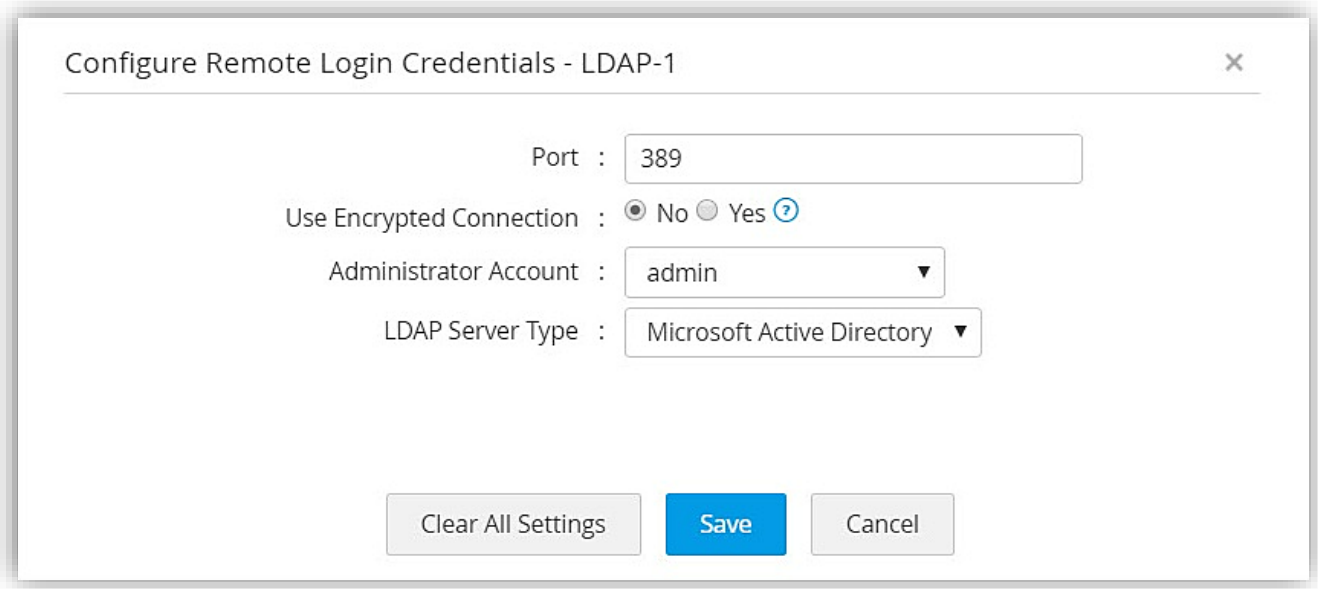
i. To enable the SSL mode, the LDAP server should be serving over SSL and you will have to import the LDAP server's root certificate into the PAM360 server machine's certificate store. You need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the PAM360 server machine and intermediate certificates, if any.

ii. To import root certificate, open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory and execute the following command:

For Windows
importCert.bat **<Absolute Path of certificate>**

For Linux
importCert.sh **<Absolute Path of certificate>**

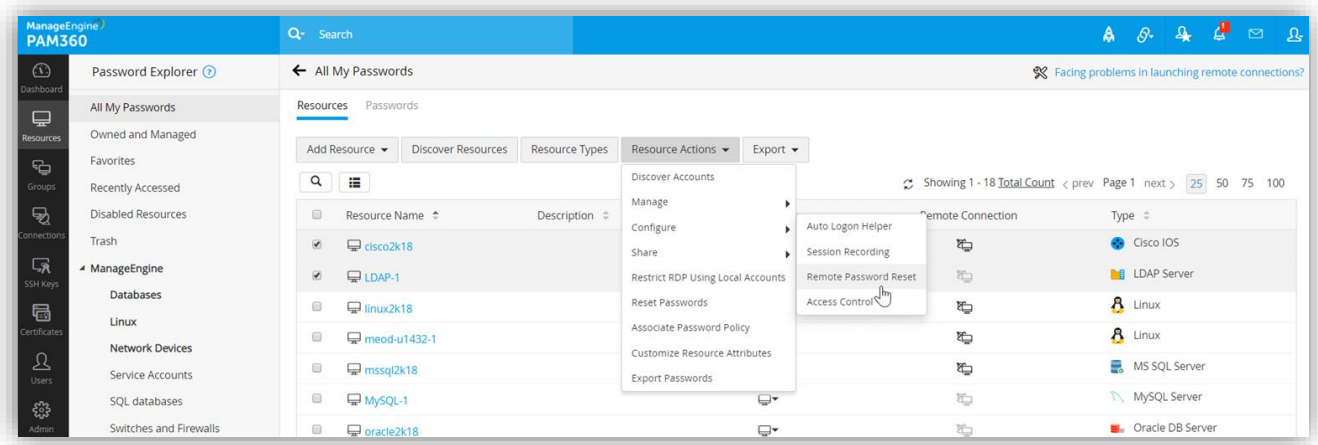
5. **Restart PAM360 server.** Then continue with the following steps.
6. Specify an administrator account of LDAP server.
7. Click **Save.**



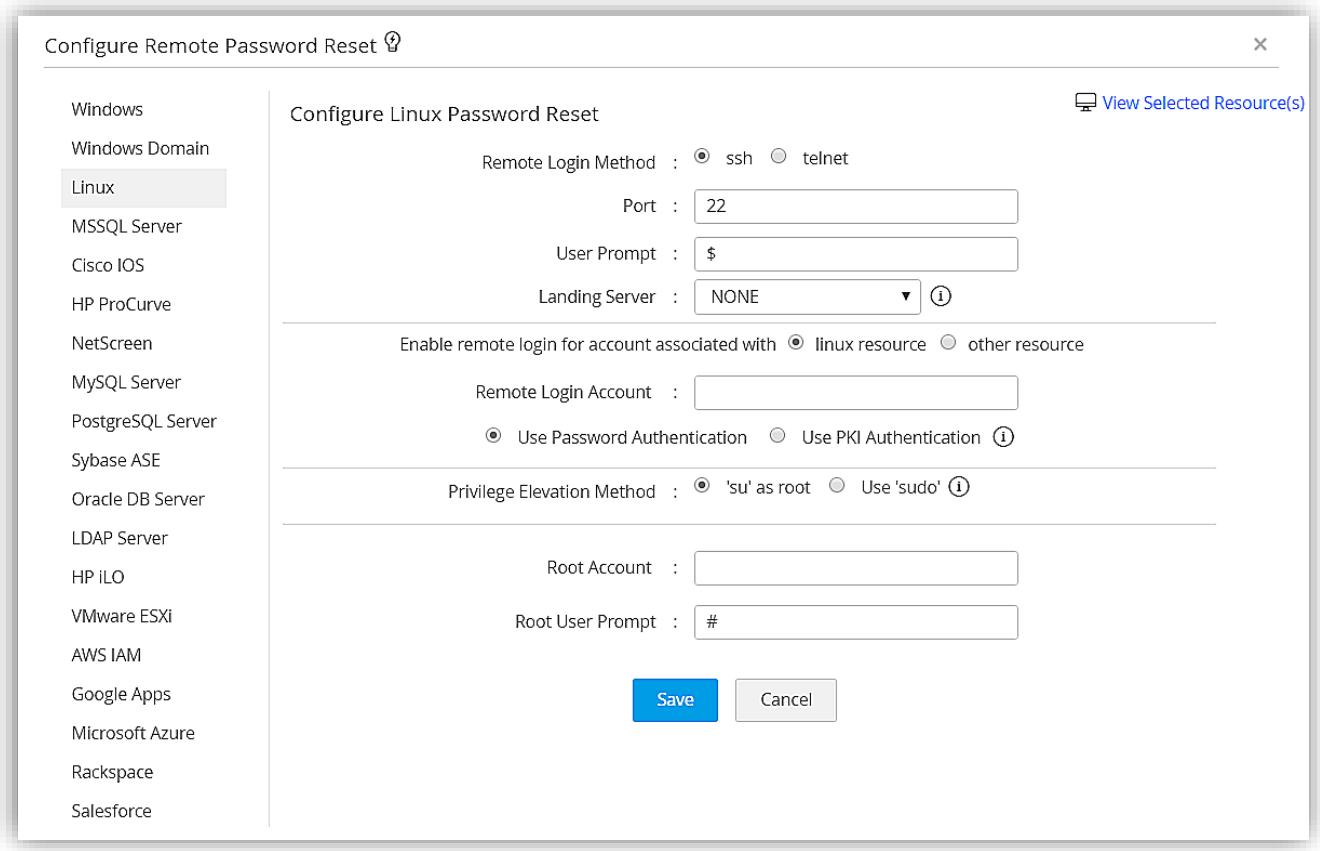
2.2 Configuring Remote Password Reset for Resource Types in Bulk

To configure remote password reset in bulk for the supported resource types, follow the below steps:

1. Navigate to **Resources** tab and select the required resources.
2. Go to **Resource Actions >> Configure >> Remote Password Reset.**



3. In the **Configure Remote Password Reset** window that opens, all the available resources will be listed. Enter configuration settings individually and save changes. Refer to section 2 for more details on how to configure password reset for each resource type.



3. Remote Password Reset via Agent Mode

- If you have devices residing in a demilitarized zone (DMZ) or if you have multiple sites/networks protected by firewalls, then PAM360 will not have direct connectivity to those target systems. In such cases, use the PAM360 Agents to manage the passwords of those target systems. PAM360 Agents operate using a one-way communication from the target system to the PAM360 application server. Therefore, the ports do not have to be opened for inbound traffic in the target network. Only outbound access is required for the PAM360 Agent to reach the PAM360 login page (Default port: 8282).
- To download the PAM360 Agent, navigate to the **Admin tab >> PAM360 Agents.** There are 64-bit and 32-bit agents for Windows, Windows Domain, and Linux. Among this, the **Windows Domain Agent** needs to be deployed in a DMZ domain controller. Click the next help section to know more about PAM360 Agents.

Password Reset Using the PAM360 Agent

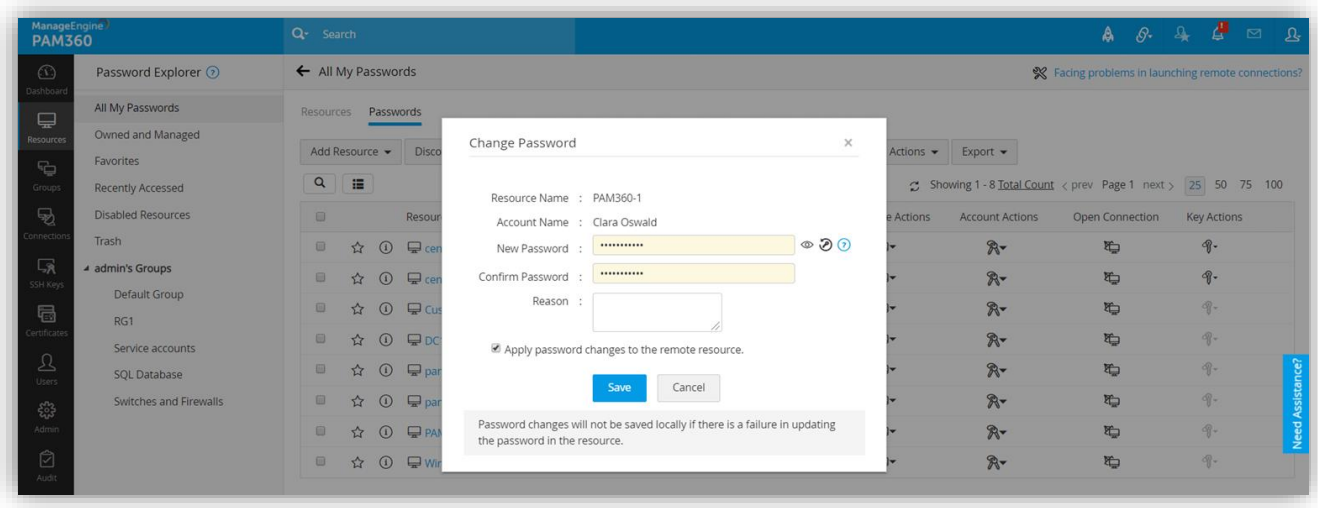
By deploying the PAM360 agent, you can reset the password of remote resources that are not connected to the PAM360 server. This document details the steps to reset passwords for local accounts that are discovered by the PAM360 agent. To know more about installing and configuring the agent, click here. Once the agent is deployed in the target machines, it will communicate with PAM360 and carry out the password changes.

1. Remote Password Reset using the PAM360 Agent
2. Troubleshooting Steps

1. Remote Password Reset using the PAM360 Agent

When the agent is started for the first time on the target machine, it will automatically add the machine as a resource in PAM360 and automatically discover the local accounts. Follow the below steps to change the passwords of the local accounts from the target machine in which the agent is installed.

1. Navigate to the **Resources** tab.
2. Click the resource added by the agent. All the accounts belonging to that resource will be listed.
3. Click the **Account Actions** icon beside the account for which password has to be changed remotely and click **Change Password** from the drop down.



4. In the **Change Password** dialog box, enter the new password. Select the **Apply password changes to the remote resource** option to apply the password changes automatically in the remote resource.
5. Click **Save**.

2. Troubleshooting Steps

Check for the following if the password reset does not take effect in the target systems:

1. Check if the user account in which the agent is installed has sufficient privileges to make password changes.
2. By default, the agent tries to communicate with the PAM360 web server through the port 8282. If you changed the default port of PAM360 to any other port such as 443, allow the agent to communicate with the server through the same port.
3. Check if the ServerName mentioned in the **agent.conf** file is reachable, if not then change it into a reachable IP address or server for the agent to be able to establish a successful connection with the PAM360 web server.
4. If you are unable to see an added resource, check if the UserName updated in the **agent.conf** file is reachable.

Configuring Remote Password Reset for Resources in Bulk

PAM360 provides remote password reset' support for a wide range of target systems. To configure remote password reset, you need to provide the administrator credentials while adding the resource. However, if you are importing the resources in bulk, associating the admin credentials for each resource would require you to manually edit each resource one by one, which would be cumbersome. So, PAM360 provides a bulk edit option to enable editing of the resources in bulk for entering the credentials.

You can select one or more resources and configure remote password reset for the chosen resources in bulk. For every chosen resource type, you need to enter the details that are required to perform remote password reset.

Editing Resources in Bulk and Configuring Remote Password Reset

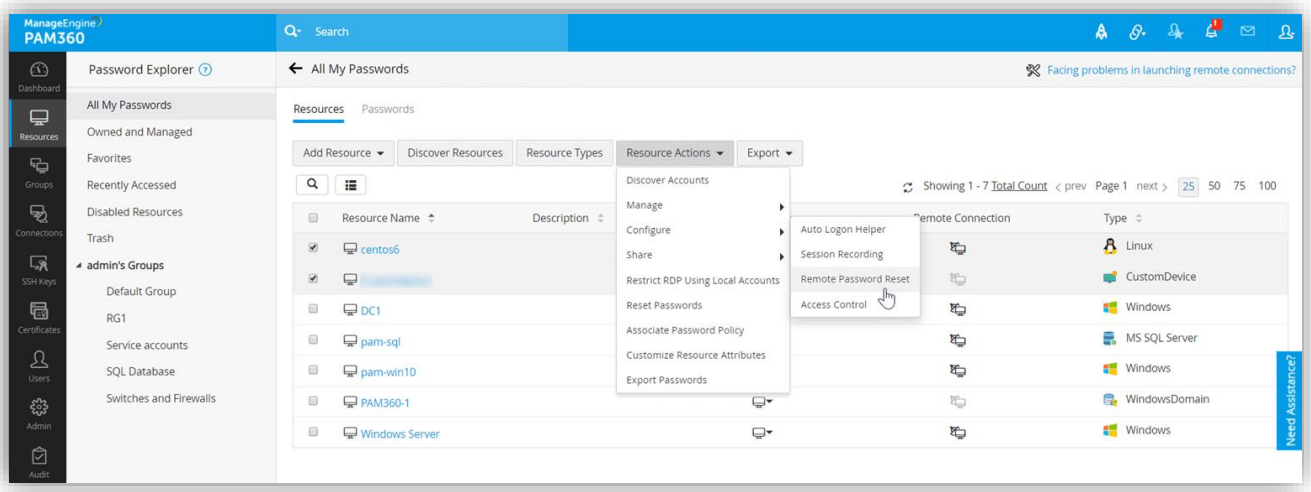
The basic design of the bulk resources edit feature is that the same configuration will be applied to all the resources of a particular resource type.

For example, assume that you want to configure remote password reset for 20 resources - 10 Windows resources and 10 Linux resources. Also assume that you have provided the credentials for all the chosen 20 resources, including the Linux resources. But, the credentials will be applied only to the 10 Windows resources and not for the Linux resources. However, after applying the credentials for the Windows resources, if you provide the credentials for the Linux resources, it will be updated for the remaining 10 Linux resources. So you must ensure that you choose only the resources of similar configuration.

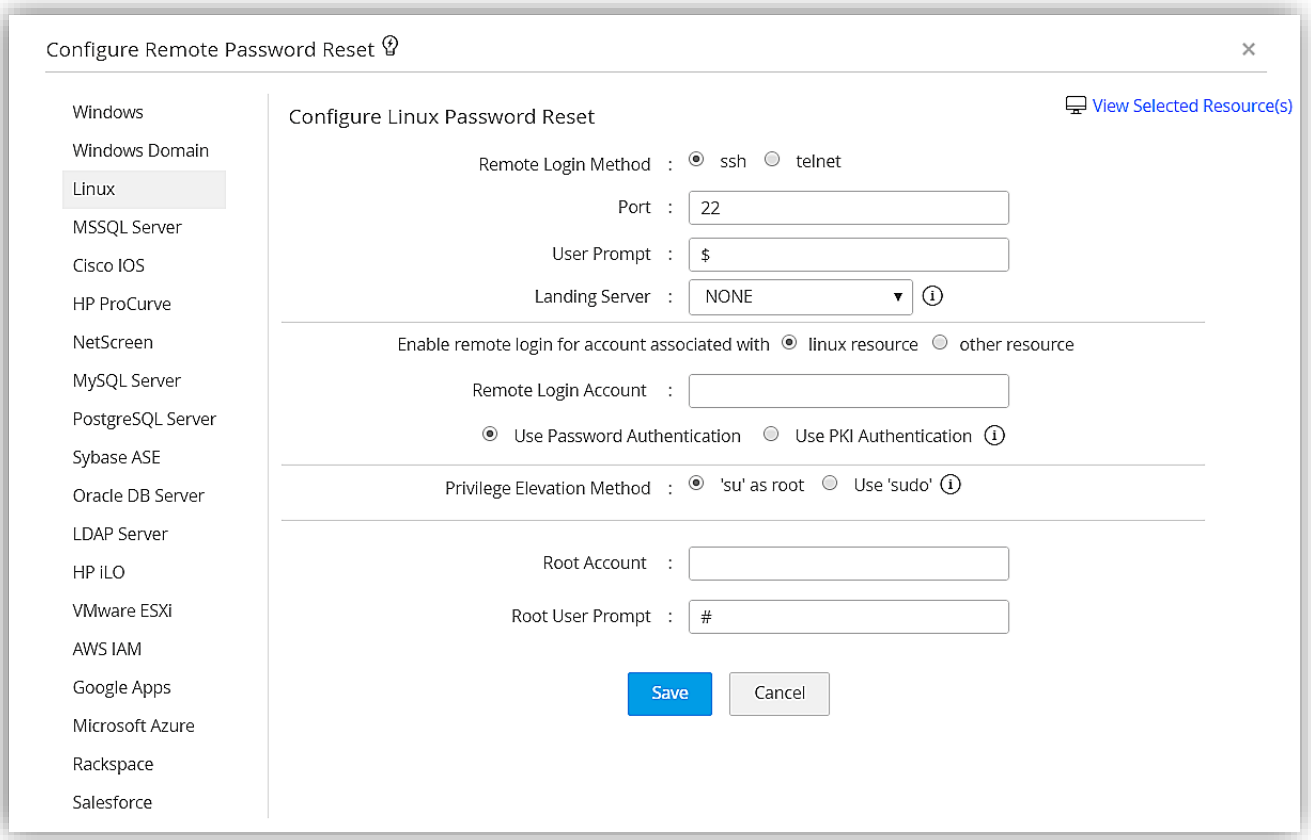
> **Note:** This bulk edit operation will simply overwrite the current password reset configuration, if any, of the chosen resources.

To Configure remote password reset for resources in bulk:

1. Navigate to **Resources** tab and select the desired resources to configure remote password reset.
2. Click **Resource Actions** from the top and select **Configure Remote Password Reset** from the drop-drown.



3. In the new dialog box that opens, select the required resource type from the list shown on the left hand side.
4. Enter the credentials based on the resource type chosen.
5. Click **Save.**



After completion, all the chosen resources will be updated with the new credentials.

Periodic Password Reset

IT security best practices recommend that passwords of sensitive resources must be reset periodically to prevent unauthorized access. PAM360's periodic password reset feature helps you achieve this by automating the process of scheduled password rotation, thereby eliminating manual password change procedures. While PAM360 provides remote password reset support for a wide range of individual target systems, scheduled password rotation can be done only at a resource group level. Password resets can be carried out either by agent-less mode or by deploying PAM360 agents in the remote resource.

Multiple options are available to setup the periodicity of password resets. And, notifications can be generated at each stage of the execution of the scheduled task. In addition, password reset history is also maintained within PAM360.

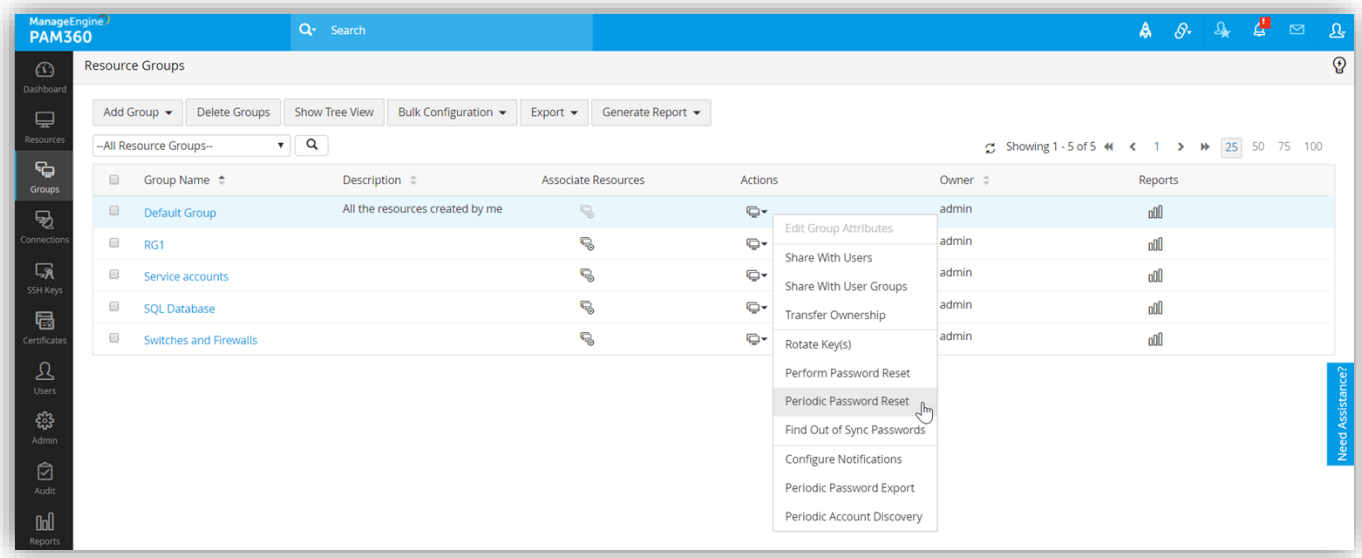
You can do the Periodic Password Reset by creating scheduled tasks for the resource groups.

Steps Required

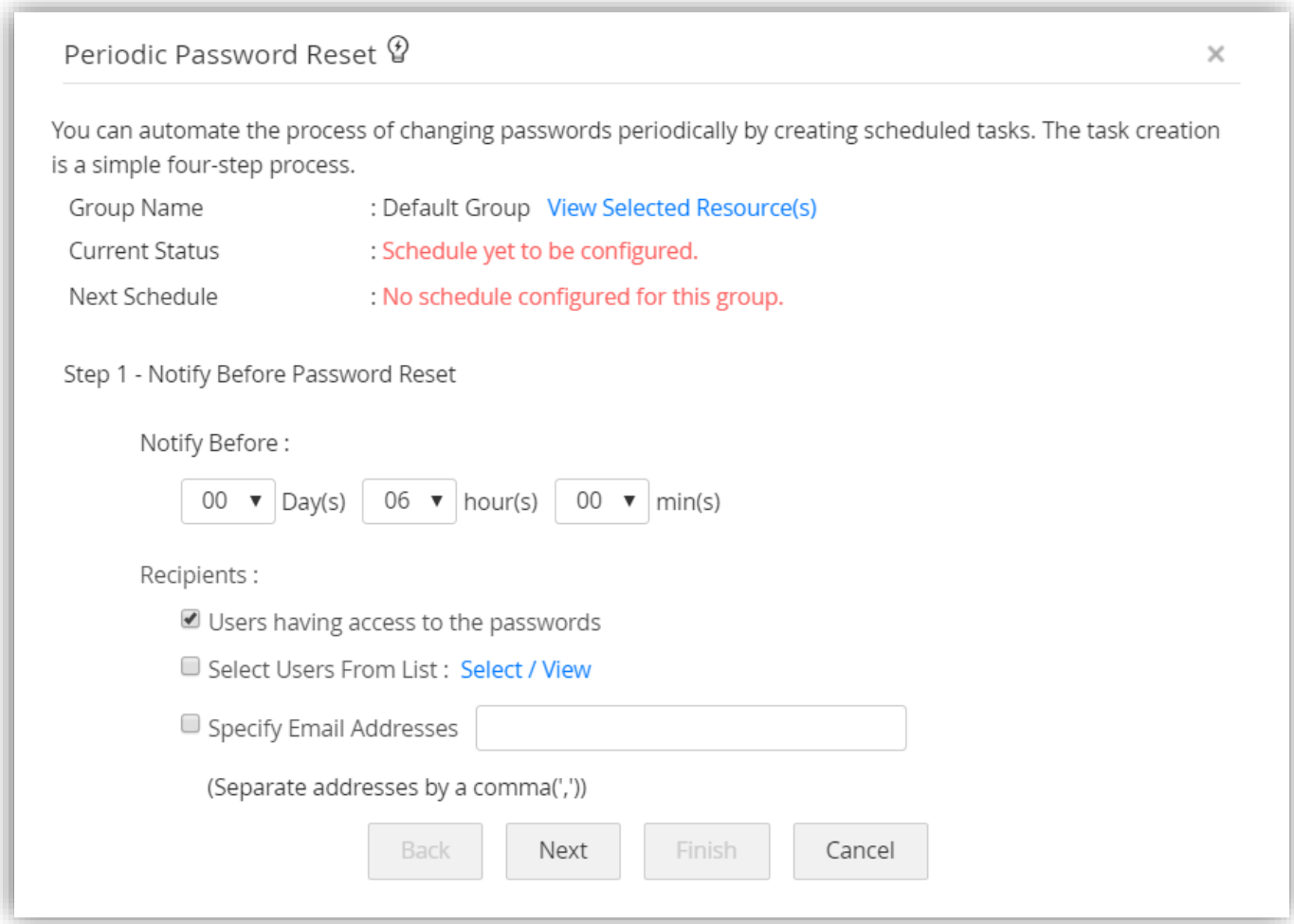
1. Initiating Password Reset
2. Scheduling Password Reset
   - 2.1 Notify Before Password Reset
   - 2.2 Password Allocation
   - 2.3 Reset Periodicity
   - 2.4 Reset Retry
   - 2.5 Notify After

1. Initiating Password Reset

1. Click the **Groups** tab from the left pane. Click **Actions >> Periodic Password Reset**.



2. The **Periodic Password Reset** window pops up which guides you through a four-step process for scheduling the password reset.



2. Scheduling Password Reset

2.1 Notify Before Password Reset

When passwords are scheduled to be reset at a specific time, notifications can be sent to the users beforehand to keep them informed on the reset operation.

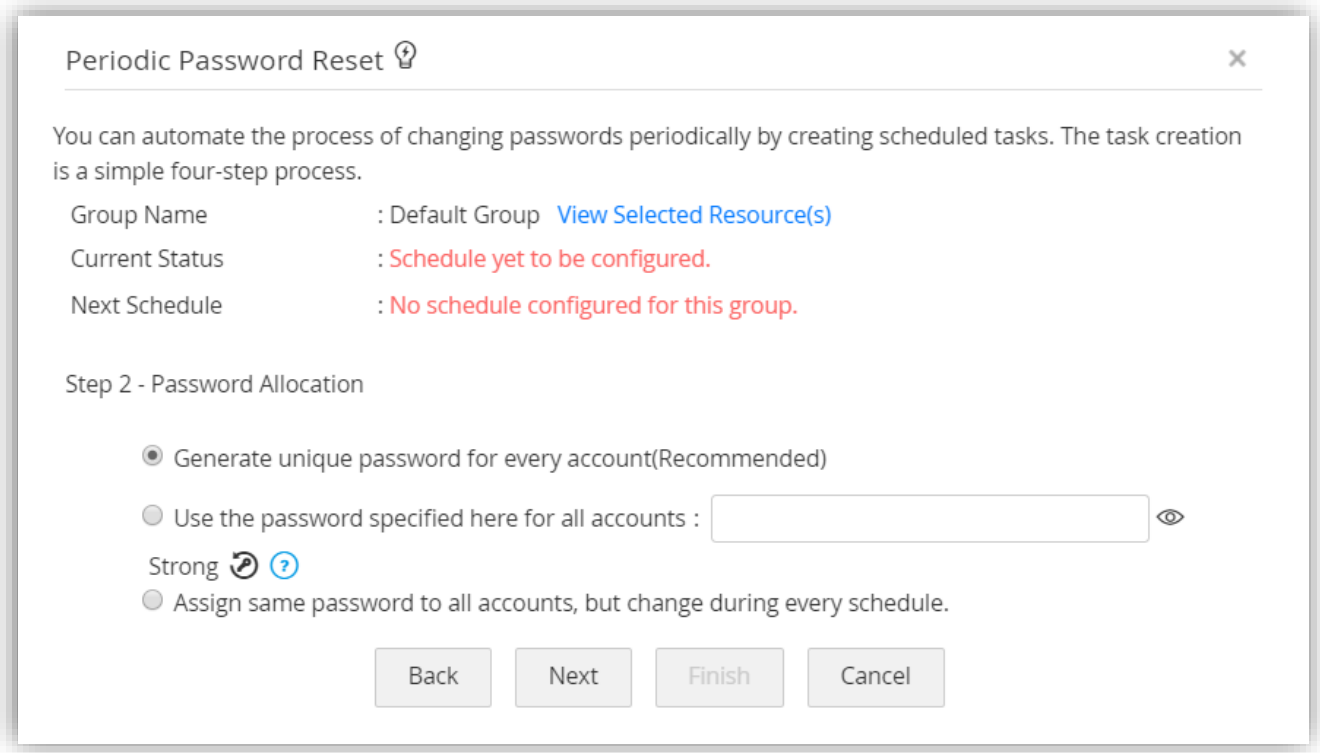
To send notifications,

1. Select the number of days and/or hours and/or minutes prior to which the notification is to be sent.
2. You can also specify the list of recipients to receive the notification.
    i. **Users who have access to specified passwords**: Users who possess any one of the share permissions (read only/read and write/manage) for the password, at the time when notification is generated.
    ii. **Select Users From List:** Any other specific user(s) to be selected from the list.
    iii. **Specify Email Addresses**: To generate notifications to specified list of email aliases or email addresses.
3. Click **Next**.

2.2 Password Allocation

Here there are three different ways in which you can allocate passwords for the group:

1. When specifying a new password, you can choose to allot a randomly generated unique password to the accounts. This random password will be based on the password policy set for the account.
2. You can specify a new password in the text field provided and allot the same to all the accounts in the particular group. This password will take after the password policy that is set for the resource group.
3. You can also assign the same password to all user accounts, on condition that the password is changed during every schedule. This password will take after the password policy that is set for the resource group.
4. Select the required choice and click **Next**.

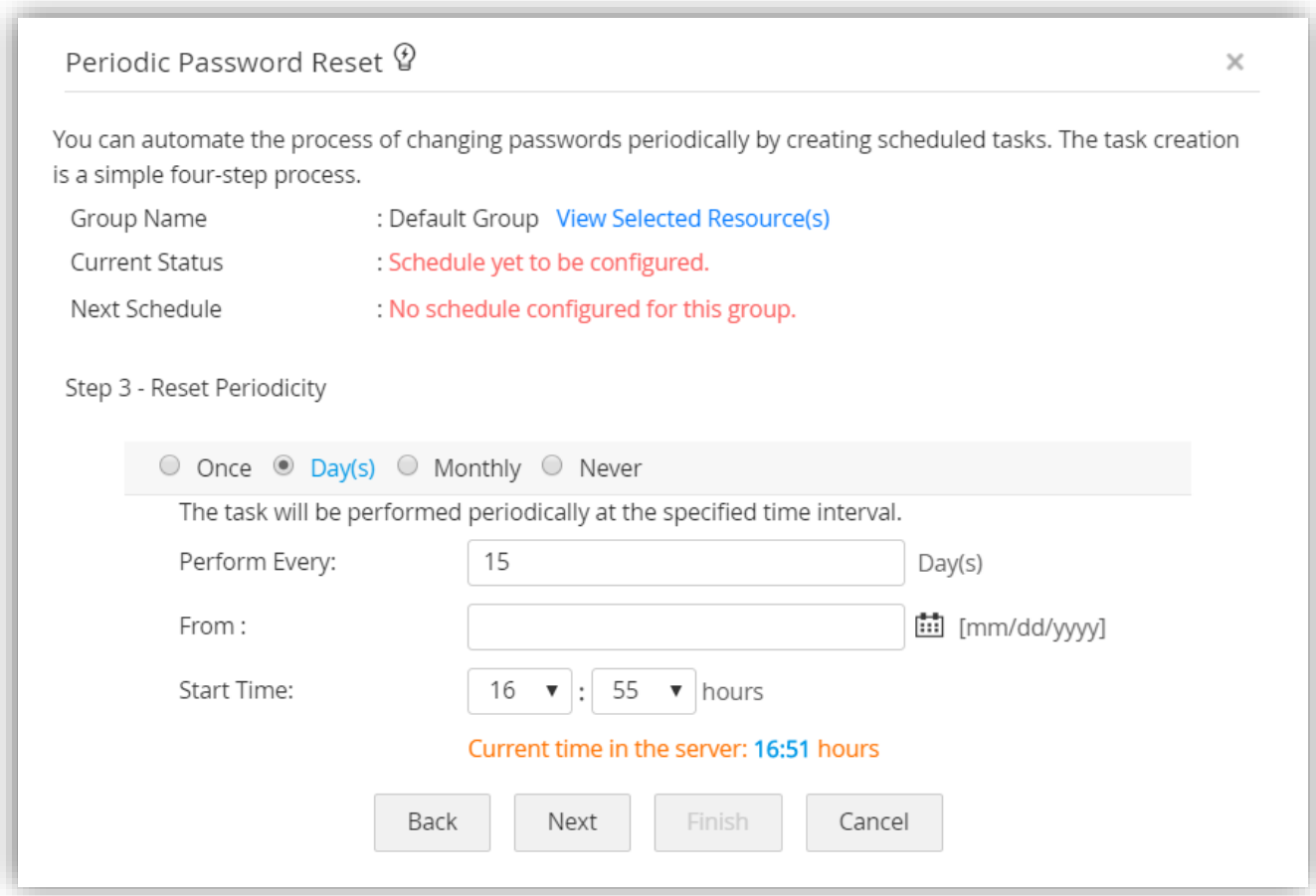


2.3 Reset Periodicity

This step specifies the actual creation of the schedule for password reset. The reset can be performed one-time or it could be set to recur at periodic intervals.

To specify the reset schedule:

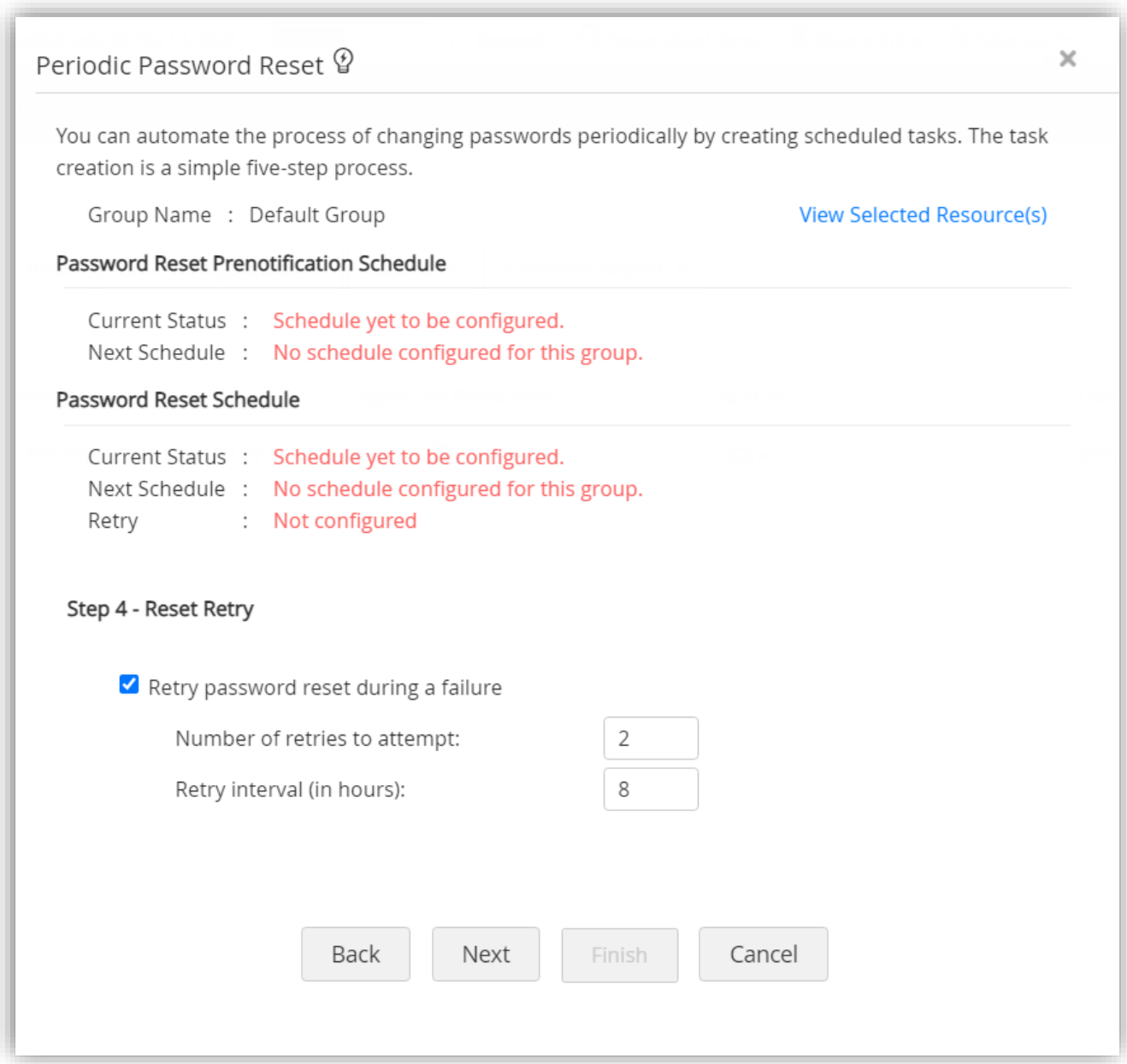
- Select from the options: **Once/Days/Monthly/Never** and specify the required details and click **Next.**



2.4 Reset Retry

Once you have finished creating the actual password reset schedule, you may proceed to configure the password reset retry settings, which is useful when a periodic password reset failure occurs. With this setting enabled, the password reset will be re-attempted after every failure at the specified retry intervals within the specified number of attempts.

1. Select the checkbox to **Retry password reset during a failure.**
2. Enter the **Number of retries to attempt** (upto 5) after a failed periodic password reset.
3. Mention the **Retry interval** (upto 24 hours) at which PAM360 should attempt the password reset again and click **Next.**



2.5 Notify After

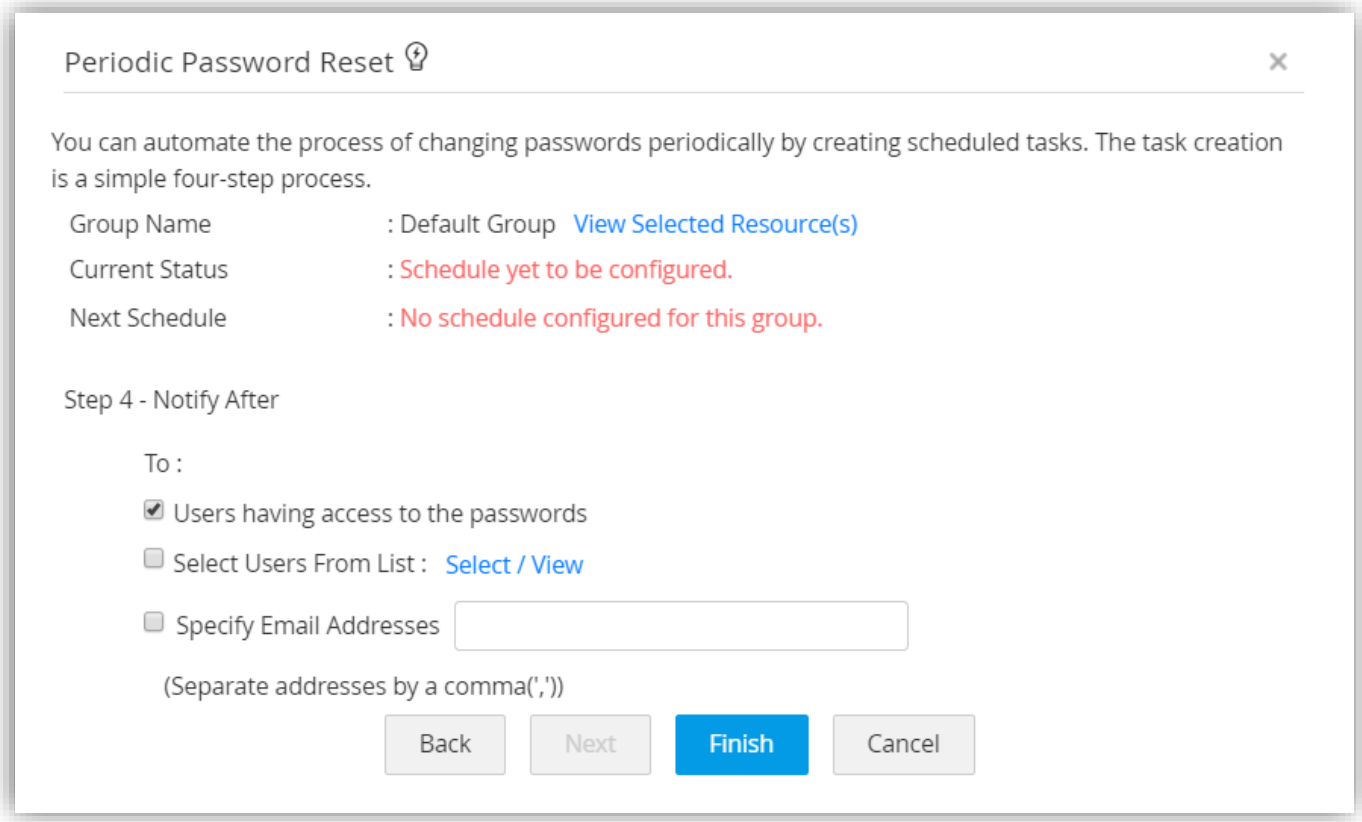
After the completion of password reset schedule, you can configure notifications to be sent regarding the password reset to all those who have access to the passwords.

To send notifications, specify the recipients for notifications:

- **Users having access to passwords:** Users who possess any one of the share permissions (read only/read and write/manage) for the password, at the time when notification is generated.
- **Select users from list**: Any other specific user(s) to be selected from the list of users.
- **Specify Email addresses**: to generate notifications to specified list of email aliases or email addresses.

Check the required boxes and click **Finish**. The required password reset schedule has been

created.


Periodic Password Reset
You can automate the process of changing passwords periodically by creating scheduled tasks. The task creation is a simple four-step process.
Group Name : Default Group View Selected Resource(s)
Current Status : Schedule yet to be configured.
Next Schedule : No schedule configured for this group.
Step 4 - Notify After
To :
Users having access to the passwords
Select Users From List : Select / View
Specify Email Addresses
(Separate addresses by a comma(','))
Back
Next
Finish
Cancel

Windows Service Account Password Reset

Windows Service Accounts, used by system programs to run application software services or processes, often possess higher or even excessive privileges than normal user accounts. These are indeed very powerful accounts that run critical business processes and services. Many third-party services or scheduled tasks or processes might make use of the same service account, resulting in a complex interconnection.

Typically, specific windows domain accounts are used as service accounts in services running in Windows servers, that need network access. PAM360 has the ability to identify the service accounts associated with a particular domain account. While resetting the password of a domain account managed in PAM360, it will find out the services which use that particular domain account as service account. It will automatically reset the service account password when the domain password is changed.

In certain cases, you will require to restart the services for the service account password reset to take effect. The windows service account password reset feature of PAM360 helps achieve this precisely, fully automated.

This section explains the following topics:

1. How does Windows Service Account Reset Work?
2. How to Setup Windows Service Account Password Reset?
3. Steps to Configure Windows Service Account Password Reset
4. Steps to View Service Account Status

1. How does Windows Service Account Reset Work?

For every Windows domain account for which the service account reset is enabled, PAM360 will find out the services which use that particular domain account as service account, and automatically reset the service account password if this domain password is changed.

2. How to Setup Windows Service Account Password Reset?

2.1 Prerequisites

1. Microsoft .Net framework 4.5.2 or above must be installed.
2. Microsoft Visual C++ 2015 redistributable must be installed.

Before enabling windows service account reset, ensure if the following services are enabled in the servers where the dependent services are running:

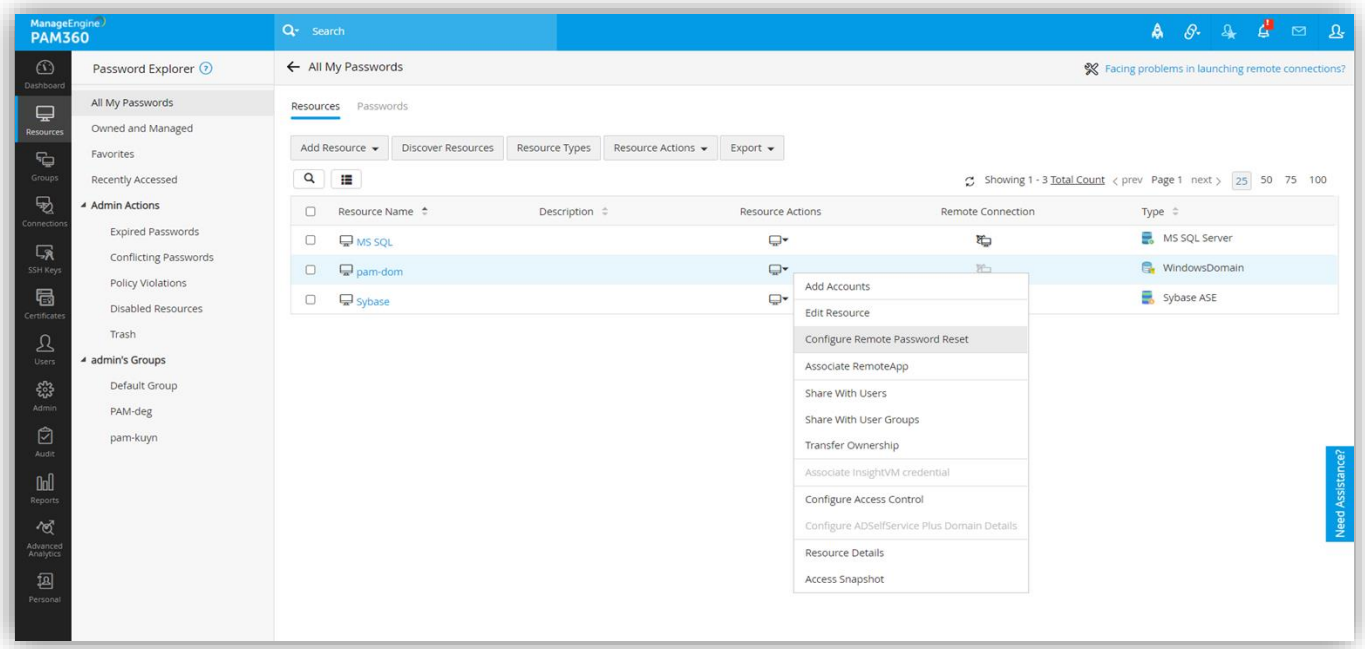
1. Windows RPC service should have been enabled.

2. Windows Management Instrumentation (WMI) service should have been enabled.
3. PAM360 service should be run with a domain admin account.

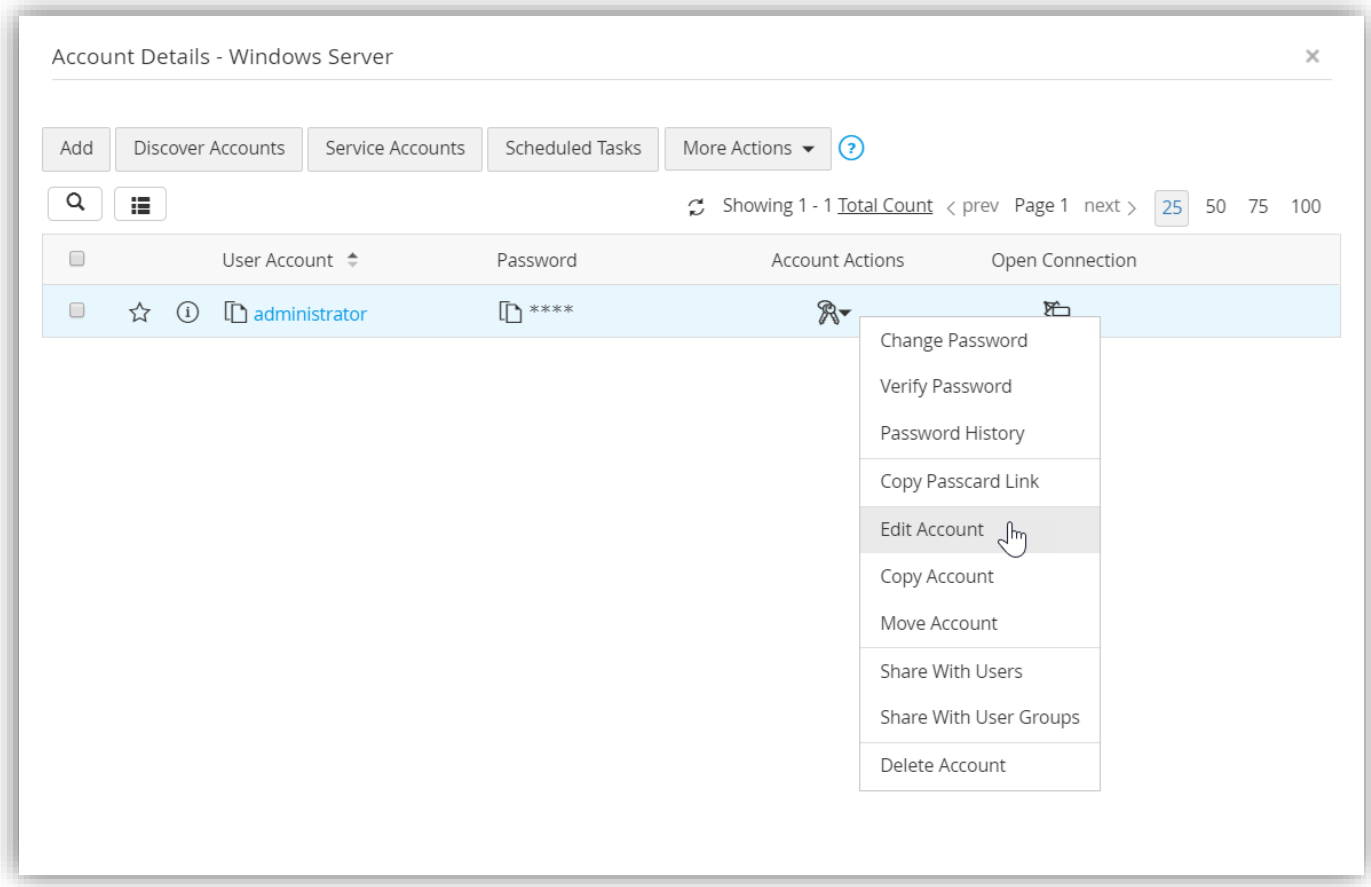
PAM360 will fetch the service accounts associated with the services in the domain members (from v8300 and above) during the privileged accounts discovery process.

3. Steps to Configure Windows Service Account Password Reset

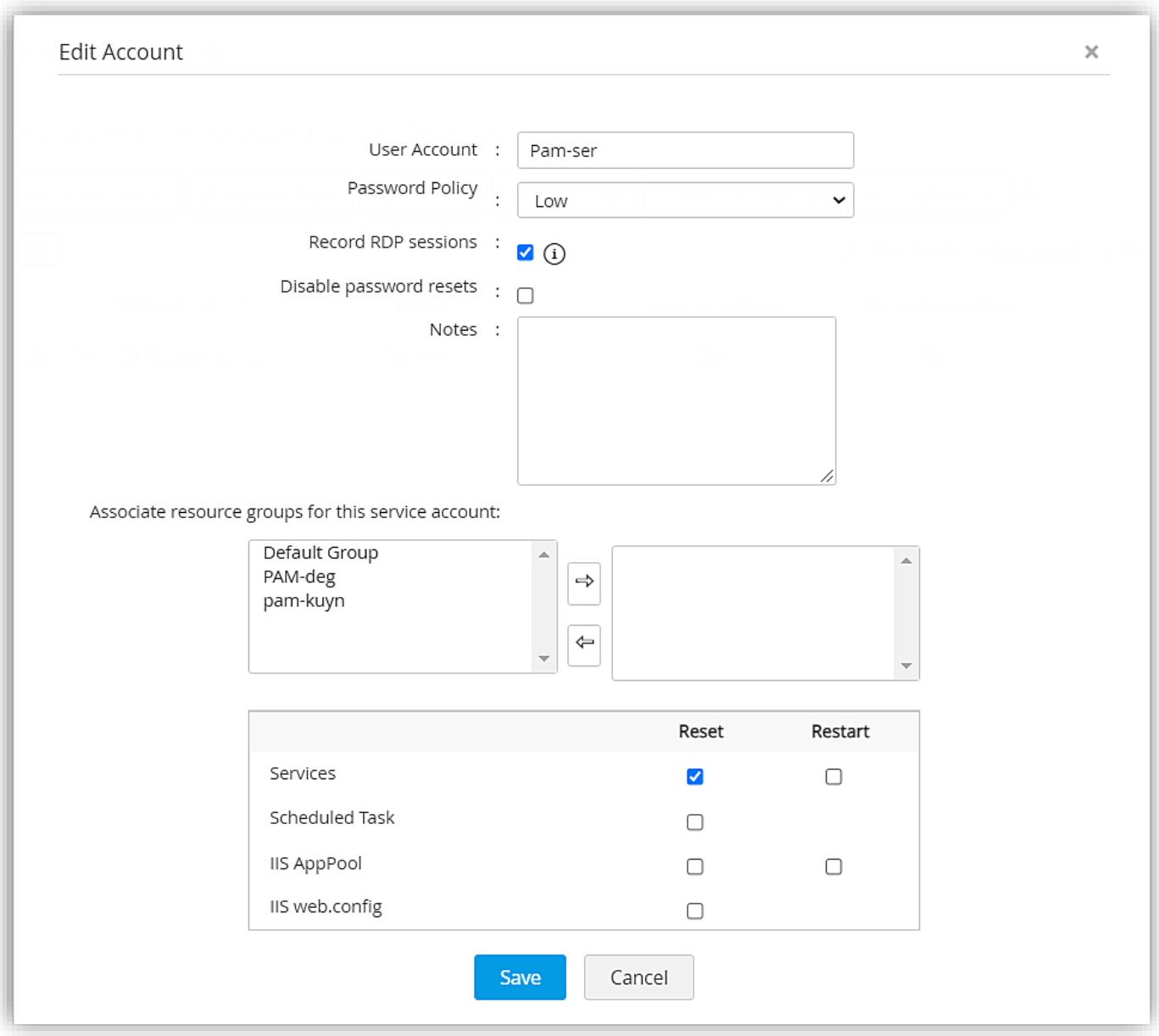
1. Navigate to the **Resources** tab and click the **Resource Actions** icon against WindowsDomain resource.
2. Select **Configure Remote Password Reset** from the drop down.



3. In the pop-up form that appears, select if you want to **Configure using an account of this resource** or **other resource.**
    i. If you choose to **Configure using an account of this resource**, select the **Administrator Account**.
    ii. If you choose to **Configure using an account of other resource**, select the **Resource Name** and **Administrator Account**.
4. Click **Save.**
5. Click on the WindowsDomain resource name. In the UI that opens, click the **Account Actions** icon against the service account and then select **Edit Account** from the drop down.



6. In the pop-up form that appears, associate resource groups for this service account by moving desired groups to the other box on the right side using the arrows.
7. Also, check **Restart** options if you would like PAM360 to restart the windows service account immediately after their passwords are updated.

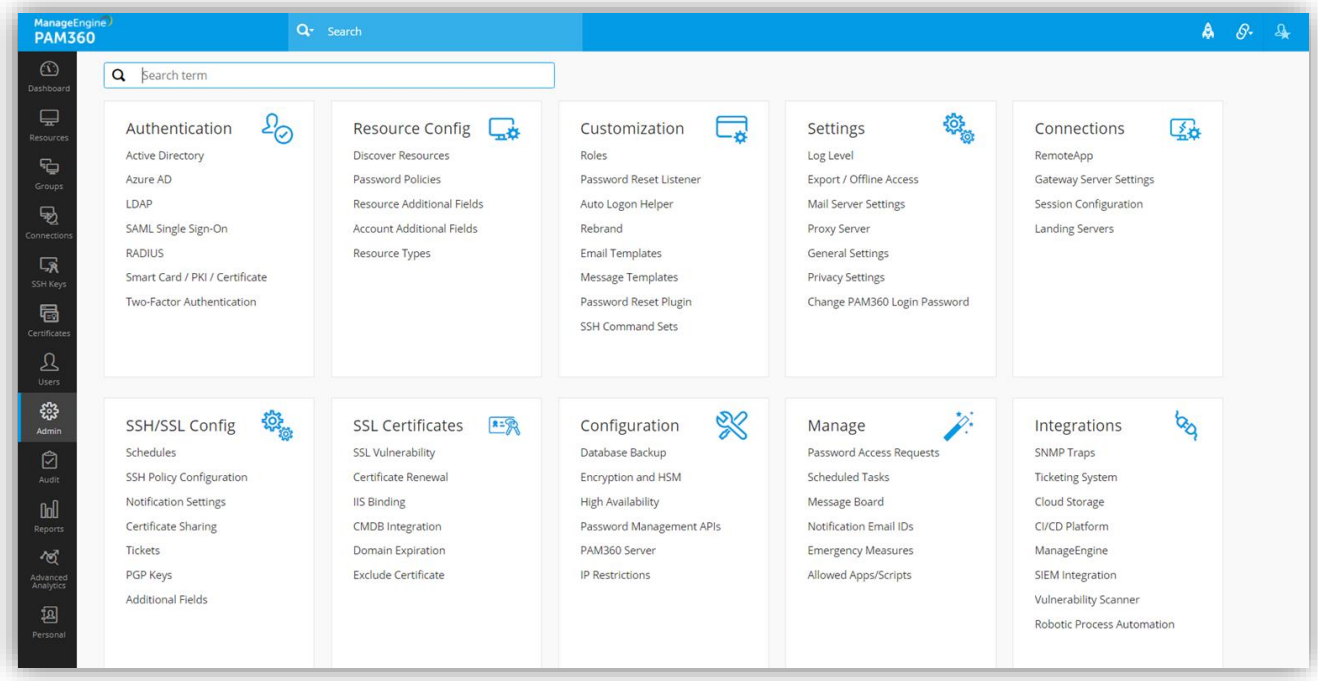


8. Check the checkbox for service account which you added in the **Windows Domain** resource and click **Save.**
9. Select an account and click **Service Accounts >> Supported Service Accounts.** Here, the Services which uses this service account as log on account will be listed. When you reset the password, it will be reset in the service running in the remote machine as well.

> **Note:** In certain cases, there would be requirements for stopping and starting the services during domain account reset. In such cases, through **General Settings** you can configure PAM360 to wait for a specified time period (in seconds) between stopping and starting the services.

To configure this,

1. Navigate to **Admin >> Settings >> General Settings.**



2. In the UI that opens, select **Password Reset** from the options on the left hand side.
3. Click the checkbox **Wait for a specified time period (in seconds) between stopping and starting the services**.
4. By default, PAM360 waits for 60 seconds. You may configure it in accordance with your needs.
5. Click **Save**.

4. Steps to View Service Account Status

For any windows domain account (for which you have enabled Windows service account reset), you can view the list of associated service accounts, scheduled tasks and information on whether the service accounts and scheduled tasks were reset upon the corresponding domain account reset.

To view this information,

1. Go to **Resources** tab and click the name of the resource.
2. In the UI that opens, select the domain account of the resource for which you wish to know the status of service account reset and click **Service Account** button at the top of the list of accounts.
3. In the dialog box that opens, switch to **Service Account Status** tab.

Note:

1. Whenever the password of the domain account is changed, the windows service account associated with it will also be changed. In case, you have created schedules for rotating domain accounts (Periodic Password Reset), the service account reset will also follow the schedule.
2. Once you create Windows Service Account Reset, the passwords of the Windows scheduled tasks associated with the service accounts will also be reset.

IIS AppPool Account Password Reset

Normally, Windows domain accounts are used as identities to run IIS app pools. Whenever the password of a domain account is changed in the domain controller, the new password has to be updated individually in all associated app pools for web applications to run without any hindrances. With each domain account used to run numerous app pools, manually effecting all password changes is a tedious job for an IT admin.

PAM360 has the ability to identify the IIS app pools that are run using a specific Windows domain account stored in PAM360. While resetting the password of the domain accounts stored in PAM360, it will find out the app pools which are run using that particular domain account and will automatically update the change in the app pool identities too after the domain account password is reset.

To add app pool accounts to PAM360 and to achieve automated password resets, carry out the following steps in the GUI:

Summary of Steps

1. Add Domain Controller as a Resource
2. Add Domain Member Servers as New Resources and Create Resource Group
3. Add Domain Account Used to Run IIS AppPool
4. Configure Remote Password Reset for IIS AppPool Account
5. Associate Resource Groups for the IIS AppPool Account
6. Verify Supported IIS AppPool Accounts
7. Change Password

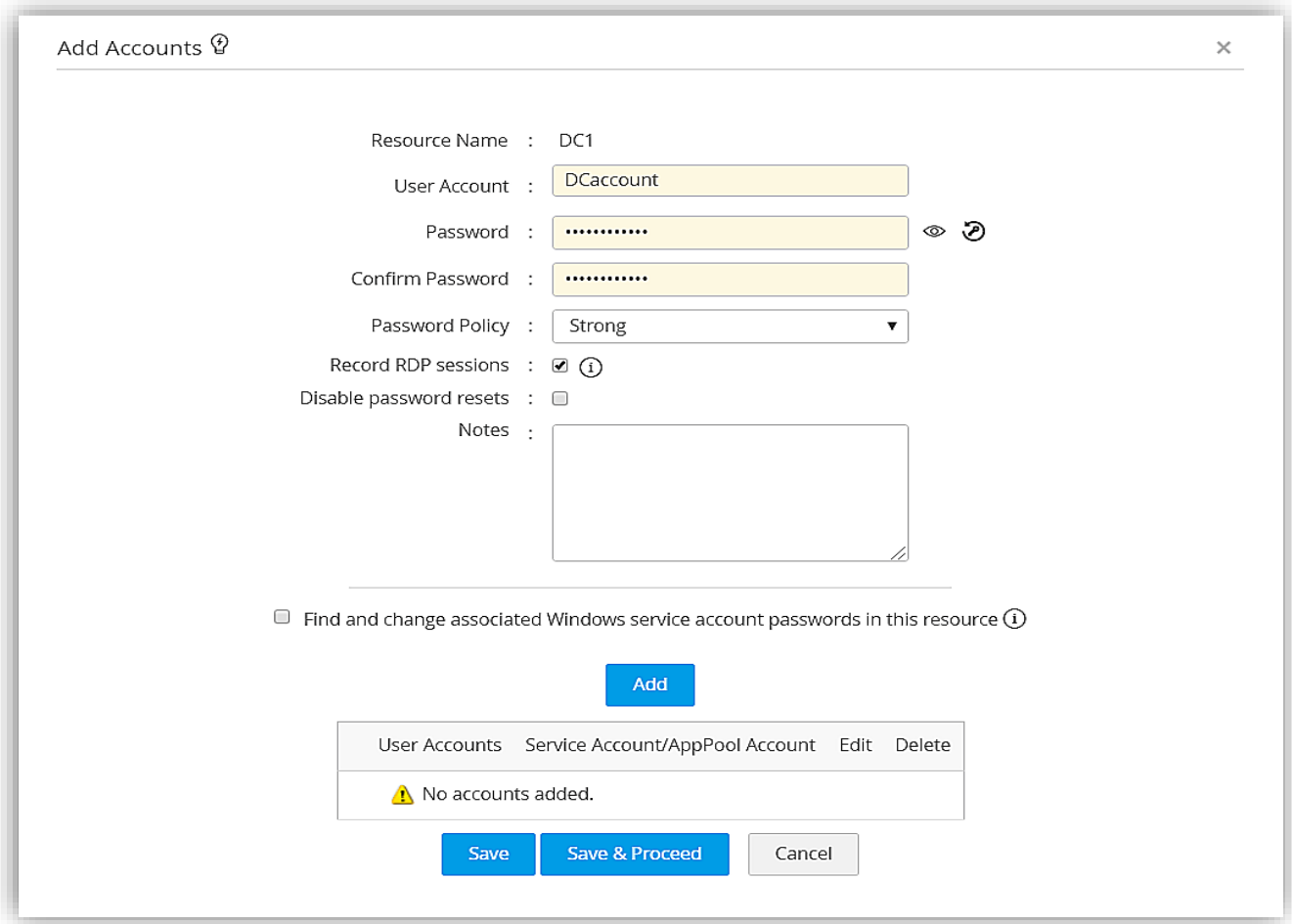
Note: Use-case illustration

For a quicker understanding of the procedure, the following references have been used in the steps:

- Domain Controller is DC1.
- Windows Domain Name is PAM360DC.
- Domain Administrator account is DA1.
- App pool accounts are A1 and A2.
- Domain member servers that make use of the app pool account A1 are Win1, Win2, Win3, and Win4.
- Resource Groups is RG1, consisting of Win1, Win2, Win3, and Win4.

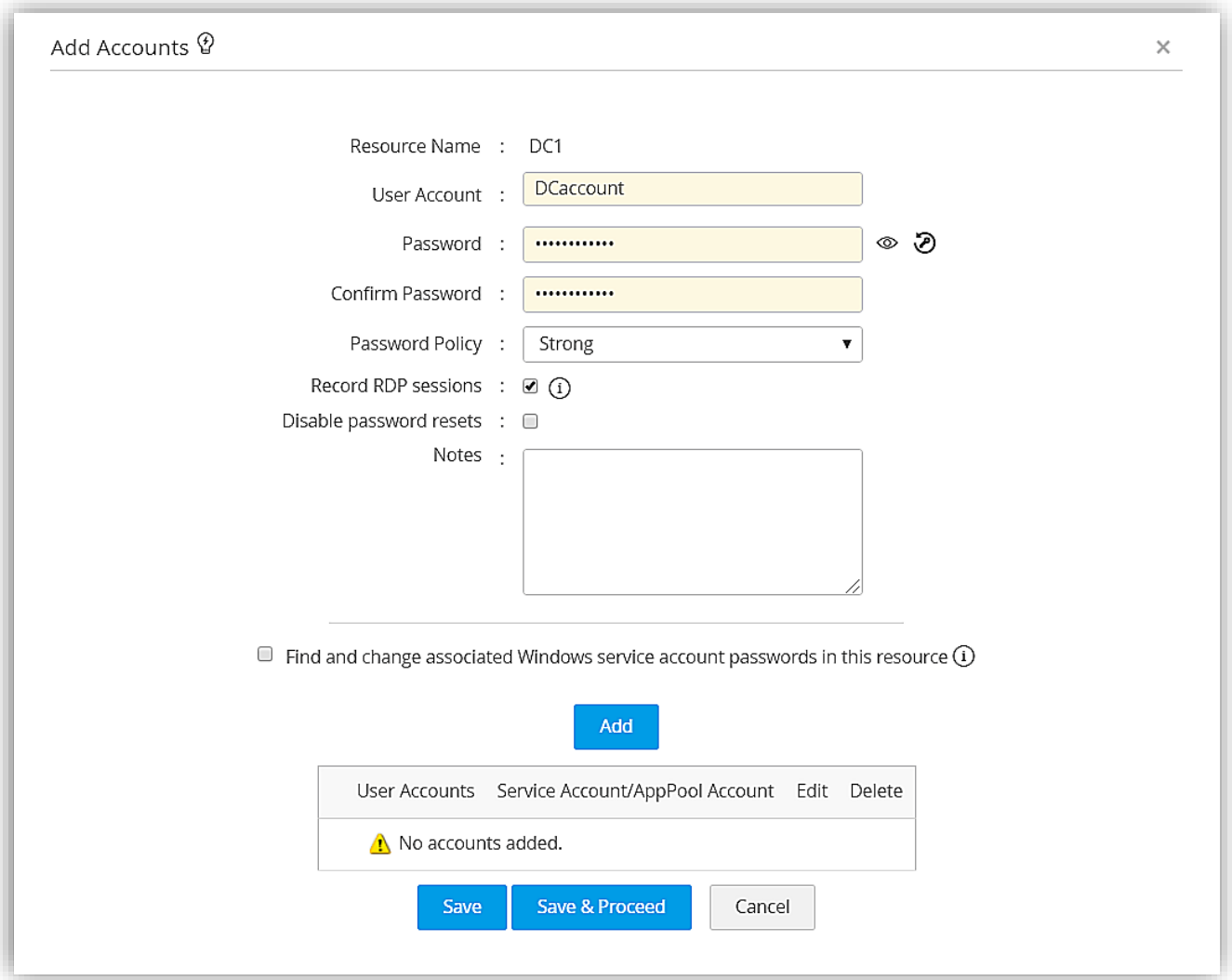
1. Add Domain Controller as a Resource

1. Navigate to **Resources** tab.
2. Click on **Add Resource** button, and select **Add Manually** from the dropdown.
3. In the pop-up form that opens, add the Domain Controller - DC1, as a new resource with **Resource Type** as Windows Domain.
4. Supply the NETBIOS name - PAM360DC, in upper case in the **Domain Name** field.
5. Fill in the other details such as DNS.
6. Click **Save & Proceed.**



2. Add Domain Admin Account and IIS AppPool Accounts.

1. Navigate to **Resources** tab.
2. Click the **Resource Actions** icon against the newly added resource and select **Add Accounts** from the drop down list.



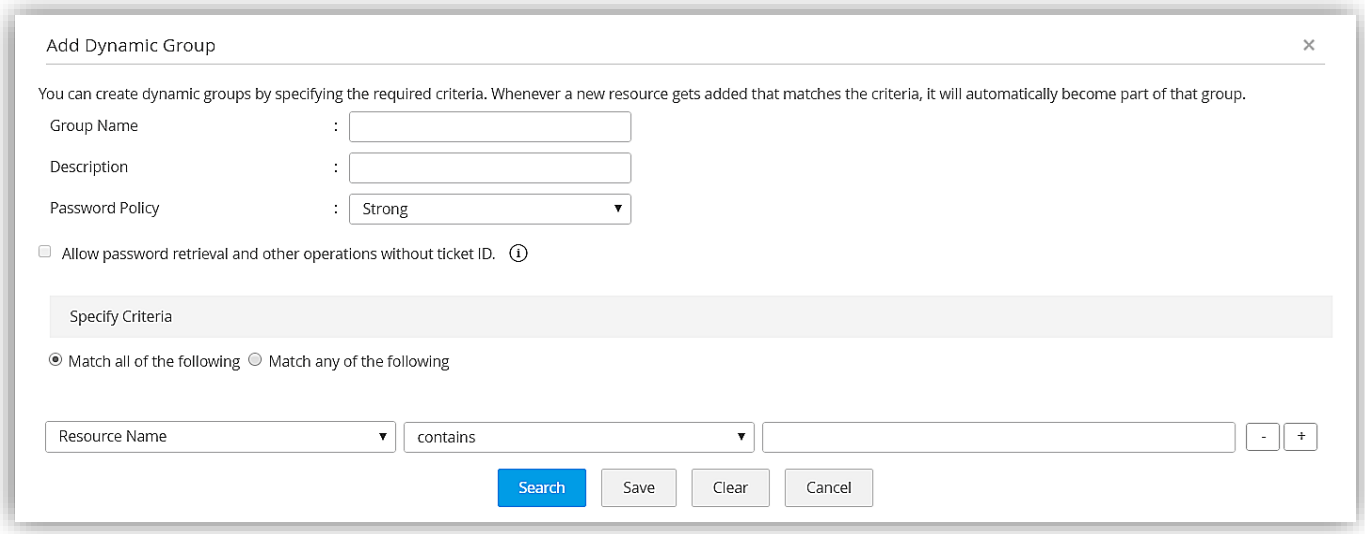
3. In the pop-up form that opens, add the domain administrator account **DA1** and click **Add**.
4. Then, continue to add the app pool accounts **A1, A2** in the same way. When you are done, click **Save**.

3. Add Domain Member Servers as New Resources and Create Resource Group

Continue adding the other member servers of the domain - Win1, Win2, Win3, and Win4 as new resources in the same way as explained above.

1. Navigate to **Resources** tab.
2. Click **Add Resources** button and add the member servers along with their respective local accounts.
3. Now, go to **Groups** tab and click on **Add group** button and select **Dynamic Group** from the drop down.
4. In the pop-up form that opens, name the group as **RG1** and choose **Match any of the following**. Select Win1, Win2, Win3 and Win4.

5. Click **Save**.



Alternate step: Automated discovery of resources and associated accounts

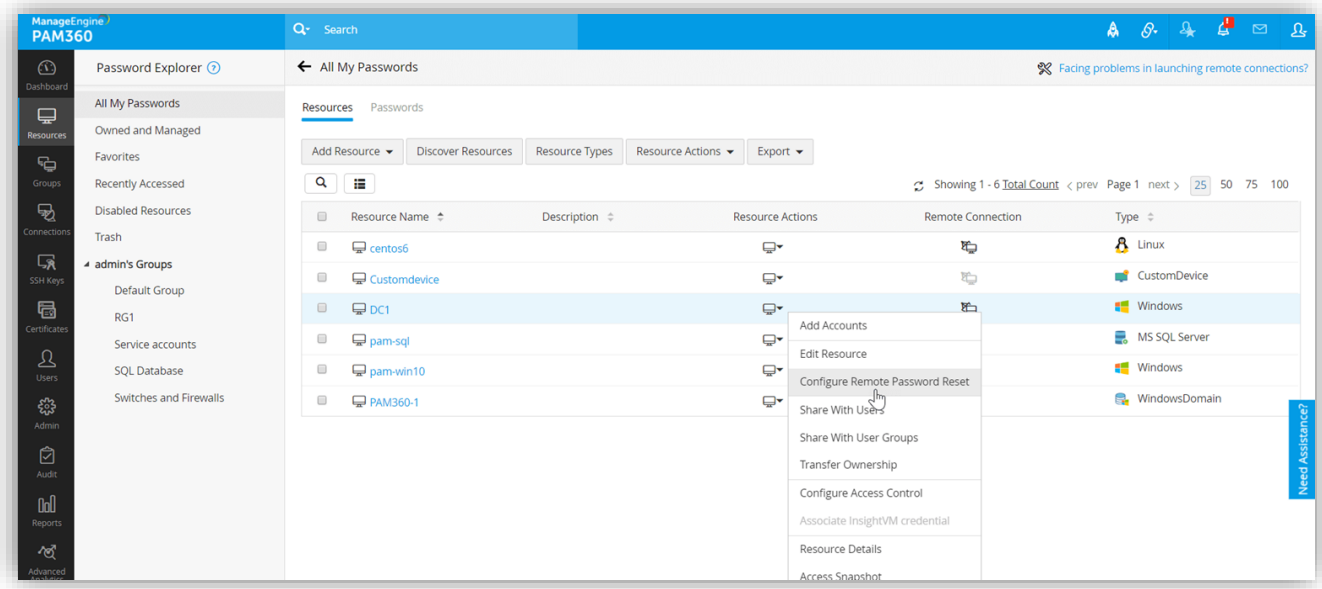
Instead of manual addition explained in Step 3, you can also discover the required resources and groups in your domain by following the steps given below:

1. Navigate to **Resources** tab.
2. Select **Discover Resources** given at the top of the resources list.
3. Supply your domain details (PAM360DC) in the **Windows** screen and click **Fetch Groups and OUs**.
4. From the enumerated list, select the Groups or OUs that you would like to import.
5. Click **Import**. This will fetch your Groups/OUs and list them under **Groups**, in this case.
6. The member servers in the imported Groups/OUs will also be listed individually under **Resources** along with their respective local accounts.

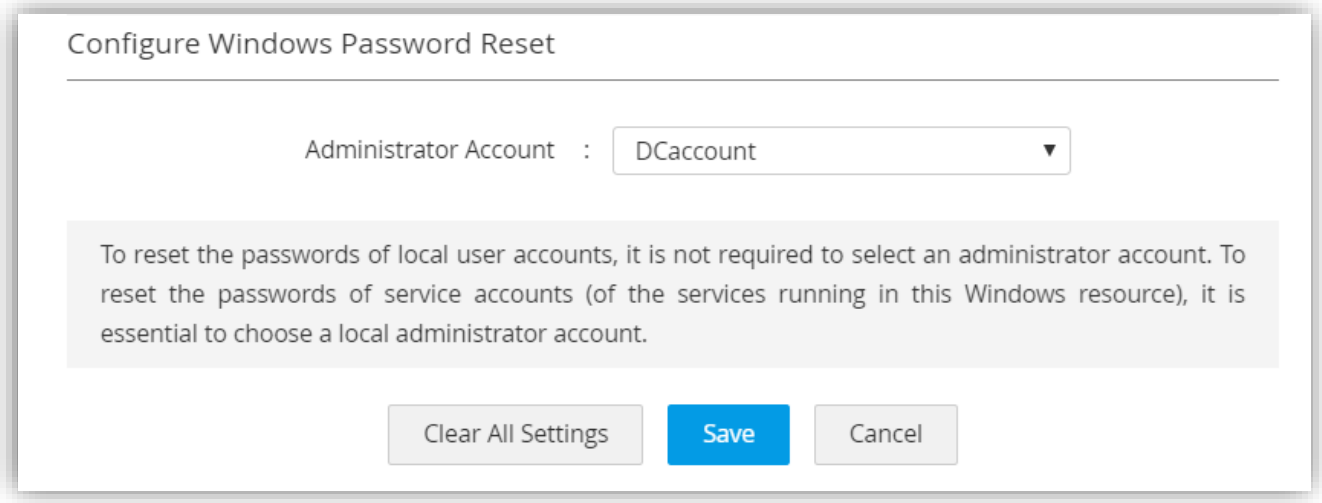
4. Configure Remote Password Reset for IIS AppPool Account.

Instead of manual addition explained in Step 3, you can also discover the required resources and groups in your domain by following the steps given below:

1. Navigate to **Resources** tab.
2. Click the **Resource Actions** icon against the WindowsDomain **DC1** resource and select **Configure password reset** from the drop down.

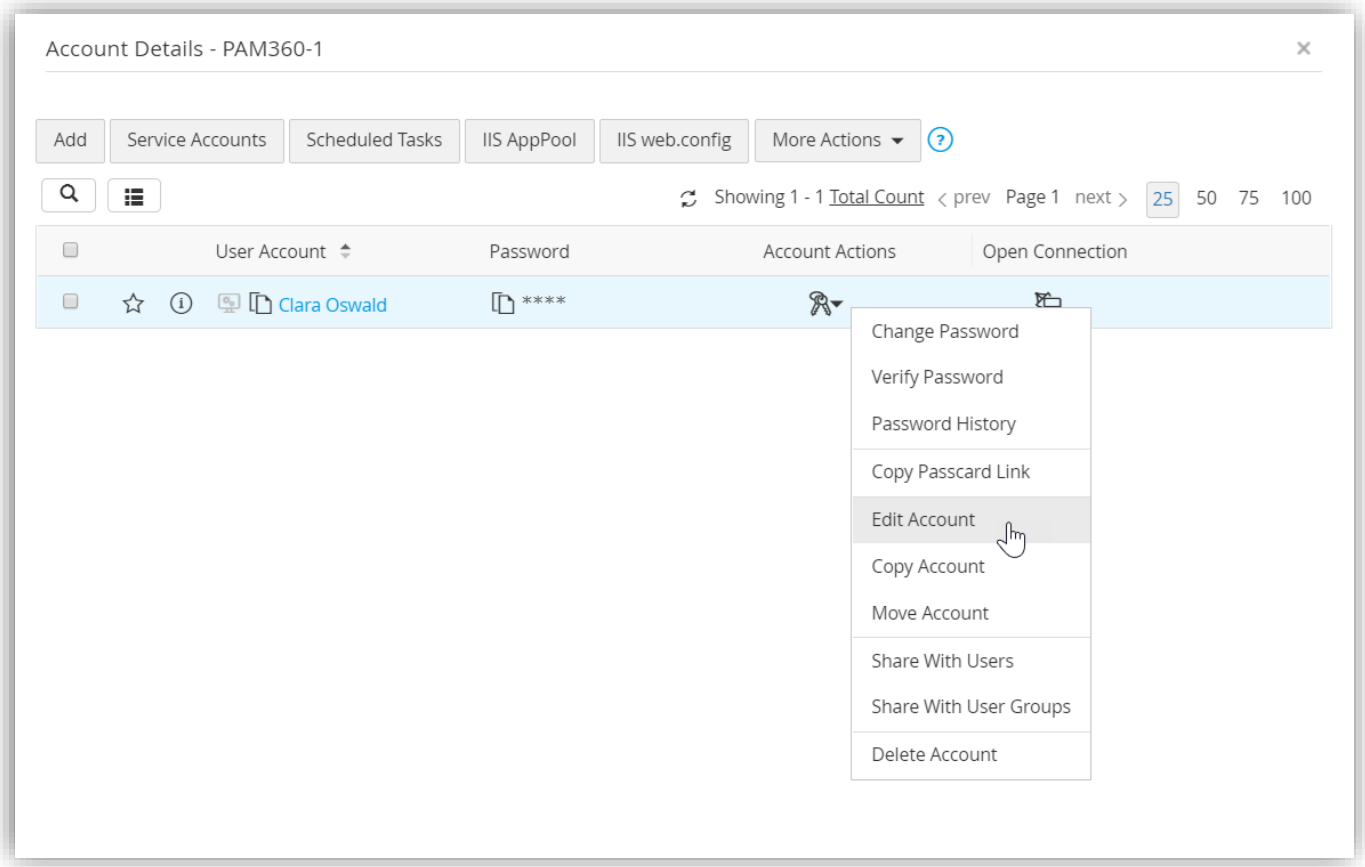


3. In the pop-up form that appears, select the 'Domain Admin' (DC1) account as the **Administrator Account**.
4. Click **Save**.

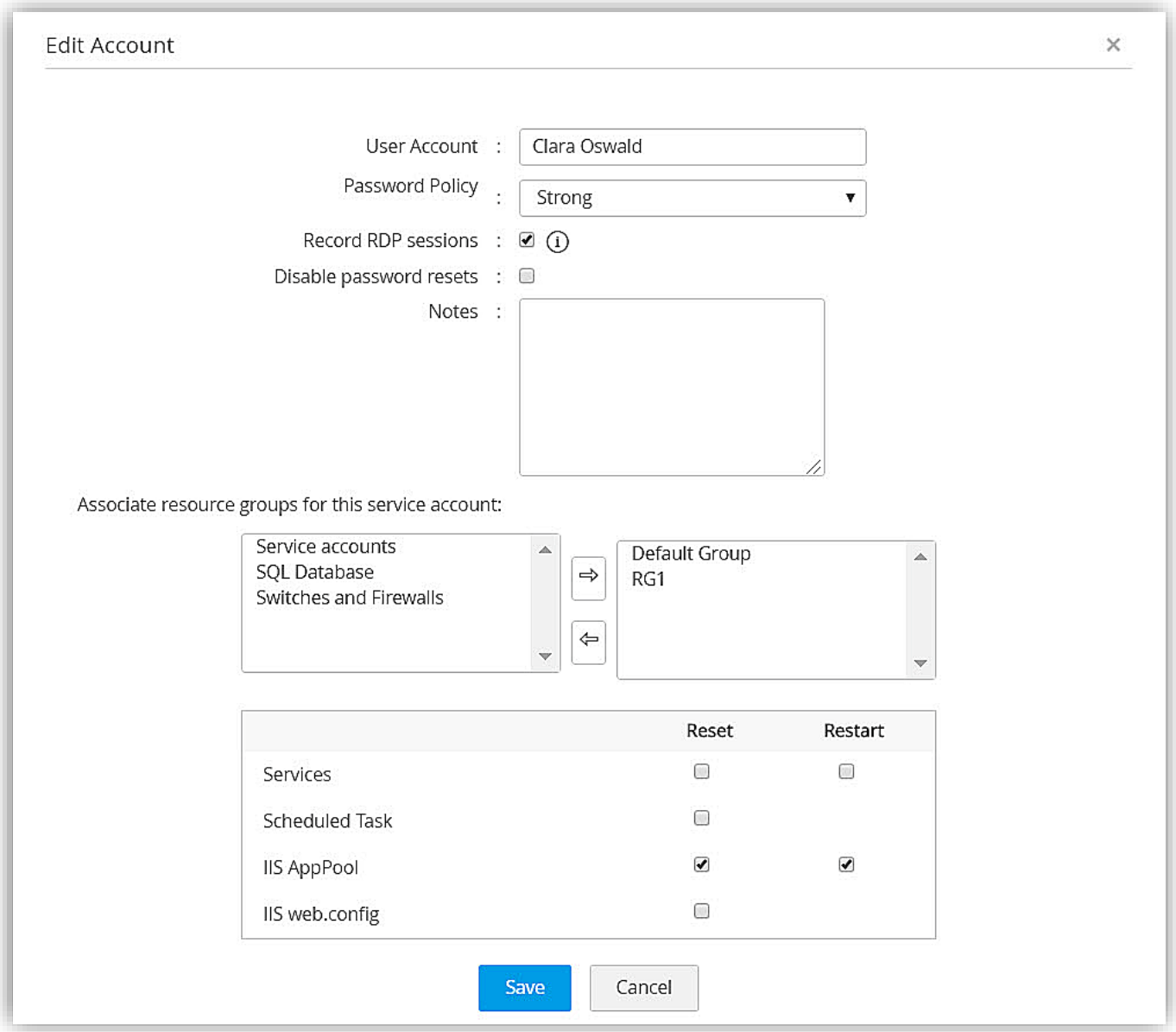


5. Associate Resource Groups for the IIS AppPool Account

1. Click on the WindowsDomain **DC1** resource name.



2. In the UI that opens, click the **Account Actions** icon against the app pool account (**M1** in this case) and then select **Edit account** from the drop down.



3. In the pop-up form that appears, associate resource groups for this service account by moving it to the other box.
4. Check **Restart IIS AppPools** if you would like PAM360 to restart the app pools immediately after their passwords are updated.
5. Click **Save**.

6. Verify Supported IIS AppPool Accounts

1. Click the WindowsDomain **DC1** resource name.
2. Select the appPool account **M1** and click the **IIS AppPool** button.
3. In the pop-up form that appears, click **Fetch Now** under **Supported IIS App Pool Accounts**.
4. PAM360 will scan and list all the app pools that are run in the servers with the respective app pool account. After reviewing the list, hit **Ok**.

Note: This step is just for verification purpose to check where the app pool account is being used. It is not mandatory.

7. Change Password

1. Click on the WindowsDomain **DC1** resource name.
2. Click the **Account Actions** icon against the app pool account **M1** and then select **Change Password** from the drop down.
3. In the pop-up form that appears, either provide or generate a new password. Make sure to enable **Apply password changes to the remote resource**.
4. Click **Save**. PAM360 will immediately reset the password in the domain first and then, automatically update the new password across all servers where M1 is used to run app pools.

Additional steps to schedule periodic password resets for IIS App Pool accounts

The aforementioned steps are adequate to carry out password resets for app pool accounts anytime on demand. If you would like to configure automatic password resets on a periodic basis, execute the additional steps given below:

To configure scheduled password reset for app pool accounts,

1. A resource group has to be first created consisting of all desired app pool accounts.
2. Click the **Actions** icon against the resource group and select **Scheduled password reset** from the drop down.
3. A pop-up form will open with a four step process through which required schedule can be created. The steps are explained below:

Step 1: Pre-notification

When passwords are scheduled to be reset at a specific time, notifications can be sent to the users beforehand giving them a heads up on the reset action.

To send notifications,

1. Select the number of days and/or hours and/or minutes prior to which notification is to be sent.
2. You can also specify the list of recipients for notification.
3. **Users having access to passwords** - users who possess any one of the share permissions (read only / read and write / manage) for the password, at the time when notification is generated.
4. **Other Users/User groups** - any other specific user(s) to be selected from the list.

5. **E-mail Ids** - to generate notifications to specified list of email aliases or email addresses.
6. Click **Next**.

Step 2: Specify the new password

1. You have the option to specify the new password(s) to be used for resources during the execution of the scheduled task.
2. To specify a new password to be used, you have the option to either allot randomly generated unique passwords to the accounts based on the password policy set for the group or you can allot a new password to all the resources in accordance with the password policy already specified for the group.
3. You can also assign same password to all user accounts provided the password is changed during every schedule.
4. Select the desired choice and click **Next**.

Step 3: Specify the reset schedule

Actual creation of the schedule for password reset is specified in this step. The reset can be performed one-time or it could be recurring at periodic intervals.

To specify the reset schedule:

1. Select from the options - **Once / Days / Monthly / Never** and specify the other details required.
2. Click **Next**.

Step 4: Post-reset notification

After the completion of password reset schedule, notifications regarding the completion of reset can be sent to all those who have access to the passwords.

To send notifications,

1. Specify the recipients for notifications.
2. **Users having access to passwords** - users who possess any one of the share permissions (read only / read and write / manage) for the password, at the time when notification is generated.
3. **Other Users/User groups** - any other specific user(s) to be selected from the list.
4. **E-mail Ids** - to generate notifications to specified list of email aliases or email addresses.
5. Click **Finish**.
6. The required password reset schedule has been created. The setting could be saved as a template for use with configuring password reset schedule for another resource groups.

Upon completion of these steps, PAM360 will continue to automatically reset the app pool

account passwords on a periodic basis.

Windows Scheduled Tasks Password Reset

PAM360 can be scheduled to reset passwords on windows for improved security.

The following topics on password reset are explained in this document:

1. Prerequisites
2. Workflow
   2.1 Add Domain Controller as a Resource with Resource Type WindowsDomain
   2.2 Add Domain Admin Account and Scheduled Tasks
   2.3 Add Domain Member Servers as New Resources and Create Resource Group
   2.4 Configure Windows Scheduled Tasks Remote Password Reset
   2.5 Associate Resource Groups for the Scheduled Tasks and Verify Supported Scheduled Tasks
3. Viewing Scheduled Tasks Status

1. Prerequisites

The following are mandatory:

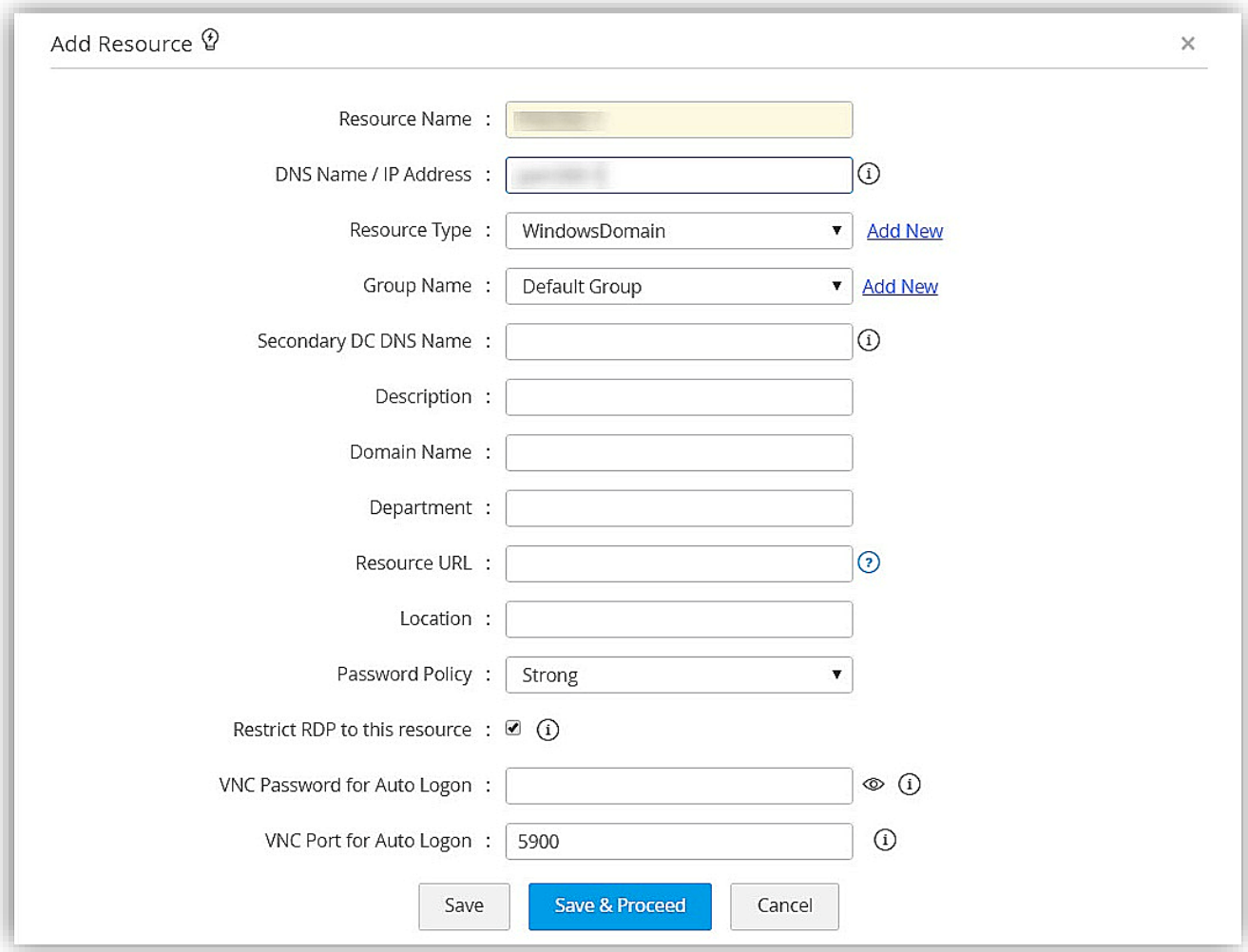
- Microsoft .Net framework 4.5.2 or above must be installed.
- Microsof0t Visual C++ 2015 redistributable must be installed.

> **Note:**
>
> - Windows scheduled task reset is supported only for V2.
> - When PAM360 is installed and run in one operating system (for eg: Windows server 2016), then the scheduled task password cannot be reset for the scheduled tasks running in lower OS versions (for eg: Windows server 2008 and below).

2. Workflow

2.1 Add Domain Controller as a Resource with Resource Type WindowsDomain

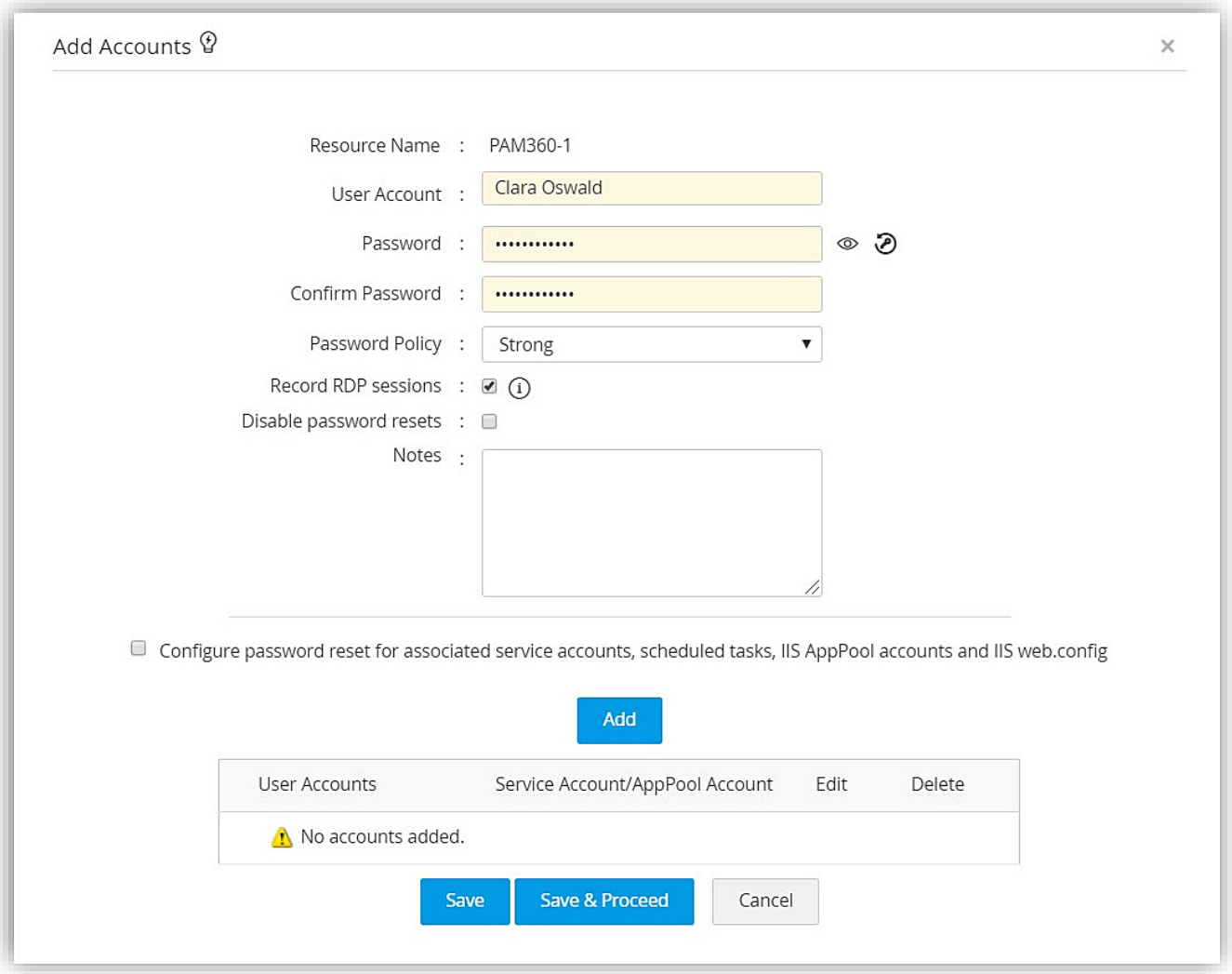
1. Navigate to **Resources >> Add Resource >> Add Manually.**



2. In the pop-up form that opens, add the Domain Controller - PAM360 Machine as a new resource with **Resource Type** as Windows Domain.
3. Fill in the other details such as DNS name and Domain name.
4. Click **Save & Proceed**.

2.2 Add Domain Admin Account and Scheduled Tasks

1. Navigate to **Resources >> Resource Actions >> Add Accounts**.

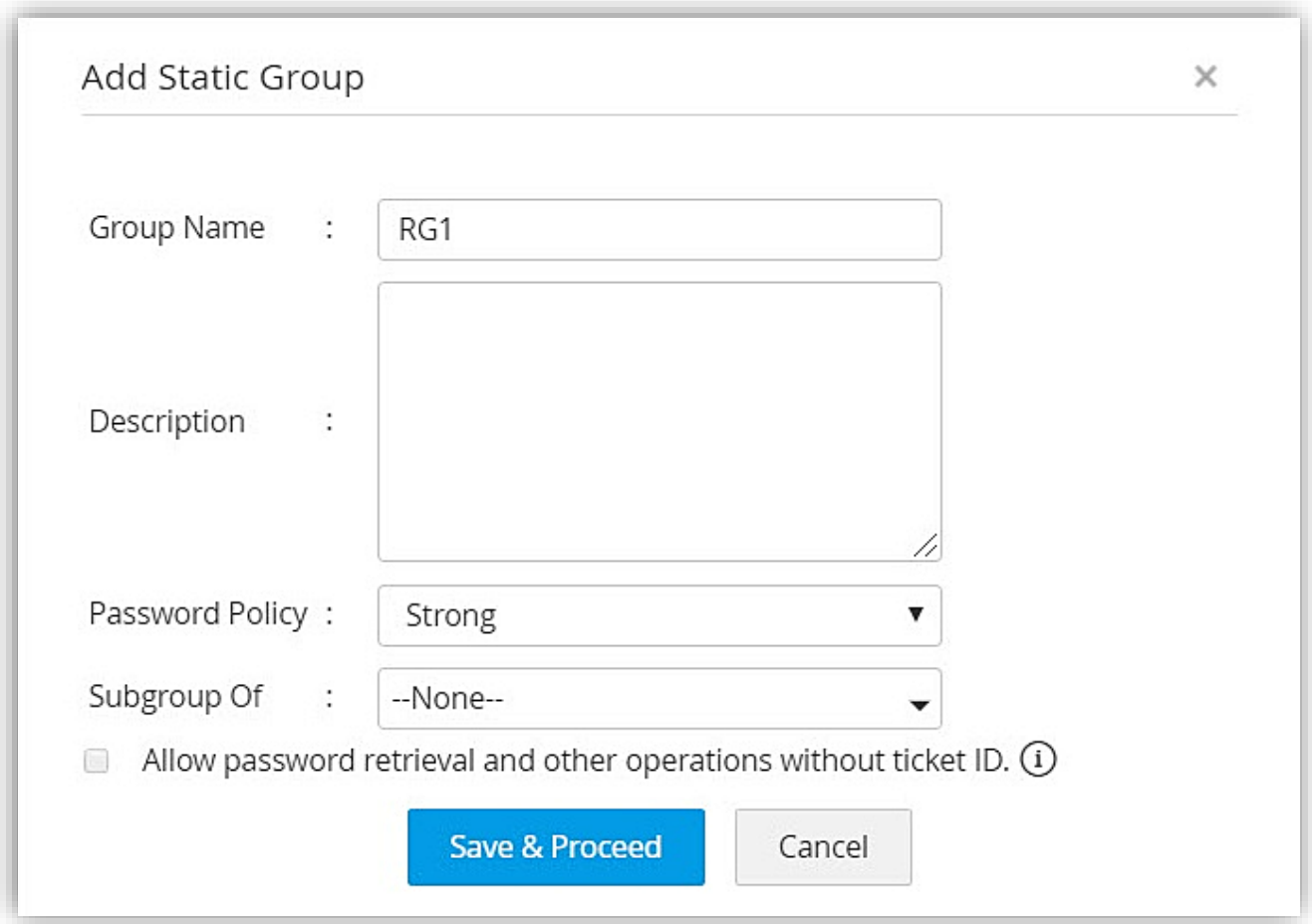


2. In the pop-up form that opens, add the domain administrator account and click **Add**.
3. Then, continue to add the user accounts in the same way. When you are done, click **Save**.

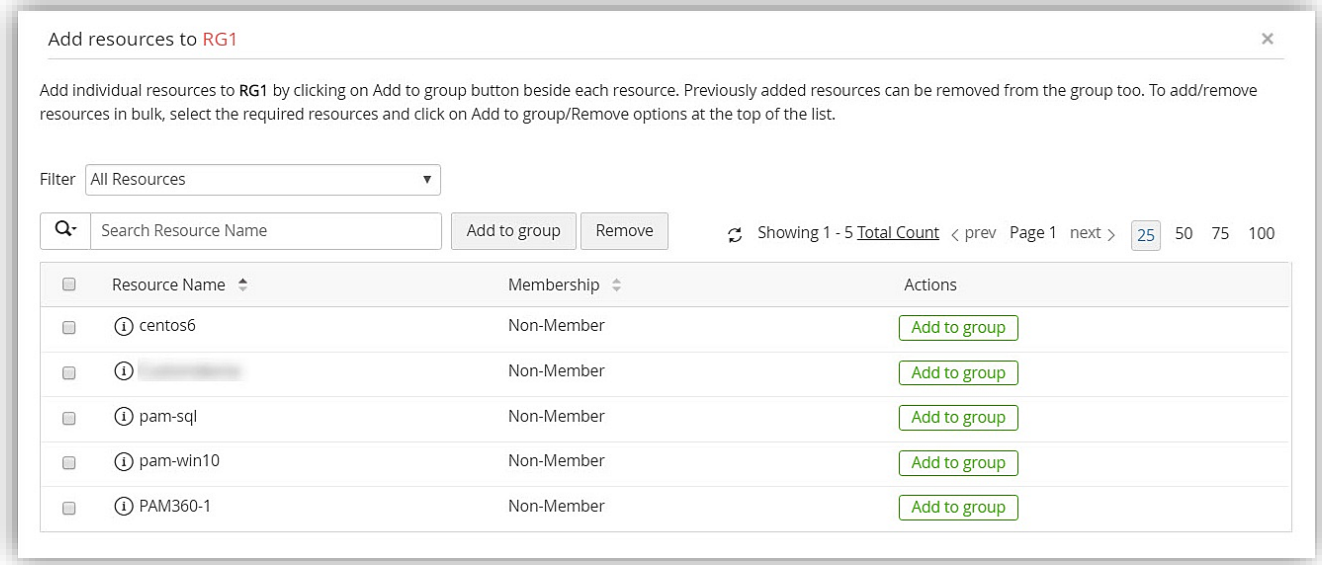
2.3 Add Domain Member Servers as New Resources and Create Resource Group

Continue adding the other member servers of the domain - Win1, Win2, Win3, and Win4 as new resources in the same way as explained above.

1. Navigate to **Resources** >> **Add Resources** and add the member servers.
2. Now, go to **Groups** >> **Add group** and select **Static Group** from the drop down.
3. In the pop-up form that opens, name the group as **RG1**, provide description and select a password policy for the group. Click **Save and proceed**.



4. Now, locate desired resources and click **Add to group** against them.



5. Click **Save**.

Alternate step: Automated discovery of resources and associated accounts:

Instead of manual addition explained in Step 3, you can also discover the required resources

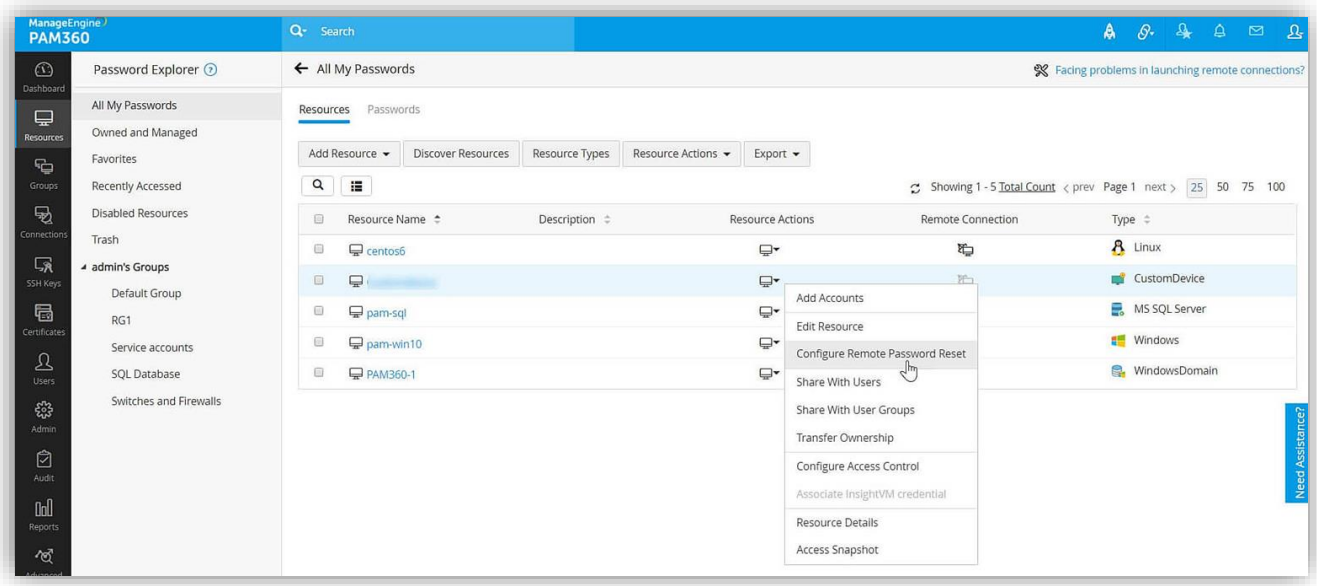
and groups in your domain by following the steps given below:

1. Navigate to **Resources** tab.
2. Select **Discover Resources** given at the top of the resources list.
3. Supply your domain details (PAM360DC) in the **Windows** screen and click **Fetch Groups and OUs**'.
4. From the enumerated list, select the Groups or OUs that you would like to import.
5. Hit **Import**. This will fetch your Groups/OUs and list them under **Groups**.
6. The member servers in the imported Groups/OUs will also be listed individually under **Resources** along with their respective local accounts.

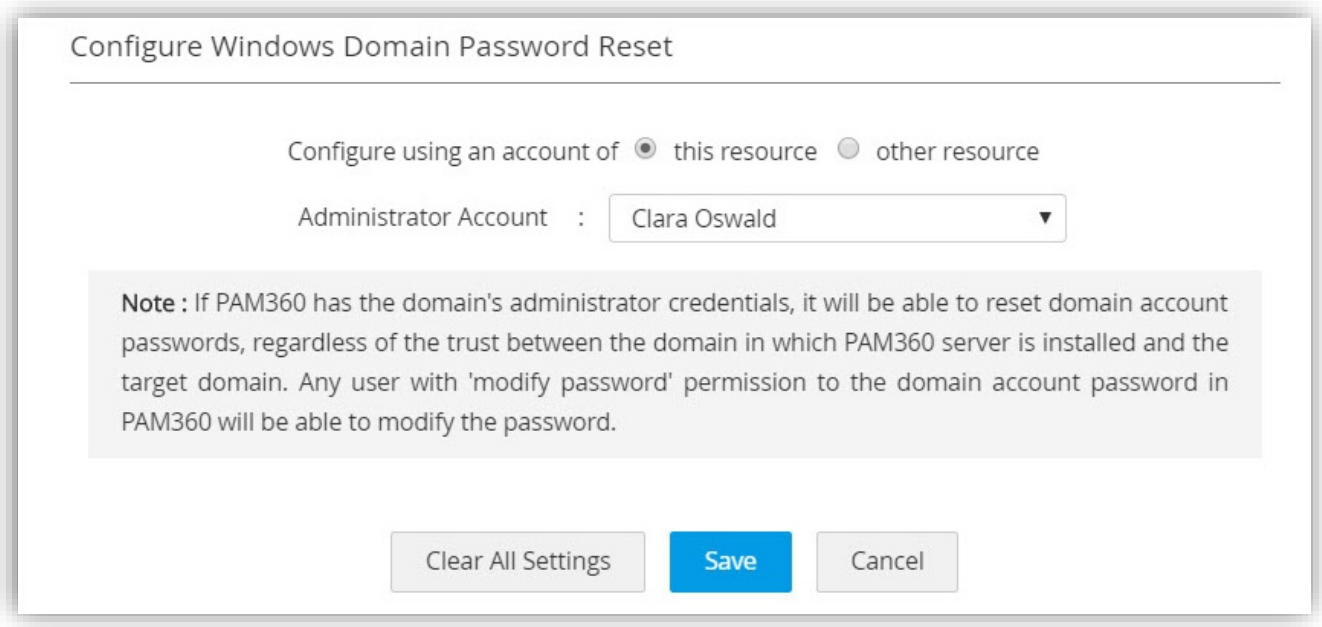
2.4 Configure Windows Scheduled Tasks Remote Password Reset

Instead of manual addition explained in Step 3, you can also discover the required resources and groups in your domain by following the steps given below:

1. Navigate to **Resources** >> **Resource Actions** against the WindowsDomain resource and select **Configure password reset** from the drop down.

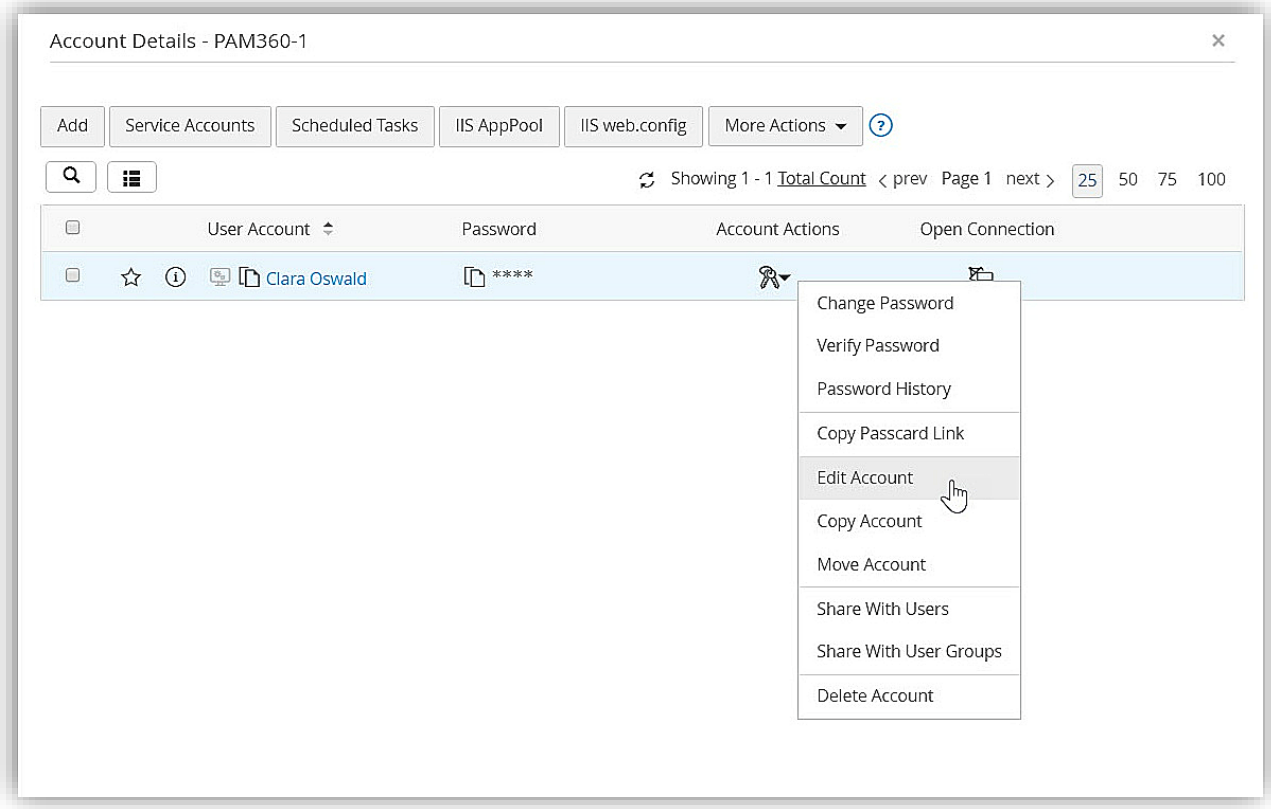


2. In the pop-up form that appears, select the 'Domain Admin' account as the **Administrator Account**.
3. Click **Save**.

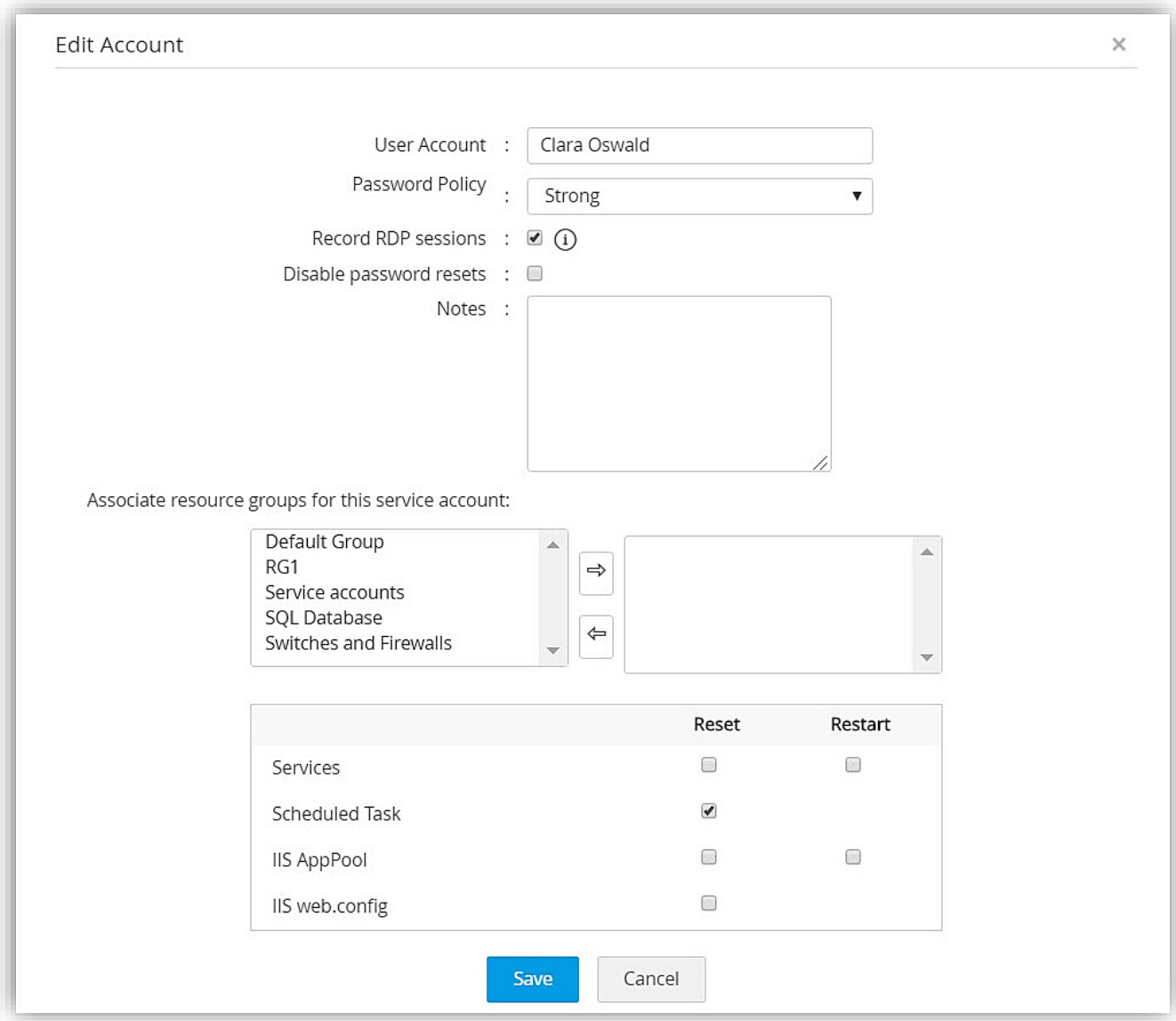


2.5 Associate Resource Groups for the Scheduled Tasks and Verify Supported Scheduled Tasks

1. Click on the WindowsDomain resource name.
2. In the UI that opens, click the **Account Actions** icon against the scheduled task account and then select **Edit Account** from the drop down.



3. In the pop-up form that appears, associate resource groups for this scheduled tasks account by moving desired groups to the other box on the right side.



4. Check the checkbox for scheduled task account which you added in the **Windows Domain** resource and click on the scheduled task account tab-> select Supported scheduled tasks tab.
5. Scheduled tasks which uses this domain accounts as log on accounts will be listed. When you reset the password, it will be updated for the accounts used in the scheduled tasks running in the remote machine as well.

3. Viewing Scheduled Tasks Status

For any windows domain account (for which you have enabled Windows scheduled tasks reset), you can view the list of associated scheduled tasks and information on Windows scheduled tasks password reset.

To view this information,

1. Go to **Resources** tab and click the name of the resource.
2. In the UI that opens, select the domain account of the resource for which you wish to know the status of scheduled tasks password reset and click **Scheduled Tasks** button at the top of the list of accounts.
3. In the dialog box that opens, switch to **Scheduled Tasks Status** tab.

Remote Password Reset Using SSH Command Sets

1. Overview
2. How SSH Command Sets work in PAM360
3. Supported resource types
4. Steps to configure SSH Command Sets for custom resource types
   4.1 Adding custom commands
   4.2 Creating a Command Set
5. Adding a custom resource type and mapping Command Sets to it
6. Adding a new resource and mapping it to the resource type
7. Adding accounts to the resource
8. Configuring remote password reset
9. Applying Command Sets to accounts in bulk

1. Overview

PAM360 supports automatic remote password reset for a wide range of commonly-used resource types such as Windows local accounts, Windows domain accounts, Linux root accounts, etc. For custom devices that allow SSH connections, PAM360 provides SSH command sets option through which you can add the password reset commands used in the command-line interface of your resource type directly to the PAM360 web interface, without the need for a CLI terminal.

PAM360 offers a default set of basic commands that you can use right away; alternatively, you can add your own commands, arrange them in the order of execution, and combine them into a new command set. This way, you'll be able to add accounts that have varying password authentication methods but fall under a single custom resource type. For example, Linux resources have different password authentication flows for root passwords and regular user passwords; similarly, Cisco devices support five different types of users. In such cases, you will be able to add any number of custom commands and specify the order in which they are to be executed.

Note: While all Administrators can view the SSH command sets, only the **Privileged Administrators** will be able to add, edit, modify, and delete the commands and the command sets.

2. How SSH Command Sets Work in PAM360

To create your own set of commands in PAM360 and ensure they work as expected, you must follow the flow given below:

1. Create one or more command sets
   1.1 Choose from the existing commands or add your custom commands.
   1.2 Combine commands in the correct sequence of execution and create a command set.
2. Add a custom resource type in PAM360 in case of devices that are not supported by PAM360.
3. Map one or more command sets to the custom resource type.
4. Add a new resource and map it to the custom resource type.
5. Create accounts in the new resource and map an individual command set to each account.

3. Supported Resource Types

You can configure remote password reset for the following SSH-based resource types using SSH Command Sets. In addition, you can also add custom commands and configure remote password reset for other SSH-based devices that are not included in this list.

1. Aruba ATP
2. ASA Firewall
3. Audiocode
4. AVAYA-GW
5. Brocade
6. Brocade VDX
7. Brocade SAN Switch
8. Checkpoint Firewall
9. Cisco Management Integration Center
10. Cisco Catalyst
11. Cisco Nexus OS
12. Cisco SG300

13. Cisco UCS
14. Cisco Wireless LAN Controller
15. Citrix Netscaler SDX
16. Citrix Netscaler VPX
17. Dell IDRAC
18. Extreme Networks
19. F5
20. Fortinet
21. Fortigate Firewall
22. Fortimail
23. FortiManager-FortiAnalyzer
24. Fujitsu Switch
25. Gigamon
26. H3C
27. HMC
28. HP Printer
29. HP Onboard Administrator
30. HPUX
31. HP Virtual Connect
32. HPE StoreOnce
33. Huawei
34. Juniper Netscreen ScreenOS
35. JunOS
36. Mac OS
37. Magento
38. Mikrotik
39. Netapp 7Mode
40. Netapp CDot
41. Nimble Storage
42. Nortel
43. OpenGear
44. Orange Firewall
45. Palo Alto Networks
46. Pfsense
47. Routerboard

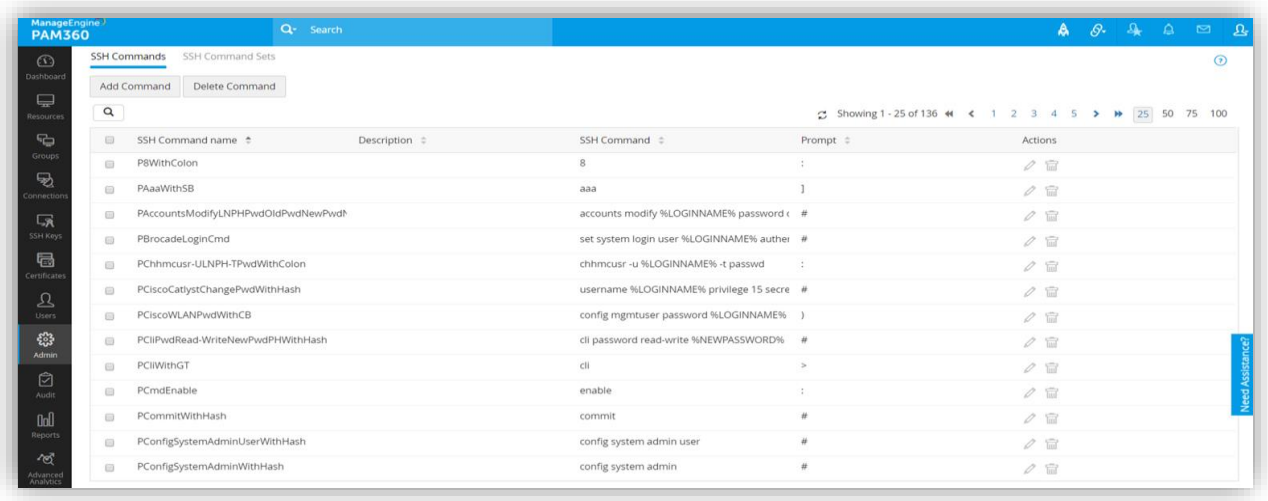
48. Ruijie
49. Sonicwall
50. TPLINK
51. VMWare VCenter, VMWare ESXi
52. Linux
53. IBM AIX
54. Solaris

4. Steps to Configure SSH Command Sets for Custom Resource Types

Follow the below steps to add or delete new commands to PAM360 and create a new command set.

4.1 Adding Custom Commands

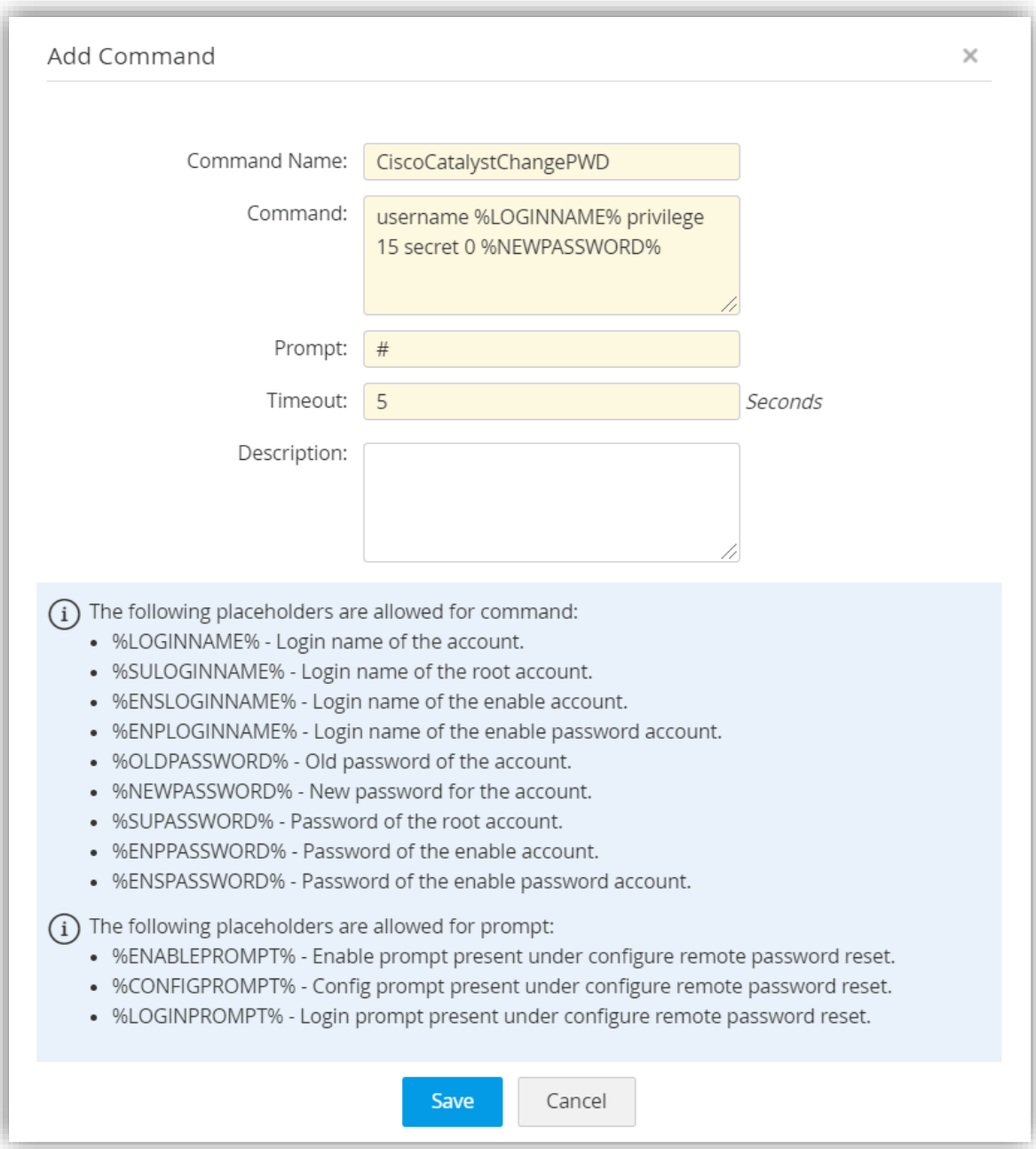
1. Navigate to **Admin >> Customization >> SSH Command Sets.**
2. Under the **SSH Commands** section, there are other default commands ready to use. You can pick the required commands from the list and create a new command set for your resource type.



3. To add new commands for your custom resource, click the **Add Commands** option and enter the Command Name, Command, the appropriate prompt, a short description, a timeout period in seconds and click **Save**.
    - The **Command** entered must be of the format specified in the tool tip below. Refer to the below tooltip text in **section 4.1.1** for examples.
    - The **Command Prompt** entered must be the same as in your CLI. For example, if

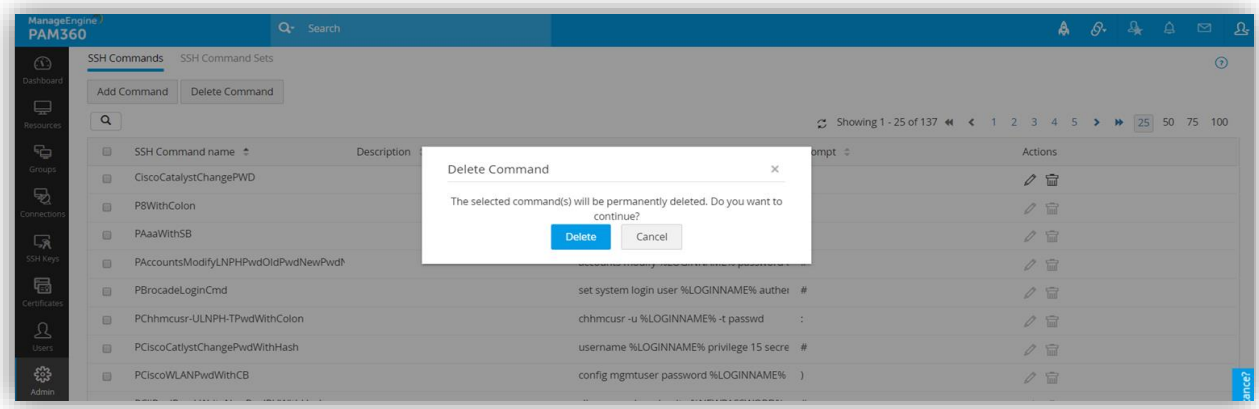
the prompt in the device is a colon and a space, then it should be entered here as such ": " (without quotes).

- The **Timeout** period denotes the amount of time for which the system awaits for an input.



4.1.1 Deleting Commands

1. To delete an existing command, click the delete icon beside the command under **Actions**.
2. To delete multiple commands at once, select the commands and click the **Delete Command** option at the top.

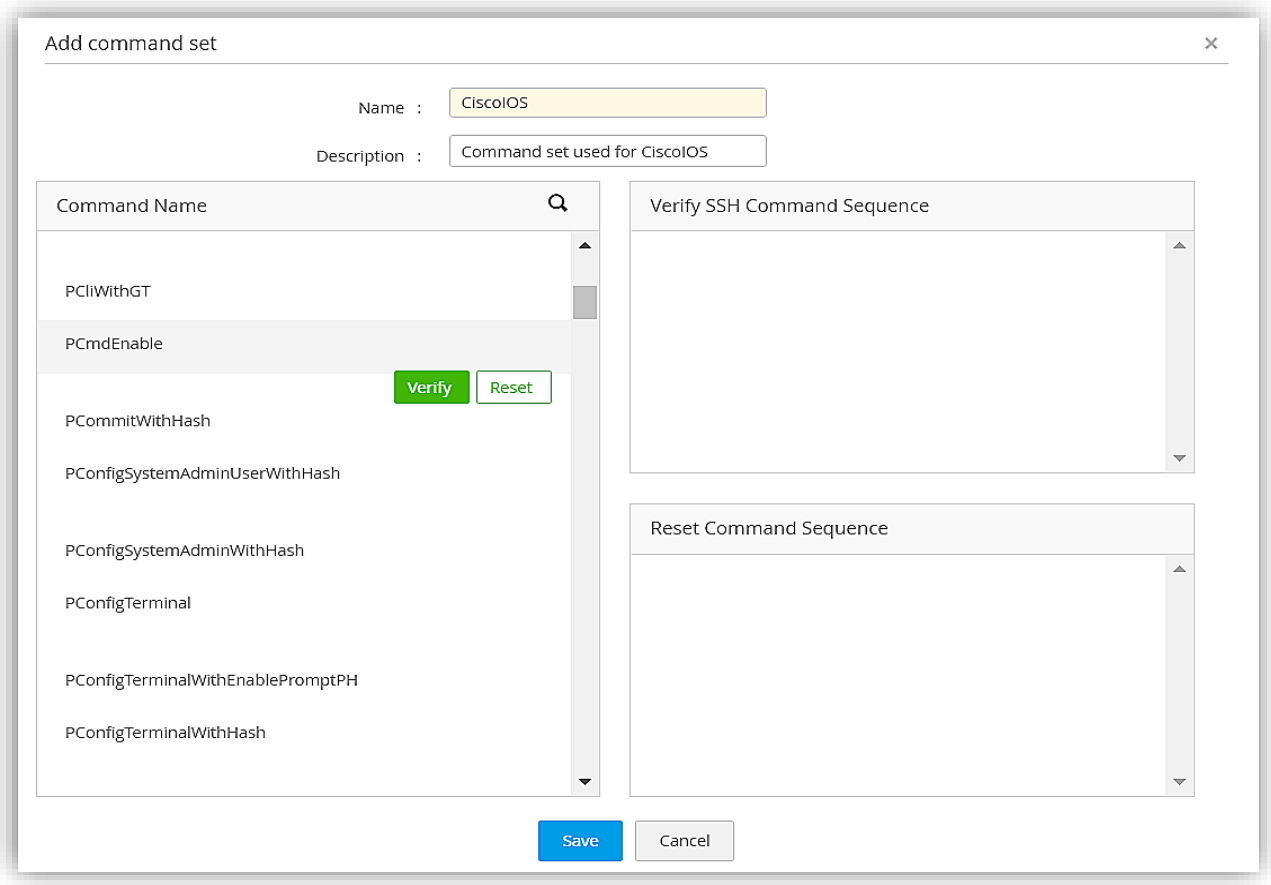


Notes:

- Default commands cannot be edited or deleted.
- Custom commands that are already associated with a resource type cannot be deleted.
- While deleting commands in bulk, in case you select a default command or a custom command that is already in use, those commands will be excluded and the rest will be deleted. Details of this operation will be registered in the Audit logs.

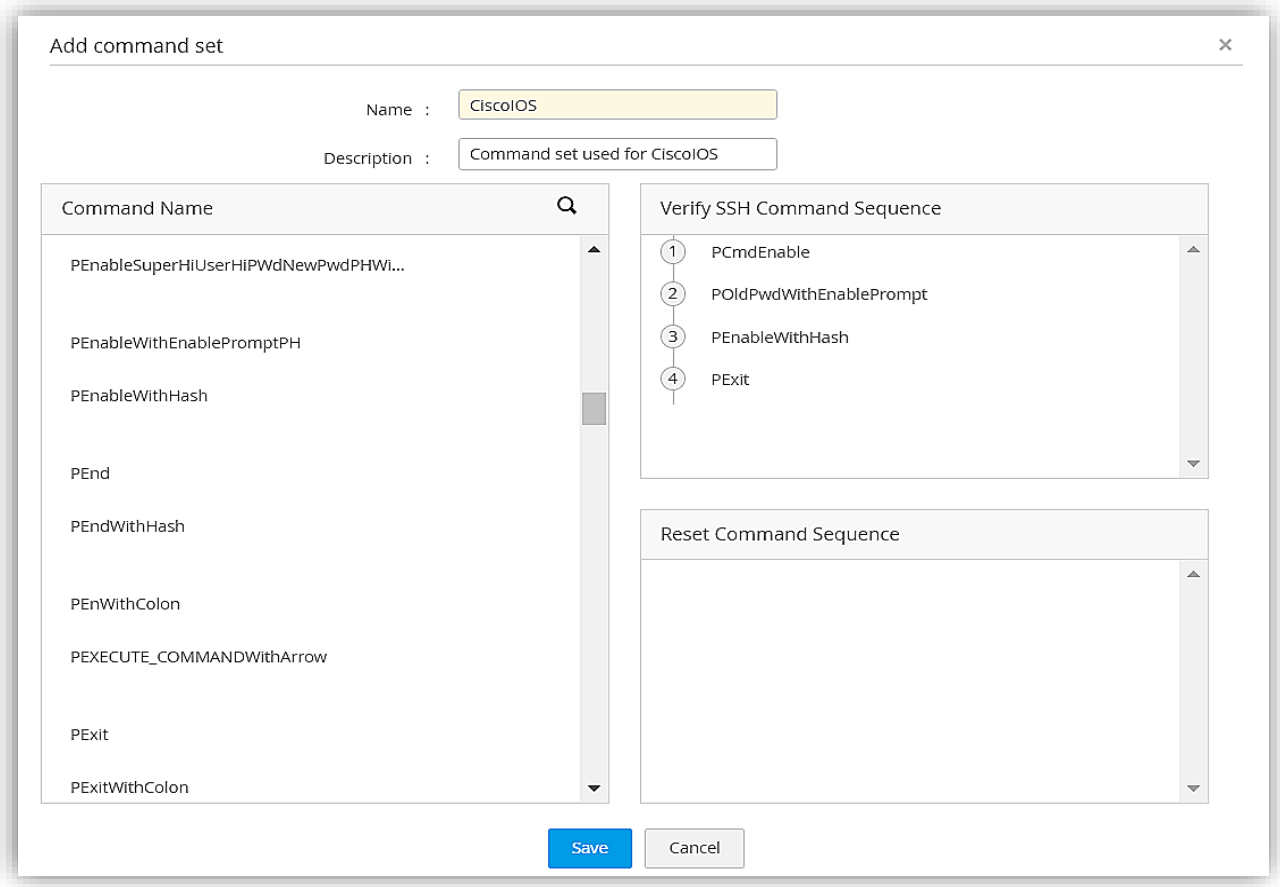
4.2 Creating a Command Set

1. Once you have added your custom commands to PAM360, go to the **SSH Command Sets** section to create your command set.
2. Click the **Add command set** option. In the **Add command set** dialog box, add a name and a description for your command set.
3. The default commands and the custom commands you have added will be listed in the **Command Name** box.
4. On the right, you will find two sections: **Verify SSH Command Sequence** and **Reset Command Sequence**.



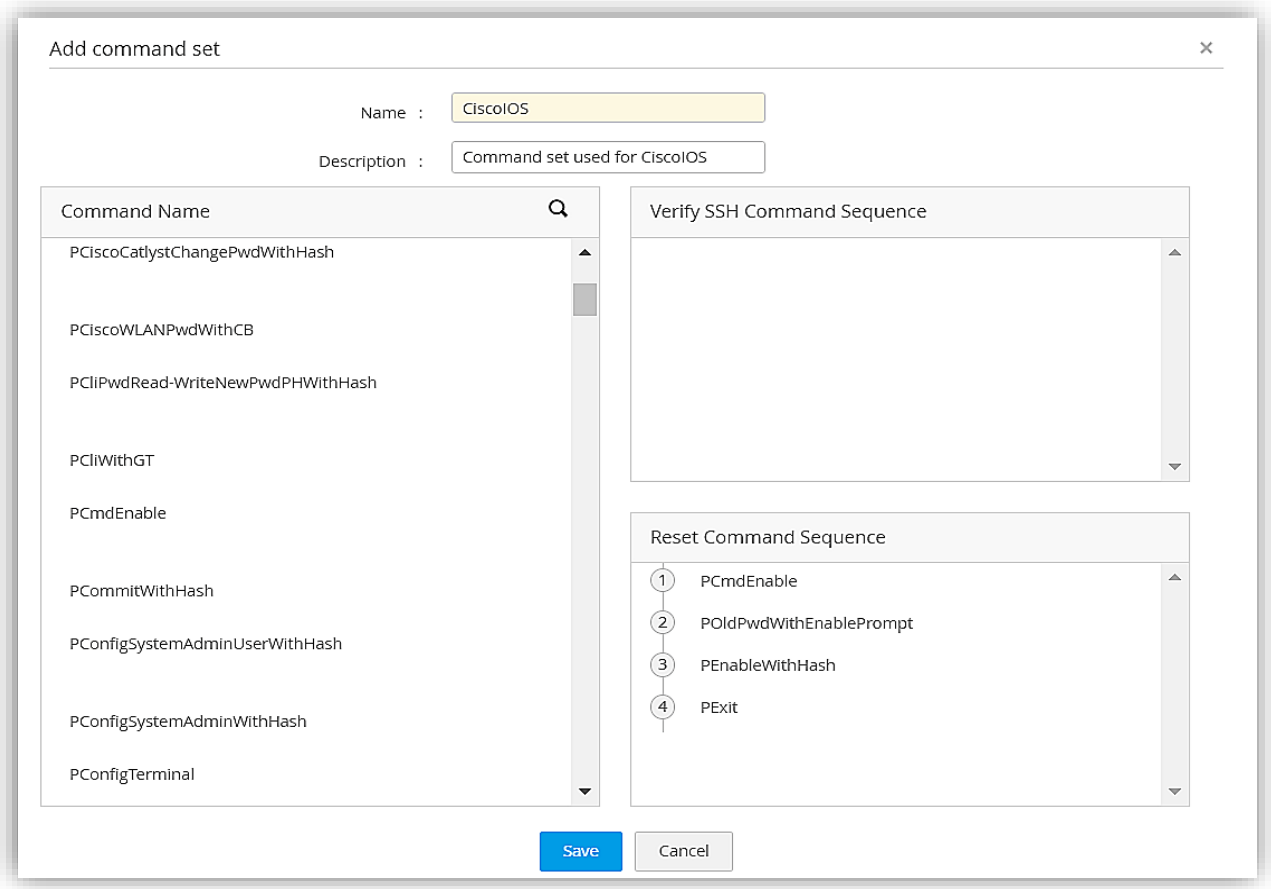
4.2.1 Verify SSH Command Sequence

1. Hover your mouse over a command in the **Command Name** box and you will see two options: **Verify** and **Reset**.
2. Click **Verify** to move the commands into the **Verify SSH Command Sequence box**. Drag the commands to re-order them into the correct sequence. This is the command sequence that is to be carried out to verify the integrity of the password i.e, check if the password of an account is in sync with the one stored in PAM360.
3. Click **Save**. A new verify password command set will be added to PAM360.
4. Once this command set is associated with an account and remote password reset is configured for the resource it belongs to, the password verification check will be carried out in given sequence.



4.2.2 Reset Command Sequence

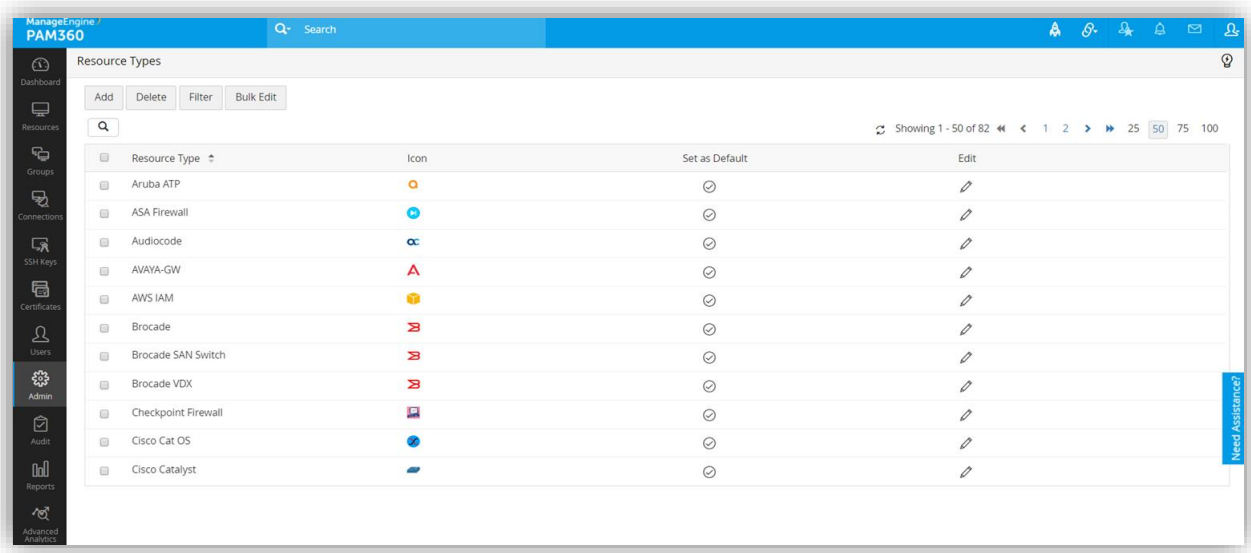
1. Hover your mouse over a command in the **Command Name** box and you will see two options: **Verify** and **Reset**.
2. Click **Reset** to move the commands into the **Reset Command Sequence box**. Place the commands in the correct sequence and click **Save**. A new command set will be added to PAM360.
3. Once this command set is associated with an account and remote password reset is configured for the resource it belongs to, the password reset will be carried out in given sequence.



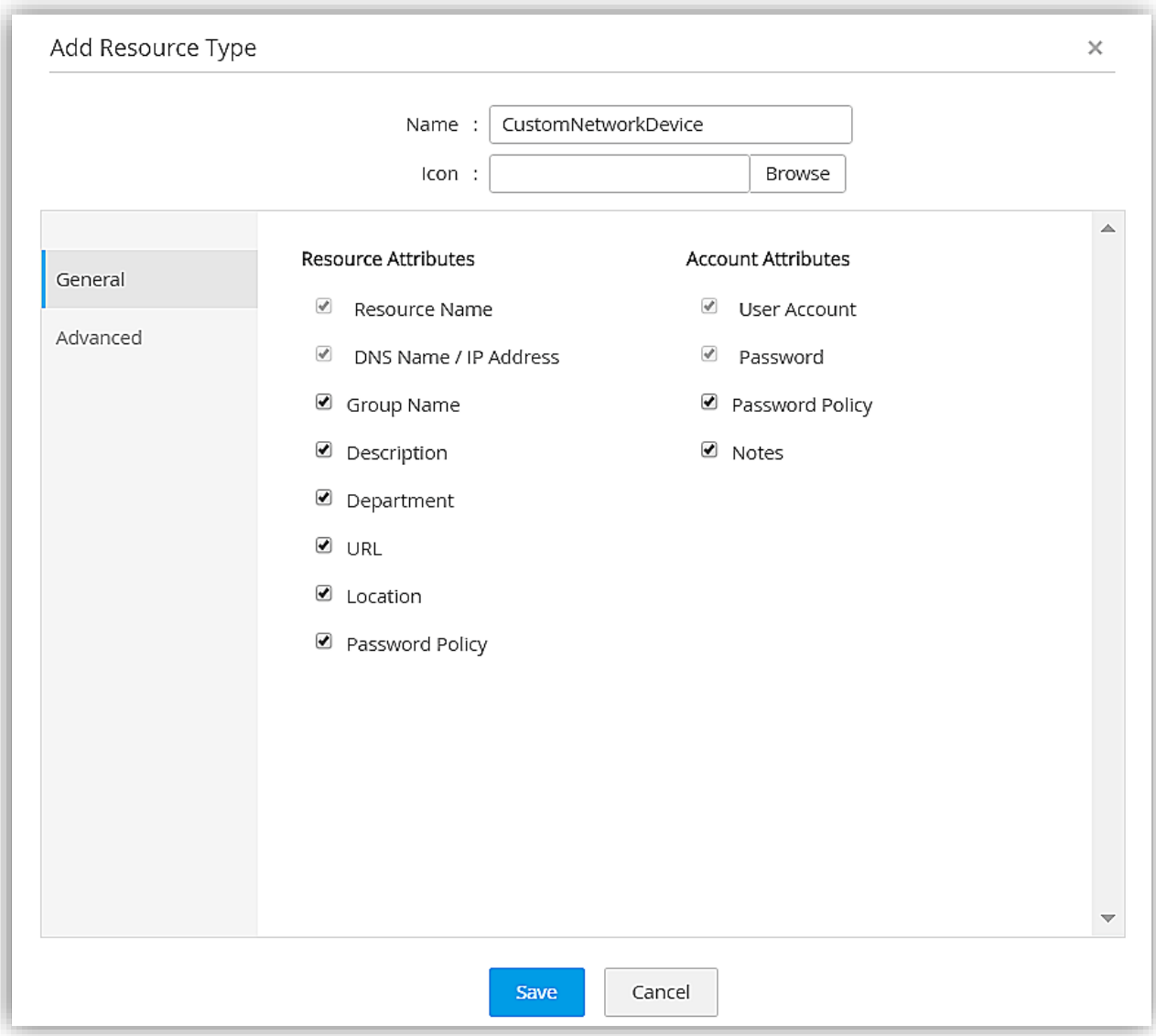
5. Adding a Custom Resource Type and Mapping Command Sets to It

Once your command sets are created, follow the below steps to create a custom resource type and map the command sets to it:

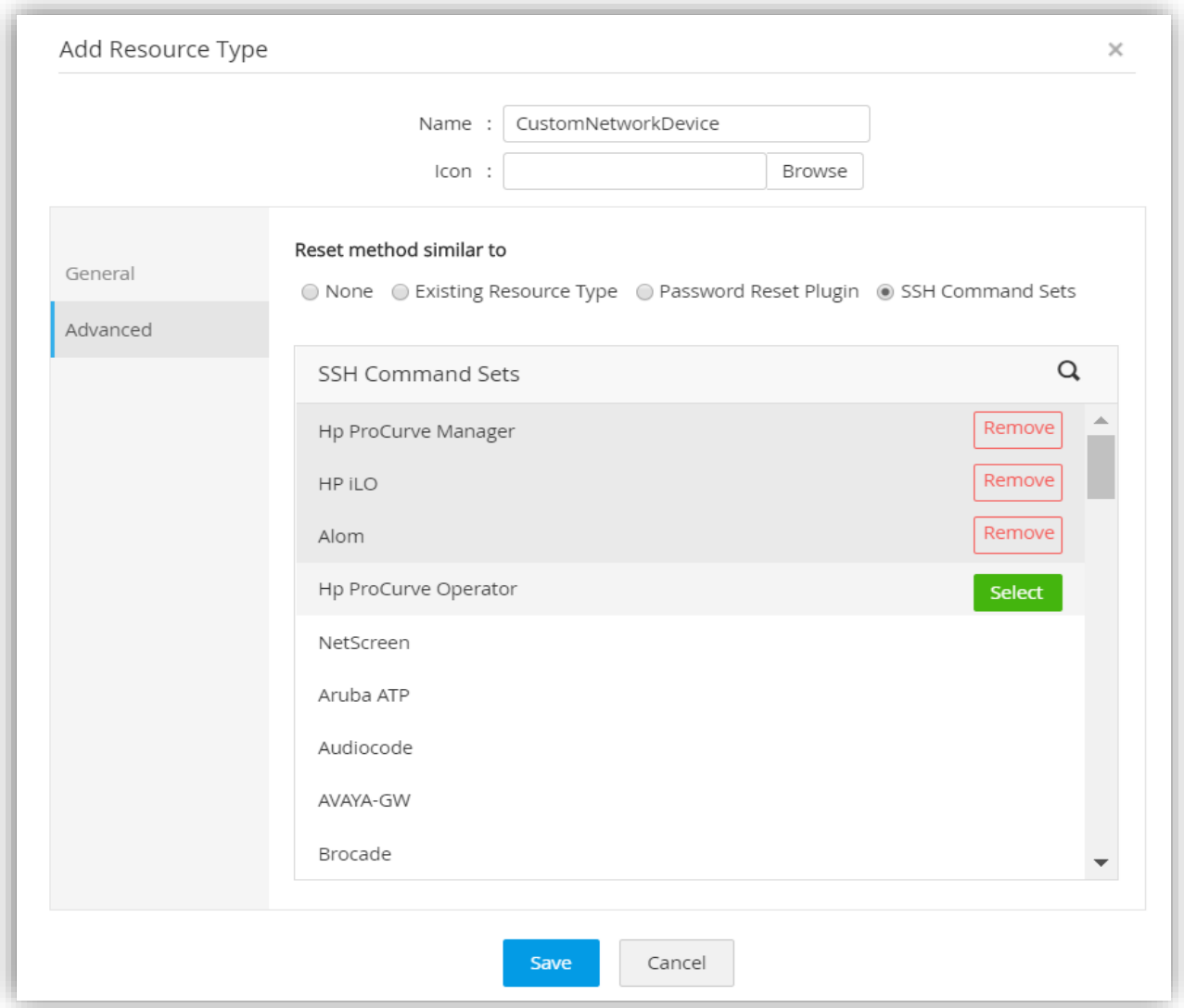
1. Navigate to the **Resources** tab >> **Resource Types** and click **Add.**
2. Enter a name and browse for an icon of your choice. This icon image will be displayed under **Type** in the **Resources** tab.



3. Under the **General** section, select the Resource and Account Attributes for the resource type.



4. In the **Advanced** section, select **SSH Command Sets.** Default and custom command sets will be listed under this option.



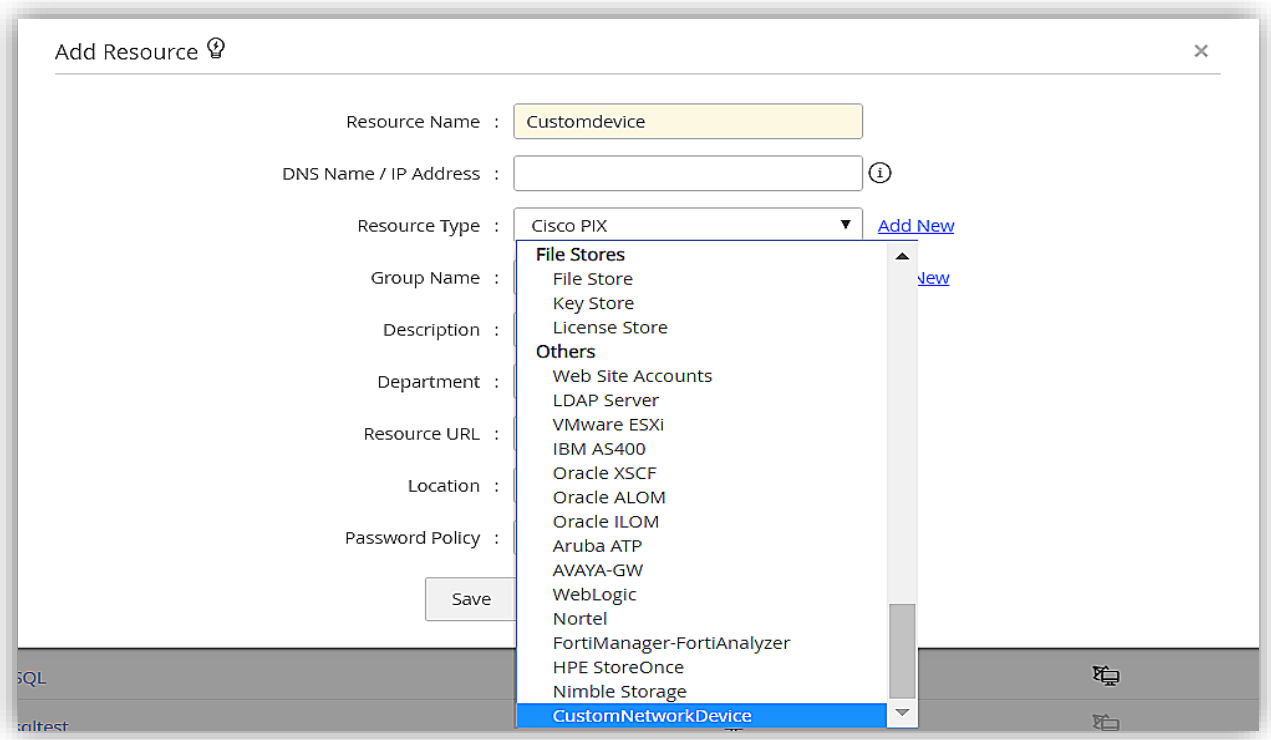
5. Choose any by clicking on the names of the command sets. You can assign multiple command sets to one resource type.
6. Once you have selected the required command sets, click **Save**. Now, the new resource type will be added to the list of resource types in PAM360.

6. Adding a New Resource and Mapping it to the Resource Type

Follow the below steps to add a new resource which can be mapped to the newly-created resource type:

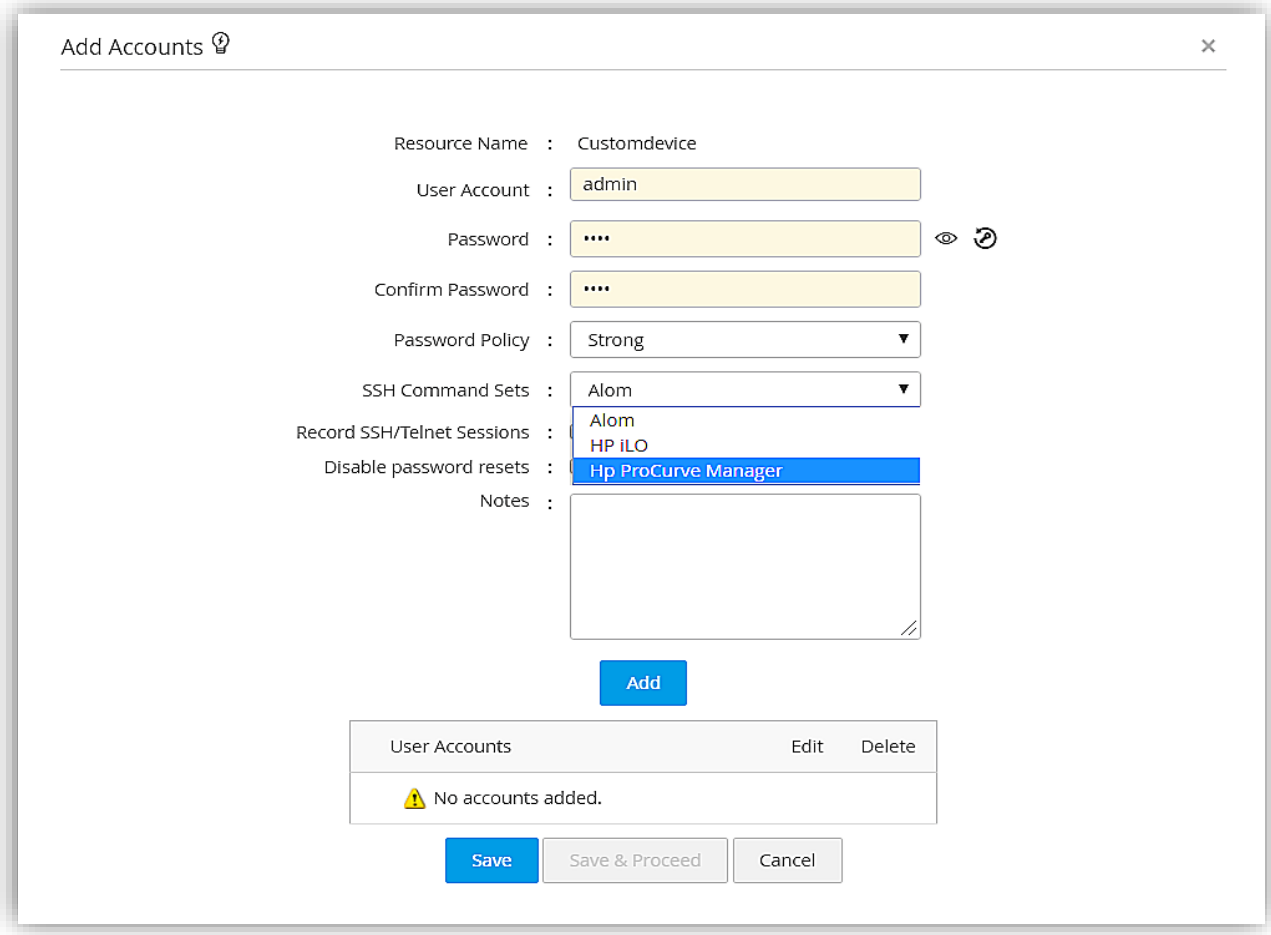
1. Navigate to the **Resources** tab **>> Add Resource >> Add Manually**.

2. Enter the Resource Name, DNS Name, and choose the new resource type from the **Resource Type** drop down under **Others**.
3. Click **Save and Proceed** to continue adding accounts to the resource.



7. Adding Accounts to the Resource

1. In the **Add Accounts** dialog box, enter the **User Account name**, **Password,** and **Password Policy.**
2. The **SSH Command Sets** drop down will display all the command sets mapped to this resource type. Pick a command set from the drop down, click **Add** and **Save**.
3. The selected command set will be mapped to the account.
4. You can add multiple accounts and map command sets to each account in the same way.

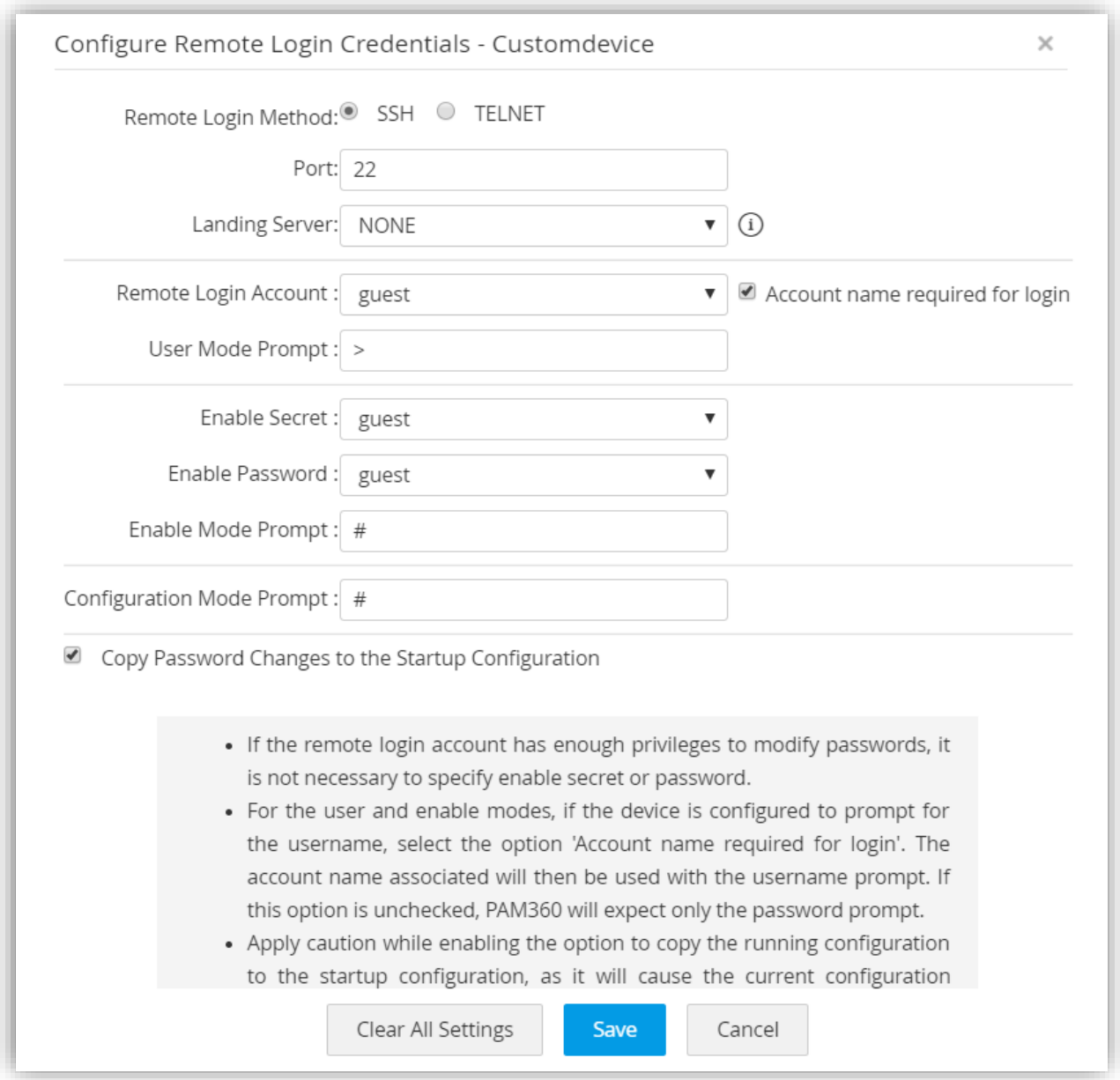


Note: The user account credentials provided here must be valid for the **Verify** and **Reset** command sets to work as expected.

8. Configuring Remote Password Reset

Once the command set is mapped to an account, follow the below steps to configure remote password reset and select a root account, if applicable.

1. Navigate to the **Resources** tab.
2. Click the **Resource Actions** icon beside the required resource and click **Configure Remote Password Reset**.



3. Select the **Remote Login Method** and **Remote Login Account** as required. Fill in the other details such as **User Mode Prompt**, **Configuration Mode Prompt.**
4. Click **Save** to save the changes.

> Refer to the **Remote Password Reset** help section to know more about remote password reset.

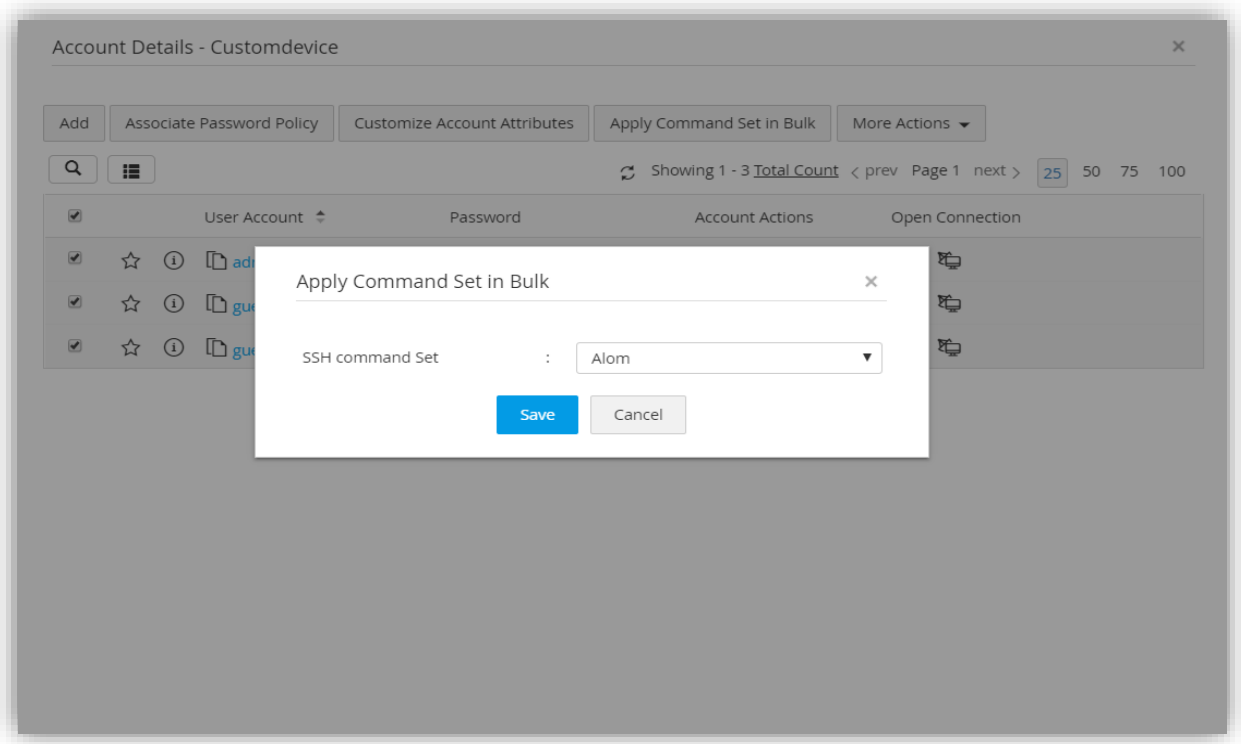
9. Applying Command Sets to Accounts in Bulk

Follow the below steps to apply a single command set to multiple accounts within a single resource:

1. Navigate to the **Resources** tab and click any resource name. A list of all the accounts

associated with that resource will be displayed.

2. Select the accounts for which you want to apply a command set, and click **Apply Command Set in Bulk** from the top.



3. In the **Apply Command Set in Bulk** pop-up form, choose the required command set from the drop down and click **Save**.
4. The chosen command set will be applied to all the selected accounts, overriding their previous command set configuration, if any.

Self-Service Privilege Elevation in PAM360

Self-Service Privilege Elevation allows end-users to perform highly privileged operations in remote sessions without relying on administrators for their approvals. The highly privileged operations include; installing applications, executing specific operations, executing commands, etc., that need administrator or root privileges, depending on the type of Operating System. The process involves configuring the selected accounts/resource with the allowed apps/scripts/commands shared with the end-users for their accessibility. Users with the administrator role control the overall configuration of Self-Service Privilege Elevation with predefined rules and policies.

Let us consider a case where an administrator has to allow a non-privileged user to install third-party applications or execute commands to access a particular directory for a specific period. It will be painful for the administrator when this has to be repeatedly done for multiple users. Here comes this elevation feature into play - it allows configuring users' operations with a privileged account, which lets users self-elevate privileges for a stipulated time until they complete their intended operations.

> **Note:**
>
> The Self-Service Privilege Elevation feature together with access control workflow and SSH command control (Linux) will ensure a higher level of security by allowing the privilege elevation with time-framed and command-based restrictions.

At the end of this document, you will have learned the following in detail:

1. Self-Service Privilege Elevation for Windows and Windows Domain
2. Self-Service Privilege Elevation for Linux

1. Self-Service Privilege Elevation for Windows and Windows Domain

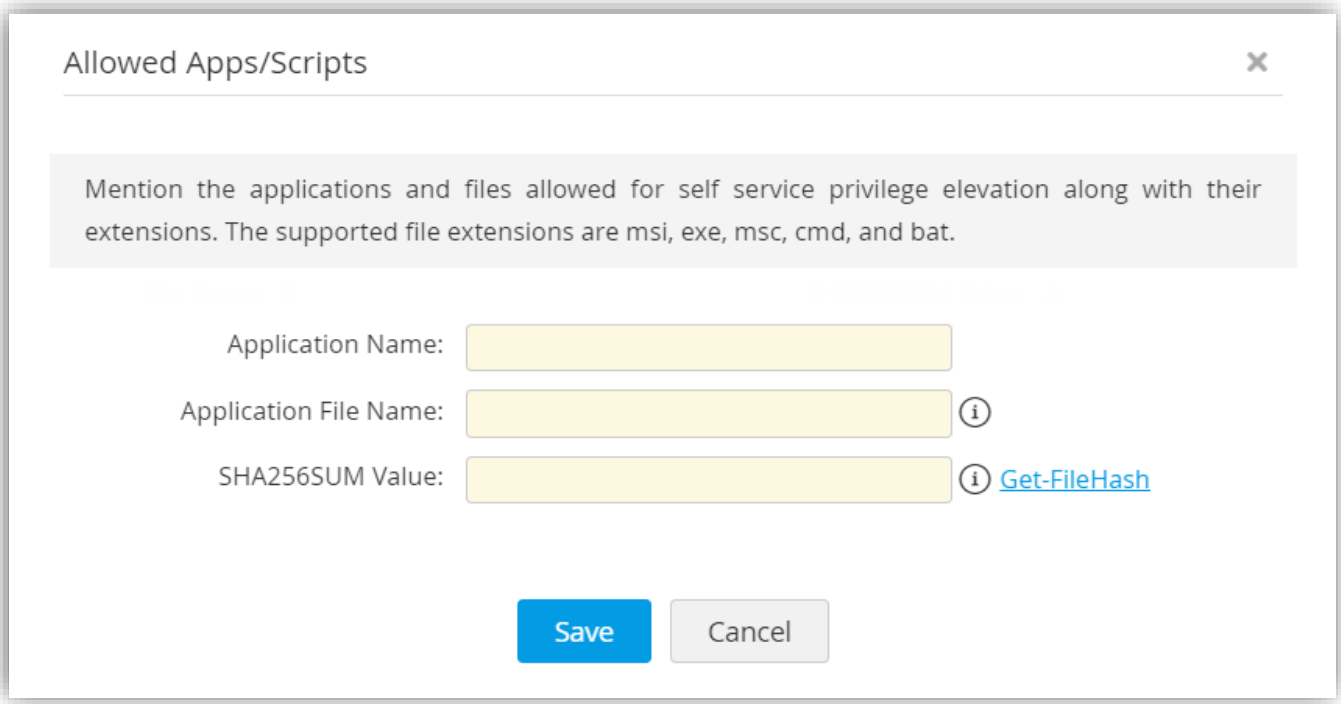
(This feature is applicable from build 5304 and later for C# Agent only)

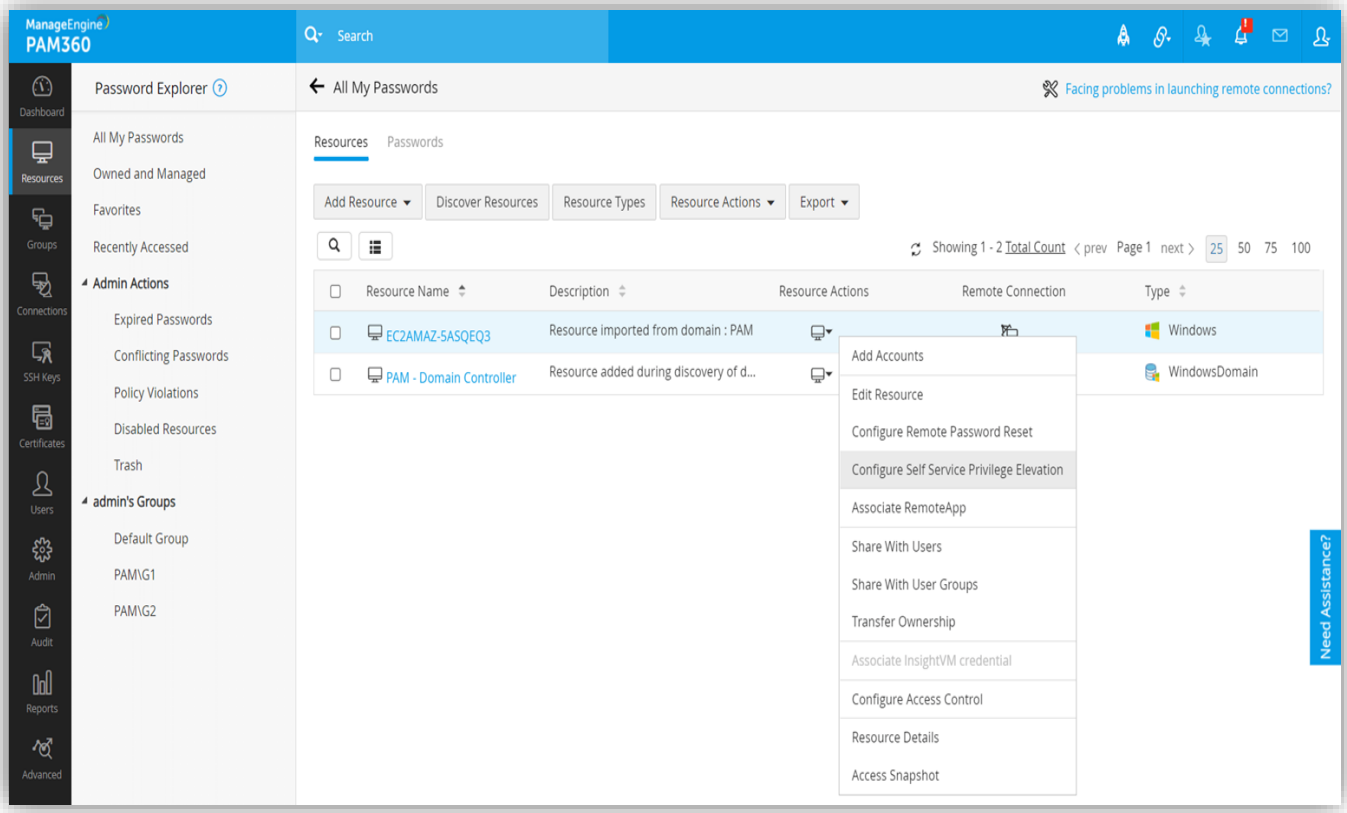
PAM360 allows administrators to configure Self-Service Privilege Elevation to the target machines. This allows users to run certain types of files/applications (.cmd, .exe, .msc, .msi, and .bat) with elevated account privileges without sharing the password of the higher privilege account.

1.1 Setting up Self-Service Privilege Elevation

First, install C# agent with Self-Service Privilege Elevation in the target machine and follow the below steps:

1. Log in to PAM360 and navigate to **Admin >> Manage >>Allowed Apps/Scripts.** Here, all the applications that are allowed for Privilege Elevation are listed.
2. Click **Add** to add a new application/file to the list.
   i. In the Application/File List pop-up, enter the **Application Name** and **Application File Name** along with the extension (.cmd, .exe, .msc, .msi, and .bat).
   ii. Mention the **SHA256SUM Value** of the application to be added. Click here to know how to get the hash value of a file/application or use this application.
   iii. Click **Save.** You have successfully added the application to the Application/File List.
3. Now, navigate to **Resources >> All My Passwords >> Resources** to view the list of all the resources added in PAM360.
4. Click the **Resource action** icon against one of the owned resources and click **Configure Self-Service Privilege Elevation.**

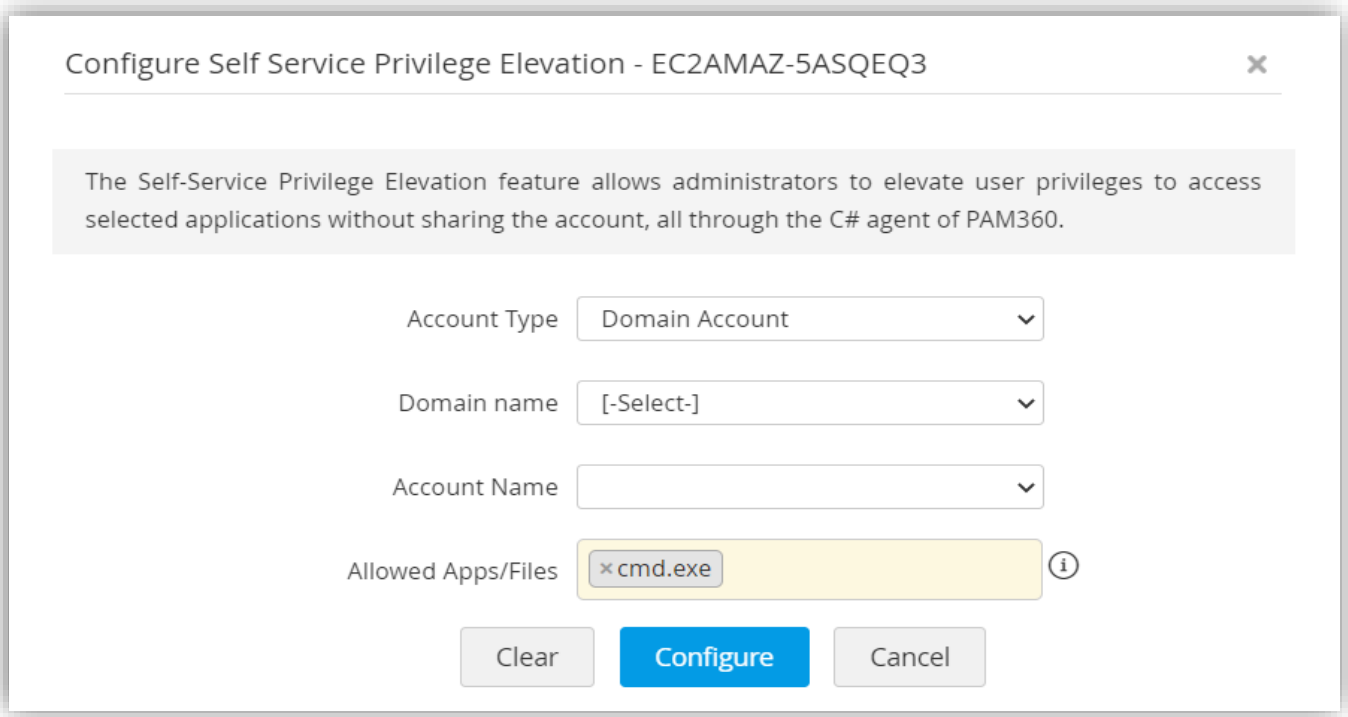




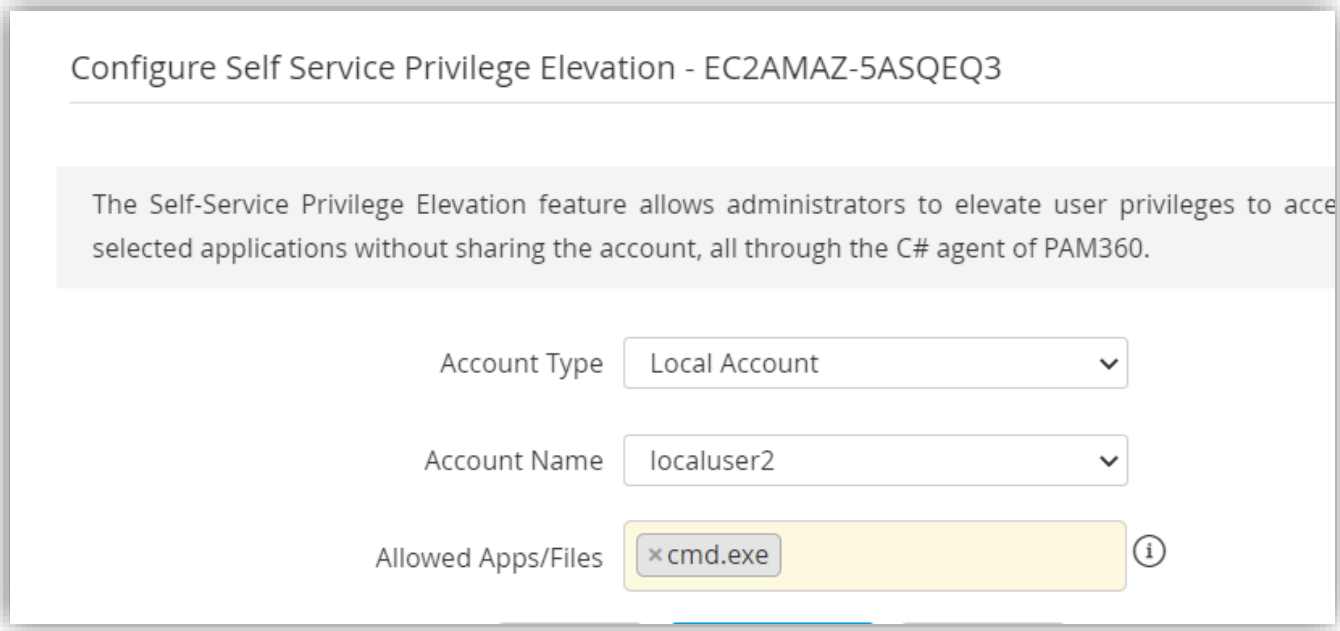
Note: The DNS name of the resource should not be empty.

5. In the pop-up that appears,

i. Select the **Account Type.**
ii. If you choose the **Account Type** as **Domain Account,** select the **Domain Name** and **Account Name.** This will allow the user to run the files/applications using the selected **Domain Account** with elevated account privileges.



iii. If you choose the **Account Type** as **Local Account**, select the **Account Name.**



Notes:

1. Here, selected account will be used for Self-Service Elevation in the Agent installed resources.
2. When access control is enabled for an account in the resource where Self-Service Privilege Elevation is configured, Self-Service Privilege Elevation will take precedence over password access control.

6. Mention the name of the files/applications that the user is allowed to access with elevated account privileges under **Allowed Apps/Files.**
   *(**Example:** cmd.exe, services.msc, etc)*

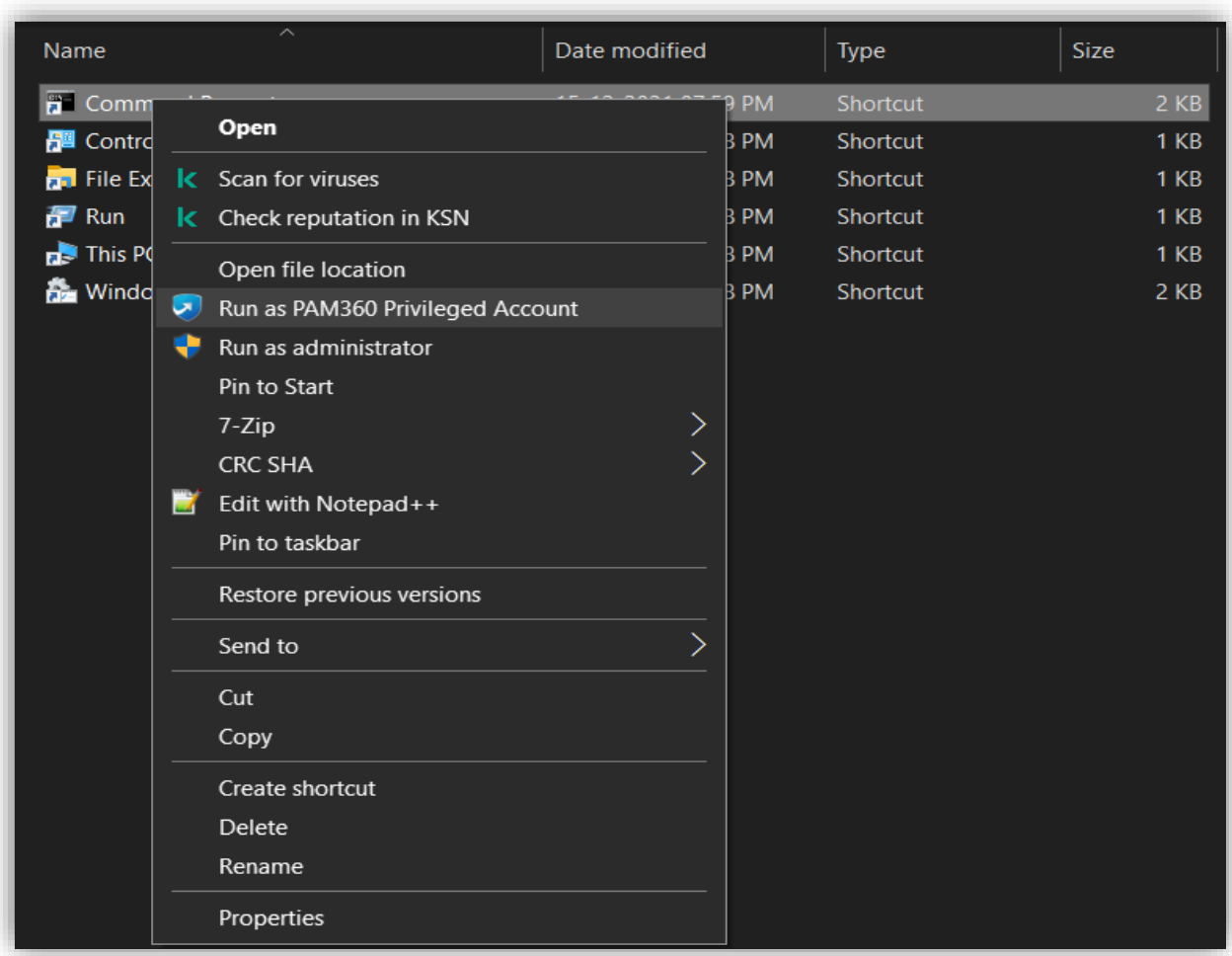
Note: .exe, .msc, .msi, .cmd and .bat are the file types that are currently available for users to access with elevated account privileges.

7. Click **Configure.** Now, you have successfully configured Self-Service Privilege Elevation.
8. Click **Clear** to reset the configurations of Self-Service Privilege Elevation.
9. To delete an application from the Application/File List, navigate to **Admin >> Manage >> Manage Applications.** Select the desired application(s) and click **Delete.**
10. Navigate to **Reports >> Query Reports >> Resources** and search **"Resources with self-service privilege elevation configuration"** under **Report Name** to find all the resources configured with self-service privilege elevation.
11. Navigate to **Reports >> Custom Reports** to find two new custom reports namely:
    - **Authorized App Privilege Elevated**
    - **Unauthorized App Elevation Triggered**

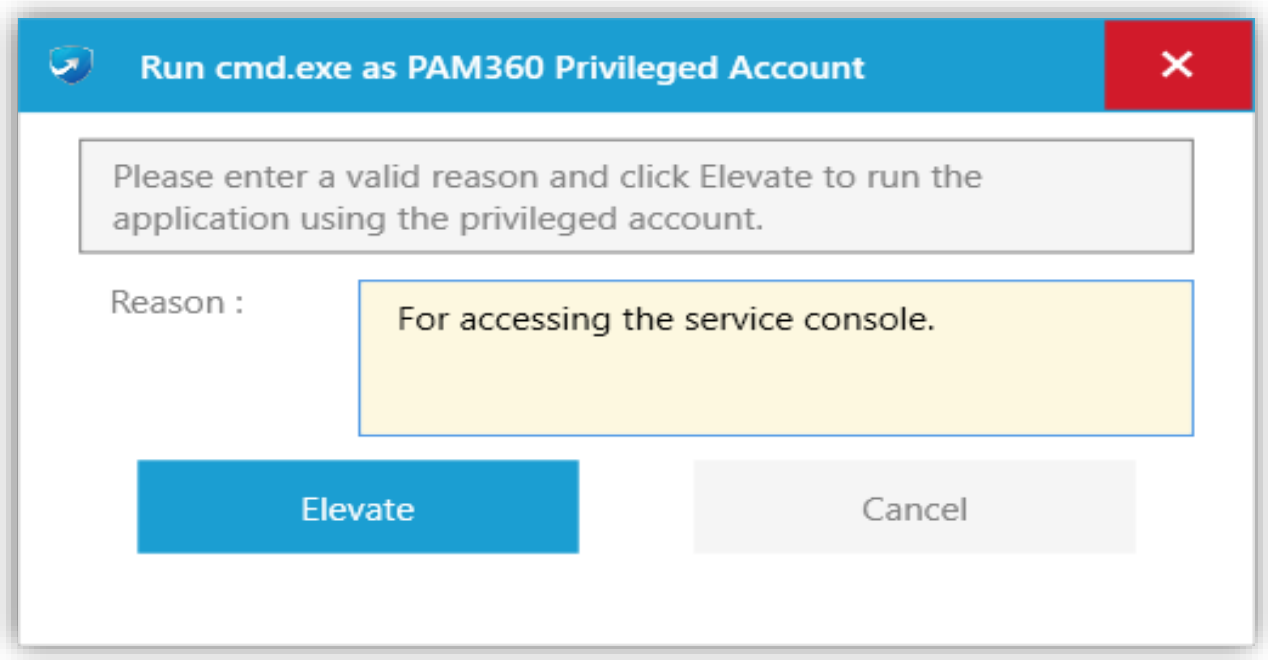
These reports allow the administrators/users with privileges to generate reports based on authorized and unauthorized self-service elevation events. To know more about creating a custom report, click here.

1.2 Using Self-Service Privilege Elevation

1. Login as any user in a resource where you have configured Self-Service Privilege Elevation.
2. Right-click on the file/application (.exe, .msc, .msi, .cmd and .bat) which is configured by administrator to open as a privilege user and select **Run as PAM360 Privileged Account.**



3. In the pop-up that appears, mention the **Reason** for elevation(mandatory) and click **Elevate.**



Now, PAM360 will allow users to run the application/file in the elevated privilege chosen by the administrator.

2. Self-Service Privilege Elevation for Linux

(Applicable from build 5950 and later for Linux Agent only)

Self-Service Privilege Elevation in Linux environments allows users to execute privileged commands with an elevated account privilege without sharing the passwords of highly privileged user accounts.

Refer to the following links to know more about configuring the Self-Service Privilege Elevation in Linux-based environments:

2.1 Installing Linux Agent

2.2 Managing Commands and Command Groups

2.3 Configuring Self-Service Privilege Elevation

2.4 Using Self-Service Privilege Elevation in Linux

2.5 Audits and Reports of Self-Service Privilege Elevation

2.6 Self-Service Privilege Elevation Precedence in Real-Time

2.1 Installing Linux Agent

Refer to this section to install the Linux agent in the desired target Linux resource for which the Self-Service Privilege Elevation is to be configured.

2.2 Managing Commands and Command Groups

After completing the agent installation, log in to your PAM360 interface and create a command group with the set of required privileged commands for which the Self-Service Privilege Elevation is to be applied in the desired target accounts or resources.

Refer to this section to learn more about creating the commands and the command groups in PAM360.

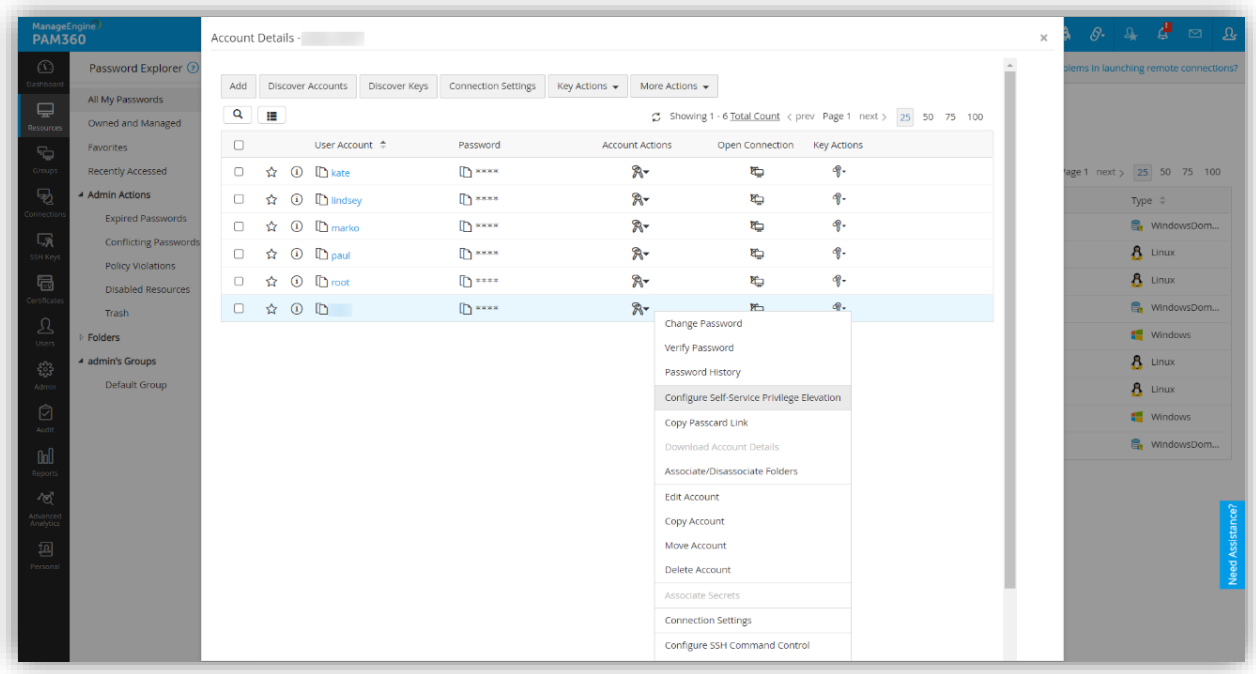
2.3 Configuring Self-Service Privilege Elevation

Once you have done with the agent installation and the command group management, you can start configuring the Self-Service Privilege Elevation for the desired accounts or resources for elevated privileges without sharing access to the privileged accounts.
Do the steps that follow to configure an account or a resource with Self-Service Privilege Elevation:

i. **Configuration at Account Level**

1. Navigate to '**Resources >> All My Passwords >> Resources**' and click on the desired resource to view the list of all the available accounts in the resource.
   [or]
   Navigate to '**Resources >> All My Passwords >> Passwords**'.

2. Click the **Account Actions** drop-down against one of the owned/shared accounts and click **Configure Self-Service Privilege Elevation**



3. In the window that opens:
    a. Provide the privileged account detail in the '**Run As**' field.

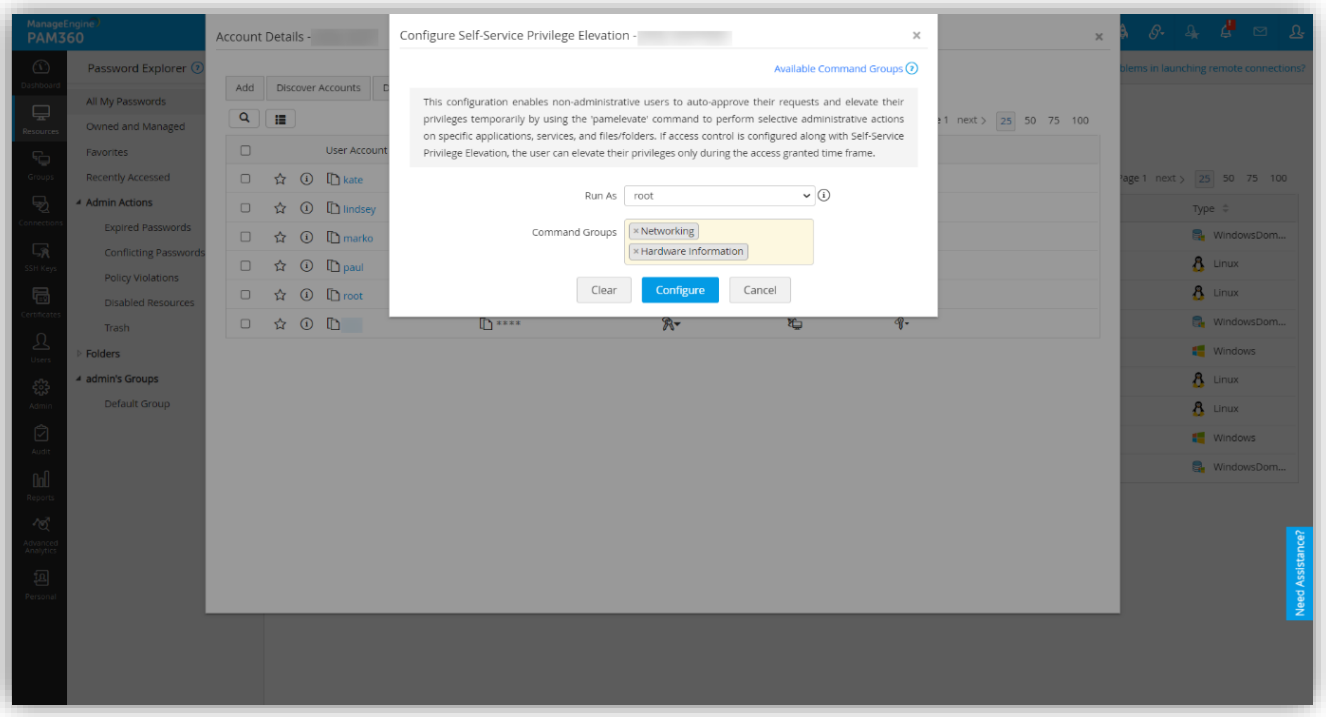
> **Note:**
>
> The account added here will be used for the Self-Service Privilege Elevation to execute the privileged commands in the devices installed with the Linux agent.

    b. Select the sets of required command groups with the privileged commands.

> **Note:**
>
> Click on the link Available Command Groups. From the pop-up that opens, you will know in detail about the commands available in the respective command groups.

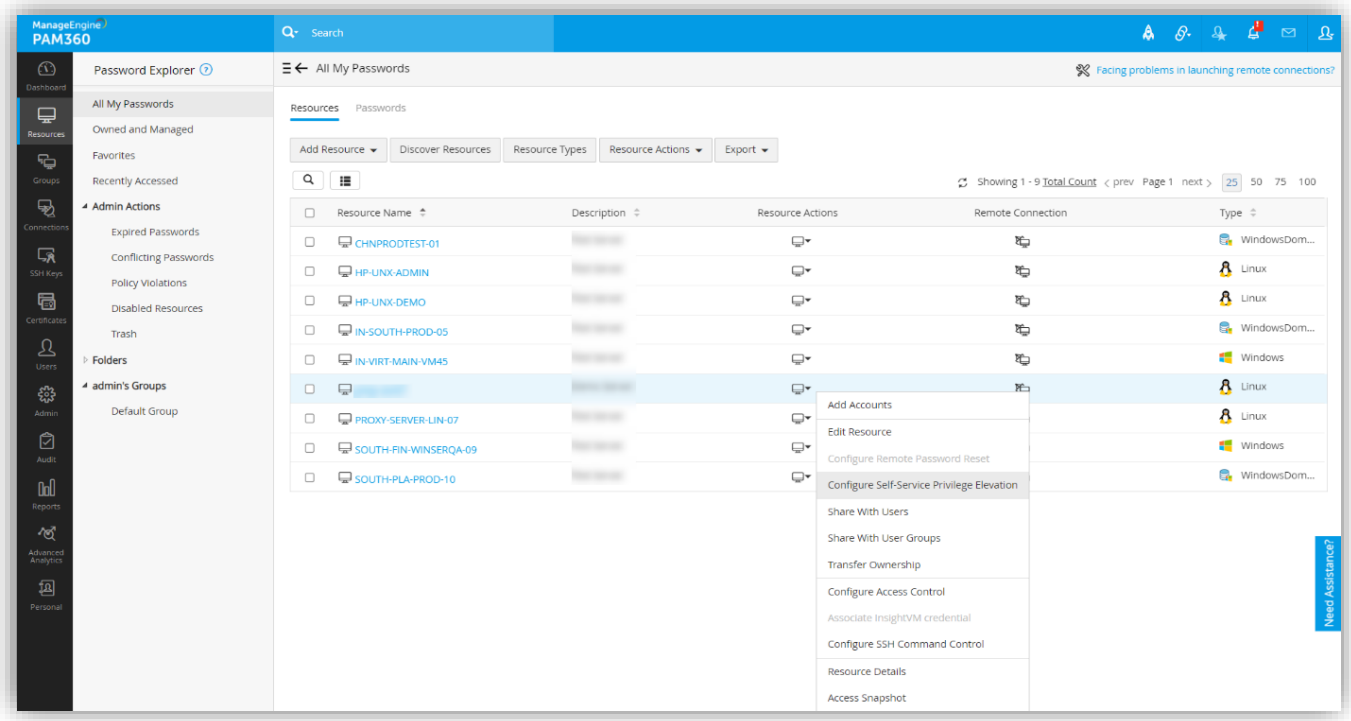
    c. Click **Configure** to complete the configuration of the Self-Service Privilege Elevation.

d. Click **Clear** to revoke the Self-Service Privilege Elevation from the account.



ii. Configuration at Resource Level

1. Navigate to '**Resources >> All My Passwords >> Resources**'.
2. Click the **Resource Actions** drop-down against one of the owned/shared accounts and click **Configure Self-Service Privilege Elevation**.



3. In the window that opens:

    a. Provide the privileged account detail in the '**Run As**' field.

> **Note:**
>
> The account added here will be used for Self-Service Privilege Elevation to execute the privileged commands in the devices installed with the Linux agent.

    b. Select the sets of required command groups with the privileged commands.

> **Note:**
>
> Click on the link Available Command Groups. From the pop-up that opens, you will know in detail about the commands available in the respective command groups.

c. Click **Configure** to complete the configuration of the Self-Service Privilege Elevation.
d. Click **Clear** to revoke the Self-Service Privilege Elevation from the resource.

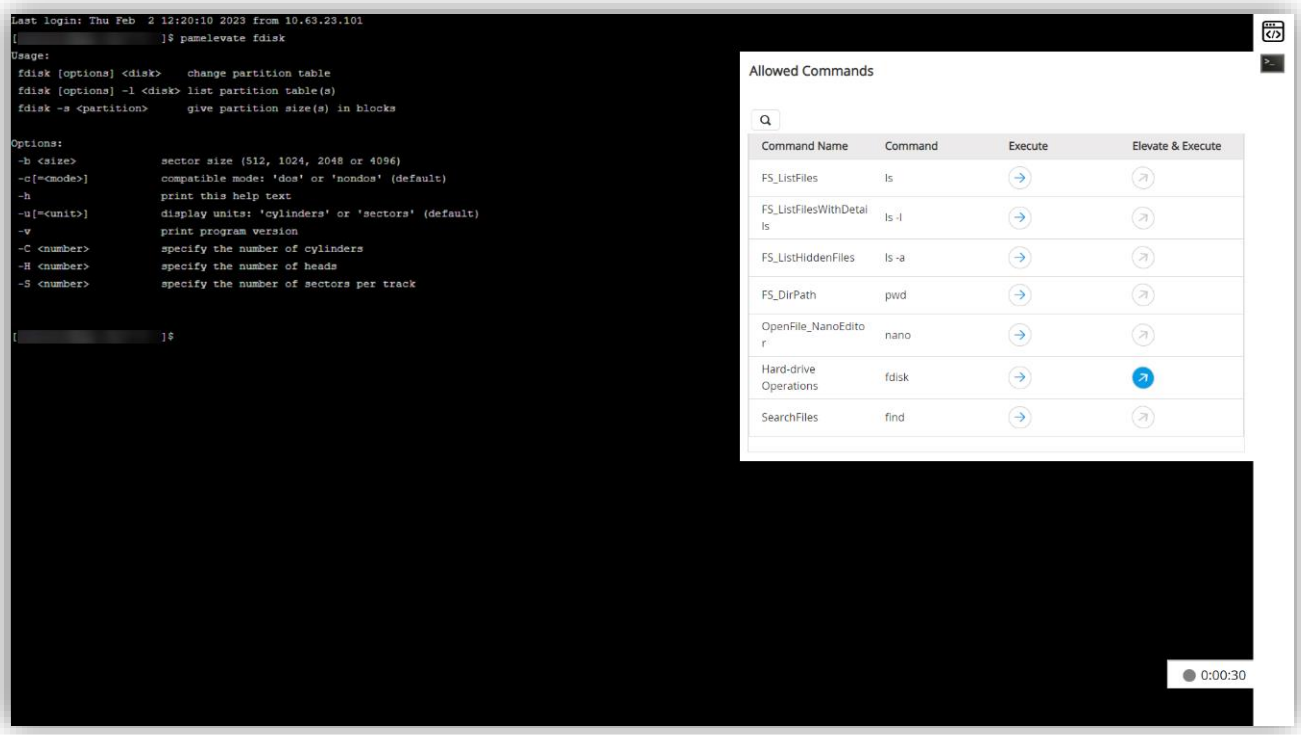
2.4 Using Self-Service Privilege Elevation in Linux

Now, users can execute privileged commands in the remote sessions of accounts configured with Self-Service Privilege Elevation. Do the steps that follow to execute the privilege commands mapped with a privileged user account for Self-Service Privilege Elevation.

> **Note:**
>
> In certain scenarios, privilege elevation might not be accessible when a user account is added to a resource after agent installation. During such situations, execute the following command first, followed by the privileged commands:
>
> **export PATH="$PATH:/(homepath)/PAM360Elevation/"**

i. From an Account Configured with SSH Command Control

1. Launch a remote session for an account configured with SSH command control and Self-Service Privilege Elevation.
2. In the session that opens, you will find a set of predefined allowed command lists associated with the logged-in SSH account.
3. Hover on the right pane and click on the execute icon under the **Elevate & Execute** list beside the desired privileged command to execute it in the launch SSH console.

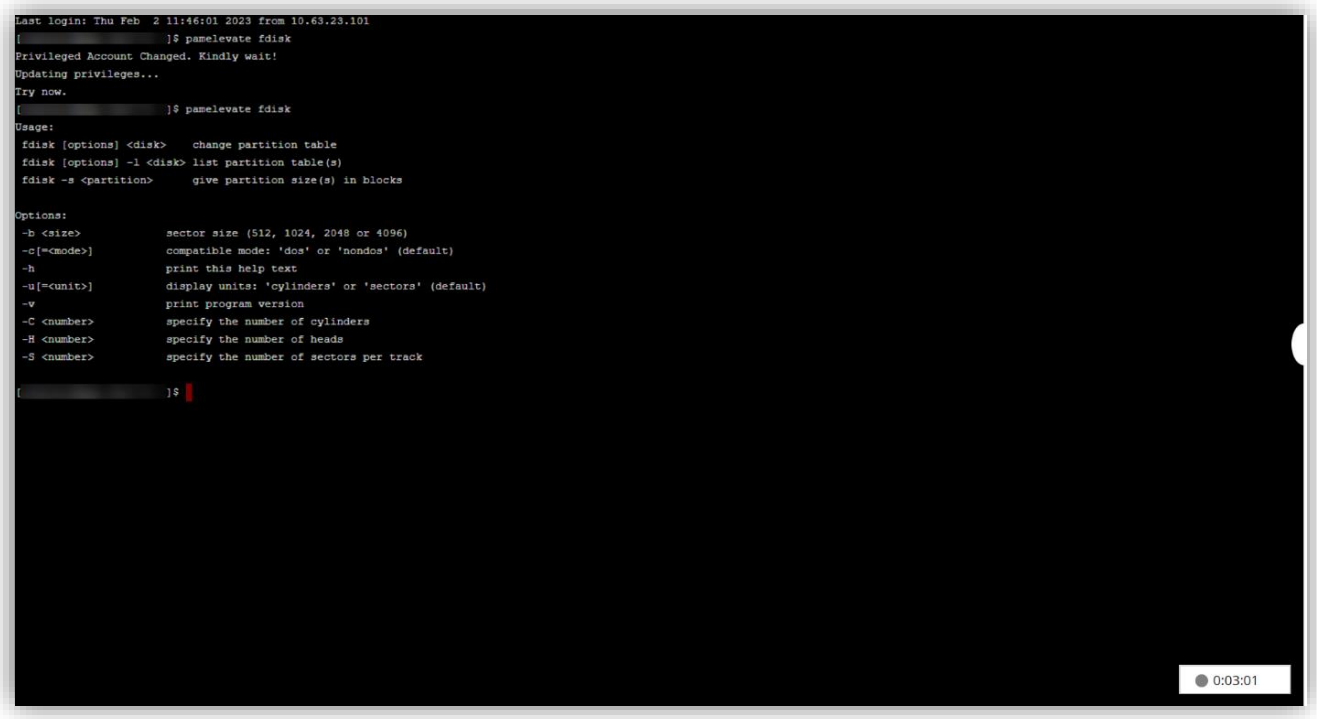


Note:

1. Under the Elevate & Execute list, the commands configured with Self-Service Privilege Elevation alone will have an enabled execute icon.
2. The Self-Service Privilege Elevation feature cannot be utilized through external SSH clients when an account/resource is configured with SSH command control.

ii. From an Account Configured without SSH Command Control

1. Launch a remote session to the account configured with Self-Service Privilege Elevation from PAM360 or from any other external SSH client such as Remote Connect, PuTTY, etc.
2. Use the prefix "pamelevate" before commands that require privileged administrative action (e.g., pamelevate fdisk). The associated privileged commands will execute as long as the Self-Service Privilege Elevation is configured for the account.



Note:

If the command is not from the part of the configured command group (or) the "Run as" account user does not have the required privilege to execute the command, then you will not have permission for the privilege elevation to execute the command.

2.5 Audits and Reports of Self-Service Privilege Elevation

Navigate to **Audit >> Resource Audit** to check the trail of audits recorded during the process of Self-Service Privilege Elevation. From here, you will get the different types of audit information that include:

- Agent installation, modification of agent modules, etc.,
- Commands and command groups audits
- Configuration of Self-Service Privilege Elevation to an account or resources
- Unauthorized execution of commands

Navigate to **Reports >> Query Reports**. From here, you can generate query reports that include information such as:

- Command groups association at different levels,
- List of unauthorized command executions using the Self-Service Privilege Elevation (pamelevate).

Refer to this section to know more about query reports and management.

2.6 Self-Service Privilege Elevation Precedence in Real-Time

Case 1:

Account Configured with SSH Command Control and Self-Service Privilege Elevation

Consider the command **"fdisk"** configured in a command group of an account for which the user requires privilege elevation.

✓ denotes - enabled Self-Service Privilege Elevation or SSH command control
✗ denotes - disabled Self-Service Privilege Elevation or SSH command control

Self-Service Privilege Elevation	SSH Command Control	Elevation Result in PAM360 Session
✓ Command "fdisk" configured	✓ Command "fdisk" not configured	**No Elevation** The command "fdisk" will not be listed in the allowed command list for execution.
✓ Command "fdisk" configured	✓ Command "fdisk" configured	**Allowed Elevation** The command "fdisk" will be listed in the allowed command list with the option **Elevate & Execute**.
✓ Command "fdisk" not configured	✓ Command "fdisk" configured	**No Elevation** The command "fdisk" will be listed in the allowed command list without the Elevate & Execute option. Existing user privileges can be used to execute the command.

✓ Command "fdisk" configured	✗	**Allowed Elevation** Users can enter the command "fdisk" with the prefix "pamelevate" to execute it with the privileged elevation.
✗	✓ Command "fdisk" configured	**No Elevation** The command "fdisk" will be listed in the allowed command list without the Elevate & Execute option. Existing user privileges can be used to execute the command.

Case 2:

Switching Self-Service Privilege Elevation between Configured User Accounts from the SSH Console

Consider the following users account with different configuration for the upcoming scenarios:

1. kate - Account listed in PAM360 and configured with Self-Service Privilege Elevation
2. marko - Account not listed in PAM360
3. lindsey - Account listed in PAM360 and not configured with Self-Service Privilege Elevation
4. paul - Account listed in PAM360 and configured with Self-Service Privilege Elevation with different sets of privileged commands.

Scenario 1:

If a user logs in to the account **kate** using PAM360 remote session and then changes internally to **marko**, which is not a PAM360 user account - then the current user account session does not allow Self-Service Privilege Elevation for the privileged commands configured in **kate**.

Scenario 2:

If a user logs in to the account **kate** using PAM360 remote session and then changes internally to **lindsey**, which is not configured with Self-Service Privilege Elevation - then the current user account session does not allow Self-Service Privilege Elevation for the privileged commands configured in **kate**.

Scenario 3:

If a user logs in to the account **kate** using PAM360 remote session and then changes internally to **paul**, which is configured with Self-Service Privilege Elevation for different sets of privileged commands - then the current user account session allows Self-Service Privilege Elevation for the privileged commands configured only in **paul**.

Application Control via PAM360

PAM360's Application Control, powered by ManageEngine's Application Control Plus, empowers administrators with advanced privilege elevation and delegation management. This functionality allows for effective oversight of applications on organizational endpoints. Using a set of crafted rules, administrators can effortlessly identify and manage applications across PAM360 resources and tailor allowlists and blocklists to control application usage. Additionally, at break-glass scenarios, administrators can temporarily authorize applications on the blocklist. Overall, this operation streamlines the process of allocating application access to users, enhancing security and efficiency within the PAM360 environment across all resources.

Notes:
i. If you are already leveraging the Application Control module through Application Control Plus/Endpoint Central, proceed with the help documentation to configure Application Control in PAM360 seamlessly.
ii. If you are new to Application Control, download Application Control Plus now to access free application management for up to 25 resources.

1. Prerequisites

1. To control applications at endpoints via PAM360, you should have the Application Control Plus application powered by ManageEngine.

   Note: Please note that if you are already using ManageEngine's Endpoint Central, you can take advantage of it by ensuring that you have the Application Control Plus module enabled.

2. The possessed version of Application Control Plus should not be less than 11.3.2404.1.
3. The user responsible for configuration should hold administrative privileges in both the Application Control Plus application and PAM360.
4. In order to leverage Application Control within PAM360 effectively, it is crucial that the user currently logged into PAM360 exists within Application Control Plus with an

identical username. If the user is authenticated via Active Directory, their corresponding account in Application Control Plus should align with the same domain name. This synchronization ensures seamless integration and functionality across both platforms.

5. The HTTPS port of Application Control Plus is required to configure Application Control in PAM360.

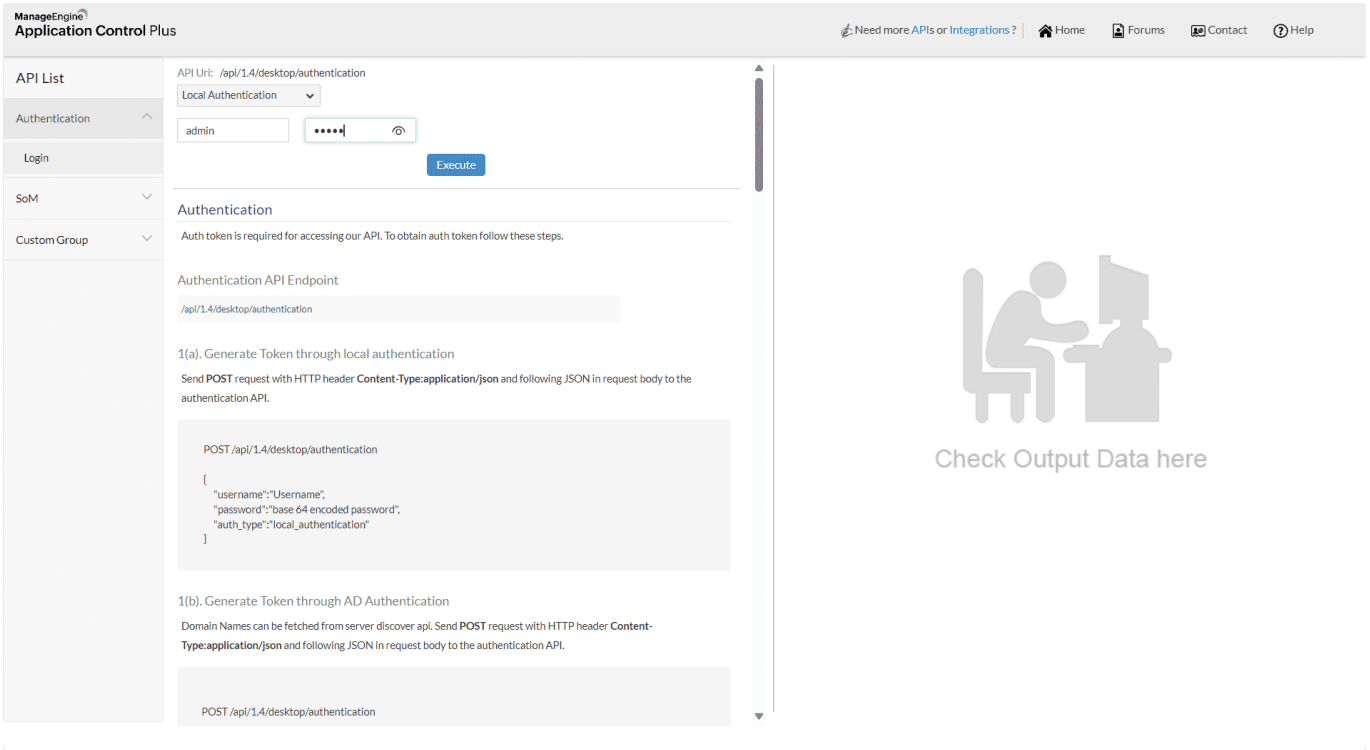
2. Role - Manage Application Control

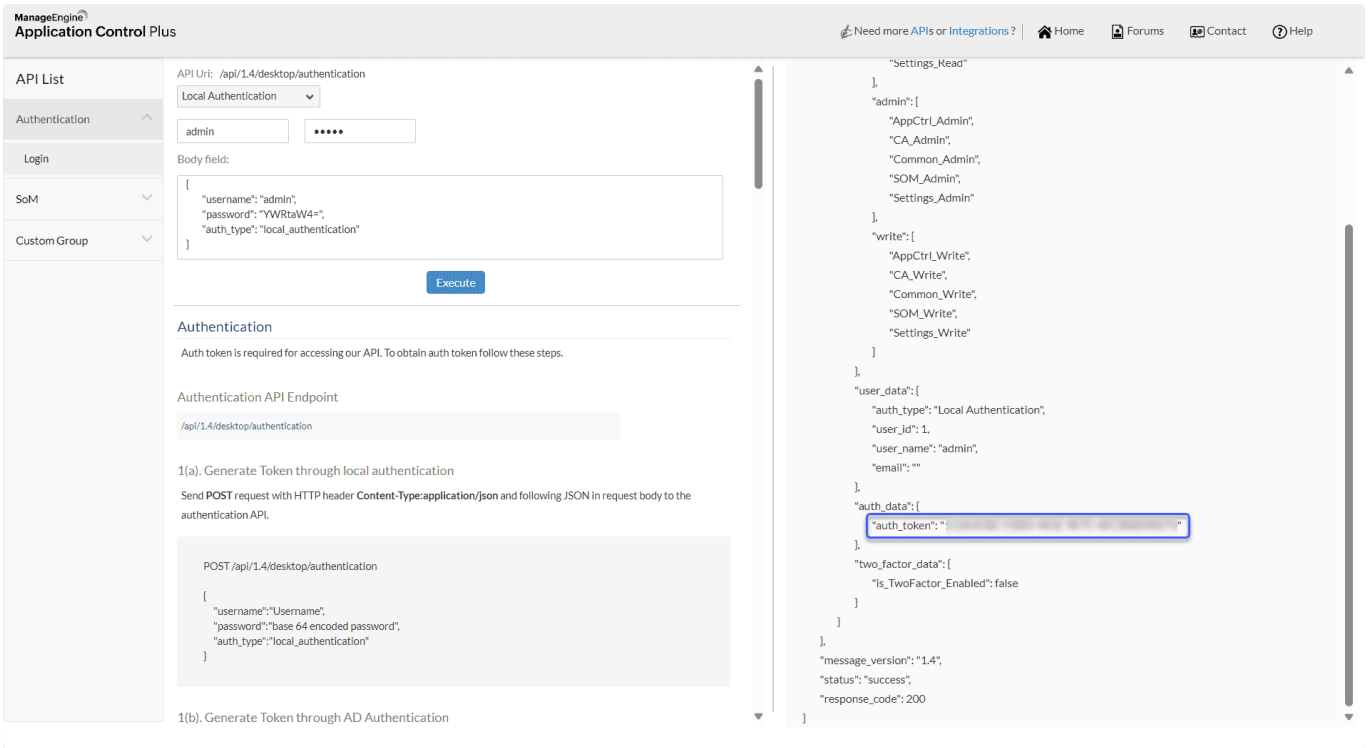
By default, users assigned the **Privileged Administrator** and **Administrator** roles can configure and manage Application Control in PAM360. Alternatively, you can grant these same responsibilities to users by creating a custom role with the **Manage Application Control** privilege enabled. Users assigned this custom role will be able to configure and manage Application Control via PAM360.

3. Generating Authentication Token

To enable the Application Control functionality, it is necessary to generate an authentication token from Application Control Plus. To generate the authentication token, perform the steps that follow:

1. Log in to **Application Control Plus**.
2. Go to **Admin**, then **Integration**, and select **API Explorer**.
3. On the page that opens, under **API List**, choose **Authentication**, then **Login**.
1. Opt for the required authentication and input your Application Control Plus' **User Name**, **Password**, and/or **Domain**.
4. Click **Execute** to generate the required authentication token for establishing communication with PAM360.
5. Copy the authentication token for configuring Application Control in PAM360.



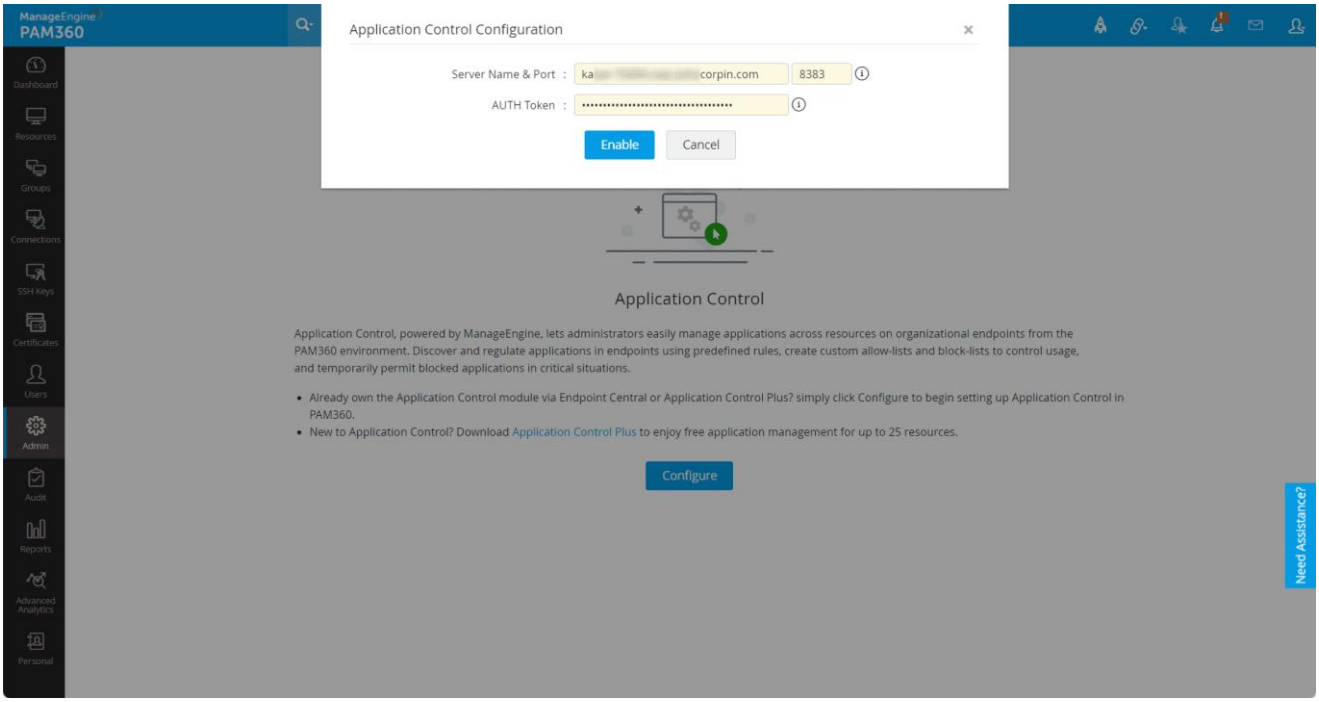


4. Configuring Application Control in PAM360

To ensure the expected functionality and perform endpoint privilege management capabilities via the PAM360 environment, configuring Application Control in PAM360 is necessary. To do so:

1. Login to the PAM360 user account.

2. Go to **Admin**, then **Privilege Elevation**, and select **Application Control**. Click **Configure**.
3. In the dialogue box that opens,
   a. Input the server name where the Application Control Plus is installed (e.g., **in-qaauto-92dt**).
   b. Enter the HTTPS port number configured for Application Control Plus (default is **8383**).
4. Click **Enable** to establish communication and complete the setup process.

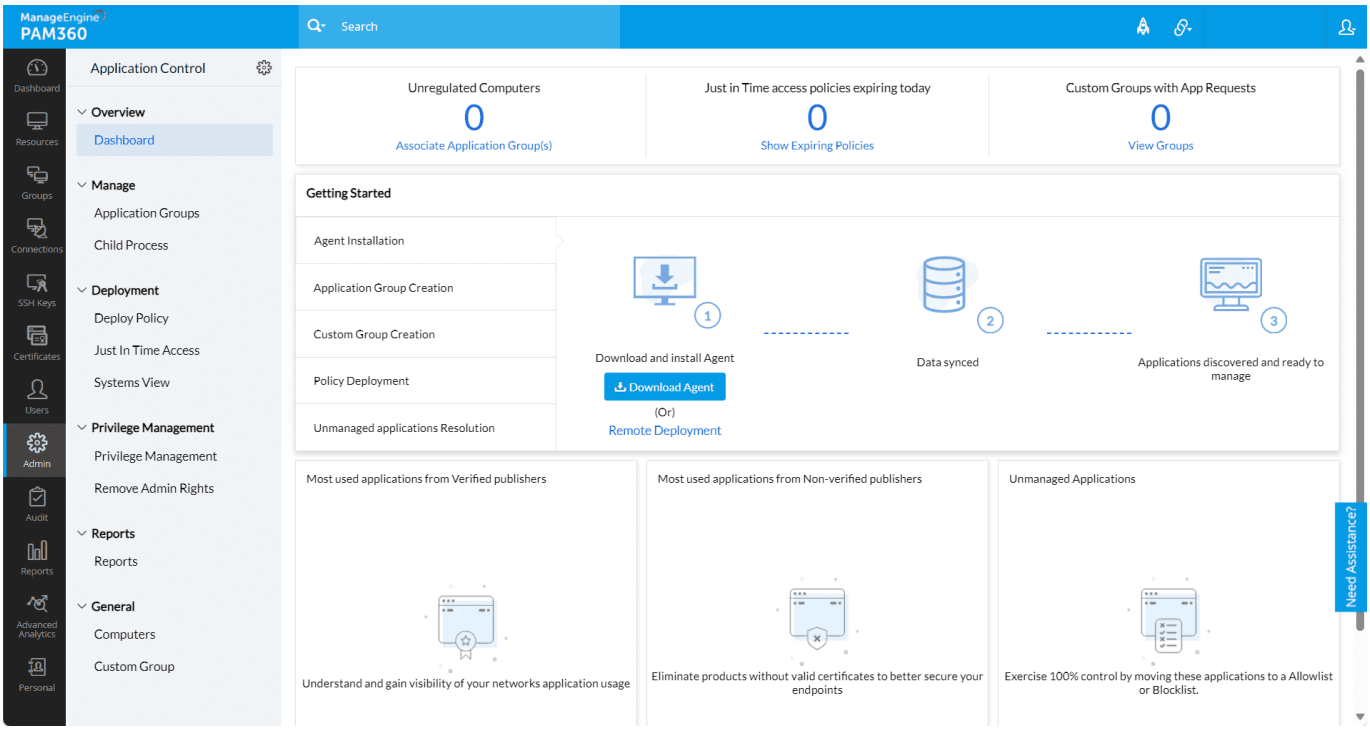


> **Note:** Once configured, you can also edit the above details using the Edit Configuration button present at the top pane of the left Application Control column.

5. Application Control in PAM360

Once communication is established between PAM360 and Application Control Plus, the Application Control window will load for further application management. Here, you can create allowlists and blocklists for endpoints across PAM360, and you can perform the following further application management actions directly from the PAM360 interface:

i. Manage Windows systems
ii. Application Allowlist/Blocklist
iii. Custom Group Creation
iv. Endpoint Privilege Management



6. Configuration and Management Failure Scenarios

Encountering difficulties while configuring or managing Application Control in PAM360 can result from various factors. It is essential to address these issues to ensure effective and efficient utilization of the Application Control feature.

a. Mismatched Privileged Roles

If a user attempts to manage Application Control via PAM360 but lacks a corresponding privileged role in Application Control Plus, issues may arise. Users should possess similar privileged roles in both platforms to access and manage Application Control seamlessly.

b. Module Absence in Endpoint Central

In cases where the Application Control module is not enabled in Endpoint Central, attempts to configure or manage Application Control will fail. It is crucial to ensure that the Application Control module is activated within Endpoint Central for proper functionality.

c. Unauthorized Access and Privileges

Configuration or management of Application Control without the appropriate privileges can lead to unauthorized access attempts. Users should be granted the necessary privileges to avoid encountering issues while configuring or managing Application Control within PAM360.

d. Authentication Token Update Requirement

Changing the login password of the responsible user in Application Control Plus disrupts the functionality of the Application Control module in PAM360. This is because the previously generated authentication token becomes invalid after the password change. To ensure smooth operation, it is essential to update the Application Control configuration with the newly generated authentication token.

e. Username Discrepancy

If a user attempting to access Application Control does not have the same username as in PAM360, issues may arise. Consistency in usernames across platforms is necessary to facilitate seamless access and utilization of Application Control functionalities.
Addressing these potential failure scenarios comprehensively ensures the effective and efficient deployment and usage of Application Control within PAM360, enhancing overall security management capabilities.

Managing Resource Groups

Resources can be grouped together in PAM360 for easier management. The grouping can be done either by specifying a set of criteria or by specifying individual resources. In case of a dynamic group, i.e. criteria-based, whenever a newly added resource matches the criteria of an existing group, it automatically becomes a part of that group.

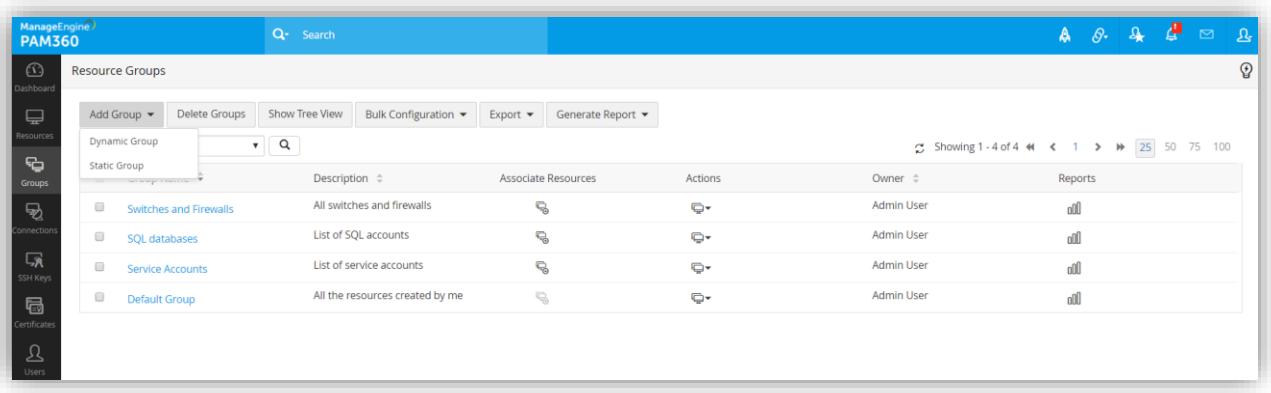
Resource groups created by the administrator users can be shared with other users or user groups. Whenever resources get added or deleted from a group, it affects the password access shared through the group. That is, users with whom a particular resource group has been shared can see passwords of only the resources that are part of the group at that point of time.

This help topic discusses the following topics:

1. Adding Resource Group
   1.1 Adding Dynamic Group
   1.2 Adding Static Group
2. Checking Password Consistency
   2.1 Finding Out of Sync Passwords
   2.2 Periodic Integrity Check
3. Viewing Resource Group
4. Deleting Resource Group
5. Generating Reports

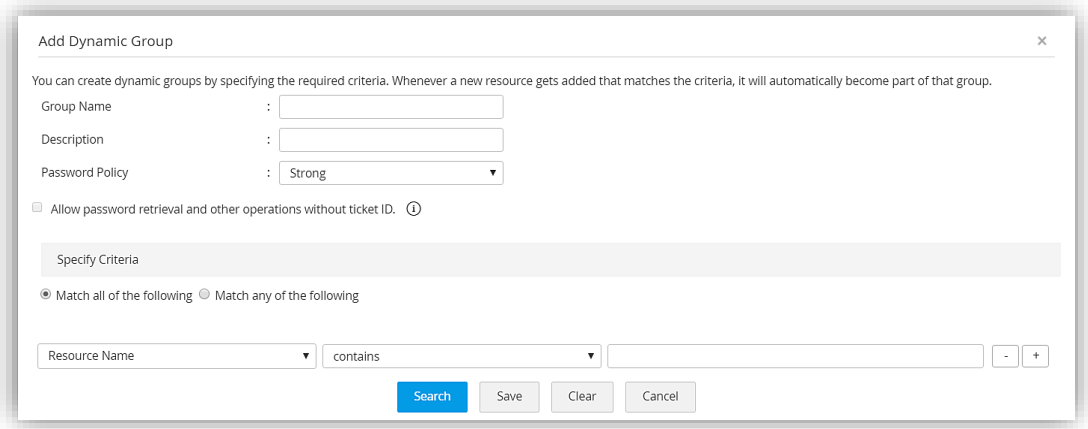
1. Adding Resource Group

1. Navigate to **Groups >> Add Group.**
2. Upon clicking, it lists two options:
   i. Dynamic group
   ii. Static group
3. Choose your desired option for creating a resource group.



1.1 Adding Dynamic Group

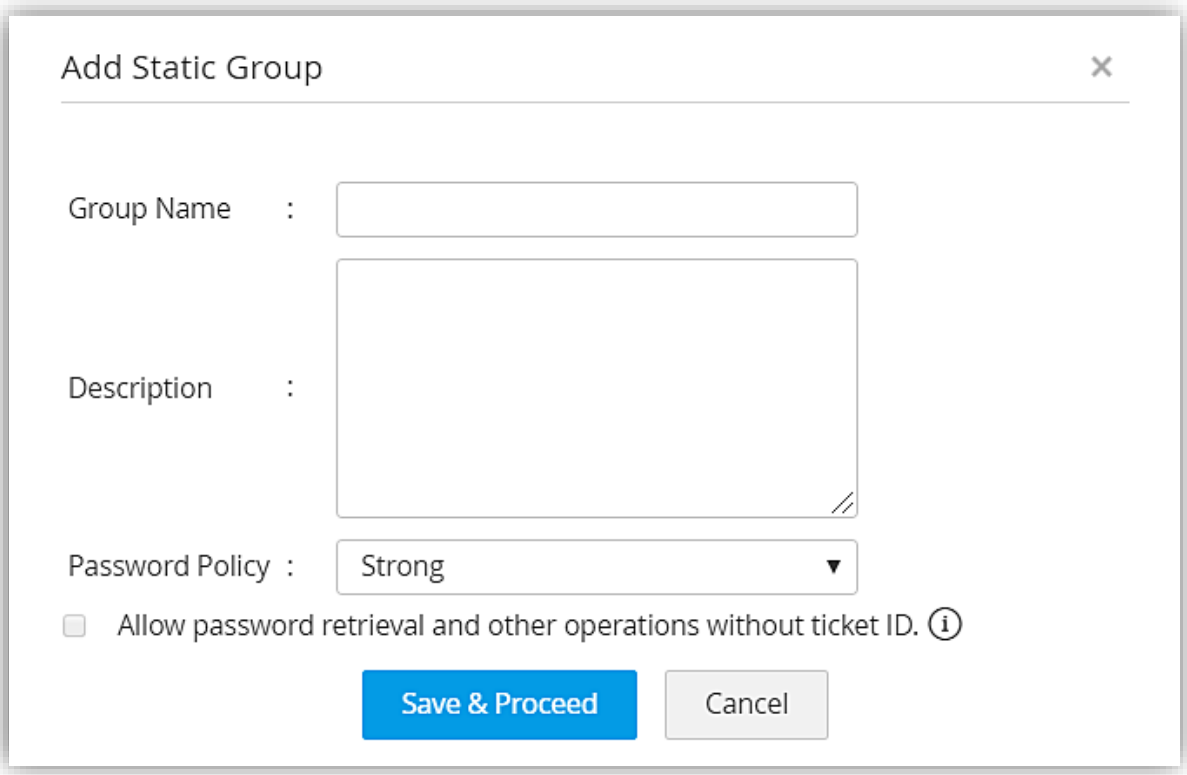
1. Select **Dynamic Group.**
2. In the pop-up form that opens,
    i. Enter the **Group Name**.
    ii. Provide a **Description** for the group for future reference.
    iii. Select a **Password Policy** for the group
    iv. **Nested Groups:** If you want to make the resource group being added as the sub-group of an already existing resource group, select the required group from the drop-down against the field **Sub Group of**. The selected group will become the parent group for the resource group being added.
    v. Specify the exact criteria based on which you want to create the group. Here, you have many options to choose from:
        a. You can search for resources based on resource name, resource type, resource description and user account



        b. Also, you can filter the search in fine-grained manner based on the criteria such as **contains**, **does not contain**, **equals, not equal**, **starts with** and **ends with.**
    vi. Once you specify the criteria, click **Search** if you want to view the list of resources that will become part of this group.
3. Click **Add** to add those resources to your resource group.

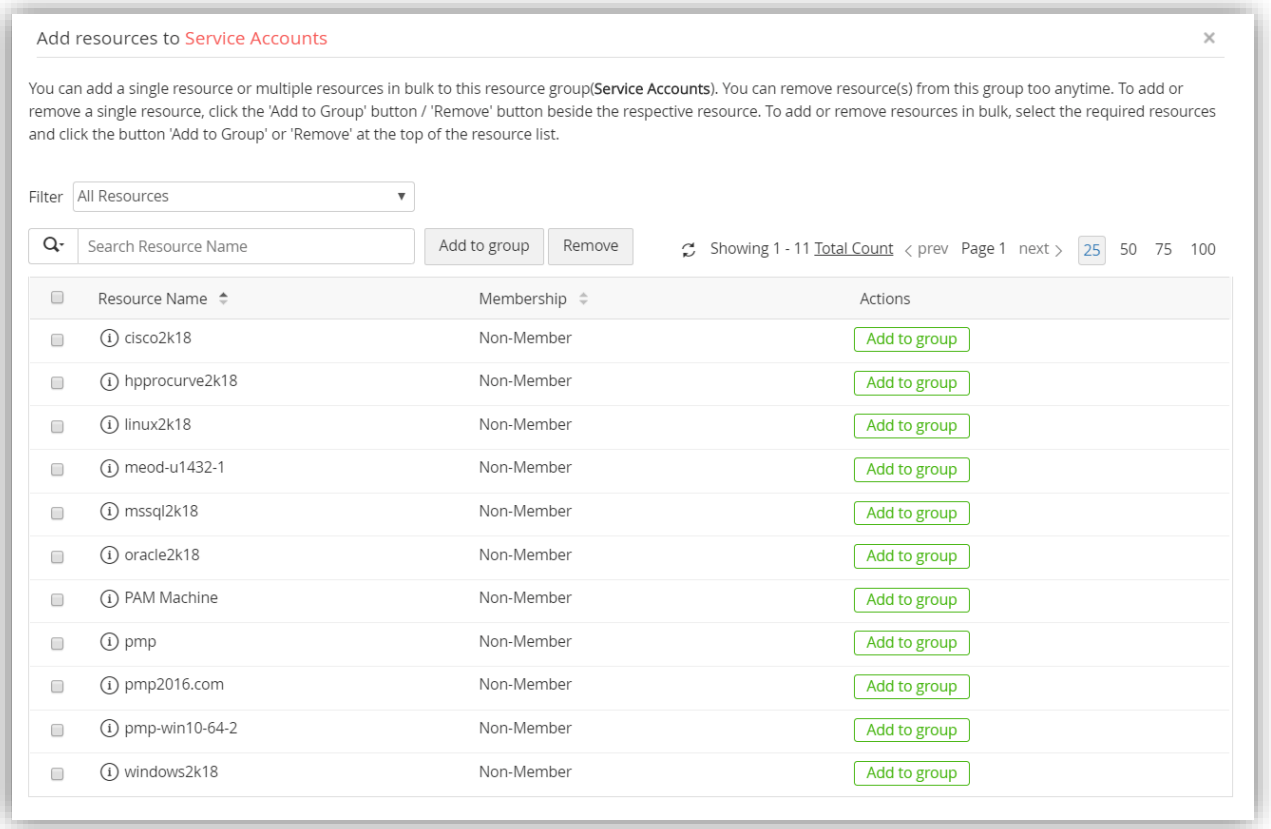
1.2 Adding Static Group

1. Select **Static Group**.
2. In the dialog box that opens,
    i. Enter the name for the group against the text field **Group Name**.



ii. Provide a **Description** for the group. It will be helpful for future reference.
iii. Select a **Password Policy** for the group. If you select **Strong** (say), it would be applicable to all the members of this resource group.
iv. Nested Groups: If you want to make the new resource group a sub-group, i.e. add it under an already existing resource group, select the required group from the drop-down against the field **Sub Group of**. The group selected by you will become the parent group for the resource group being added.
v. Click **Save & Proceed**.

3. In the pop-up form that opens, locate desired resources and click **Add to group** against them.
4. Click **Ok**.

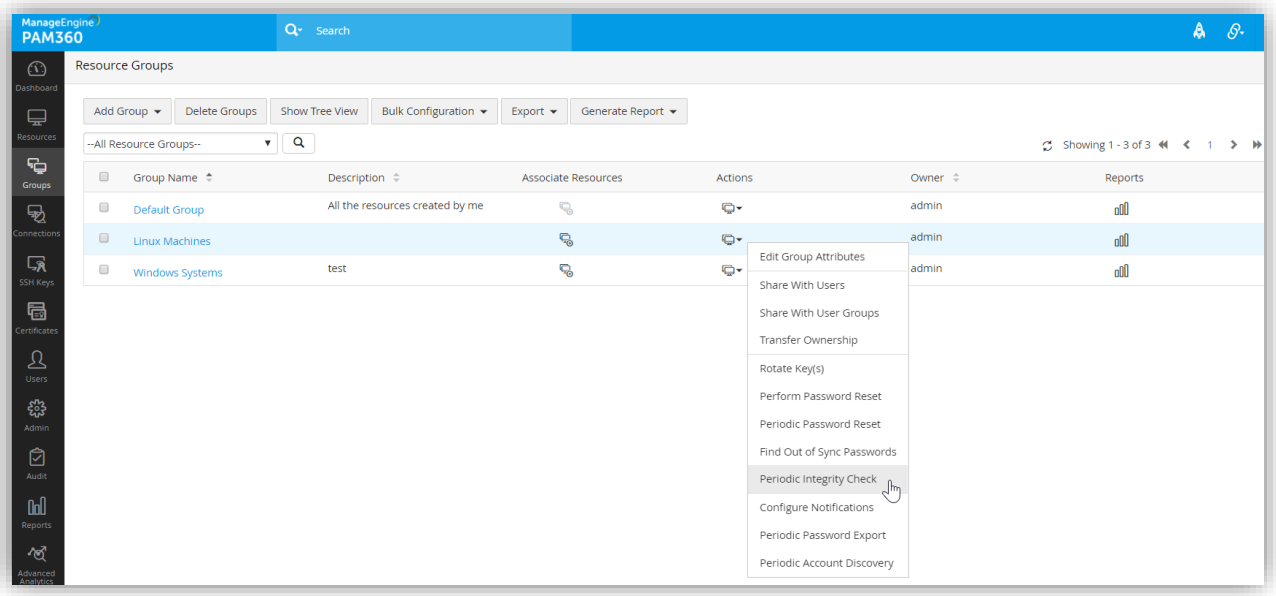


2. Checking Password Consistency

Check if all passwords in a resource group available in PAM360 are in sync with the passwords in the target devices. There are two ways of checking this:

Click the **Actions** drop-down beside the required **Group Name** and you will find the following two options:

i. Find Out of Sync Passwords
ii. Periodic Integrity Check



2.1 Finding Out of Sync Passwords

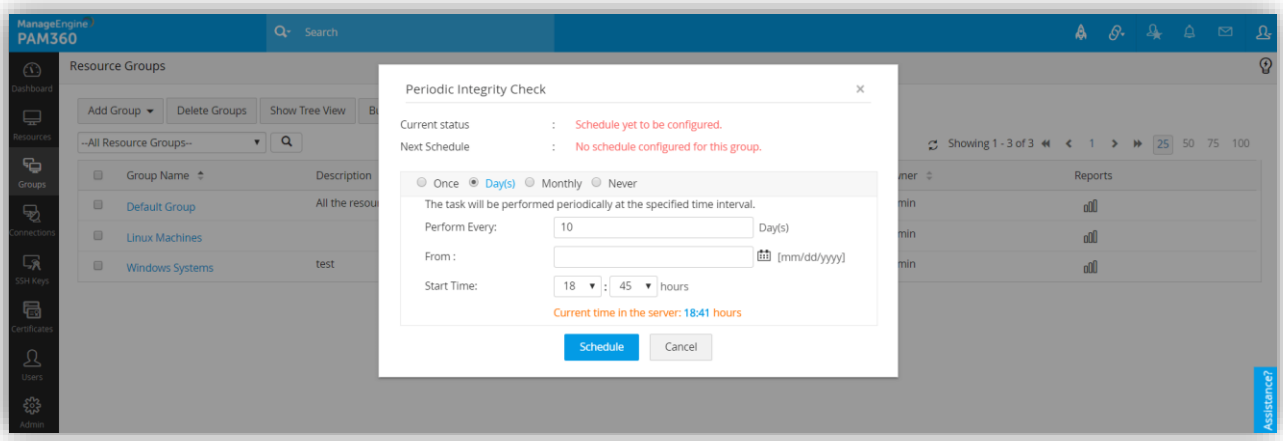
Click this option to find instantly if the passwords stored in PAM360 and the passwords in the target devices are in sync. This is a one-time operation. Click the **Start Now** button to schedule the check.

2.2 Periodic Integrity Check

In the **Periodic Integrity Check** window, choose the frequency with which the check must be performed:

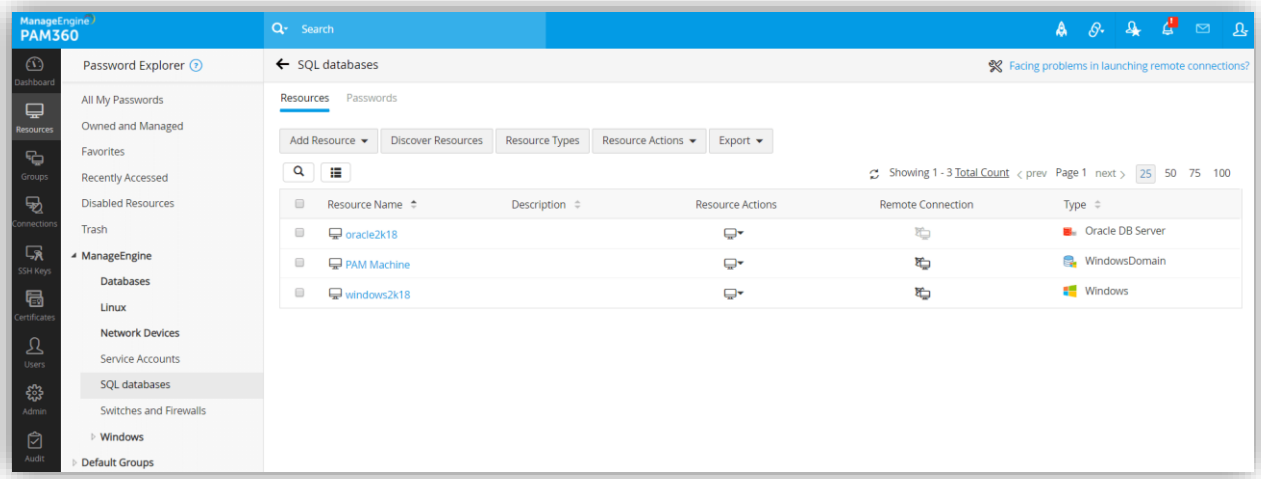
i. **Once**: Choose this option to perform to integrity check only once without creating a schedule
ii. **Day(s)/Monthly**: Specify a number of days/months as the time interval between two scheduled integrity checks
iii. Choose a date from which the schedule should commence and a **Start Time** at which every periodic check will begin.
iv. Choose **Never** to clear any previously saved schedule.

Once your preferences are set, click **Schedule** to create a schedule for the periodic integrity check.

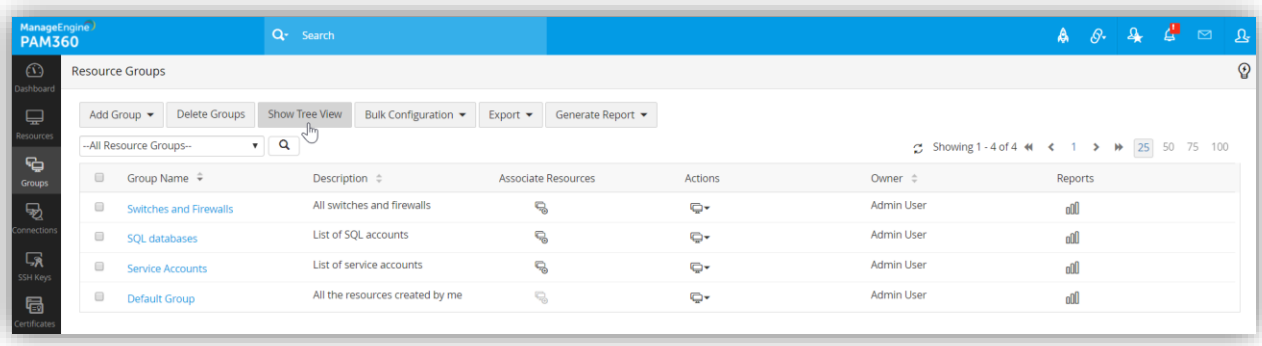


3. Viewing Resource Group

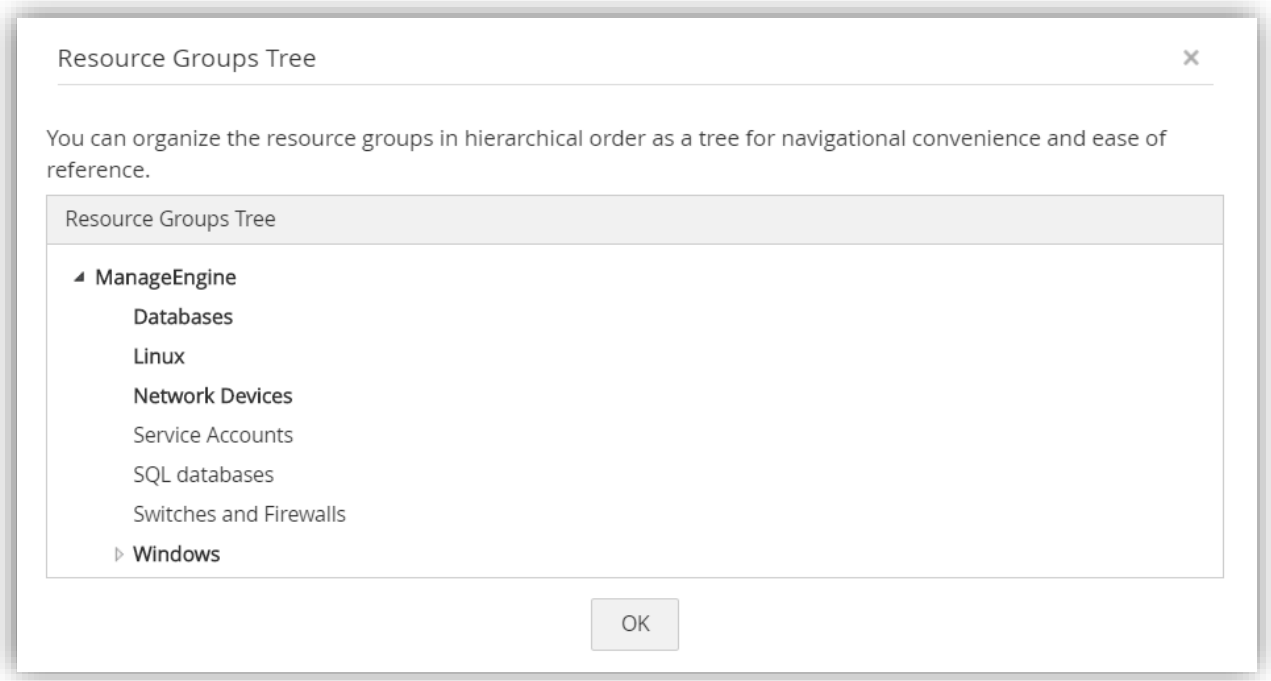
1. Click the **Resources** tab.
2. Here, you will be able to view the resources and their passwords belonging to a particular resource group by clicking on the group's name available in the left pane.
3. These resource groups are displayed in a tree view in a hierarchical structure.



4. To view only the hierarchical order, Navigate to **Groups >> Show Tree View.**



5. A pop-up appears on the screen displaying the Resource Group Trees in a hierarchical order.
6. To Edit the name of the root node of the nested resource group tree, Click **Edit** button present near the filed **Root Node Name**. After making necessary changes, click **Update**.



4. Deleting Resource Group

In the **Groups** tab, select the required groups you want to delete and hit the **Delete Groups** button on top of the list view.

5. Generating Reports

1. Navigate to **Groups >> Generate Report.**
2. Click **Password Inventory / Policy Compliance / Password Expiry / Password out of sync.** to generate the necessary report(s).
3. To know more about these reports, click here.

Nested Resource Groups

PAM360 provides an option to maintain resource groups in hierarchical structure, i.e. tree view. For example, assume that your organization contains some departments/sections in the following hierarchy. You can group the resources belonging to the respective sections and create sub-groups as required.

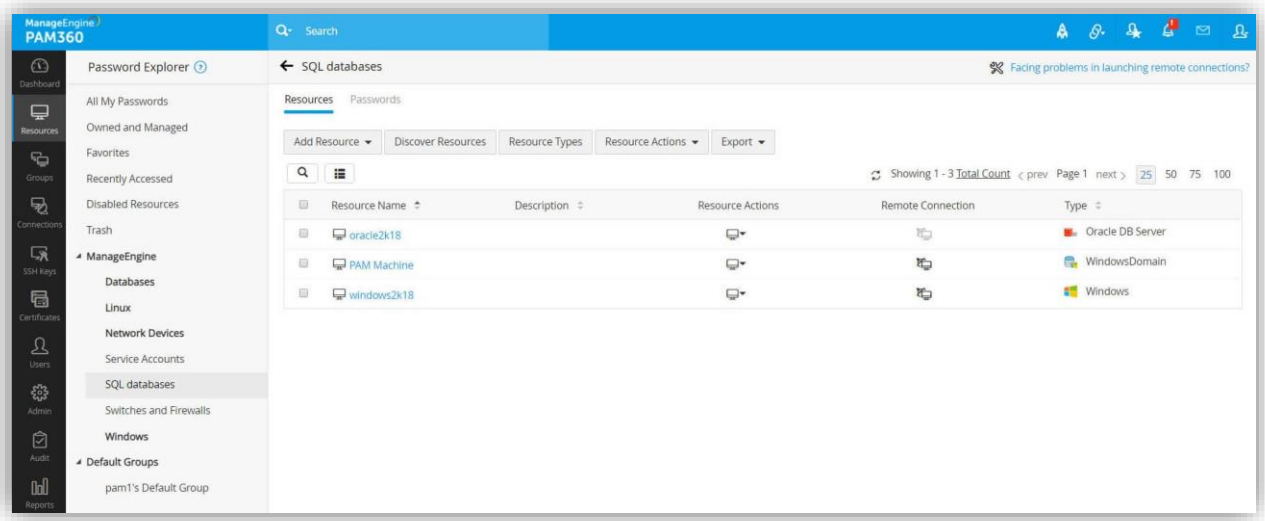
This document discusses about the following topics:

1. View Nested Resource Groups
2. Components of Nested Resource Group
3. Constructing Nested Resource Groups
4. Guidelines on Nested Resource Group Construction for Admins and Password Admins

1. View Nested Resource Group

To view the hierarchical order of the resource groups as well the resources that are part of the respective group,

1. Navigate to **Resources** tab.
2. On the left hand side, the resource groups are displayed in tree view. Select the required resource group.
3. All the resources belonging to that group will also be displayed.



Important Notes:

1. Every administrator and password administrator can create their own tree with the resource groups they own and manage.
2. When you create a nested resource group, by default, the name of the root node of the tree will have your login name. For example, if you are logging into PAM360 as "admin", the name of the root node will be **Admin's Group**. If you want to have a different name for the root node, you can edit it.
3. Nested Resource Groups are purely for navigational convenience only. You can just view the passwords belonging to the respective resource groups directly. The sub-groups created under an already existing group will not inherit sharing and other configurations like scheduled password reset, password action notification and other events from their parents.

2. Components of Nested Resource Group

Nested Group Tree, depicted on the left hand side of **Resources** tab under the title **Password Explorer**, has the following components:

1. All My Passwords
2. Owned and Managed
3. Favorites
4. Recently Accessed
5. Nested Resource Group Tree

2.1 All My Passwords

All the passwords that are owned by you and the ones shared with you will be displayed. If you own resources or some resources had been shared with you, those resources will be displayed.

To view this,

- Navigate to **Resources >> Password Explorer >> All My Passwords.**

Important Note: The resources and passwords that are individually shared and not through groups, which are also not part of any of the shared resource groups, will not be found under the tree. They will be listed only under **All My Passwords**.

2.2 Owned and Managed

All the passwords that are owned by you and the ones shared with you with 'Full Access' permission will be displayed. Those passwords shared to you without Full access (view passwords or modify passwords) permission will not be displayed.

To view this,

- Navigate to **Resources >> Password Explorer >> Owned and Managed**.

2.3 Favorites

PAM360 provides the option to retrieve your favorite passwords with ease. You need not have to search for the resources to locate your favorite passwords. Right near the name of all the accounts, you will find a greyed out 'star' icon. When you click the star, it will be highlighted and the respective password will be marked as your favorite password. At any point of time, you may remove any password from the 'favorites' list by unmarking the star icon.

To view this,

- Navigate to **Resources >> Password Explorer >> Favorites**.

> **Important Note:** Assume that you have marked a password that was shared by an admin with you as favorite. Later, the admin revokes the share permission for that particular password. Now, when you click the 'My Favorite Passwords' link, you will see the resource still listed there. However, if you try to retrieve the password, you will not be permitted to view the password. Also, the resource would be removed from the 'Favorites'. By default, you will land up in the **"Favorites"** section only.

2.4 Recently Accessed

The passwords that were accessed by you most recently will be displayed under this section to facilitate easy access to a recently used password. The recently accessed passwords will be shown on top of other available passwords.

To view this,

- Navigate to **Resources >>Password Explorer >> Recently Accessed**.

2.5 Nested Resource Group Tree

This tree consists of the following components:

Resource group tree created by you. In this tree, all the resource groups and sub-groups owned by you will be depicted. As mentioned above, by default, the root node of your tree will be named as - 's Group. If you want, you can edit the name of the root node to make it more meaningful or to make it reflect your organizational structure. For example, if you are a

Database Administrator, you can name the root node as "Database Passwords". Click here to know how to edit/rename the root node. You can click on any desired group or sub-group to view the resources and passwords therein.

Resource group trees shared with you by other admins. Only the groups that the other admins have shared with you will appear in the tree under his/her root node. For example, if an admin has created a tree with 10 groups but had shared only 3 groups with you, you will only see those 3 groups under his/her tree.

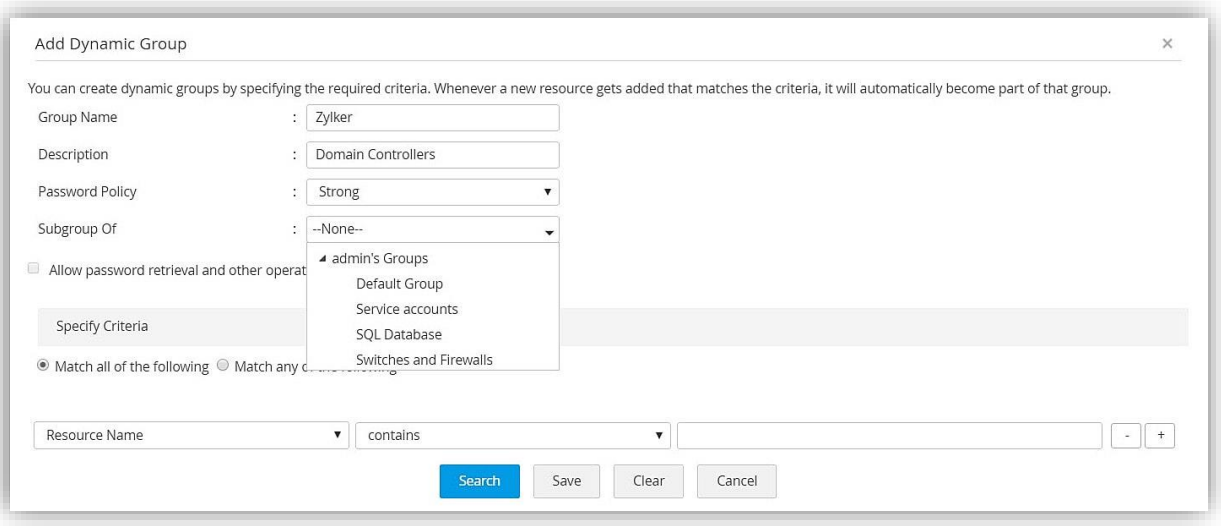
Notes:

- The resources and passwords that are individually shared and not through groups, which are also not part of any of the shared resource groups, will not be found under the tree. They will be listed under **All My Passwords** only.
- Super administrators will see the entire tree of all other administrators and password administrators under their 'Password Explorer' in the 'Resources' tab.
- Password users will not be able to create nested resource groups, but they can see the groups that have been shared with them in tree form.

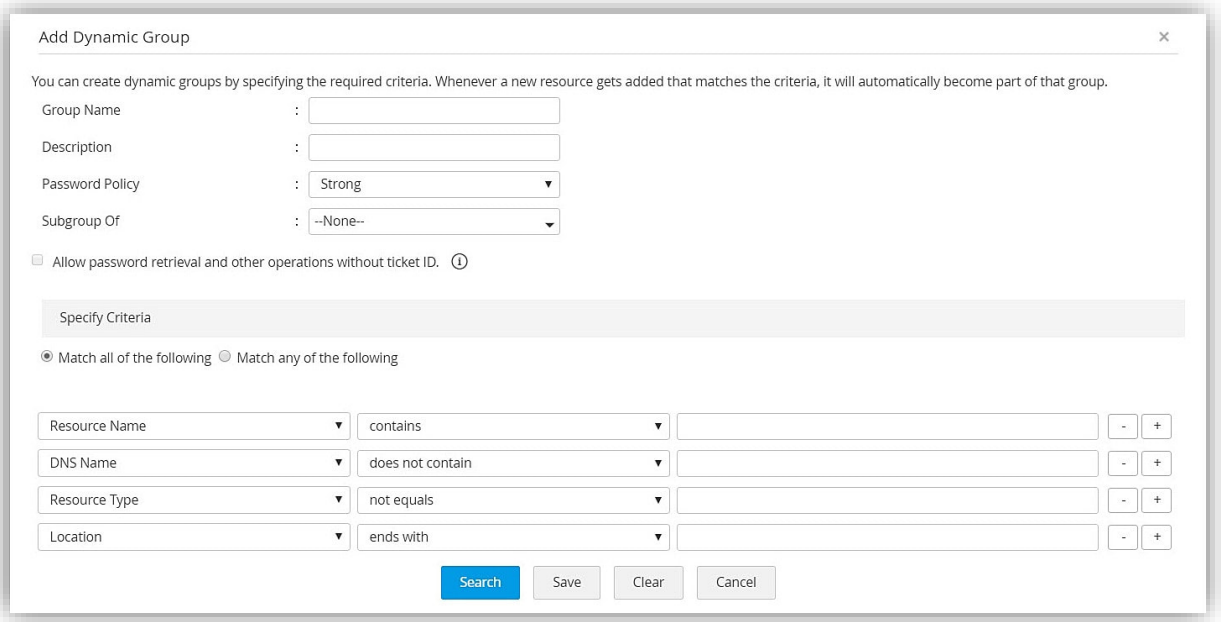
3. Constructing Nested Resource Groups

3.1 Add Dynamic Group

1. Navigate to the **Groups** tab.
2. Click **Add Group** and select **Dynamic Group**.
3. In the pop-up form that opens,
   i. Enter the **Group Name.**
   ii. Provide a **Description** for the group. It will be helpful for future reference.
   iii. Select a **Password Policy** for the group.
   iv. **Nested Groups:** If you want to make the resource group being added as the sub-group of an already existing resource group, select the required group from the drop-down against the field **Sub Group of**. The group selected by you will become the parent group for the resource group being added.
   v. Specify the exact criteria based on which you want to create the group. Here, you have many options to choose from:
   vi. You can search for resources based on resource name, resource type, resource description and user accounts.



vii. Also, you can filter the search in fine-grained manner based on the criteria such as **contains, does not contain, equals, not equal, starts with and ends with.**



viii. Once you specify the criteria, click **Search** if you want to view the list of resources that will become part of this group.

ix. Click **Add** to add your resource group.

4. A dynamic group has been created successfully.

3.2 Add Static Group

1. Navigate to **Groups** tab.
2. Click **Add Group** and select **Static Group.**
3. In the pop-up form that appears,

i. Enter the **Group Name**.
ii. Provide a **Description** for the group. It will be helpful for future reference.
iii. Select a **Password Policy** for the group. If you select 'Strong' (say), it would be applicable to all the members of this resource group.
iv. **Nested Groups:** If you want to make the new resource group a sub-group, i.e. add it under an already existing resource group, select the required group from the drop-down against the field **Sub Group of**. The group selected by you will become the parent group for the resource group being added.
v. Click **Save & Proceed**.
vi. In the pop-up form that opens, locate desired resources and click **Add to group** against them.
vii. Click **Ok.**

4. A static group has been created successfully.

4. Guidelines on Nested Resource Group Construction for Admins and Password Admins

Though the nested resource groups are mainly intended for navigational convenience, by properly creating the tree, you can leverage a lot of benefits, mainly ease of use.

Assume that you are a Database Administrator responsible for managing the passwords of various databases. In this case, you can construct the resource group tree as explained below:

- By default, the root node of your resource group tree will have your login name.
- Rename it as **Database Passwords**.
- Create a resource group for each database that you own - say, My SQL Passwords, MS SQL Passwords, Oracle Passwords, Sybase Passwords etc.
- All these resource groups could be made as the sub-groups of the root node - Database Passwords.

Once you do this, you will see your resource group tree in the **"Resources"** tab of PAM360 web-interface:

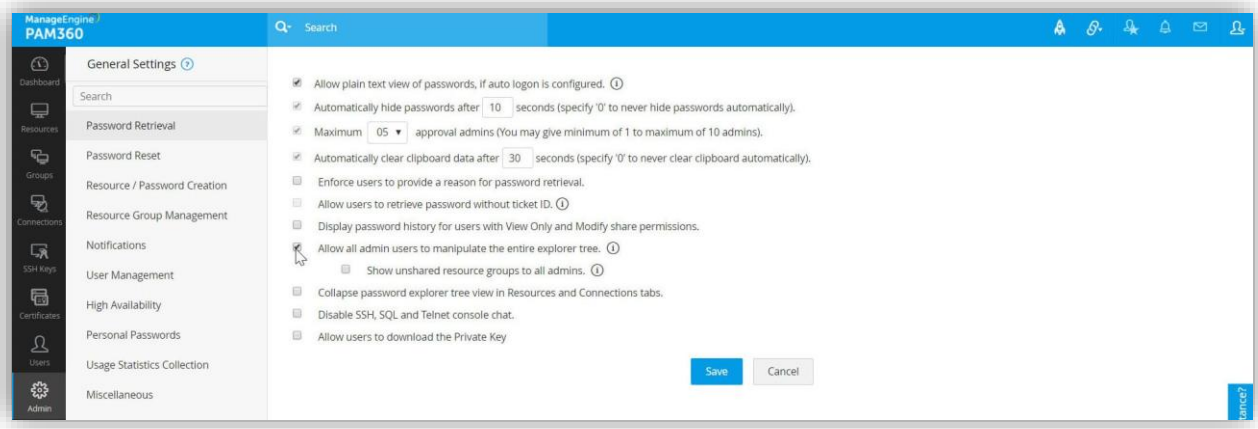
4.1 Allowing administrators to manipulate the nested resource group explorer tree

PAM360 offers provision to allow admin users to manipulate the entire explorer tree structure as they wish. Through a configuration setting in "General Settings", PAM360 administrator can enable this option. Once this is enabled, PAM360 creates an organization wide, global explorer tree structure containing the names of resource groups under a root node. Any administrator in PAM360 would be able to create/edit the explorer tree structure of resource groups. The tree structure will be accessible to all admins, password admins and end users. Admins and password admins can add their resource groups anywhere into the global tree and the whole structure will be available for view to all the end users.

This feature allows depicting resource groups of your organization in the form of a global tree for easy access, identification and navigation. Users can view the resource groups in the same structure as that of the internal grouping structure in your organization. Externally the tree structure depiction will be the same for all the members of the organization (that means all the users will see the entire structure). But, the users will be allowed to view only the resources that are owned by them and the ones shared with them. The resource groups that are not related to them will be shown as empty sub-nodes (without any resources inside) in the explorer tree.

4.1.1 How to enable this option?

1. Navigate to **Admin >> Settings >> General Settings**.
2. Select the option **Password Retrieval.**
3. Select the check box **Allow all admin users to manipulate the entire explorer tree**.
4. Click **Save**.



4.1.2 How to manipulate the tree structure?

1. Navigate to **Resources** or **Connections** tab
2. You will see the resource groups of your organization as a tree structure under a root node.
3. Just right-click the name of any node or sub-node to edit, modify or delete. You can manipulate the structure in any manner you want. The **delete** operation here just deletes the particular structure in the tree. It does not delete the resource.

Export Resource Groups

PAM360 provides three options to export all the passwords that are part of any specific resource group for secure offline access.

- The basic option is to export the resources in plain text in a spreadsheet.
- The more secure option is to export them to an encrypted HTML file.
- There is also an option to create a scheduled task to export the resources belonging to any resource group as an encrypted HTML file periodically during specified time intervals.

In all the above options, you can export the resources, accounts and passwords that are part of specific resource groups for offline access.

This section will walk you through the following topics:

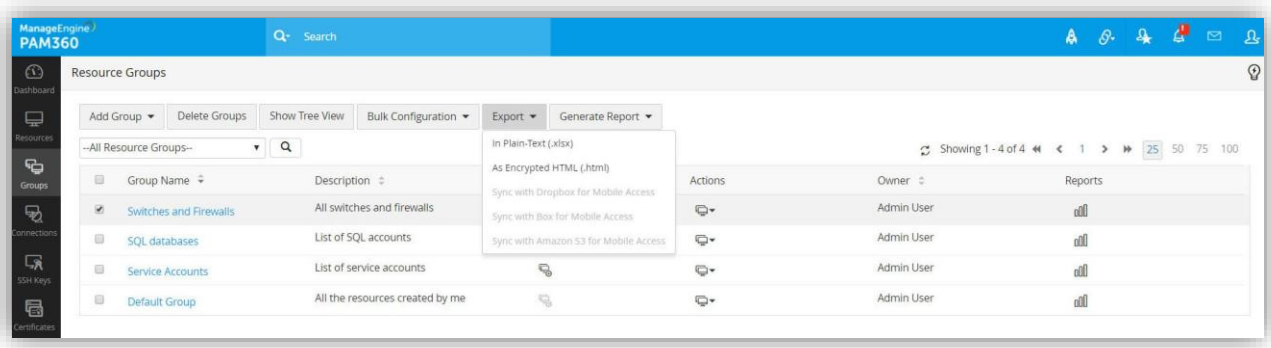
1. **Exporting the Passwords Belonging to Resource Groups in Plain Text**
2. **Exporting Passwords as Encrypted HTML**
3. **Creating a Scheduled Task to Export Passwords as an Encrypted HTML File**

1. Exporting the Passwords Belonging to Resource Groups in Plain Text

The passwords belonging to specific resource groups can be exported by administrators, password administrators and privileged administrators in plain text in (.xlsx) format.

To export any resource group,

1. Navigate to **Groups** tab.
2. Select the required resource group(s).
3. Click the **Export** button and select **In Plain Text (.xlsx)** from the drop down.



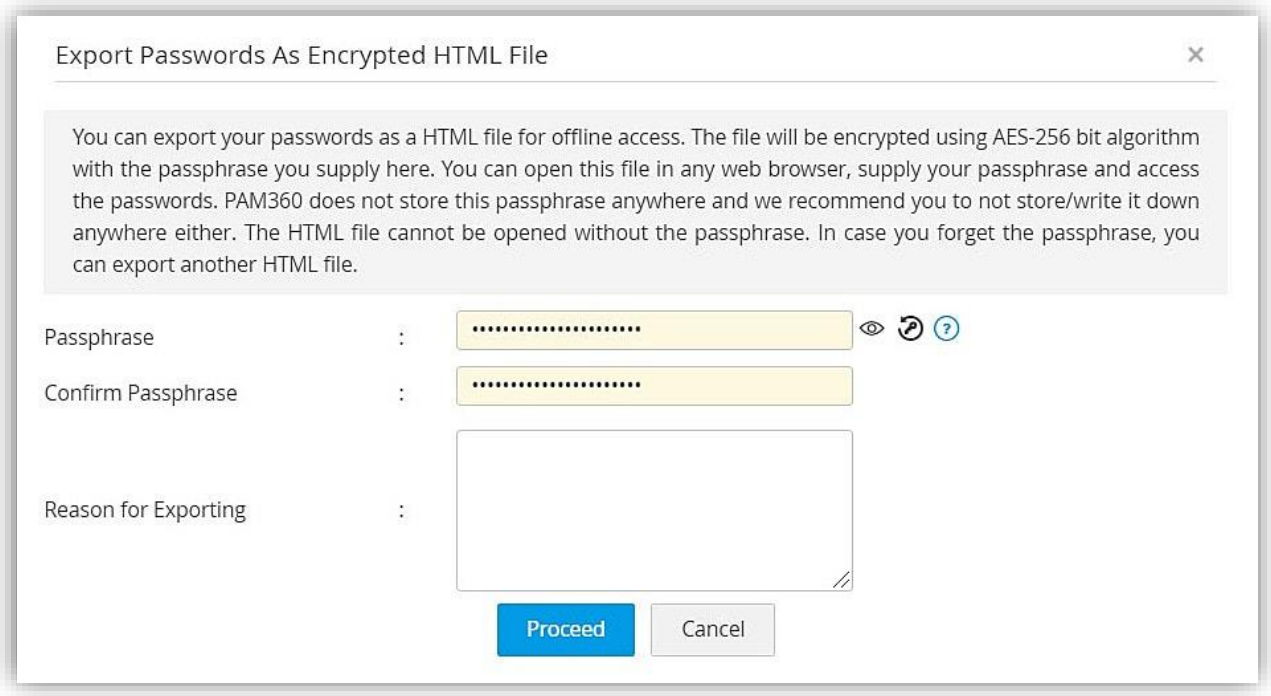
4. The resources that are part of the selected resource groups will be exported to a file.
5. Save the file in a secure location in (.xlsx) format.

2. Exporting Passwords as Encrypted HTML

PAM360 provides an option to export passwords belonging to a specific resource group to an encrypted HTML file so as to view the passwords even when there is no internet connection.

To export any resource group,

1. Navigate to **Groups** tab.
2. Select the required resource group(s).
3. Click the **Export** button and select **As Encrypted HTML (.html)** from the drop down.
4. In the pop-up form that appears, you need to specify a passphrase in accordance with the password policy as enforced by your administrator that will be used for encrypting (AES 256) the HTML for offline access. You can open this file in any web browser, supply the same passphrase, but you can create another offline file with a different passphrase.

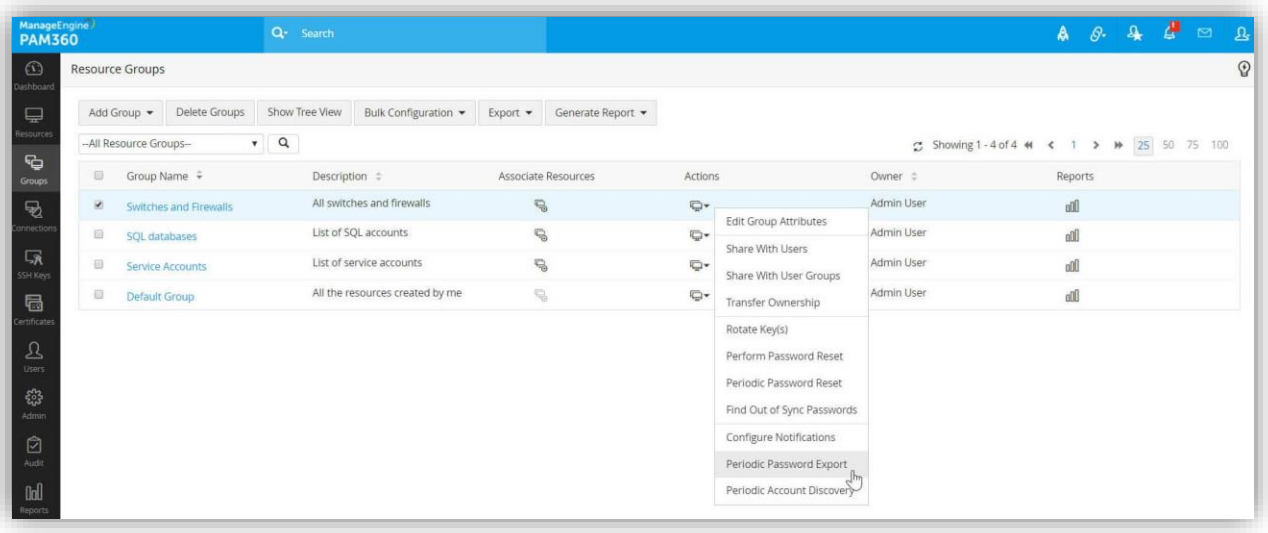


5. Confirm the passphrase and also enter a reason for exporting the passwords.
6. The resources will be exported as a HTML file. Save the file in a secure location in (.html) format.

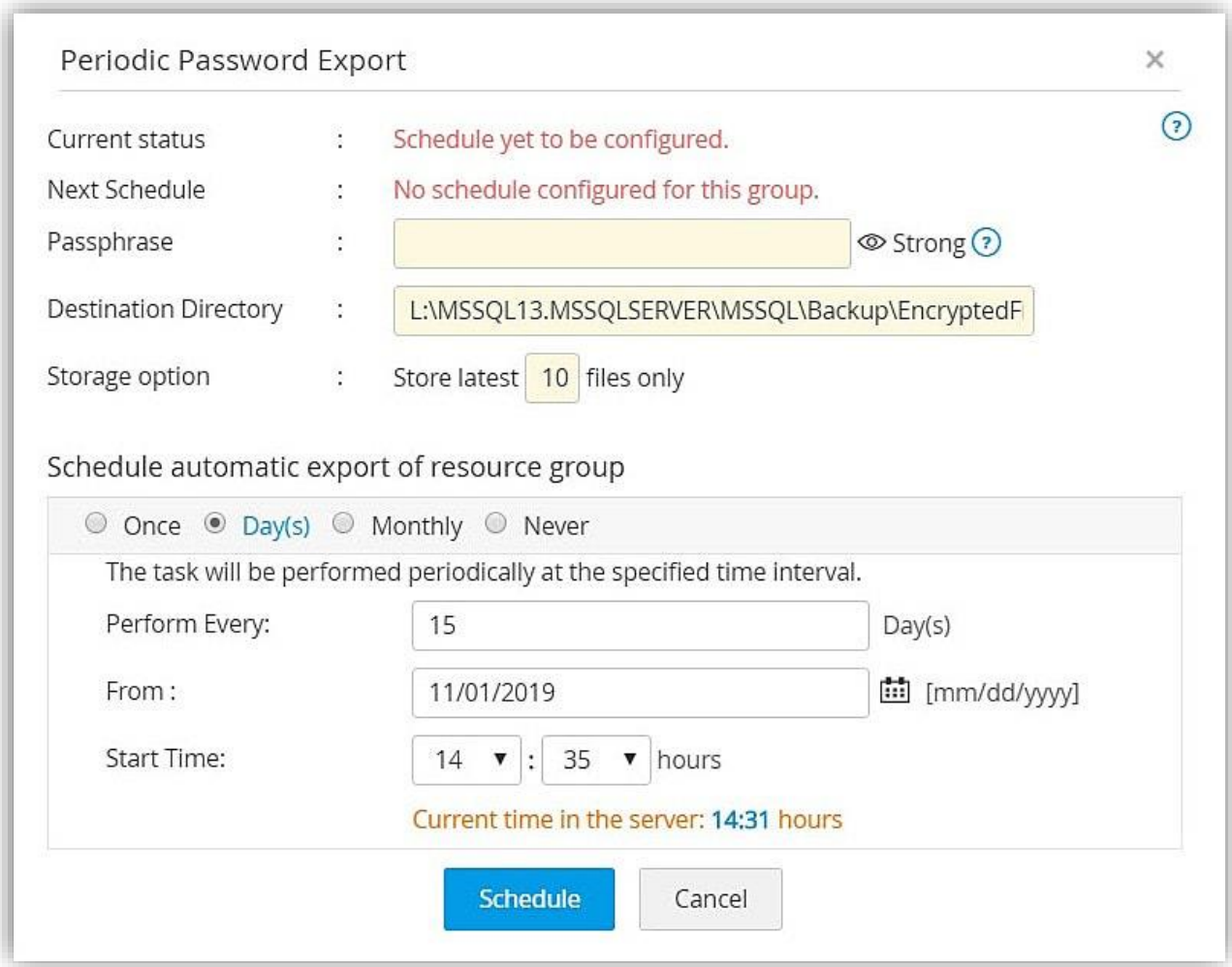
> **Note:** PAM360 will not store the passphrase anywhere and we recommend you not to store or write it down anywhere either. The contents cannot be read if you forget the passphrase, but you can create another offline file with a different passphrase.

3. Creating a Scheduled Task to Export Passwords as an Encrypted HTML File

1. Navigate to **Groups** tab.
2. Click the **Actions** icon against the required resource group and select **Periodic Password Export** from the drop down list.



3. In the pop- up that appears, you need to specify a passphrase in accordance with the resource group's password policy that will be used for encrypting (AES 256) the HTML file for offline access. You can open this file in any web browser, supply the same passphrase and access the contents.
4. Specify the destination where the exported HTML file has to be stored. You may specify any location accessible to PAM360 for write operation. By default, the files are stored under **<PAM360-Installation-Folder>/Backup/EncryptedFiles.**



5. Specify the number of files to be stored. By default, only the latest 10 files will be kept during every export schedule. Others will be deleted.
6. Specify the schedule for resource group export. The schedule can be for one-time rotation or it could be for recurring one at periodic intervals. Depending on your requirements, choose any one among the options - Once / Days / Never.
7. After selecting the option, specify other details as required and click **Schedule.**

The required schedule will be created and resources belonging the selected resource groups will be exported as encrypted HTML.

Folders

PAM360 allows you to club necessary accounts into various custom folders based on your requirements for ease of management and accessibility. Instead of selecting each account separately, you can pick multiple accounts at once in the folder and perform bulk operations on them based on the user's privilege. The folders will be accessible through the Resources and Connections tabs. However, you can create or modify the folders from the Resources tab only, and the Connections tab will reflect every change made to the folder from the Resources tab. Please note that Folders are user-specific, so you cannot share them with other users.

Real-time use case:

- Users can create a folder and add accounts based on a specific resource type or the resource's location.
- For example, consider a user managing a number of resources, some of which are located throughout Asia, Europe, and Africa. The user can create folders specific to the resource's location and add the accounts in the respective folders for easy access.
- Similarly, when a user has access to multiple resources with different resource types, the user can create folders such as Operating Systems, Database servers, and Network devices and add the resources to the folders specific to the resource type.

Notes:

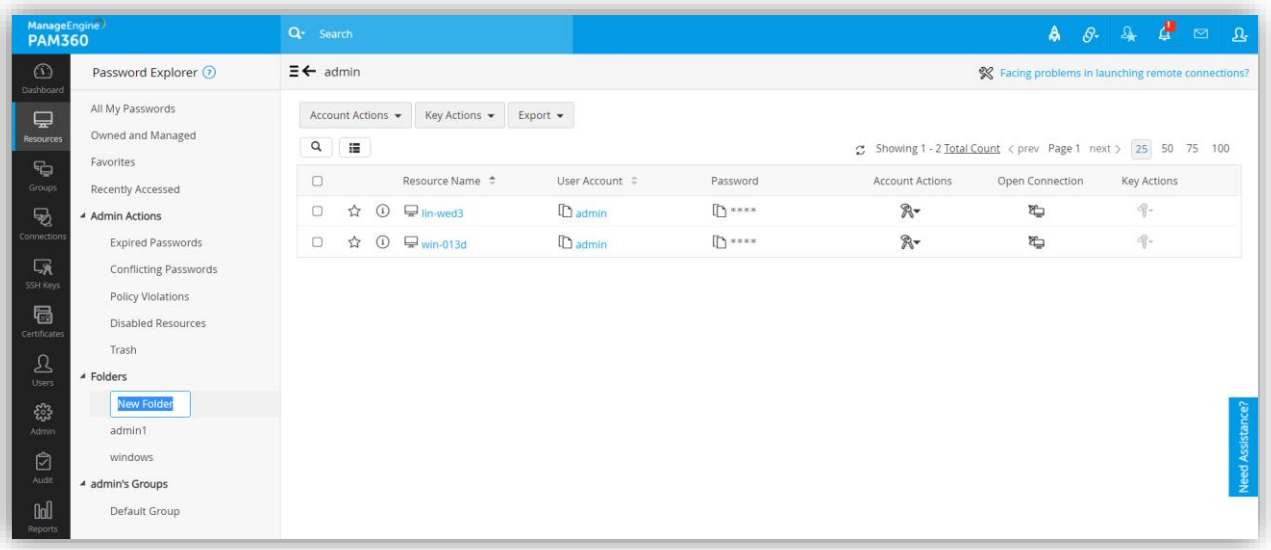
1. The decision to retain the accounts in a particular folder is up to the user.
2. You can add the same account in any number of folders.

You can perform the following operations using Folders:

1. **Creating a New Folder**
2. **Adding Accounts to Folders**
3. **Removing Accounts from Folder**
4. **Renaming a Folder**
5. **Deleting a Folder**
6. **Enabling/Disabling Folders Option**

1. Creating a New Folder

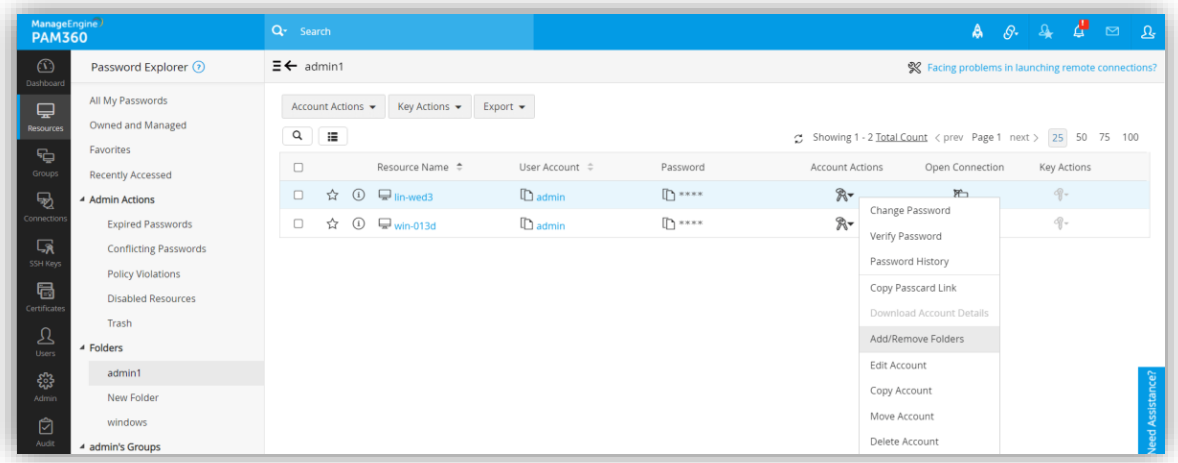
1. Navigate to the **Resources** tab.
2. Click the **+** icon besides **Folders** tag from the left pane and enter a name for the folder and hit enter.



You have successfully created a new folder.

2. Adding Accounts to Folders

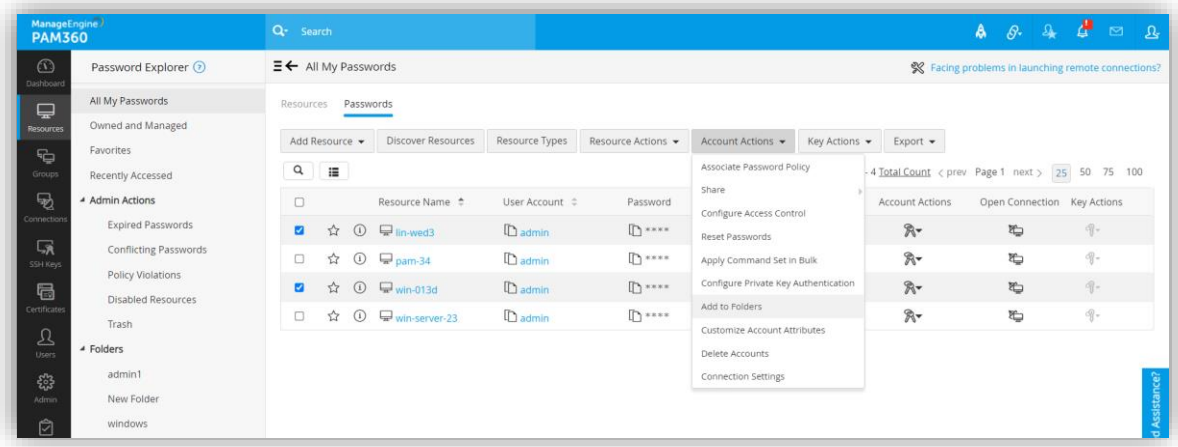
1. Users will be able to add accounts to folders from the following locations:
    i. Navigate to **Resources >> All My Passwords** and select the **Password** tab from the top pane.
    ii. Navigate to **Resources >> All My Passwords** and select the **Resources** tab from the top pane. Select a resource to access the '**Account Details**' window.
    iii. From one Folder to another. Open the folder from which you want to add the account(s).
    iv. From 'Global Search'.
2. **To add accounts individually,**
    i. Select the **Account Action** icon beside the desired account and select **Add/Remove from Folder.**



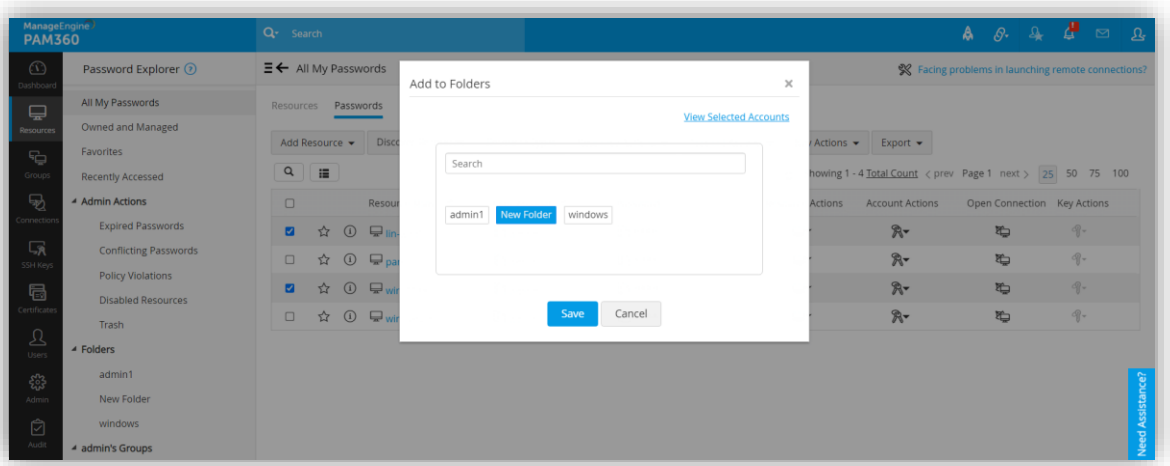
ii. In the pop-up that appears, select the folder(s) to which you wish to add the account and click **Save.**

3. **To add accounts in bulk,**

i. Select the required accounts and click **Account Actions >> Add to Folders** from the top pane.



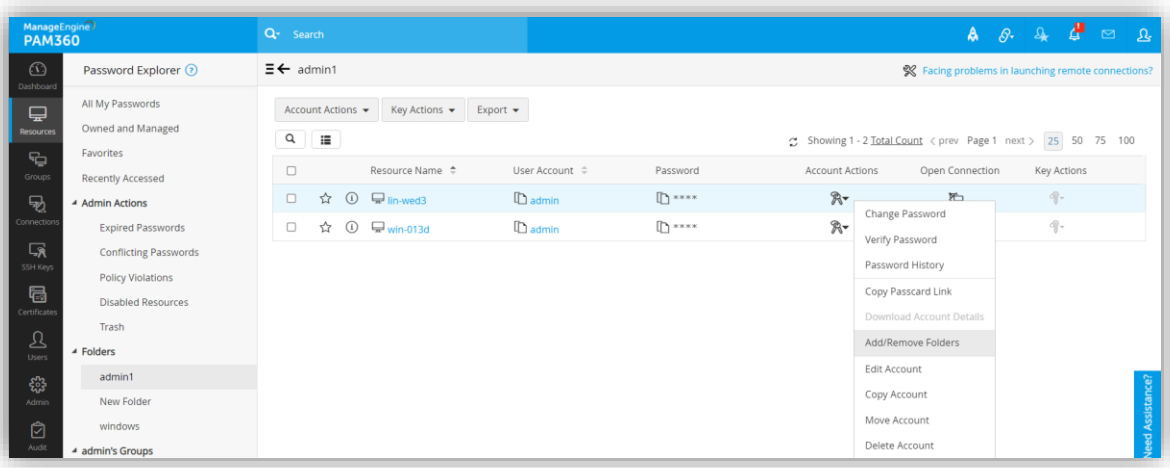
ii. In the pop-up that appears, select the folder(s) you wish to add the selected accounts and click **Save.**



You have now successfully added the selected account(s) to the selected folder(s).

3. Removing Accounts from Folders

1. Users will be able to remove accounts from folders from the following locations:
    i. Navigate to **Resources >> All My Passwords** and select the **Password** tab from the top pane.
    ii. Navigate to **Resources >> All My Passwords** and select the **Resources** tab from the top pane. Select a resource to access the '**Account Details**' window.
    iii. From a Folder. Open the folder from which you want to remove the account(s).
    iv. From 'Global Search'.
2. **To remove accounts individually,**
    i. Select the **Account Action** icon beside the desired account and select **Add/Remove from Folder.**

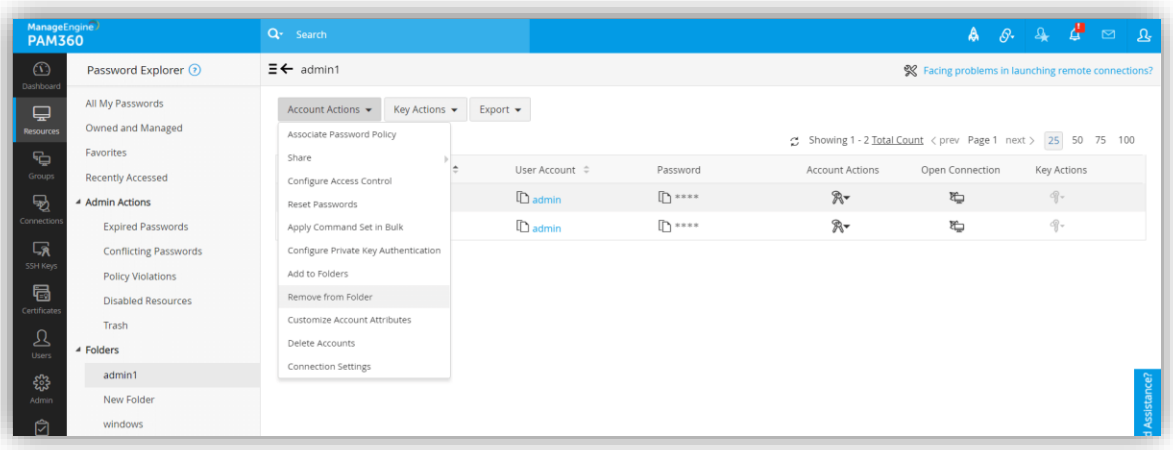


    ii. In the pop-up that appears, deselect the folder(s) from which you wish to remove the account and click **Save.**

3. **To remove accounts in bulk,**

> **Note:** You can remove accounts in bulk only from inside a folder.

i. Select the accounts and click **Account Actions >> Remove from Folder.**



ii. In the pop-up that appears, click **Remove.** This will remove the account(s) from the folder only and will not delete the account(s).

You have successfully removed the accounts from the current folder.

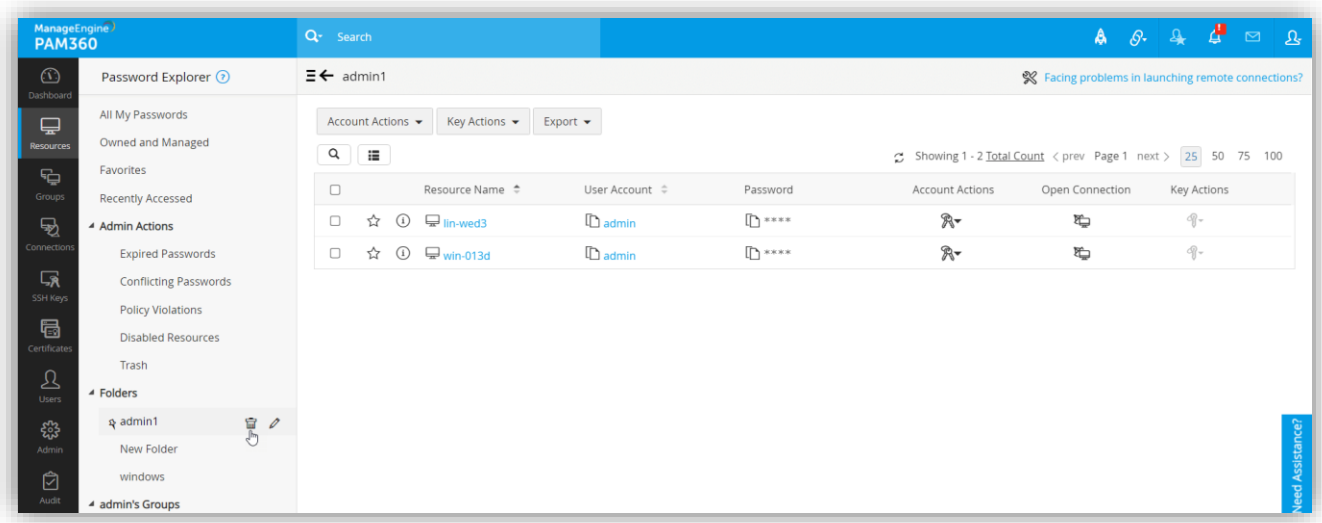
4. Renaming a Folder

1. Click the **edit icon** beside the folder name from the left pane.
2. Enter the new folder name and hit enter.

You have successfully renamed the folder.

5. Deleting a Folder

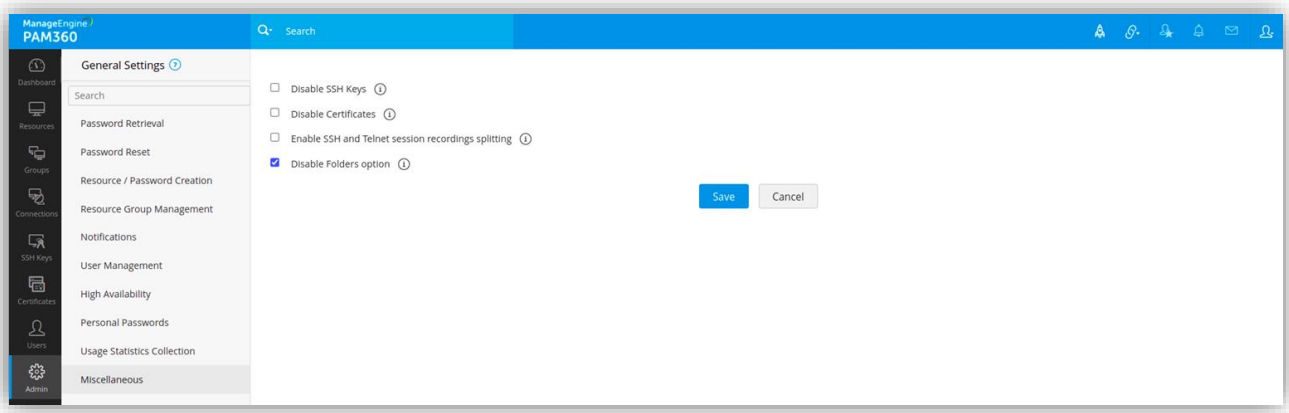
Click the **delete icon** beside the folder name from the left pane and click **Delete** in the pop-up to delete the folder.



Note: This action will remove the accounts from the folder and delete the folder only. This action will not delete the accounts from PAM360. Users will not be able to delete the pinned folder.

6. Enabling/Disabling Folders Option

1. Login to PAM360 as an administrator and navigate to **Admin >> Settings >> General Settings.**
2. Select **Miscellaneous** from the left pane.
3. Now, select the checkbox **Disable Folders option** to disable folders function for all users in PAM360.



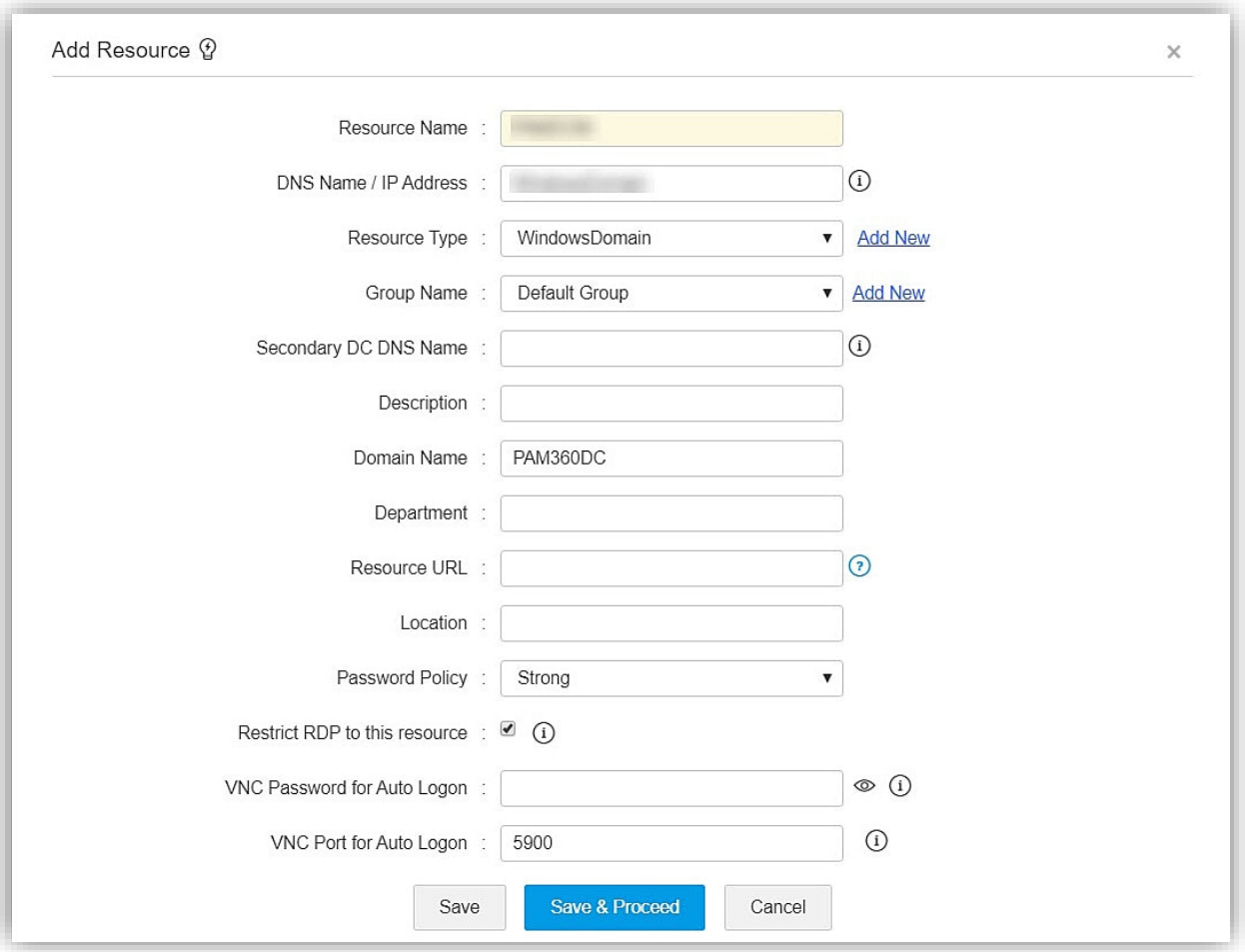
Discovery of IIS Web.Config and Password Reset

Steps Required

1. Add Domain Controller as a Resource
2. Add Domain Admin Account
3. Add Domain Member Servers as New Resources and Create Resource Group
4. Configure Remote Password Reset for IIS Web.config Files
5. Associate Resource Groups for IIS Web.config File
6. Verify Supported IIS Websites
7. Change Password
8. Additional Steps to Schedule Periodic Password Resets for IIS Websites

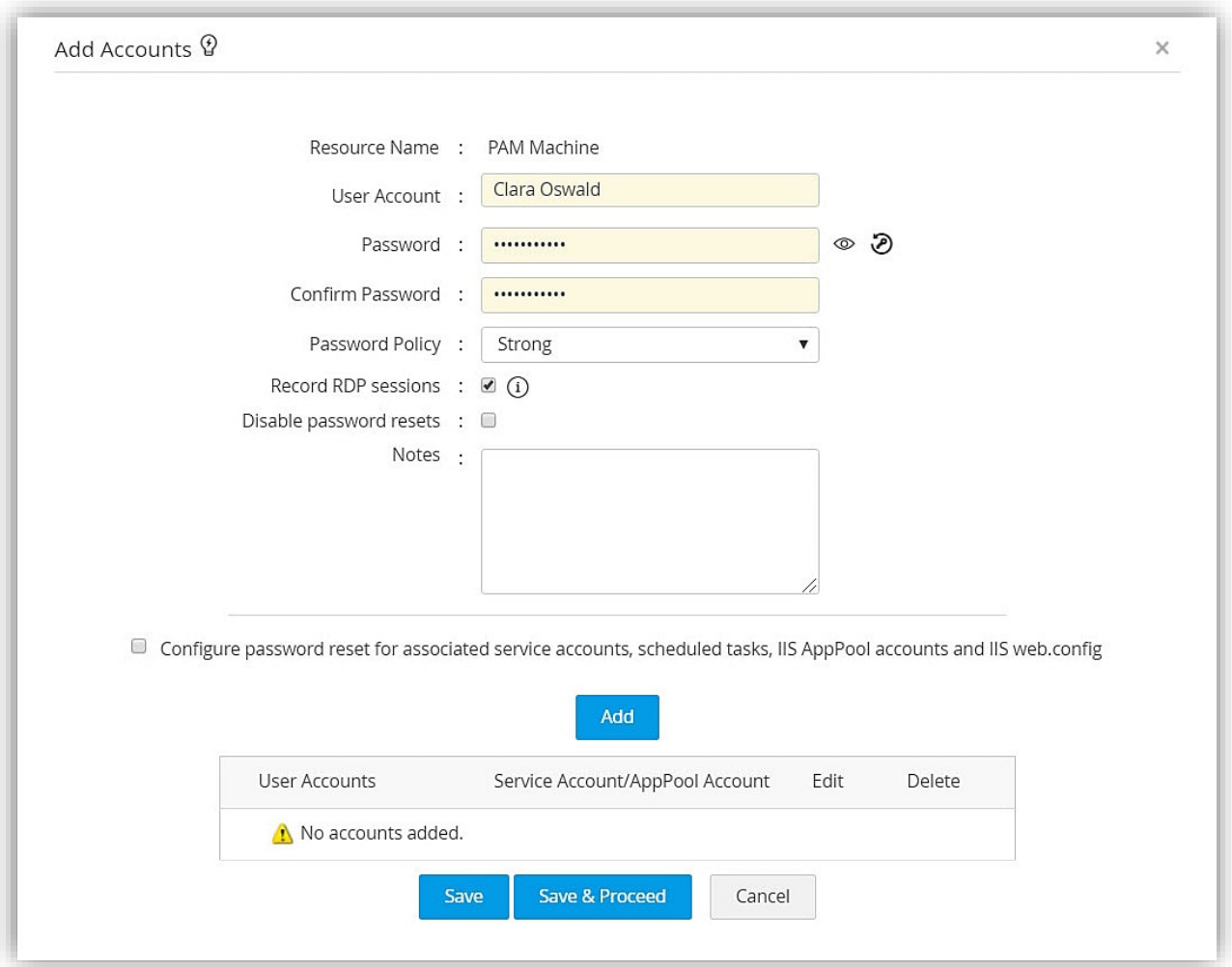
1. Add Domain Controller as a Resource

1. Navigate to **Resources** tab.
2. Click on **Add Resource** button, and select **Add Manually** from the dropdown.
3. In the pop-up form that opens, add the Domain Controller - PAM360 Machine, as a new resource with **Resource Type** as Windows Domain.
4. Supply the NETBIOS name - PAM360DC, in upper case in the **Domain Name** field.
5. Fill in the other details such as DNS.
6. Click **Save & Proceed**.



2. Add Domain Admin Account and IIS Websites

1. Navigate to **Resources tab**.
2. Click the **Resource Actions** icon against the newly added resource and select **Add Accounts** from the drop down list.

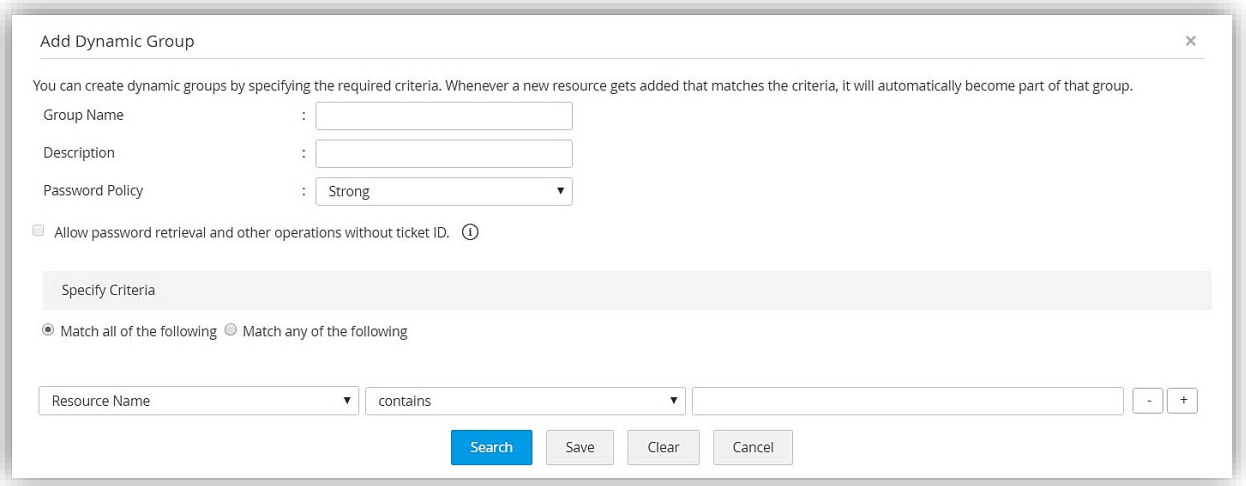


3. In the pop-up form that opens, add the domain administrator account (John Newton) and click **Add**.
4. Then, continue to add the accounts in the same way. When you are done, click **Save.**

3. Add Domain Member Servers as New Resources and Create Resource Group

1. Continue adding the other member servers of the domain - Win1, Win2, Win3, and Win4 as new resources in the same way as explained above.
2. Navigate to **Resources** tab.
3. Click **Add Resources** button and add the member servers along with their respective local accounts.
4. Now, go to **Groups** tab and click on **Add group** button and select **Dynamic Group** from the drop down.
5. In the pop-up form that opens, name the group and choose **Match any of the following**.

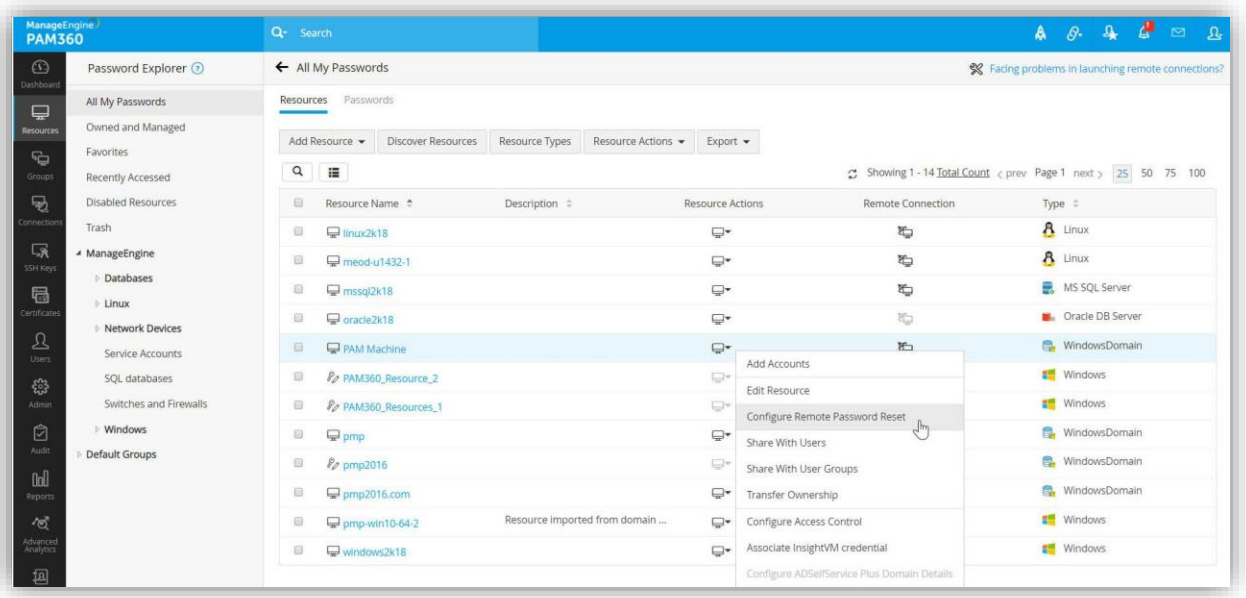
6. Click **Save**.



4. Configure Remote Password Reset for IIS Web.config Files

Instead of manual addition explained in Step 3, you can also discover the required resources and groups in your domain by following the steps given below:

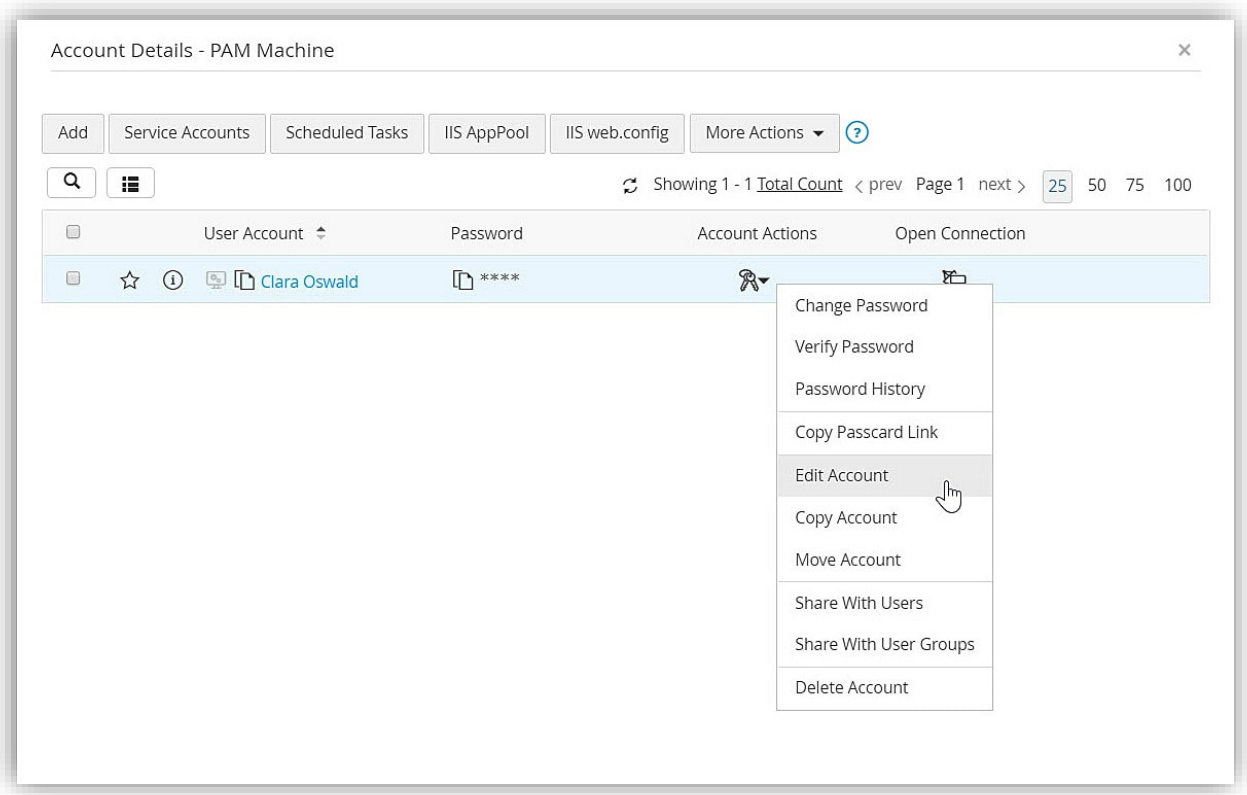
1. Navigate to **Resources** tab.
2. Click the **Resource Actions** icon against the WindowsDomain **PAM360 Machine** resource and select **Configure password reset** from the drop down.



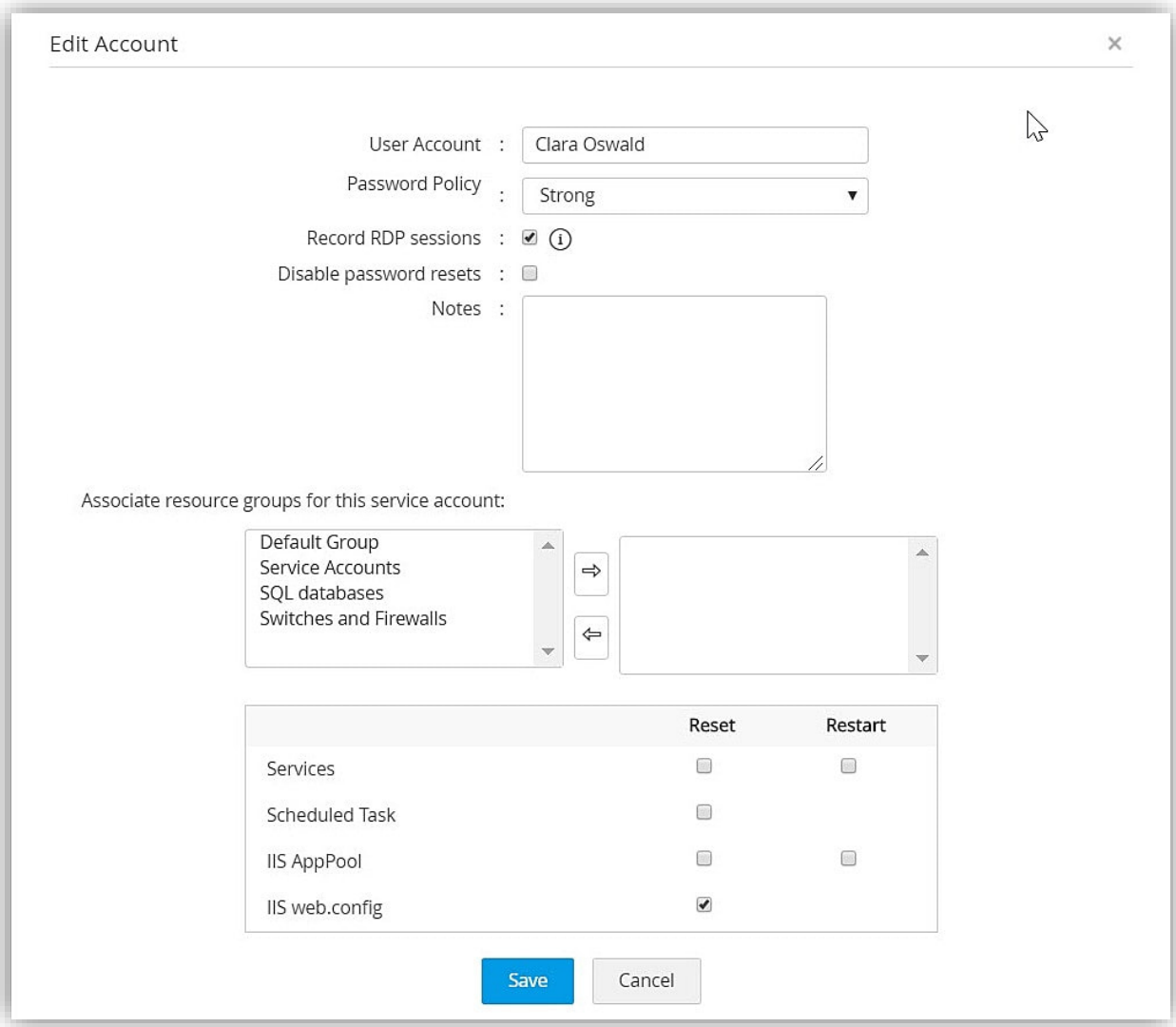
3. In the pop-up form that appears, select the **Domain Admin** (John Newton) account as the **Administrator Account**.
4. Click **Save**.

5. Associate Resource Groups for IIS Web.Config Files

1. Click on the WindowsDomain **PAM360 Machine** resource name.
2. In the UI that opens, click the **Account Actions** icon against the app pool account (John Newton in this case) and then select **Edit account** from the drop down.

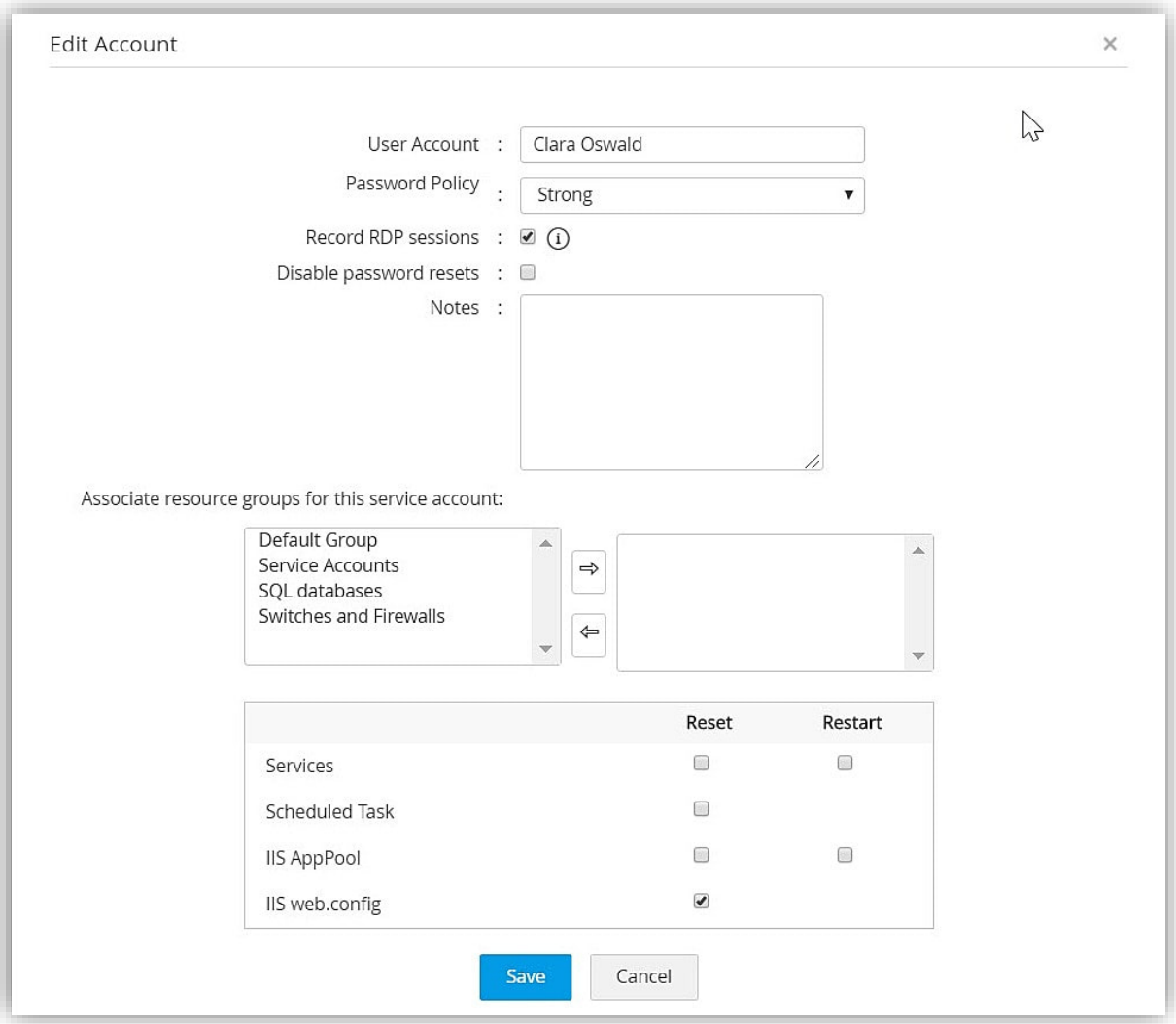


3. In the pop-up form that appears, associate resource groups for this service account by moving it to the other box.
4. Click **Save**.



6. Verify Supported IIS Websites

1. Click the WindowsDomain **PAM360 Machine** resource name.
2. Select the IIS website **John Newton** and click the **IIS web.config** button.
3. In the pop-up form that appears, click **Fetch** under **Supported IIS websites**.
4. PAM360 will scan and list all the websites that are run in the servers of IIS websites in which the service account is used in the connection string of the web.conf files. After reviewing the list, hit **Ok**.



7. Change Password

1. Click on the WindowsDomain **PAM360 Machine** resource name.
2. Click the **Account Actions** icon against **John newton** and then select **Change Password** from the drop down.
3. In the pop-up form that appears, either provide or generate a new password. Make sure to enable **Apply password changes to the remote resource**.
4. Click **Save**. PAM360 will immediately reset the password in the domain first and then, automatically update the new password across all servers where **John Newton** is used to run IIS websites.

8. Additional Steps to Schedule Periodic Password Resets for IIS Websites

The aforementioned steps are adequate to carry out password resets for app pool accounts anytime on demand. If you would like to configure automatic password resets on a periodic basis, execute the additional steps given below:

To configure periodic password reset for IIS websites,

1. A resource group has to be first created.
2. Click the **Actions** icon against the resource group and select **Periodic Password Reset** from the drop down.
3. A pop-up form will open with a four step process through which required schedule can be created.

Connections and Privileged Sessions

The **Connections** tab in PAM360 serves as a one-stop place to view all the added Connections, Favorites, and Connection Groups. The tab holds some useful options, such as a new SFTP-based file transfer option, and a new search filter that facilitates the search of resources within the tab using Name, DNS name, or type of OS. The connections within have quick access control buttons; Connect, Request, Checkin, Checkout, RemoteApp, and Secure File Transfer. Use the **Connections** tab to establish secure and interactive remote sessions to RDP, SSH, VNC, and SQL systems where the sessions are tunneled through the PAM360 server, which provides a secure channel to protect your remote connections from third-party interceptions. In addition, it allows you to observe all privileged sessions in real-time, terminate the sessions if necessary, and record the remote sessions to review later.

> **Note:** PAM360 uses HTML-5 compatible browsers to initiate the remote sessions. Examples of HTML5 compatible browsers include IE 9 or above, Firefox 3.5 or above, Safari 4 or above, and Chrome.

At the end of this section, you will have learned the following:

1. **Connections Tab - A General Overview**
2. **Options to access from the Connections tree (left pane)**

1. Connections Tab - A General Overview

Resources and the related accounts added from the **Resources** tab are accessible from the **Connections** tab. To learn in detail about the different ways of adding resources and accounts into PAM360, click the below links:

i. **Add Resources Manually**
ii. **Import Resources**
iii. **Discover Resources and Privileged Accounts**

Once you have finished adding your resources to PAM360, there are numerous ways in which you can use the **Connections** tab to manage your resources effectively. Basically, the **Connections** view has three sections:

a. **The leftmost pane** - Displays all the added Connections category-wise, such as **Owned and Managed, Recently Accessed**, etc., **Favorites**, and **Connection Groups**.
b. **The 'Resources' pane** - Displays the list of resources under the specific category as

clicked from the leftmost pane.

c. **The 'Accounts' pane** - Reveals all accounts in each resource as clicked from the 'Resources' pane.

2. Options to Access from the Connections Tree (Left Pane)

The left pane you see on the Connections page lists all the available connections in PAM360 organized under different categories. Click a category to view the connections only under that specific category. Read further to know in detail about each category in detail:

1. **All My Connections** - Click this option to display all the resources that are shared to you and available for your usage. Click the name of a resource to display all accounts corresponding to the selected resource. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type.
2. **Owned and Managed** - This option is for users with admin privileges. All resources owned by administrators and shared to them by other users are available here. Click the name of a resource to display all accounts corresponding to the selected resource. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type.
3. **Favorites** - All accounts marked as a 'favorite' are available here. To mark an account as a favorite, go to the **Resources** tab, switch to the **Passwords** tab and click the star icon (☆) beside an account name. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type.
4. **Recently Accessed** - All recently accessed resources are listed under this option for a quick reference. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type.
5. **Web App Connections** - All web-based applications added as a resource in PAM360 are listed under this option. From here, you can perform a one-click logon to the resources.
6. **HTTPS Gateway Connections** - All resources that support HTTPS-based web links as the resource URL and configured will be listed under this option. Click here to learn more about HTTPS gateway connections in detail.
7. **Secure File Transfer** - Click this option to perform a secure bi-directional file transfer between two folders residing in different resources. Click here to learn about secure file transfer in detail.
8. **Resources groups added by you** - This option is for users with admin privileges. All resource groups created by you are available under this options. To search for a resource, enter the resource name, DNS name, or the operating system (OS) type. Click here to learn more about different types of resources groups in PAM360.

Use the icons  and  to toggle between the old and new connections views.

Connection Actions and Configurations

As explained in the previous document, the **Connections** tab offers you a comprehensive view of all the resources that are owned by you and/or shared to you as well as the accounts belonging to them. In this document, you will learn about the various actions and all possible configurations that can be performed on connections.

Click each of the below links to learn in detail about the different connection actions and configurations in detail:

3.1 Different Resource Pane Scenarios

3.2 Launching Secure Remote Sessions

3.3 Working with Files present in the Remote Machines

3.4 Requesting Passwords for Accounts with Controlled Access

3.5 Accessing RemoteApps

3.6 Configuring Connection Settings for Accounts

3.7 Configuring Gateway Settings for Remote Sessions

3.8 Configuring SSH Command Control (Filtering)

3.1 Different Resource Pane Scenarios

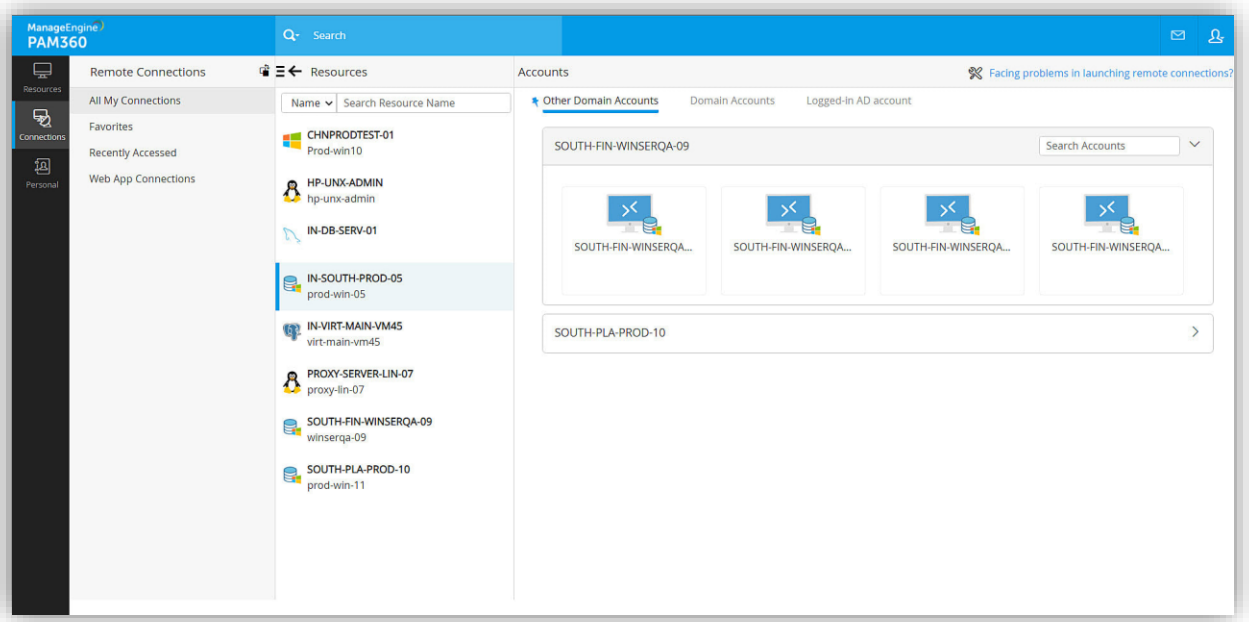
Based on the type of resource you select from the Resources pane, the view in the Accounts pane will change. Consider the following scenarios:

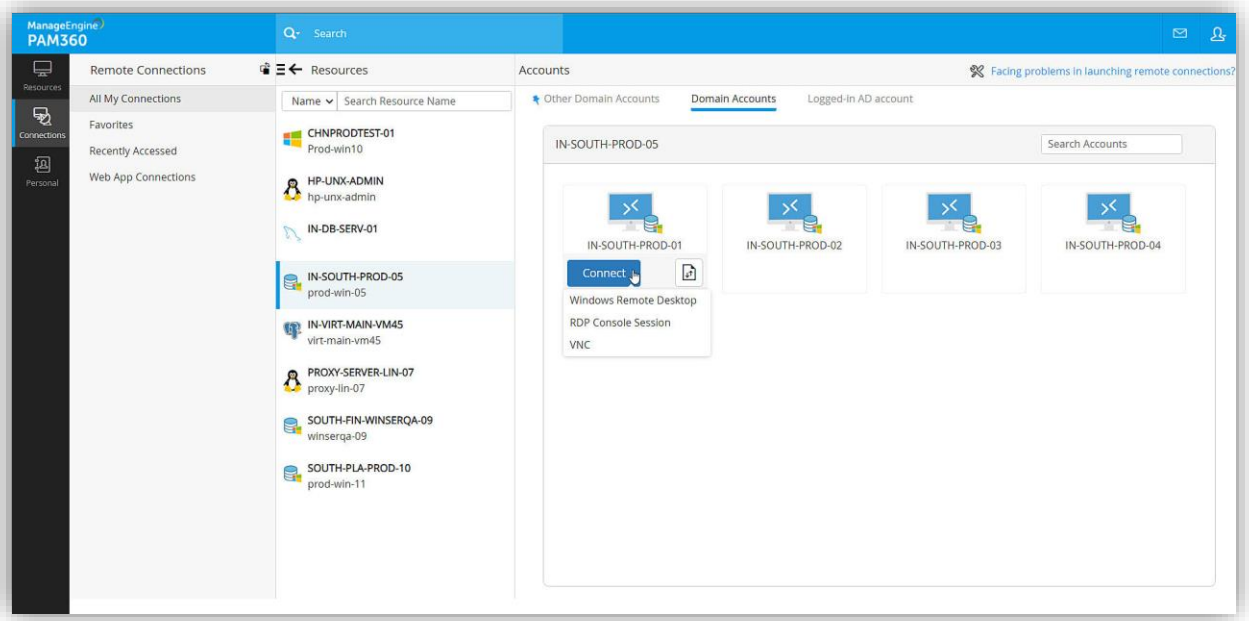
Scenario 1: You have selected a Windows Domain resource named CHNPRODTEST-01 in the Resources pane.

In this case, the Accounts pane will display two columns:

1. **Domain Accounts** - the domain accounts belonging to CHNPRODTEST-01 will be listed here with all the available logon options. You may search for accounts with keywords using the search bar.
2. **Other Domain Accounts** - the Domain accounts belonging to the other Windows Domain

resources available to you will be listed in this column along with the available logon options.



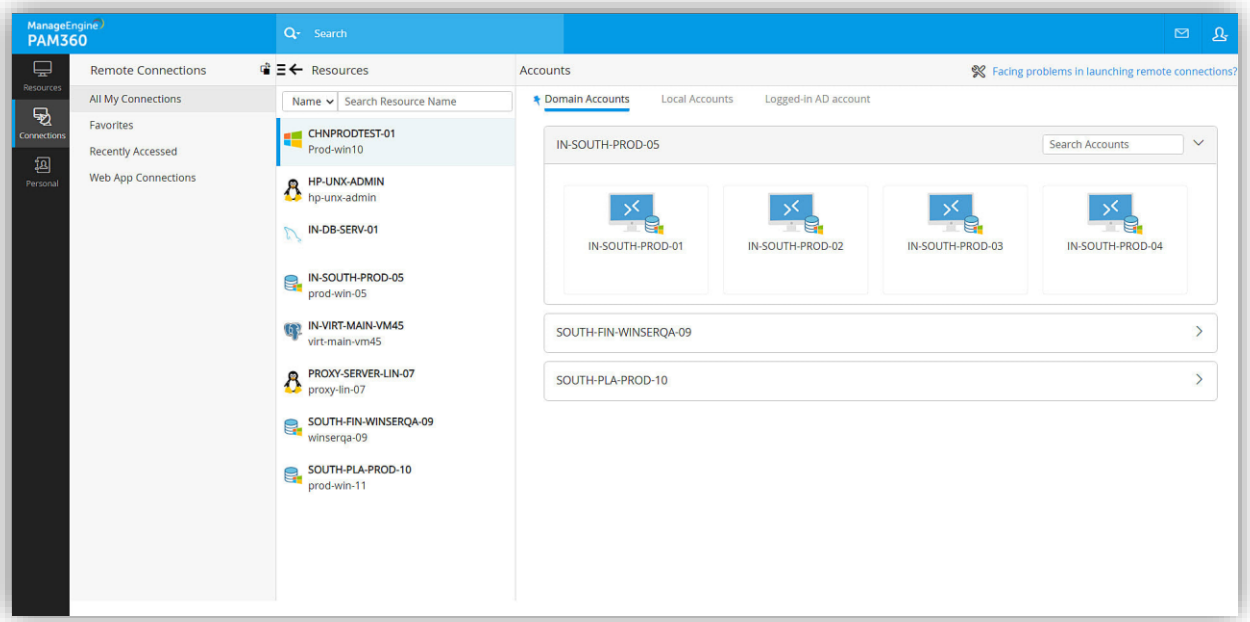


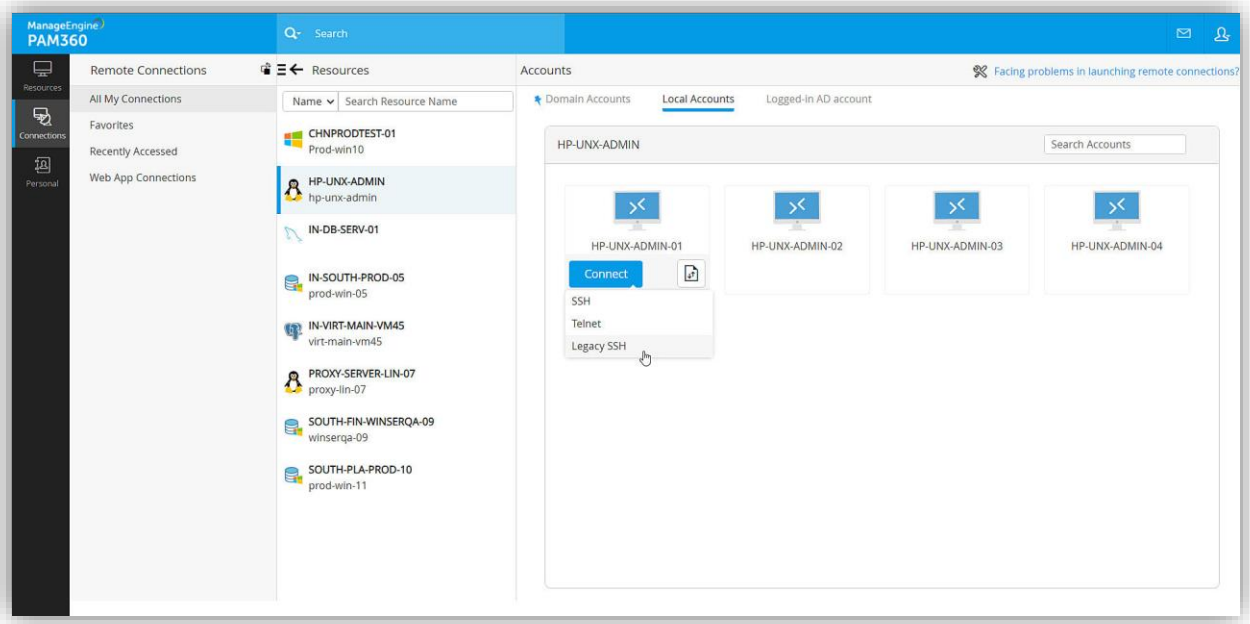
Scenario 2: You have selected a non-Windows Domain resource, such as a Windows or a Linux resource in the Resources pane.

In this case, the Accounts pane will display two columns:

1. **Local Accounts** - the local accounts belonging to the selected resource will be listed here with all the available logon options.

2. **Domain Accounts** - the Domain accounts belonging to the other Windows Domain resources available to you will be listed in this column along with the available logon options.





Note:

Apart from the SSH protocol, Telnet, Legacy SSH, and other auto logon helpers will be disabled for the accounts applied with SSH command control (filtering).

Scenario 3: You have logged into PAM360 using your Active Directory (AD), Azure AD, or LDAP credentials.

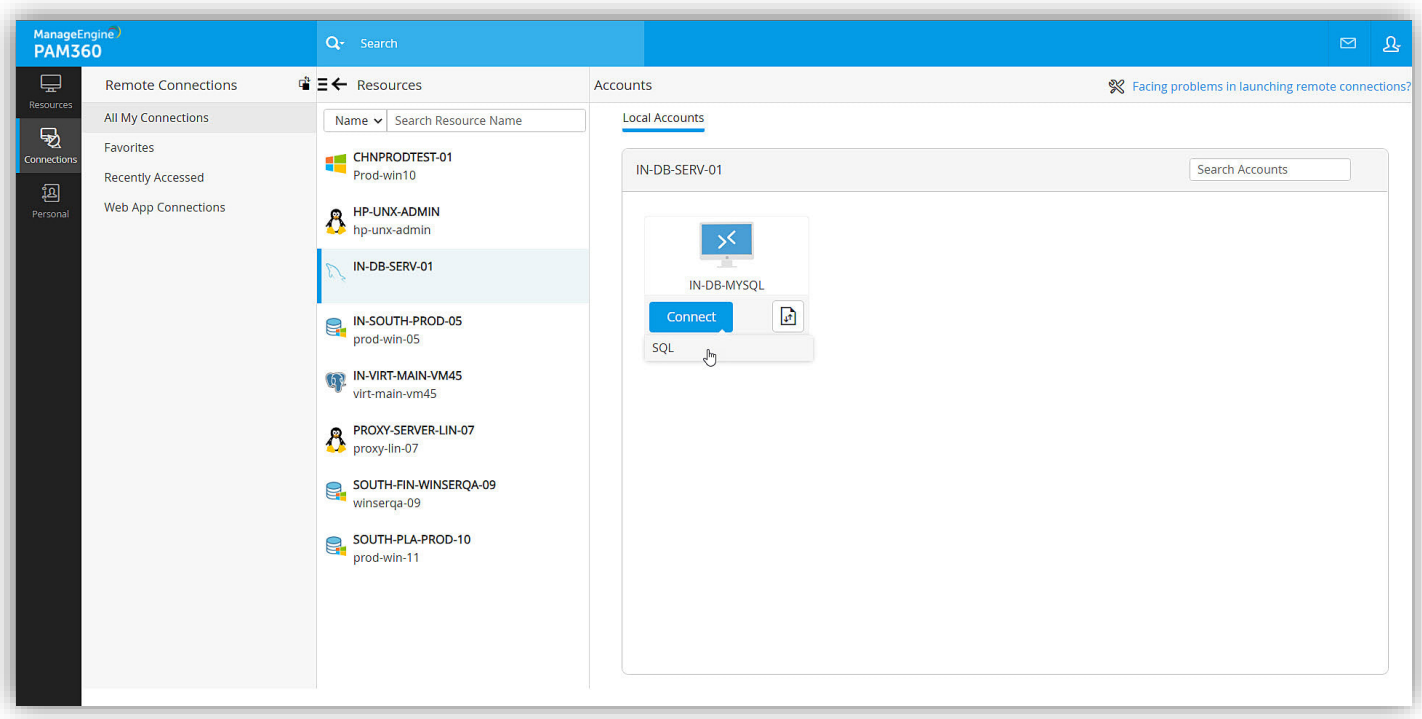
Here, you will see two tabs based on your choice of resources in Scenarios 1 and 2. In addition to that, the Accounts pane will also show the following tab as the third one:

Logged in AD/Azure AD/LDAP Account - the AD/Azure AD/LDAP account with which you have currently logged in will be displayed here. You can use this account to log in to other resources. Refer to the section **3.1.1 Single-click Auto Logon using AD, Azure AD, and LDAP** to learn about this in detail.

> **Note:** The logon options available for Logged in AD/Azure AD/LDAP Account will be Windows Remote Desktop for Windows and SSH for Linux systems.

Scenario 4:

For certain resource types like PostgreSQL, MySQL, and Oracle DB Server, both Domain accounts and AD/Azure AD/LDAP accounts will not be shown. For those types, the Accounts pane will display only the Local Accounts tab.



> **Note**: In the Accounts pane, you can pin a specific tab for quick access and reference. For example, if you pin the **Local Accounts** tab, whenever you choose a resource, the local accounts of the resource will be displayed first. This operation is user-specific and does not affect the view for other users accessing the same installation.

3.2 Launching Secure Remote Sessions

PAM360 allows you to establish privileged remote sessions to RDP, SSH, VNC and SQL systems through HTML-5 compatible browsers. PAM360 carries out remote sessions and file transfer operations using secure protocols such as the Remote Desktop Protocol (RDP), SSH File Transfer Protocol (SFTP), Secure Copy Protocol (SCP), File Transfer Protocol (FTP). As the privileged remote sessions are tunneled through the PAM360 server, it creates a secure channel to protect your remote connections from third-party interceptions. The passwords needed to establish the remote connections are securely stored in PAM360. There is also a provision to enforce password access control the resources. These safety measures ensure your data stored in the PAM360 repository and remote sessions carried out from PAM360 always remain secure. In addition to launching secure remote sessions, you can record, playback, and archive the remote sessions launched from PAM360. The archived files support forensic audits and compliance requirements of organizations.

To launch a remote session to a resource, follow the below steps:

1. Navigate to the **Connections** tab and click the required resource name under the **Resources** pane.
2. If you have selected a Windows Domain resource, all the local accounts of the selected domain resource and the accounts of other Windows Domain resources will be displayed on the right in two separate tabs. Hover your mouse over the thumbnail of the required account and click **Connect**. Depending on the resource type, multiple logon options will appear in a pop-up menu. For example: If you select a Windows resource, you will get the following options for Local accounts: **Windows Remote Desktop, RDP Console Session,** and **VNC.** And these logon options for Domain accounts: **Windows Remote Desktop** and **RDP Console Session.**
3. Click the type of remote session you want to launch. Now, a new tab will open up and the remote session will begin once PAM360 authenticates the connection using the password stored in the repository.

When a privileged remote session is active, you can view the details from the **Notifications** panel, the **Password Dashboard**, and under **Audit >> Active Privileged Sessions**. All remote connections can be recorded and archived. Refer to the help section **Privileged Session Recording** to learn about session recording in detail.

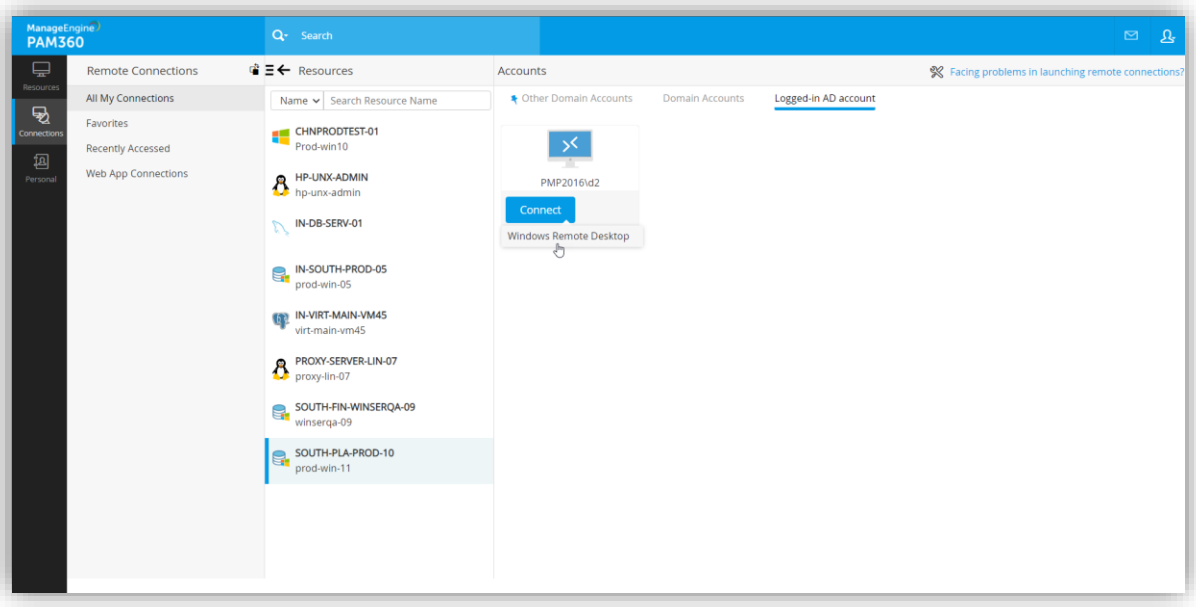
3.2.1 Single-click Auto Logon using AD, Azure AD, and LDAP

PAM360 allows users to launch a direct RDP connection with the target resource using any domain account that is owned by you or shared with you. Users can select the required Domain account or can use the currently logged in AD/Azure AD/LDAP account to connect to the desired resource.

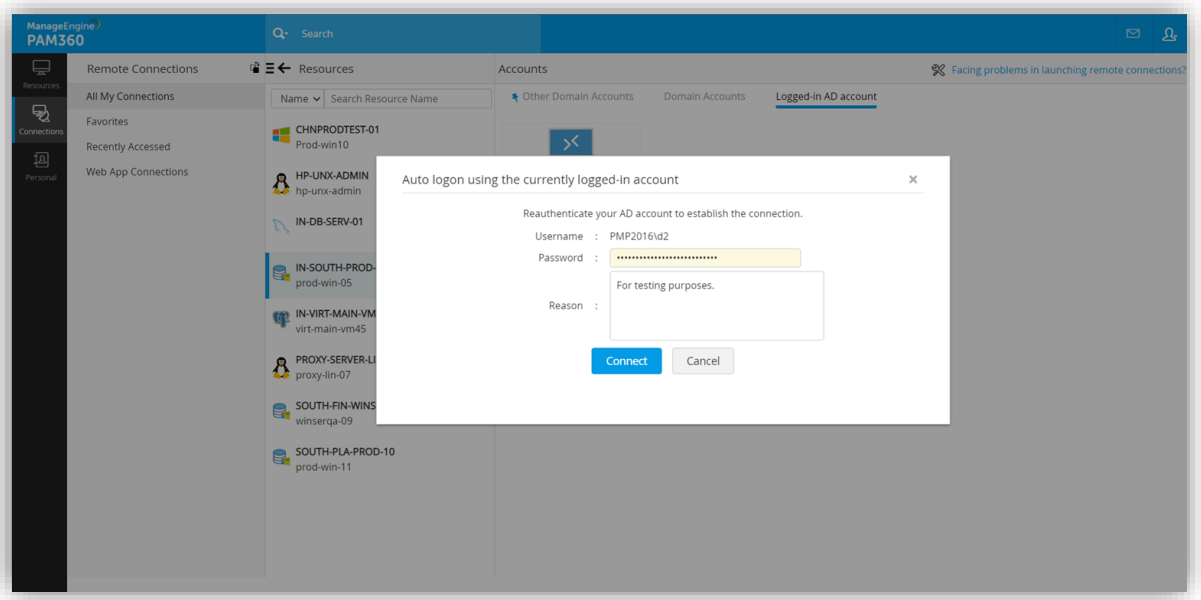
For a selected set of resource types, PAM360 allows you to log into resources that are shared to you or owned by you using the AD/Azure AD/LDAP credentials with which you have currently logged in. When you are logged into PAM360 using your AD/Azure AD/LDAP credential, you will find your details displayed in the Connections tab as a separate column named **Logged in AD/Azure AD/LDAP account.** For example, this option will not be available for resource types that do not support Domain accounts login such as PostgreSQL and MySQL.

From this space, you can log into the required resource with a single click using the auto logon options that are displayed with a mouse hover.

1. Navigate to the **Connections** tab and under the **Resources** pane, click the required resource. Now all the local accounts belonging to the resource as well as other available Domain accounts will be displayed in the Accounts pane.
2. Here, to log into a resource using a Domain account, simply hover over the Domain account which you want to use and click Connect. PAM360 will authorize your connection to the selected resource using the Domain account you chose.
3. Alternatively, you may use your currently logged in AD/Azure AD/LDAP credentials to log into a resource (as explained in scenario 3). To do this, select the required resource from the left pane and switch to the **Logged-in AD/Azure AD/LDAP account** tab on the right.
4. Here, hover over the connection icon and click **Connect**. You will see Windows Remote Desktop as the logon option for Windows resources and SSH for Linux-based resources.



5. To reauthenticate the connection, must enter your AD/Azure AD/LDAP password once in the pop-up that appears. Click **Connect** to open the remote connection.



6. Enter the **Reason** for establishing the connection (mandatory) and click **Connect.**
7. Now, you have successfully established a connection with that resource.

Click here to learn about enabling **Active Directory**, **Azure AD** or **LDAP authentication** in PAM360.

3.3 Working with Files Present in the Remote Machines

PAM360 allows you to transfer large files between two systems using the SSH File Transfer Protocol (SFTP). To use this feature, the SFTP server must be installed in the target remote systems. Apart from bi-directional file transfer, PAM360 lets you upload and download files between the user's machine and the remote connection they have established, without the need for a remote session. This upload and download mechanism is made possible through the Secure Copy Protocol (SCP). For upload and download mechanisms, there is a file size limit of 16 MB.

Click here to know in detail on how to perform SFTP-based file transfer in PAM360.

3.4 Requesting Passwords for Accounts with Controlled Access

When dealing with accounts that are secured using the Password_Access_Control_Workflow, the **Connections** tab serves as a one-stop place to make all the password request-related options easily accessible. When an account protected by the access control workflow is shared to you, you may gain access to it by requesting for the password and getting it

approved by the resource owner/administrator. In case of Domain accounts, the Connections tab helps you send password requests directly from the Domain Accounts view.

Click here to learn more about the three possible operations you can do:

3.4.1 Request for the Password

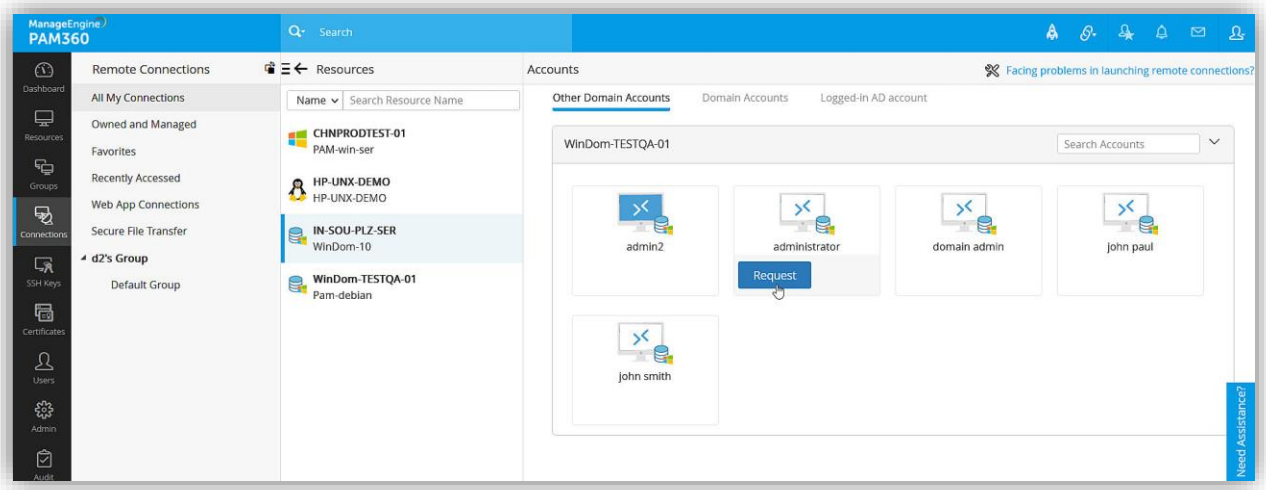
3.4.2 Check out the Password

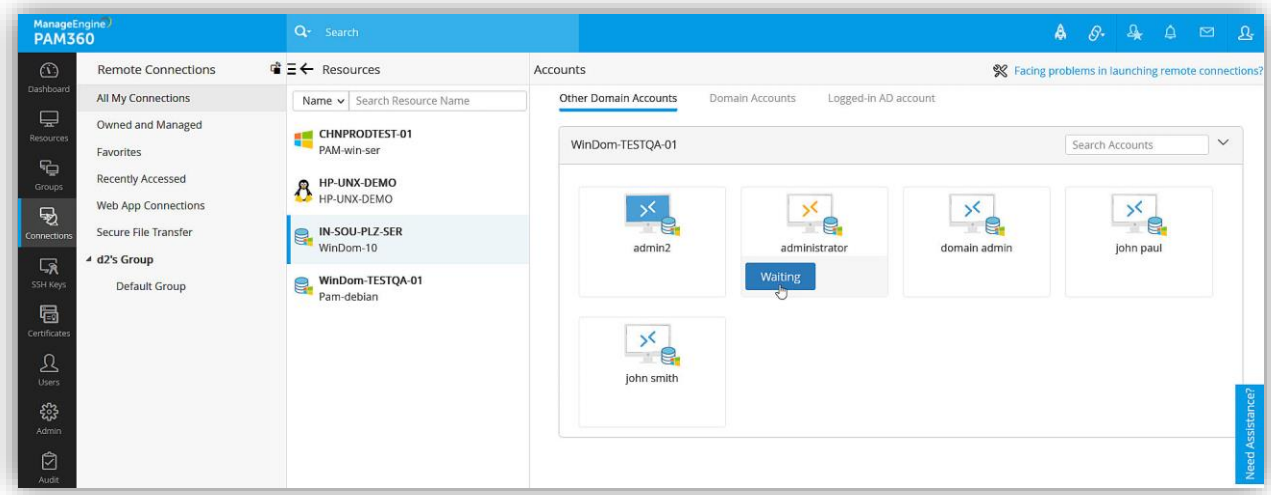
3.4.3 Check in the Password

3.4.1 Request for the Password

1. Navigate to the **Connections** tab and click the required resource name under the **Resources** pane.
2. All accounts corresponding to the selected resource and any Windows Domain accounts that are also shared to you will be displayed on the right as per the scenarios detailed above. Hover your mouse over the thumbnail of the required account and click **Request**.
3. Now, a request will be sent to the authorized administrators. Once the request is approved, you can check out the password and launch a remote session to the account.

When the password of the account is available for request, you will see the **Request** option. After you send a request and it is yet to be approved by an admin, the status will change to **Waiting**.

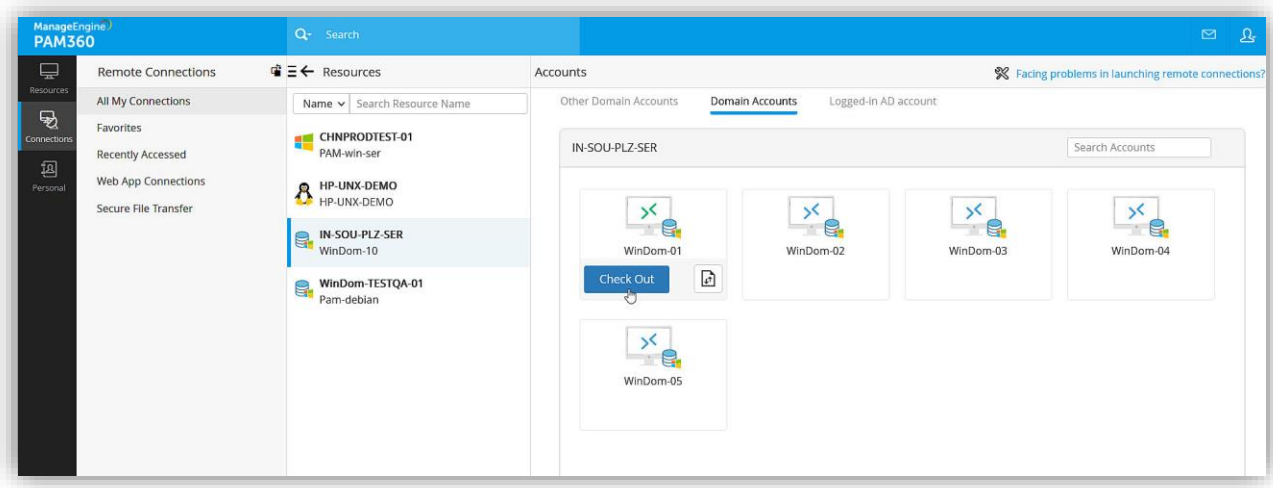




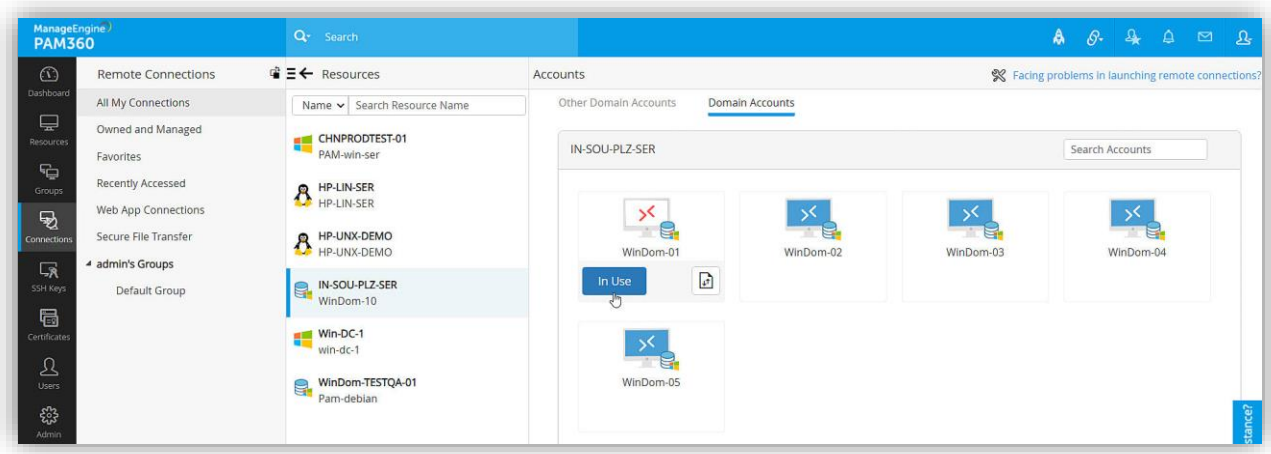
3.4.2 Check Out the Password

1. Once the administrators approve your password request, navigate to the **Connections** tab and find the account.
2. Hover your mouse over the thumbnail of the required account and click **Check Out** to check out the password and gain access to the account. You can use the account for 30 minutes after which the password will be automatically checked in and your access will expire.

The green icon indicates that the password request is approved and the password is available for check out.

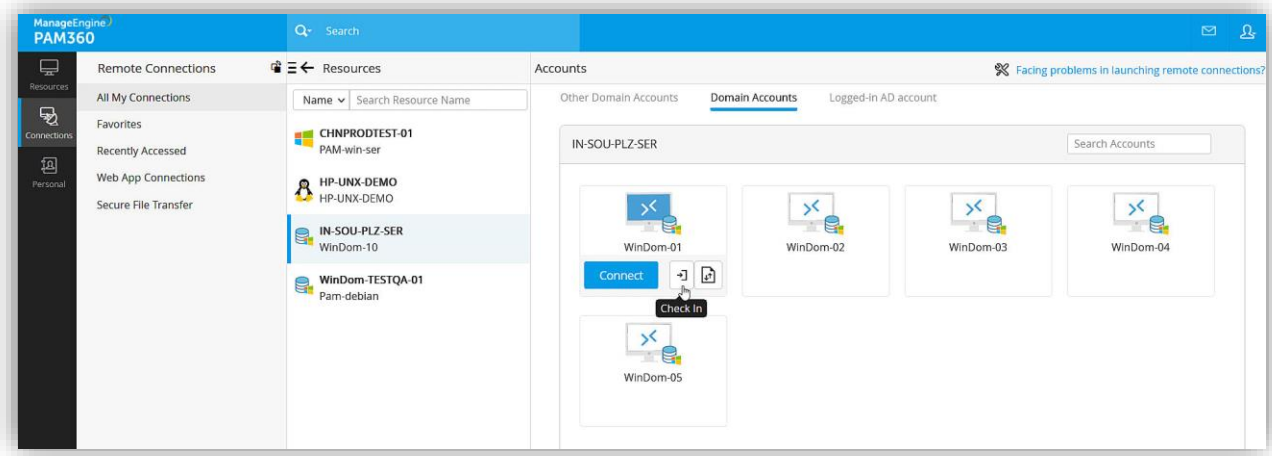


If a user has checked out the password and is currently using it, other users will not be able to request for access. During this time, you can see the option **In Use** and a red icon on the thumbnail to indicate that the password is currently in use.



3.4.3 Check In the Password

Once you are done using the password, hover your mouse over the thumbnail of the account and click **Check In** to check in the password. Now, the password will be available for request again.



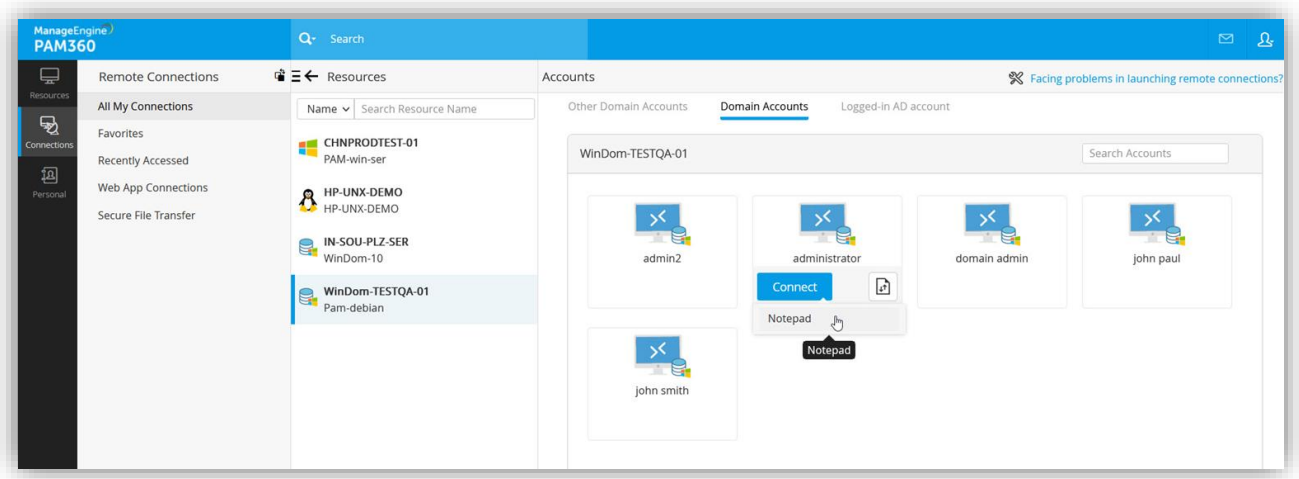
3.5 Accessing RemoteApps

Configure RemoteApp for Windows and Windows Domain resources to allow access only to specific applications in an account. Click here to learn in detail about how to configure RemoteApp in PAM360. Once you have configured the RemoteApps and associated them with the resources, you will find the option to launch a remote session and open the particular app alone.

To launch a RemoteApp:

1. Navigate to the **Connections** tab and find the resource which is associated with the RemoteApp.

2. Hover your mouse over the thumbnail of the required account and click **Windows Remote Desktop.** A list of RemoteApps associated with this account will pop up. Click the required RemoteApp name and it will open up in a new tab.



Note: RemoteApp configuration overrides the access level provided to a user while sharing the resource.

3.5.1 Use Case Scenarios

Let's assume that **CHNPROD-WIN10** is a Windows resource and **CHNWinDom-01** is a Windows Domain resource.

Scenario 1: RemoteApp is configured in the Windows resource

The Windows resource is shared to User A with **RemoteApp Only** access level and the Windows Domain resource is shared with **View** level access.
RemoteApp is configured at a resource-level in CHNPROD-WIN10 for the Notepad application. In this case, if User A tries to log into CHNPROD-WIN10 using the Domain accounts of CHNWinDom-01, PAM360 will allow them to connect to the Notepad application only.

Scenario 2: RemoteApp is configured in the Windows Domain resource

RemoteApp is configured at a resource-level in CHNWinDom-01 for the Notepad application. If User A tries to log into CHNPROD-WIN10 using the Domain accounts of CHNWinDom-01, PAM360 will allow unrestricted access to the CHNPROD-WIN10 resource. That is because, in this case, User A's target resource is not the Windows Domain resource for which the RemoteApp is configured. The domain accounts belonging to CHNWinDom-01 are only being used to log into the target resource, which is CHNPROD-WIN10 and User A's View level access to CHNPROD-WIN10 will be invoked as it has no RemoteApp configuration to override it.

Scenario 3: Windows resource and Windows Domain resource are configured with different RemoteApps.

At a resource-level, Notepad is configured as the RemoteApp for CHNPROD-WIN10 and Calculator is configured for CHNWinDom-01.
If User A tries to log into CHNPROD-WIN10 using the domain accounts belonging to CHNWinDom-01, they will be able to access only the Notepad application.
Similarly, if they try to access CHNWinDom-01 using the domain accounts, they will be able to access the Calculator. To access the Calculator application instead, User A must log into CHNWinDom-01 using one of the domain accounts available.

3.6 Configuring Connection Settings for Accounts

Customize the accounts added to PAM360 using the advanced configuration settings provided by PAM360. Through this customization, you can optimize SSH, RDP, and VNC connections launched from PAM360 and improve the overall user experience. Please note that all the configuration changes made here will be applied locally to the remote system also.

Refer to the help section **Connection Settings for Accounts** to know more in detail.

3.7 Configuring Gateway Settings for Remote Sessions

Customize gateway settings from the **Admin** tab to set up a different port, customize HTTP header log settings, choose SSL protocols to be used for securing remote connections initiated from the PAM360 interface. Here, you can also edit and control the cipher suites used for SSL communication.

Refer to the help section **Gateway Settings** to know more in detail.

3.8 Configuring SSH Command Control (Filtering)

SSH command control (filtering) is a feature that allows users to execute a set of predefined commands in remote sessions. In PAM360, this is achieved by configuring command groups at different group levels that include accounts, resources, and resource groups. The entire process minimizes the privilege for highly privileged accounts, thus making them more secure and constrained from internal exploitation.

Click here to learn how to configure SSH command control (filtering) in detail.

Connection Settings for Accounts

PAM360 offers advanced configuration settings for remote connections added to it. Use these settings to customize SSH, RDP, and VNC connections, thereby improving the overall user experience while initiating remote sessions from PAM360 to the respective remote resources. Some of the advanced settings include changing the SSH terminal type, modifying the desktop composition for RDP connections, changing the encoding type of VNC connections, etc. PAM360 provides a centralized configuration that unifies the functionalities of SSH, RDP, and VNC connections for ease of use. Remember, all the changes to the settings made here will be applied locally to the remote resources as well.

You will learn the following topics in this document:

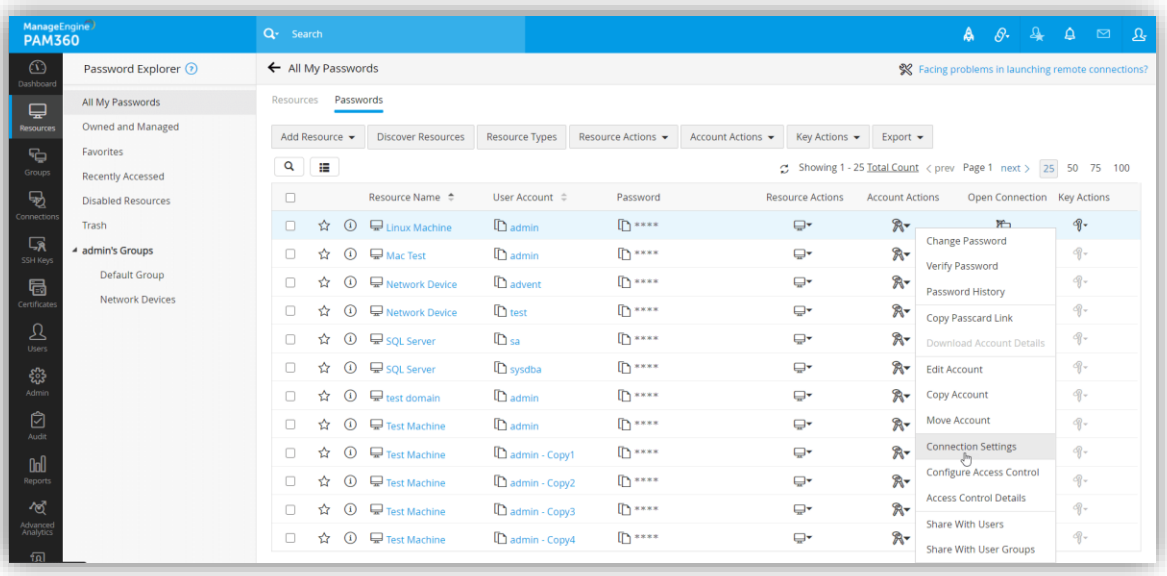
1. **Steps to Configure**
2. **Connection Settings for Different Connection Types**
3. **Glossary of Terminologies and Definitions**

1. Steps to Configure

Use the below steps to configure Connection Settings either for an individual account or for multiple accounts in bulk:

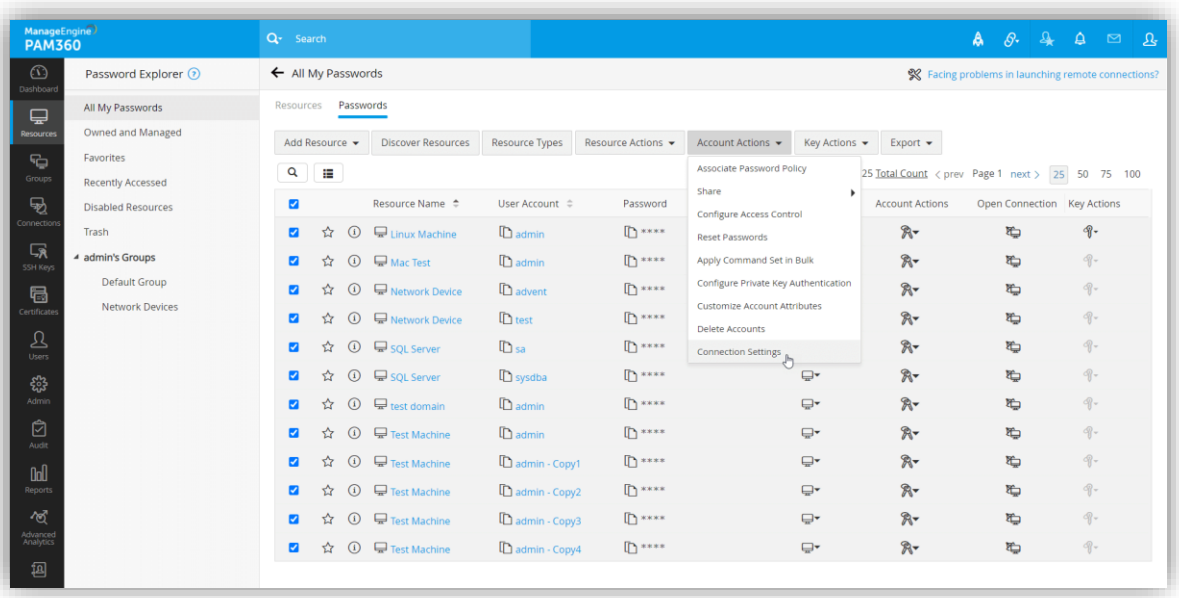
1. To configure Connection Settings for an individual account:

Navigate to the **Resources** tab and switch to the **Passwords** tab. Here, click the **Account Actions** drop-down beside the required account and click **Connection Settings** in the drop-down. **Connection Settings** options for the selected account type (SSH/RDP/VNC) alone will open up.

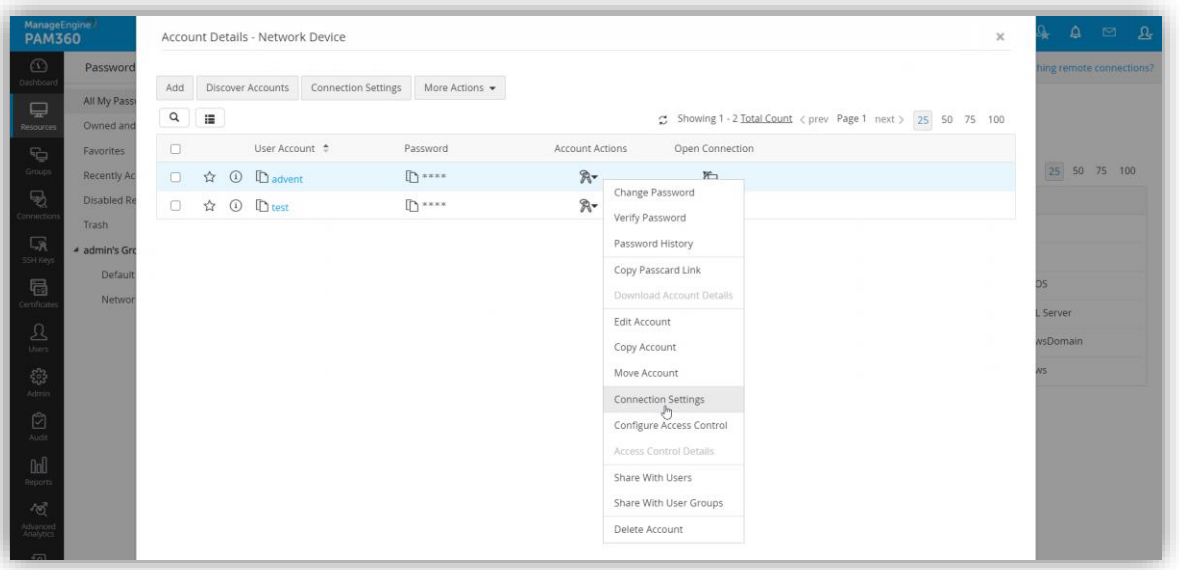


2. To configure Connection Settings in bulk:

i. In the **Passwords** tab, select a number of accounts using the check-boxes, click the common **Account Actions** drop-down at the top and click **Connection Settings** in the drop-down. In this case, **Connection Settings** options for all three types of accounts will open up to facilitate applying settings for multiple accounts in bulk.

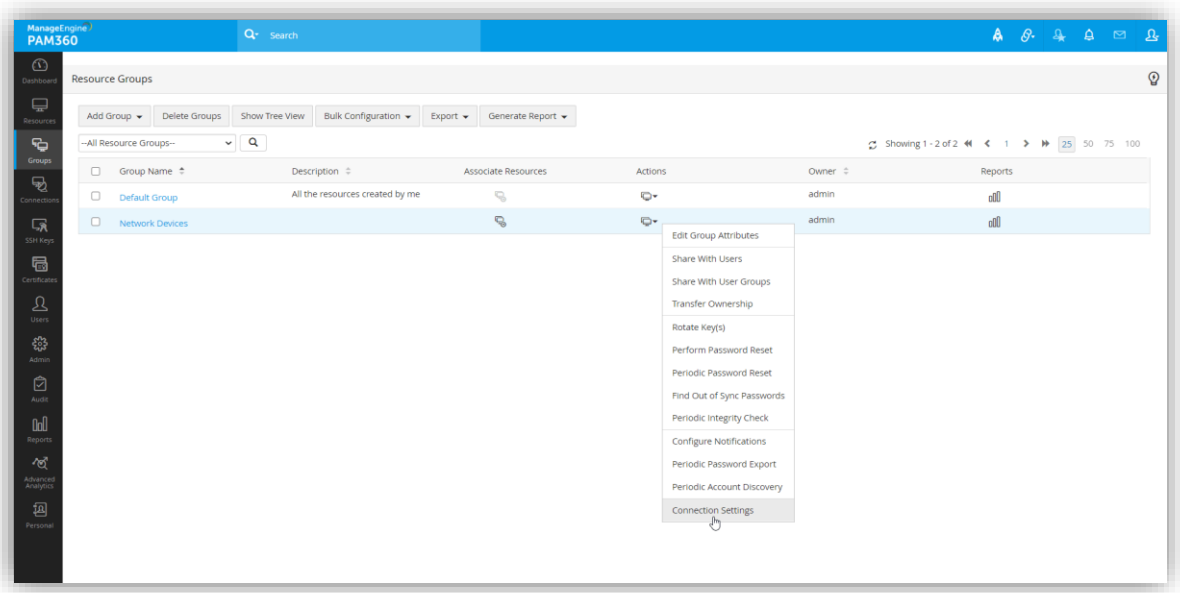


ii. To apply Connection Settings for a group of accounts within a particular resource, switch to the **Resources** tab and click the name of the required resource. All accounts added under this resource will be displayed in the **Account Details** dialog box. Here, either click **Account Actions** beside particular account or select multiple accounts using the check-boxes and click the common **Connection Settings** option available at the top. Any connection settings applied here will be confined to the accounts of the selected resource only.



3. To configure Connection Settings for a group of resources:

i. Navigate to the **Groups** tab. Click the **Actions** drop-down beside the required resource group name and click **Connection Settings** in the drop-down. **Connection Settings** options for all three types of accounts will open up to facilitate applying settings for all the accounts within the selected resource group. Click here to learn more about how to add resource groups in PAM360.



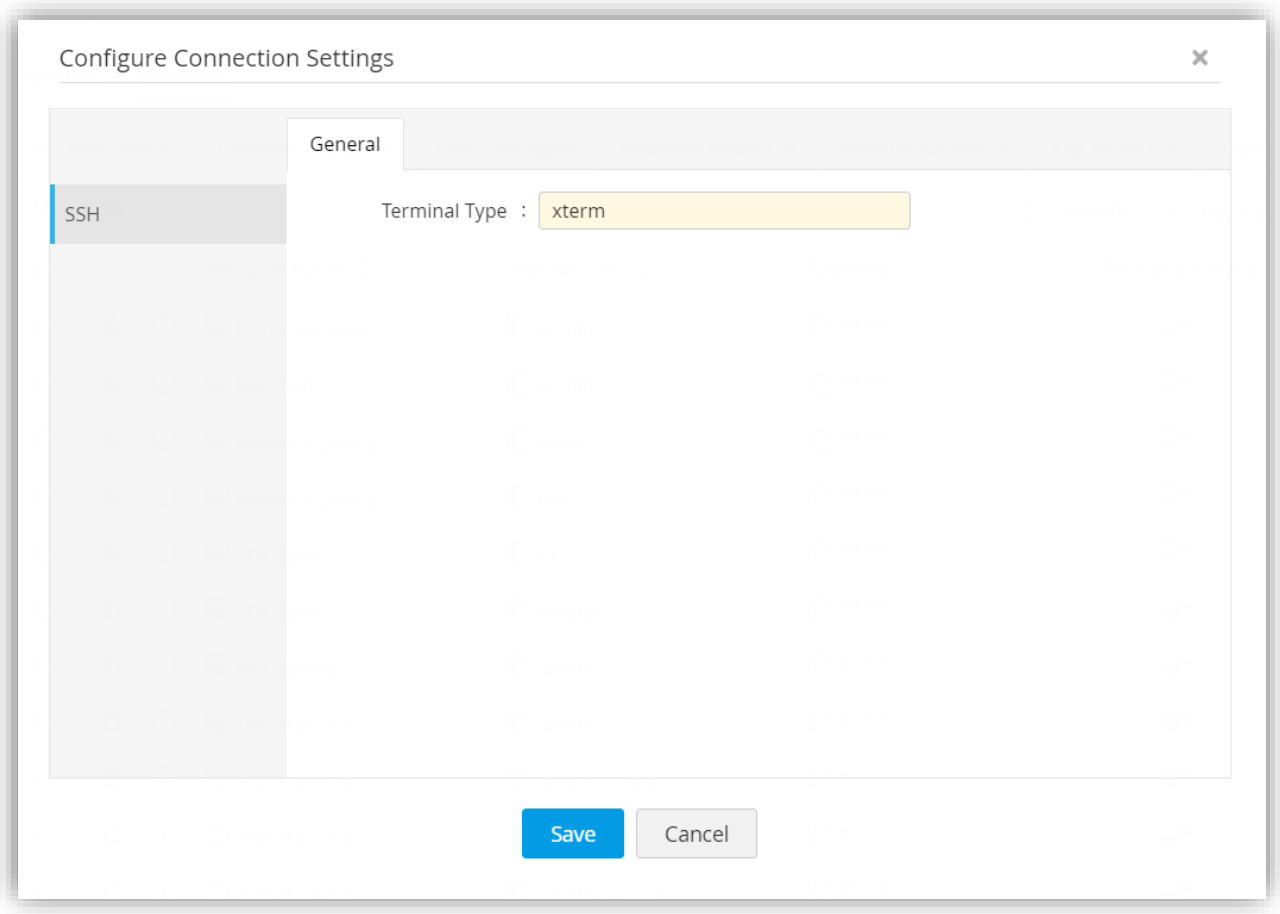
4. There are three types of connections for which PAM360 offers **Connection Settings**.
    i. **SSH Connection**
    ii. **RDP Connection**
    iii. **VNC Connection**

2. Connection Settings for Different Connection Types

2.1 SSH Connection

Typically, terminal types and corresponding sets of commands vary from one SSH device to another. For example, if the SSH device added to PAM360 is IBM AS400, but the terminal type is a Linux terminal type, say 'xterm', a few commands will not work as expected, thereby reducing the efficiency considerably. Hence, it is essential to define the exact terminal type for each SSH device added to PAM360 so that PAM360 can emulate the terminal and be prepared to process the types of commands used on that particular terminal. All you need to do is to type in the name of the Terminal Type in the text field for the selected SSH device and click **Save**.

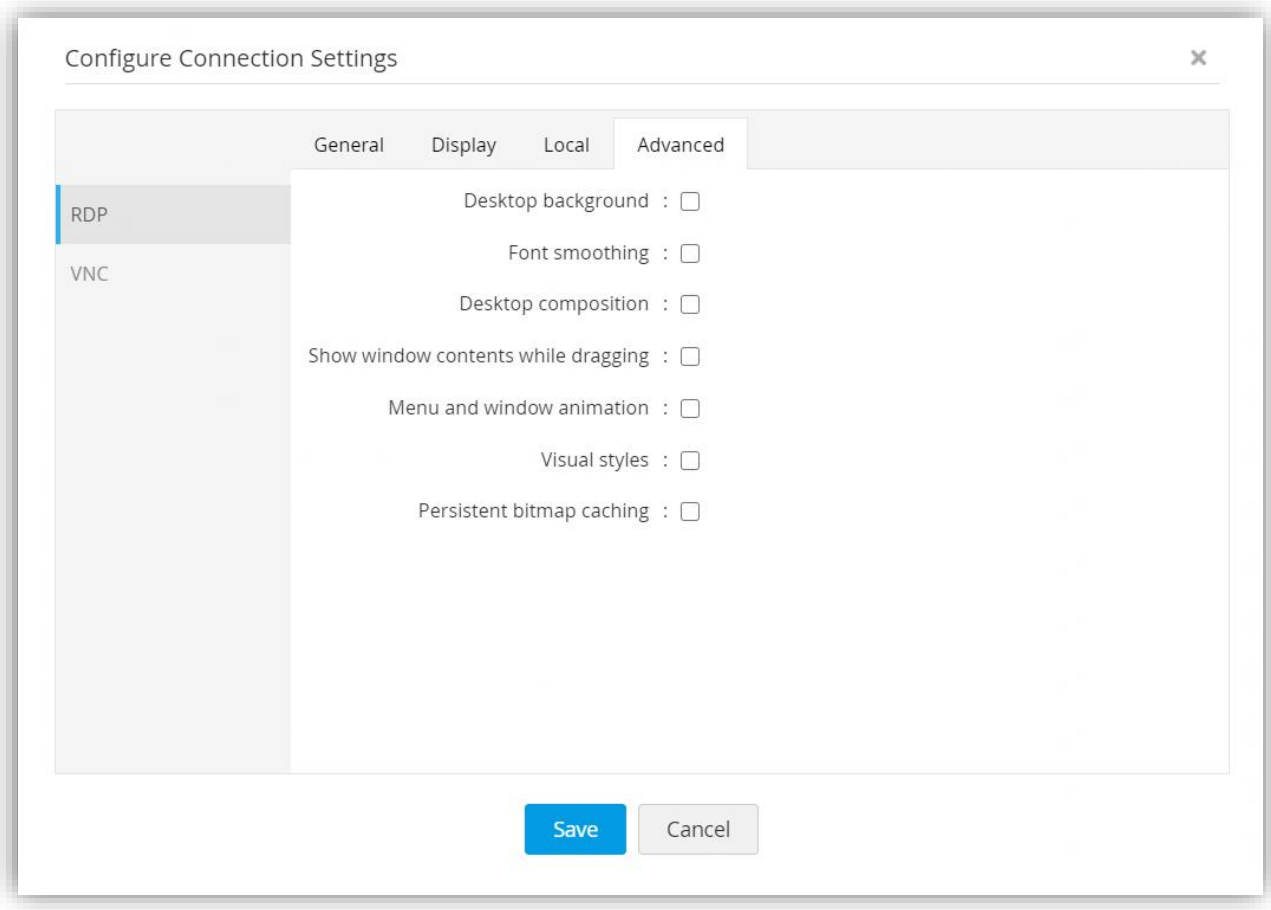
Click here for a brief list of terminal emulators.



2.2 RDP Connection

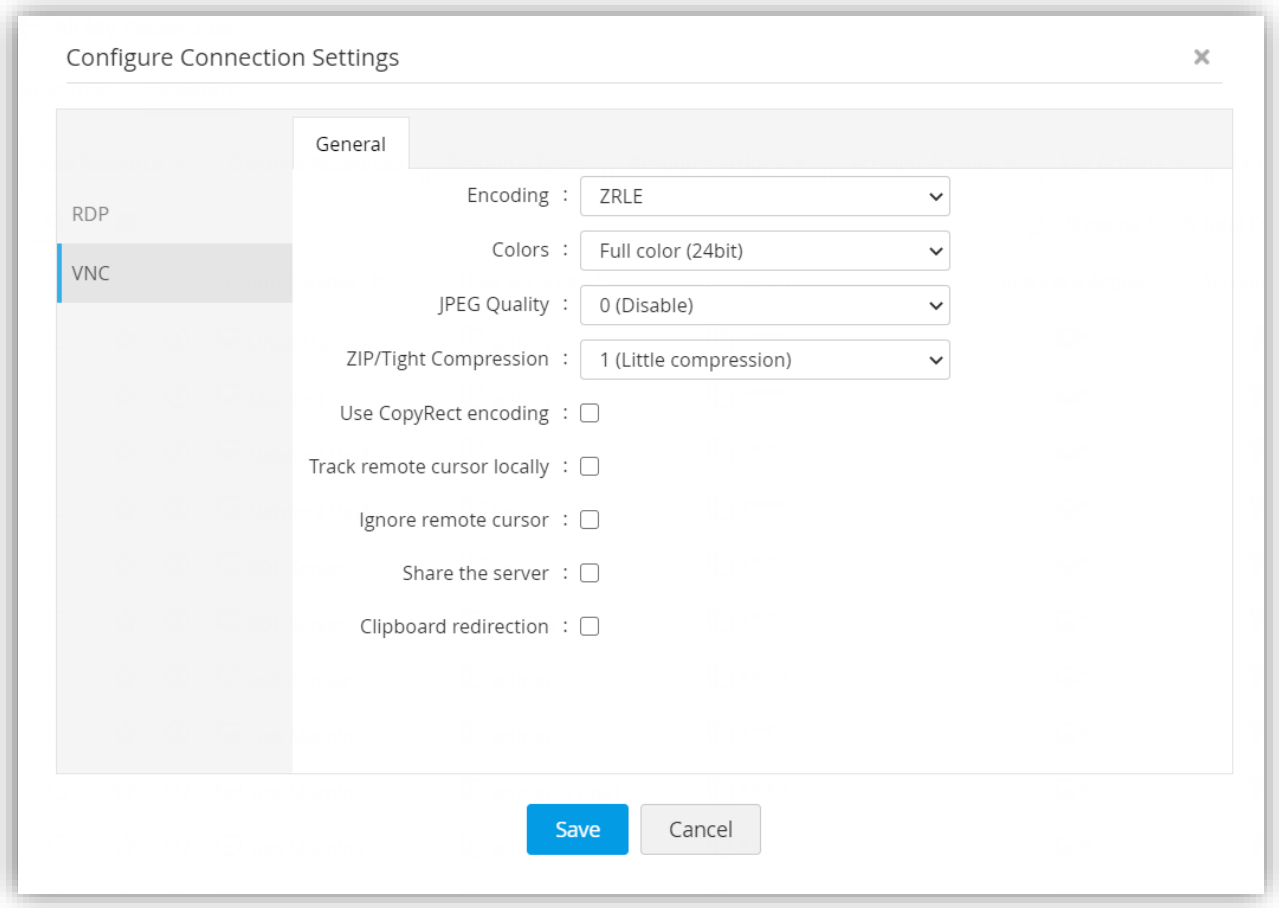
Connection settings for RDP connections are divided into four types - **General, Display, Local,** and **Advanced.**

- General - Here, you can find options to change the keyboard language in the remote Windows machine. Click the **Connect to console session** check-box to initiate a console session to the remote machine. Please note that a console window will not open when a remote session is initiated.
- Display - Change the color intensity of the display and/or disable remote cursor for the remote session.
- Local - Choose whether to play audio in the remote machine, or allow access to the drives, clipboard, printer. Select the **Text only** option to make the remote session text-only.
- Advanced - This section comprises of options that will decide how the remote session is visually rendered and how it can enhance the client experience during a remote session. Click here for the Microsoft documentation on these settings to learn in detail about each of the options.



2.3 VNC Connection

For VNC sessions, use the following settings to enhance the user experience and also enforce some controls over the remote sessions. Choose an encoding format from the available list: ZRLE/Raw/Tight/Hextile/CopyRect. Also, choose how to display colors, the JPEG quality, and the extent to compress the ZIP files. Additionally, you can disable the remote cursor/switch on the tracker for the cursor on the local machine.



3. Glossary of Terminologies and Definitions

Term	Definition
ZRLE	ZRLE stands for Zlib Run-Length Encoding. It is considered to be best for low-bandwidth network environments.
Raw	The raw encoding sends width*height pixel values. Raw encoding minimizes processing time and increases connection speed when the server and VNC viewer are on the same machine.
Tight	Tight encoding is considered to be the best choice for low-bandwidth network environments such as e.g. slow modem connections. Tight encoding uses zlib library to compress raw pixel data, but it pre-processes data to maximize compression ratios and to minimize CPU usage on compression. JPEG compression may be used to encode color-rich screen areas.

Hextile	Hextile encoding is considered to be the best choice for high-speed network environments such as Ethernet local-area networks.
CopyRect	Copy Rectangle or CopyRect encoding is useful when data is being moved; the only data sent is the location of a rectangle from which data is to be copied to the current location.

SSH Command Control (Filtering) in PAM360

PAM360 can launch remote connections via SSH protocol to perform the desired operations by executing the relevant commands. The SSH Command Control (filtering) feature allows you to configure a set of predefined command lists in remote sessions by associating command groups with accounts, resources, and/or resource groups, as required.

Say, if you are a user having access to a particular resource with applied command control, you can execute only those commands within the allowed command lists, thereby ensuring security with an enhanced scope of access control.

SSH Command Control (Filtering) Workflow -
Add Command → Associate Command to Command Group → Configure Command Group at the Required Level (Accounts, Resources, and/or Resource Groups)

> **Note:**
>
> The command and command group operations performed in PAM360 will have a trail of records in the resource audit section with the relevant operation types and reasons.

At the end of this document you will have learned the following topics:

1. Enable Command Control Access
2. Manage Commands
3. Manage Command Groups
4. Configure SSH Command Control
5. Execute Filtered Commands

6. How does the Precedence Works in Real-Time

1. Enable Command Control Access

The first step to SSH command control (filtering) is enabling command control-related permissions for custom roles based on required privileges. To do this, navigate to '**Admin >> Customization >> Roles >> Add Role >> Privilege Elevation**' and do the following:

a. **Manage Command Lists**
   Enabling this option lets the user manage the command list and command groups in PAM360. This role enabled users can create new commands and command groups with operations that include edit, delete, associate, and dissociate.

b. **Associate Command Groups**
   Users enabled with this role can associate/dissociate a command group with/from the accounts, resources, and resource groups and view the commands and command groups from the **Manage Command Lists** window.

c. **Use Command Control**
   Users with this role can execute only the predefined commands associated with the SSH-based resources. By enabling this role, the user privilege will be limited by not allowing SSH commands apart from the predefined list. Administrator, Privileged Administrator, Password Administrator, and Connection users will be given this role by default. Also, users disabled with this role cannot take any connection for the accounts configured with SSH command control.

2. Manage Commands

Important Note:

Before proceeding with the command management, users with the Manage Command Lists and Associate Command Groups roles have to verify the following criteria for the proper execution of commands in the launch SSH console:

1. The commands added to the PAM360 should have the valid input.
2. The target system has to be checked for the alias commands if any, and it has to be considered the same while adding it to the PAM360 Commands tab.

Navigate to '**Admin >> Privilege Elevation >> Manage Command**'.

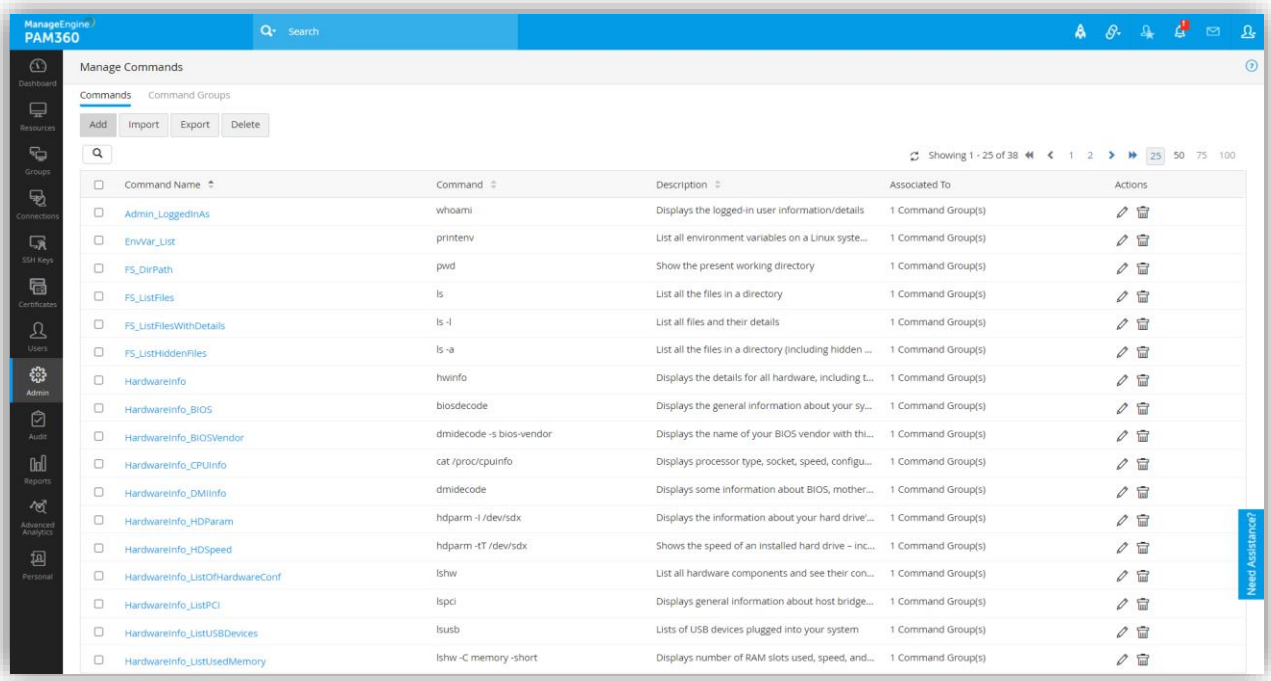
From the **Commands** tab under the **Manage Commands** window, you can perform the necessary operations related to the commands, which include Add, Import, Edit, Delete, and Export. The following sub-sections will guide you with a brief step-by-step procedure about each operation mentioned above:

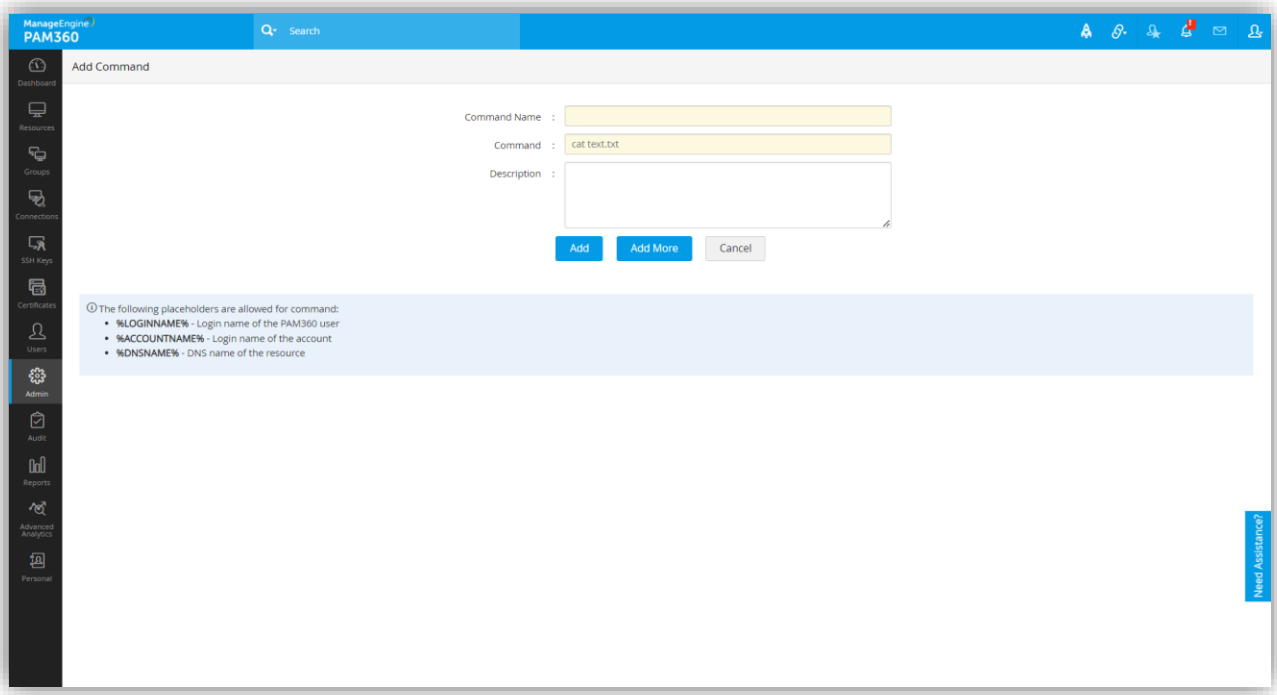
a. Add Command

You can add commands to the command list in two available methods:

i. Adding Command Manually

1. In the **Commands** tab, click the **Add** button.
2. In the window that opens, enter the **Command Name**, **Command**, and **Description**.
3. Upon entering the respective fields, click the **Add** button to add the command or **Add More** to add the subsequent commands.





The added command(s) will be available in the **Commands** tab of the **Manage Commands** window.

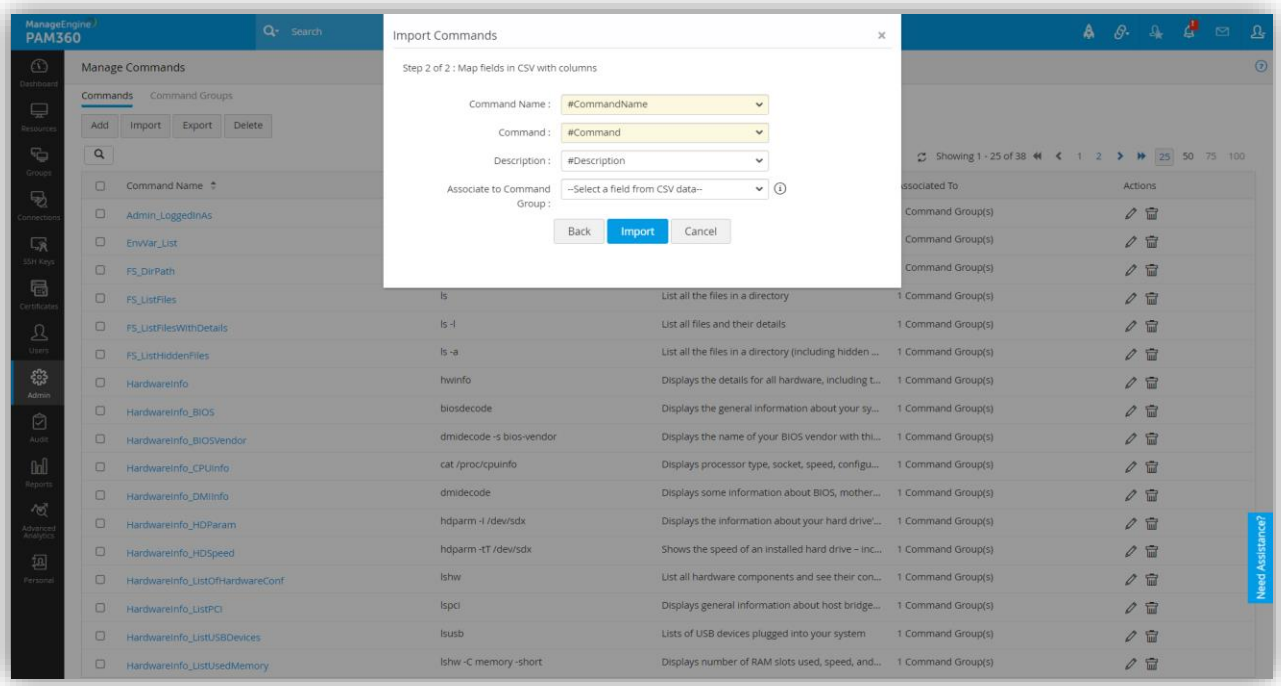
ii. Import Commands from CSV

1. In the **Commands** tab, click the **Import** button.
2. In the pop-up that appears, select the file **Type**, provide the directory of the file in the **Attach File** field and click **Next**.

Tip:

For a better understanding of the CSV file format, you can manually add a few commands and command groups and export them as a CSV file for reference.

3. If you select the file type as **Password protected ZIP file**, enter the file name in the zip file and the password to access the file in the zip.
4. The import inventory of the command list contains four fields by default. Out of these four fields, **Command Name** and **Command** are mandatory, and the CSV file can hold the values of these fields in any order. You can also associate the commands to the command groups from here.



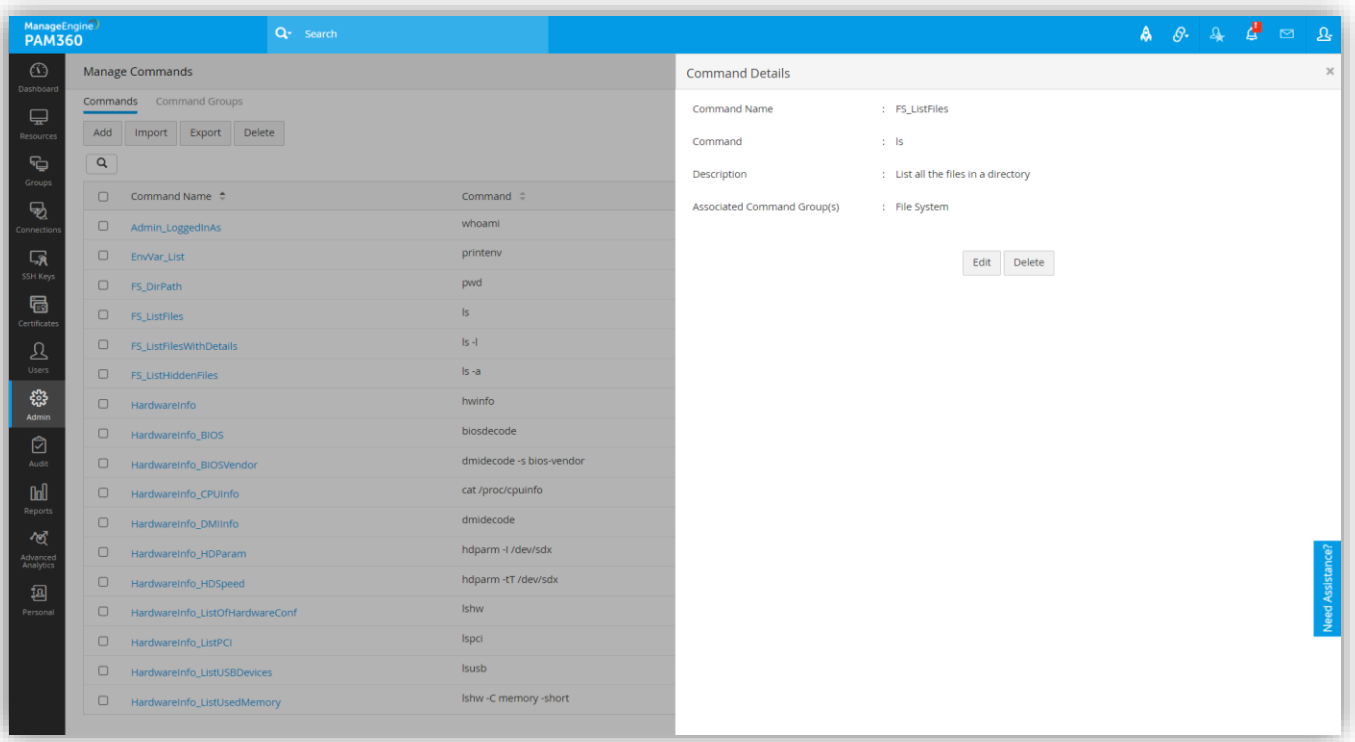
Note:

Mapping the Associate to Command Group field will associate the commands with the command groups of the same names. If a command group name in the CSV file does not exist in the Command Groups tab of Manage Command Lists, a new command group will be created in the same name, and the respective command will be associated with it.

5. Select the fields in the CSV to map to the corresponding attributes and click **Import**.

The commands imported from the CSV file will be available in the **Commands** tab of the **Manage Commands** window.

Click on the desired command from the command list. From the **Command Details** window that opens, you will get the command information, and you can also perform operations that include **Edit** and **Delete**.



b. Edit Command

1. In the **Commands** tab, click the **Edit Command** icon under **Actions** beside the desired command or the **Edit** button from the **Command Details** window.
2. In the window that opens, update the necessary fields and click **Save** to edit the existing command details.

> **Note:**
>
> Select the required command groups available in the Associate to Command Group field to associate the command to the respective command group(s).

c. Delete Command(s)

1. In the **Commands** tab, click the **Delete Command** icon under **Actions** beside the desired command or the **Delete** button from the **Command Details** pop-up.
2. In the pop-up that opens, click on the **Delete** button to delete the command from the command list.
3. To delete the commands in bulk:
    i. Select the desired commands to be deleted.
    ii. Click the **Delete** button on the top pane.
    iii. Click **Delete** to delete the selected commands in bulk.

> **Note:**
>
> Deleting the command from the Commands tab will dissociate it from the existing command group, if any, and will remove it permanently from the command list.

d. Export Commands

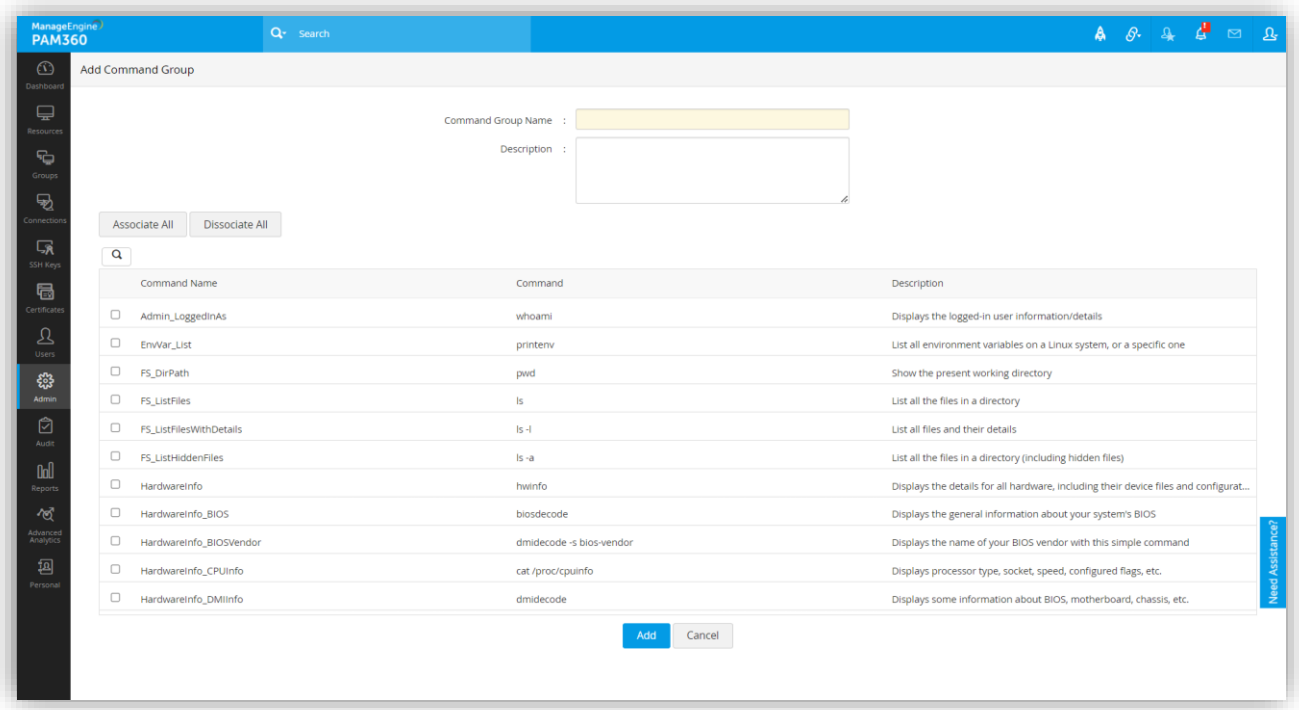
You can export the commands available in the **Commands** tab of the **Manage Commands** window. From the **Commands** tab, click on the **Export** button to export all the commands as a CSV file. Upon execution, a CSV file with all the available commands will be downloaded in the default directory as set in your browser.

3. Manage Command Groups

After managing the desired commands, you can start performing the command groups operations that include Add, Edit, Associate/Dissociate and Delete from the **Command Groups** tab under the **Manage Commands** window. The following sub-sections will guide you with a brief step-by-step procedure about the different operations mentioned above:

a. Add Command Group

1. In the **Command Groups** tab, click the **Add** button.
2. In the window that opens, enter the Command Group Name and Description and click **Add**.



Note:

Before submitting the confirmation to add a command group, you can select the desired commands from the below command list to associate them with this newly added command group.

Click on the desired command group from the **Command Groups** tab. From the **Command Group Details** window that opens, you will get the command group information with the associated command details, and you can also perform operations that include Edit and Delete.

b. Edit Command Group

1. In the **Command Groups** tab, click the **Edit Command Group** icon under **Actions** beside the desired command group or the **Edit** button from the **Command Group Details** pop-up.
2. In the window that opens, update the necessary and click **Save** to edit the command group detail.

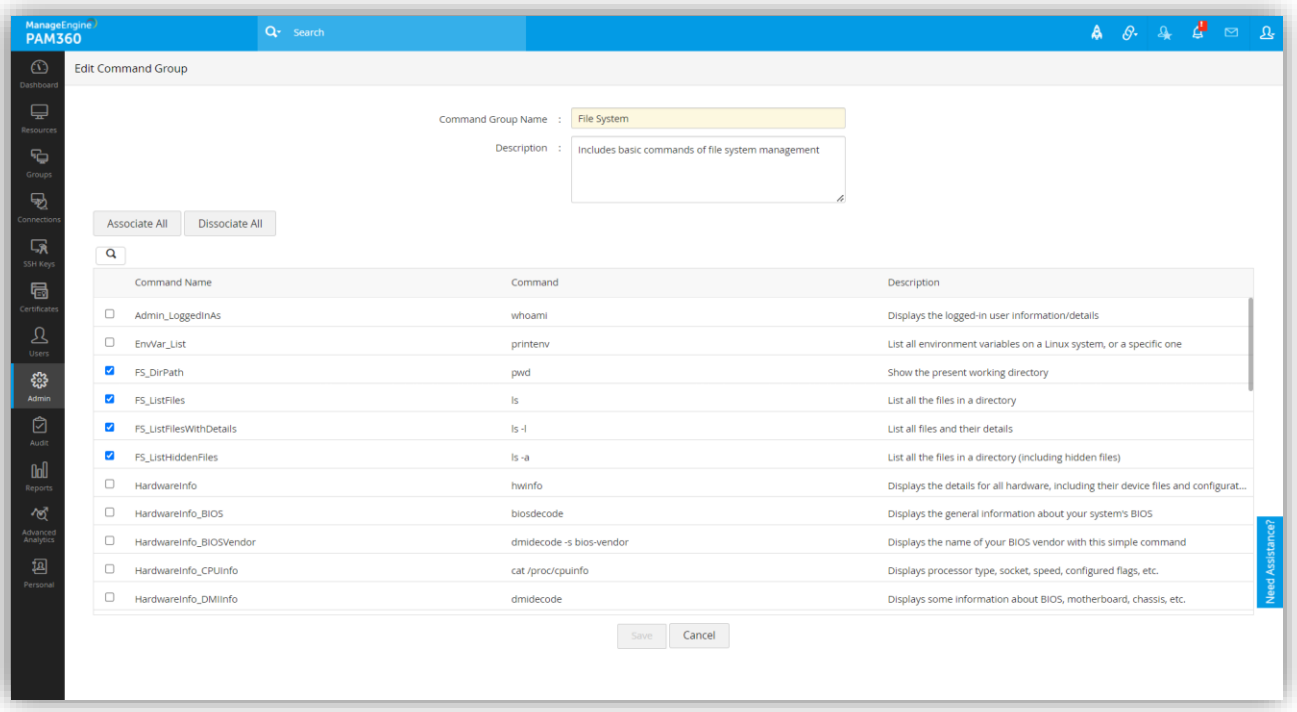
c. Delete Command Group(s)

1. In the **Command Groups** tab, click the **Delete Command Group** icon under **Actions** beside the desired command group or the **Delete** button from the **Command Group Details** pop-up.
2. In the pop-up that opens, click **Delete** to delete the command group from the command group list.
3. To delete the command groups in bulk:
    i. Select the desired command groups to be deleted.
    ii. Click the **Delete** button on the top pane.
    iii. Click **Delete** to delete the selected command groups in bulk.

> **Note:**
>
> Deleting the command group will delete it permanently, but will not delete the commands associated with it.

d. Associate/Dissociate Command(s) with/from Command Group(s)

1. In the **Command Groups** tab, click the **Edit Command Group** icon under Actions beside the desired command group or the **Edit** button from the **Command Group Details** pop-up.
2. Select/deselect the command(s) from the available command list to associate/dissociate the commands with/from the command group.
3. Click **Save** to apply the changes.



Note:

You can also associate commands with the command group while adding a new command group.

4. Configure SSH Command Control

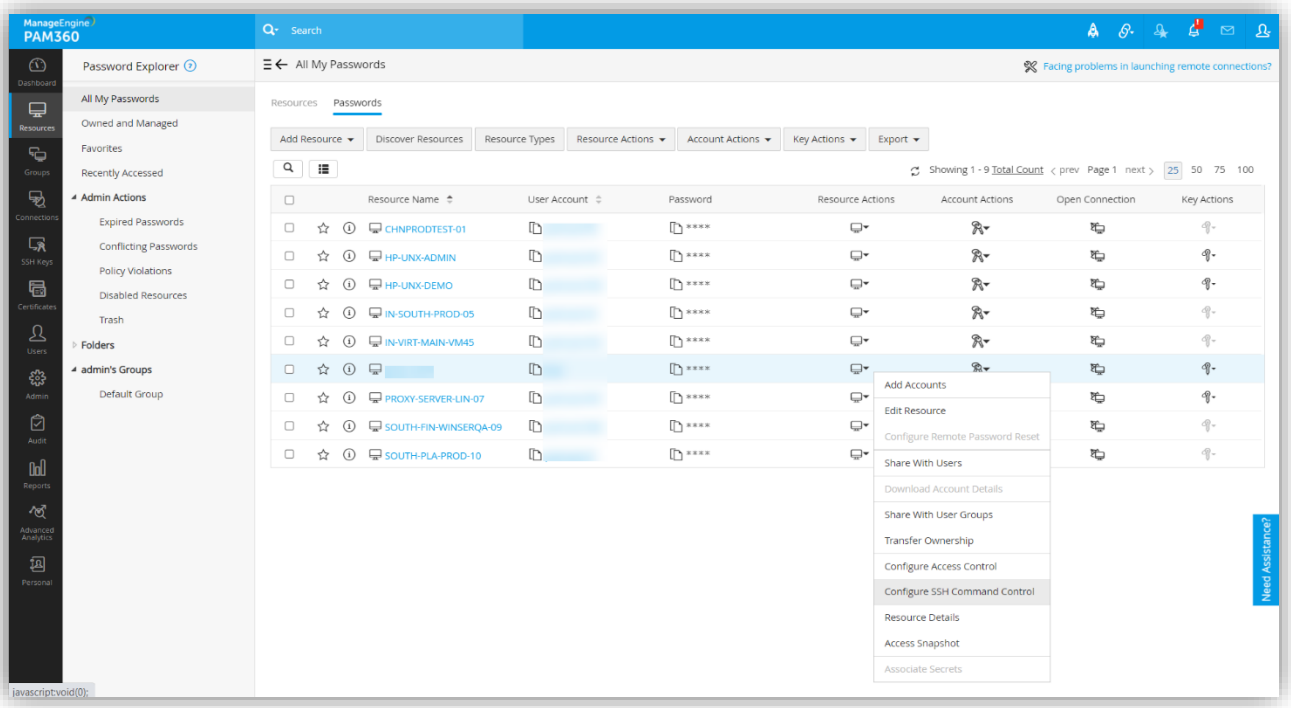
Once you are ready with the desired command groups, you can start configuring them via SSH command control at the accounts, resources, and resource groups level. The below sub-sections will describe you briefly about the step-by-step process for configuring SSH command control at different levels:

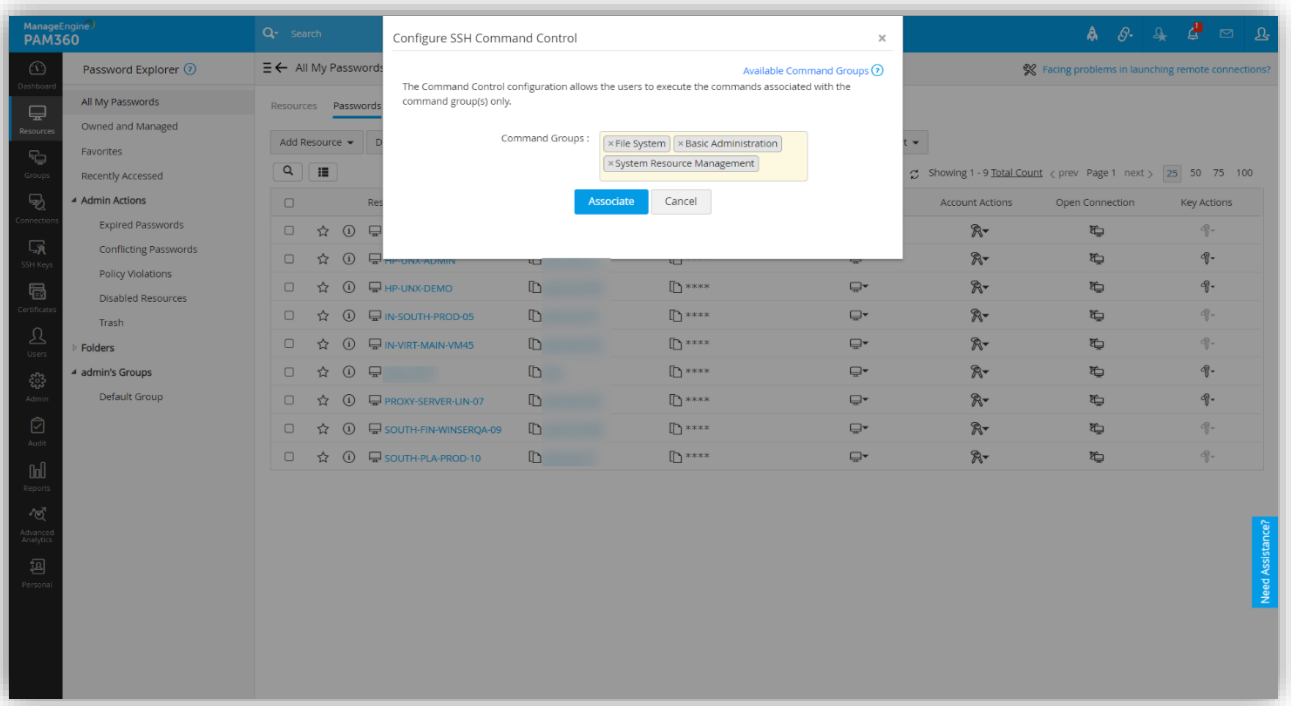
Important Note:

We strongly suggest using command control (filtering) with configured access control. This is to restrict users from accessing the shared accounts passwords. If an account password is accessible as plain text, the users can use any third-party SSH clients to execute commands on their own without any command control restrictions.

a. Configure Command Control to Account(s)

1. Navigate to '**Resources >> All My Passwords >> Resources**' and click the desired SSH resource.
   [or]
   Navigate to '**Resources >> All My Passwords >> Passwords**'.
2. In the page that appears, click the **Account Actions** drop-down beside the desired account and select **Configure SSH Command Control**.
3. In the pop-up that opens, select the required command group(s) to be associated with the account and click **Associate**.





Now, the command group(s) is(are) associated successfully, and the command control is enabled for the account.

Note:

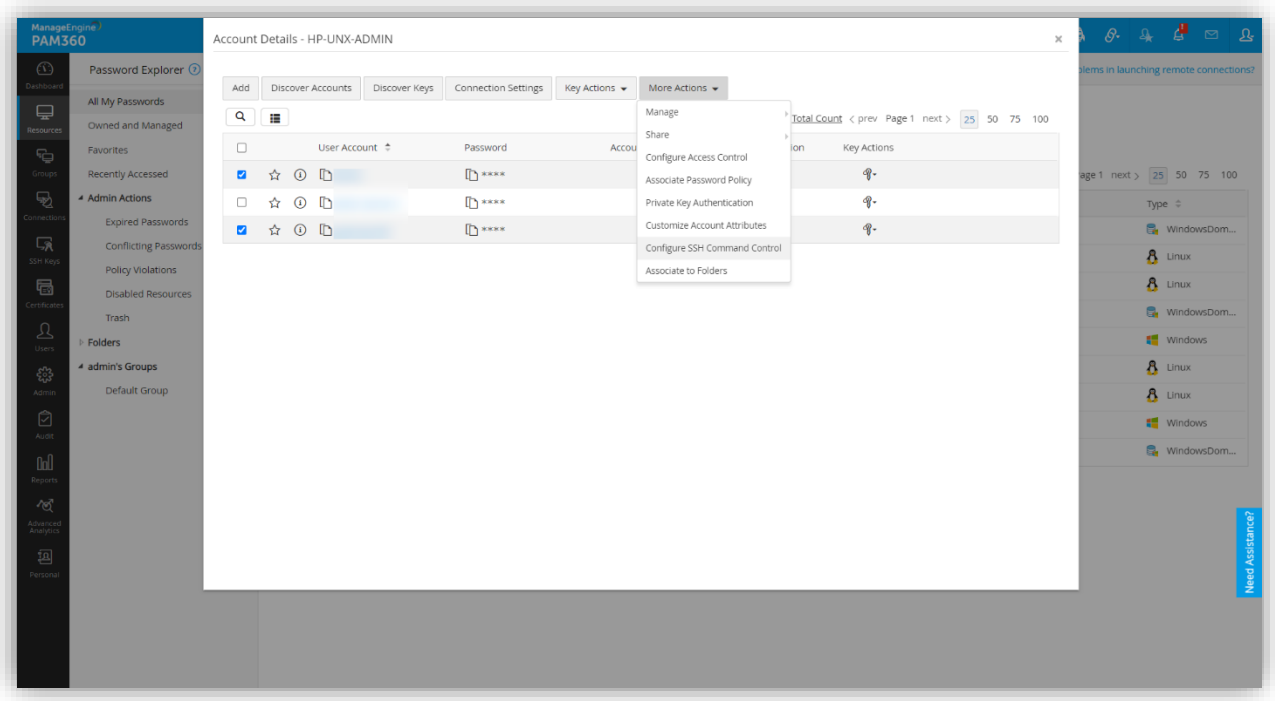
Deselect the command group(s) to dissociate the command group from the account or click the Dissociate button to revoke the command control for the account.

4. To configure command control in bulk:

   i. Select the desired accounts, click the **More Actions** drop-down and select **Configure SSH Command Control**.
   [or]
   Select the desired accounts, click the **Account Actions** drop-down at the top pane and select **SSH Command Control** in the **Configure** section.

   ii. In the pop-up that opens, select the command group(s) to be associated with the accounts and click **Associate**.

   Now, the command group(s) is(are) associated successfully in bulk, and the command control is enabled for the selected accounts.



b. Configure Command Control to Resource(s)

1. Navigate to **Resources >> All My Passwords >> Resources**.
2. Click the **Resource Actions** drop-down beside the desired SSH resource and select **Configure SSH Command Control**.
3. In the pop-up that opens, select the required command group(s) to be associated with the resource and click **Associate**.

   Now, the command group(s) is(are) associated successfully, and the command control is enabled for the resource.

Note:

Deselect the command group(s) to dissociate the command group(s) from the resource or click the Dissociate button to revoke the command control for the resource.

4. From the **Resources** tab, to configure command control in bulk:

   i. Select the desired SSH resources, click the **Resource Actions** drop-down at the top pane, and select **SSH Command Control** in the **Configure** section.
   ii. In the pop-up that opens, select the required command group(s) to be associated with the resources and click **Associate**.

   Now, the command group(s) is(are) associated successfully in bulk, and the command control is enabled for the selected resources.

c. Configure Command Control to Resource Group(s)

1. Navigate to the **Groups** tab.
2. Click the **Actions** drop-down beside the desired resource group and select **Configure SSH Command Control**.

3. In the pop-up that opens, select the required command group(s) to be associated with the resource group and click **Associate**.

   Now, the command group(s) is(are) associated successfully, and the command control is enabled for the resource group.

> **Note:**
>
> Deselect the command group(s) to dissociate the command group(s) from the resource group or click the Dissociate button to revoke the command control for the resource group.

4. To configure command control in bulk:

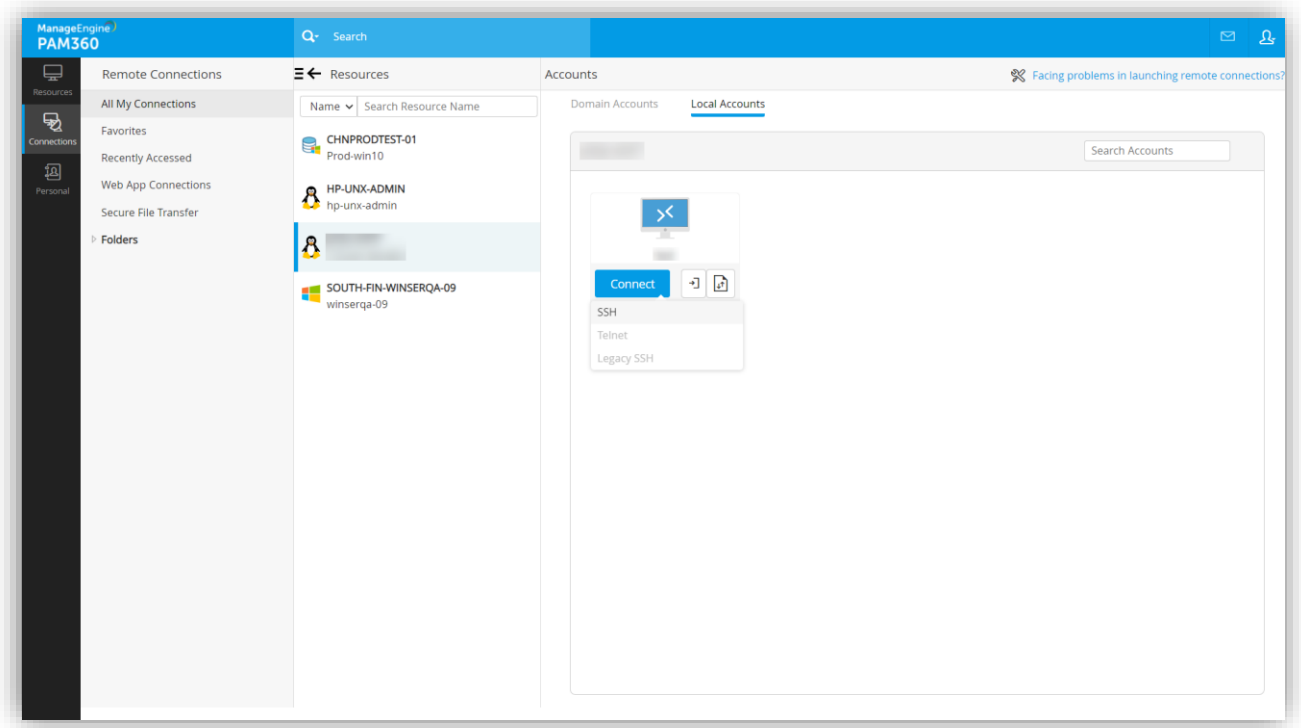
   i. Select the desired SSH resource groups, click the **Bulk Configuration** drop-down at the top pane and select **SSH Command Control** in the **Configure** section.
   ii. In the pop-up that opens, select the required command group(s) to be associated with the resources and click **Associate**.

   Now, the command group(s) is(are) associated successfully in bulk, and the command control is enabled for the selected resource groups.

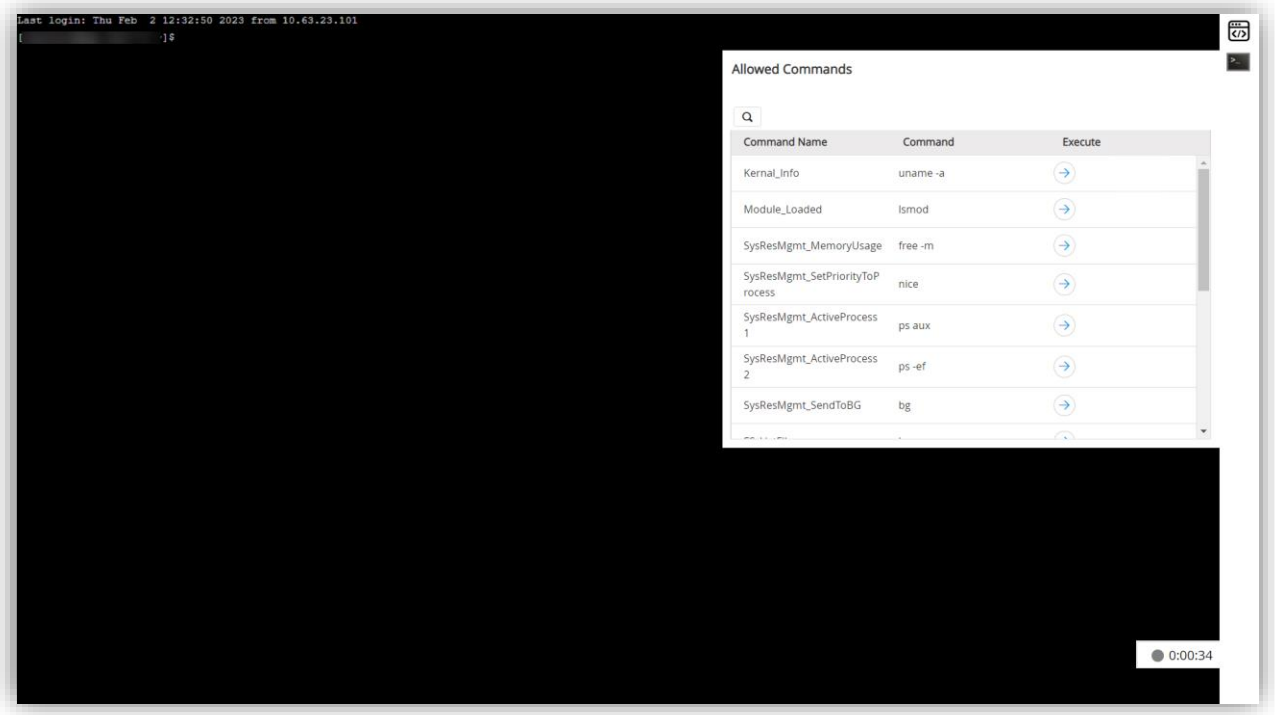
5. Execute Filtered List

Users enabled with the Use Command Control role can execute only the commands applied at the different group levels. To execute the allowed list of commands:

1. Launch a remote session for the desired account using the SSH protocol.



2. In the session that opens, you will find a set of predefined allowed list of commands associated to the logged in SSH account.
    a. Hover on the right pane and click on the **Execute** icon beside the desired command from the command list to execute the command in the launch SSH console.
    b. Click on the **Preview** icon on the right pane to see the command execution logs of the SSH session.



Note:

- Configuring SSH command control will allow users to execute the commands that are predefined by the administrator.
- The users will not be able to manually execute any commands in the accounts configured with SSH command control.
- Accounts configured with SSH command control will restrict remote sessions for users without the Use Command Control role.

6. How does the Precedence Work in Real-Time?

Case 1:

If an SSH connection to a device gets SSH command control configuration from an account, resource, and resource group level, then the authorized SSH session of that particular account will take the commands associated via command groups at the

account level.

> **Note:**
>
> The precedence will be given to the lower level (Account << Resource << Resource Group) when configured with different command groups at different group level.

Case 2:

Similarly, if an SSH connection to a device gets SSH command control configuration from the resource and resource group level, then the authorized SSH session of that account will take the commands configured via command groups at the resource level.

Case 3:

If an SSH connection to a device gets SSH command control configuration from different resource groups, then the authorized SSH session will take the consolidated commands in the command groups configured with the different resource groups.

PAM360 Remote Connect

PAM360 Remote Connect is an independent desktop client for Windows, designed to help you launch direct remote connections via password-less login to Windows and SSH-based target resources without needing to install multiple remote clients or a web browser.

To achieve this, Remote Connect utilizes the PAM360 server's API to act as a standalone client for remote connections that is independent of the PAM360 web application. Similar to PAM360's web application, PAM360 Remote Connect ensures seamless operation of the authentication and remote access mechanisms for RDP and SSH-based connections. Essentially, PAM360 Remote Connect acts as both the Microsoft Terminal Services Client (MSTSC) client and SSH PuTTY client rolled into a single, lightweight application with auditing capabilities.

To learn how to configure the PAM360 Remote Connect application in a user endpoint and attain remote sessions from it, refer to the Configuring PAM360 Remote Connect section.

As long as the source machine and the target endpoints can achieve connectivity through the required RDP/SSH protocols, PAM360 Remote Connect can be installed in the individual workstations of users and used to launch remote connections to the endpoints by leveraging PAM360's access control functions.

However, with a configured SSH proxy, the source machine connectivity with the PAM360 server is sufficient to attain the remote connection. To learn about configuring the SSH Proxy for remote sessions in the PAM360 Remote Connect application, refer to the sections described below.

SSH Proxy for Remote Connections

To avoid direct communication between the PAM360 Remote Connect application and the target endpoints during remote sessions for enhanced security, configure the SSH proxy available in PAM360 for the PAM360 Remote Connect application.

1. Roles Required to Perform this Operation

- Privilege Administrator
- Administrator

- Any custom role with the 'Configure SSH Proxy' enabled operation

2. Prerequisites

Below are the prerequisites for the SSH proxy to work seamlessly to attain a secured remote connection:

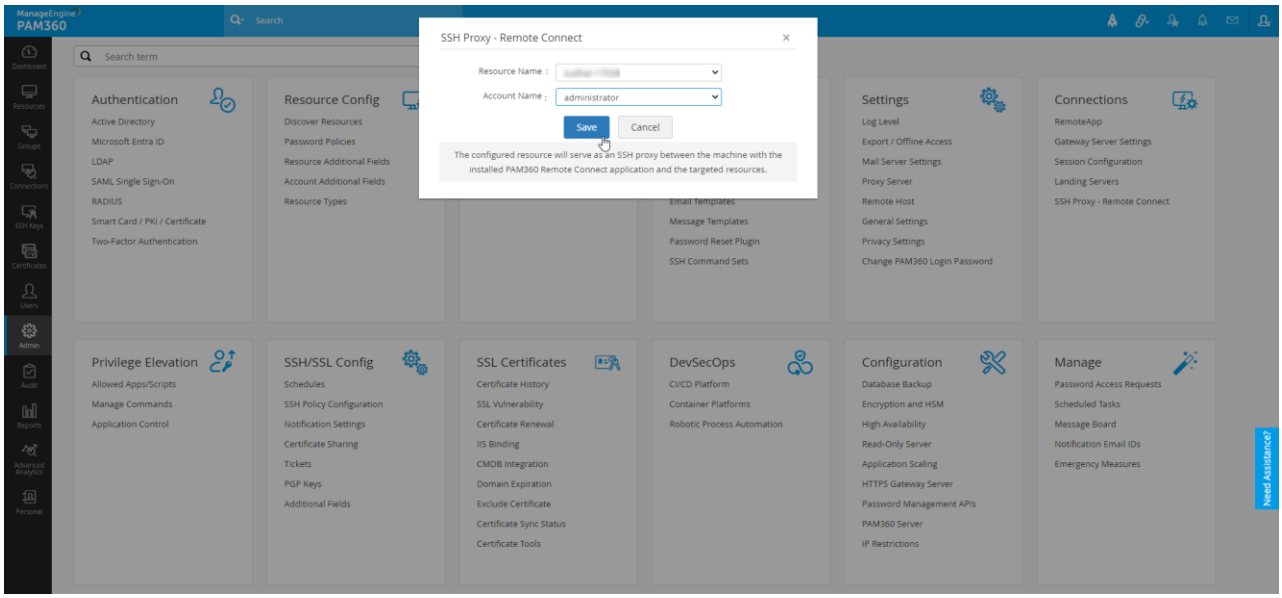
- Add the endpoint that will act as the proxy between the PAM360 Remote Connect and the target machine as a resource in PAM360.
- The user machine installed with the PAM360 Remote Connect must be able to communicate with the PAM360 server.
- Similarly, the PAM360 server must be able to communicate with the resource configured as proxy, and the proxy resource must be able to communicate with the target endpoints.
- Add the system property sshtunnel.tunnelapi.bindaddress=<PAM360 Installed Server's IP or FQDN> in the system_properties.conf file located in the conf folder of the PAM360 installation directory.

3. Configuring SSH Proxy for PAM360 Remote Connect

1. Log in to PAM360 and navigate to **Admin >> Connections >> SSH Proxy - Remote Connect**.
2. In the pop-up that opens, select the resource that acts as an SSH proxy in the **Resource Name** dropdown.

   > **Note:** You can also set the PAM360 installed server/resource as the SSH proxy resource.

3. Select an account from the **Account Name** dropdown, which is used to access the above-selected resource.
4. Click **Save** to make the selected resource act as an SSH proxy between the PAM360 server and the target endpoints.


ManageEngine
PAM360
Search
Search term
SSH Proxy - Remote Connect
Resource Name :
Account Name :
administrator
Save
Cancel
The configured resource will serve as an SSH proxy between the machine with the installed PAM360 Remote Connect application and the targeted resources.
Authentication
Active Directory
Microsoft Entra ID
LDAP
SAML Single Sign-On
RADIUS
Smart Card / PKI / Certificate
Two-Factor Authentication
Resource Config
Discover Resources
Password Policies
Resource Additional Fields
Account Additional Fields
Resource Types
Message Templates
Password Reset Plugin
SSH Command Sets
Settings
Log Level
Export / Offline Access
Mail Server Settings
Proxy Server
Remote Host
General Settings
Privacy Settings
Change PAM360 Login Password
Connections
RemoteApp
Gateway Server Settings
Session Configuration
Landing Servers
SSH Proxy - Remote Connect
Privilege Elevation
Allowed Apps/Scripts
Manage Commands
Application Control
SSH/SSL Config
Schedules
SSH Policy Configuration
Notification Settings
Certificate Sharing
Tickets
PGP Keys
Additional Fields
SSL Certificates
Certificate History
SSL Vulnerability
Certificate Renewal
IIS Binding
CMDB Integration
Domain Expiration
Exclude Certificate
Certificate Sync Status
Certificate Tools
DevSecOps
CI/CD Platform
Container Platforms
Robotic Process Automation
Configuration
Database Backup
Encryption and HSM
High Availability
Read-Only Server
Application Scaling
HTTPS Gateway Server
Password Management APIs
PAM360 Server
IP Restrictions
Manage
Password Access Requests
Scheduled Tasks
Message Board
Notification Email IDs
Emergency Measures
Need Assistance?

Configuring PAM360 Remote Connect

The PAM360 Remote Connect application (an independent desktop client for Windows) revolutionizes remote access by offering seamless, password-less connectivity to PAM360 resources with just one click. The remote client integrates RDP and SSH connections into a unified interface, eliminating the hassle of switching between external desktop clients. Also, the ability to launch concurrent sessions and customize SSH connections enhances user experience significantly.

This document outlines the installation process, system requirements, and operations within the interface. Read further to learn about Remote Connect in detail.

1. Benefits of Using PAM360 Remote Connect
2. Prerequisite
3. System Requirements
4. Steps to Install and Log into Remote Connect
5. Possible Operations in the PAM360 Remote Connect Interface
6. Real-time Scenario
7. Limitations of PAM360 Remote Connect
8. Troubleshooting Tips

1. Benefits of Using PAM360 Remote Connect

1. PAM360 Remote Connect offers password-less, one-click login for seamless access to remote endpoints.
2. Remote Connect is a lightweight client, capable of launching both RDP and SSH-based connections from a single interface—thus eliminating the need to install multiple applications to get the job done.
3. Remote Connect can launch concurrent active remote connections in multiple tabs.
4. SSH-based remote sessions initiated via Remote Connect are highly customizable. The client allows you to modify system settings within the remote session window and lets you perform operations that you can carry out in a local machine such as opening the

session window in full screen and changing the keyboard configurations. This provision helps elevate the overall user experience.

2. Prerequisite

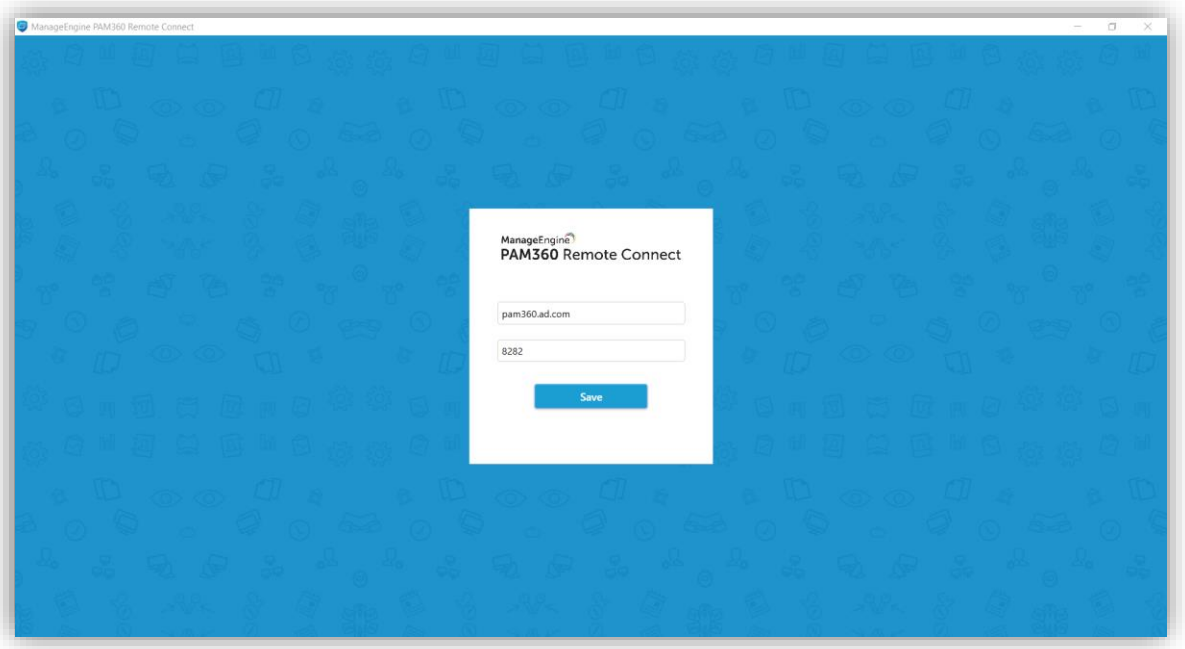
A working instance of the PAM360 web application, accessible from the end-user workstation.

3. System Requirements

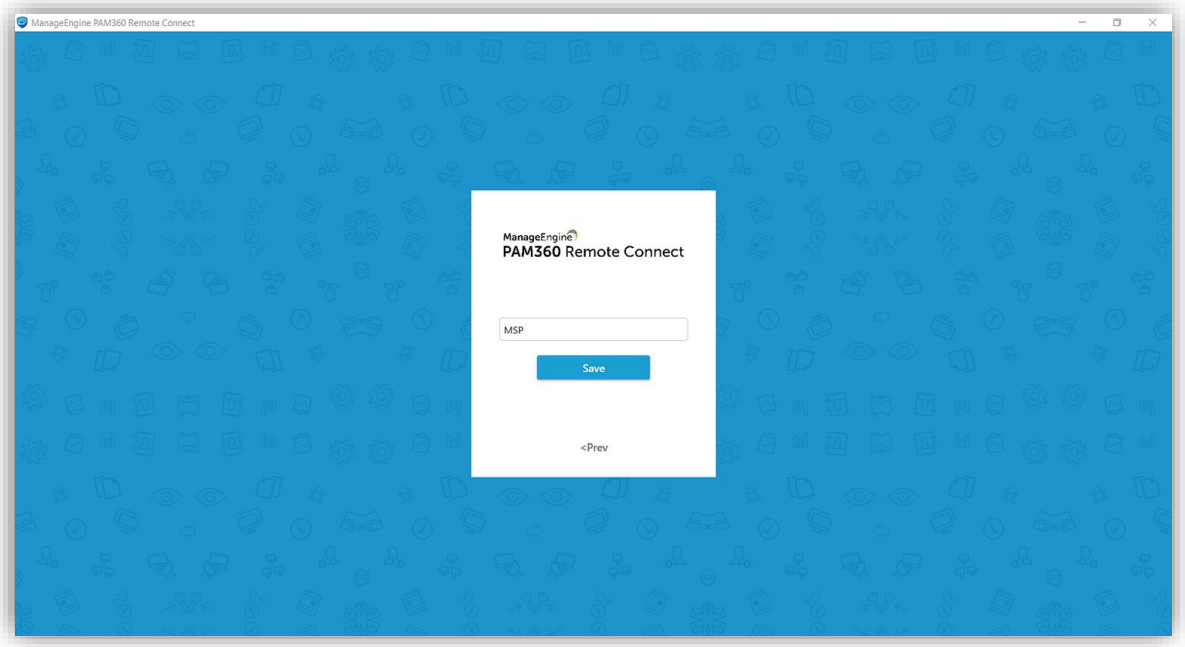
Hardware Requirements	Supported Operating Systems
Processor • Dual Core/Core2Duo or above **RAM** • 4 GB or above **Hard Disk** • 200 MB or more	**Windows** • Windows Server 2016 • Windows Server 2019 • Windows 10 and above **Note:** PAM360 Remote Connect can also be run on VMs of the above operating systems.

4. Steps to Install and Log into Remote Connect

1. Go to the PAM360 Remote Connect download page and download the **PAM360RemoteConnect.exe** file. Follow the instructions in the Installation Wizard to install the application.
2. Once the application is successfully installed, launch PAM360 Remote Connect.
3. In the **Server Configuration** page, do as follows:
    a. Enter the hostname and port of your PAM360 web server and click **Save**.



b. If you have an MSP build, enter the **Org** name. If you are unsure of your Org name, navigate to the PAM360 web interface, go to **Admin >> Organizations** and find your Org name.



c. If you do not have an MSP build, you will be redirected to the login page directly without the prompt to enter Org name.

4. Enter your PAM360 login credentials. All the authentication modes that are enabled in your PAM360 server such as AD/Azure AD/LDAP authentication, SAML single sign-on methods, and two-factor authentication will be applied to Remote Connect as well. For example, if AD/Azure AD/LDAP authentication is enabled for your PAM360 login, you can log in to Remote Connect using your AD/Azure AD/LDAP credentials.

Notes:

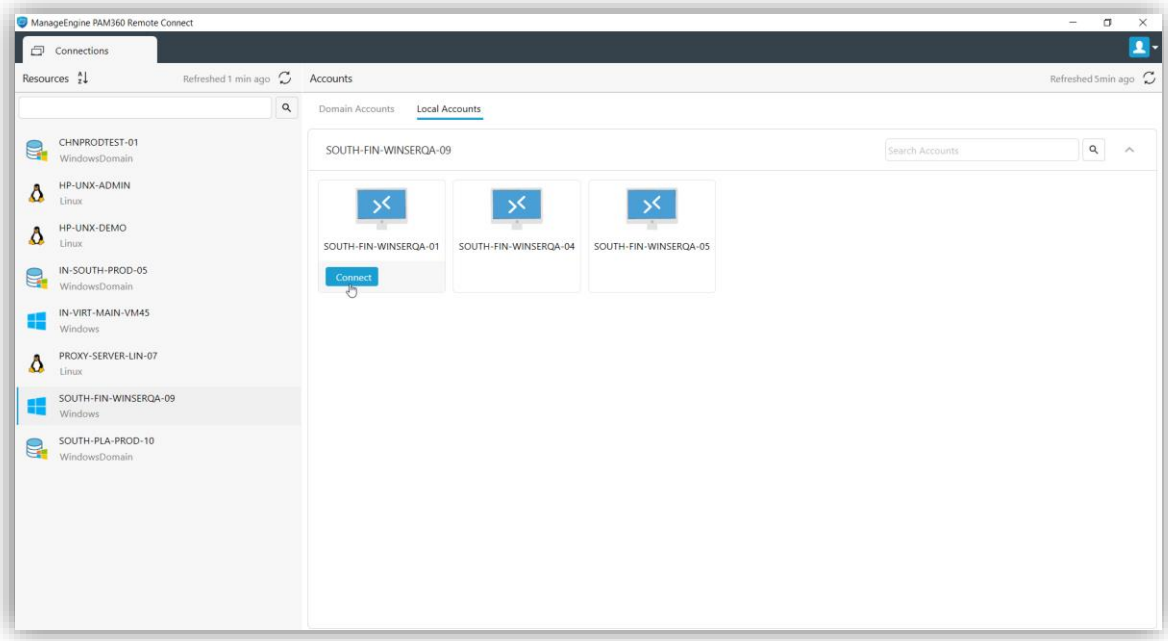
1. Ensure that the PAM360 service is running for a successful login.
2. Click the **Server Configuration** option present at the right top corner in the login page to modify the server details at any time.

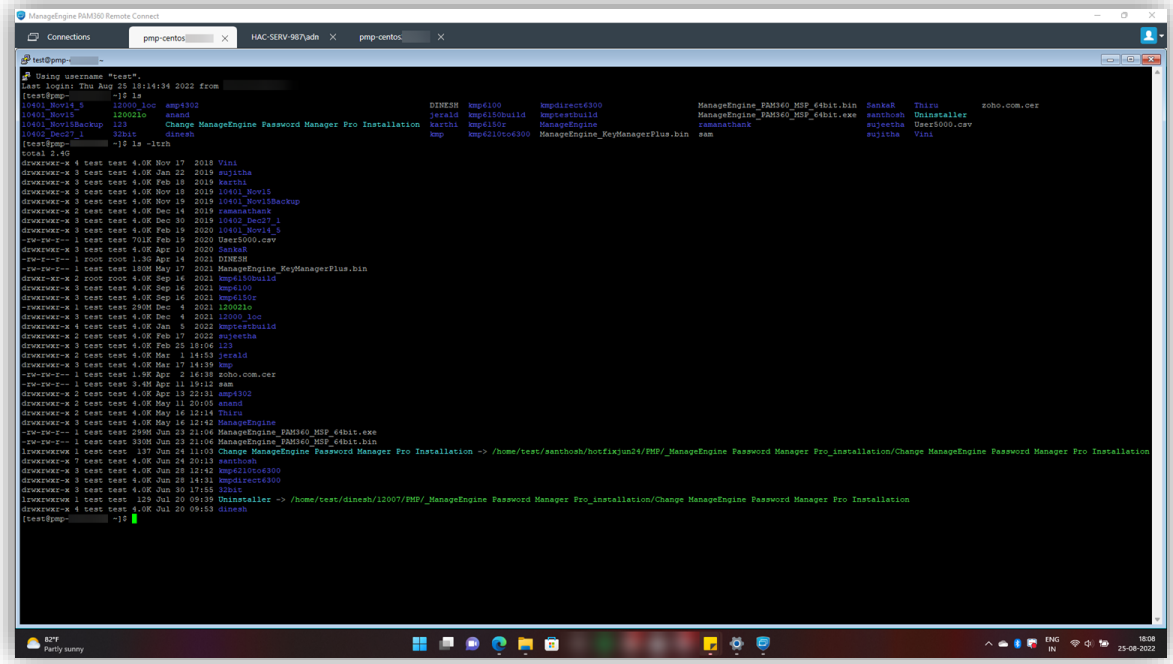
5. Possible Operations in the PAM360 Remote Connect Interface

All RDP and SSH-based resources and accounts owned by you and/or shared with you will be available for your use in the Remote Connect interface. The display area is split into two panes: **Resources** and **Accounts**.

Click any resource from the **Resources** pane on the left to view the accounts belonging to it in the display area on the right. Similar to the **Connections** tab in PAM360's web application, PAM360 Remote Connect displays Domain Accounts and Local Accounts of the selected resource in separate columns. You can establish remote connections to a resource using either the local accounts or one of the available domain accounts. Refer to the help section **Connections Tab Operations** to learn more in detail.

Hover over any account and click **Connect** to successfully launch a remote connection to the selected resource. You can launch concurrent remote connections and manage them from different tabs in the same window. Use the sort option in the **Resources** pane to sort the resources as per alphabetical or reverse alphabetical order. Both the panes have individual search bars to help you locate resources and accounts using keyword search. All operations that you can perform in an MSTSC connection and via SSH PuTTY client are possible using Remote Connect.


ManageEngine PAM360 Remote Connect
Connections
Resources
Refreshed 1 min ago
Accounts
Refreshed 5min ago
Domain Accounts
Local Accounts
CHNPRODTEST-01
WindowsDomain
HP-UNX-ADMIN
Linux
HP-UNX-DEMO
Linux
IN-SOUTH-PROD-05
WindowsDomain
IN-VIRT-MAIN-VM45
Windows
PROXY-SERVER-LIN-07
Linux
SOUTH-FIN-WINSERQA-09
Windows
SOUTH-PLA-PROD-10
WindowsDomain
SOUTH-FIN-WINSERQA-09
Search Accounts
SOUTH-FIN-WINSERQA-01
SOUTH-FIN-WINSERQA-04
SOUTH-FIN-WINSERQA-05
Connect


ManageEngine PAM360 Remote Connect
Connections
pmp-centos
HAC-SERV-987\adn
pmp-centos
Using username "test".
Last login: Thu Aug 25 18:14:34 2022 from
[test@pmp- ~]$ ls
[test@pmp- ~]$ ls -ltrh
total 2.4G
drwxrwxr-x 4 test test 4.0K Nov 17 2018 Vini
drwxrwxr-x 3 test test 4.0K Jan 22 2019 sujitha
drwxrwxr-x 3 test test 4.0K Feb 18 2019 karthi
drwxrwxr-x 3 test test 4.0K Nov 19 2019 10401_Nov15
drwxrwxr-x 3 test test 4.0K Nov 19 2019 10401_Nov15Backup
drwxrwxr-x 2 test test 4.0K Dec 14 2019 ramanathank
drwxrwxr-x 3 test test 4.0K Dec 30 2019 10402_Dec27_1
drwxrwxr-x 3 test test 4.0K Feb 19 2020 10401_Nov14_5
-rw-rw-r-- 1 test test 701K Feb 19 2020 User5000.csv
drwxrwxr-x 3 test test 4.0K Apr 10 2020 SankaR
-rw-r--r-- 1 root root 1.3G Apr 14 2021 DINESH
-rw-rw-r-- 1 test test 180M May 17 2021 ManageEngine_KeyManagerPlus.bin
drwxr-xr-x 2 root root 4.0K Sep 16 2021 kmp6150build
drwxrwxr-x 3 test test 4.0K Sep 16 2021 kmp6100
drwxrwxr-x 3 test test 4.0K Sep 16 2021 kmp6150r
-rwxrwxr-x 1 test test 290M Dec 4 2021 120021o
drwxrwxr-x 3 test test 4.0K Dec 4 2021 12000_loc
drwxrwxr-x 4 test test 4.0K Jan 5 2022 kmptestbuild
drwxrwxr-x 2 test test 4.0K Feb 17 2022 sujeetha
drwxrwxr-x 3 test test 4.0K Feb 25 18:06 123
drwxrwxr-x 2 test test 4.0K Mar 1 14:53 jerald
drwxrwxr-x 3 test test 4.0K Mar 17 14:39 kmp
-rw-rw-r-- 1 test test 1.9K Apr 2 16:38 zoho.com.cer
-rw-rw-r-- 1 test test 3.4M Apr 11 19:12 aam
drwxrwxr-x 2 test test 4.0K Apr 13 22:31 amp4302
drwxrwxr-x 2 test test 4.0K May 11 20:05 anand
drwxrwxr-x 2 test test 4.0K May 16 12:14 Thiru
drwxrwxr-x 3 test test 4.0K May 16 12:42 ManageEngine
-rw-rw-r-- 1 test test 299M Jun 23 21:06 ManageEngine_PAM360_MSP_64bit.exe
-rw-rw-r-- 1 test test 330M Jun 23 21:06 ManageEngine_PAM360_MSP_64bit.bin
lrwxrwxrwx 1 test test 137 Jun 24 11:03 Change ManageEngine Password Manager Pro Installation -> /home/test/santhosh/hotfixjun24/PMP/_ManageEngine Password Manager Pro_installation/Change ManageEngine Password Manager Pro Installation
drwxrwxr-x 7 test test 4.0K Jun 24 20:13 santhosh
drwxrwxr-x 3 test test 4.0K Jun 28 12:42 kmp6210o6300
drwxrwxr-x 3 test test 4.0K Jun 28 14:31 kmpdirect6300
drwxrwxr-x 3 test test 4.0K Jun 30 17:55 32bit
lrwxrwxrwx 1 test test 129 Jul 20 09:39 Uninstaller -> /home/test/dinesh/12007/PMP/_ManageEngine Password Manager Pro_installation/Change ManageEngine Password Manager Pro Installation
drwxrwxr-x 4 test test 4.0K Jul 20 09:53 dinesh
[test@pmp- ~]$
DINESH kmp6100 kmpdirect6300 ManageEngine_PAM360_MSP_64bit.bin SankaR Thiru zoho.com.cer
jerald kmp6150build kmptestbuild ManageEngine_PAM360_MSP_64bit.exe santhosh Uninstaller
karthi kmp6150r ManageEngine ramanathank sujeetha User5000.csv
kmp kmp6210to6300 ManageEngine_KeyManagerPlus.bin sam sujitha Vini
82°F Partly sunny
ENG IN
18:08 25-08-2022

Notes:

1. Single-click auto logon using AD/Azure AD/LDAP credentials is not available in PAM360 Remote Connect for now. Therefore, the 'Logged-in AD/Azure AD/LDAP credential' tab will not be displayed here.
2. For now, Remote Connect does not have the provision to add new connections or edit the existing ones—to do so, add the connections in the PAM360 web application and refresh the view using the **Refresh** icon in Remote Connect to update the display in the client.

5.1 Launching Remote Connections to Resources with Password Access Control

When Password Access Control is enabled for a resource that is shared with a user, the user will be able to send a password request, check out the password after admin approval, launch the remote connection, and check the password back in, right from PAM360 Remote Connect without the need to open the PAM360 web interface.

As of now, the resource owners can't terminate an active remote session taken via Remote Connect. However, if access control is enabled for the resource, the password will be automatically checked back in after the specified time and the remote session will end. Refer to the **Miscellaneous Settings** in Password Access Control Workflow to learn more about in detail.

5.2 Auditing Remote Sessions

Detailed audit trails for all remote sessions taken via PAM360 Remote Connect will be recorded in the **Audit** section of the PAM360 web interface.

5.3 Optional Admin Operations

1. By default, PAM360 Remote Connect access is disabled for all users. Administrators can enable Remote Connect access from the **Add User** or **Edit User** windows. This privilege applies to all admin users by default. However, administrators can also allow other users to grant Remote Connect access by enabling the custom user role **Manage Remote Access** for them.
2. Administrators can set a time limit for a period of inactivity, after which the application will automatically end all active sessions and log out. Refer to the **User Management** section in Managing_General_Settings to learn how to set the time limit.

6. Real-time Scenario

PAM360 Remote Connect is recommended for a trusted subset of privileged users in an

enterprise who do not require metered access to the resources in the environment. For such users, Remote Connect is highly beneficial since it can be installed in any Windows machine without the need to run the PAM360 server in the same machine.

Consider John, an IT Admin, whose responsibility is to perform a routine sweep of the test machines in his environment to check for suspicious software.

In this case, John must ensure that the following conditions are satisfied:

1. The test machines must be added as resources in the PAM360 web application.
2. The test machines need not reside in the same network but they need to be able to connect to each other via RDP/SSH protocols.

If the above conditions are satisfied, John can install PAM360 Remote Connect in his own laptop or any other test machine independently and launch remote connections to other endpoints and perform his duties.

7. Limitations of PAM360 Remote Connect

1. As of now, PAM360 Remote Connect does not come with Privileged Session Management (PSM) features such as session recording, session monitoring, and termination. Please access PAM360's web interface to avail the product's extensive PSM features.
2. As of now, advanced connection settings configured for remote connections in the PAM360 web application will not apply to the remote sessions launched via Remote Connect.
3. The Secure File Transfer option is not available in the Remote Connect interface. However, direct file transfer will work between machines once the RDP/SSH connection is established.
4. As of now, Remote App support is not available. If Remote App is configured for any resource, users will not be able to connect to it via Remote Connect.
5. Once an end-user has launched a remote connection via Remote Connect, resource owners cannot terminate the session from the PAM360 web server.
6. The single-click auto logon method to launch remote connections using AD/Azure AD/LDAP credentials is not available for now.
7. The Ctrl+Alt+Del option will not work in an RDP session initiated via Remote Connect.

8. Troubleshooting Tips

1. My PAM360 web server is running but I'm unable to connect to Remote Connect.

The Remote Connect client only works with PAM360 version 5600 and above, so please ensure that the PAM360 web server is up-to-date. If not, click here to upgrade the web server to the latest version and try connecting to Remote Connect once again.

2. My PAM360 web server is up-to-date but I'm still not able to connect to Remote Connect.

It is possible that Remote Connect access is disabled for your user profile. Please contact your administrator. If you are an administrator, refer to above section 5.3 for steps on how to enable access.

3. When I hover over an account, why do I see the 'Disabled' option instead of 'Connect' or 'Request'?

If you see the **Disabled** option on an account, it could be due to one of the following reasons:

i. Plain text view of passwords is disabled for all resources under 'General Settings' in the PAM360 web server.

ii. Remote App is configured for the selected account. Remote App does not work in Remote Connect as of now.

iii. RDP access using local accounts is restricted for the selected resource.

iv. Remote connection is disabled for the selected resource type under 'Auto Logon Helper' in the PAM360 web server.

Privileged Session Recording

1. Overview
    1.1 How secure is session recording?
2. Configuring session recording
    2.1 Configuring session recording for specific resources
    2.2 Configuring session recording globally
3. Viewing the recorded sessions
4. Splitting of session recordings
5. Session shadowing/real-time session monitoring
    5.1 Monitoring sessions in parallel
    5.2 Terminating a suspicious session
    5.3 Deleting selective session recordings

1. Overview

It is possible to record, playback, and archive privileged sessions launched from PAM360, to support forensic audits and allow enterprises to monitor all actions performed by the privileged accounts during privileged sessions. The session recording caters to the audit and compliance requirements of organizations that mandate proactive monitoring of activities, thereby enabling administrators to readily answer the 'who,' 'what' and 'when' questions of privileged access. You can use PAM360 to record Windows RDP, SSH/Telnet, and SQL sessions launched from PAM360's interface.

1.1 How Secure is Session Recording?

PAM360 employs first-in-class, browser-based remote login mechanism for the session recording process. From any HTML5-compatible browser, users can launch highly secure, reliable and completely emulated Windows RDP, SSH and Telnet sessions with a single click, without the need for an additional plug-in or agent software. Remote connections are tunneled through the PAM360 server, requiring no direct connectivity between the user device and the remote host. In addition to superior reliability, the tunneled connectivity provides extreme security as passwords needed to establish remote sessions do not need to be available at the user's browser. The session recording capability is an extension of the robust remote login mechanism of PAM360.

PAM360 comes bundled with RDP, SSH and Telnet session gateways. This allows the users to launch remote terminal sessions from their browser that are tunneled through the PAM360 server. The remote terminal sessions are emulated in the browser screen itself and hence there

is no need for installing any plug-in or agent in any of the end-points. The only requirement is that the browsers should be HTML 5 compatible (For example IE 9 or above, Firefox 3.5 or above, Safari 4 or above, and Chrome).

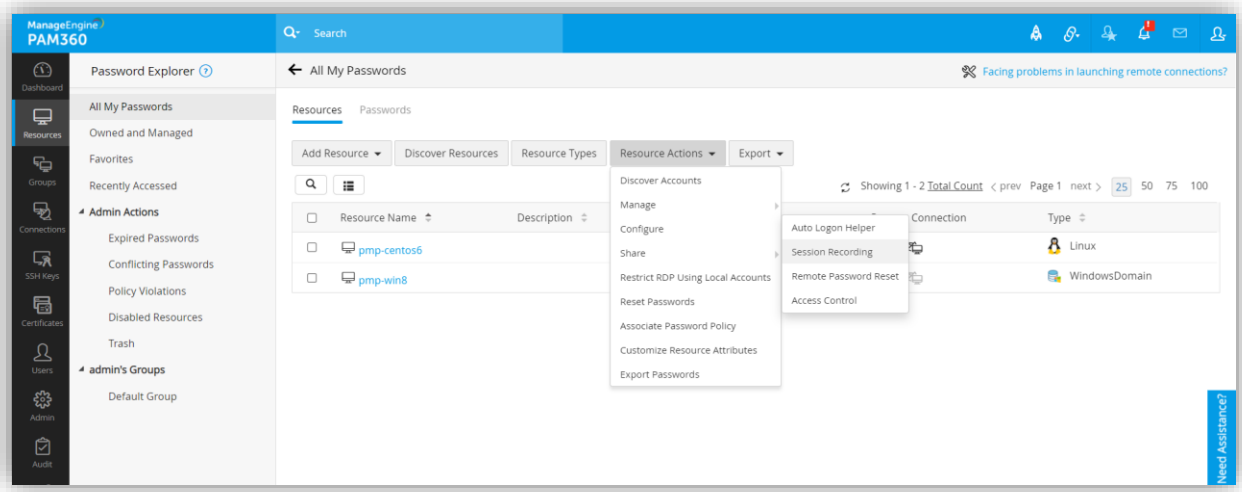
2. Configuring Session Recording

There are two ways to configure remote session recording:

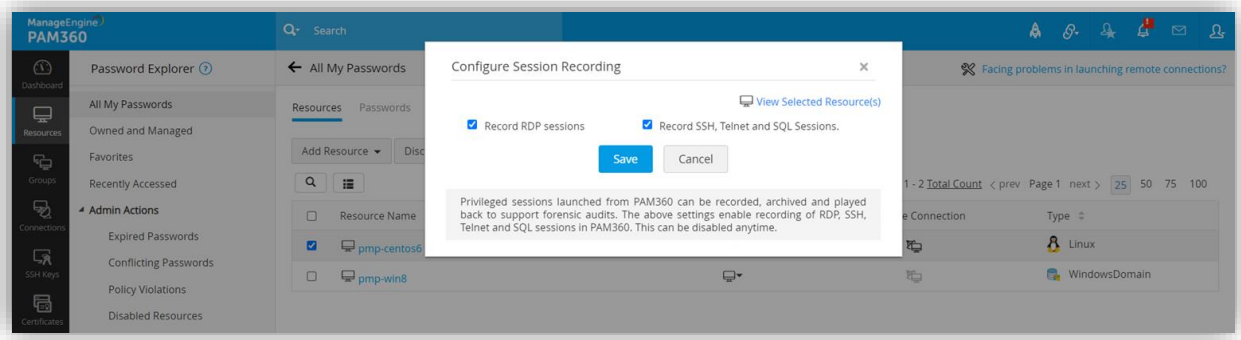
1. Configuring session recording for specific resources
2. Configuring session recording globally

2.1 Configuring Session Recording for Specific Resources

1. Navigate to the **Resources** tab and select the resources for which you want to configure session recording.
2. Go to **Resource Actions >> Configure >> Session Recording**.



3. In the pop-up form that opens, select the options **Record RDP sessions** and/or **Record SSH, Telnet and SQL Sessions** as required and click **Save**.



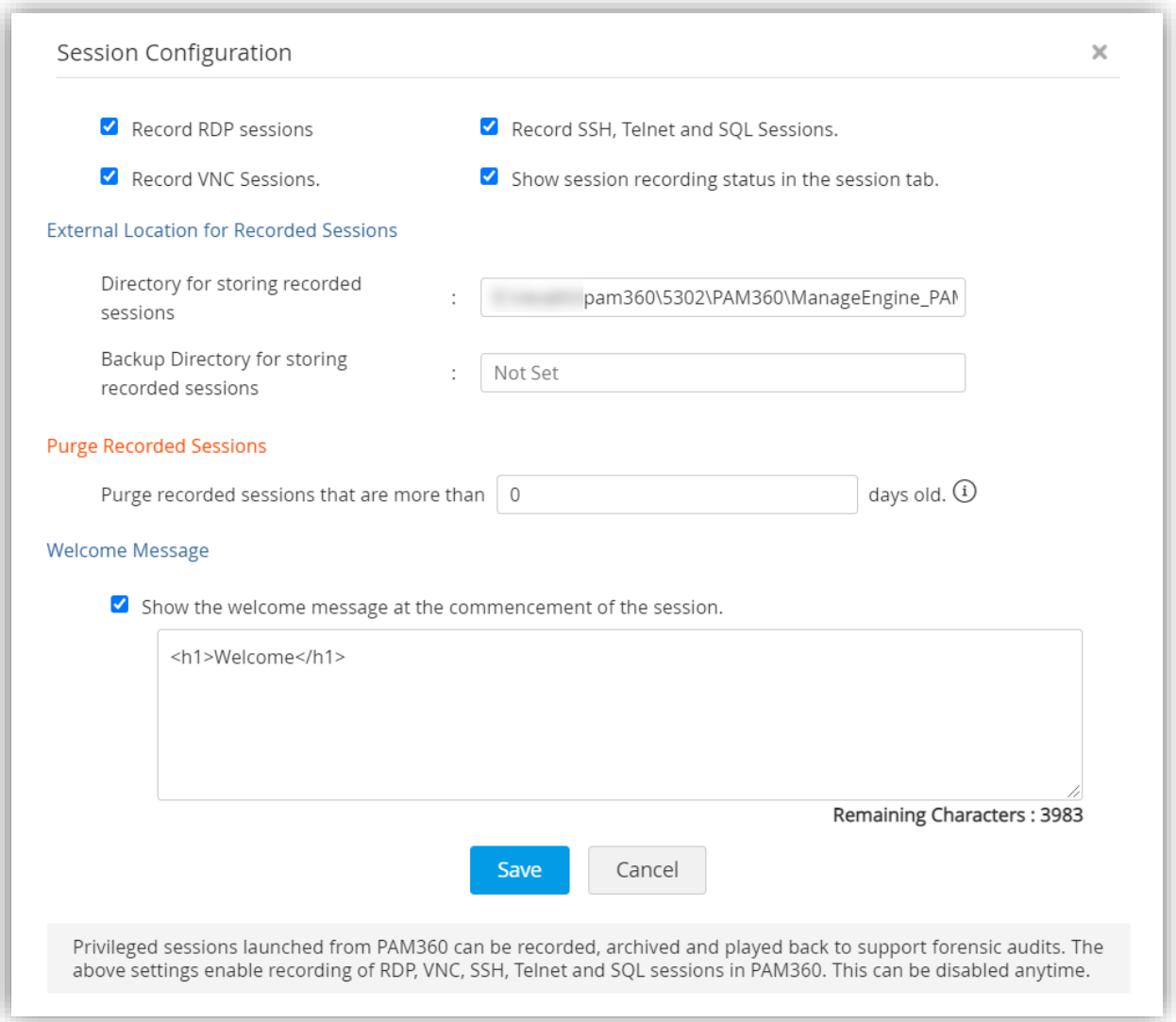
Note: The recordings will be stored by default in the path <PAM360_Install_Directory\PAM360\recorded_files>. This external location to store recording can be changed at any time by navigating to **Admin >> Configuration >> Session Recording.**

2.2 Configuring Session Recording Globally

1. Navigate to Admin >> Configuration >> Session Configuration.
2. In the pop-up form that opens,
    i. Select the options Record RDP sessions and/or Record VNC sessions and/or Record SSH, Telnet and SQL sessions as required.
    ii. Select the check-box - **Show session recording status in the session tab** if you wish to display the session recording status in the session window.
    iii. Enter a valid path to store the recorded sessions under **External Location for Recorded Sessions**. You can also set a backup directory for storing the recordings, in which case the recorded files will be stored in both locations.
    iv. To purge the records that are older than a specified number of days, enter the number under Purge recorded sessions that are more than __ days old. You can disable purging by leaving the text field empty or by entering 0 as the value.
    v. Select the check-box - **Show the welcome message at the commencement of the session** and enter the message that you want to display in the text field given below. This text field has a limit of 4000 characters and supports CSS in In-line styles. This way, you can enable and customize the welcome message as desired.
    vi. Click **Save** to save the changes.

    Note: For MSP, you should apply the above settings for each client ORG account individually.

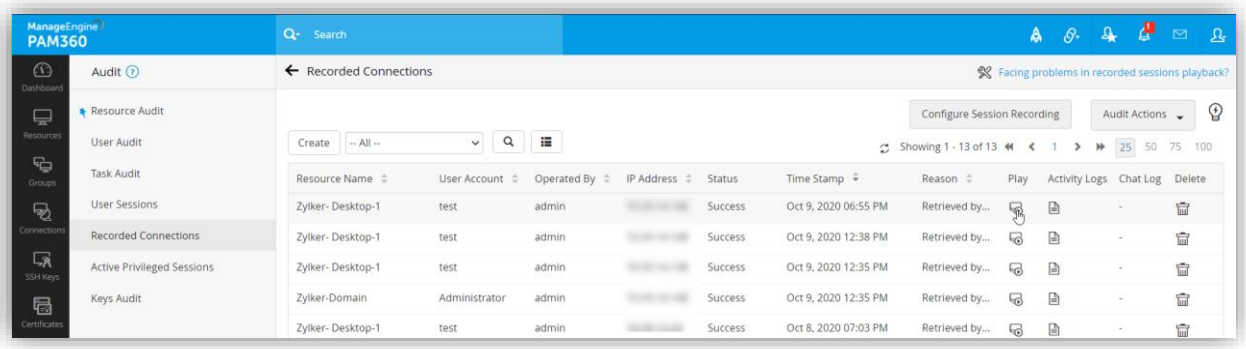
3. Now, the session recording feature becomes available as soon as an administrator adds a resource that supports one of these remote terminal session types (RDP, SSH, Telnet).



3. Viewing the Recorded Sessions

View the recorded sessions from the **Audit** tab in the PAM360 interface by following the steps below. You can trace sessions using any detail such as the name of the resource, the user who launched the session, or the time at which the session was launched.

1. Navigate to the **Audit >> Recorded Connections.**
2. Click **Play** against the recorded session which you want to view. While viewing a recorded session, click the seek bar to skip a part of the recording and progress.



4. Splitting of Session Recordings

PAM360 has a provision to split session recording files obtained from remote sessions into several small files and encrypt them individually. This option applies to session recording files that are larger than 10 MB in size. By default, PAM360 encrypts all session recordings stored in your local storage. For long recordings of huge file sizes, there is a chance of encryption failure. Hence, those recordings are split and stored in chunks whose size does not exceed 10 MB. PAM360 ensures that the split parts are encrypted successfully and saved. The recordings, though stored as multiple files, will be played as a single file only during playback. In addition to successful encryption, session splitting also ensures a smooth playback without buffer time.

Example:
Consider a session recording of 25 MB file size. PAM360 will split this into three files that are 10 MB, 10 MB, and 5 MB in size.

By default, the session splitting option is disabled in PAM360. Follow the steps detailed in the **Enable Splitting of SSH and Telnet Session Recordings into Multiple Files** section of General Settings help to enable session splitting. Remember, with this option disabled, PAM360 will save all session recordings as a single file only.

Notes:

i. Session splitting works only for Legacy SSH and Telnet sessions.

ii. This option will not work for RDP, VNC, and SSH sessions as they are video-based, and PAM360 does not encrypt video-based recordings. PAM360 saves these session recordings as video files in the external storage. However, you cannot play these files outside the PAM360 interface using standard media players.

5. Session Shadowing/Real-time Session Monitoring

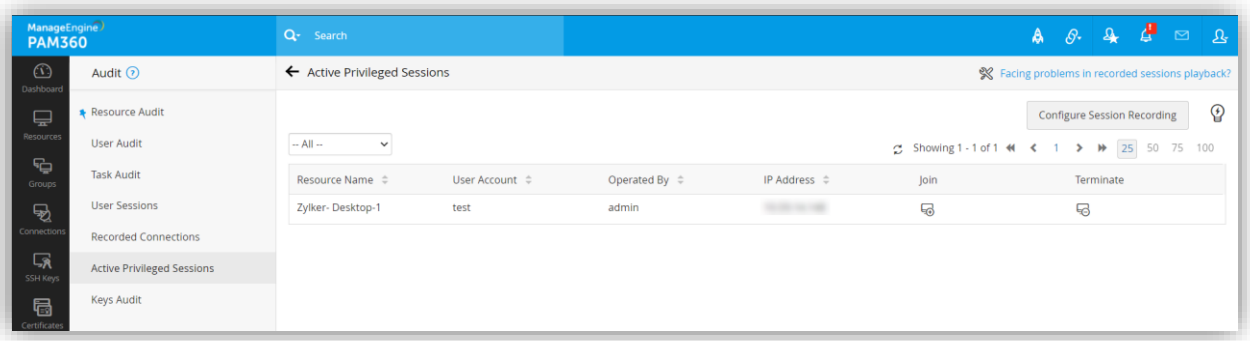
PAM360 lets administrators monitor the privileged sessions of highly sensitive IT resources. Session Shadowing allows admins to join active sessions, observe user activities parallelly, and terminate them in case of suspicious activities. Admins can also offer assistance to users while monitoring the users' activities during troubleshooting sessions.

5.1 Monitoring Sessions in Parallel

1. Navigate to **Audit >> Active Privileged Sessions.**
2. Trace the session to be monitored through the name of the resource.
3. Click the **Join** button. You will be able to view the ongoing session in parallel.

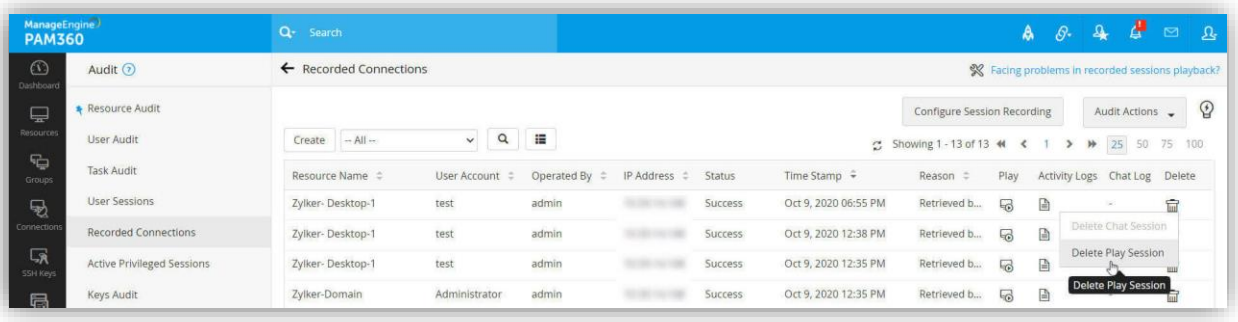
5.2 Terminating a Suspicious Session

1. Navigate to **Audit >> Active Privileged Sessions.**
2. Trace the session to be monitored through the name of the resource.
3. Click the **Terminate** button. The remote session will be terminated and the user will lose connection with the remote resource.



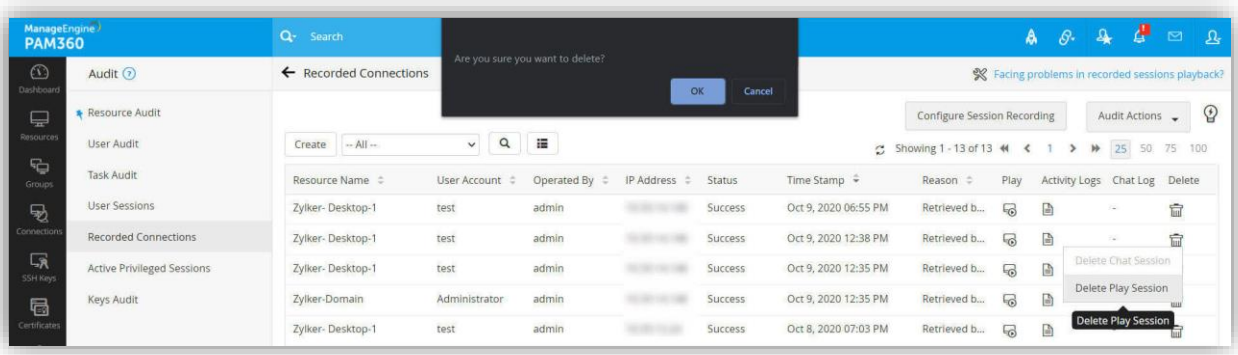
5.3 Deleting Selective Session Recordings

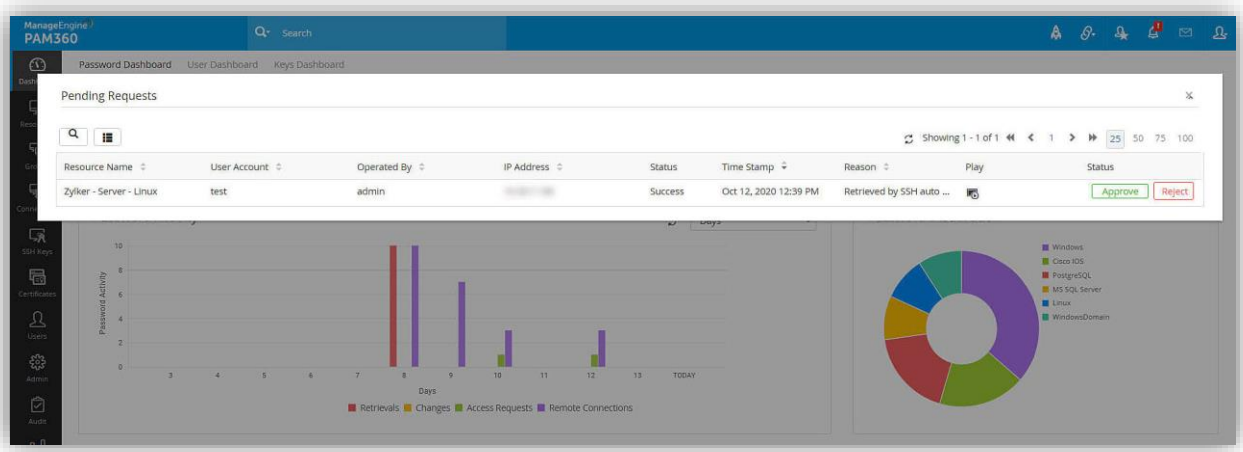
1. Navigate to **Audit >> Recorded Connections.**
2. Choose the session you want to delete and then click the delete icon beside it under the **Delete** column.
3. You can either choose to delete the recording of the session or the chat logs of a particular session as shown below:



Note: In order to delete selective sessions from the PAM360 database, there should be **at least two active administrators**, including yourself. This is to ensure that no important session is deleted without proper confirmation.

4. Once you have chosen to delete the chat log or the session recording, a dialog box will appear prompting you to confirm the action as shown below.





5. The other administrator(s) will be notified and a request for approval will be sent to them. They can either approve or reject this decision. Note that the deletion process requires the consent of just two administrators, i.e., if an administrator apart from you

approves, then the deletion will take place, irrespective of the approval of the other administrators (if any).

6. Based on whether the session files are present in the system or in any external device, their deletion will take place as explained below:
    - **Scenario 1:** If the file is present in the system, PAM360 will delete the recording once the request has been approved by another administrator.
    - **Scenario 2:** If the recordings are present in an external device and not in PAM360 during this process, PAM360 will run a system scheduler to delete these files. In this case, the file(s) will be deleted **only** if the external device containing the session recordings is connected to the PAM360 server when the scheduler runs.

> **Note:** Once the deletion of a recording has been approved but the action hasn't been carried out yet as explained in scenario 2 above, PAM360 will temporarily disable the video recording until deletion and it cannot be viewed by anyone including the administrators.

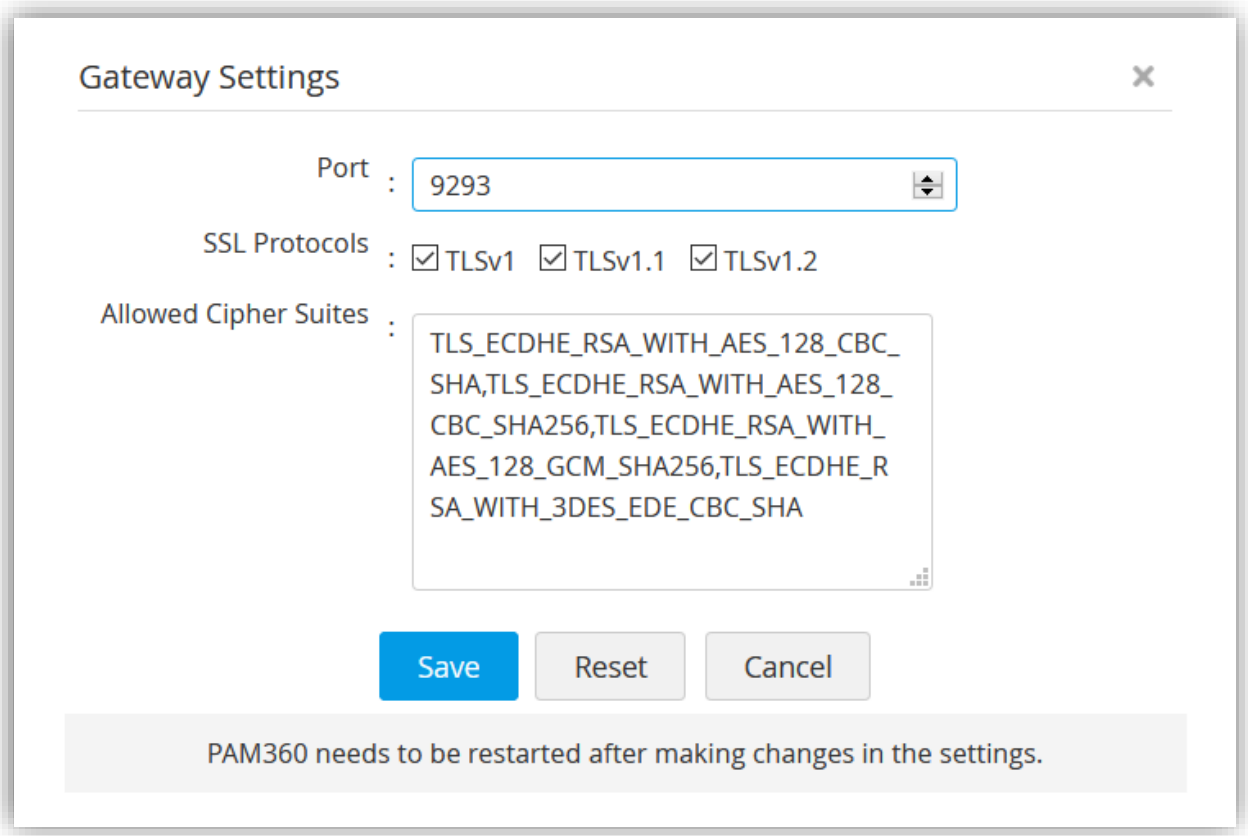
Gateway Settings

Customize gateway settings in PAM360 to set up a different port, customize HTTP header log settings, choose SSL protocols to be used for securing remote connections initiated from the product, edit and control the cipher suites used for SSL communication, and much more. For a more extensive customization, apart from the options provided in the PAM360 web interface, you can edit the **gateway.conf** file found in the path **<PAM360_installation_directory>\conf.**

Steps Required

Follow the below instructions:

1. Navigate to **Admin >> Connections >> Gateway Settings.**



2. In the pop-up that opens, edit the following attributes:
    i. **Gateway Port:** The default port is set to 9293. Change the port by typing the new port number in the text field.
    ii. **Session Recording:** This option pertains to session recording in PAM360 and it is enabled by default.
    iii. **SSL Protocols:** Supported SSL protocols are TLSv1, TLSv1.1, TLSv1.2. By default, all three are selected.
    iv. **Allowed Cipher Suites:** The cipher suites are used by PAM360 are:

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA. To edit, simply type in a cipher suite in the text field.

v. **Recording Notification:** This option sends a warning to the user that the session is being recorded, it is enabled by default. Change the setting to **Disable** to not display the notification.

3. Click **Save** to save the changes. You can reset all the changes by clicking **Reset.**

As mentioned above, refer to the **gateway.conf** file in the path **<PAM360_installation_directory>\conf** to edit more gateway settings and for other technical details.

HTTPS Gateway Server

PAM360 now allows you to configure a secure HTTPS gateway server to act as an intermediary proxy, facilitating the launch of privileged connections to resources that support URLs and are not accessible from PAM360 user devices. The connections are established using HTTPS-based web links, where the target URL can be an internal or external resource URL or an intranet link. You can also configure the HTTPS gateway server with a preferred port, KeyStore path, and KeyStore password to secure the connection to the target URL.

For additional information on the configurations and limitations of the HTTPS gateway server, please refer to the following sections.

1. Roles and Permissions
2. Configuring HTTPS Gateway Server
3. Configuring Resources for HTTPS Gateway Connections

    3.1 Configuring Auto Logon Helper for HTTPS Gateway Connections

    3.2 Adding URL (HTTPS-Based) to the Resources

    3.3 HTTPS Gateway Connections

4. Functional Behavior in Multi-Server Environment
5. Limitations of HTTPS Gateway Server

1. Roles and Permissions

By default, users with the administrator role can configure the HTTPS gateway server, and users with administrator and connection user roles can take HTTPS connections through the gateway server. Apart from the user roles described above, administrators can allow other PAM360 users to either configure the HTTPS gateway server and(or) to take HTTPS connections through the configured gateway by enabling the custom roles that follow:

1.1 HTTPS Gateway Server

Navigate to '**Admin >> Customization >> Roles >> Add Role >> PAM360 Settings**', and enable the custom role '**HTTPS Gateway Server**'. Enabling this custom role will allow the users to configure the HTTPS gateway server.

1.2 HTTPS Gateway Connection

Navigate to '**Admin >> Customization >> Roles >> Add Role >> Remote Access**', and enable the '**HTTPS Gateway Connection**'. Enabling this custom role will allow the users to launch HTTPS connections through the configured gateway server.

2. Configuring HTTPS Gateway Server

Post PAM360 installation, by default, the HTTPS gateway server will be configured and running in PAM360. To reconfigure the HTTPS gateway server as per your requirements mentioned below, navigate to '**Admin >> Configuration >> HTTPS Gateway Server**' and follow the below steps:

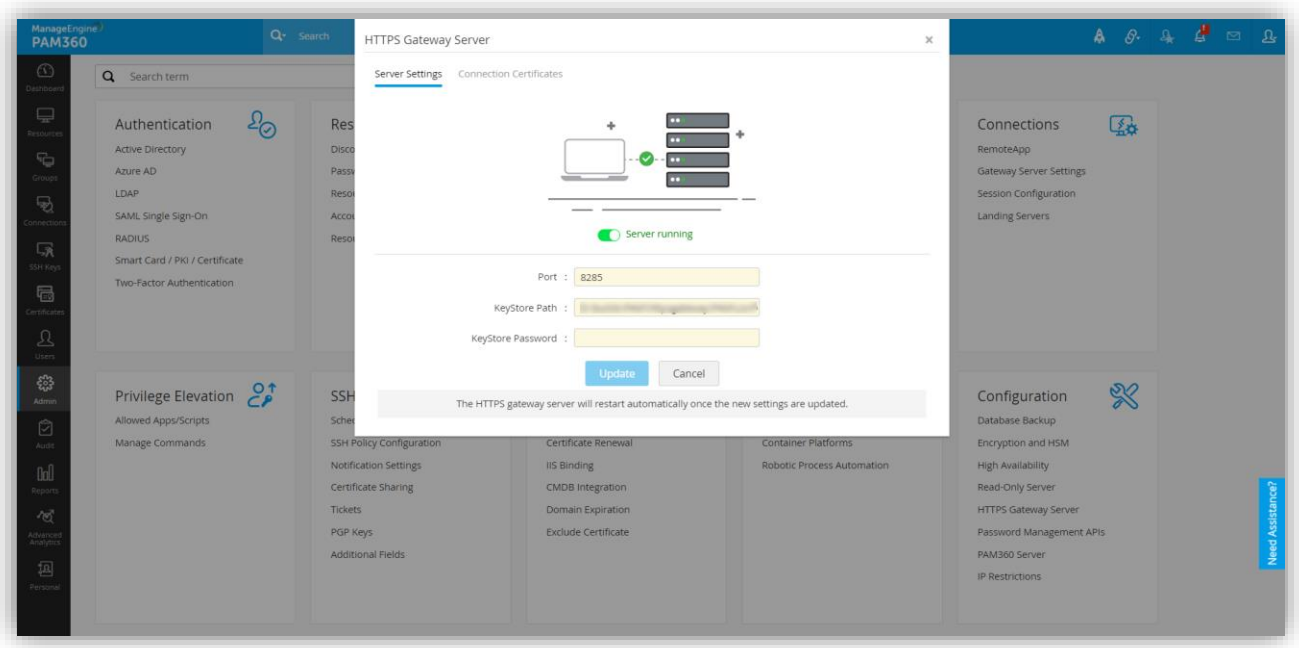
1. **Port** - The HTTPS gateway server is configured with port 8285 by default. If you have port 8285 configured for another application/instance in your organization, update the port at your convenience as available.
2. **KeyStore Path** - By default, a KeyStore file named '**httpsCerts.keystore**' will be available in the **conf** folder of the PAM360 installation directory to save all the HTTPS connection-related certificates. If you need:

    i. A unique KeyStore file for greater security reasons to save all your HTTPS connection-related certificates
    ii. To make your HTTPS gateway connection secure

    You can create a new KeyStore file of type '**.keystore**' and enter the respective file path in this **KeyStore Path** field.

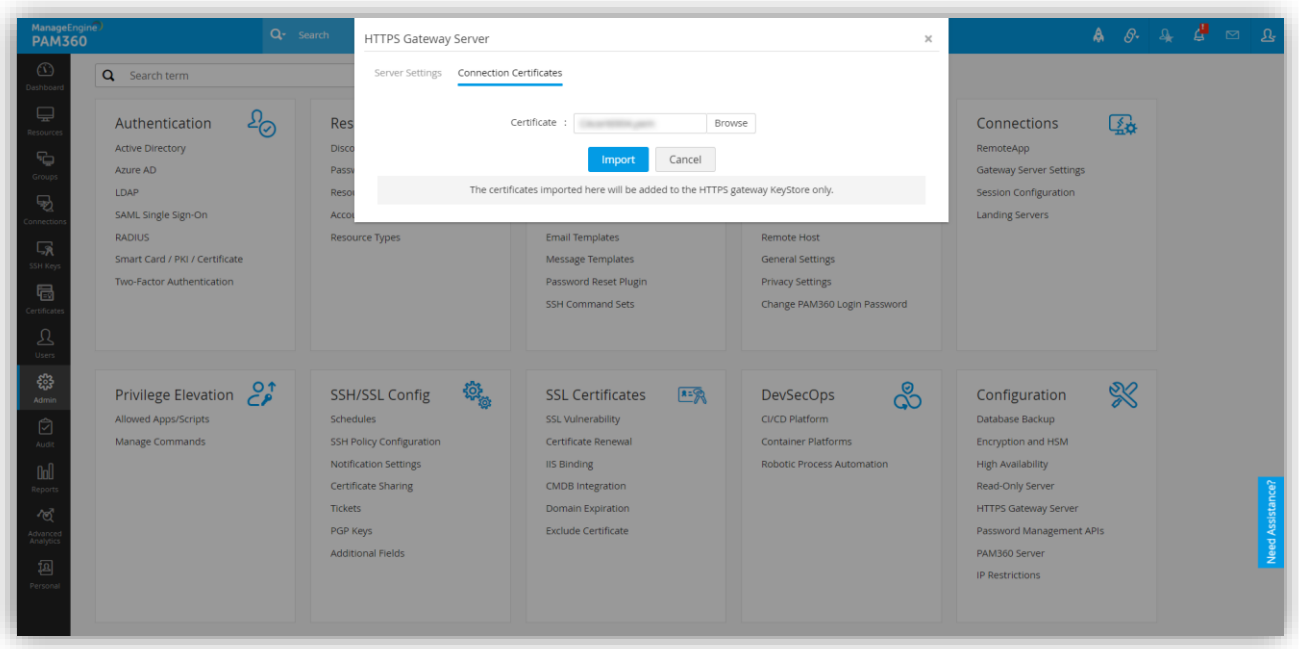
3. **KeyStore Password**: If you have created a new KeyStore file specific to this HTTPS gateway server, enter the respective KeyStore password that you have added while generating the new KeyStore file.

4. Click **Update** to save and start the HTTPS gateway server with the updated configuration.



5. Most HTTPS connections will work securely through the HTTPS gateway server. A few specific HTTPS connection URLs require their respective root certificate to connect securely through the HTTPS gateway server. For those URLs to work securely, their relevant root certificates have to be imported into the HTTPS gateway server's KeyStore. To import those certificates into the KeyStore, do the steps that follow:

    i. Navigate to '**Admin >> HTTPS Gateway Server >> Connection Certificates**'.
    ii. Browse the path of the respective URL's root certificate.
    iii. Click **Import** to save the added certificate in the configured KeyStore file for further secure HTTPS connections.
    iv. After importing each certificate, the HTTPS gateway server has to be restarted. To do so, you can use the toggle button in the **Server Settings** tab.



For the HTTPS gateway server to work efficiently in an organization with load balancer(s) configured for PAM360 web service, do the steps that follow:

1. Configure the remote host feature of PAM360.
2. Navigate to **<PAM360 Installation Directory/conf>** and open the file named **system_properties**.
3. Add a new system property **https.gateway.server.loadbalancer.enabled=true**.

> **Note:**
>
> Without the configured remote host feature and new system property, the server will receive the load balancer IP address for all the received requests instead of the actual one, which allows the IP address to reach the maximum HTTPS gateway threshold than the permitted value.

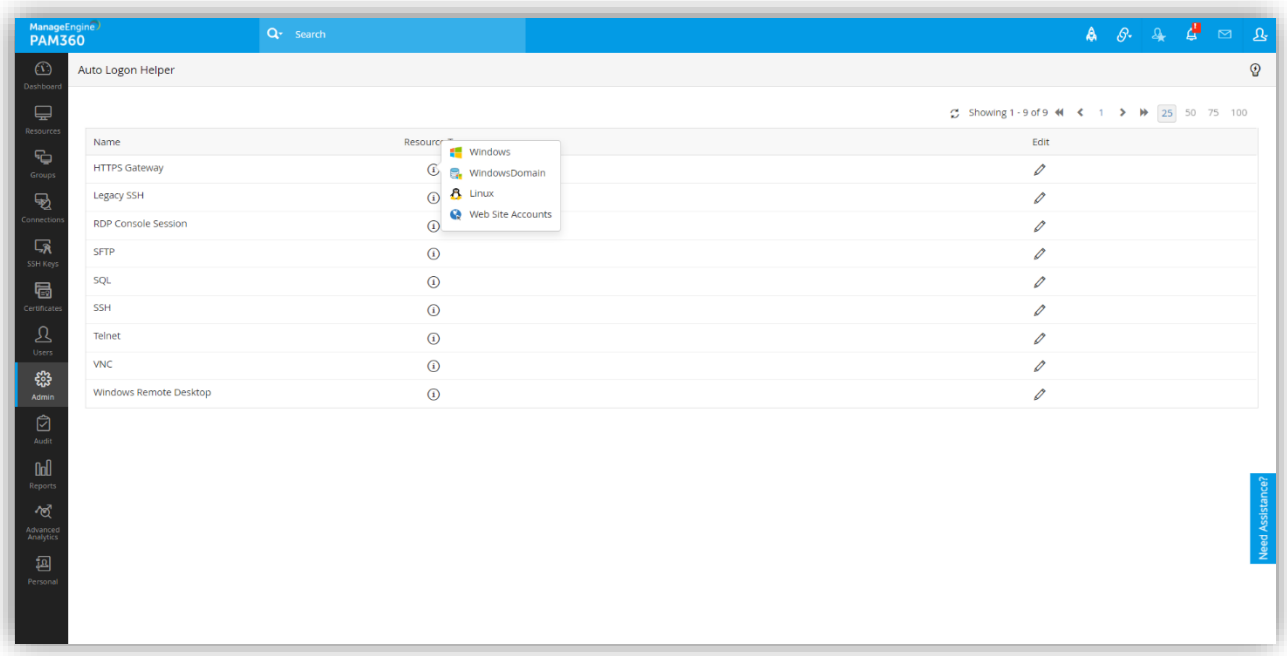
3. Configuring Resources for HTTPS Gateway Connections

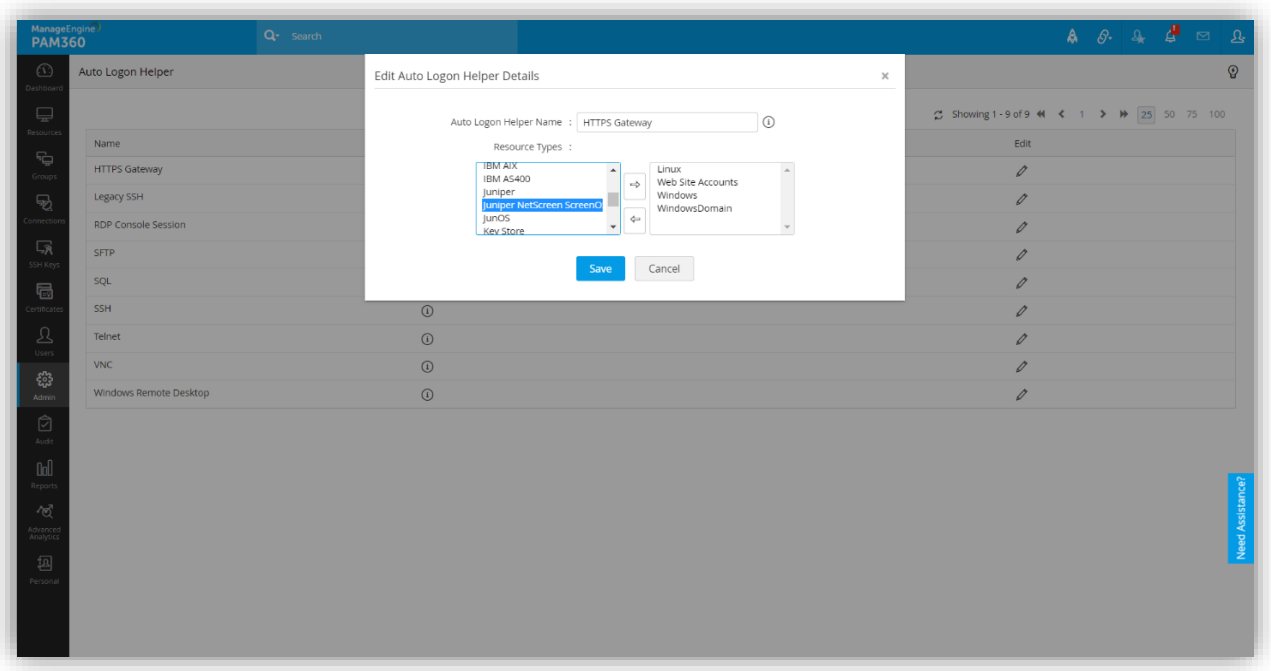
Once done with the HTTPS gateway server configuration, you can proceed with auto-logon configuration and adding resource URLs from the **Resources** tab for further use of HTTPS gateway connections.

3.1 Configuring Auto Logon Helper for HTTPS Gateway Connections

By default, the HTTPS Gateway connection supports resources of types - **Web Site Accounts**, **Windows**, **WindowsDomain**, and **Linux**. If you want to use this HTTPS gateway for other resources that support web-based URLs, do the steps that follow:

1. Navigate to '**Admin >> Customization >> Auto Logon Helper**'.
2. Click the edit icon beside the **HTTPS Gateway**.
3. Select the resource types that support web-based URLs and move them to the right column.
4. Click **Save** to update the supported resource types.

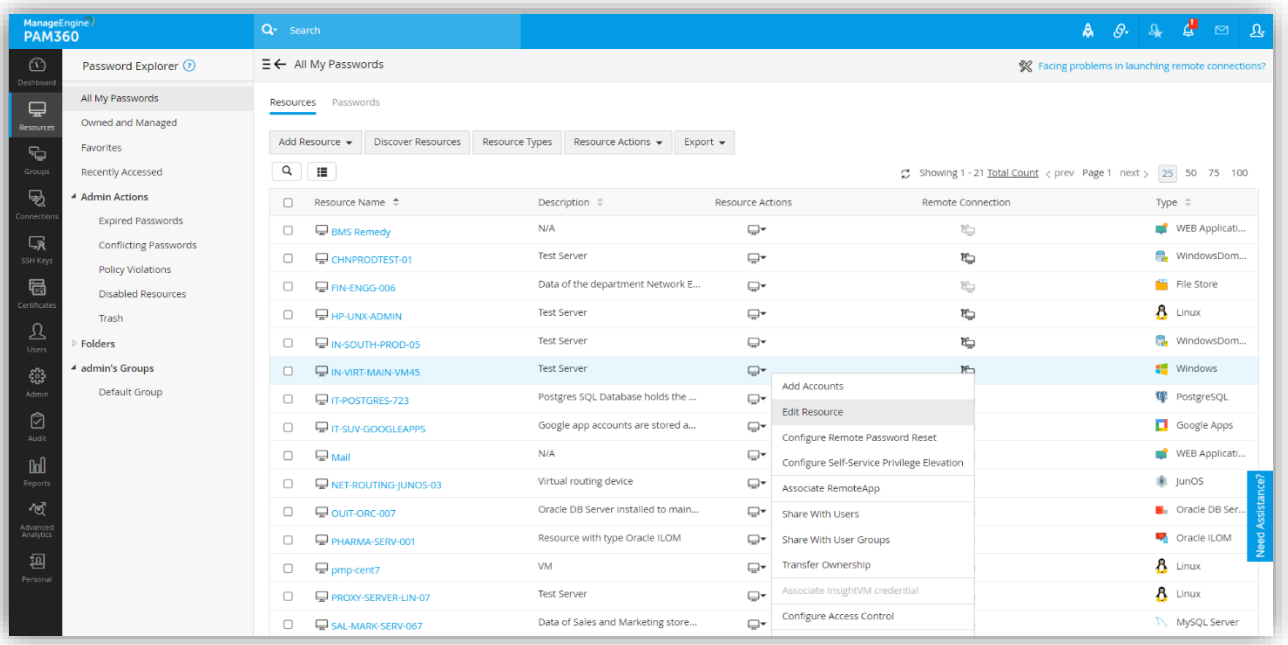


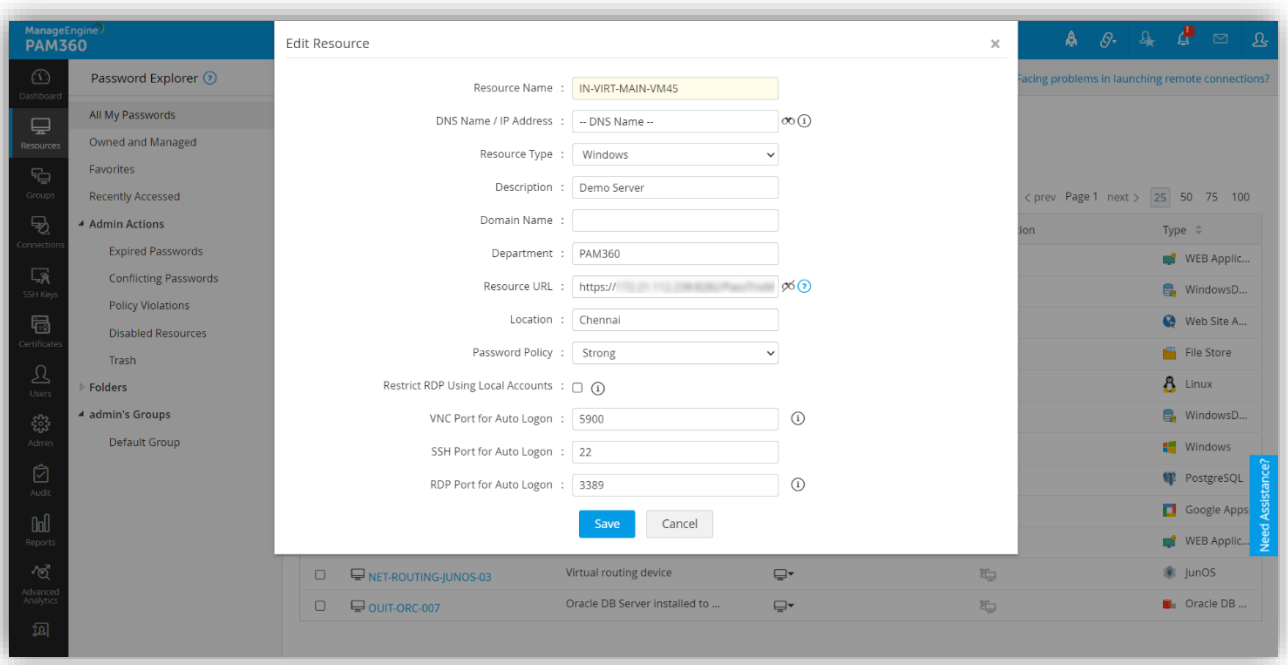


3.2 Adding URL (HTTPS-Based) to the Resources

You can add URLs to the resources in two different scenarios. You can add it either while adding a new resource or for the existing available resources using the resource edit option. For the available resources in PAM360:

1. Navigate to the **Resources** tab.
2. Under the **Resource Actions** column, beside the respective resource for which the remote connection is to be taken via HTTPS gateway connection type, select **Edit Resource**.
3. In the pop-up that appears, enter a valid URL of type HTTPS web link in the **Resource URL** field.
4. Click **Save** to update.



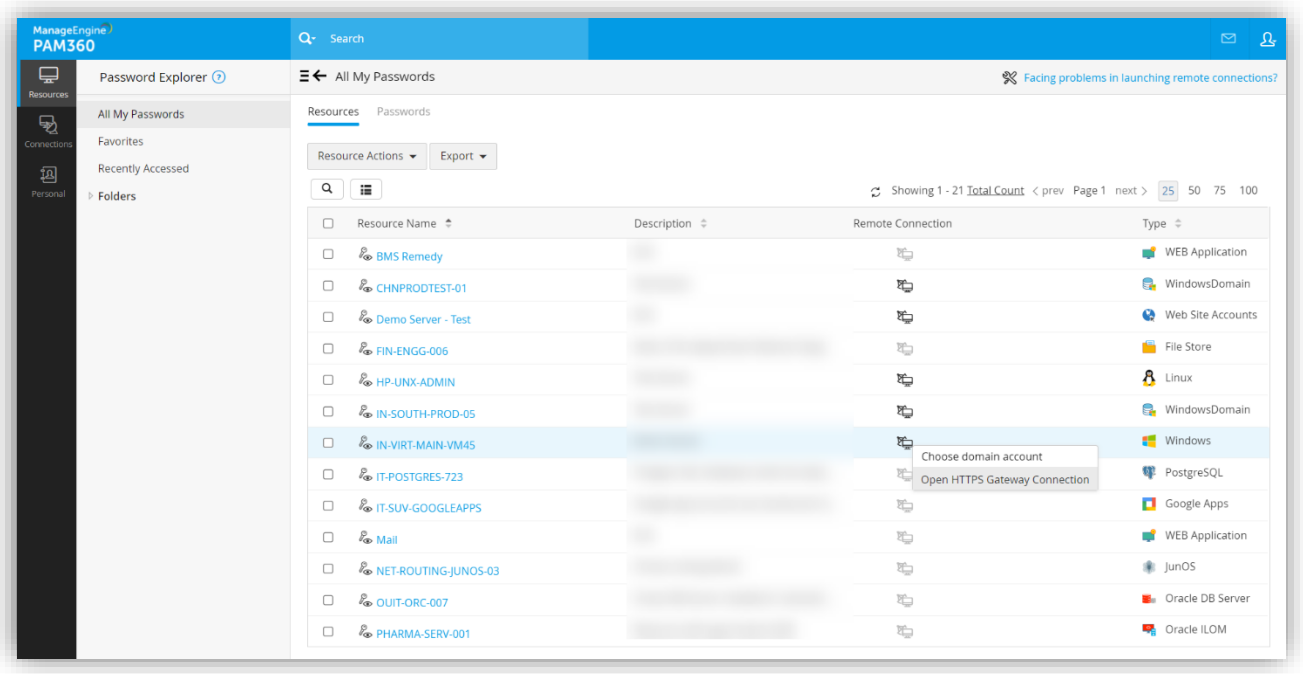


5. Now the respective resource will have an HTTPS gateway connection as a type for the remote connection.

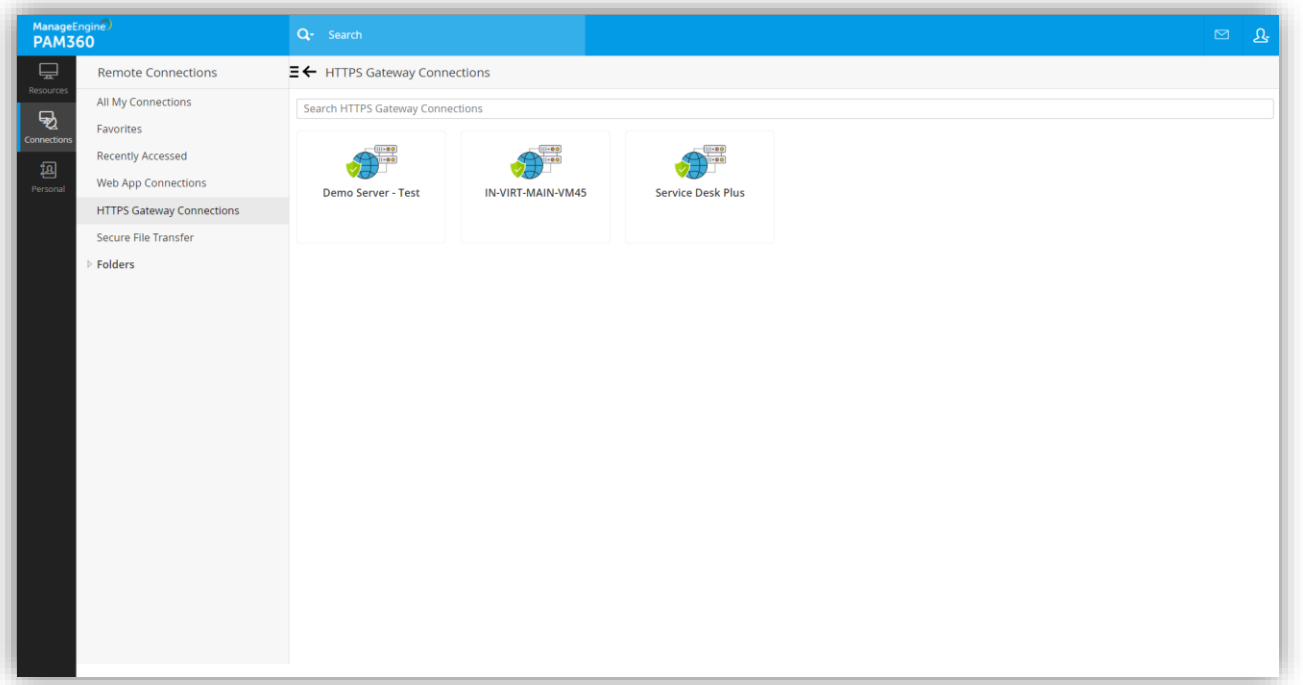
3.3 HTTPS Gateway Connections

Users with the **HTTPS Gateway Connection** role (administrators, connection users, users with custom roles) can take remote connections using the following methods:

1. From **Connections >> Remote Connections >> HTTPS Gateway Connections**.



2. In the **Resources** tab, beside the configured resources, from the **Open HTTPS Gateway Connections** option in the **Remote Connection**.



Once the session to the target URL is launched from the respective page, the web page will open in a new tab with the server URL and the custom port as provided (E.g., https://server-name:8285/GS_36c1cc2f_/{uri}.

Notes:

1. The HTTPS gateway server is limited to the configuration in the MSP Org and cannot be configured in client Orgs. Nevertheless, resources at client Orgs can be set up with resource URLs to use the HTTPS gateway server configured at the MSP Orgs for their HTTPS gateway connection.
2. Adjust the PAM360 cookie settings to authenticate a session to the ManageEngine products through the HTTPS gateway server. This update is necessary as ManageEngine application services like ADMP and ADFS have similar cookie names as in PAM360.

4. Functional Behavior in Multi-Server Environment

1. Disabling the HTTPS gateway server on a single server within the application scaling-configured environment will not stop the gateway server entirely. Further, to stop the HTTPS gateway server entirely, you need to restart the PAM360 application on all the remaining available servers.
2. For the HTTPS gateway connection functions to work seamlessly on multiple servers (primary and secondary):
    i. The KeyStore path must be provided in the form of a common UNC path.
    ii. The port should be the same across multiple servers.
3. It is not possible to set up the HTTPS gateway server on the Read-Only server.

5. Limitations of HTTPS Gateway Server

1. We support adding only HTTPS-based web links as connections in PAM360.
2. If users navigate to sites different from the configured target URLs, their actions will no longer be routed through the HTTPS proxy server. This rule also pertains to websites utilizing external sites for authentication and related functions.
3. Currently, one can enter just the host name or domain name as the target URL, while the use of the target URL with the Uniform Resource Identifier (URI) is still unsupported.

4. We do not support websites that contain absolute css and js source paths.
5. We do not support websites that allow requests only from trusted domains.
6. Connections to other ManageEngine product URLs such as Password Manager Pro, ServiceDesk Plus cannot be authenticated as they share common cookies with PAM360.

Working with Files in PAM360

PAM360 allows the bidirectional file transfer between two systems through the Secure File Transfer Protocol (SFTP). Accomplish this by installing the SFTP server in the target remote systems. The size limit for upload through the SFTP file transfer mechanism is 6GB. This allows PAM360 to authenticate the connection and securely transfer large files without the risk of security breaches. Besides file transfer, PAM360 permits bidirectional upload and download of files between your machine and the remote connection you have established, without the need for an actual remote session. This upload and download mechanism is made possible through the Secure Copy Protocol (SCP). The size limit for upload through SCP mechanism is 5 GB.

There are three ways to handle files in PAM360:

1. **Uploading Files**
2. **Downloading Files**
3. **Bidirectional File Transfer**

Prerequisite

For a successful file transfer, it is mandatory to install the Secure File Transfer Protocol (SFTP) server in all the target remote systems that will be involved in file transfer functions.

1. **Notes:**
   The upload limit for **SFTP** and **SCP** is **6 GB** and **5 GB** respectively. There is no size limit for download through SFTP file transfer mechanism.
2. **SFTP** option will be disabled for the accounts configured with SSH command control.

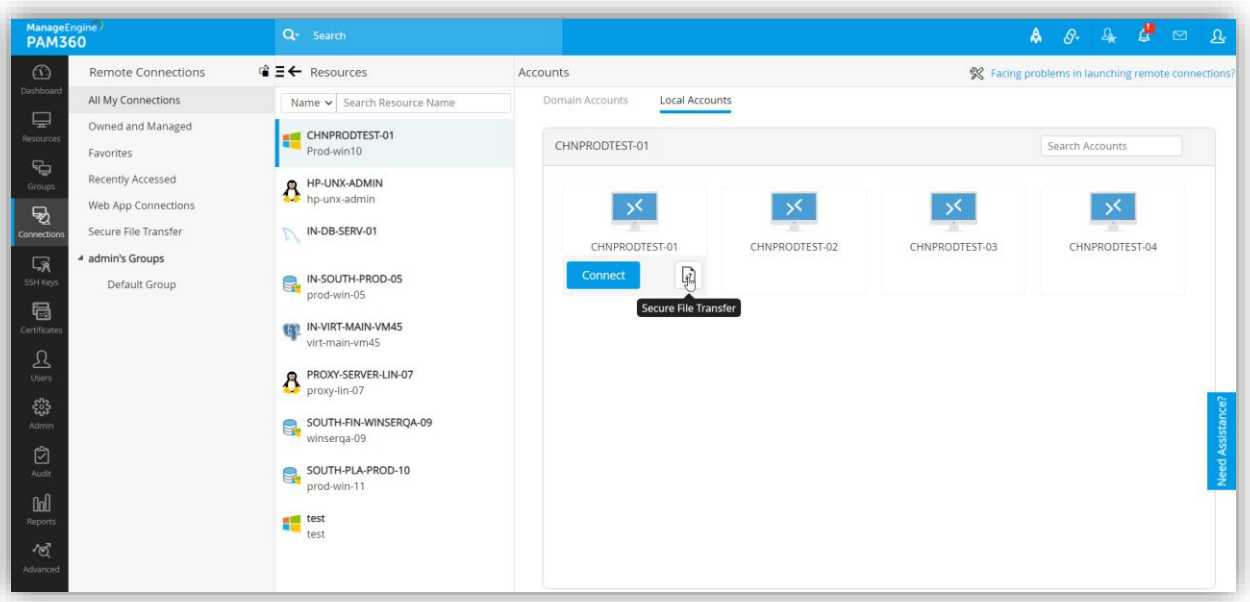
1. Uploading Files

You can upload files in two ways; to a directory in the remote system and to a particular account.

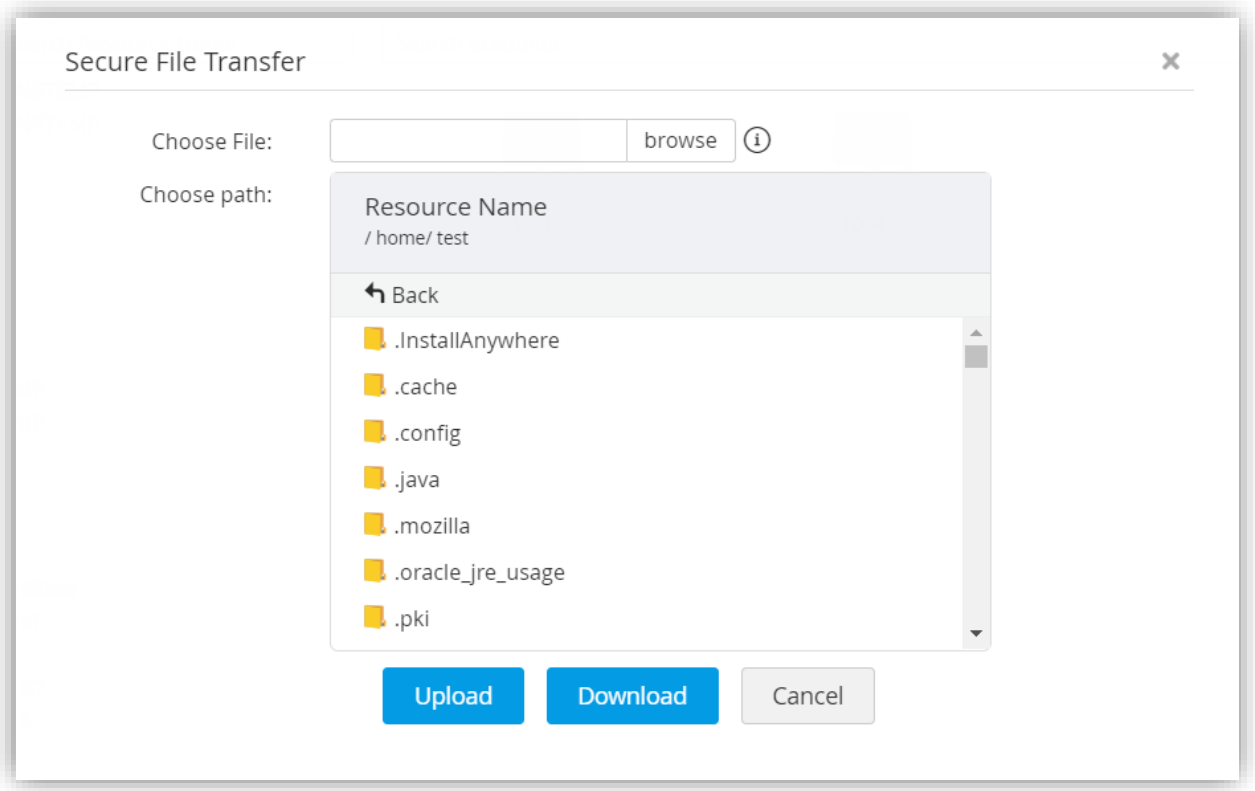
1.1 Uploading Files to Remote System Directory

Follow the below steps to upload files to a directory in the remote system from your local or domain account:

1. Navigate to the **Connections** tab and click the name of a resource from the left pane. Now, the display area on the right will display all the accounts that belong to the selected resource.
2. Hover your mouse over the thumbnail of an account, click the file transfer icon and click **Secure File Transfer**.



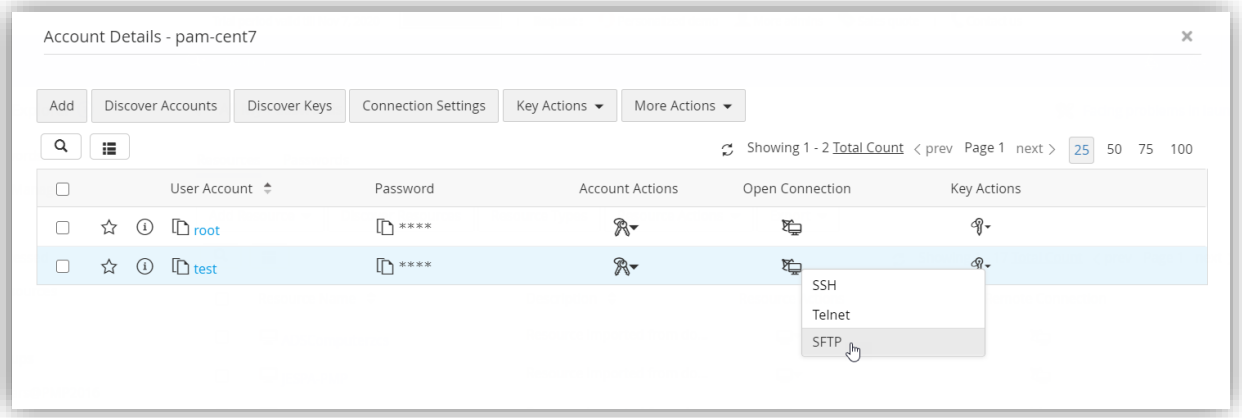
3. The **Secure File Transfer** dialog box will open up, in which PAM360 will authenticate the connection and all the directories in that system will be listed in the **Choose path** section. Click the required directory name to choose it.
4. Click **Browse** and choose a file to upload from your local computer.
5. Choose the required directory and click **Upload**.



1.2 Uploading Files to Account

Alternatively, to upload a file to a particular account, follow the below steps:

1. Navigate to the **Resources** tab, click the name of the required resource and the **Account Details** dialog box appears.
2. Beside the required account, click the **Open Connection** icon and click **SFTP** from the dropdown. The **Secure File Transfer** dialog box will open up. Here, click the required directory name under **Choose path**.



3. Click **Browse** and choose a file to upload from your local computer.
4. Choose the required directory and click **Upload**.

You will get a confirmation message once the file is uploaded successfully. In case of an upload failure, navigate to **Audit >> Resource Audit** for more details.

2. Downloading Files

You can download files in two ways; from a directory in the remote system and from a particular account.

2.1 Downloading Files from Remote System Directory

Follow the below steps to download files from a directory in a remote system to your local or domain account:

1. Navigate to the **Connections** tab and click the name of a resource from the left pane. Now, the display area on the right will display all the accounts that belong to the selected resource.
2. Hover your mouse over the thumbnail of an account, click the file transfer icon and click **Secure File Transfer**.
3. The **Secure File Transfer** dialog box will open up, in which PAM360 will authenticate the connection and all the directories in that system will be listed in the **Choose path** section.
4. Click the required folder to display all the files and sub-folders present in it. Choose a file and click **Download**.

2.2 Downloading Files from Account

Alternatively, to download a file from a particular account, follow the below steps:

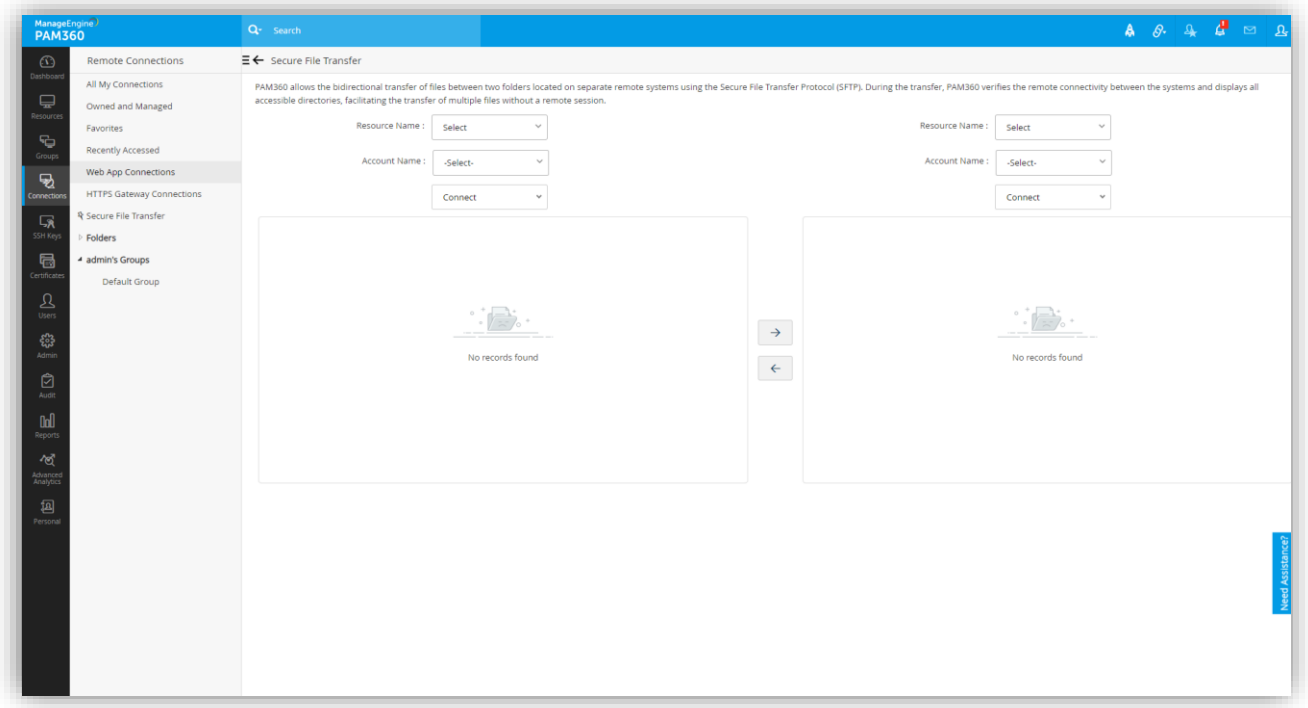
1. Navigate to the **Resources** tab, click the name of the required resource and the **Account Details** dialog box appears.
2. Beside the required account, click the **Open Connection** icon and click **SFTP** from the dropdown. The **Secure File Transfer** dialog box will open up. Here, click the required directory name under **Choose path**.
3. Click the required folder to display all the files and sub-folders present in it. Choose a file and click **Download**.

In case of a download failure, navigate to **Audit >> Resource Audit** for more details.

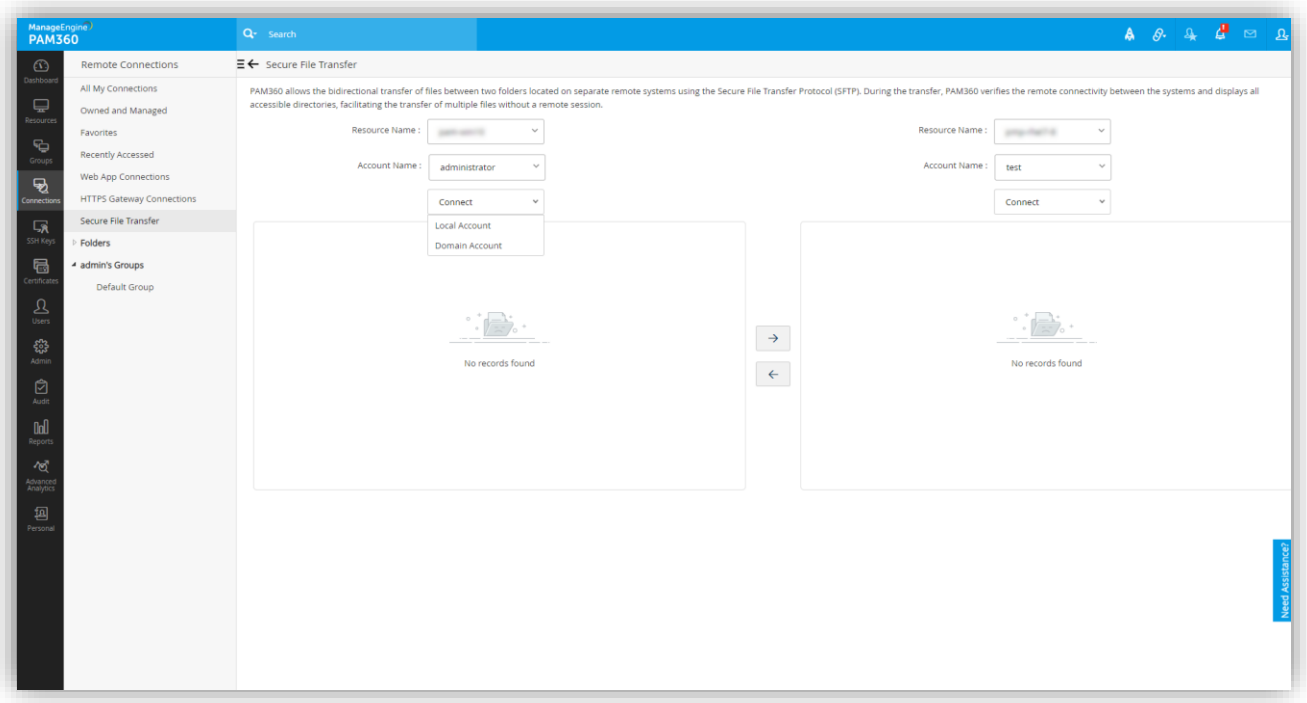
3. Bidirectional File Transfer

PAM360 web interface supports the bidirectional transfer of files between folders located on separate remote systems using the Secure File Transfer Protocol (SFTP). Follow the steps below to initiate a file transfer.

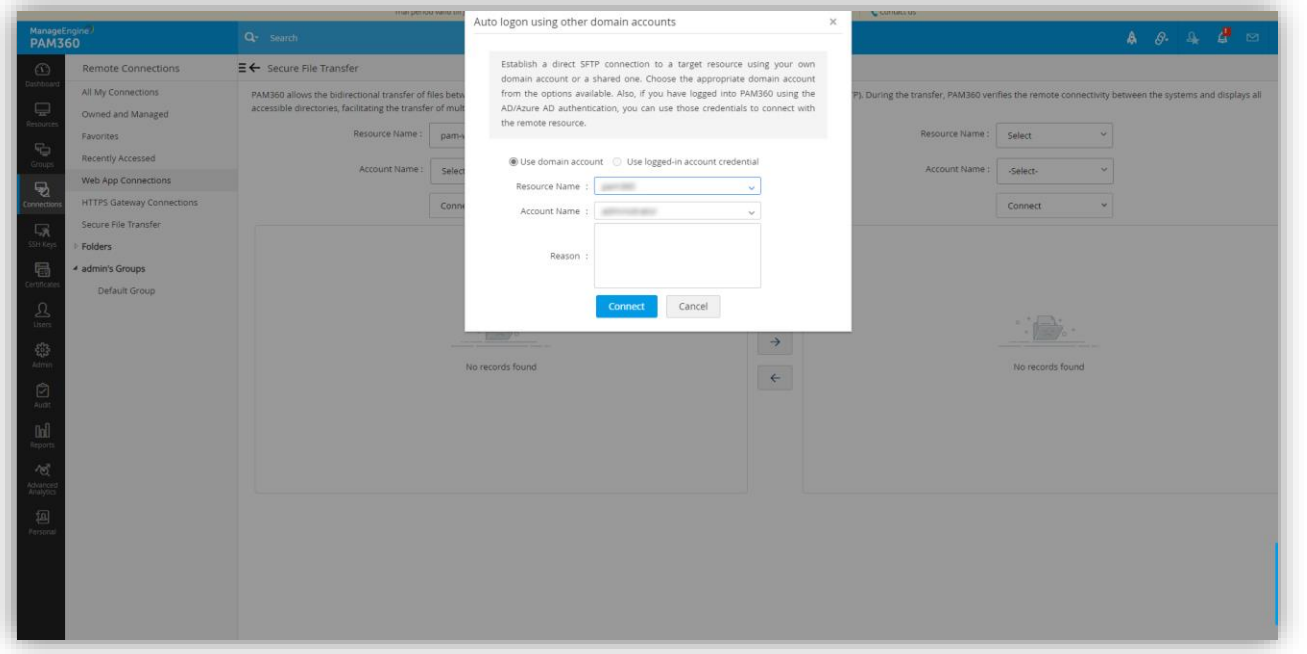
1. Navigate to the **Connections** tab and click **Secure File Transfer** on the left pane.
2. In this section, you will find two columns. The left column represents the origin folder, while the right column represents the destination folder.



3. To initiate the transfer, select the required **Resource Name** and **Account Name** using the drop-down menus from either of the available two columns, left and right.
4. Click the **Connect** dropdown and choose either **Local Account** or **Domain Account**.

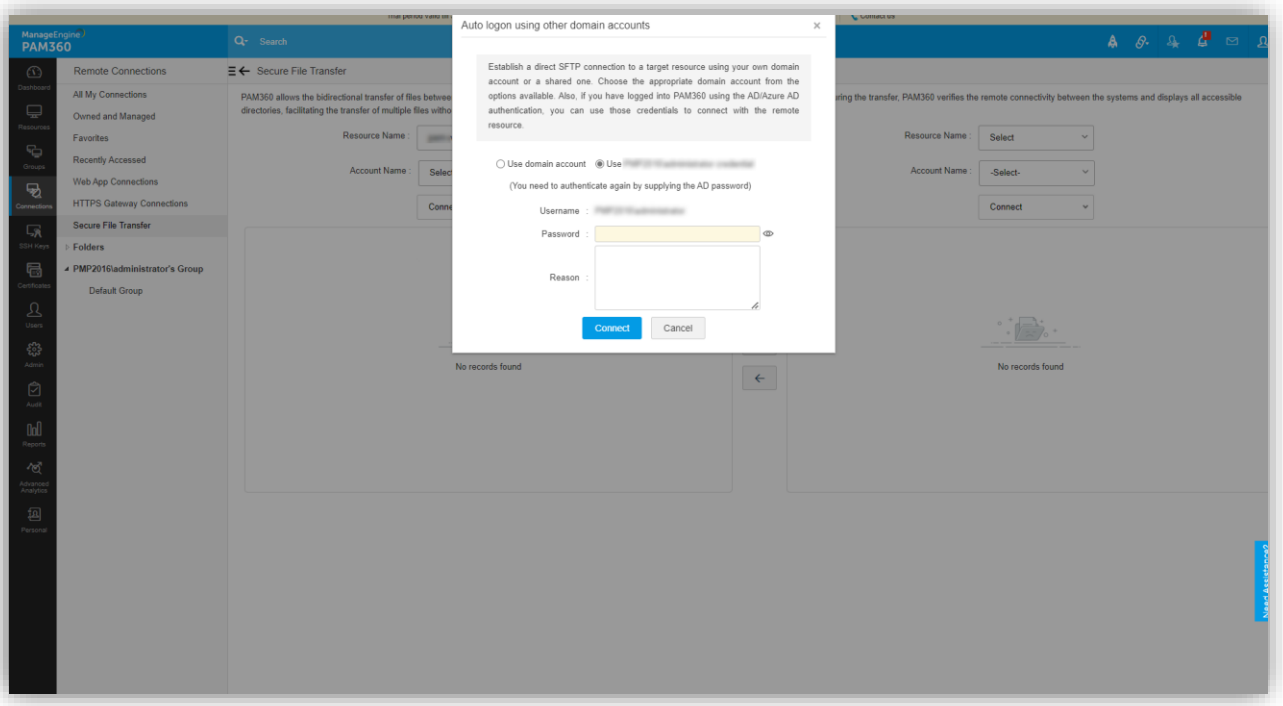


5. If you select the **Domain Account** option, you will see a pop-up box - **Auto logon using other domain accounts** with the **Use domain account** radio button enabled.

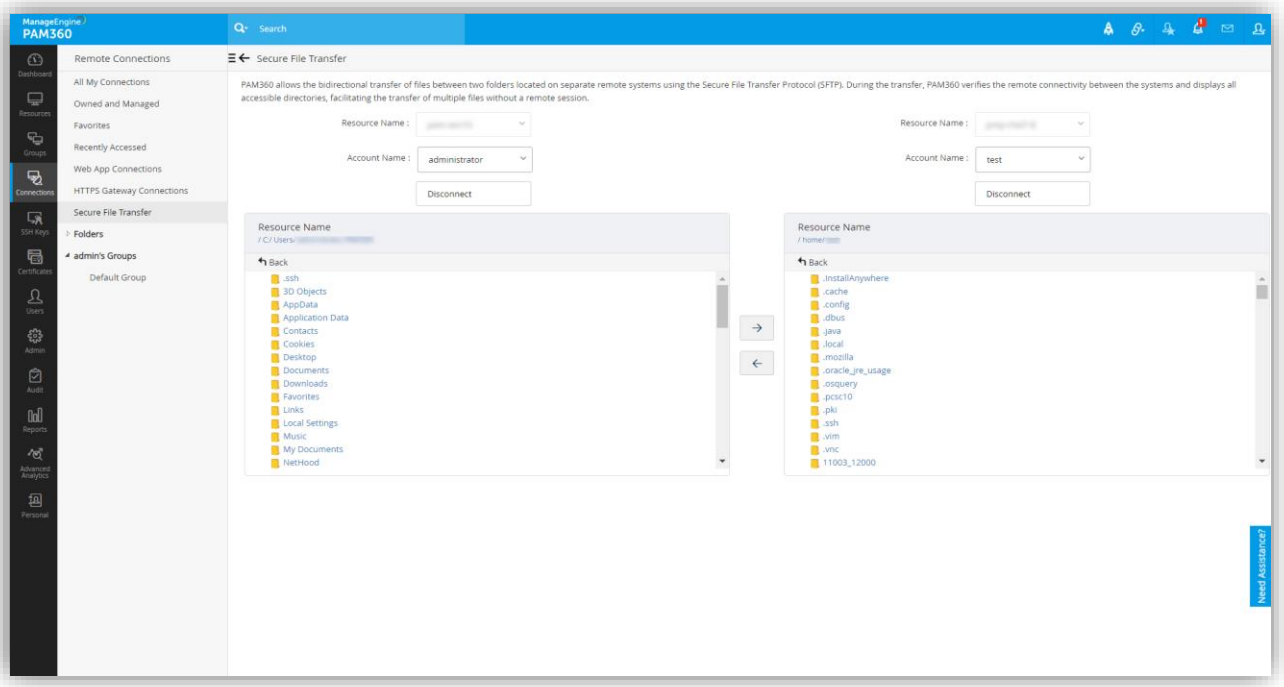


6. Select your domain account credentials using the **Resource Name** and **Account Name** dropdowns. Then, click **Connect** to establish a direct SFTP connection using the selected credentials.
7. If you have logged into PAM360 using the AD/Azure AD/ authentication, you will have the option to use your logged-in account credentials to connect to the remote resource.

8. Enter your logged-in account password in the required field and click **Connect**.



9. PAM360 will now authenticate the connection, and you will see all the folders in both systems under their respective sections.



10. Choose the required file from either of the columns and click the relevant arrow icon in the middle to initiate data transfer between the selected paths.

Once the file transfer is complete, you will see that file in the destination directory you selected previously. In case of transfer failure, navigate to **Audit >> Resource Audit** for more details.

Notes:

1. To perform file transfer on a resource for which Password Access Control is enabled, you need to send a password request. Once the resource owner approves your request, PAM360 will allow you to perform file transfers on that resource for the duration of your access.
2. Secure File Transfer works only for users with **File Transfer** permission in their user role. The two types of default user roles that have the File Transfer permission are:
    i. Admin roles **(Administrators, Privileged Administrators, and Password Administrators)**
    ii. **Connection User** role.
3. The Secure File Transfer function works only on two conditions:
    i. File transfer must be performed on resources that run on operating systems supported by PAM360. The operating system types supported by PAM360 are: Windows, Windows Domain, Linux, Mac, Solaris, HP UNIX, IBM AIX, HPUX, and JunOS.
    ii. The target resources must have the Secure File Transfer Protocol (SFTP) installed.

Working with Remote Apps

PAM360 allows you to remotely connect to applications (apps) already configured in target systems. Also, launch direct connections to the remote systems. Adding remote apps to RDP connections increases the accessibility and ease of use when connecting to the remote systems. IT admins use the remote apps to gain easy control over the privileged sessions, as it limits users' access to only specific applications launched. For example, a user clicking the Remote App configured for Notepad will be able to access only the Notepad application in the remote machine and will not be allowed to access any other programs.

You will be able to perform the following actions on remote apps:

1. **Adding Remote Apps Manually**
2. **Discovering Remote Apps Automatically**
3. **Associating Remote Apps with a Resource**

Before you jump to the actions, make sure the following prerequisites are satisfied:

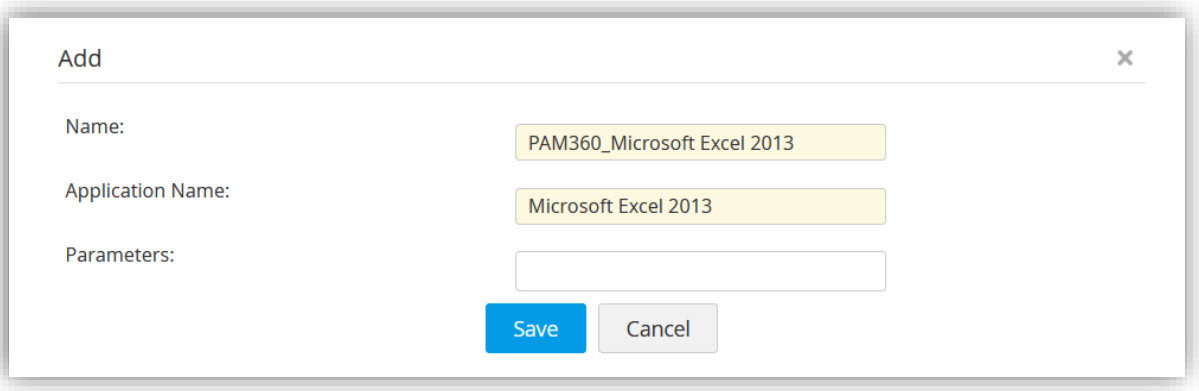
Prerequisites

1. To use the application-based connection in PAM360, make sure you configure the Remote App feature in the main Domain Controller machine. For more details on setting up Remote Apps in Windows server machines, click here.
2. To discover the remote apps automatically, make sure you have installed the Microsoft .NET framework and Visual C++ Redistributable (for Visual Studio 2015 and above).

1. Adding Remote Apps Manually

PAM360 allows you to add remote apps manually and associate them to the resources based on your requirement. You will be able to access these remote apps only through the associated resources. Follow the steps below to add remote apps to PAM360:

1. Navigate to **Admin >> Connections >> Remote App.**
2. Click **Add.**
3. In the pop-up that opens, enter the following attributes:
    i. **Name:** Enter the name for the remote app to be displayed in PAM360.
    ii. **Application Name:** Enter the name of the application as it is in the remote system.
    iii. **Parameters:** Parameters can be a specific folder or a particular file to be opened when the application is invoked. **Example:** If the application name is notepad.exe, the parameter can be a specific text file to be opened using the notepad application. This is an optional field.
    iv. Click **Save** to save changes.



Now, you have successfully added a remote app manually.

2. Discovering Remote Apps Automatically

In addition to manually adding remote apps, PAM360 has the capability to discover remote apps from machines which already have remote apps configured in them. Before proceeding with the setup, ensure you have read the prerequisites. Follow the below steps to discover remote apps automatically:

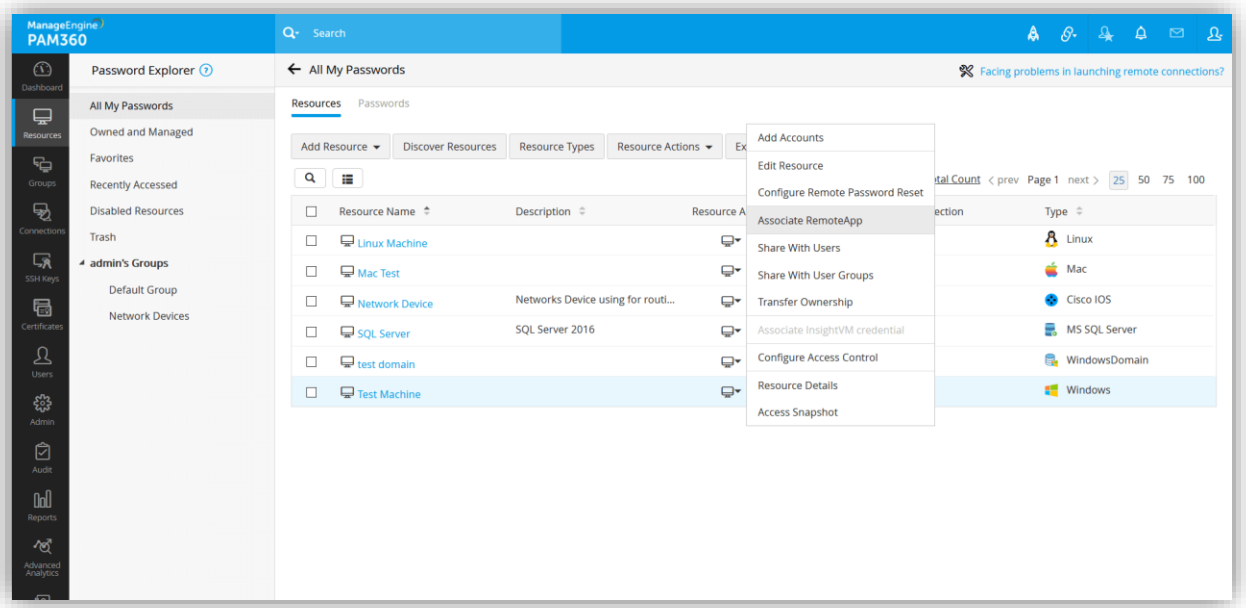
1. Navigate to **Admin >> Connections >> Remote App.**
2. Click **Discover.**
3. From the **Choose Connection** drop-down, choose a machine that has remote apps configured in it and click **Fetch.**
4. All the remote apps available in the chosen machine will be listed below. Select the remote apps using checkboxes and click **Add and associate.**
5. The selected remote app will be added to the Remote App dashboard.
6. From here, you can associate the remote app to any available connection through the **Configure remote app** option under **Actions.**

3. Associating Remote Apps with a Resource

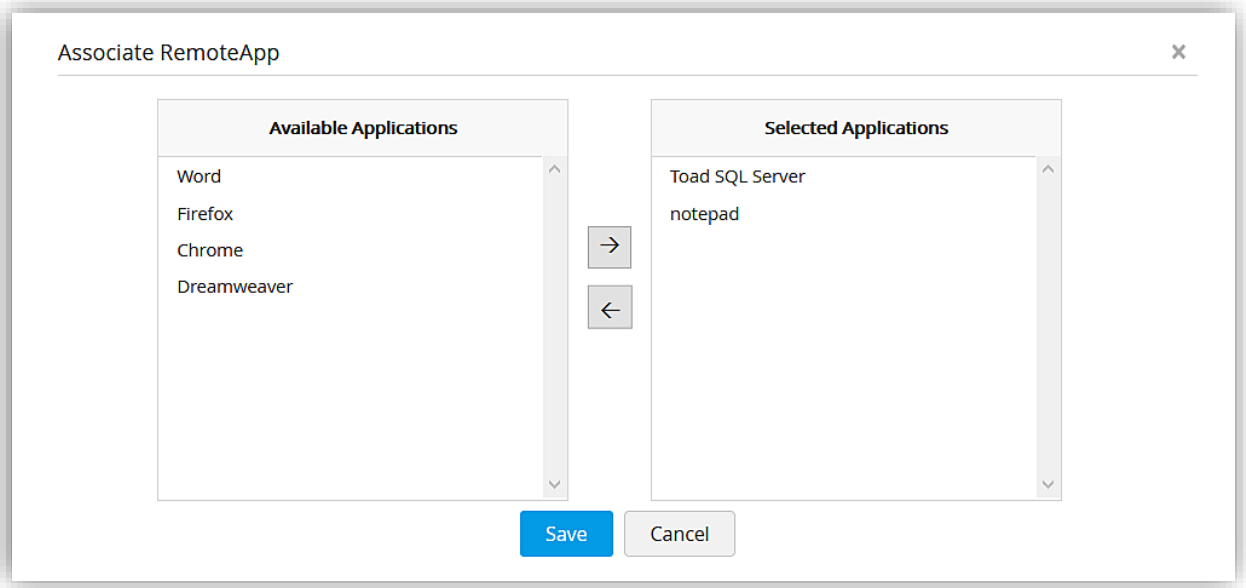
> **Note:** PAM360 supports Remote App only for Windows and Windows Domain resources.

PAM360 allows you to associate the remote apps that were added manually or discovered into PAM360 with a selected resource. After this, you will be able to access these remote apps through the resource. Read further to know about associating the remote apps:

1. Click the **Resources** tab.
2. From the list of available resources, click **Resource Actions >> Associate Remote App** beside the particular resource to which you want to associate the remote apps.



3. In the pop-up that appears, select the applications from the **Available Applications** column and move them to the **Selected Applications** column using the arrow keys. Click **Save**.



Now, you have successfully associated the remote apps to the selected resource.

Auto Logon Helper

PAM360 stores the passwords of remote systems and applications. Normally, organizations use tools such as remote desktop applications, Putty or SecureCRT to connect to remote target systems. PAM360's **Auto Logon Gateway** feature provides an option to automatically connect to the remote target systems and applications without the need for handling passwords in plaintext.

At the end of this section, you will have learned the following:

1. **How the Auto Logon Gateway Feature Works**
2. **How to Set Up Auto Logon Gateway**
3. **Invoking Auto Logon Through Gateway**

1. How the Auto Logon Gateway Feature Works

PAM360 comes bundled with RDP, SSH, and SQL gateway engines. This feature allows the users to launch remote terminal sessions from within their browser. All the sessions invoked from the **Connections** tab are initiated and tunneled through the PAM360 server. This allows the administrators to disable RDP, SSH, and SQL permissions in the end user systems such as laptops and desktops but still allow users to access the target systems through tunneled remote sessions. The remote terminal sessions are emulated inside the browser tab and hence there is no need for installing any plug-in or agent in the end points. The only requirement is that the browser should be HTML 5 compatible (For example, IE 9 or above, Firefox 3.5 or above, Safari 4 or above, and Chrome).

As soon as an administrator adds a resource that supports one of these remote terminal session types, the feature becomes available to all users in the system who have access to that resource, with no further configuration anywhere. In addition, the **Connections** tab will allow users to easily locate remote accounts and launch a session with a single click. The entries in the **Connections** page with the names **RDP and VNC Connections**, **SSH Connections,** and **SQL Connections** belong to this type and come bundled with the product.

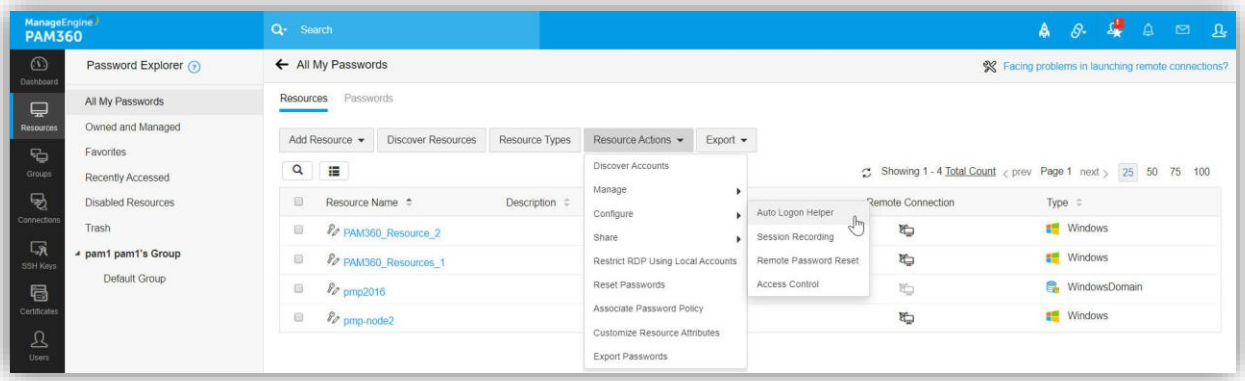
2. How to Set Up Auto Logon Gateway

You can set up Auto Logon Gateway in three ways:

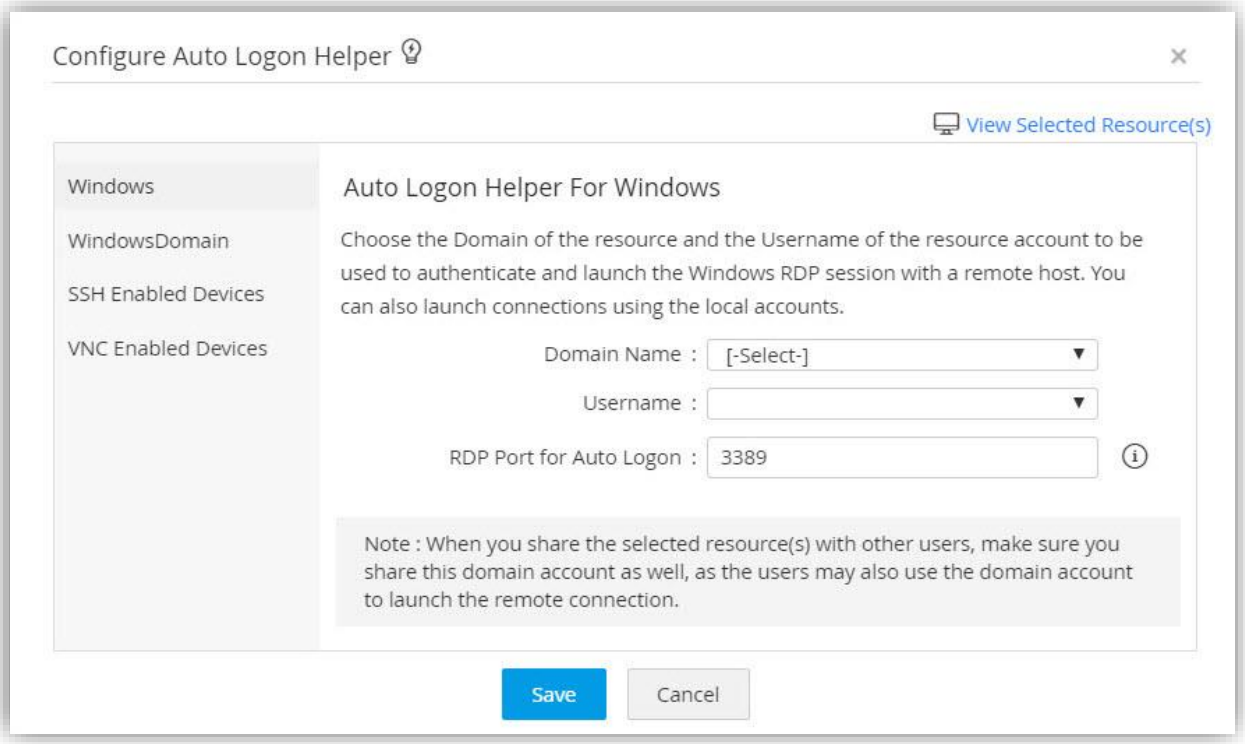
1. RDP and VNC Connections
2. SSH Connections
3. SQL Connections

2.1 RDP and VNC Connections

1. All Windows systems can be automatically connected to an RDP session. To log into a Windows resource, you need to configure either a domain account or a local account that can be used by users to authenticate and launch a Windows RDP session with the remote host. Alternatively, an administrator can also allow users to launch RDP sessions using their AD account with which they have logged into the PAM360 vault.
2. To configure a domain account, go to the **Resources tab and** select the desired resource(s).
3. Click **Resource Actions >> Configure >> Auto Logon Helper** from the drop-down.

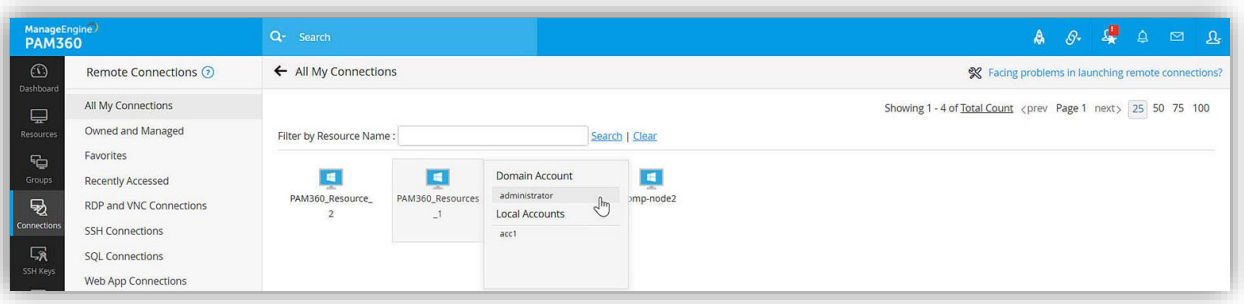


4. In the Configure Auto Logon Helper window that opens, configure the domain account by choosing the required domain from the **Domain Name** drop-down, specify the **Username** and the **RDP Port for Auto Logon.**

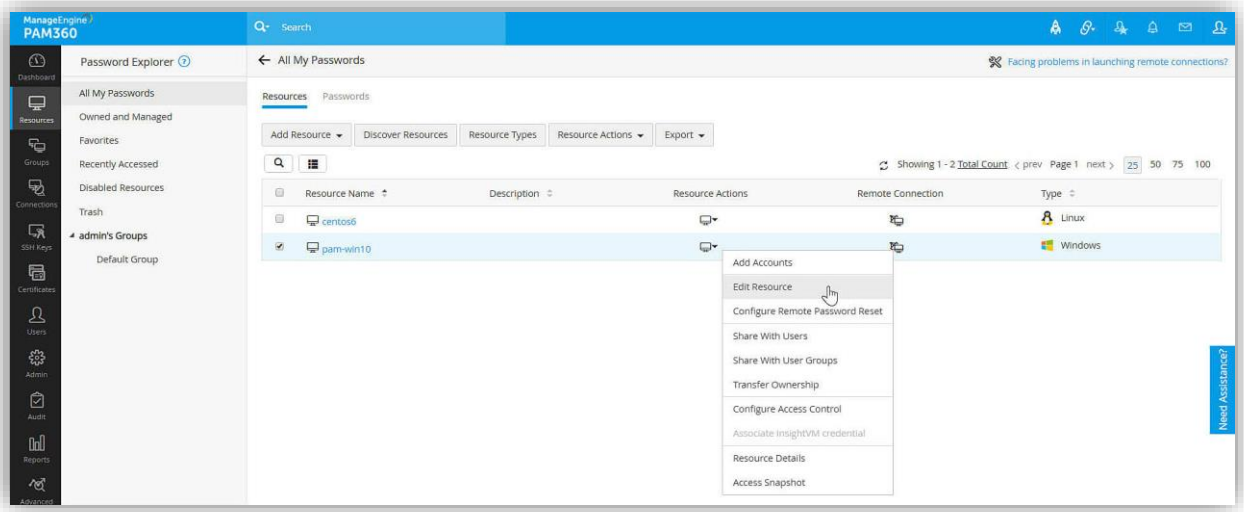


5. Click **Save.**

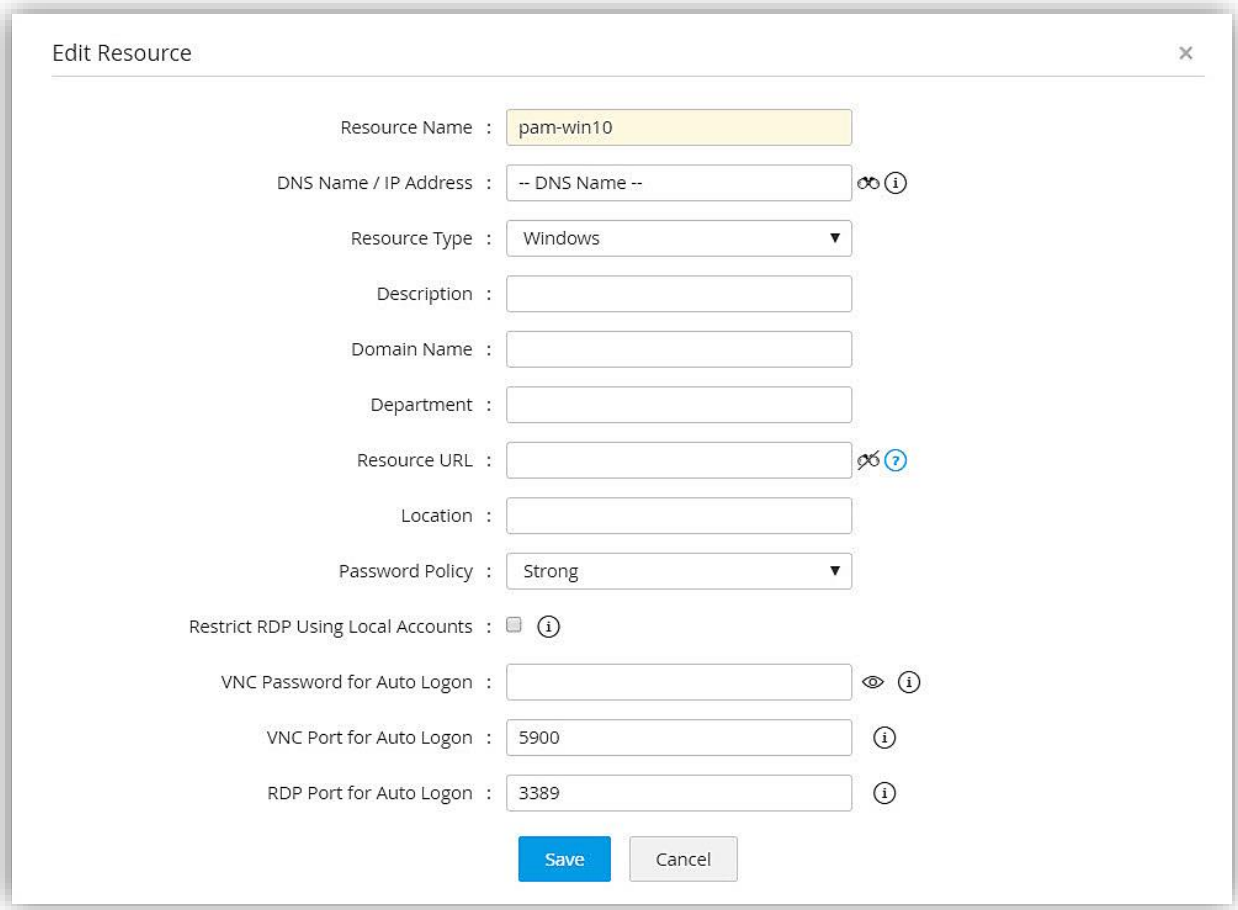
6. Once you have configured your domain account, it will appear under the **Connections** tab as shown below:



7. To customize the port for RDP and VNC for each resource, go to the **Resources** tab, select the desired resource(s) and click **Resource Actions >> Edit Resource.**

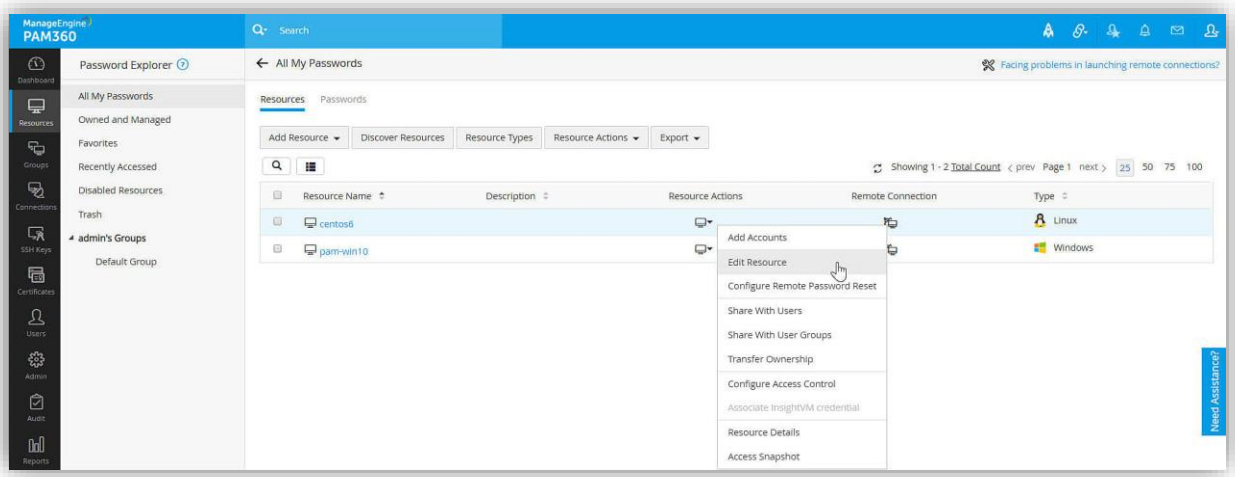


8. In the **Edit Resource** window that opens, enter the RDP and VNC ports in the respective fields, and click **Save.**

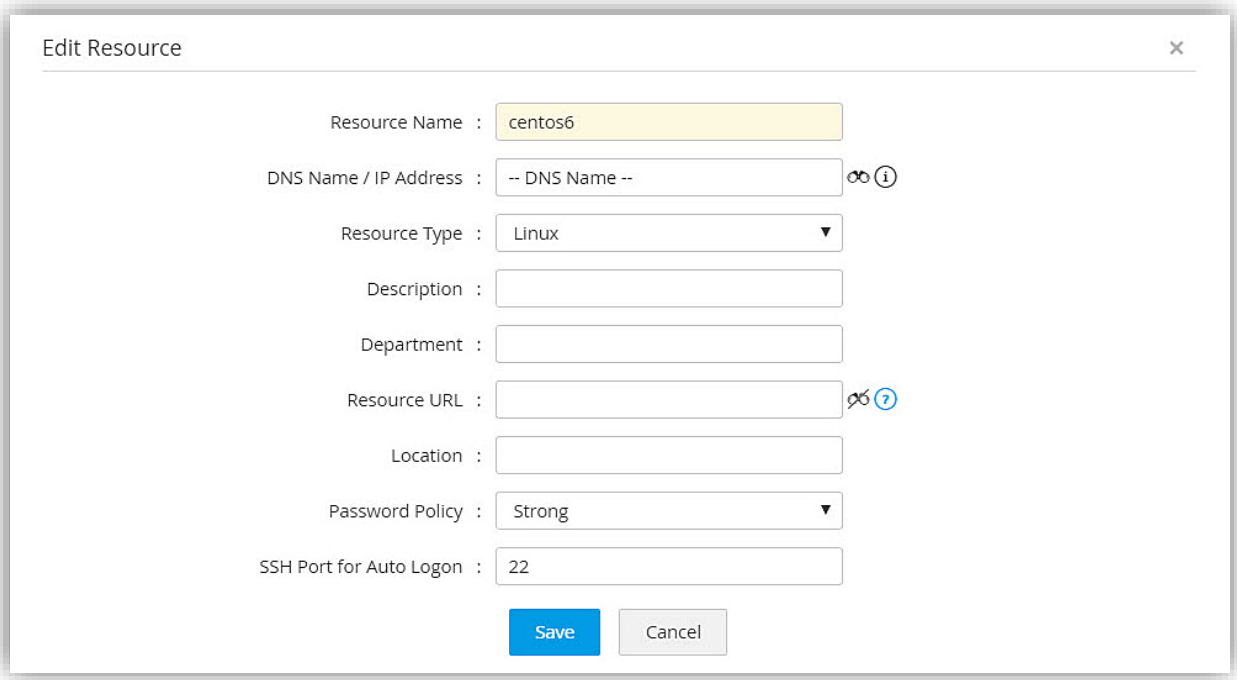


2.2 SSH Connections

1. Any SSH based device such as Linux servers or network devices can be added into PAM360 as a resource. This allows administrators and other users to connect to the target system via a remote SSH session.
2. You can configure the SSH port in which the SSH service is listening on the remote host. PAM360 will use this port for launching the session. To do this, navigate to the **Resources** tab, select the desired resource(s), and choose **Resource Actions >> Edit Resource** from the drop-down beside the resource(s).



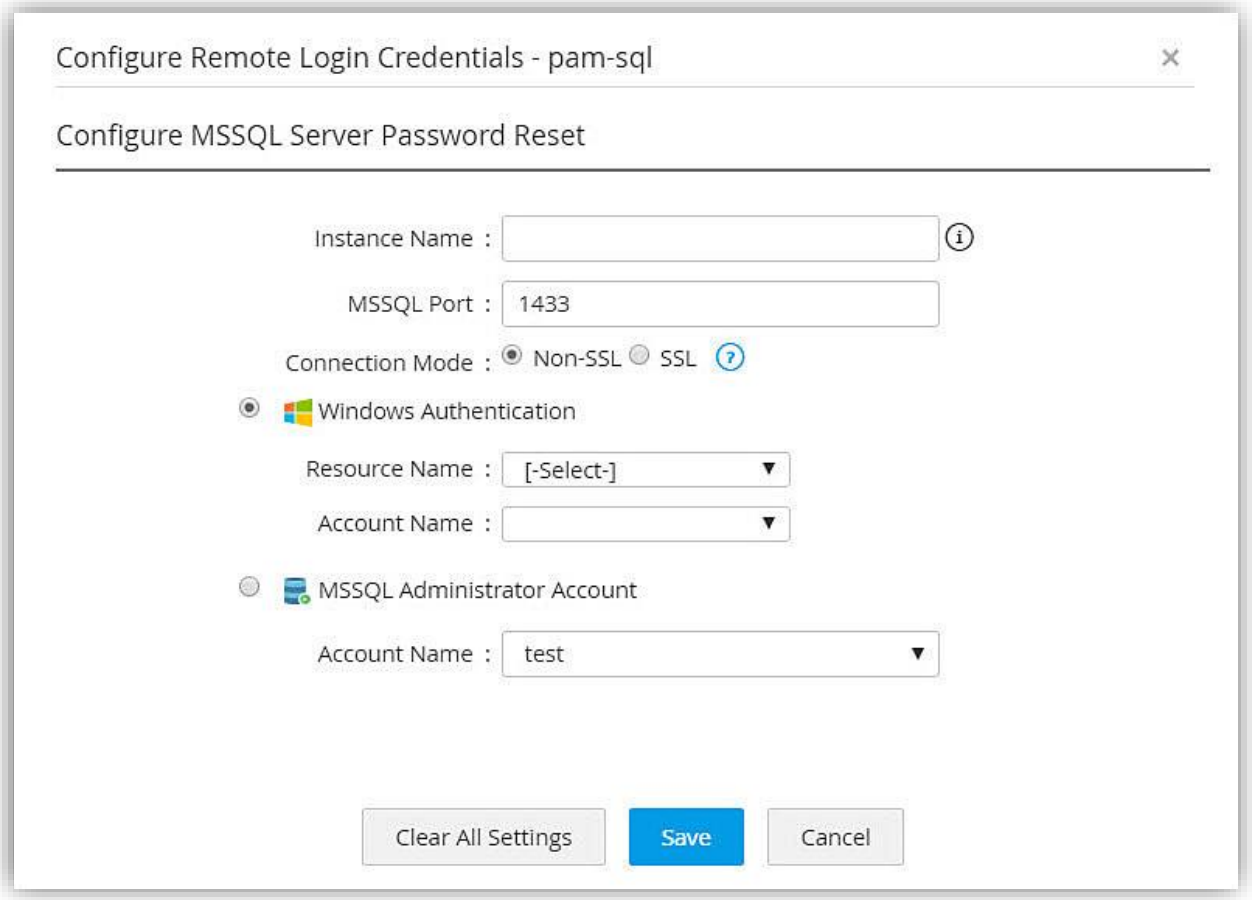
3. In the **Edit Resource** window that opens, enter the SSH port through which you want to connect to the remote system, and click **Save.**
4. The end users will be able to launch SSH sessions using the local SSH accounts that are shared with them by the administrators.



2.3 SQL Connections

You can add a database instance as a resource in PAM360 to enable remote connections. This feature is supported for PostGres and MS-SQL databases. Note that the SQL connections are CLI based, meaning they allow users to execute queries to perform operations.

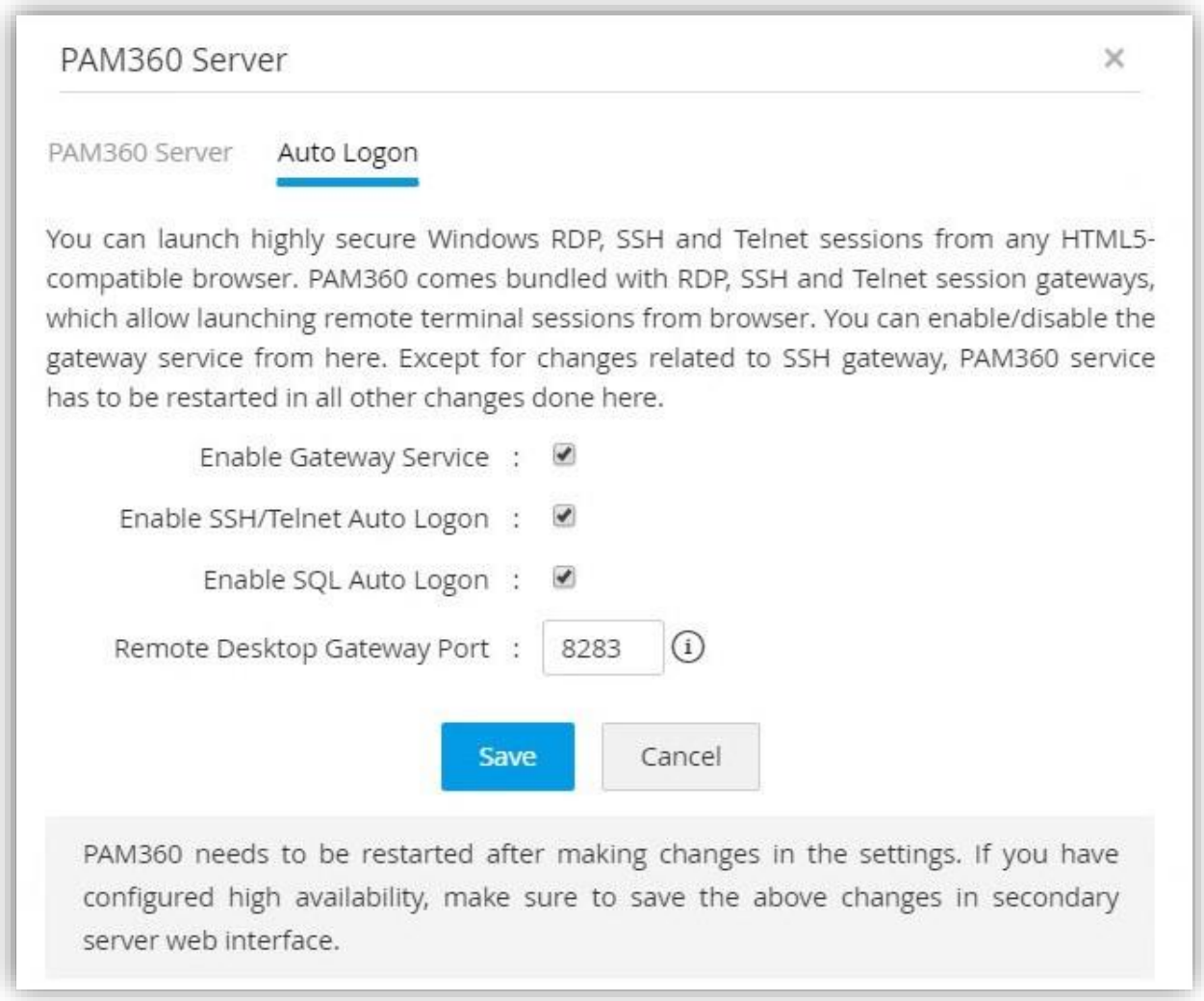
1. To configure an SQL connection for remote sessions, navigate to the **Resources** tab, click **Resource Action** present next to the SQL resource and select the **Configure Remote Password Reset.**



2. Specify the port number that needs to be used for SQL connection. The SQL session will be initiated in this port with the account that is shared with the users.

2.4 Port Requirements for Client Access

1. The Windows RDP Auto Logon Gateway listens at port 8283 in PAM360 server by default. This is a secure web socket port (wss://) and you should allow traffic to this port from the end user machines for this feature to work.
2. You can change this port by navigating to **Admin >> Configuration >> PAM360 Server.**
3. In the new window that opens, switch to **Auto Logon** tab and then enter the port in the **Remote Desktop Gateway Port** field.
4. PAM360 web server (8282 in PAM360 server) and this gateway should open and listen at different ports. The SSH and Telnet Gateways have no such requirement as they use the same PAM360 web server port for all communication.

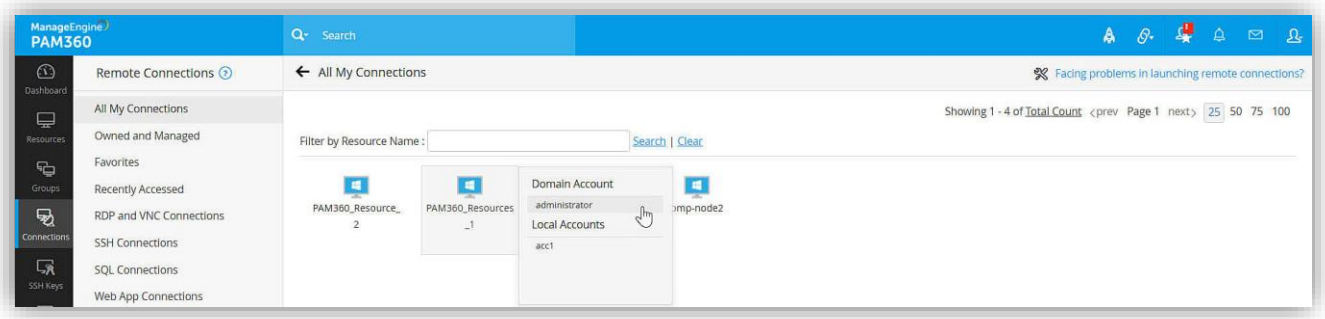


Note: When PAM360 is installed, it generates a self-signed SSL certificate for the instance which is also used by the Auto Logon Gateway to encrypt the traffic. It is recommended that you apply a CA signed certificate to the PAM360 instance before opening it out for end users. In case of a self-signed certificate, connecting to the gateway is not possible unless users explicitly mention the gateway port in the URL, accept the warning and install the self-signed certificate. (For steps to generate unique SSL certificate, refer to this section of our site).

3. Invoking Auto Logon Through Gateway

As soon as an administrator adds a resource that supports one of the three remote terminal session types (Windows RDP, SSH and SQL sessions), the feature becomes available to all users in the system who have access to that resource, with no further configuration anywhere.

The **Connections** tab will allow users to easily locate remote accounts and launch a session with a single click.



Remote Connection to SSH-based Devices Using SSH Keys

PAM360 allows you to launch remote connections to SSH command-based remote systems directly from the PAM360 web interface through SSH keys. This feature is in addition to its ability to launch remote connections using the corresponding user account's login credentials. To launch remote connections through SSH keys, you need to associate the SSH keys with the required accounts. This document discusses the procedure to achieve this.

1. Associating keys with accounts
    1.1 Creating a new SSH key and associating it with an existing account
    1.2 Associating an existing key with a new account
    1.3 Associating an existing key with an existing account
    1.4 Enabling private key login option for an existing account
2. Enabling PKI authentication option for remote password reset

1. Associating SSH Keys with Accounts

You can enable remote connections through SSH keys using the option **Use private key to login to this account instead of password** available while creating an account or an SSH key. However, for the remote connection to work via the private key, you need to associate the SSH keys with the required accounts. There are four different ways of associating keys with accounts before enabling the private key login.

Notes:

1. Although it is possible to associate one SSH key with multiple user accounts through the **Key Actions >> Associate Keys** option, as a best practice, it is recommended to associate only one SSH key per account to preserve data security.
2. We strongly recommend the **Map private key to locally, if remote key association fails** option only for the cases, where the target server is reachable only through a jump server.

Prerequisite

Before proceeding with the steps, check if the private key option is enabled for the Linux resource type. If not, follow the below steps to enable the option:

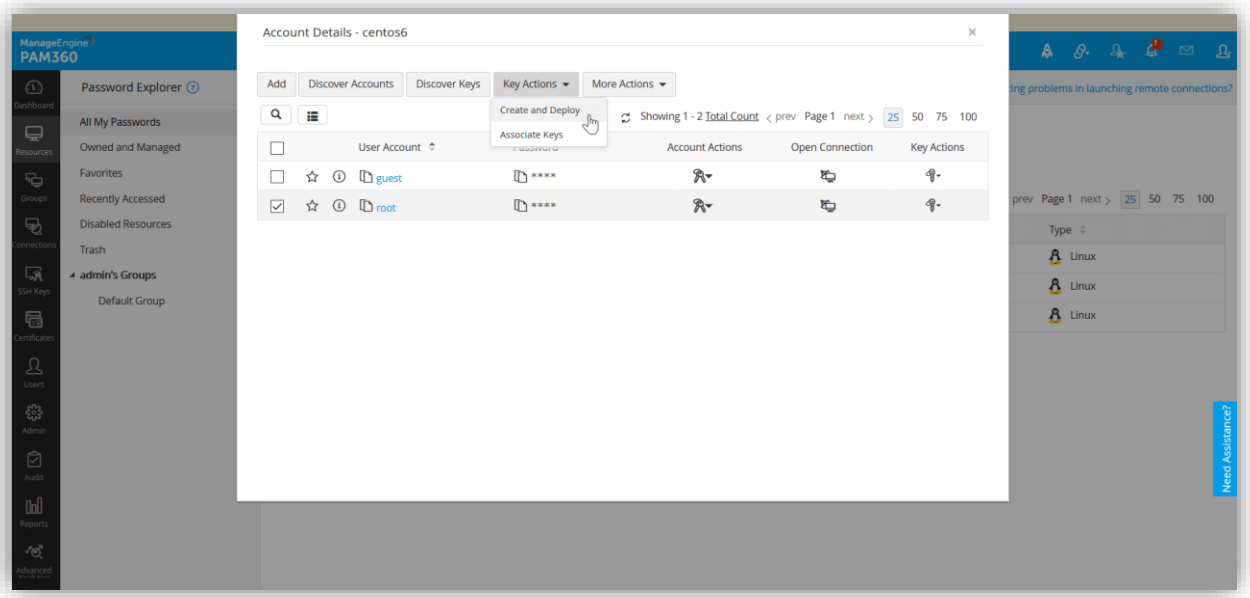
i. Navigate to **Admin >> Resource Config >> Resource Types**.

ii. Click the edit icon beside the **'Linux'** resource type.

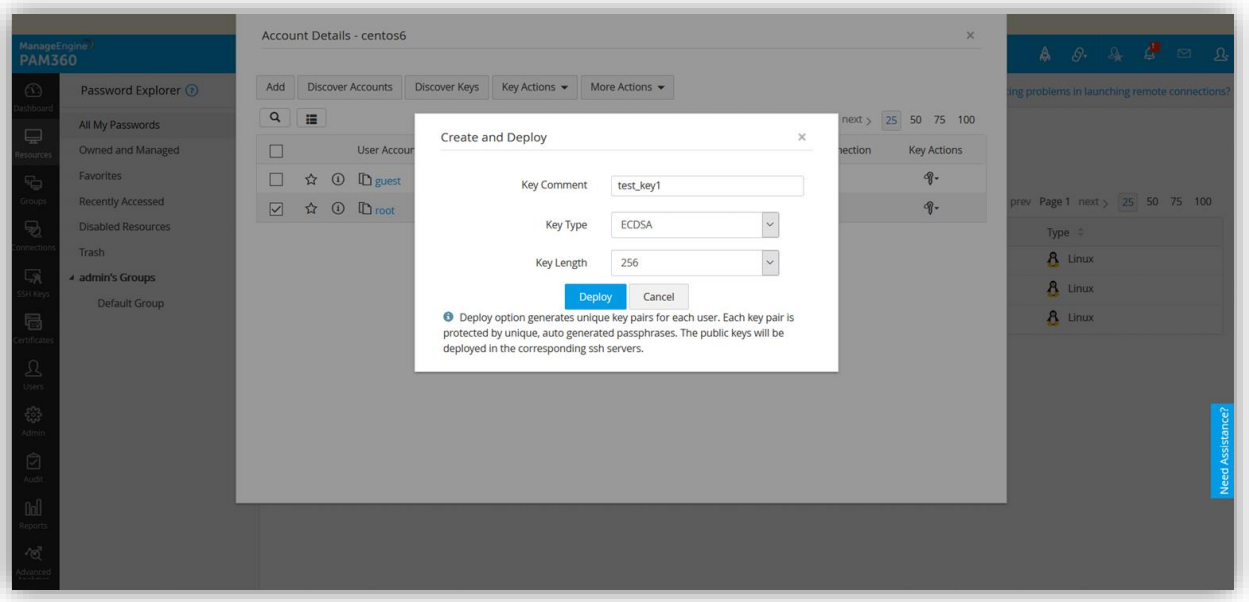
iii. Under **Account Attributes**, enable the **Private Key** option and click **Save**.

1.1 Creating a New SSH Key and Associating it with an Existing Account

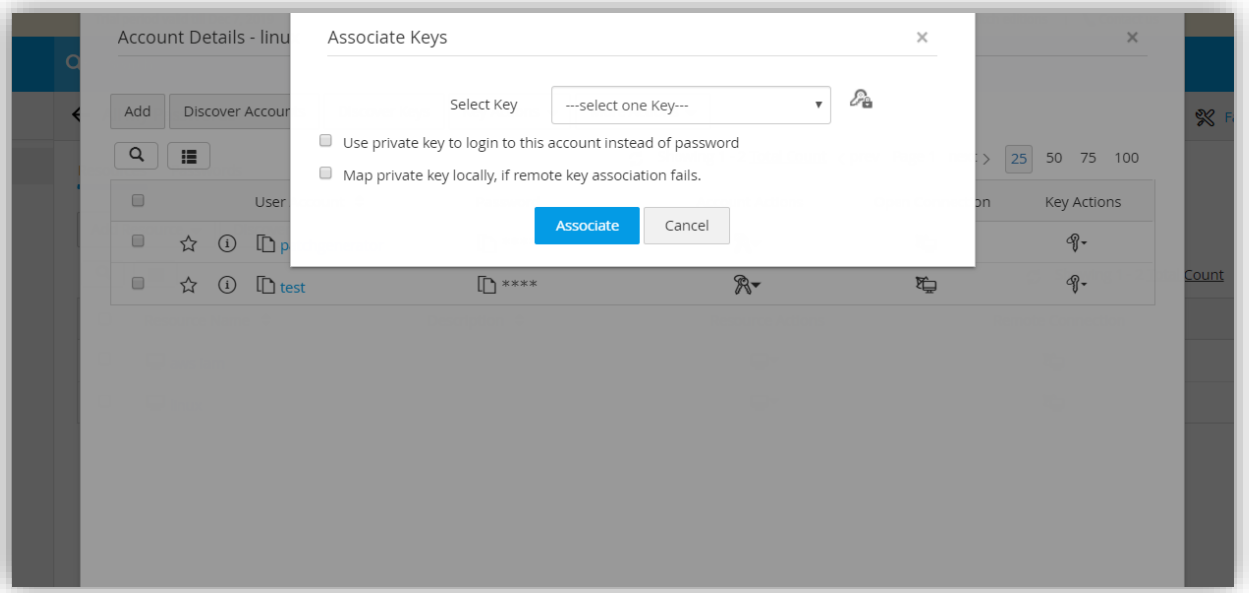
1. Navigate to the **Resources** tab and click the resource under which the required accounts are added.
2. Select the required account and click **Create and Deploy** from the **Key Actions** drop-down at the top.



3. In the pop-up form that appears, enter the details such as **Key Comment, Key Type** and **Key Length**. Click **Deploy** to save the changes. The newly created key will be associated with the selected account.



4. To associate an existing key with an existing account, select the required account, navigate to **Key Actions >> Associate Keys** to choose the key.
5. Select the checkbox **Use private key to login to this account instead of password** to authorize remote connections using SSH keys instead of account credentials.
6. Select the checkbox **Map private key locally, if remote key association fails** to force map SSH keys to user accounts, even if the target systems are not reachable.
7. Click **Associate** to save changes.

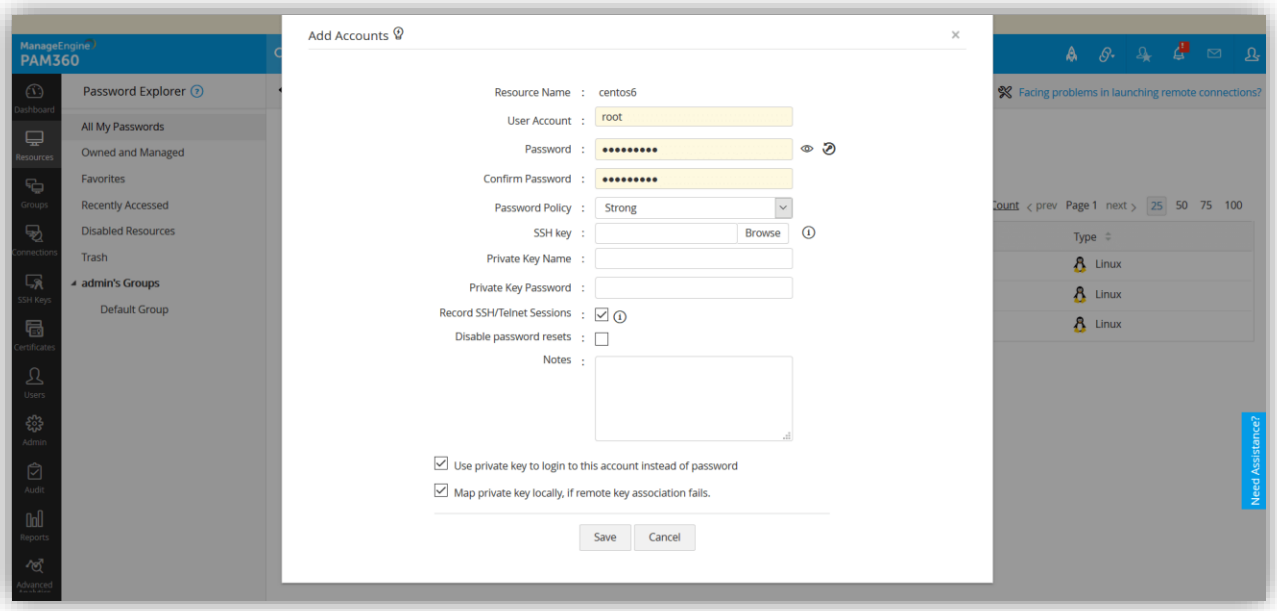


Note: Click here this to learn how to create a key from the **SSH Keys** tab and then associate it with an account.

1.2 Associating an Existing Key with a New Account

You can still import an existing SSH key created using a key generation tool into PAM360, even if you do not have the **SSH Keys** tab activated in your environment. Create a new account and add the existing key to it. Follow the below steps:

1. Refer to the section Adding an Account to a Resource to create the new account. In the process, select the checkbox **Use private key to login to this account instead of password** to authorize remote connections using SSH keys instead of account credentials.
2. Select the checkbox **Map private key locally, if remote key association fails** (shown in the below screenshot) to force map SSH keys to user accounts, even if the target systems are not reachable.
3. Click **Save** to add the account.



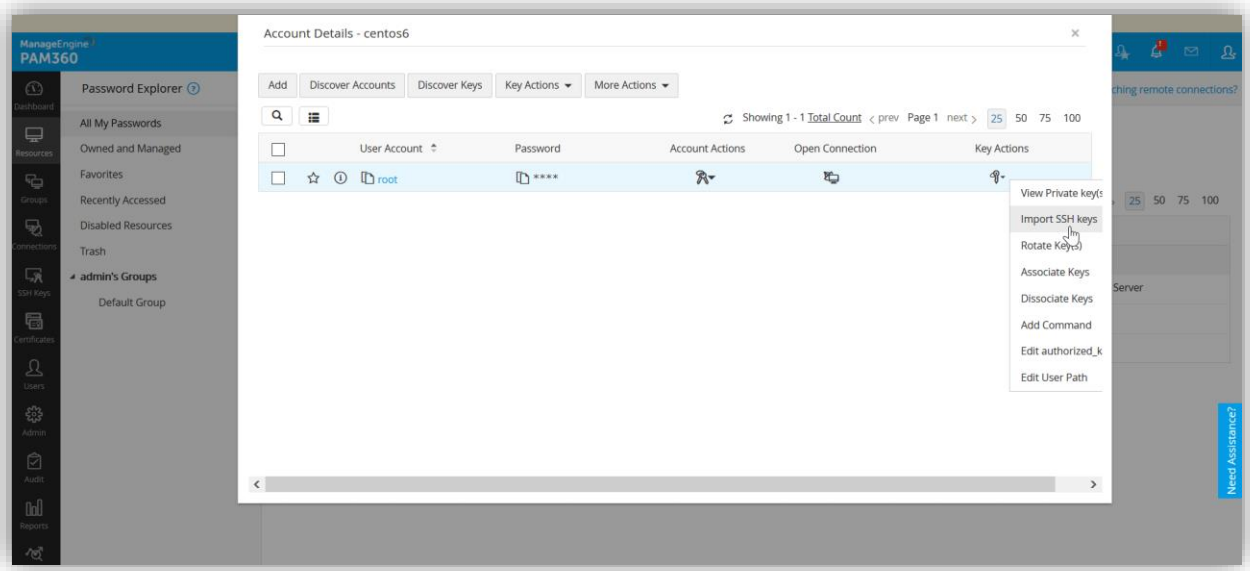
Note: If Account level access control is deactivated and there is a Resource level access control already in place for the resource, then the Resource level access control will be automatically applied to the account as well. Check the **Precedence in Password Access Control** section to more about how precedence works for access control settings.

1.3 Associating an Existing Key with an Existing Account

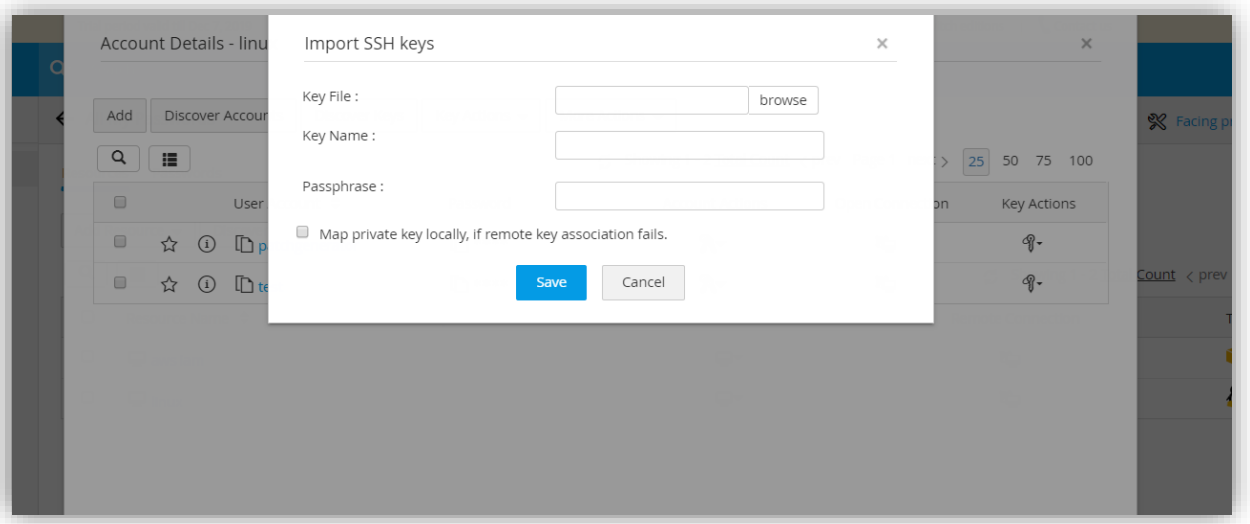
You can also add an existing key to an existing account using the **Import SSH Keys** option. Follow the below steps:

1. Navigate to the **Resources** tab and click the resource name. In the **Account Details** pop-up window, select the required account.
2. Go to **Key Actions >> Import SSH Keys**. You will be prompted to browse and add the key,

along with the Key name and passphrase details.



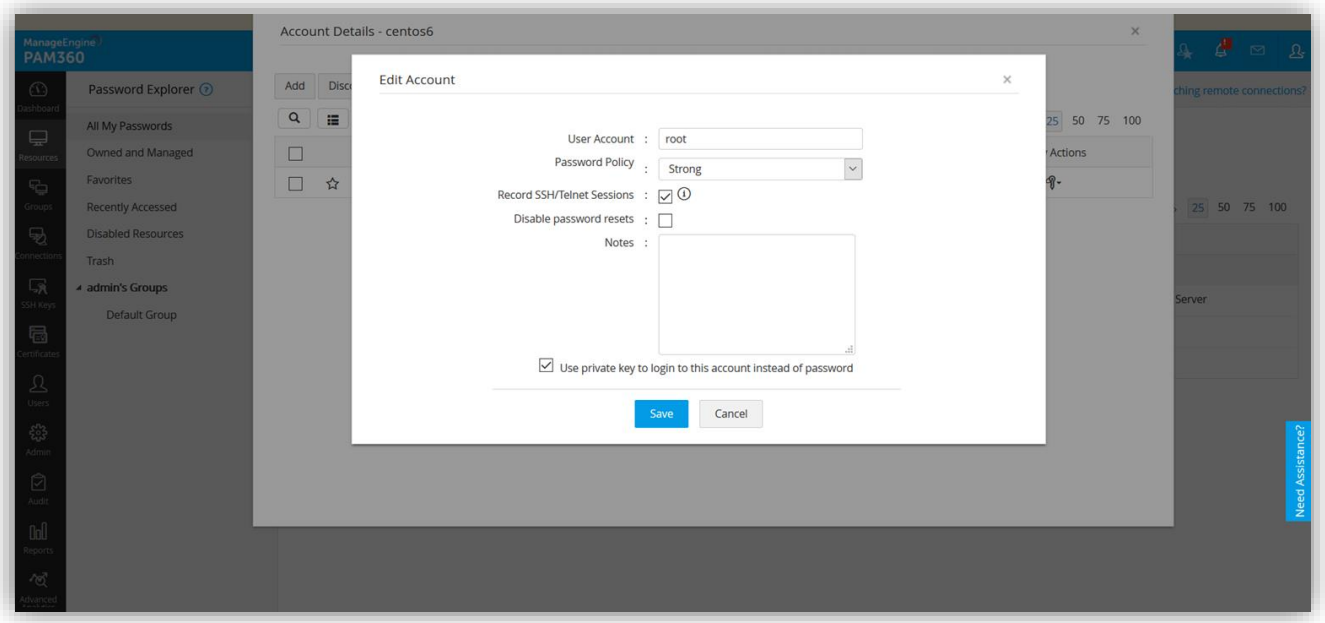
3. Select the checkbox **Map private key locally, if remote key association fails** to force map SSH keys to user accounts, even if the target systems are not reachable.
4. Click **Save** to import the SSH key into PAM360.



1.4 Enabling Private Key Login Option For an Existing Account

If the remote login using private key option is not enabled during the account creation or key association, you can enable the same by editing the account details.

Refer to the section Adding an Account to a Resource to edit the existing account. In the process, select the checkbox **Use private key to login to this account instead of password** (shown in the below screenshot) to authorize remote connections using SSH keys instead of account credentials.

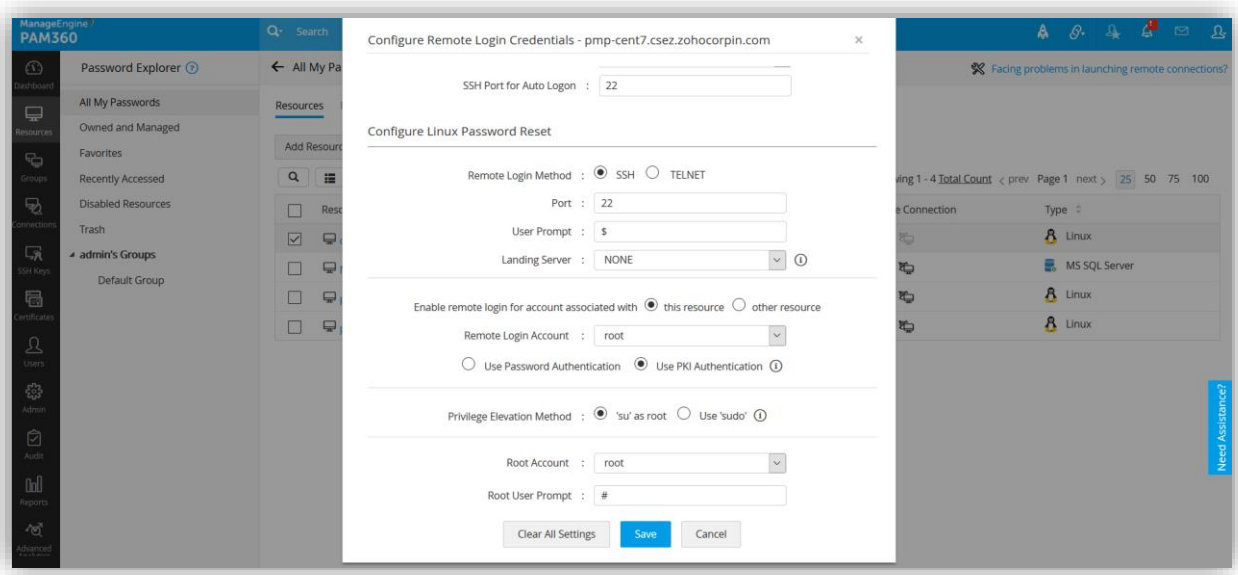


2. Enabling PKI Authentication Option for Remote Password Reset

> **Note:** This step is necessary only if you want to use a particular account to carry out remote password reset. To simply launch SSH connections using SSH Keys, PKI authentication need not be enabled.

Use the PKI authentication option to carry out remote password reset through the account which launches remote connection using SSH keys. To enable this option:

1. Navigate to the **Resource** tab and click **Resource Actions >> Configure Remote Password Reset** beside the required resource.
2. Under **Configure Linux Password Reset**, choose the account which has the private key option enabled as the **Remote Login Account.**
3. Now choose **Use PKI Authentication** and click **Save**.


Configure Remote Login Credentials - pmp-cent7.csez.zohocorpin.com
SSH Port for Auto Logon : 22
Configure Linux Password Reset
Remote Login Method : SSH TELNET
Port : 22
User Prompt : $
Landing Server : NONE
Enable remote login for account associated with this resource other resource
Remote Login Account : root
Use Password Authentication Use PKI Authentication
Privilege Elevation Method : 'su' as root Use 'sudo'
Root Account : root
Root User Prompt : #
Clear All Settings
Save
Cancel
Password Explorer
All My Passwords
Owned and Managed
Favorites
Recently Accessed
Disabled Resources
Trash
admin's Groups
Default Group
Facing problems in launching remote connections?
Need Assistance?

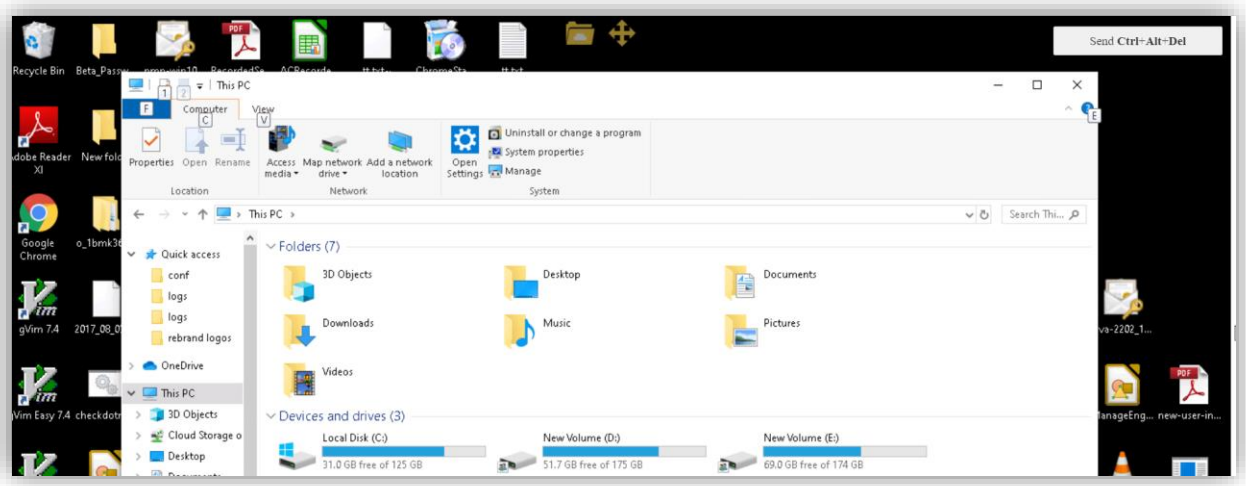
Remote File Transfer During Windows RDP Sessions

PAM360 lets you establish a secure remote connection to Windows resources using the Remote Desktop Protocol (RDP). PAM360 authenticates the remote connections automatically by using the passwords stored in its repository, thereby eliminating the need for you to enter passwords manually. Once the secure connection is established via PAM360's session gateway, transfer files to and from the remote target machine during the RDP sessions.

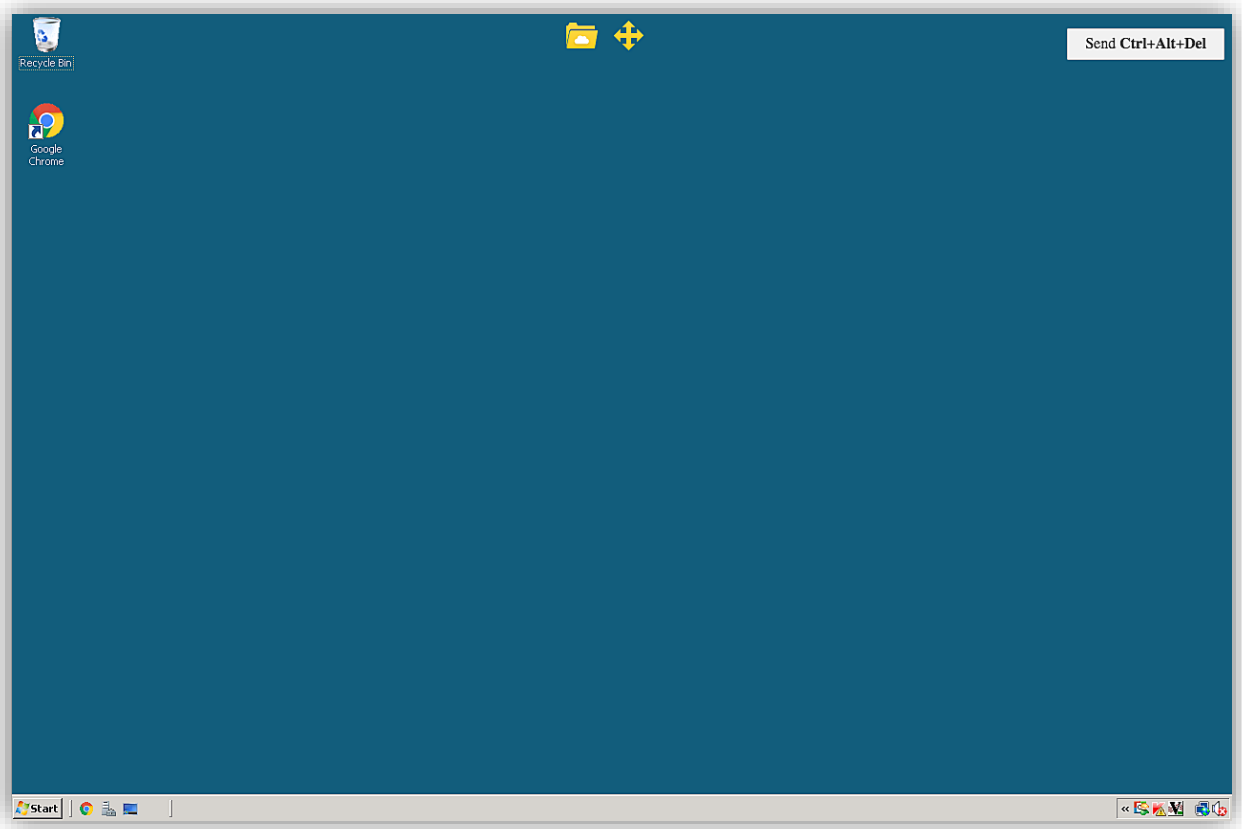
1. Transferring Files to a Remote Windows Resource

Follow the steps below to transfer files from your local machine to a remote Windows resource:

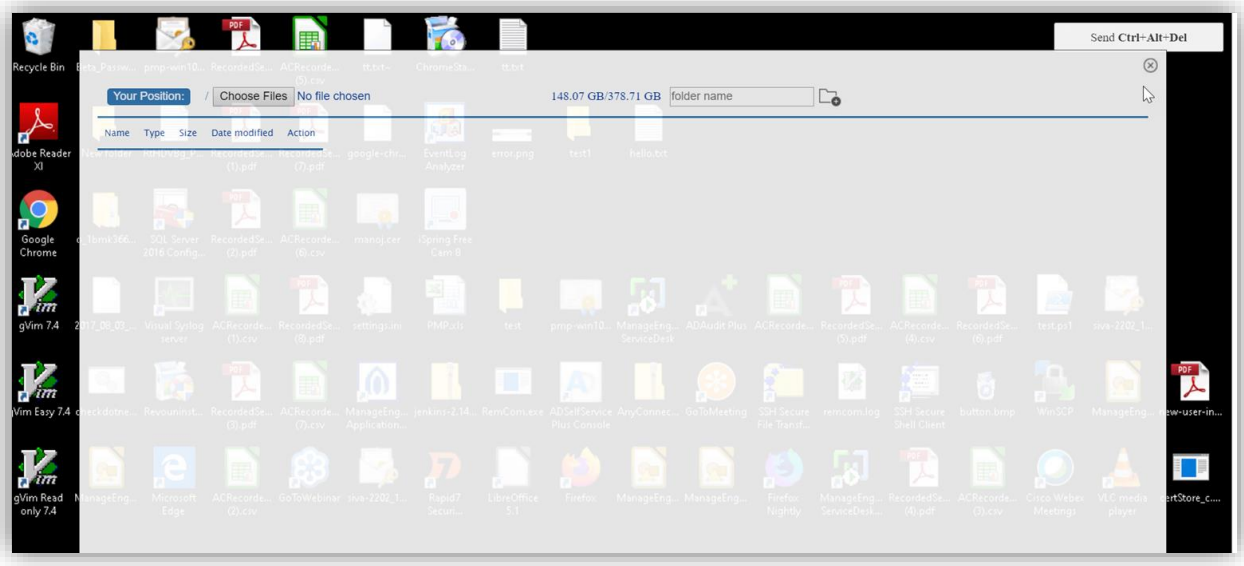
1. Launch a remote session to the Windows resource from PAM360's web interface. You can launch the remote session either from the **Connections** tab or from the **Resources** tab, by clicking the **Open Connection** icon shown beside the respective Windows resource.
2. PAM360 will authenticate the connection using the password stored in its repository and open a secure RDP console. In the RDP console, navigate to the remote machine's My Computer folder. A new drive named Cloud Storage on <IP address> will be available. This is the temporary folder using which you can transfer files to and from the remote machine.



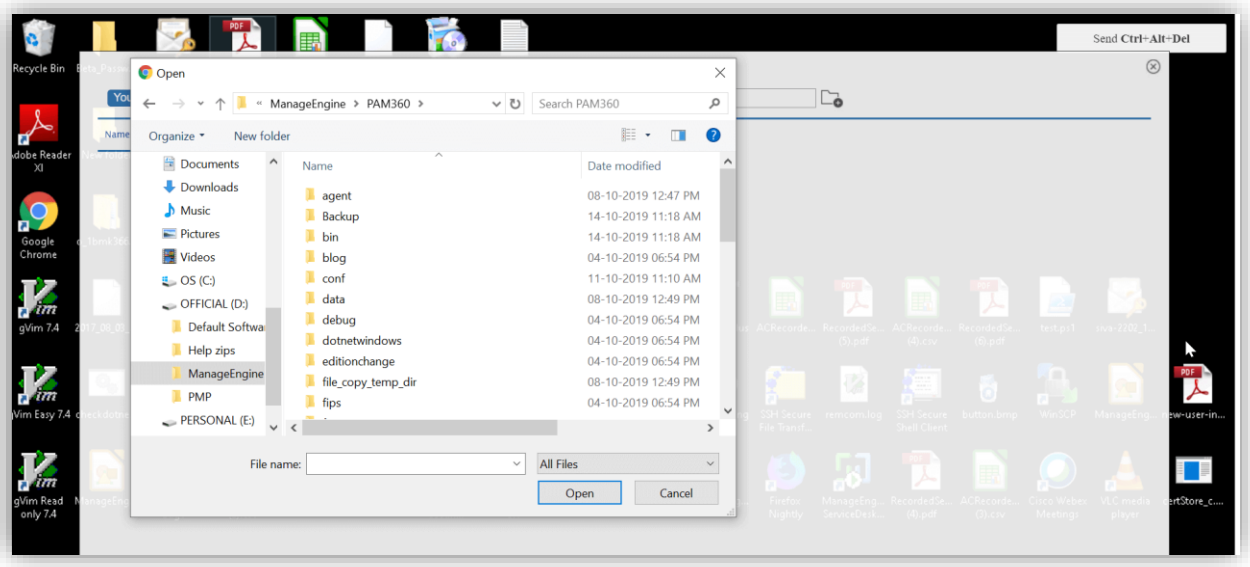
3. Now, go back to the remote machine's desktop screen and click the folder icon that appears at the top of the screen as shown in the image below.



4. A new window will open within the console. To transfer files from your local machine, click the **Choose Files** option and select your required files.



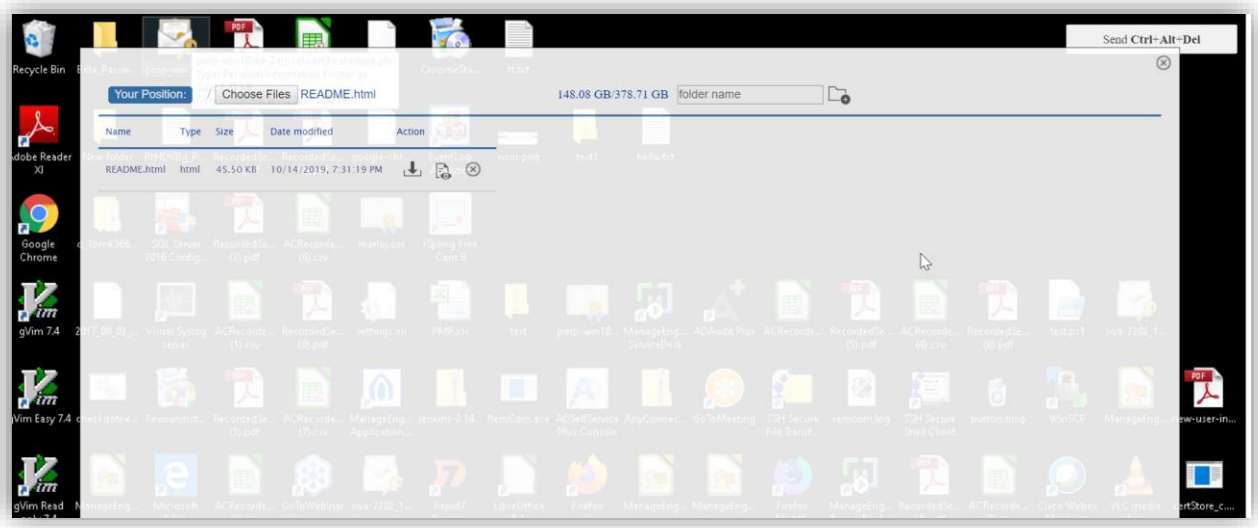
5. Once you have selected the files, they will be automatically uploaded to the cloud storage drive. Now, you can simply copy the uploaded files from the cloud storage drive to your remote machine.



2. Transferring Files from a Remote Windows Resource to the Local Machine

Follow the steps below to transfer files from a remote Windows resource to your local machine:

1. Launch a remote session to the Windows resource from PAM360's web interface. In the RDP console that opens, navigate to the remote machine's My Computer folder. A new drive named Cloud Storage on <IP address> will be available. This is the temporary folder using which you can transfer files to and from the remote machine. Open the cloud storage drive and drop the files that you need to transfer into it. Immediately, the files will appear in the file transfer window as shown below.
2. Here, click on the **Download** icon beside the file to download it to your local machine.



See Also:

- SFTP-based bi-directional file transfer for different types of resources

Configuring Landing Servers for Data Center Remote Access

Typically, data centers limit direct access to remote devices via SSH, Telnet, and RDP connections. Hence, data center admins working remotely first connect to a landing server and then hop to the target system. Admins can decide on whether to take a single hop (for RDP) or multiple hops before connecting to the target devices. At each step of the remote access process - from the initial landing server to each subsequent hop and the target device, the Admin must provide the username and password, as well as know the IP address of the landing server.

PAM360 has simplified this entire data center remote access management. Use PAM360 to effectively launch direct connections (TELNET, SSH, RDP, SFTP) to access IT equipment in the data center, overcoming access barriers created by network segmentation, while adhering to data center access protocols. PAM360 also supports full password management for those remote devices.

First, configure any number of landing servers, to remotely access the IT equipment in your data centers. Next, associate the landing servers with the resources managed by PAM360. Once the configuration is complete, you will be able to launch direct connections with the remote resources through a single click, without worrying about the intermediate hop(s). PAM360 takes care of automatically establishing the connection with the landing server(s) and finally with the remote resources.

Supported Connection Types

PAM360 supports configuring landing servers for the following types of connections:

1. SSH
2. Telnet
3. RDP
4. SFTP

Note: RDP is applicable from PAM360 build 5000 only. Similarly, SFTP is applicable from PAM360 build 6530 only.

At the end of this section, you will have learned the following topics:

1. **Adding the Landing Servers as Resources**
2. **Creating Identities for Landing Servers**
3. **Associating Resources with Landing Servers**

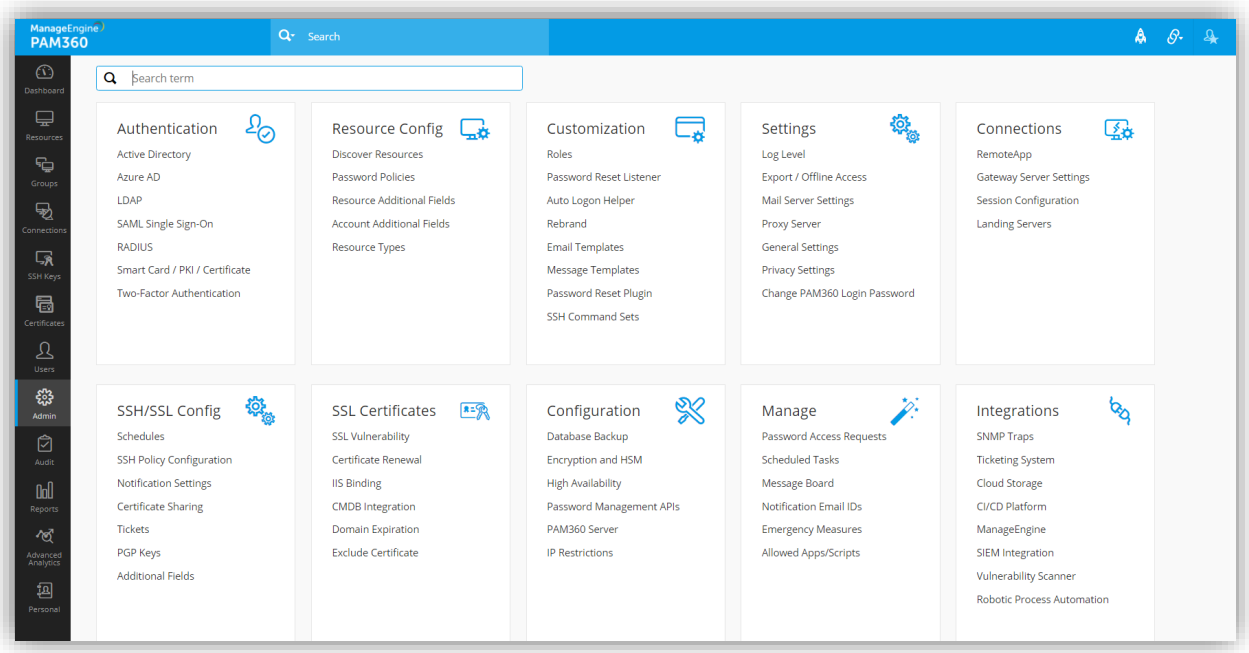
1. Adding the Landing Servers as Resources

Basically, Landing servers are also resources in PAM360. Remote access to data centers starts with establishing a connection with the landing servers. So, the first step is to add the required landing servers as resources in PAM360 through the usual resource addition process. Landing servers typically have primary and secondary setups. All you need to do is to add both primary and secondary servers as resources in PAM360.

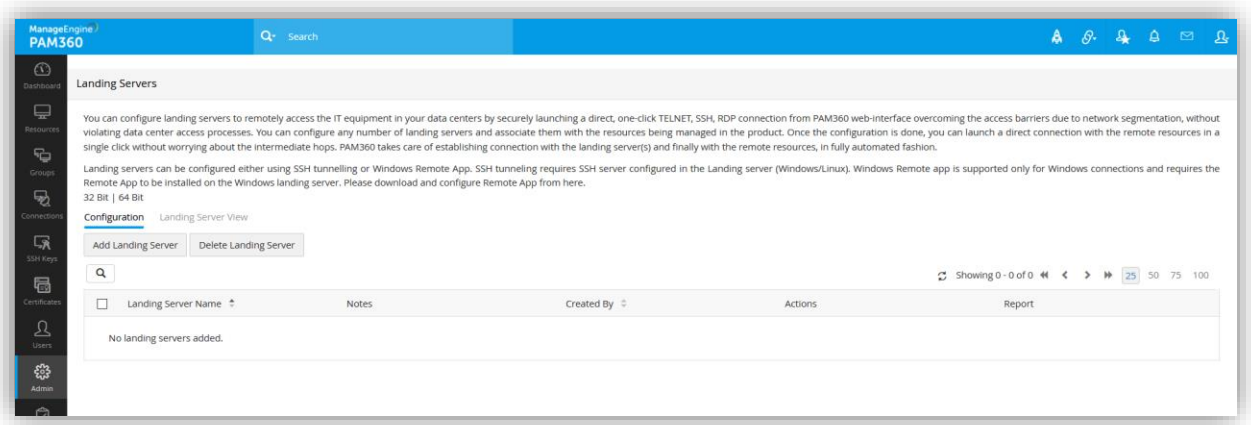
2. Creating Identities for Landing Servers

After adding the required landing servers as resources in PAM360, you need to establish an identity for each landing server. Do this by providing a name for each landing server.

1. Navigate to **Admin >> Configuration >> Landing Servers.**

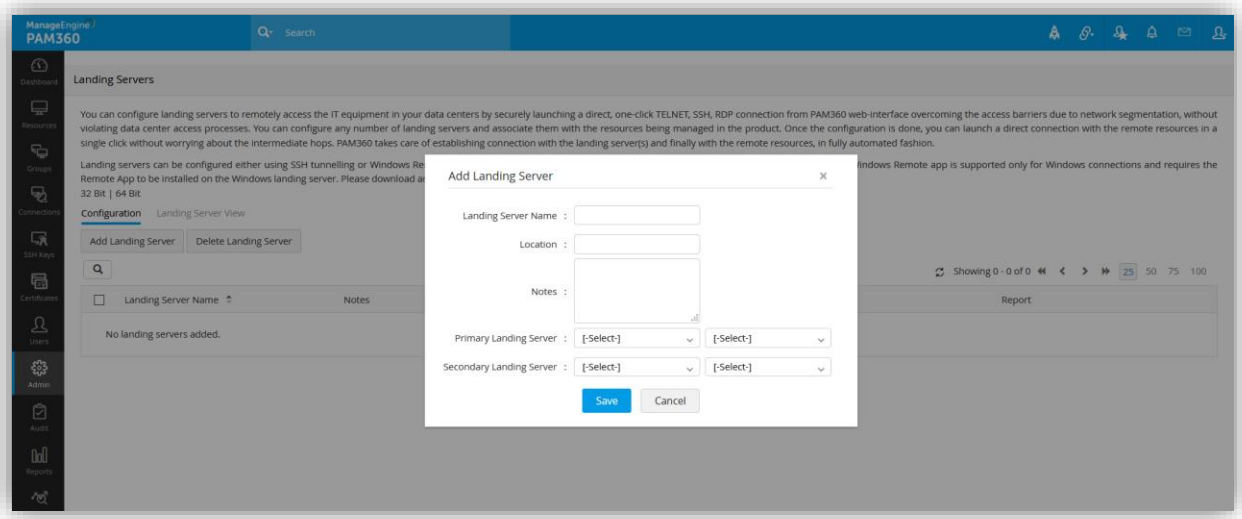


2. Click **Add Landing Server** available on the top left corner.



3. In the pop-up form that opens,
    i. Enter a name for the **landing server**. This will help you uniquely identify it.
    ii. Enter other details like **Location,** descriptive **Notes.**
    iii. If you have primary and secondary instances for your landing server, select the respective resources from the drop-down(the resources that were added by you in step 1 above).
    iv. Also, select the account that is used to login to the landing server.
4. Click **Save.**

Repeat the above steps and create identities for as many landing server as needed.



3. Associating Resources with Landing Servers

After adding the landing servers, you need to associate resources with the respective landing servers. This is a crucial step as this is where you are connecting the resources with the landing servers. You will also be defining the direct connection launching path.

For example, assume that you want to connect to your corporate mail server, which runs on a Linux host in the database and you need to hop to 'Landing Server A' first. Now, you will have to associate the mail server with Landing Server A.

Associate as many resources with a landing server as needed - different resources have different landing servers and different connecting paths. Quite often, there could be multiple landing servers (or multiple hops) to connect to a resource. In that case, you should be associating resources as explained below:

3.1 Example Use Case Scenario

Assume the following landing server configuration setup:

PAM360 Server -> Landing Server 1 -> Landing Server 2 -> Proxy Server in Data Center

1. To connect to your proxy server in data center from PAM360, first you need to connect to Landing Server 1, then to Landing Server 2, and finally to the actual resource, i.e., the Proxy Server in Data Center.
2. Associate the landing servers and the Proxy Server with the resources in PAM360 using the steps below:
    i. Navigate to **Admin >> Configuration >> Landing Servers.**
    ii. Click the **'Configure Resources to use this Landing Server'** icon under the **'Actions'** drop down against the respective landing server.
    iii. In the window that opens, select the required resources/connections.
    iv. Click '**Associate Connections**'.

    Now, all the three entities - landing server 1, landing server 2 and the proxy server are resources in PAM360.
3. First, associate the Landing Server 1 with the Landing Server 2, and then Landing Server 2 with the Proxy Server.

Once you establish the association this way, PAM360 will take care of finding the connection path automatically and establish a direct connection with the resource.

3.2 Providing landing server details during resource addition:

If you have added the landing servers and created identities for them using step 2 and 3 above, the association (step 3) can be done during the resource addition process, where you need to select the Resource Type as the landing server. Alternatively, you can associate the landing servers with the resources by editing them.

Managing SSH Keys and Key Groups

SSH keys serve as a secure means of authentication and establishing encrypted connections between a client and server. They offer a highly secure alternative to password-based authentication for remote logins and file transfers. Widely employed in system administration and secure network communication, SSH keys deliver enhanced security, convenience, and automation features while decreasing reliance on passwords. By adhering to best practices in key generation, management, and usage, one can maximize the advantages and overall security provided by SSH keys. PAM360 allows you to manage the entire life-cycle of SSH keys of your SSH resources.

The sequence indicated below just illustrates the flow of SSH key events in PAM360. It is not necessary that you should follow them in the same order as explained below.

1. SSH Resource Discovery
2. Elevating Privilege for SSH Keys Management
3. Discover SSH Keys from the SSH Resources
4. Import the Discovered Keys to PAM360
5. Create New Keys and Deploy
6. Associating the SSH Keys with the User Accounts
7. SSH Key Management Operations (Rotate, Edit, Push, Dissociate, Delete)
8. Organize SSH Key Groups for Bulk Management
9. Miscellaneous Operations

1. SSH Resource Discovery

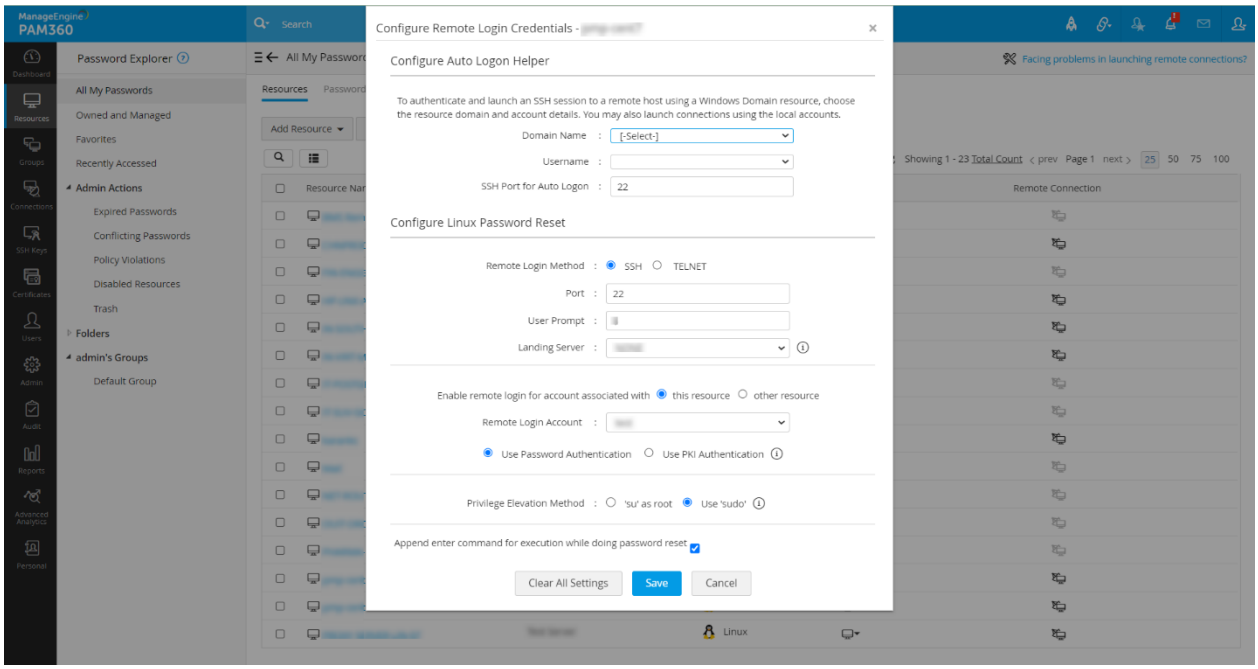
The SSH keys management starts with the SSH resource discovery process. To discover the SSH keys from the organization resources via PAM360, it is required to add the respective SSH resources in the PAM360 repository. You can add the SSH resources manually or via the Linux resource discovery process.

Note: The term SSH keys mentioned here only represent the private keys of the SSH resources.

2. Elevating Privilege for SSH Keys Management

To discover, associate, deploy, and rotate SSH keys, PAM360 requires a remote login method, a login account for authentication, and privilege elevation configured with root privileges. To configure those above requirements,

1. Navigate to **'Resources >> All My Passwords >> Resources'**.
2. Click the **Resource Actions** icon beside the respective SSH resource and click '**Configure Remote Password Reset**'.
3. Select the desired **Remote Login Method**, **Landing Server** (if configured), and enter the **Port** details (if modified).
4. Select the remote login account that has to be used for authentication with the respective authentication method.
5. Provide the privilege elevation method as **'su' as root** or **Use 'sudo'**. If you choose the option '**su**' **as root**, select the root account with the sudo privilege. If you choose the option **Use 'sudo'**, the account used for remote login will get the root privileges for further operations.
6. Now, click **Save**.

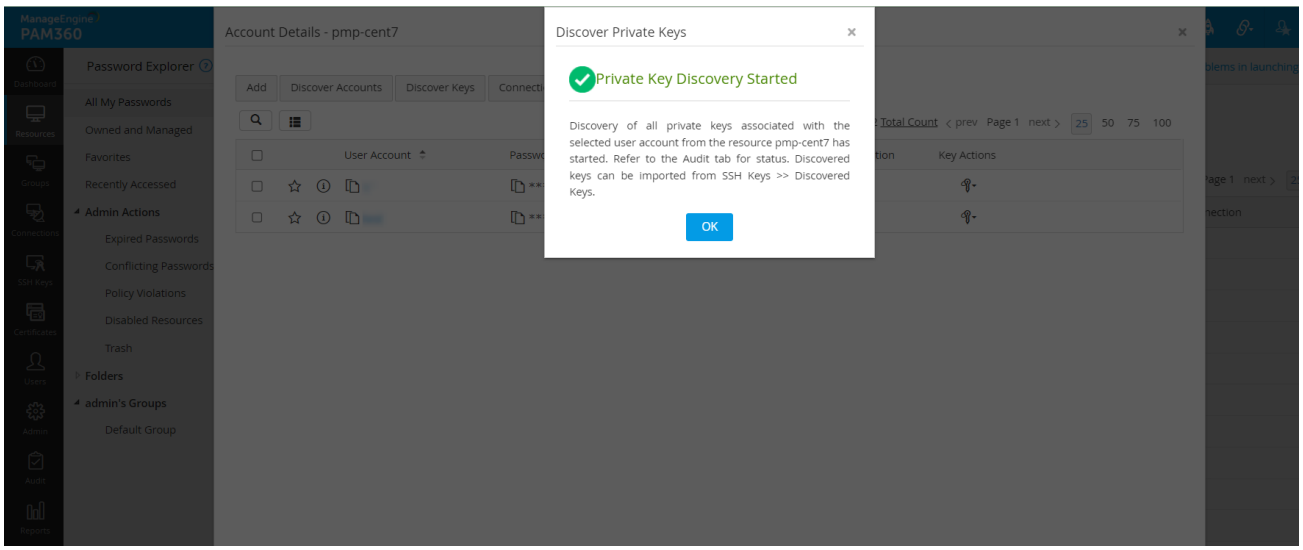


3. Discover SSH Keys from the SSH Resources

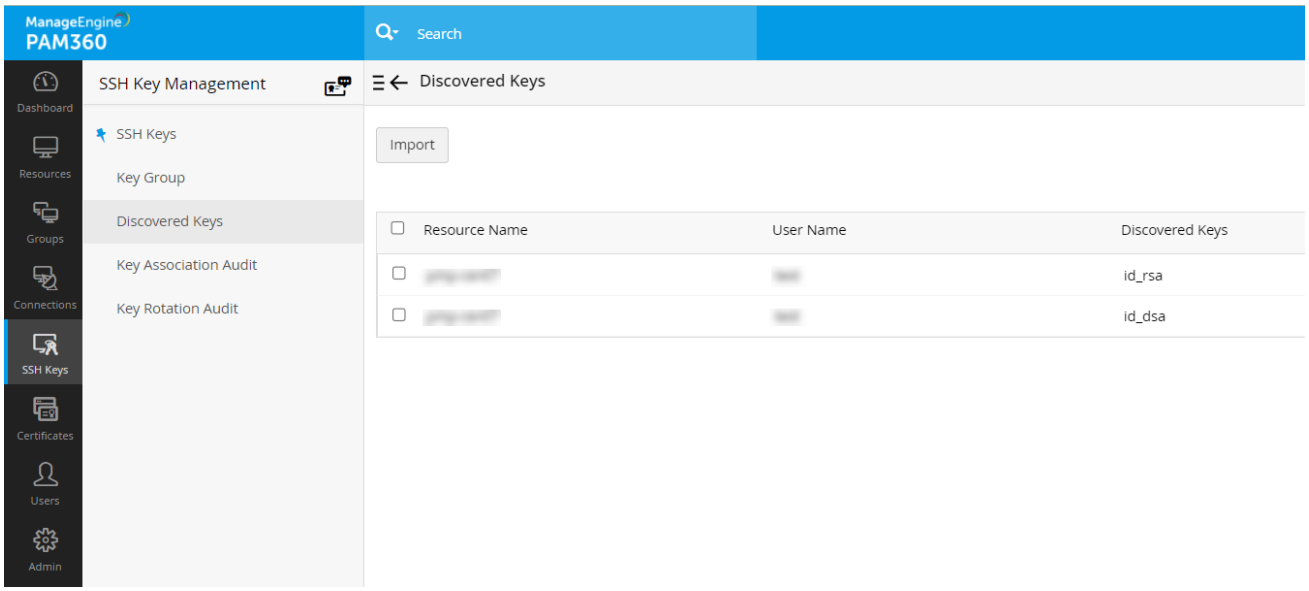
To discover the private keys associated with the accounts of the added/discovered SSH resources,

1. Navigate to **Resources >> All My Passwords >> Resources** and click on the respective Linux resource.

2. Select the user accounts from which the SSH keys are to be discovered, or select the accounts in bulk.
3. Now, click **Discover Keys** from the top pane.



4. The SSH keys present in the selected user accounts will be discovered in PAM360 with the relevant audit detail.
5. You can see the discovered SSH keys from the **SSH Keys >> Discovered Keys** tab.



4. Import the Discovered Keys to PAM360

PAM360 requires SSH user credentials for SSH key management. If the credentials are in place, you can import the SSH keys already discovered. To import the key files from the discovered SSH resource:

1. Navigate to the **SSH keys >> SSH keys tab** in the GUI.

2. The SSH keys are listed with their details. Select the keys you want to import.
3. Click the **Import** button.

The imported keys can be viewed from the **SSH keys >> SSH keys** tab.

> **Note:** If the keys are protected with a passphrase, even though the import operation will execute successfully, while associating with user accounts, you need to enter the passphrase to use the key.

4.1 Import Keys from Systems

In addition to the discovery of key files from the SSH resources, you can also specify the location, and import the keys present in any system. To import the key files from the system:

1. Navigate to the **SSH Keys >> SSH Keys >> More** and click **Import Key**.
2. Click the **Browse** button and select the key file within the system.
3. Enter the name and passphrase of the key.

> **Note:** If the key is protected with a passphrase, then the same has to be entered to import the key successfully.

4. Enter a **Key Comment** for your reference.
5. Click the **Add** button to include the key in the SSH keys repository.

To edit a **Key Comment** in the already imported keys, follow the below steps:

1. Navigate to the **SSH Keys >> SSH Keys** tab.
2. Select the required key from the repository.
3. Click the **More** dropdown from the top menu, choose **Edit**, and enter the required comment.
4. Select the checkbox **'Update the comment in the authorized keys file of the associated user(s) account'** to apply the updated key comment in the associated end servers as well. This option eliminates the need to update the key comments manually in the authorized_keys file in the end servers.

Note: Key Comment can be edited for only one key at a time.

5. Create New Keys and Deploy

PAM360 also allows you to create new key pairs and deploy them on target systems. The create and deploy feature of PAM360 can be used for one-click generation and deployment of keys. Unique key pairs are generated for each user account, and the corresponding keys are deployed automatically in the user accounts of the target servers.

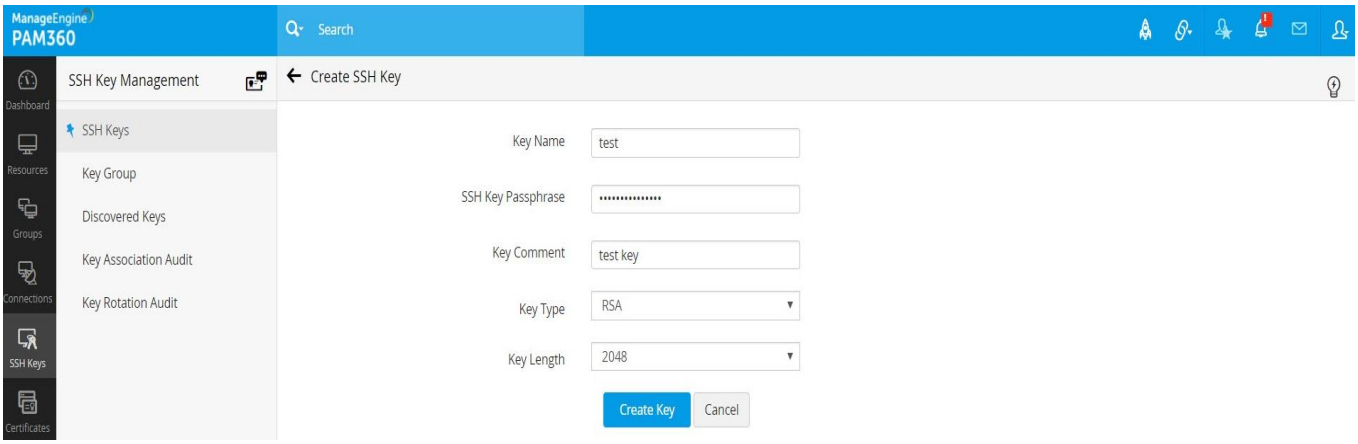
The SSH key pair can be generated using RSA / DSA algorithms as per the details below:

- RSA – 1024, 2048, or 4096-bit keys
- DSA – 1024-bit keys.
- ECDSA – 256, 384, or 521-bit keys
- ED25519

5.1 To Create SSH Keys

1. Navigate to **SSH Keys >> SSH Keys** tab in the GUI.
2. Click the **Create** option.
3. In the **Create SSH Key** window, enter the details of the key, and select the key type and length.
4. Click the **Create Key** button to generate the key pair.

You will get confirmation that the new key has been created. All the keys that are created are automatically added to the centralized repository of PAM360. You can view these keys from the **SSH Keys >> SSH Keys** tab in the user interface. PAM360 allows you to search SSH Keys using **Key Name, Key Type, Key Length, Finger Print, Created By, Age**, and **additional fields** (if available).



Administrators can view the passphrases of keys by clicking on the show passphrase icon provided at the right end of the keys.

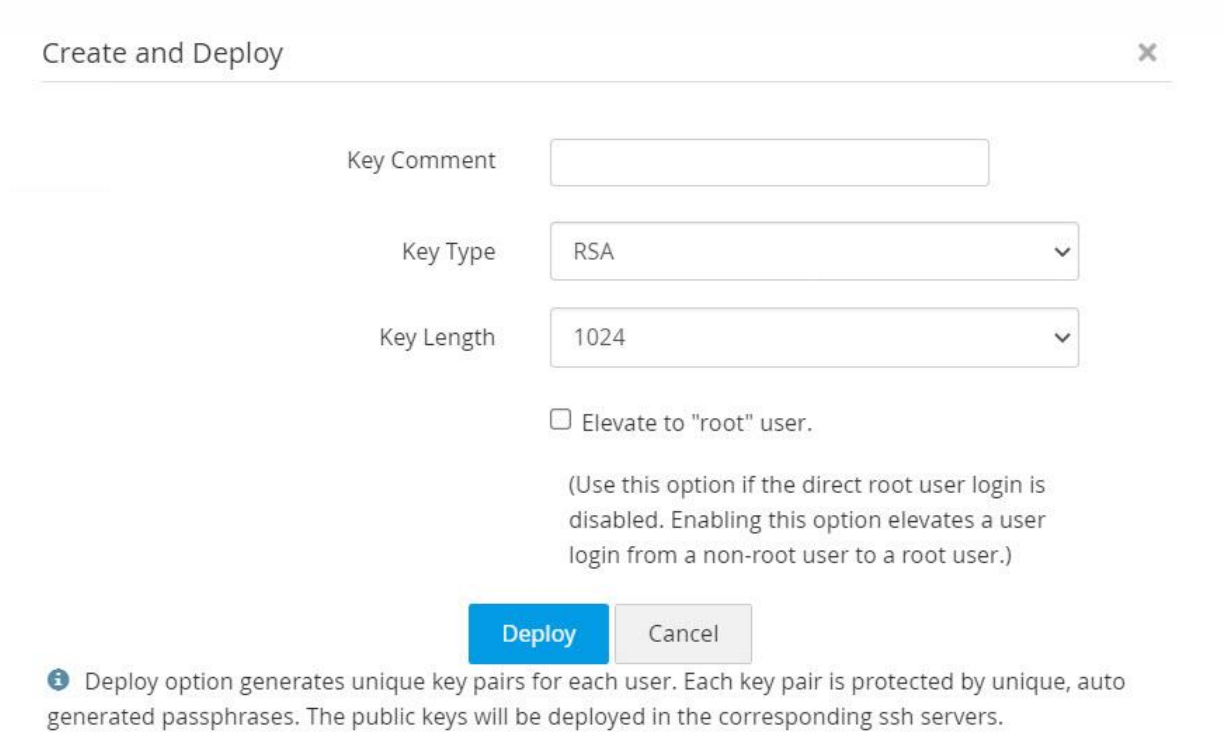
5.2 Create SSH Keys and Deploy

To create and associate keys with all the user accounts in a discovered resource:

1. Navigate to **Resources >> All My Passwords >> Passwords**.
2. Select the required account and select **Create and Deploy** under the **Key Actions** in the top pane to deploy the keys in all its enumerated user accounts.
3. Select the **Key Comment, Key Type,** and **Key Length**.
4. Select the checkbox to **Elevate to "root" user**.

> **Note:** For security reasons, root user login might be disabled for servers/machines. Enabling this option elevates a user login from a non-root user to a root user and allows you to associate keys with all other users on the server. Users have to provide root user and any non-root user credentials to PAM360 to elevate to a root user.

5. Click the **Deploy** button to create key pairs and deploy them simultaneously in all the user accounts of the resource for which the credential is available.



6. Associating the SSH Keys with the User Accounts

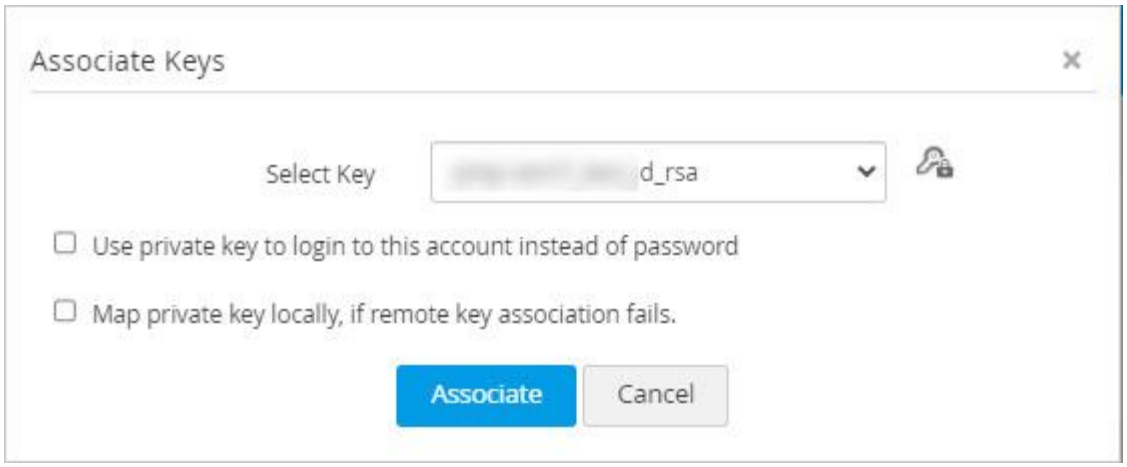
After importing/creating keys, you can associate the keys with SSH users.

Note: If a root user or administrator credential has been provided for a resource, keys can be associated with all enumerated user accounts of the resource. If there are no keys available in the PAM360 database, then you will be prompted to create a key during association. Create a key pair and return to these steps.

6.1 Associating the SSH Keys with the User Accounts

1. Navigate to **Resources >> All My Passwords >> Passwords**.
2. Select the user accounts for association.
3. Click the **Associate** button under **Key Actions** from the top pane.
4. Enable the following permission as required with respect to the SSH key:
    i. **Use private key to login to this account instead of password**
    ii. **Map private key locally, if remote key association fails**

5. Select a key and click the **Associate** button.

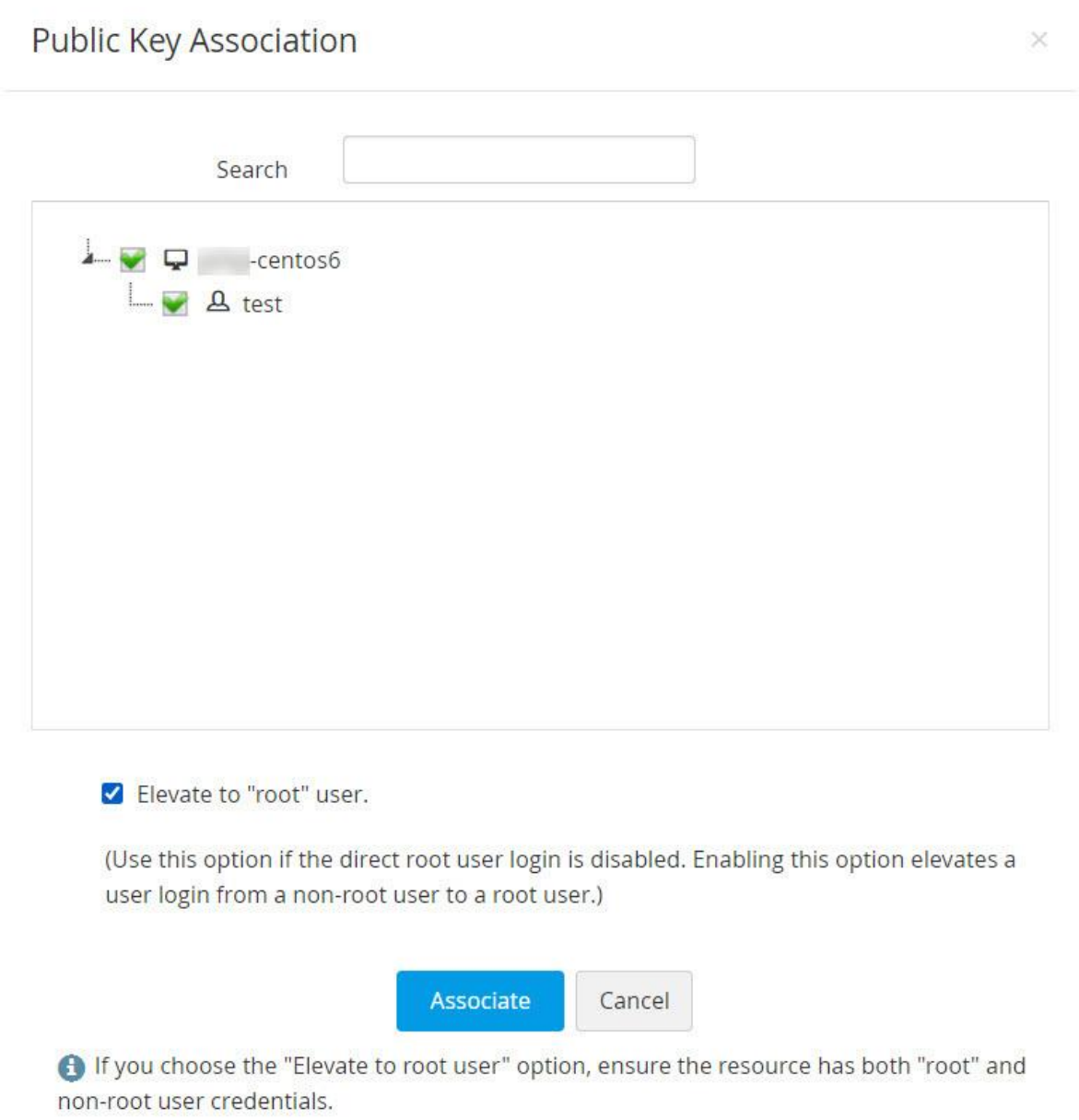


6.2 Associating the SSH Key with the Resources

1. Navigate to **SSH keys >> SSH Keys**.
2. Select an SSH key from the list displayed and click the **Associate** button.
3. In the **Public Key Association** window, select the user accounts.
4. Select the checkbox to **Elevate to "root" user.**

> **Note:** For security reasons root user login might be disabled for servers/machines. Enabling this option elevates a user login from a non-root user to a root user and allows you to associate keys to all other users on the server. Users have to provide root user and any non-root user credentials to PAM360 to elevate to a root user.

5. Click the **Associate** button.



Now you have successfully associated a particular SSH key to the resources/user accounts.

7. SSH Key Management Operations (Rotate, Dissociate, Delete) and Launch Direct Terminal Connections.

7.1 Rotate SSH Keys

You can configure PAM360 to automatically rotate the SSH keys at periodic intervals. With a single click, all the deployed keys can be replaced. The keys can be rotated based on a schedule, or anytime based on your need.

i. Manual Key Rotation

To rotate the keys manually:

1. Navigate to **SSH keys >> SSH Keys tab.**
2. Select the keys to be rotated.
3. Click the **Rotate** option.
4. In the pop-up that opens, enable the requirements that follow and click **Rotate**:
   i. Push private key file to remote user account
   ii. Push public key file to remote user account
   iii. Use keyname as filename

A confirmation message will be displayed and you will be redirected to the **Key Rotation Audit** page where the status of rotation is updated.

> **Note:** Only the keys which have already been associated with user accounts of resources can be rotated.

ii. Scheduled Key Rotation

To schedule the rotation of keys:

1. Navigate to **Admin >> SSH/SSL >> Schedules.**
2. Click the **Add Schedule** button.
3. In the **Add Schedule** window, enter a **name** for the schedule and select the **type** of schedule as **Key rotation** from the drop-down list.
4. Select the keys to be rotated.
5. Enable the requirements that follow:
   i. Push private key file to remote user account
   ii. Push public key file to remote user account
6. Select the **Resource Type**, **Start Time,** and **Start Date** for rotation. Enter the email addresses of the users with the **Subject, Content, Signature** to be notified.
7. Click **Save.**

The result of the schedule execution will get updated in the **Key Audit**, and the result of the rotation of the keys will get updated in the **Key Rotation Audit**.

7.2 Dissociate Keys from SSH Users

When a SSH user leaves the organization or is provided temporary privileged access, you can dissociate the keys associated with the user to and discontinue access. Until you dissociate all the SSH keys, you cannot delete the user account nor the resource.

i. Disassociating Key from User Accounts

1. Navigate to **SSH keys >> SSH Keys**.
2. Select a single key which has to be dissociated.
3. Click **Dissociate** from the **More** drop-down list.
4. If the key is associated with a single user account, select this checkbox to **Dissociate key locally if remote dissociation fails** and click **OK** in the confirmation dialog box to dissociate the key.
5. If the key is associated with multiple user accounts, select the user accounts from which the key has to be dissociated, select this checkbox to **Dissociate key locally if remote dissociation fails** and and click **Dissociate** in the **Dissociate Users** window.

ii. Dissociating Keys from Selected User Account

1. Navigate to **Resources >> All My Password >> Passwords.**
2. Select a user account for which you wish to dissociate keys and click **Dissociate** from the **Key Actions** column**.**
3. If the user account is associated with a single key, select **Ok** in the pop-up window.
4. If more than one key is associated with the selected user, select the keys which have to be dissociated and click the **Dissociate** button in the **Dissociate Keys** window.

> **Note:** When you select and delete the user accounts enumerated in PAM360, the SSH keys associated with them are automatically dissociated.

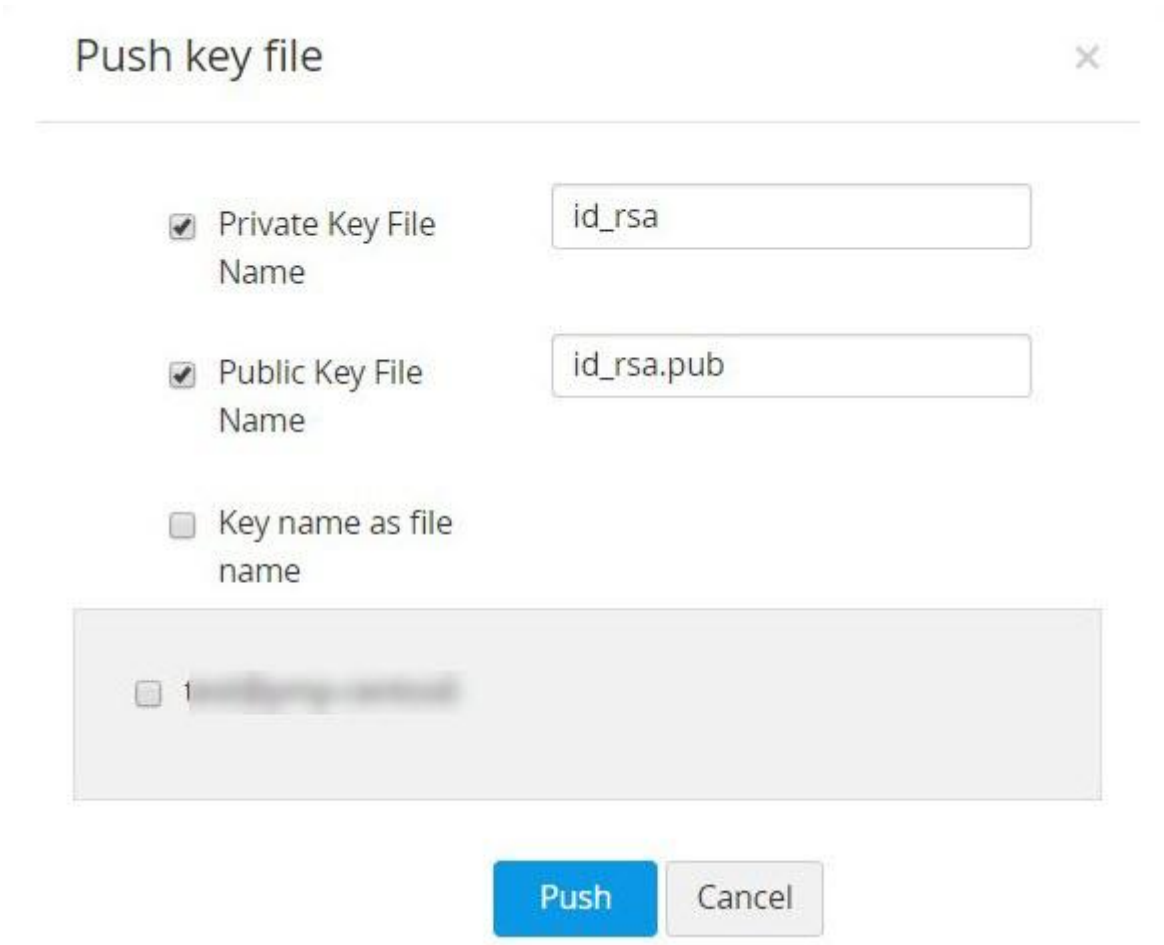
7.3 Push Keys to Remote User Accounts

In addition to deployment, PAM360 allows you to push a private key or a public key, or both onto its associated users.

i. **To push a key file to remote user accounts:**

1. Navigate to **SSH Keys >> SSH Keys**.
2. Click on the **Push Key to User** icon ( ) beside the selected key.
3. Select the key(s) that needs to be pushed (private, public, or both), provide the appropriate key names, select the required associated users and click **Push**.
4. The key file(s) is/are pushed to the selected users.

This feature is also available as a part of **Key Rotation** schedule. After the scheduled key rotation is performed and fresh key pairs are created and deployed, you can automatically push either the private key or both the private and public keys onto its selected associated users by enabling the 'push key to user' option instead of pushing the key files manually after every scheduled rotation.



ii. Add commands and restrict host per key:

You can add commands to specific user accounts, thereby providing an additional layer of restriction enabling them to only execute the commands on establishing connection with the host. Also, you can predefine appropriate key to user relationship by specifying the IP address of the user in the appropriate format (as specified below).

To add command to a public key,

1. Navigate to **Resources >> All My Passwords >> Passwords.**
2. Select the user account for which you want to add a command and click on **Add Command** from the **Key Actions** column.
3. An **Add Command** dialog box opens up, where you can add commands to be executed in the following format. **i.e., (command="usr/local/bin/script.sh").**

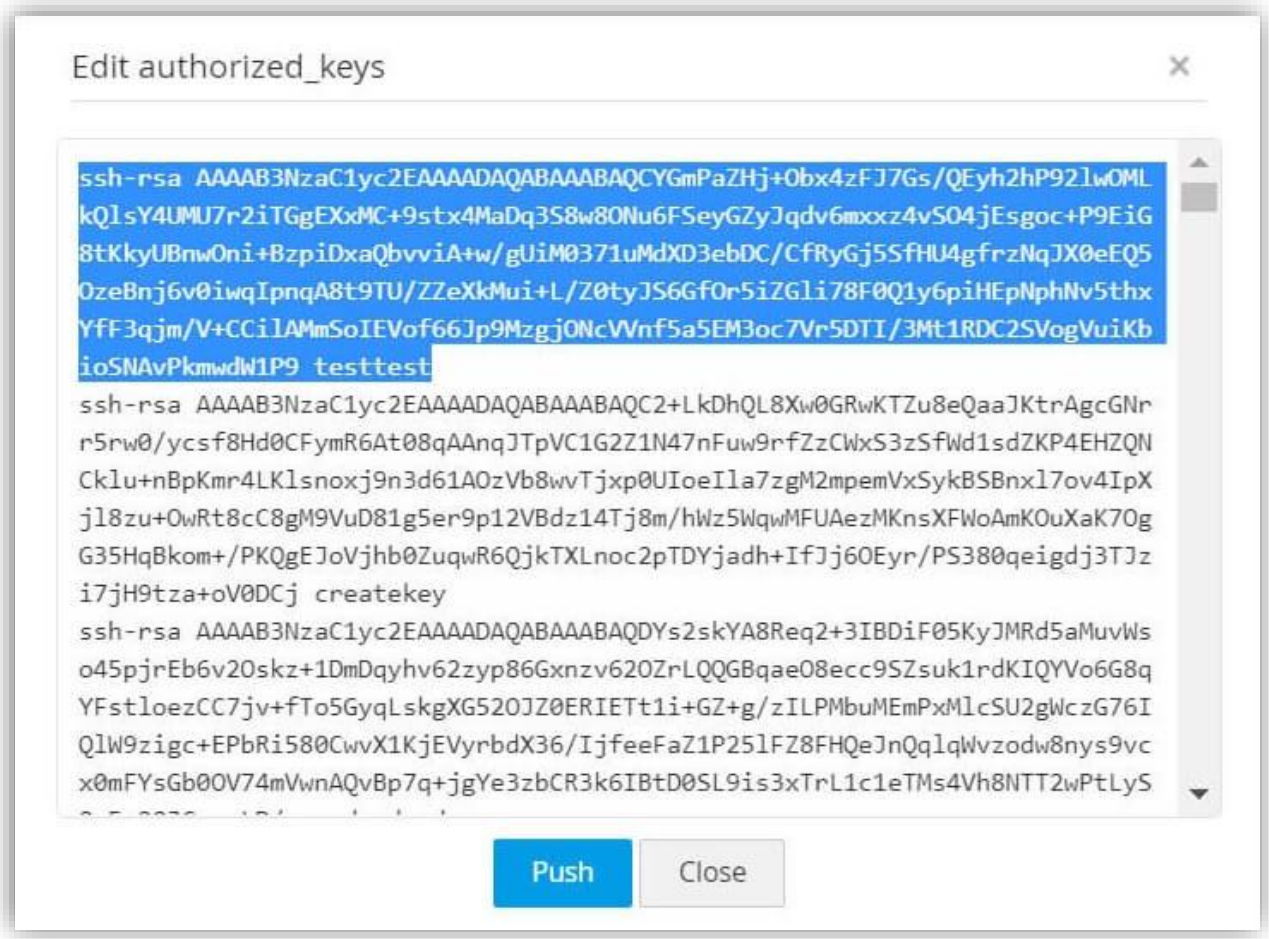
To restrict hosts for a key, click on **Add Command** and provide the name or IP address of the hosts in the following format. **i.e., (from="host1/ip1,host2/ip2")**

7.4 Edit Authorized Keys File

You can fetch authorized_keys files from various user accounts, edit the key content and push them to respective user accounts from PAM360.

To do this,

1. Navigate to **Resources >> All My Passwords >> Passwords.**
2. Select the required user account and click on **Edit Authorized Keys** from the **Key Actions** column.
3. A window opens displaying the list of public keys in the authorized keys file of the respective user. The keys that are managed using PAM360 are highlighted.
4. You can now edit the contents of the keys displayed, and deploy them back to the respective user accounts by clicking the **Push** button.



7.5 Delete Keys

When you try to delete the SSH keys from PAM360 repository, they are first dissociated automatically from their user accounts. Key deletion fails for the SSH keys that are not dissociated from all their user accounts.

To delete the SSH Keys:

1. Navigate to the **SSH keys >> SSH Keys** tab.
2. Select the keys to be deleted.
3. Click the **Delete** button from the **More** drop-down list.
4. Click **OK** in the confirmation window.

8. Organize SSH Key Groups for Bulk Management

PAM360 gives the provision to create key groups for easy organization and to carry out operations in bulk. You can assign, delete, or modify the group similar to working with a SSH key.

The list of items available in a group is enumerated in their respective tabs. You can drill down to the individual items by clicking the name of a group.

8.1 Create Key Groups

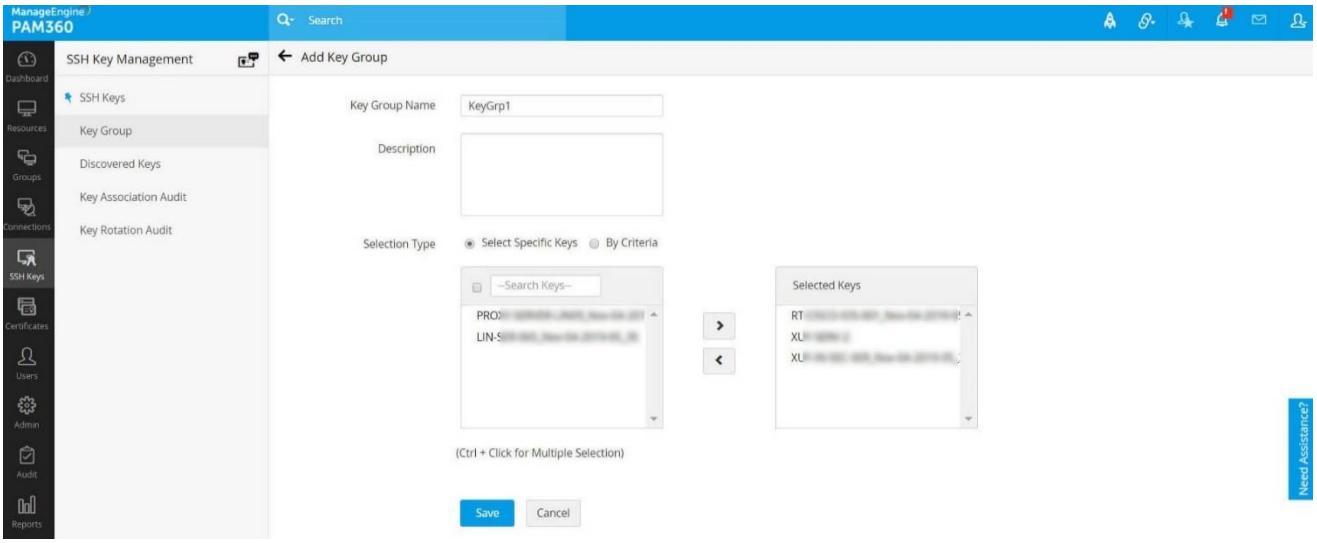
To create a group of SSH keys:

1. Navigate to **SSH keys >> Keys Group.**
2. Click the **Add Group** button. You will be redirected to the **Add Key Group** window.
3. Enter the name of the group. Take care while choosing the name since it cannot be edited later.
4. You can choose the resources to be added in a group in 2 ways:
    - **By Specific key** – Select the keys to be added to the group, individually.
    - **By Criteria** – This serves as dynamic key grouping. You will specify the exact criteria based on which you want to create the group. Here, you have many options to choose from - you can search for specific keys based on its name, type, length, or creator, and filter the search in a fine-grained manner based on the criteria such as "contains", "does not contain", "equals" "not equal", "starts with" and "ends with". Click the Matching Keys button at the bottom-right corner of the window to see the corresponding keys.

    > **Note:** If you select the **By Criteria** option, the conditions specified are applicable to keys that are discovered later too. If any of those keys match the criteria, they will be automatically included into the new group.

5. Click **Save.**

In addition, you can directly select individual keys from the **SSH keys >> SSH Keys** tab and click the **Save** button for faster group creation.



8.2 Edit Key Groups

To make changes to an existing key group:

1. Navigate to **SSH keys >> Keys Group.**
2. Click the **Edit** icon present in the right corner of the table view.
3. You can change the key selection type and edit the keys available in a group or add, modify, or delete the filters applicable to a group.

Once you make changes to the group and save, a message will be displayed confirming the update of the changes.

> **Note:** The name of the group cannot be modified. However, you can add or modify the description and the list of keys available in it.

8.3 Rotate Keys of a Key Group

To rotate all the keys of a key group:

1. Navigate to **SSH keys >> Keys Group.**
2. Select the key groups and click the **Rotate** button.

You will be redirected to the **Key Rotation Audit** window, where the status of key rotation is updated.

8.4 Delete Key Groups

To delete a key group:

1. Navigate to **SSH keys >> Keys Group.**
2. Select the key groups.
3. Click the **Delete** button.

A pop-up window will appear to make sure that the selected groups are to be deleted. Click **OK** to delete the groups.

9. Miscellaneous Operations

9.1 Customize User Home Directory

You can customize the home directories of the users, i.e, the location where the public key is to be deployed. To do this:

Navigate to **Resources >> All My Passwords >> Passwords.**

1. Click the **Edit User Path** from the **Key Actions** dropdown.
2. Enter the modified path and click **Save.**

9.2 Export SSH Keys

To export key files by selecting them from the resources with which they are associated:

1. Navigate to the **Resources >> All My Passwords >> Passwords** tab in the GUI.
2. Click the name of the resource in which the key is deployed and click the **Export** button.

To export the key files:

1. Navigate to the **SSH keys >> SSH Keys** tab.
2. Click the **Export Keys** icon available in the right corner of the table view corresponding to the required key.

Note: Even while exporting, the passphrases used to protect the keys are still in effect. That is, if the keys are to be used elsewhere, the passphrases have to be provided.

9.3 SSH Key Audits

Audits are generated when SSH keys are associated or rotated using PAM360. These reports are available in the SSH keys tab.

1. **Key Association Audit** – View the result of the spontaneous, and scheduled key association operations executed using PAM360
2. **Key Rotation Audit** – View the status of the spontaneous, and scheduled key rotation operations executed using PAM360.

9.4 View SSH Key History

Using PAM360 you can view the history of each SSH key, from the moment it was created or imported, and the subsequent rotations along with time stamps.

To view the history of any key:

1. Navigate to the **SSH keys >> SSH Keys** tab.
2. Select a single key.
3. Click the **Key History** button.

9.5 Export Discovered Keys Report

A report of the discovered keys can be exported as PDF, or to an email id. To export the report:

1. Navigate to the **SSH keys >> Discovered Keys**.
2. Select a single key.
3. Click the **Export** button. You can export the report to the system as PDF file, or to desired email addresses.
    - **PDF** – Export and save the report of the discovered keys as a PDF in the system.
    - **Email** – Specify the email addresses to which the report of the discovered SSH keys is to be exported.

Manage SSL Certificates

Create, discover and store SSL certificates in the centralized repository of PAM360. Raise requests for new certificates and domain additions to the existing certificates. You receive notifications when the certificates are about to expire, to help you with their timely renewal.

Use PAM360 to:

1. Create, discover, or import self-signed or CA issued certificates in the network.
2. Generate Certificate Signing Request (CSR).
3. Add requests for new certificates or adding a sub domain to an existing certificate.
4. Receive notifications when certificates are about to expire.

Steps to Manage SSL Certificates

1. Discover SSL certificates in your network
    - 1.1 Discover SSL certificates on demand
    - 1.2 Discover SSL certificates from SMTP servers
    - 1.3 Discover SSL certificates deployed to load balancers
    - 1.4 Discover SSL Certificates from a Shared Directory Path
    - 1.5 Discover SSL certificates using the Key Manager Plus (KMP) agent
    - 1.6 Discover SSL certificates automatically through schedules
    - 1.7 Discover certificates mapped to user accounts in Active Directory
    - 1.8 Discover SSL Certificates Hosted on AWS (ACM & IAM)
    - 1.9 Discover SSL Certificates using ManageEngine Mobile Device Manager Plus
2. Create self-signed certificates
3. Generate CSRs
4. Certificate signing
    - 4.1 Microsoft Certificate Authority
    - 4.2 Microsoft CA with Agent
    - 4.3 Sign with Root
5. Import and Export Certificates
6. Certificate Renewal
7. Certificate History
8. Certificate Sync Status
9. Edit and Delete Certificates

10. Certificate requests
    10.1 Add Certificate Request
    10.2 Certificate request status
    10.3 Terminate the certificate request life-cycle
11. Control expiry notification schedule
12. Track domain expiration through WHOIS lookup
13. SSL certificate group
    11.1 Create certificate groups
    11.2 Edit certificate groups
    11.3 Delete certificate groups

1. Discover Certificates in your Network

You can automatically discover all the certificates available in your network using PAM360, irrespective of the CA. You can discover the certificates anytime as needed or periodically based on scheduled tasks. The discovery options are quite flexible - you can discover certificates from a single server or multiple servers, and from multiple ports, at one go. PAM360 also allows users to rediscover the expired and about-to-expire certificates from the 'Certificate Expiry' widget in the Dashboard.

1.1 Discover SSL Certificates On Demand

To discover the certificates manually:

1. Go to **Certificates >> Discovery.**
2. Click the **Certificates** tab.
3. Select an option for the type of discovery.
    i. **Hostname/IP address** – Enter the name or IP address of the server from which the SSL certificates are to be discovered.
    ii. **IP address range** – Specify an IP range and discover all the SSL certificates available in the servers falling under the range.
    iii. **From file** – If you have a list of the servers in which certificates are available in your network saved as a text file, it can be loaded directly and all these certificates can be discovered.
    iv. **Subnet** – Use this option to discover resources from specific subnetworks within an IP range.
    v. In SSL Hostname discovery if you want the host name to resolve to a specific IP

address, provide the IP address after host name separated by colon (:) as shown below

complex:172.168.203.56

Same format can be provided in "From file" discovery also.

Notes:

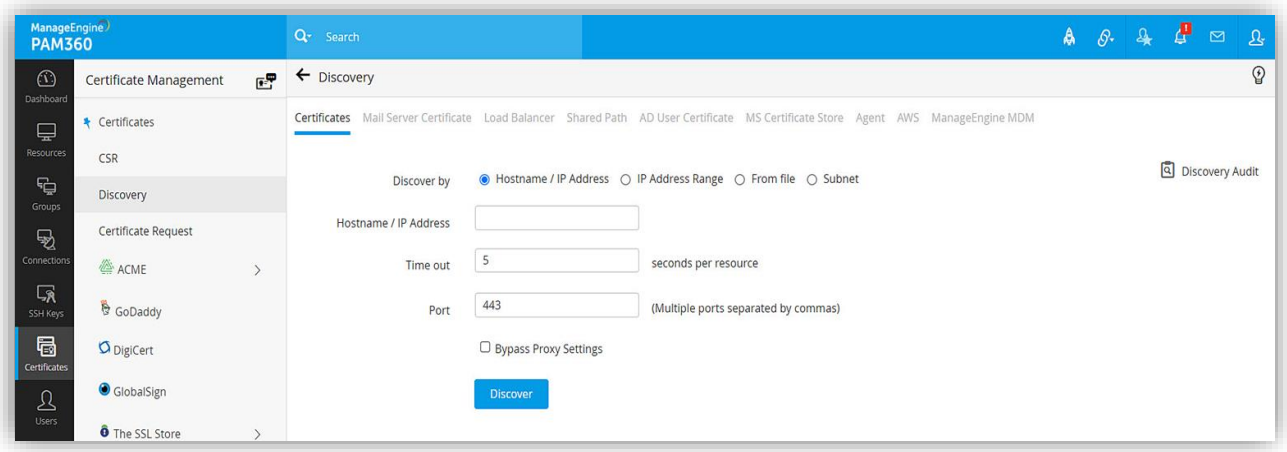
1. You can specify multiple ports separated by commas for the discovery of SSL certificates in a single discovery instance
2. During SSL discovery or when manually adding certificates to the PAM360 repository, you can exclude specific certificates by providing their details (common name and serial number) under **Admin >> SSH/SSL Config >> Excluded Certificates**. The specified certificate will be excluded from being imported into the PAM360 certificate repository during discovery or manual addition.

0.0.0.0	6565
test-username-10	443
192.168.20.20 8282	

1. For bulk discovery using IP address range and Subnet options, there is an **Exclude IP Address** field that allows you to exclude specific resources from being discovered. Specify the IP addresses of the resources that need to be excluded one below another.
2. Specify values for the Time out and the Port options.
    i. **Time Out:** Refers to the number of seconds the application tries to discover the certificates (each). The default value is 5 seconds.
    ii. **Port:** It refers to the port on the end terminal used for SSH communication. Port 443 is used by default for SSL certificates.

Note: You can specify multiple ports separated by commas for the discovery of SSL certificates in a single discovery instance.

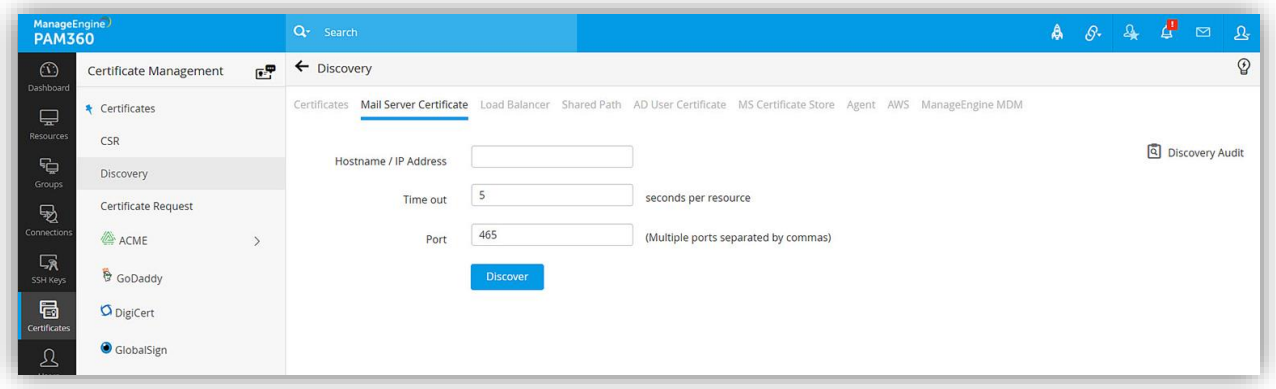
3. Select the **Bypass Proxy Settings** checkbox to bypass proxy server settings if you have enabled them under Admin Settings. If this option is selected, PAM360 will bypass the proxy server and directly perform online certificate discovery. The option to bypass the proxy server is available for SSL certificate discovery using **Hostname/IP Address, IP Address Range, From File,** and **Subnet** modes**.** In addition, you can bypass proxy server during scheduled certificate discovery as well.
4. Click **Discover**. You will be redirected to the **Discovery Status** page where the status of the current discovery instance is updated.



1.2 Discover SSL Certificates from SMTP Servers

You can discover SSL certificates used by mail servers present in your network and consolidate them in PAM360's centralized certificate repository. To perform mail server certificate discovery:

1. Navigate to **Certificates >> Discovery >> Mail Server Certificate**.
2. Provide the **Hostname / IP address** from which the certificate is to be discovered and specify the port number. You can specify multiple port values by separating them with commas.
3. Click **Discover**. On successful discovery, the certificates are fetched from the specified resources and added to PAM360's repository.



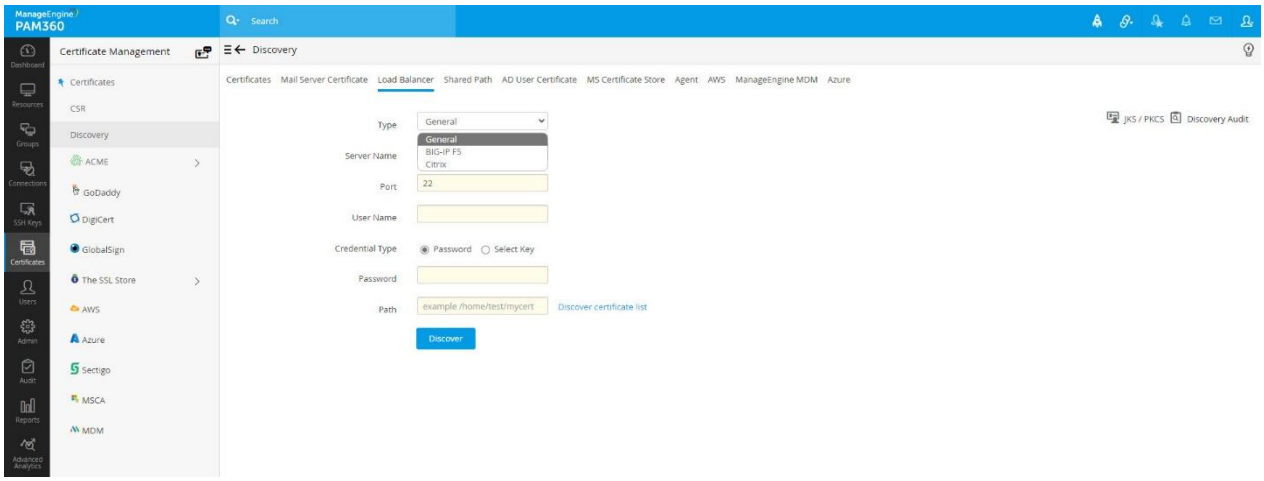
1.3 Discover SSL Certificates Deployed to Load Balancers

PAM360 allows you to discover SSL certificates deployed to load balancers, within your network, and consolidate them in its secure, centralized repository. As of now, PAM360 supports discovery of certificates from Linux-based load balancers only (i.e., Nginx, F5, etc) and the process is tunneled via SSH. To perform load balancer certificate discovery:

1. Navigate to **Certificates >> Discovery >> Load Balancer.**
2. Specify the **Server Name, Port, User Name, Credential Type, Password** and **Path.**
3. You can opt for a key-based authentication for password-less resources by choosing the **Select Key** option. Upload the private key associated with the required user account and specify the key passphrase.
4. Select a load balancer type from the drop-down. PAM360 supports three types of Load Balancer discovery: **General, BIG-IP F5,** and **Citrix.** You can perform Citrix type discovery in two ways: using CLI commands and using REST API.
5. Once you have provided the user credentials, specify the path to the folder in the server from where the certificates have to be discovered.
6. The **Discover certificate list** option fetches all the certificates available in the specified path and helps you choose certificates that you wish to discover and import.
7. To discover Citrix load balancers, do the following:
   i. Choose the type as **General**, enter the Citrix load balancer path, and click **Discover**.
   ii. In case that does not work, choose the type as **Citrix**, enter the path, and try again.
   iii. If both the above methods fail, choose the type as **Citrix**, select the checkbox **Use REST API (By default PAM360 uses CLI commands for discovery and fetching certificates),** enter the path, and click **Discover**.

iv. Select a **Citrix Credential** from the dropdown.
v. Click **Manage Credentials** to add or delete a credential.
vi. In the pop-up that appears, click to **Add** and mention the Credential Name, Server IP, Citrix Username and Citrix Password.
vii. Click **Test Login** to test the credential and click **Save Credentials**.
viii. To Delete a credential, select a credential you want to delete and click **Delete** and in the pop-up that appears click **OK**.
ix. Enter the path, and click **Discover**.
x. During Citrix load balancer discovery using REST API, you can choose to bypass your proxy server settings by selecting the Bypass Proxy Settings checkbox. This option allows you to bypass the proxy server you have enabled under Admin settings directly perform Citrix load balancer discovery through the internet.
xi. Please note that you can choose to bypass proxy server settings for Citrix load balancer discovery only if you select the Use REST API (By default PAM360 uses CLI commands for discovery and fetching certificates) option. The bypass proxy server option is also available during scheduled Citrix load balancer discovery.

8. The certificates are successfully discovered and imported into PAM360's centralized certificate repository. You can view them from the **Certificates** tab. The **Discover certificate** list option fetches all the certificates available in the specified path and helps you choose certificates that you wish to discover and import.
9. Certificate files with the extensions .keystore and .pfx are not automatically imported into the certificate repository; they require their passphrases to be provided in order to be imported into PAM360. To import these files, click **JKS / PKCS** at the top-right corner of the window. In the window that pops up, choose the certificate file(s) that you wish to import and click **Import** from the top menu. In the pop up that opens, provide the file passphrase(s) and again click **Import**.
10. The chosen certificate files are successfully imported and added to PAM360's certificate repository.



Note: During the Citrix REST API-based load balancer discovery, the user credentials you provide must have sufficient permissions to read files and for REST API access. Therefore, to ensure success of the discovery, it is recommended that you supply the credentials of an account which has the superadmin role.

1.4 Discovering SSL Certificates from a Shared Directory Path

PAM360 allows you to discover SSL certificates that are saved in a shared directory path within your network and consolidate them in its secure, centralized repository. Using this option, you can discover all the certificate files saved in a particular folder and then, either add all the certificates to the repository or choose the ones you want to import. During the discovery process, PAM360 will scan only the folder specified in the path and nowhere else in the target machine.

Follow the below steps to discover and import SSL certificates from a shared directory path:

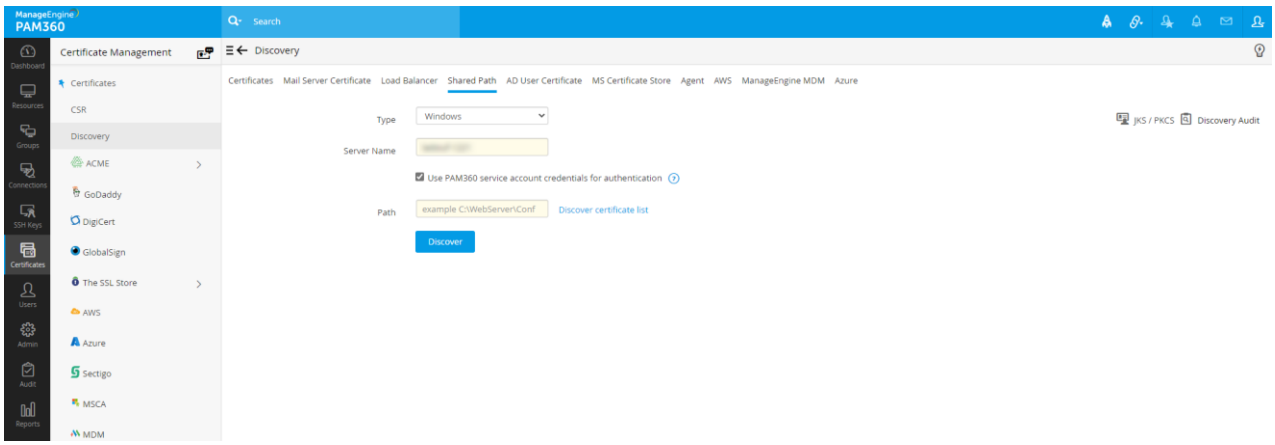
1. Navigate to **Certificates >> Discovery >> Shared Path.** Choose **Windows** or **Linux/Mac OS** from the **Type** dropdown.
2. For **Windows**:
    i. Enter the **Server Name** of the target machine where the shared path resides; leave this field empty if you are entering a directory path from your local machine.
    ii. Select the checkbox to **Use PAM360 service account credentials for authentication** or provide a username and password.
    iii. Specify the directory path of the target machine. Example:

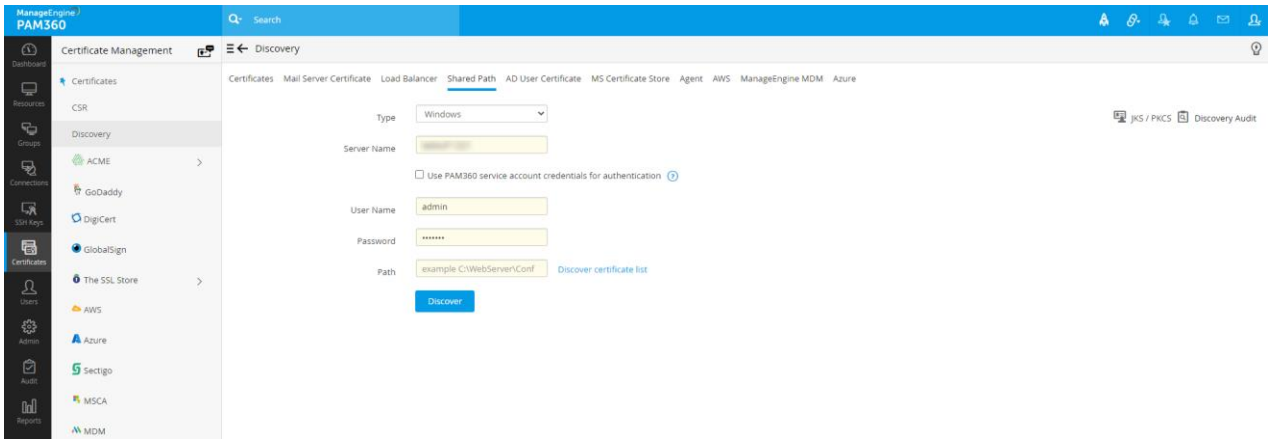
D:\sharedpath\subsharedpath.

3. For **Linux/Mac OS**:
    i. Enter the **Server Name** of the target machine where the shared path resides, the port, and the username.
    ii. For authentication, either choose the **Password** option and enter the password directly or choose the **Select Key** option and upload a private key with its passphrase for SSH key-based authentication.
    iii. Specify the directory path of the target machine. Example: \home\test\shared.
4. Click the **Discover certificate list** option to fetch all the certificates available in the specified path. From this list, choose certificates that you require and click **Discover**. If you don't choose any specific files, all certificate files found in the shared path will be imported.
5. Certificate files with extensions .keystore and .pfx are grouped separately under the **JKS / PKCS** option in the top right corner. To import these certificates, click **JKS / PKCS**, choose the certificate files that you wish to import, provide the file passphrase, and click **Import**.

To check the status of the discovery, click the **Discovery Audit** tab.

> **Note:** Certificate files that are over 30 KB in size will not be imported during this discovery operation.





1.5 Discover SSL certificates using the Key Manager Plus (KMP) Agent

You can discover SSL certificates deployed across your network using the KMP agent right from the PAM360 web interface. This functionality enables you to download and deploy KMP Windows agent to target systems. It also allows you to discover and import the certificates from those systems into a centralized certificate repository directly from the PAM360 web interface. The server(s) in which the agent is deployed is connected to the PAM360 server via a secure HTTPS connection.

Discovering certificates through the KMP agent is helpful in the following scenarios:

- When the administrative credentials of the target server(s) required to perform the discovery operation are not available in the PAM360 server.
- When you have to discover the certificates from servers that PAM360 doesn't have direct access to—say, for instance, the servers in demilitarized zones (DMZs). In such cases, the agent is usually installed in an intermediate jump server which has the permission to access the remote servers and pass on the required information to the PAM360 server.

To discover the SSL certificates using the KMP agent, you need to download and install the agent first. Follow the steps below:

To perform SSL certificate discovery through KMP agent:

1. Navigate to **Certificates >> Discovery >> Agent**.
2. Choose the type of discovery you want to perform—**Domain-based, Certificate Store,** or **Certificates issued by Microsoft Certificate Authority.**
3. Select the required agent from the drop down to perform the operation.

4. If the agent is busy, wait and try again after sometime.
5. For **Microsoft CA discovery**, you can choose to exclude expired / revoked certificates or perform discovery based on issue date or certificate template using the filters provided.
6. Click **Discover**.

The certificates are discovered from the servers in which the agent is installed and imported into PAM360's certificate repository.

1.5.1 Discover SSL Certificates from a Directory Path in a Remote Machine

PAM360 allows you to discover SSL certificates that are saved in a directory path in a remote machine that is not directly accessible by the PAM360 server—this is achieved through the Key Manager Plus agent. Once the certificates are discovered, you can consolidate them into PAM360's centralized repository. Using this option, you can discover all the certificate files saved in a particular folder and either add all the certificates to the repository or select only the ones you require. During the discovery process, the Key Manager Plus agent will scan only the folder specified in the path and nowhere else in the target machine.

Follow the below steps to discover and import SSL certificates from a directory path in remote machine:

1. Navigate to **Certificates >> Discovery >> Agent** and choose **Directory** as the type of discovery.
2. Select an agent from the drop-down menu.
3. Specify the directory path of the target machine, eg: D:\sharedpath\subsharedpath.
4. Click the **Discover certificate list** option to fetch all the certificates available in the specified path.
5. From this list, choose certificates that you require and click **Discover**.
6. Enter a time out interval in seconds.
7. Certificate files with extensions .keystore and .pfx are grouped separately under the **JKS / PKCS** option in the top right corner. To import these certificates, click **JKS / PKCS**, choose the certificate files that you wish to import, provide the file passphrase, and click **Import**.

To check the status of discovery, click the **Discovery Audit** tab.

Notes:

- This feature will work with the latest Key Manager Plus agent only.
- Certificate files that are over 30 KB in size will not be imported during this discovery operation.

1.6 Discover SSL Certificates Automatically Through Schedules

SSL Certificate discovery can also be scheduled to occur at periodic intervals.

1. Navigate to **Admin >> SSH/SSL Config >> Schedule**.
2. Click the **Add Schedule** button.
3. In the **Add Schedule** window, enter a name for the schedule and select the type of schedule as **SSL Discovery**.
4. Specify the start and end IP addresses and the port on the end terminal to check for **SSL certificates**.
5. Select the recurrence type – hourly, daily, weekly, monthly, or once only. Set the starting time, date, or day corresponding to the option chosen.
6. Enter the email addresses of the users to be notified. The email settings can be configured from the **Settings >> Mail Server Settings** tab.
7. Click the **Save** button.

You will get a message confirming addition of a new schedule.

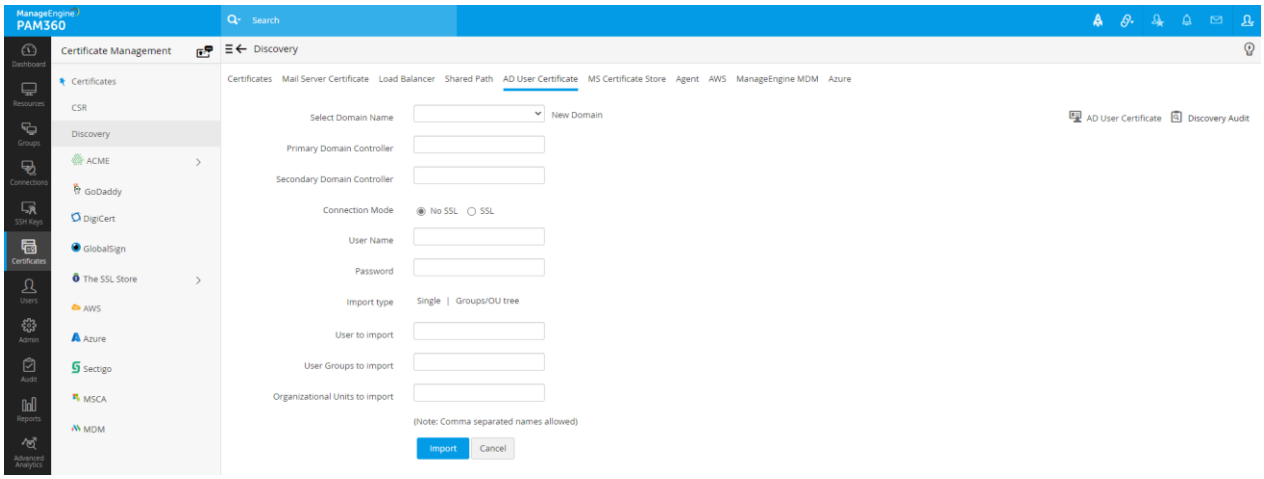
1.7 Discover SSL Certificates Mapped to User Accounts in Active Directory

PAM360 helps you discover and manage the certificates mapped to user accounts in Active Directory.

To perform AD user certificate discovery,

1. Navigate to **Certificates >> Discovery >> AD User Certificate**
2. Select the required **Domain Name**, which forms part of the AD from the drop-down.
3. Specify the DNS name of the domain controller. This domain controller will be the primary domain controller.

4. In case, the primary domain controller is down, secondary domain controllers can be used. If you have secondary domain controllers, specify their DNS names in comma separated form. One of the available secondary domain controllers will be used. When you use **SSL mode,** make sure the DNS name specified here matches the CN (common name) specified in the SSL certificate for the domain controller.
5. Enter a valid user credential (user name and password) of a user account within the particular domain. Then enter the users / user groups / OUs in which you want to perform the certificate discovery and click **Import**. To perform certificate discovery for groups/OUs as a whole, choose Groups/OU tree Import type and select the required groups from the drop-down list.
6. PAM360' also provides an option to import AD users while performing the certificate discovery. Enable the check box **Import AD users** to import those AD user accounts into PAM360 for which the certificate discovery is done.
7. The discovered certificates automatically get added to the certificate repository of PAM360.



1.7.1 Manage SSL Certificates from MS Certificate Store and Local CA

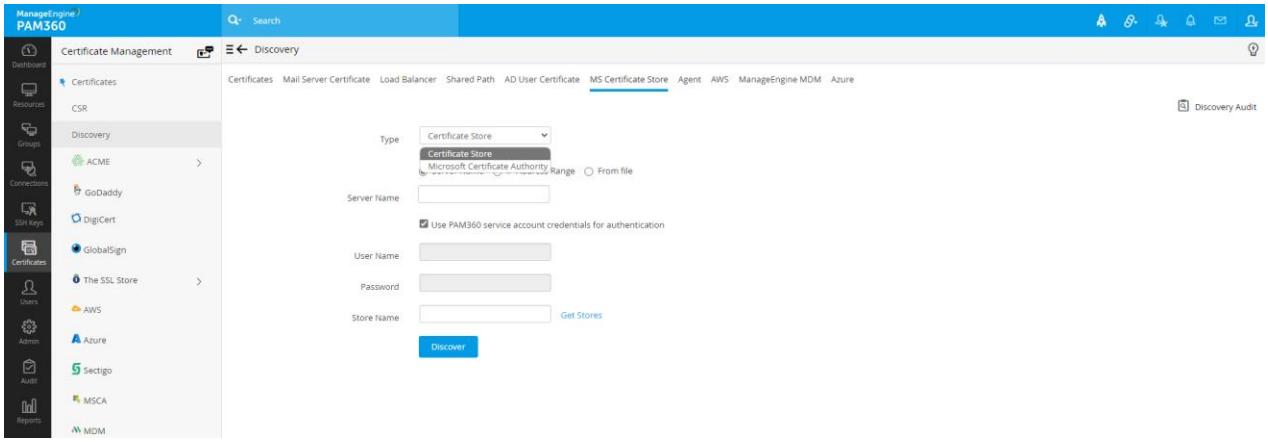
PAM360 helps you request, acquire, discover, consolidate, track and manage certificates from MS Certificate Store and those issued by Local certificate authority. Before importing / acquiring certificates from MS Certificate Store and Local CA, ensure that you use your domain administrator account as PAM360' service logon account.

1. Navigate to **Certificates >> Discovery >> MS Certificate Store.**
2. To discover and import certificates issued by Microsoft CA alone, select **Local**

Certificate Authority option from the drop down. In the process, you can choose to exclude expired / revoked certificates by de-selecting the check-boxes below.

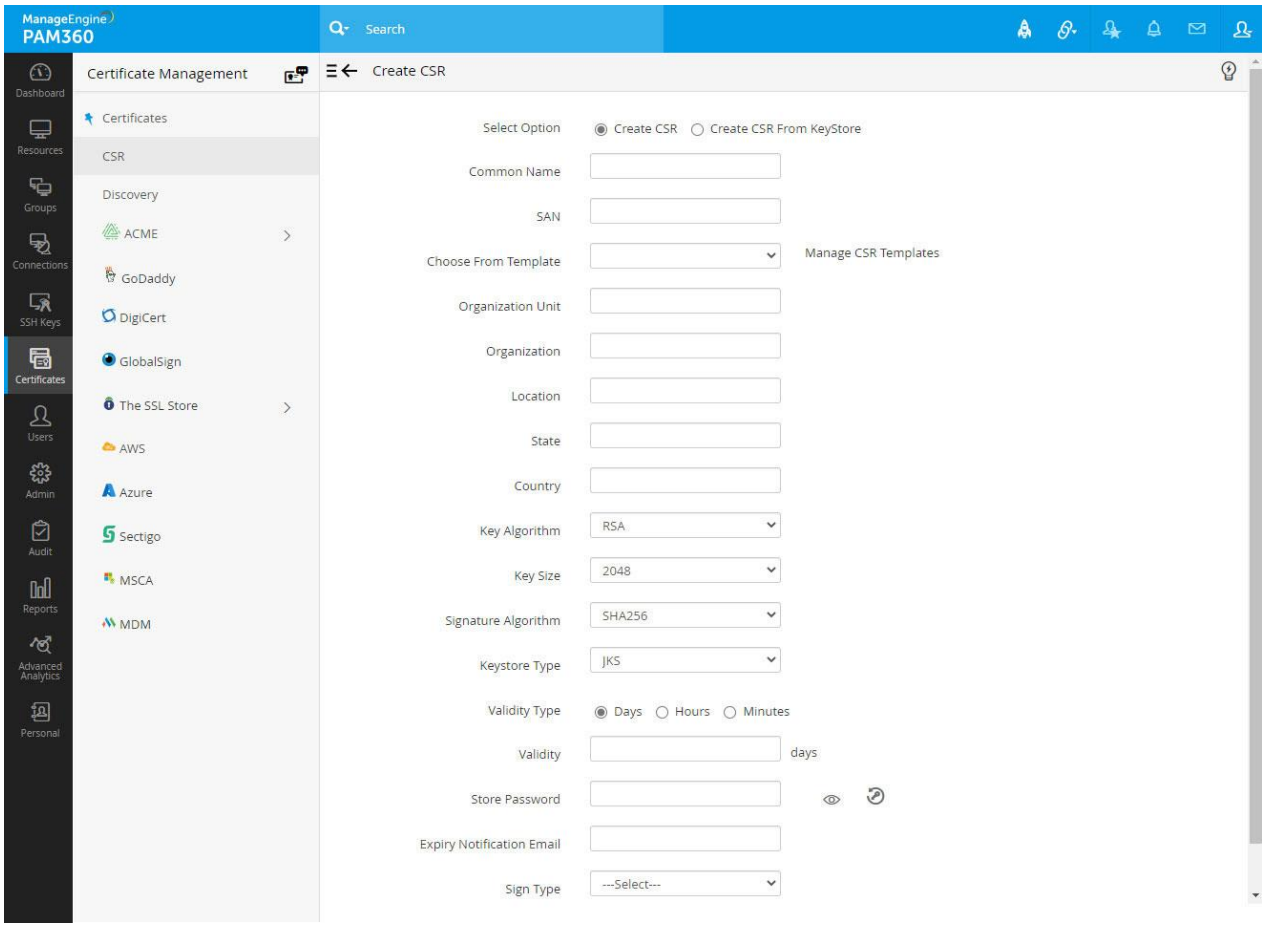
3. To discover all the certificates from MS certificates store, choose **Certificate Store** type from the drop-down menu.
4. Select the checkbox to **Use PAM360 service account credentials for authentication** or you can specify the other details such as the **Name** of the Windows domain controller machine and domain admin credentials.
5. If you choose to **Use PAM360 service account credentials for authentication**, you can select **IP Address Range** to mention the **Start IP** and **End IP** to discover the certificates.
6. Specify the certificate store name from which the certificates are to be discovered and imported.
   i.e., Following format to be used while specifying the certificate **store name:\\server_name\store_name**
   i. **e.g., server_name\Root** (To discover certificates from trusted root certification authorities)
   ii. **e.g., server_name\My** (To discover personal certificates)
7. Or you can also click **Get stores** to fetch the list of stores available in the Windows Domain Controller and choose the required certificate store that you want to discover.
8. Click **Discover**. You can view the discovered certificates in **Certificates** tab.
9. To discover certificates issued by a particular MSCA, select Type as **Microsoft Certificate Authority** from the drop-down, enter the **Server Name**, required credentials, and enter an MSCA name in the **Microsoft Certificate Authority** text box. Please note that this text box will be visible only if your PAM360 server is installed in a Windows Server machine.
10. During discovery, you can choose to include expired, revoked certificates by selecting the respective check boxes. Select **Date Filter** and enter a date range to filter the discovered certificates as per the given range. Select the **Template Name / OID** option to choose certificate templates. You can add upto five certificate templates for each discovery operation. This option is available during scheduled discovery of certificates issued by a particular MSCA as well.

Note: During Windows Certificate Store discovery, if the target server name is not specified, choosing Get Stores option will list down all the certificate stores available in the local host.



To request and acquire certificates stored in Local CA from PAM360, you have to initially generate a certificate signing request, then get it signed from the local certificate authority using the steps mentioned below.

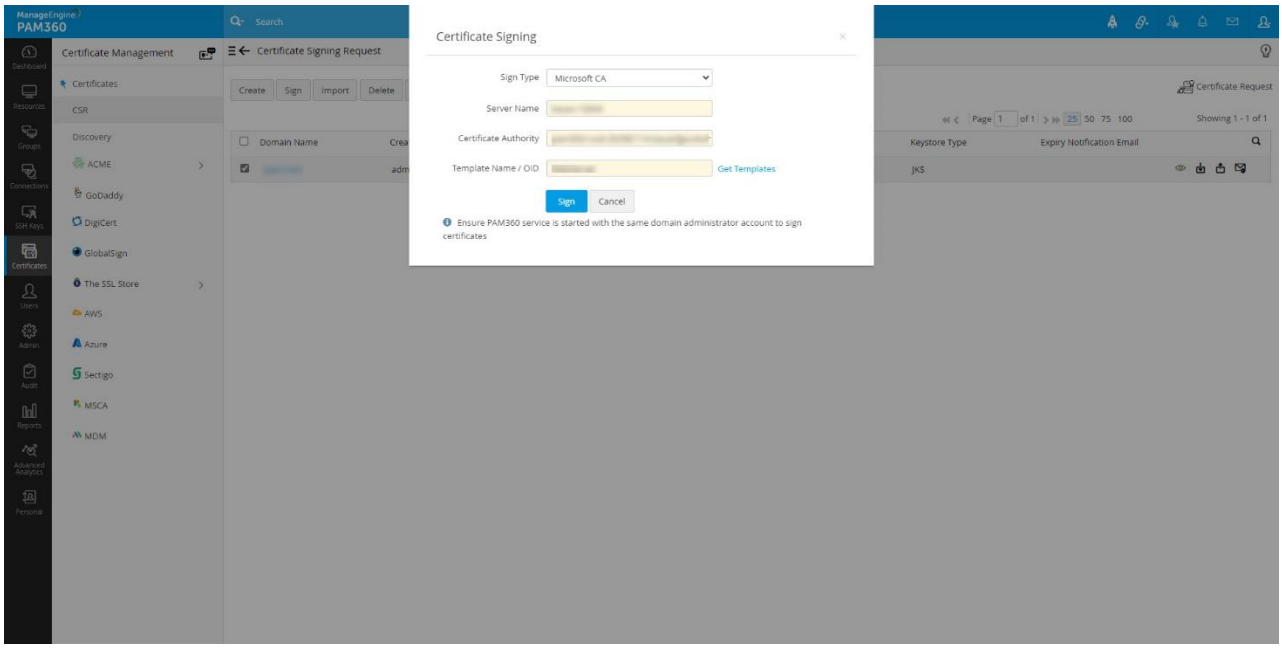
1. Navigate to **Certificates >> Create CSR** and click **Create.**
2. In the **Create CSR** window that opens, fill in the domain details, organization details, choose the key algorithm, key size, signature algorithm, keystore type and specify the validity (days) and keystore password and click **Create.**



3. If you want to generate a CSR from an already existing key, choose **'Create CSR From Private Key'** option and specify the key location, password and click **Create.**
4. The CSR will be generated and you can view it from **Certificates >> Create CSR** tab.

You can also get the CSR signed from Microsoft Certificate Authority directly from PAM360 itself.

1. Navigate to **Certificates >> Create CSR** tab, select the required CSR and click **Sign** from the options available above the CSR table view.
2. In the dialog box that opens, provide the name of the server that runs the internal certificate authority, CA name and choose the certificate template based on your requirement. Click **Sign.**
3. The CSR is signed and the issued certificate can be viewed from the **Certificates** tab.



1.7.2 Rediscover SSL Certificates

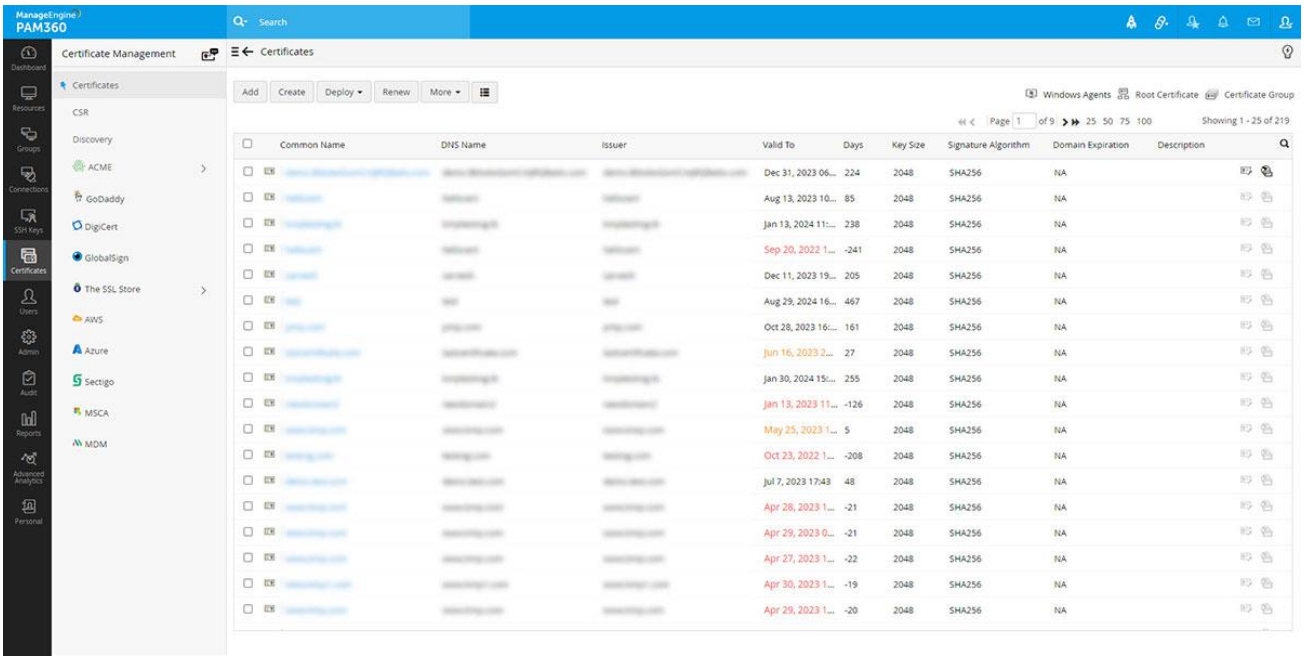
From PAM360 build 5300 onwards, PAM360 allows you to rediscover SSL certificates from the same source using the server details entered during the previous discovery operation. Follow the below steps to perform certificate rediscovery:

1. Navigate to the **Certificates** tab.
2. Select the required certificates and click **More >> Re Discover**.

The rediscovery operation begins immediately. You can track the discovery status in the **Discovery Audit** page. Please note that for agent-based discovery to work properly, upgrade Key Manager Plus Agent to version 6000 before commencing the discovery operation.

1.7.3 The Centralized Certificate Repository

All the discovered SSL certificates, those that are discovered manually as well as those discovered through scheduled discovery operations are automatically added to the centralized repository of PAM360. You can view these certificates under the **Certificates >> Certificates** option in the user interface.



i. Search SSL Certificates

PAM360 allows you to search certificates using **Common Name, DNS Name, Issuer, Key Size, Signature Algorithm, Description,** additional fields, etc.

1. Navigate to **Certificates >> Certificates.**
2. Click the **search icon** present on the right corner of the table header and mention the search phrase(s) in the text box(es) that appears.

1.7.4 Export Private Key/Keystore File

PAM360 allows you to identify and export the private keys / keystore files of SSL certificates stored in the certificate repository. You can also export certificates in other formats such as PKCS12/PFX or PEM format. Click the Keystore icon () enabled beside the certificates for which the private keys are managed using PAM360.

To export the private key or the certificate file:

1. Navigate to **Certificates >> Certificates**.
2. Click the **Keystore** icon () beside the certificate for which you need to export the private key.
3. From the dropdown, choose from the following options as per your requirement:
    i. **Export Keystore / JKS**: The keystore file of the selected certificate will be downloaded.

ii. **Export PKCS12/PFX**: The selected certificate will be downloaded in the PFX format.
iii. **Export PEM**: The selected certificate will be downloaded in the PEM (Privacy Enhanced Mail) format.
iv. **Export Private Key**: The private key of the selected certificate will be downloaded.

4. The corresponding certificate is downloaded in the selected format.

1.7.5 Track and Manage Various Certificate Versions

Sometimes, there occurs a situation where you have to use different certificates on different end-servers for the same domain. Under such circumstances, it is necessary for you to track the usage and expiry of all these certificates individually even though they represent a common domain. Monitoring various such certificate versions manually is daunting and error-prone. PAM360 helps you simultaneously track and manage the usage and expiry of various certificate versions from a single window.

To track certificate versions,

1. Navigate to the **Certificates** tab.
2. Click the **certificate history** icon ( ) present in the right corner of the table view, corresponding to the required certificate.
3. In the certificate history window that opens, choose the certificate version you wish to manage and click the certificate settings () icon. Click **Manage Certificate.**
4. The particular certificate version is set for managing and PAM360 starts tracking the usage and expiry individually for that version.
5. Repeat the same procedure for all the certificate versions that you wish to manage.

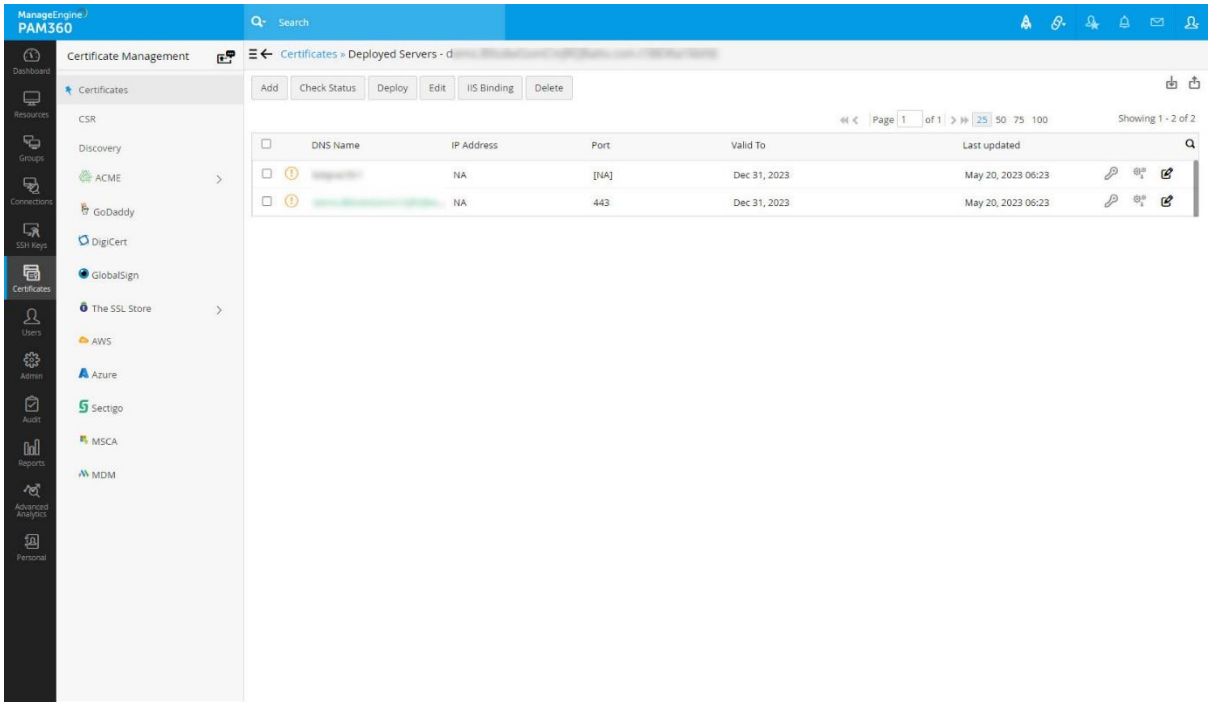
1.7.6 Update Servers with Latest Certificate Versions

In case of wildcard certificates or single SSL certificate deployed to multiple servers, it is necessary to keep track of servers in which the certificate is deployed and also check if the latest certificate version is in use. PAM360 helps you ensure this.

1. Navigate to **Certificates >> Certificates tab**
2. Click the **Certificate History** icon ( ) corresponding to the required certificate
3. A window opens listing the various versions of the certificate. Ensure that the latest

version of the certificate is set as the main certificate. If not, click the ( ) icon beside the required version to set that version of certificate as main certificate in the PAM360 repository.

4. Then again, navigate to **Certificates >> Certificates tab and click multiple servers icon** ( ) corresponding to the required certificate.
5. A window opens listing the servers in which the certificate is deployed along with other information such as IP address, port and certificate validity.
6. If any of the servers listed has an older / expired version of the certificate, update it with the latest version immediately. Select the server and then click **Deploy**. Refer to the detailed deployment procedure here.
7. Click edit icon corresponding to the required server to modify the server details.
8. Click **Add** to add a new server.
   i. In the pop-up that appears, mention the **DNS Name, IP Address** and **Port.**
   ii. Click **Save.**



9. Click edit icon corresponding to the required server to modify the server details.
10. Select a certificate and click **Check Status** to check the sync status of the certificate. To know more about Certificate sync status, click here.

Also, you can edit details pertaining to a particular certificate or delete irrelevant certificates by selecting the certificate and clicking the **More** dropdown.

1.8 Discover SSL Certificates Hosted on AWS (ACM & IAM)

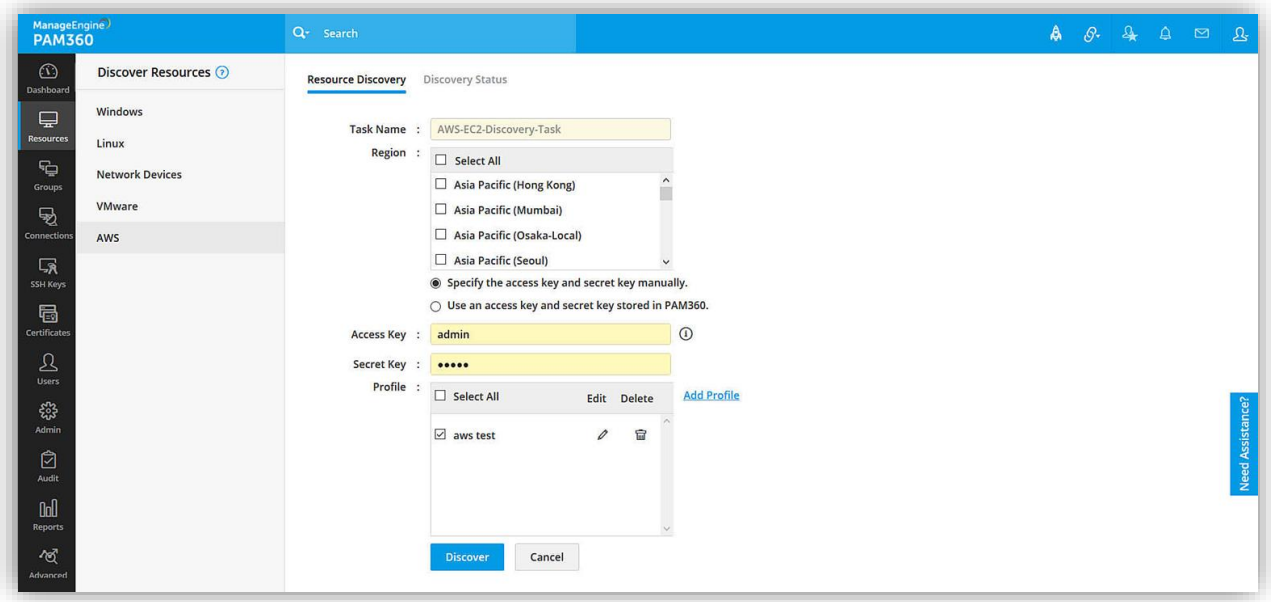
PAM360 enables you to discover, import, and configure expiry notifications for SSL certificates hosted in the following Amazon Web Services: AWS Certificate Manager (ACM) and AWS Identity and Access Management (IAM).

Follow the steps below to discover and import SSL certificates from ACM / IAM into PAM360.
Navigate to **Certificates >> Discovery >> AWS**.

Step 1: Configure AWS credentials in PAM360

Follow the below steps if you have not added an AWS-IAM resource in PAM360:
To add your AWS credentials in PAM360,

1. Click **Manage AWS Credential** and click **Add.**
2. In the Create AWS Credentials window that opens, provide the **Credential Name, Description, Access Key** and **Secret Key.**
3. Use the **Test Login** option and check if the login is successful. You will be notified if the login is successful.
4. Then click **Save.** The credentials are successfully saved in PAM360.
5. Now, navigate to **Certificates >> Discovery >> AWS** and choose the appropriate **AWS Credentials** from the drop-down or provide your **Access Key** and **Secret Key** manually.



If you have already added an AWS-IAM resource in PAM360,

1. Choose if you want to **Specify the access key and secret key manually** or **Use an access key and secret key stored in PAM360.**
2. If you have chosen **Specify the access key and secret key manually**, enter your **Access Key** and **Secret Key.**
3. If you have chosen **Use an access key and secret key stored in PAM360**, select the **Resource Name, Access Key** and **Secret Key** from the dropdown.

Step 2: Discovery and Import

1. Choose the required **AWS Service** from which certificates need to be imported: **ACM or IAM.**
2. To import certificates from ACM, select ACM under AWS service and choose the service **Region.**
3. Click **Discover.**
4. Certificates are discovered from resources in the selected region and imported into PAM360.
5. To import certificates from IAM, specify the required AWS **User Name(s)** or use the **List AWSUser Names** option to retrieve the usernames. Choose the required usernames and click **Discover.**

6. You can also choose to import server certificates for the corresponding AWS users by checking the **Include Server Certificate** option.

User certificates are imported into PAM360.

1.9 Discover SSL Certificates using ManageEngine Mobile Device Manager Plus

PAM360 integrates with ManageEngine Mobile Device Manager Plus (MDM). Once the integration is done, you can discover and import SSL certificates from the devices managed through your MDM server and store the SSL certificates in the PAM360 repository. You can also deploy SSL certificates from PAM360 to the mobile devices listed in your MDM environment. Refer to this document for steps on how to discover certificates using ManageEngine MDM.

2. Create Self-Signed Certificates

PAM360 allows administrators to create their own self-signed certificates using Java keytool. These certificates are automatically imported into the PAM360 repository on successful creation.

To create a self-signed certificate using PAM360:

1. Navigate to the **Certificates >> Certificates >> Create.**
2. Enter the details of the organization and certificate validity, and select the key algorithm and length, signature algorithm, and enter a keystore password in the Create certificate tab.
3. Click the **Create** button. You will be redirected to the certificate window where the certificate content is displayed.
4. To create an ephemeral certificate with limited validity period, choose the **Validity Type** as **Hours** or **Minutes** and provide the validity period. The certificate will expire after the specified time.
5. Mention the email address to which the **Expiry Notification Email** should be sent.
6. You can denominate the certificate to be generated as a root certificate by enabling the **Generate root certificate** checkbox.
7. To add optional properties to the new certificate, click **Advanced Options** to expand the menu. Here, there are two categories of options, **Key Usage** and **Extended Key Usage**.

Select the required options to set the preferred flags for the certificate to denote the purpose for which the new certificate may be used. The **Key Usage** options include Non Repudiation, Digital Signature, Data or Key Encipherment, Server/Client Authentication etc. You can choose the properties and mark them as critical by selecting the **Critical** checkbox.

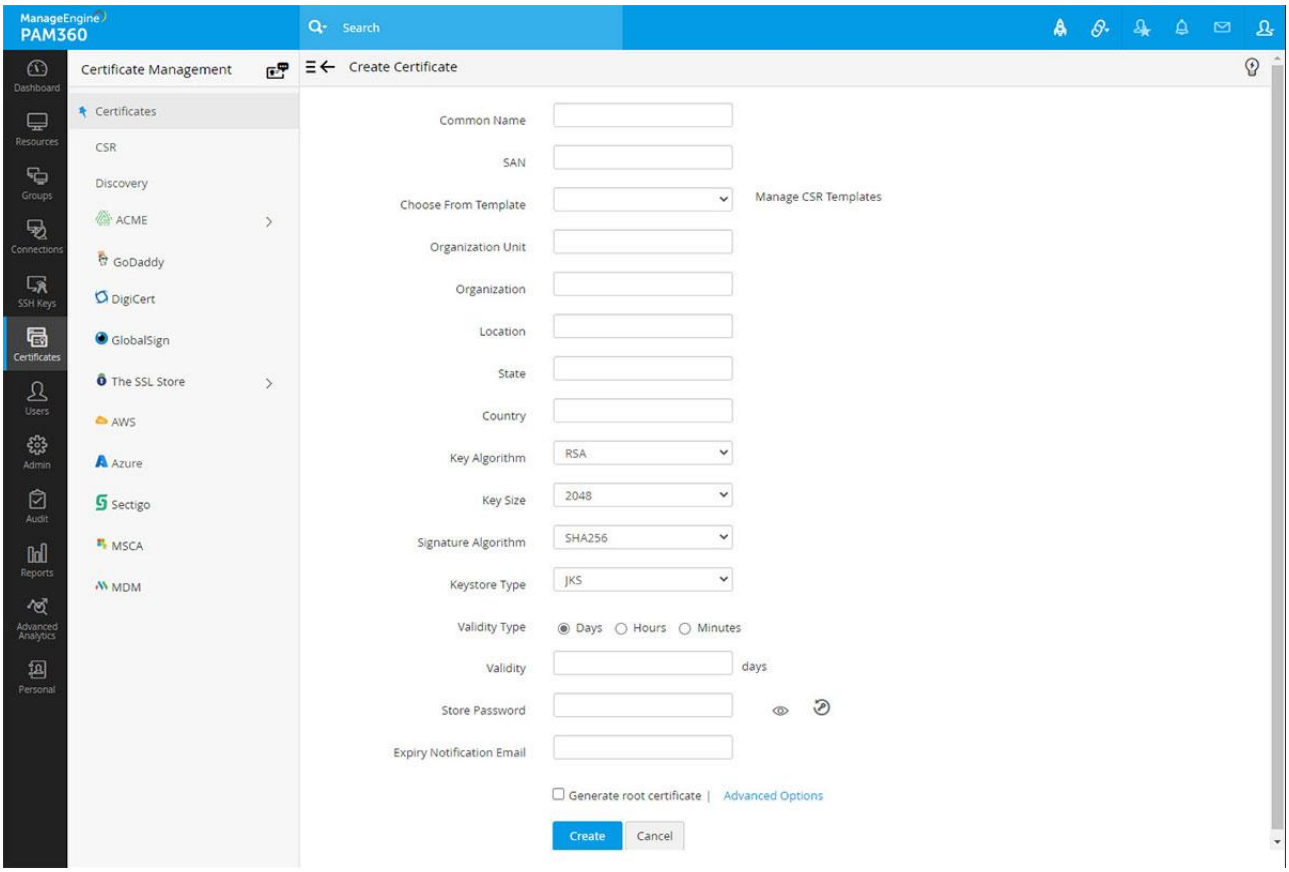
8. Click the **Create** button. You will be redirected to the certificate window where the certificate content is displayed.
9. You can copy the certificate content, or export the certificate to required email or system.
    a. **Email** – Select this check box to send the certificate file via email to the specified mail id.
    b. **Export** – Select this check box to export the file to your system.
10. Both the options take effect once you click **Save.**
11. Click the **Save** button to save the certificate in the PAM360 repository, and export the certificate file, if opted in the earlier step.

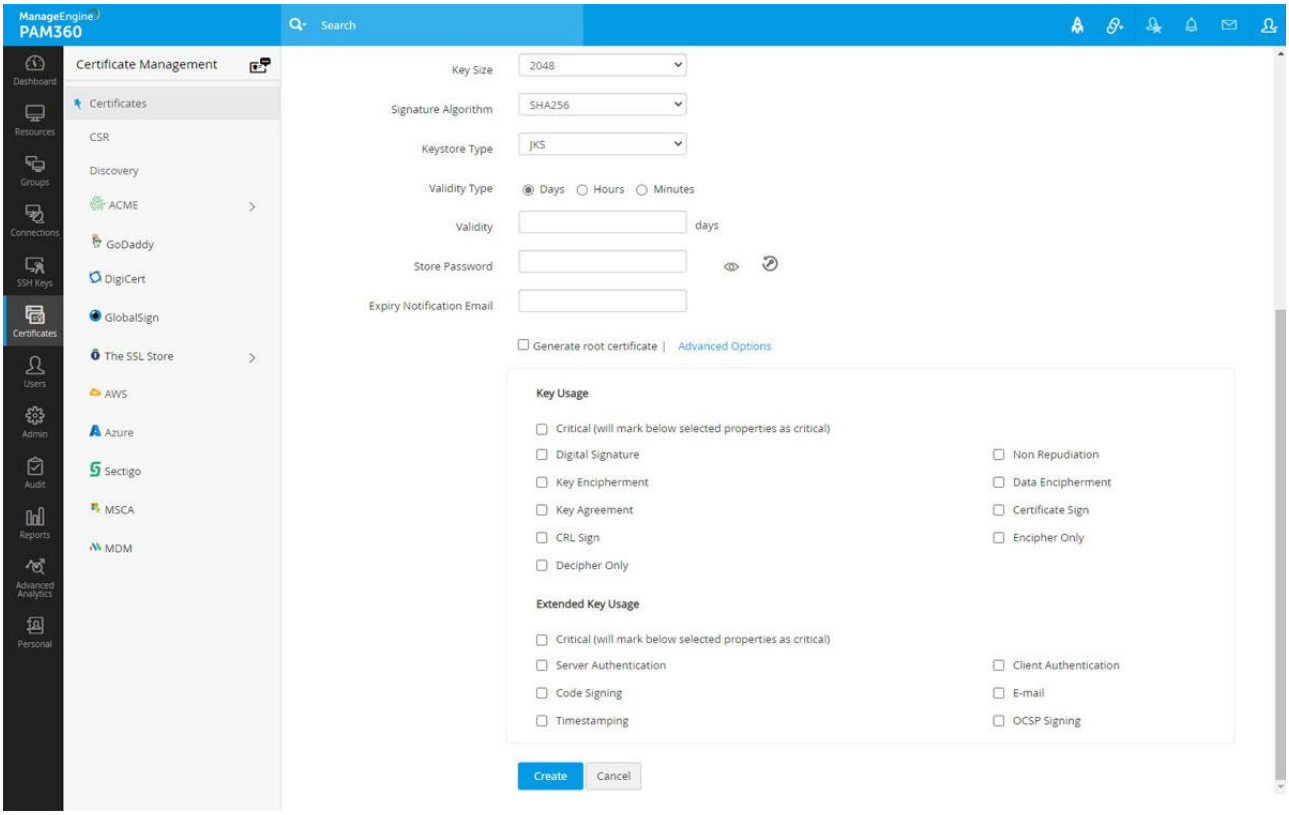
(Applicable from build 5000 onwards)

Note:

Apart from having a wildcard certificate name in the Common Name field, you can add the wildcard name in the SAN field while creating a self-signed certificate. With wildcard certificates, one can secure an unlimited number of subdomains for a registered base-domain.

For example, consider the base-domain zoho.com, a wildcard certificate for *.zoho.com can secure any-subdomain.zoho.com. The asterisk (*) is the wildcard that corresponds to any valid subdomain.





3. Generate CSRs

To generate a CSR using Java keytool from PAM360:

1. Navigate to the **Certificates >> CSR.** You will see all the available CSRs in a list view along with their details such as **Domain Name, Created By, Created Time, Key Size, Key Algorithm, etc.**
2. Click **Create** to generate a new CSR. In the form displayed, do the following:
    i. Choose between **Create CSR** manually or **Create CSR from Keystore.** You can also choose from a **CSR template**. Click the **Manage CSR Templates** link and choose one.
    ii. If you choose to **Create CSR from Keystore:**
        a. Select the Keystore file by clicking **Browse**.
        b. Enter the **Private Key Password** and click **Create.**
    iii. If you choose to **Create CSR** manually:
        a. Specify the required details such as **Common Name, SAN, Organization Unit, Organization, Location, State and Country.**
        b. Select the **Key Algorithm, Key Size, Signature Algorithm, and Keystore Type.**
        c. Choose a **Validity Type (Days, Hours or Minutes)** and mention the **Validity**.
        d. Enter the **Store Password** and **Expiry Notification Email** address. Click the **Generate Password** icon to generate a key store password.
        e. Select the **Sign Type** and enter the required details.
        f. You can also sign your CSR later by not choosing the **Sign Type** now. To know more about signing the CSR later, refer to the **Certificate Signing** section below.
        g. Click **Create**. You will be redirected to a CSR window where the CSR content is displayed.

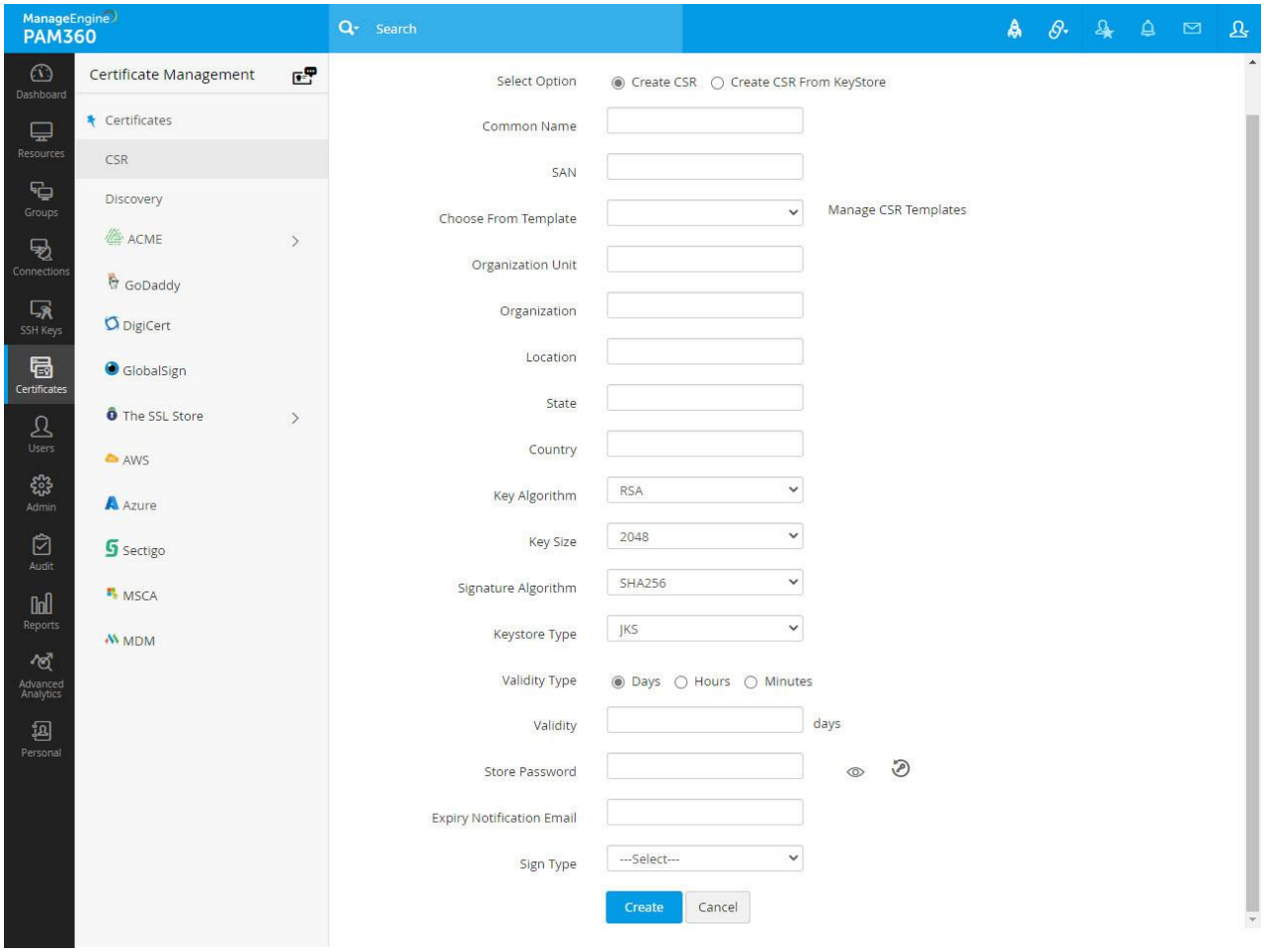
You have successfully created a CSR and it has been added to the list view.

(Applicable from build 5000 onwards)

Note:

Apart from having a wildcard certificate name in the Common Name field, you can add the wildcard name in the SAN field while creating a self-signed certificate. With wildcard certificates, one can secure an unlimited number of subdomains for a registered base-domain.

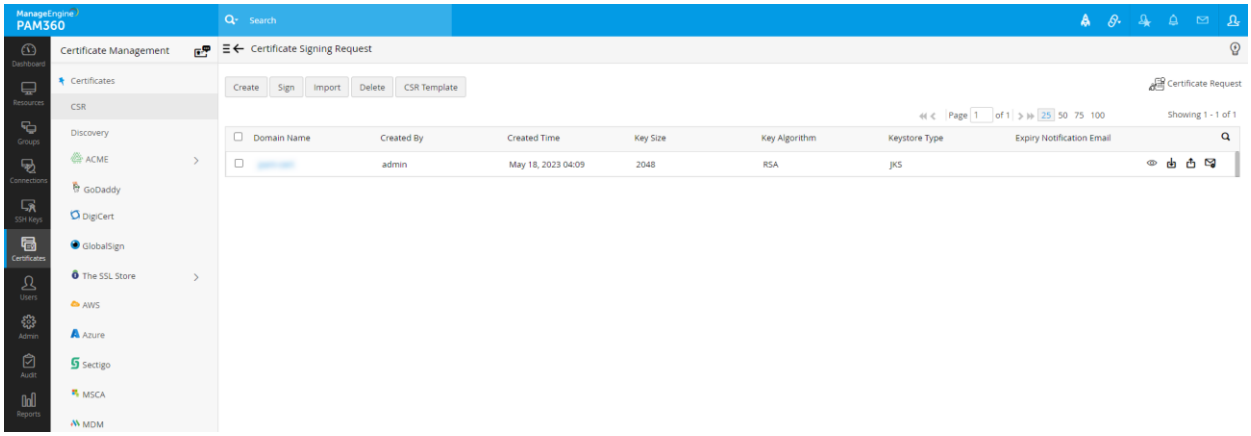
For example, consider the base-domain zoho.com, a wildcard certificate for *.zoho.com can secure any-subdomain.zoho.com. The asterisk (*) is the wildcard that corresponds to any valid subdomain.



3.1 Managing CSR

1. You can view the saved CSR from **Certificates >> Create CSR** tab.
2. **Show Passphrase:** The show passphrase icon ( ) corresponding to every CSR allows administrators to view the keystore passwords of respective CSR files.

3. **Export:** You can export and mail the CSR to a specified mail id by using the icon (✉) in the CSR displayed in the list view.
4. **Import:** If you choose to import a CSR, click **Import**. A pop-up appears.
    i. **Browse** and **Select a CSR file** and **Select a Key file.**
    ii. Enter the **Private Key Password** and click **Import**.
    iii. Your CSR has been successfully imported and can be viewed in the list view.
    iv. PAM360 automatically pins the certificate file with its corresponding private key and adds it to its centralized repository.
5. **Delete:** To Delete a CSR, select the CSR you wish to delete and click **Delete**.
    i. In the pop-up that appears, click **Ok**.
    ii. You have successfully deleted the selected CSR.
6. **CSR Template:** Click **CSR Template** to add, delete or manage the templates. These templates after generated can be used while generating CSR's.



Note: Self-signed certificates and CSRs can be generated using RSA / DSA / EC key algorithms and SHA signature algorithm as per the details below:

- RSA – 1024, 2048, or 4096 bit keys; & SHA-2 (256, 384, or 512 bit) signature.
- DSA – 512, or 1024 bit keys; & SHA-1 (160 bit) signature.
- EC – 128, or 256 bit keys; & SHA-2 (256, 384, or 512 bit) signature.

4. Certificate Signing

PAM360 provides the option to sign and issue certificates to all clients in your network either from your Microsoft Certificate Authority or using a custom root CA certificate that is trusted within your environment.

To request and acquire certificates from Local CA from PAM360, you have to initially generate a CSR, then get it signed from the local certificate authority using the steps mentioned below. There are three ways to sign your certificates:

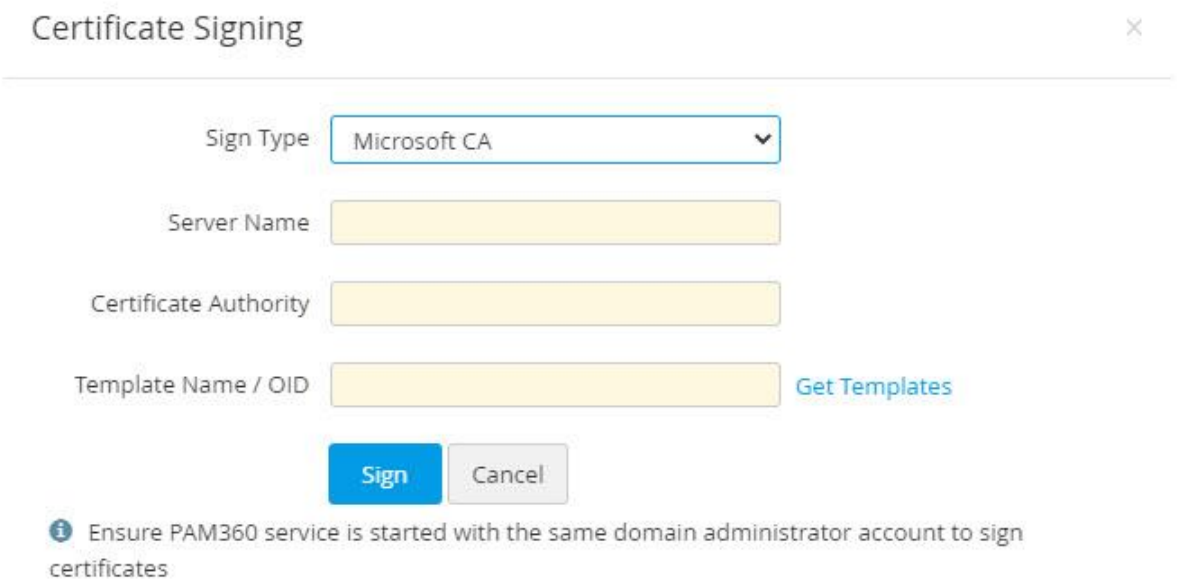
1. MS Certificate Authority
2. MS CA with agent
3. Sign with Root

Navigate to **Certificates >> CSR.**

4.1 Microsoft Certificate Authority

You can get the CSR signed from Microsoft Certificate Authority from PAM360.

1. Select the required CSR and click **Sign** from the top menu.
2. In the pop-up that opens, select the **Sign Type** as **Microsoft Certificate Authority.**
3. Mention the **Server Name** that runs the internal CA and also the **Certificate Authority** name.
4. Select the **Certificate Template** based on your requirement or select any of the pre-defined templates by clicking the **Get Template** link and click **Sign**.



The CSR is signed and the issued certificate can be viewed from **Certificates >> Certificates.**

Notes:

1. Start PAM360 using your domain administrator account to begin management of certificates from Microsoft Certificate Store and those issued by your Local CA. If you use a domain service account to run PAM360, make sure that you have configured it in your local admin group beforehand.
2. During MS Certificate Store discovery, **Get Stores** option will list all stores available in the local host if the **Server Name** field is left empty.
3. For MS CA auto-renewal to take effect, the certificate(s) need to be of type **Microsoft CA.** For manually added certificates, the certificate type needs to be changed to **Microsoft CA** using **Edit** option from **More** top menu.

4.2 Microsoft CA with Agent

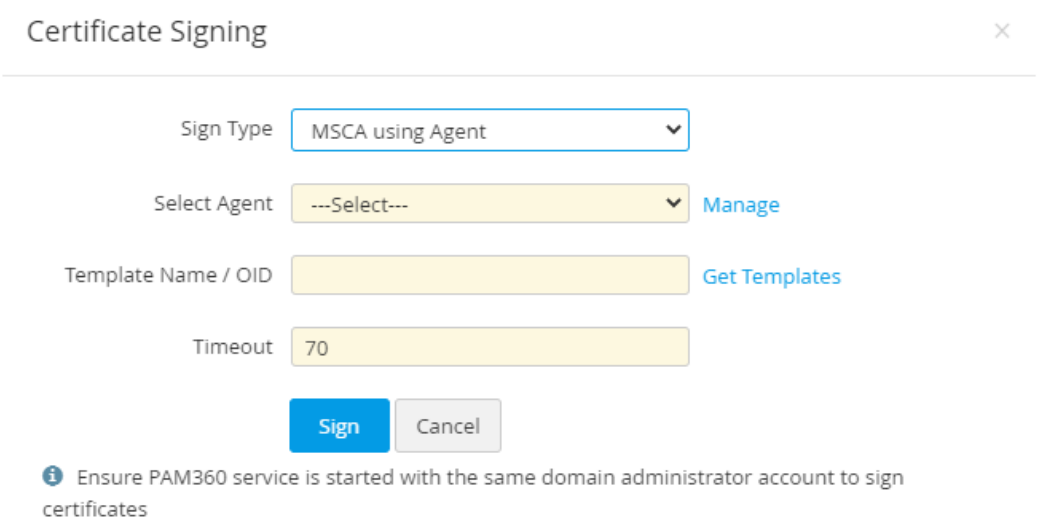
1. Select the required CSR from the list view and click **Sign** from the top menu.
2. In the pop-up that appears,
   i. Select the **Sign Type** as **Microsoft CA with Agent.**
   ii. **Select theAgent** from the list available in the drop-down. You can also **Manage** the agent by referring to section 1.5. To know more about agents, refer to **section 1.5 -**

Discover SSL certificates using the Key Manager Plus (KMP) Agent in this topic.

iii. Specify the **Certificate Template** or click Get Template to get new templates.

iv. Mention the agent **Time out** in seconds within which the agent should respond. If the agent doesn't respond within the timeout period, the operation will be audited as failed.

v. Click **Sign**.



The CSR is signed and the issued certificate can be viewed from **Certificates >> Certificates.**

4.3 Sign with Root

PAM360 provides the option to sign and issue certificates to all clients in your network either from your Microsoft Certificate Authority or using a custom root CA certificate that is trusted within your environment.

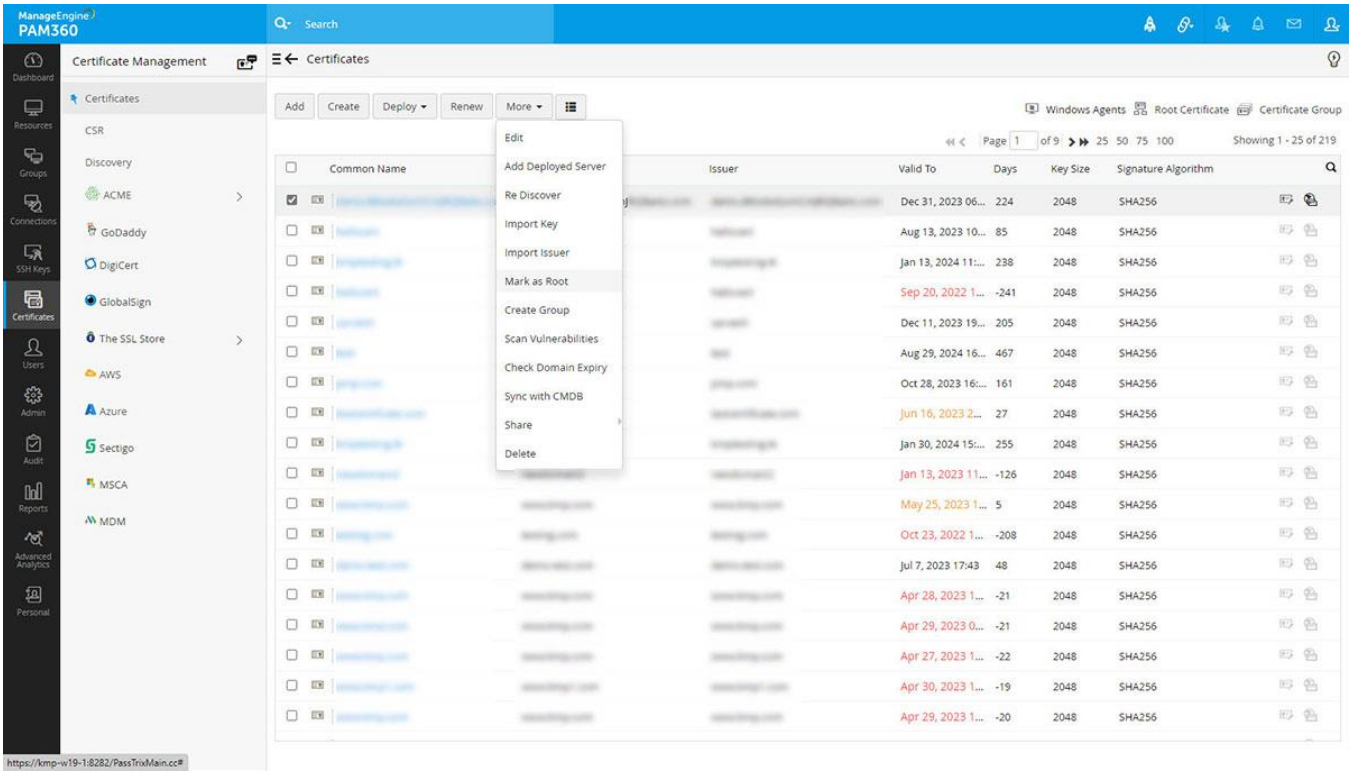
1. Create a custom root CA
2. Sign certificates with the custom root CA
3. Deploy the signed certificates to target systems

4.3.1 Create a custom root CA

To sign locally generated certificate requests with the root CA certificate, you have to initially create a custom root CA.

1. Navigate to **Certificates >> Certificates** tab.
2. Select a certificate and click **More >> Mark as Root** from the top menu.

The chosen certificate is successfully denominated as a root CA certificate and is listed under the **Root Certificate** tab. You can then use this certificate to sign locally generated certificate requests.



Note: You can also generate new root CA certificates from PAM360 by enabling **Generate root certificate** check-box while creating a certificate from **Certificates >> Certificates >> Create.**

4.3.2 Sign certificates with the custom root CA

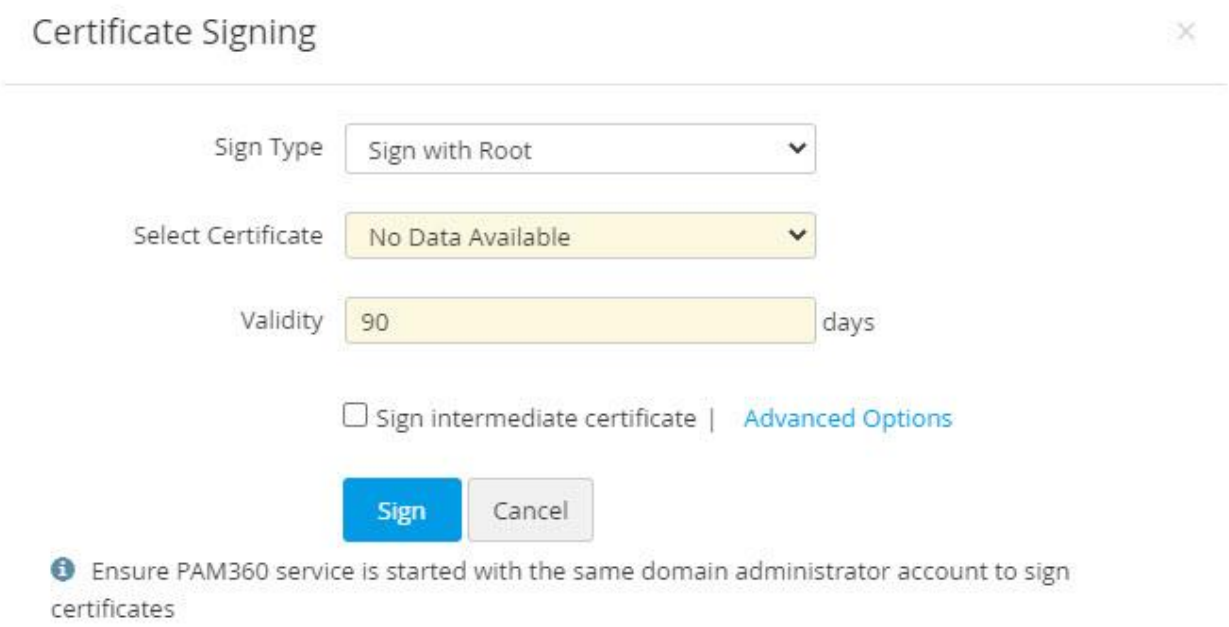
To sign certificates with the custom root CA, generate a certificate signing request (CSR) and then sign it using the root certificate.

1. Select the CSR and click **Sign** from the top menu.
2. Select the **Sign Type** as **Sign with Root.**
3. Select the **Root Certificate** and specify the **Validity** in days. Click **Sign**.
4. Select checkbox to **Sign intermediate certificate**. This allows users to sign the certificate on behalf of Root CA.
5. To add optional properties to the new certificate, click **Advanced Options** to expand the

menu. Here, there are two categories of options, **Key Usage** and **Extended Key Usage**. Select the required options to set the preferred flags for the certificate to denote the purpose for which the new certificate may be used. The **Key Usage** options include Non Repudiation, Digital Signature, Data or Key Encipherment, Server/Client Authentication etc. You can choose the properties and mark them as critical by selecting the **Critical** checkbox.

6. Click **Sign**.

The certificate is signed based on the selected root certificate and is listed under **Certificates >> Certificates** tab.



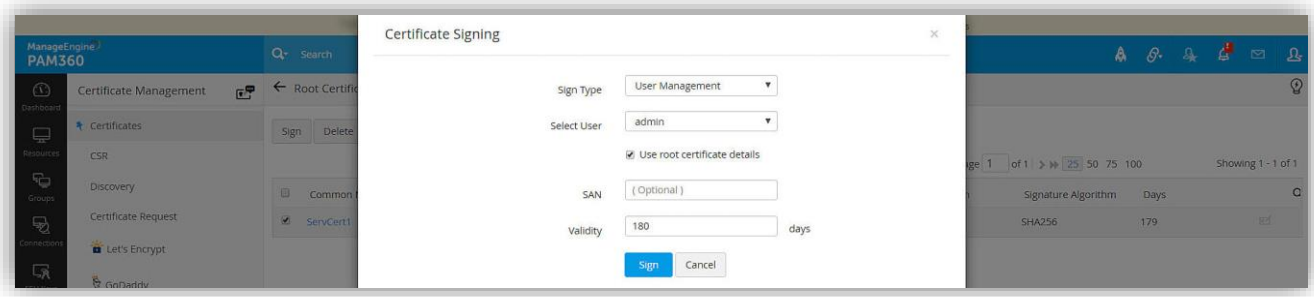
Also, you can use the root CA certificate to simultaneously generate and sign certificates to user groups in bulk directly from PAM360.

1. Navigate to **Certificate** and click **Root Certificate** on top right corner of the window.
2. Select the required root CA certificate and click **Sign.** In the pop-up that opens, choose the sign type, user / user groups to which certificates have to be created and deployed, mention the SAN and validity (in days).
3. The sign type **User Management** allows you to generate and sign certificates for user accounts in PAM360.
    i. Select the user account for which you need to generate a certificate.
    ii. By default, the user certificates inherit the same parameters as that of the root certificate. You can change it by unselecting the **Use root certificate details**

option.

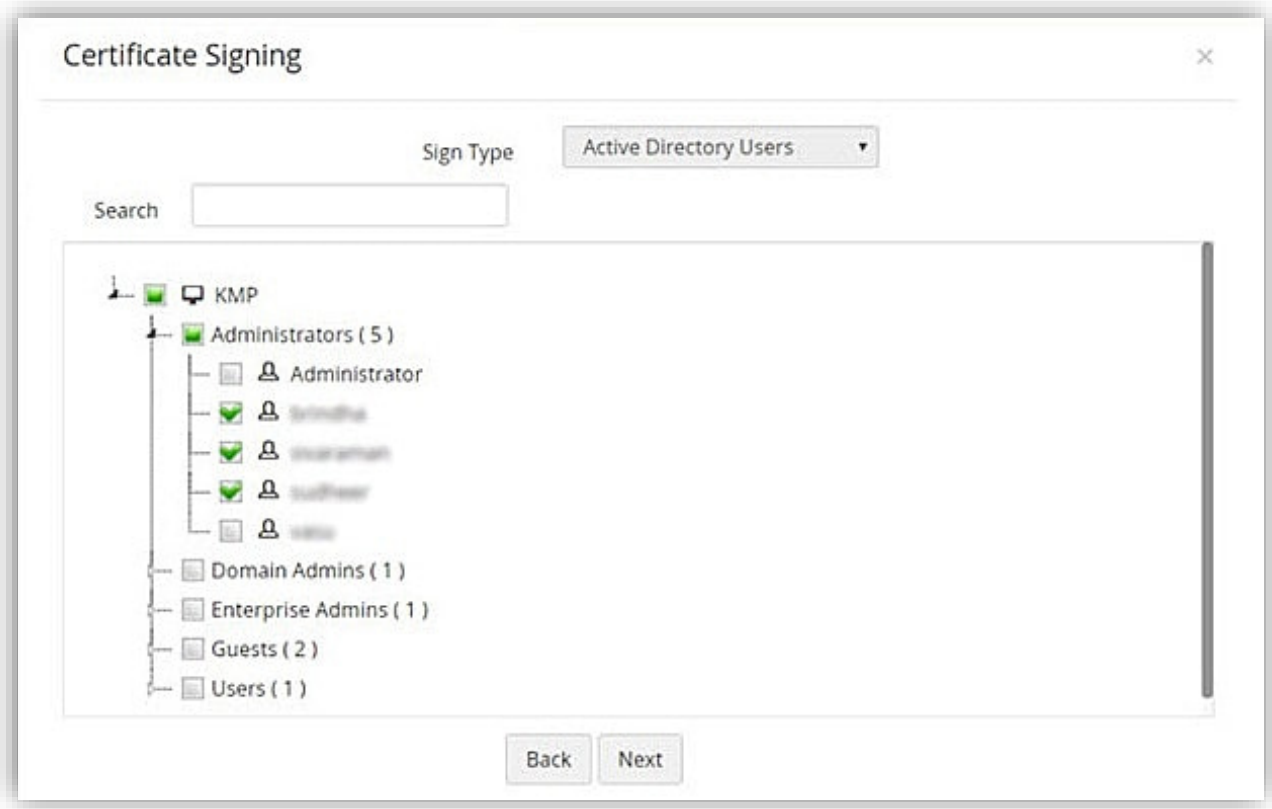
iii. After filling in the details, click **Sign.**

The certificate is signed and you can find listed in PAM360's certificate repository.



The sign type **Active Directory Users** allows you to generate and sign certificates to user accounts mapped to the Active Directory within your network environment.

1. Select the **Domain Name** and provide the primary domain controller address, username and password.
2. Choose import type **Single** and specify the user groups or use **Groups/OU tree** import type to choose the users or user groups for which certificates need to be created.
3. After selecting the users, enter the certificate validity in days. By default, the user certificates inherit the same parameters as that of the root certificate. You can change it by unselecting the **Use root certificate details** option.
4. After filling in the details click **Sign.**
5. This will generate certificates for the selected users which will be listed in PAM360' certificate repository.



4.3.3 Deploy the signed certificate to target systems

After signing the certificate requests and obtaining the certificate, you have to deploy them to the necessary end-servers. Refer to this section of help for step-by-step explanation on certificate deployment.

> **Note:** When signing certificates with custom root CA for web-applications, make sure all the browsers in your network are configured to trust the root CA certificate in order to avoid security error messages.

5. Import and Export Certificates

5.1 Allowed Certificate Types

PAM360 allows you to import and export the following certificate types:

- .cer
- .crt
- .pem
- .der

- .p7b
- .pfx
- .p12
- .pkcs12
- .jks
- .keystore

5.2 Steps to Import the Certificates in your Network

In addition to certificate discovery, PAM360 provides a few other ways in which you can manually add SSL certificates into the repository. To do so, follow the below steps:

1. Navigate to the **SSL >> Certificates** tab and click the **Add** button.
2. The **Add Certificate** window displays the following options:
   i. **Certificates** – Browse and import the required certificate file directly from your system.
   ii. **Certificate Content** – Copy the content of the required certificate file and paste it in the text box.
   iii. **Keystore Based** – Import all individual certificates available in a Keystore simultaneously. Upload the required Keystore file and enter its corresponding password (if any).
   iv. **Certificate Details** – Browse and import the .csv file with the required certificate details.
3. Click **Add**. The certificates or certificate details will be imported to the PAM360 repository.

5.3 Steps to Import Issuer Certificates

PAM360 allows you to import issuer certificates into the repository and build a complete certificate chain in the product.

1. Navigate to **Certificates >> Certificates**. Select the required end certificate.
2. Under the **More** dropdown, select Import Issuer.
3. In the pop-up that appears, **Browse** and add the issuer certificate andh click **Import**.
4. The additional issuer certificates you add will be appended to the existing SSL certificate in the repository based on the issuer name. To download the complete chain with the private key, export the certificate in **JKS**, **PKCS**, or **PEM** formats.

5.4 Steps to Export the Certificates in your Network

1. Navigate to **Certificates >> Certificates.**
2. In the list view, click the certificate you want to export.
3. In the certificate details window, click **Export** on the top right corner and select the required format in the which you want to export the certificate.
4. The certificate will be downloaded to your machine in the selected format.

6. Certificate Renewal

The **Certificates** tab in PAM360 is a centralized console where all types of SSL certificates such as Self Signed, Root Signed, Microsoft CA Signed, certificates issued by third-party CAs etc., are consolidated and displayed. Through the **Renew** option, these certificate types can be renewed in the **Certificates** tab directly. These renewed certificates will automatically inherit the deployed servers and their credentials. For certificates issued by third-party CAs, the renewal will be initiated and redirected to the respective CA's tab. To proceed further, follow the below steps:

1. Navigate to **Certificates >> Certificates**.
2. There are three types of certificate renewal:
    i. Self Signed certificate renewal
    ii. Root Signed certificate renewal
    iii. Microsoft CA Signed/Signed with Agent certificate renewal

i. Self Signed Certificate Renewal

To renew a Self Signed certificate, follow the below steps:

1. Select a Self Signed certificate and click **Renew** at the top.
2. The renewal type will be **Self Signed** by default.
3. Specify the number of days for which the certificate shall be valid in the **Validity** field. Click **Renew**.

The certificate will be renewed successfully and the **Valid To** date will change according to the new validity period specified.

ii. Root Signed Certificate Renewal

To renew a Root Signed certificate, follow the below steps:

1. Select a Root Signed certificate and click **Renew** at the top.
2. The renewal type will be **Renew with Root** by default and the **Issuer** name will be autopopulated in the **Root Name** field.
3. Specify the number of days for which the certificate shall be valid in the **Validity** field. Click **Renew**.

The certificate will be renewed successfully and the **Valid To** date will change according to the new validity period specified.

iii. Microsoft CA Signed/Signed with Agent Certificate Renewal

To renew a Microsoft CA signed certificate, follow the below steps:

1. Select a Microsoft CA Signed certificate and click **Renew** at the top.
2. If the certificate does not have a private key, PAM360 allows you to create a new private key. Click **OK** in the pop-up that appears.
3. Attributes such as **Renewal Type**, **Server Name**, **Template Name / OID**, **Certificate Authority** will be autopopulated from the certificate details. The **Server Name** is the name of the Microsoft CA server which signed the certificate. Certificate Authority is the CA service that runs in the specified Microsoft CA server.
4. For certificates signed by Microsoft CA directly or using the KMP agent, validity days will be taken from the Microsoft CA server and therefore it cannot be entered manually during renewal. These type of certificates will be renewed only till the date specified in the the Microsoft CA server.

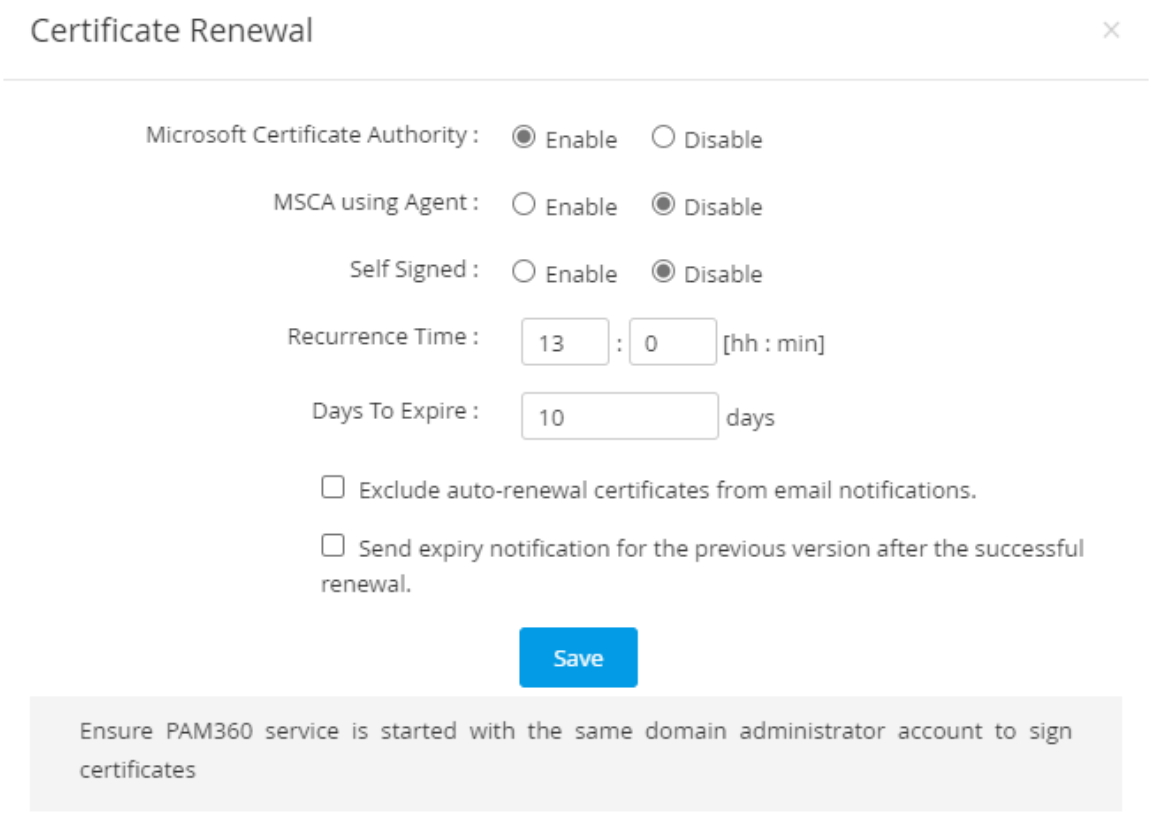
In addition to the above types, third-party CA signed certificates can also be renewed using this renewal option. Follow the same procedure to initiate renewal and PAM360 will redirect the renewal request to the respective third-party CA. Follow the steps detailed in the next section to learn how to set up auto-renewal for certificates in PAM360.

6.1 Auto Renewal

Certificates issued by Local CA can be renewed automatically from the **Admin** page in PAM360.

To enable auto-renewal of Local CA certificates, follow the below steps:

1. Navigate to **Admin >> SSL Certificates >> Certificate Renewal.**
2. Enable **Microsoft Certificate Authority, MSCA using Agent** or **Self Signed** and specify the **Recurrence Time**.
3. Certificates that have already expired and certificates due to expiry in 10 days or less are automatically renewed and updated in the certificate repository.
4. The certificates that are due to expire in the number of days mentioned in the **Days to Expire** field will also be auto-renewed.
5. Select the checkbox to **Exclude auto-renewal certificates from email notifications**. This allows the certificates marked for auto-renewal to be excluded from the email notifications even if they fall under the expiry notification configuration.
6. Select the checkbox to **Send Expiry Notification for the Previous version after successful Renewal**.
7. Click **Save**.
8. After successful auto-renewal, the previous version of the certificate will be listed under **Certificate History**.



Notes:

- During the renewal process, a CSR will be generated from the available values, along with a new Private Key.
- SHA1 certificates will be renewed using the SHA256 algorithm.

7. Certificate History

PAM360 allows you to group the certificates under a common name. To enable this,

1. Navigate to Admin >> SSL Certificates >> Certificate History.
2. Choose Enable or Disable the Group Certificates by CommonName option.
3. Enabling the option will group the certificates under one Common Name.
4. Disabling this option will create new certificates based on the unique Serial Numbers assigned to the certificates.
5. To view these certificates, navigate to Certificates >> Certificates and enable Certificate History from column chooser.
6. Now, click the certificate history icon corresponding to the required certificate to view the certificates.

Note: On certificate renewal, the older version of the renewed certificate will be moved to Certificate History.

8. Certificates Sync Status

PAM360 allows users to perform periodic and automatic checks on the synchronization status on the SSL certificates deployed to multiple servers.

When enabled, PAM360 gives you options to check for out-of-sync servers and delete the servers in which there is a certificate mismatch. Follow the below steps to enable certificate sync status check:

1. Navigate to **Admin >> SSL Certificates >> Certificates Sync Status**.
2. Click **Enable** and enter a recurrence time interval in hours or minutes.
   i. **Check only the Non-Sync servers** - select this option to check and consolidate only the out-of-sync servers.

ii. **Delete the server if Non-Sync** - select this option to delete the servers that are found to have a certificate mismatch after the synchronization check.

3. Click **Disable** to stop the synchronization check.

9. Edit and Delete Certificates

9.1 Steps to Edit a Certificate from PAM360 Repository

To edit a certificate from PAM360 repository:

1. Navigate to the **Certificates >> Certificates.**
2. Select the certificate to be edited, click **More** and select **Edit** from the dropdown.
3. In the Edit Certificate pop-up that appears, edit the **DNS Name, Port, Description, Expiry Notification Email,** and **Type.**
4. You can choose to **Deploy Certificate on Auto Renewal.**
5. Click **Save.**

> **Note:** You will be able to deploy certificate to all servers on auto renewal only if the user credentials are available.

9.2 Steps to Delete a Certificate from PAM360 Repository

You can delete the certificates that are currently not in use. To delete a certificate from PAM360 repository:

1. Navigate to the **Certificates >> Certificates.**
2. Select the certificates.
3. Click **More** and select **Delete** from the dropdown.
4. In the pop-up that appears, select the checkbox to **Add selected certificates to 'Excluded certificates'** and mention the **Reason.**
5. Click **OK** in the pop-up that appears.

10. Certificate Requests

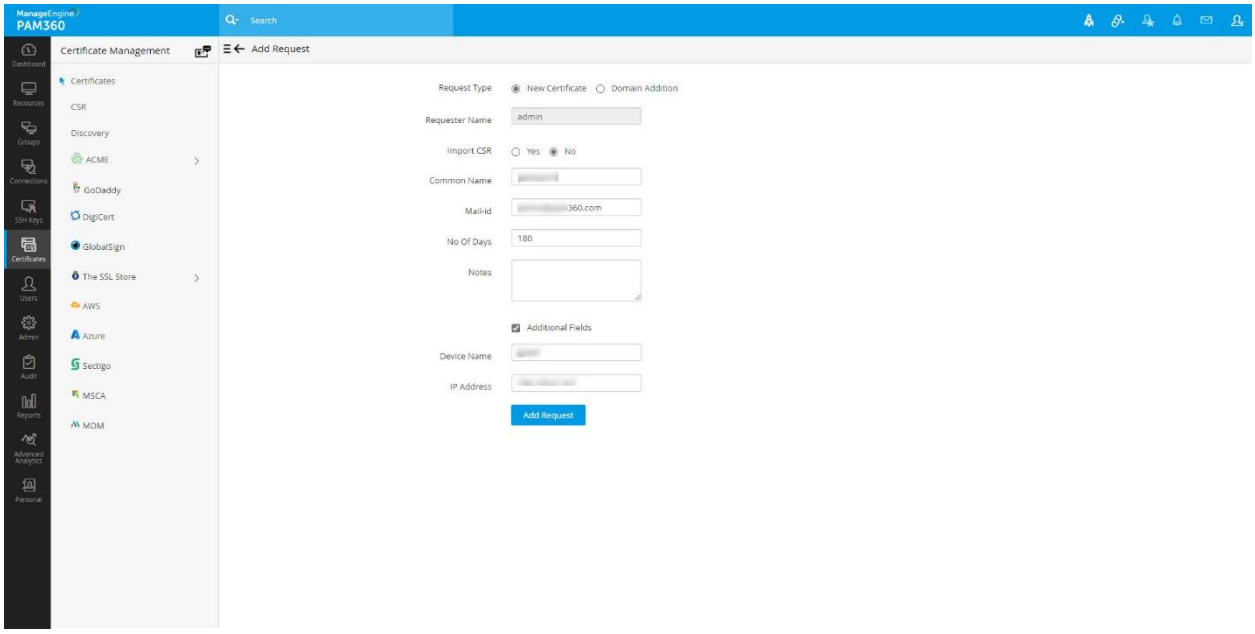
The certificate request workflow is as follows:

1. Add certificate request
2. Close certificate request

10.1 Add Certificate Request

To add requests for new certificates or addition of sub-domains to existing certificates, in PAM360:

1. Navigate to the **Certificates >> Certificate request.**
2. Click the **Add Request** button.
3. Select the type of request – New Certificate or domain addition.
    i. **New Certificate** – Attach a CSR to your request (optional) and a domain name for the new certificate.
    ii. **Add Domain** – Enter the name of the new domain and select a parent domain from the certificates added to the PAM360 repository.
4. Enter the mail addresses to which you would like to send the request and specify the certificate validity period. These mail addresses can be that of an administrator, an intermediary who handles certificate requests, or even your help desk software to raise the certificate request as a ticket.
5. Click Additional fields to add additional information such as device name and IP address
6. Click the Add Request button to add it to the list of request in the Certificate Request tab and to send the same to the specified email addresses.



10.2 Certificate Request Status

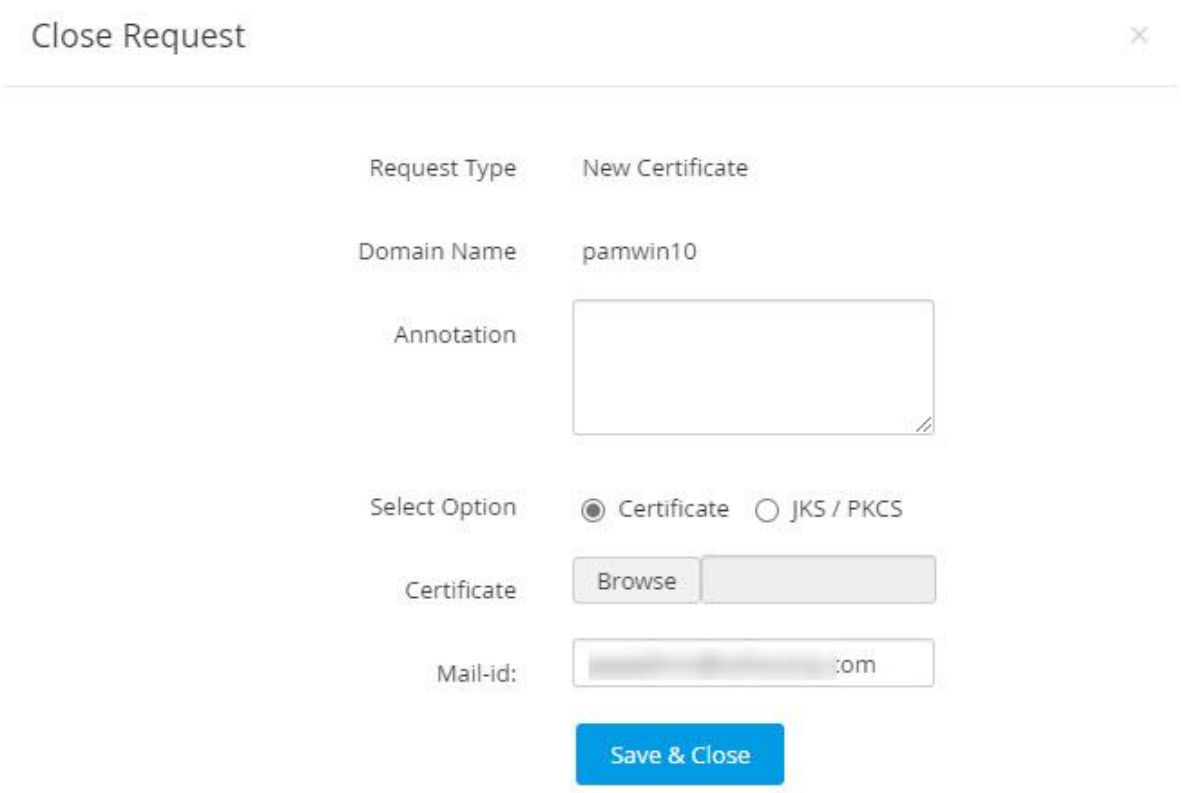
A certificate request is in either of the following statuses.

1. Open
2. Closed

When a certificate request is raised, it is automatically elevated to the Open state. The request details can be viewed from **Certificates >> Certificate Request**, on clicking the domain name of the request.

10.3 Terminate the Certificate Request Life-cycle

1. Navigate to the **Certificates >> Certificate Request**.
2. Click the Open status link in the right corner of the table against the required open request process.
3. In the Close Request window, add an optional annotation, and attach the certificate issued (optional), specify the e-mail ids of users to whom the certificate is to be sent and click the Save & Close button. Once you click the button, the request is automatically moved to the Closed state.
4. If a SSL certificate is attached while closing the request, the certificate is automatically imported to the PAM360 repository.
5. Also, the issued certificate is e-mailed to the user who raises the request, the user who closes the request and also to those e-mail ids specified at the time of closing the request.



11. Control Expiry Notification Schedule

You can customize the periodicity of notifications you receive when a certificate is about to expire. To customize the notifications:

1. Navigate to the **Admin >> SSH/SSL Config >> Notification Settings.**
2. Select the **Notify about SSL certificates are expiring within** checkbox and the number of days before the expiry of certificate within which you should start receiving notifications.
3. Select the **Email** or **Syslog** checkbox and enter appropriate details. To know more about configuring notifications, click here.
4. Click **Save**.

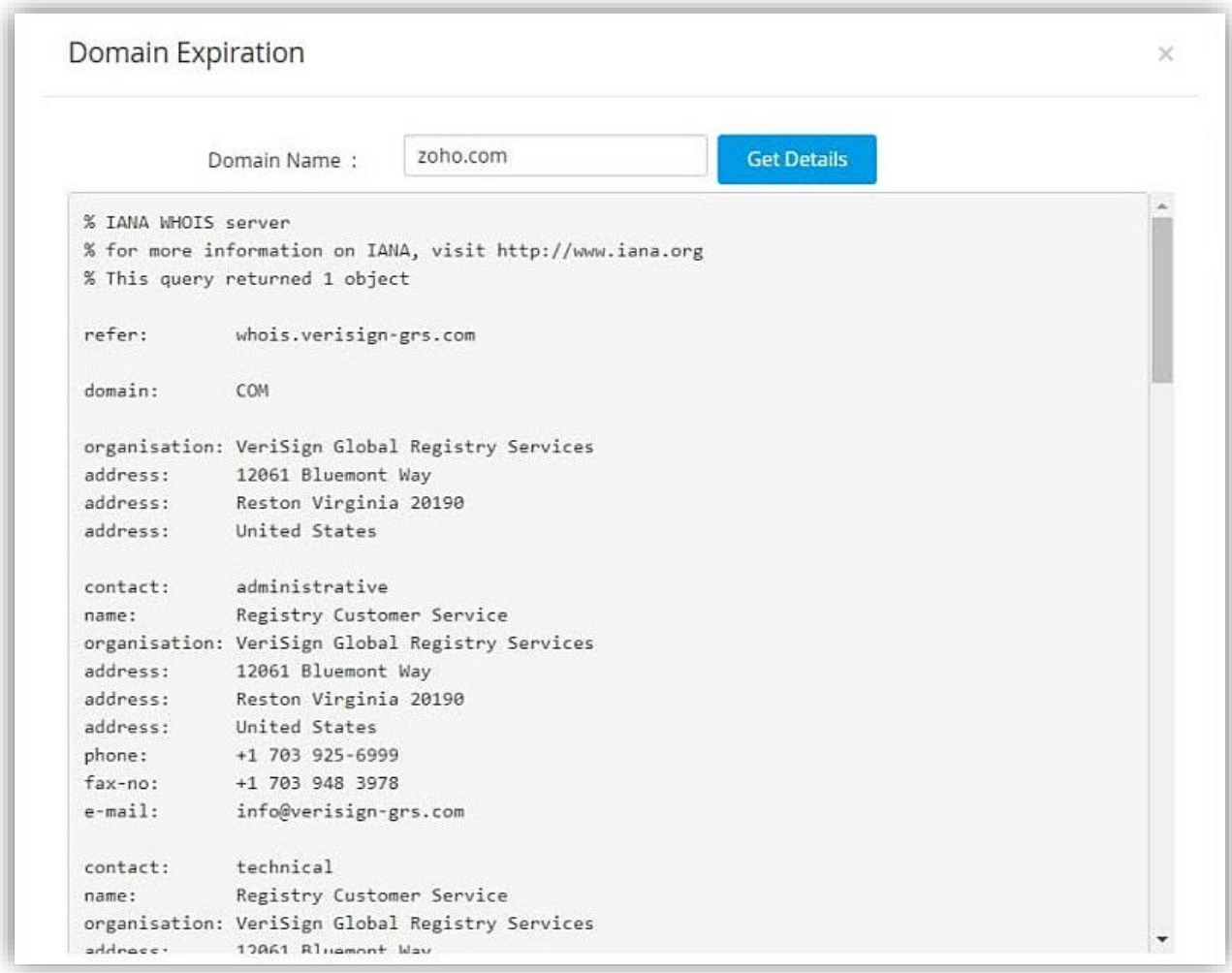
Note: You will receive notifications every day after the selected date before the expiry of a certificate. For instance, if a certificate is about to expire in the last week of a month, and you select the Notify if SSL certificates are expiring within 7 days option, then, you will receive a notification that your certificate is about to expire every day of the week before the expiry of the certificate.

12. Track Domain Expiration through WHOIS Lookup

Apart from tracking certificate expiration, PAM360 also helps administrators keep a tab on their expiring domain names through an automated WHOIS look up. The domain expiration details fetched through the lookup are displayed in **Certificates >> Certificates** tab against its corresponding SSL certificate. Also, administrators can choose to receive timely email notifications of their expiring domains by configuring it under **Admin >> SSH/SSL Config >> Notification**.

12.1 How does the WHOIS lookup work?

Fetching domain expiration details requires a two-stage lookup to WHOIS servers from PAM360. The first lookup provides the details of the WHOIS server with which the domain was registered by its domain registrar. The second lookup provides information about the domain such as owner details, expiration date etc., All these operations are automated the from PAM360's interface.



Note: Connection to WHOIS servers requires the use of **Port 43.** Ensure that port 43 is open in your environment, else the connection would fail and **Domain Expiration** will be marked Not Available (NA) in the **Certificates** tab.

13. SSL Certificate Group

PAM360 allows you to organize SSL certificates into various logical groups and execute actions in bulk on the groups.

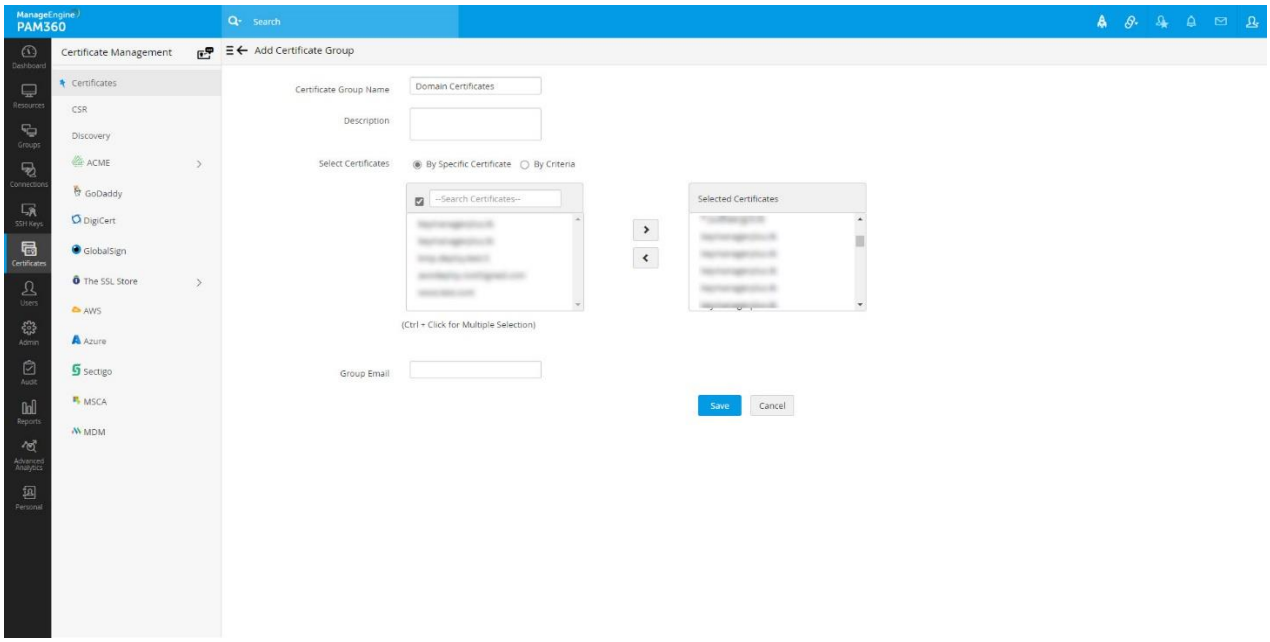
13.1 Create Certificate Groups

To create a certificate group,

1. Click the **Certificate Group** icon in the top-right corner of the **Certificates** tab.
2. Click **Add Group.** You will be directed to the **Add Certificate Group** page.

3. Provide a name for the certificate group and an optional description. Exercise caution while providing the name since it cannot be changed later.
4. You can choose certificates to be added to a group in either of the following ways:
   i. **By Specific Certificate** - Select the certificates to be added to the group individually and click **Save**.
   ii. **By Criteria** - This serves as a dynamic method of grouping certificates. You will specify various criteria based on which the group will be created. Here, you can choose certificates based on various criteria such as issuer, common name, key algorithm, key size, key length etc. The additional fields that are added will also be displayed in the list. You can filter the search in a fine-grained manner based on conditions such as **equals** or **does not equal**, **contains** or **does not contain**, **starts with** or **ends with**. Click the **Matching Certificates** button at the bottom-right corner to see the corresponding certificates. Click **Save**. The certificate group is created.
5. Mention the Group Email address to send expiry notifications and click **Save.**
6. The certificate group is created. To know more about additional fields, click here.

> **Note:** If you choose to group certificates based on criteria, the conditions will be applied to certificates discovered in the future and they will automatically be added to groups that match the criteria.



13.2 Edit Certificate Groups

To make changes to existing certificate groups,

1. Click the **Certificate Group** icon on the top-right corner **Certificates** tab.
2. Click the edit icon present in the right corner of the table view.
3. You can change the certificate selection type, edit the certificates present in a group or add, modify or delete the filters applied to a group.
4. Once you update the changes and save them, a pop up message will be displayed confirming the updates.

> **Note:** The certificate group name cannot be modified. However, you can add or modify the list of certificates in a group or the description.

13.3 Delete Certificate Groups

To delete a certificate group,

1. Click the **Certificate Group** icon on the top-right corner of the **Certificates** tab.
2. Select the groups that you want to delete and click **Delete.**
3. A pop-up window will appear asking you to confirm the action. Click **OK** and the selected certificate groups will be deleted.

Integration with Trusted Public Certificate Authorities

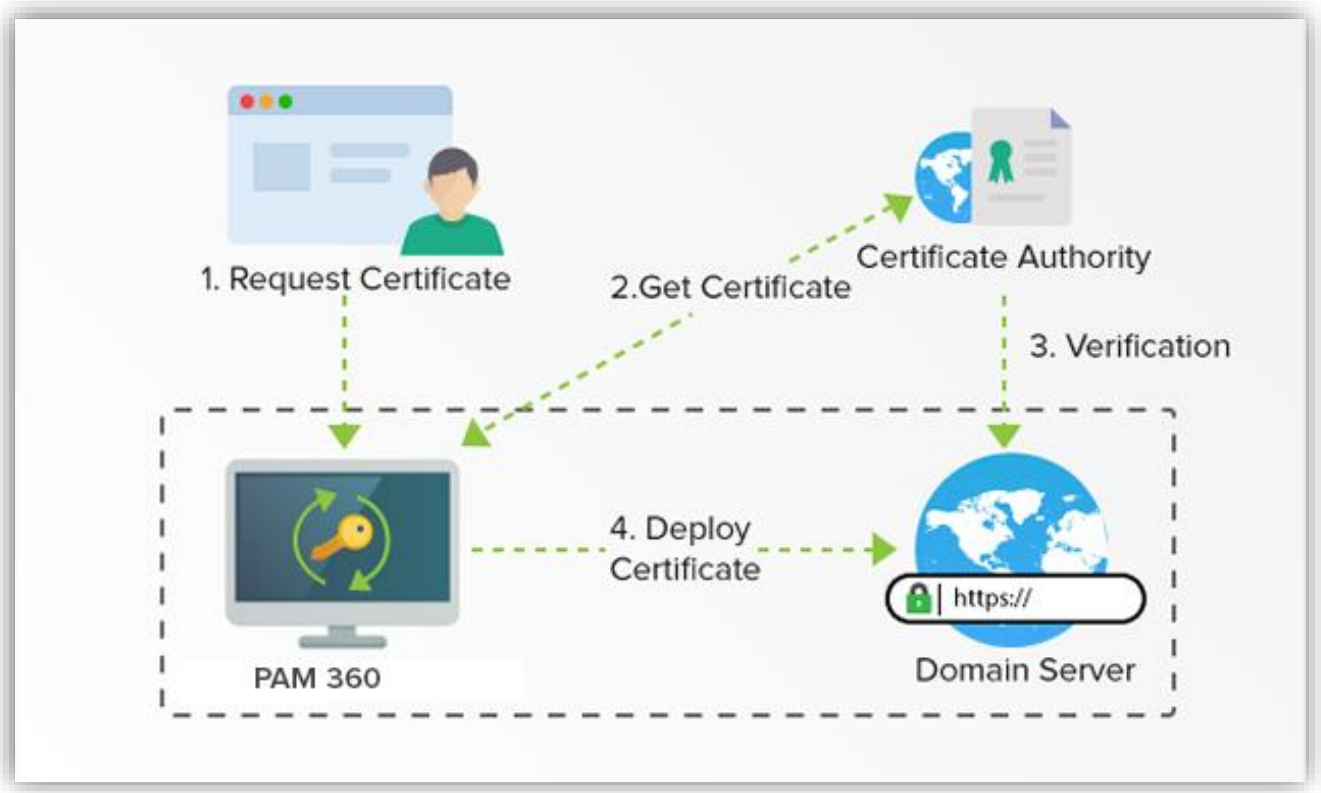
PAM360 facilitates end-to-end life cycle management of certificates issued by public certificate authorities. This functionality, powered through seamless API integration with third-party certificate authorities, allows administrators to request, acquire, consolidate, deploy, renew, and track the life cycles of certificates in a centralized fashion directly from the PAM360's web interface. PAM360 currently supports the complete life cycle management of certificates issued by the following certificate authorities: **Let's Encrypt, GoDaddy, Thawte, Symantec, RapidSSL, Geotrust, Sectigo (formerly Comodo CA), DigiCert, GlobalSign.**

> **Note:** While PAM360 leverages the open APIs of **Let's Encrypt** and **GoDaddy** to establish a connection, the tie-in with rest of the certificate authorities is powered through an integration with **The SSL Store™**, a platinum partner of the above mentioned certificate authorities.

Click the below links for the step-by-step description of the end-to-end certificate life cycle management of the relevant public certificate authority.

- **Let's Encrypt**
- **GoDaddy**
- **The SSL Store™** (Thawte, Symantec, RapidSSL, Geotrust, Sectigo [formerly Comodo CA])
- **DigiCert**
- **GlobalSign**
- **Buypass Go SSL**
- **ZeroSSL**

The flow diagram below gives a quick overview of how the integration works and the necessary steps to acquire and manage the certificates issued by the public certificate authorities using PAM360.



1. **Request**

   Raise requests for certificates from public certificate authorities using the built-in CSR generation tool.

2. **Forward**

   Forward the request to the certificate authority for domain verification.

3. **Validate**

   Complete the domain control validation procedure. Acquire and import the issued certificates to PAM360's certificate repository.

4. **Deploy**

   Deploy the certificates to their corresponding end-servers.

Integrating PAM360 with Let's Encrypt SSL Certificate Authority

1. Overview
2. Creating a Let's Encrypt account
3. Raising a certificate request
   3.1 Configuring the DNS account
4. Let's Encrypt challenge verification
   4.1 Domain Validation Through HTTP-01 Challenge Verification
   4.2 Domain Validation Through DNS-01 Challenge Verification
5. Procuring and saving the certificate
6. Renewing certificates
   6.1 Automatic renewals through automatic domain validation
7. Revoking certificates
8. Deleting certificates
9. About Let's Encrypt

1. Overview

Maintaining a threat-free network requires much more than just securing your domains with SSL certificates. For organizations that deal with a large SSL environment, the process of purchasing, deploying and renewing SSL certificates often proves to be cumbersome, time-consuming and has hardly been straightforward. Oversight, manual errors, improper configuration, weak ciphers, and expiration often lead to downtimes, compliance issues and security breaches. Certificate life-cycle management is a practice that streamlines the certificate management process by automating acquisition, issue, deployment, re-issue, renewal and revoking of certificates. PAM360 facilitates end-to-end certificate life-cycle management for your public facing websites by integrating with the renowned open Certificate Authority, Let's Encrypt. This means you can procure domain validated certificates from Let's Encrypt for your public domains, deploy, track, request alerts on expiry, renew certificates; everything done entirely from the product interface.

You can request, procure, deploy, monitor, track and renew certificates from Let's Encrypt CA directly from PAM360 interface.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to Let's Encrypt's CA Services.

Production URL: https://acme-v02.api.letsencrypt.org/directory

Staging URL: https://acme-staging-v02.api.letsencrypt.org/directory

Port: 443

Follow the step-by-step procedure below to integrate Let's Encrypt with PAM360:

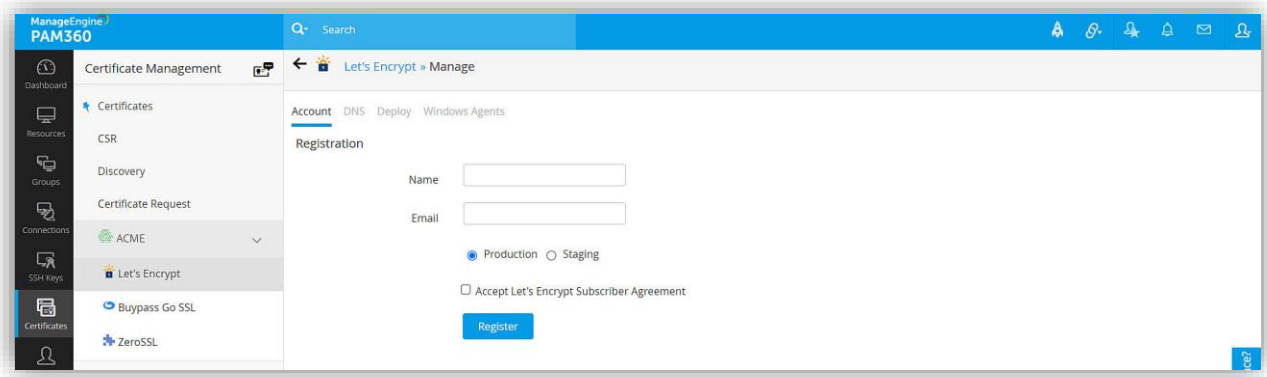
2. Creating a Let's Encrypt Account

The first step in requesting for certificates from Let's Encrypt CA is creating an account with Let's Encrypt. This is a one-time process and can be done from PAM360 interface itself.

To create Let's Encrypt account,

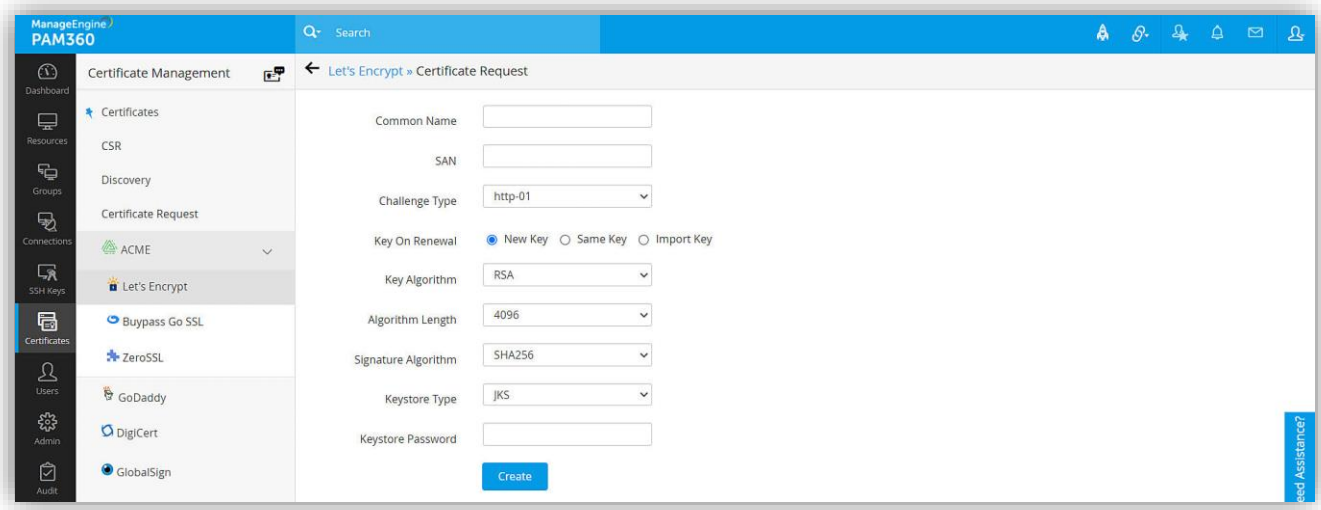
1. Navigate to **Certificates >> Let's Encrypt >> Manage.**
2. Under **Account** tab, click **New Registration.**
3. In the UI that opens, provide an account name and specify a valid email address. Choose **Production** or **Staging**, based on your requirement.
4. Accept the Let's Encrypt Subscriber Agreement by enabling the checkbox.
5. Click **Register**.
6. An account with Let's Encrypt is created.

Note: This privilege is available for only the administrator users and only one Let's Encrypt account can be created from PAM360.



3. Raising a Certificate Request

After creating an account with Let's Encrypt, you have to generate a certificate request. You are then presented with a challenge which you have to fulfill for Let's Encrypt to validate your domain and issue the certificate.



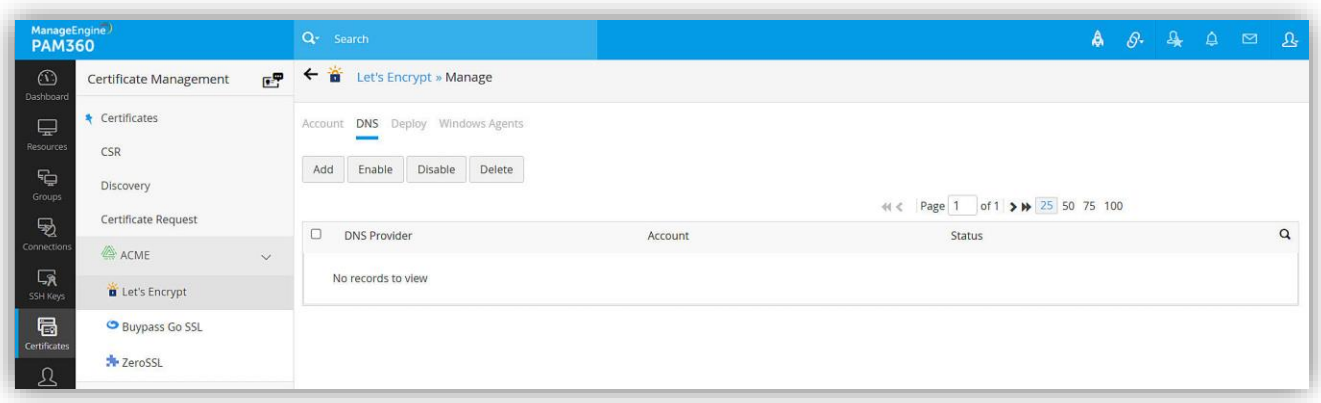
1. Navigate to **Certificate >> Let's Encrypt >> Certificate Request.**
2. Fill in the domain name, choose the **Key Algorithm**, **Algorithm Length**, **Signature Algorithm**, **Keystore Type**, enter the **Keystore Password** and click **Create**.
3. For dns-01 challenge type, you can choose and assign a **DNS** account from the dropdown if you have already configured your DNS credentials. This will be used for automatic challenge verification for all the domains specified in the request.
4. Also, you have options to change the private key whenever the certificate is renewed.
    - If you need to change the key, use **New Key.** This option will generate a new key every

time the certificate is renewed.

- If you want to retain the same key on renewal, use the **Same Key** option.
- To use your own key, use the **Import Key** option. This key will be used for the first time when the certificate is generated and also for subsequent renewals.

3.1 Configuring the DNS Account

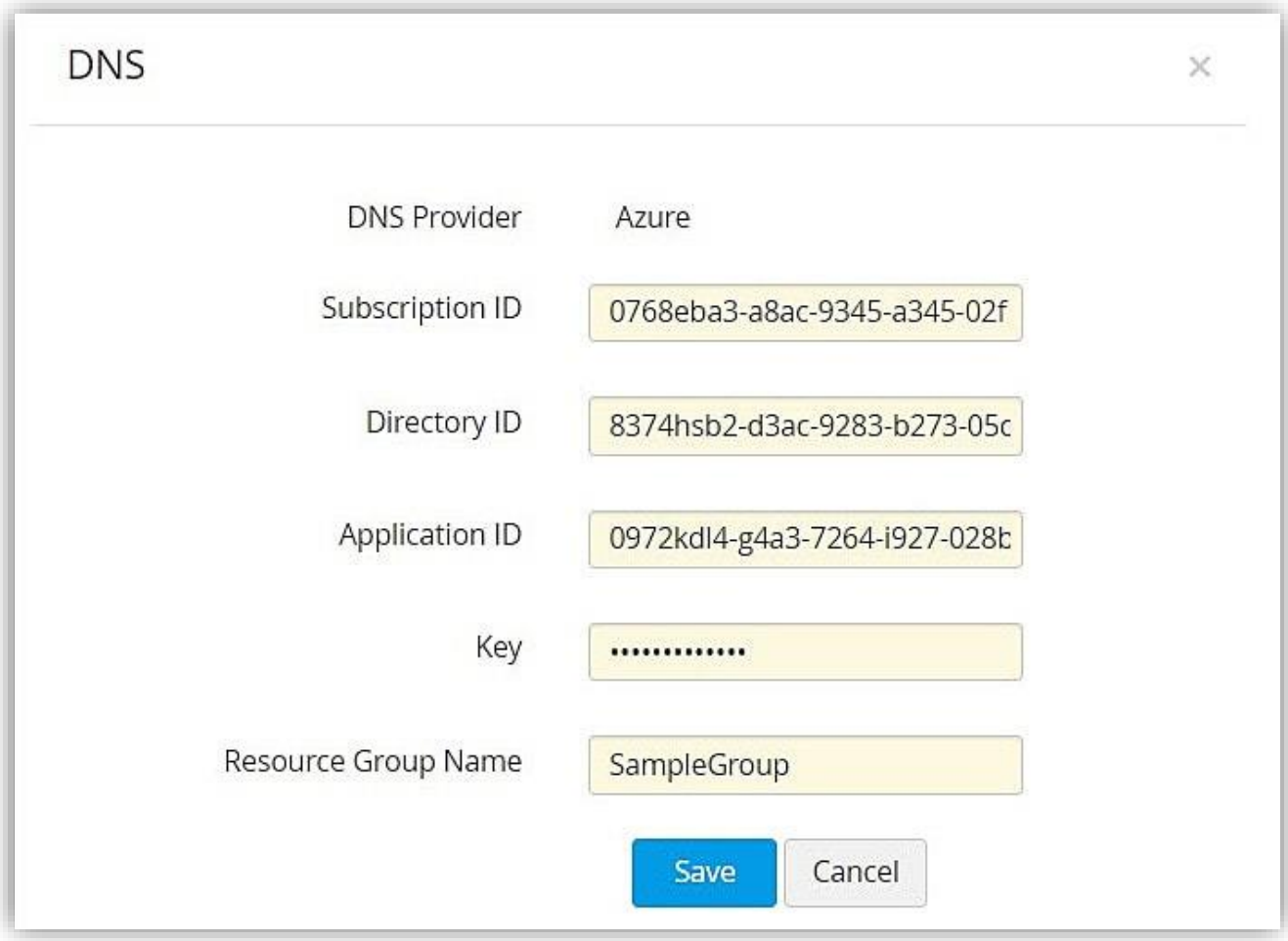
1. Navigate to **Let's Encrypt >> Manage.**
2. Switch to the **DNS** tab.



3. Here, you can add a maximum of one DNS account for each DNS provider supported. PAM360 currently supports automatic challenge verification for Azure, Cloudflare DNS, Amazon route 53 DNS, RFC2136 DNS update (nsupdate), GoDaddy DNS, ClouDNS.
4. Click **Add.** In the pop-up that opens, choose the DNS provider.

3.1.1 For Azure DNS

1. Provide the **Subscription ID,** which is available in the **Overview** page of the **Azure DNS zone.**
2. Provide the **Directory ID,** which is available in **Azure Active Directory >> Properties.**

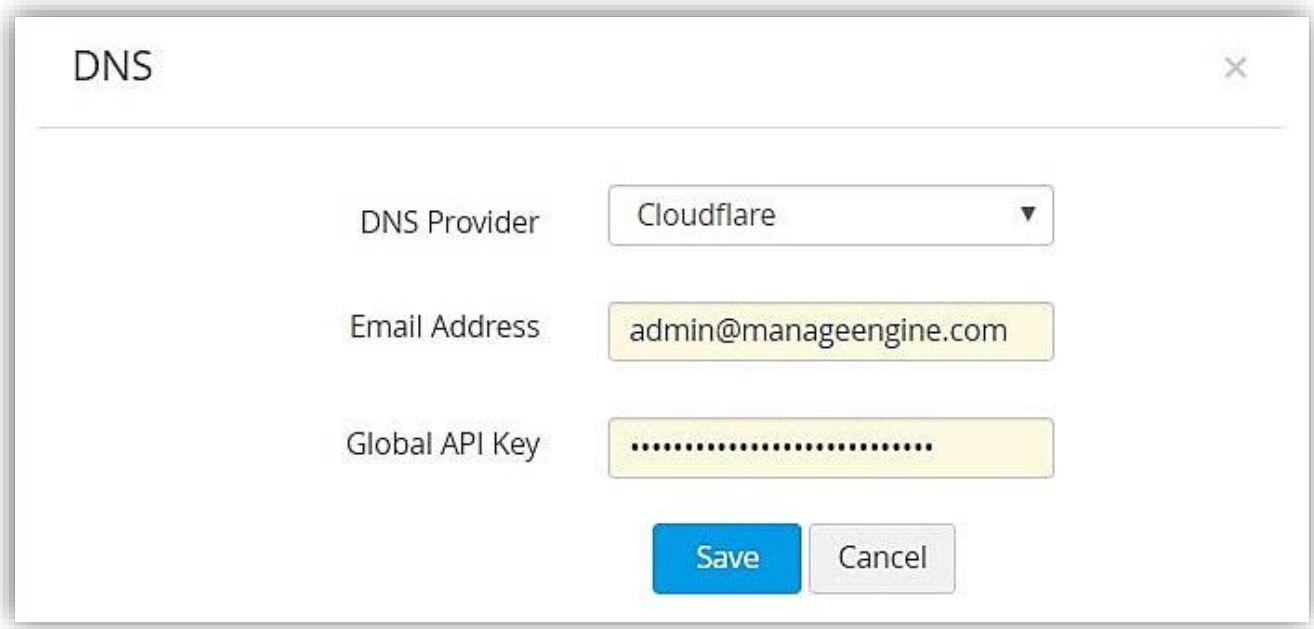


3. If you have an already existing Azure application, provide its **Application ID** and **Key.** If not, follow the steps mentioned below to create the Azure application and key, and give the application access to the DNS zones for making API calls.
4. To create the Azure application and key,
   i. Navigate to **App registrations >> New application registration.**
   ii. Provide the application name, select the application type **Web app / API** and provide the sign-on URL. Click **Create.**
   iii. After successful creation, you are directed to a window that displays the **Application ID.**
   iv. To get the application key, navigate to **Keys** and create a key.
   v. Provide the key description, duration and click **Save.**
   vi. Once the key is saved, key value is displayed. Copy and save the key value for future references.

5. To give the application access to DNS zones,
    i. Navigate to the resource group where all DNS zones or created or switch to a specific DNS zone.
    ii. Switch to **Access Control (IAM)** and click **Add.**
    iii. Choose the role as Contributor, assign access to **Azure AD user,** group or application, search and select the application created in Azure Directory and click **Save.**
    iv. The created Azure application is now given access to DNS zones for making API calls.
6. Finally, enter the **Resource Group Name,** which is the group name in which you have created the DNS zone and click **Save.**
7. Your DNS account details are saved and listed under **Manage >> DNS.**

3.1.2 For Cloudflare DNS

1. In the **Email address** field, specify the email address associated with the Cloudflare account.



2. For **Global API Key**, use the 'Generate API' key option in the domain overview page of the Cloudflare DNS to generate the key and paste the value in this field.
3. Click **Save.** Your DNS account details are saved and listed under **Manage >> DNS.**

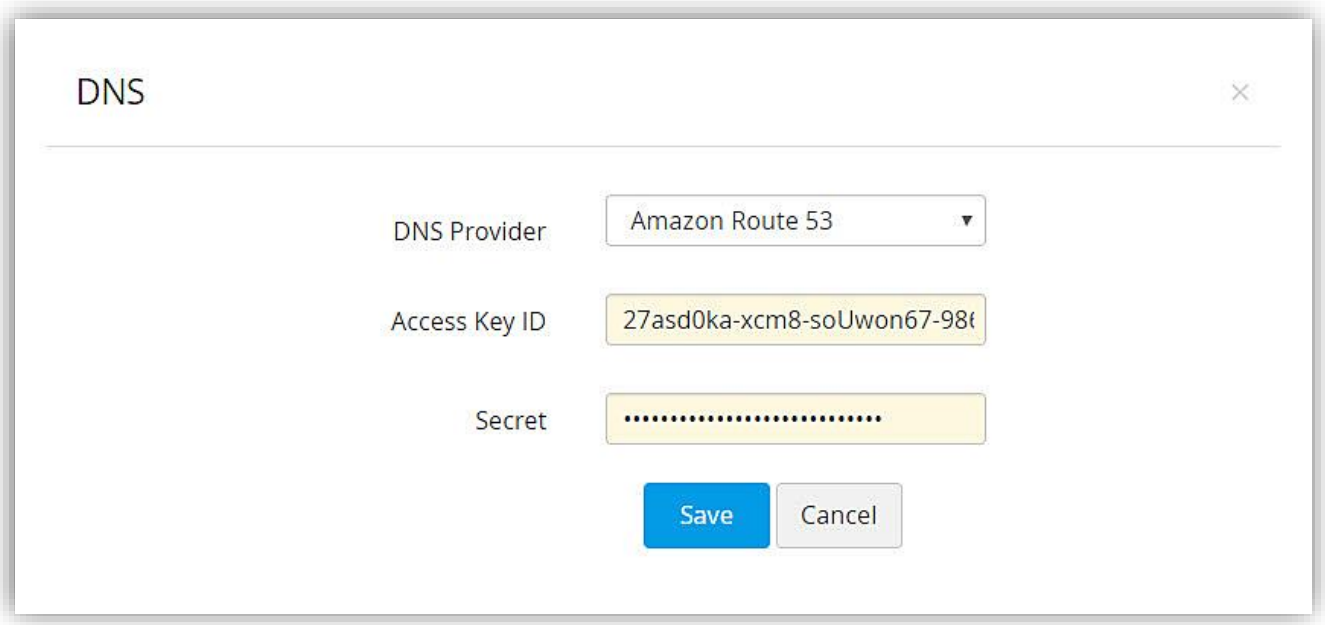
3.1.3 For AWS Route 53 DNS

1. Generate and specify the **Access Key ID** and **Secret** associated with your AWS account.
2. If you do not have an AWS account, create one and generate the Access Key ID and Secret by following the steps given below:
   i. Login to the AWS console and navigate to **IAM Services >>Users**.
   ii. Click **Add user**.
   iii. Provide the user name and select the access type as **Programmatic access**.
   iv. Switch to the next tab, click **Attach existing policies** directly under **Set Permissions** and search for "**AmazonRoute53FullAccess**".
   v. Assign the policy that is listed and switch to the next tab.
   vi. In the tags section, add appropriate tags (optional) and switch to the next tab.
   vii. Review all the information entered and click **Create user**.
   viii. The user account is created and subsequently, an access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.
3. If you already have an AWS user account, you have to grant "**AmazonRoute53FullAccess**" permission to the user and generate the access key if the user doesn't have one. And if the user account has an access key associated already, it is just enough to ensure the required permission is granted.

To grant the required permissions,

1. Navigate to the **Permissions** tab, select the required user account and click **Add Permission**.
2. Click **Attach existing policies** directly under **Set Permissions** and search for "**AmazonRoute53FullAccess**".
3. Assign the listed policy and hit **Save**.
4. To generate the access key,
5. Select the particular user account and navigate to the **Security Credentials** tab.
6. In the window that opens, click **Create access** key.

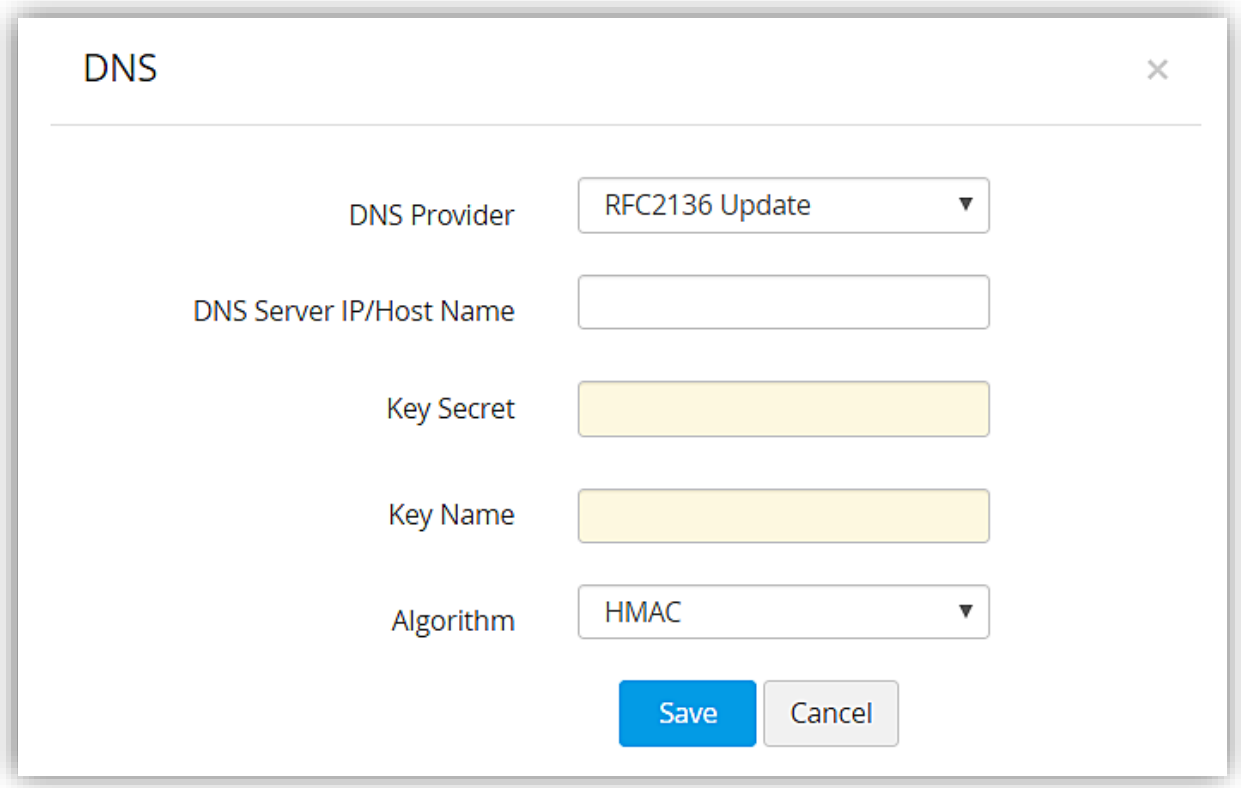
7. An access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.



3.1.4 For RFC2136 DNS Update

If you are using open source DNS servers such as Bind, PowerDNS etc., that support RFC2136 DNS update, follow the steps below to automate DNS-based domain control validation procedure using PAM360:

1. The DNS Server IP / Hostname represents the server name / IP address in which the DNS server is installed or running.
2. The server details are found in the server installation directory. For instance, in the case of Bind9 DNS server, you can find these details in the file named .local.conf in the server installation directory.
3. Provide the Key Secret, which is the key content found in the server installation directory.
4. Provide a name for the key, choose the signature algorithm and click **Save**.



3.1.5 GoDaddy DNS

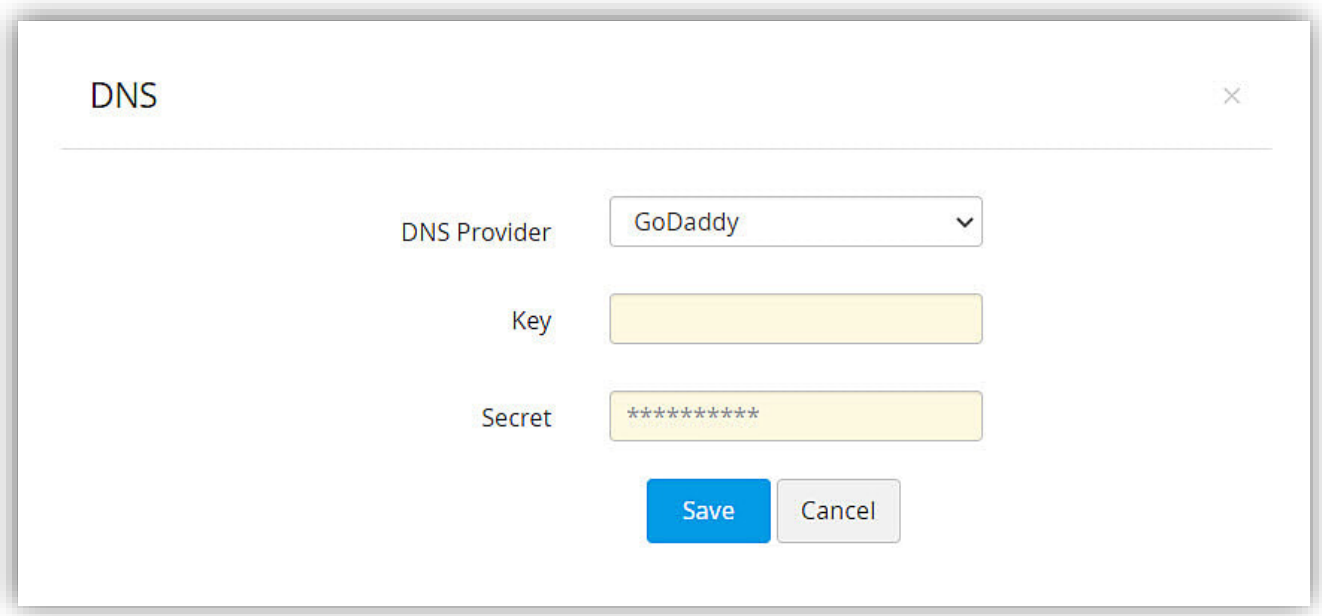
If you are using GoDaddy DNS for DNS validation, follow the steps below to automate DNS-based domain control validation procedure using PAM360.
Steps to Obtain GoDaddy API Credentials:

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Log in to your GoDaddy account if you aren't logged in already.
3. Once you log in, you will be redirected to the API keys page where you can create and manage API keys. Click **Create New API** key.
4. Provide your application name, choose the environment type as **Production** and click **Next**.
5. The API key and its secret is generated. Copy and save the secret in a secure location, as it will not be displayed again.

Now, in the PAM360 interface, follow the below steps to add GoDaddy DNS to Let's Encrypt certificate repository:

1. Navigate to **Certificates >> Let's Encrypt** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.

3. Choose **GoDaddy** from the DNS Provider drop-down menu.
4. Enter the **Key** and **Secret** that was previously generated from the GoDaddy portal. Click **Save**.



3.1.6 ClouDNS

If you are using ClouDNS for DNS validation, follow the steps below to automate the DNS-based domain control validation procedure using PAM360:

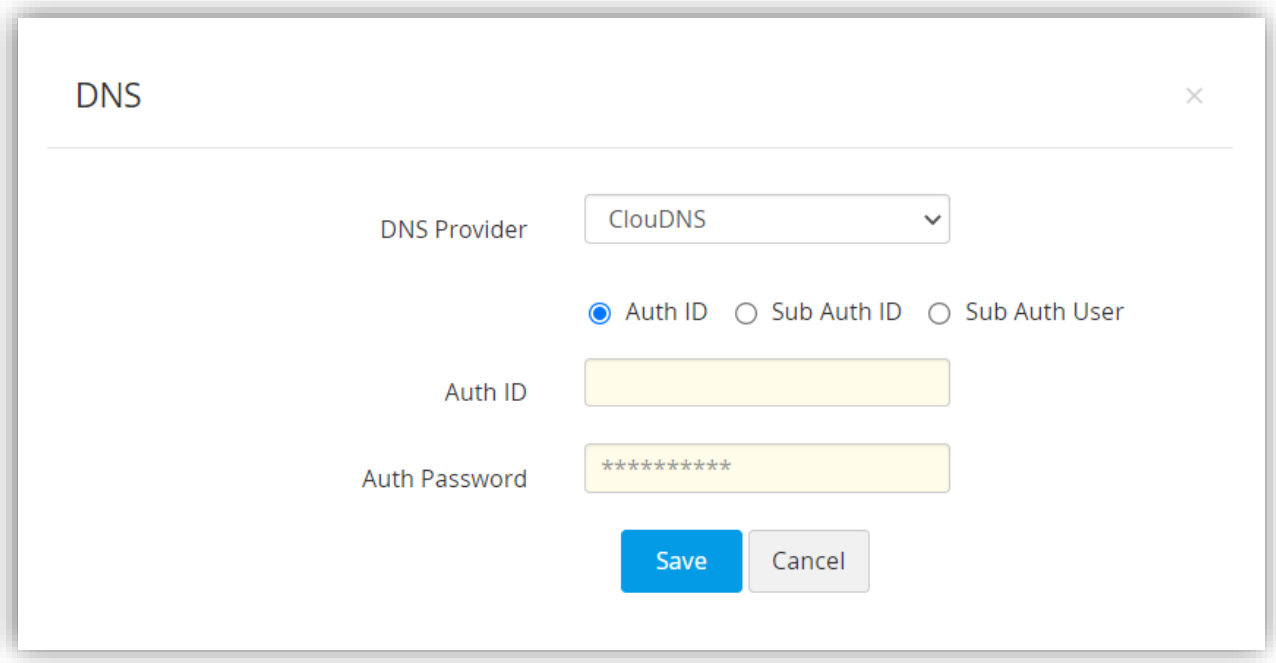
Steps to Obtain ClouDNS API Credentials:

1. Login to your ClouDNS account and go to **Reseller API.**
2. If you have already created an API user id, you will find it under **API Users**. If not, click **Create API** to generate a new one.

Click here to learn more about ClouDNS API Auth IDs.

Now, in the PAM360 interface, follow the below steps to add ClouDNS to Let's Encrypt CA:

1. Navigate to **Certificates >> Acme >> Let's Encrypt** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **ClouDNS** from the **DNS Provider** drop-down.
4. Choose one of the following options: **Auth ID, Sub Auth ID, Sub Auth User.**
5. Enter the chosen ClouDNS Auth ID, its respective **Auth Password**, and click **Save**.



Notes:

- One certificate can secure up to 100 domains. You can enter a maximum of 100 names in the 'domain name' field out of which the first name is considered as the common name and the rest are treated as Subject Alternative Names (SAN).
- PAM360 supports http-01 and dns-01 based domain validations. Choose the challenge type based on your requirements.
- For dns-01 based domain validation, if you are using your configured DNS account for challenge verification, make sure that the status of the chosen DNS account is marked **Enabled** under **Manage >> DNS.**
- Option to change the private key currently works only with the RSA key algorithm.

4. Let's Encrypt Challenge Verification

PAM360 expedites domain validation through automatic verification of HTTP-01 and DNS-01 challenges (currently Azure, Cloudflare, Amazon Route 53 DNS, RFC2136 DNS update, ClouDNS, and GoDaddy DNS). For the automation to take effect, you have to initially map the end-server details to PAM360, which is a one-time process.

4.1 Domain Validation Through HTTP-01 Challenge Verification

For domain validation through http-01 challenge

1. A window opens displaying the challenge to be fulfilled.
2. Click the **Agent mapping** icon.
3. A pop up will open. If the domain server is a Linux machine, fill in the required details and click **Save.**
4. If the domain server is a Windows machine, download and install the PAM360 agent for Windows server using the steps mentioned below:

4.1.1 Downloading PAM360 agent for Windows servers

The PAM360 agent package is a zip file comprising of the necessary executables, configuration files required for automatic verification of Let's Encrypt challenges through automatic domain validation. You have to just unzip and install the agent on your Windows domain server after download. To download the agent,

1. Navigate to **Certificates >> Let's Encrypt** tab, and click **Manage** button in the top right corner.
2. Switch to the **Windows Agents** tab.
3. Download the PAM360 agent from the top right corner of the window based on your server compatibility (32 bit or 64 bit).

4.1.2 Installing PAM360 agents for Windows Server:

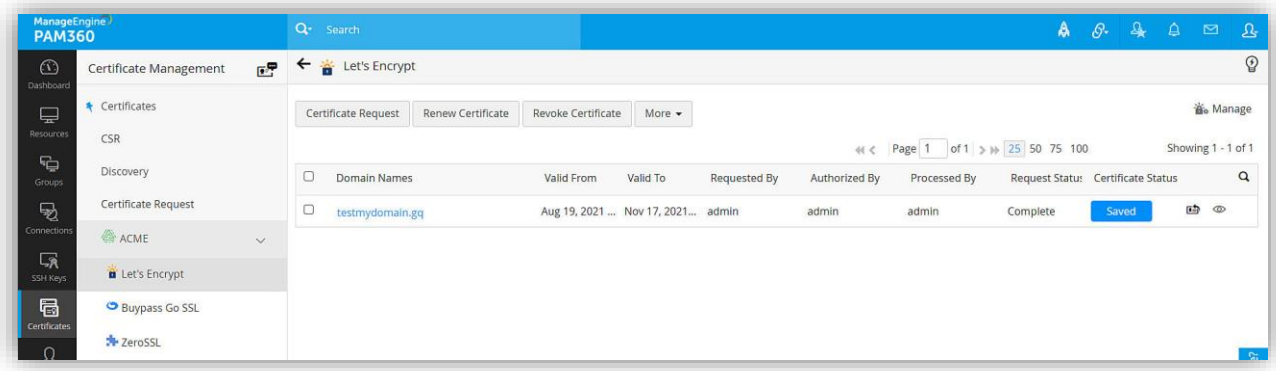
To install PAM360 agent as a Windows service,

1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command **'AgentInstaller.exe start.'**

To stop the agent and uninstall the Windows service,

1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command **'AgentInstaller.exe stop.'**
3. If the domain server is a Windows machine, download and install the Windows agent on the domain server. Navigate to **Manage >> Windows Agents,** download and install the agent on the domain server.

4. Once, the above agent mapping settings are configured (agent mapping is a one-time configuration), PAM360 automatically handles the verification of challenges presented by Let's Encrypt.
5. After configuring agent mapping, click **Pending** on the pending requests and click **Verify.** The challenge is verified and the certificate request is submitted to Let's Encrypt CA.



4.2 Domain Validation Through DNS-01 Challenge Verification

For DNS-01 challenge verification from PAM360,

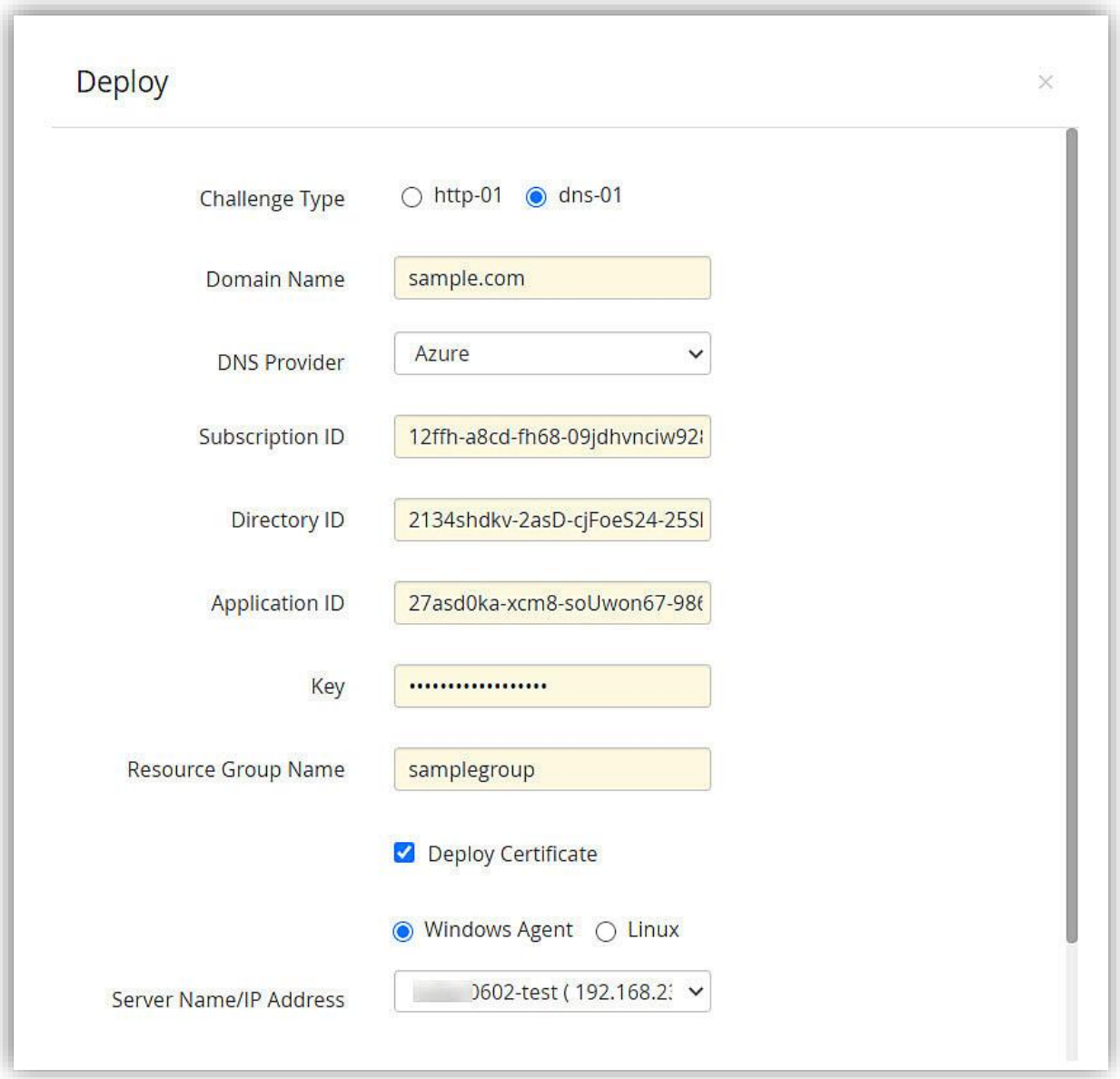
1. Switch to **Let's Encrypt** tab and click on the request status **(Pending)** corresponding to the certificate request.
2. You'll be directed to a window that displays the DNS challenge value and TXT record.
3. If you have already configured your **DNS** account details and have opted for DNS while creating the certificate request, you can assign the DNS account to the request.
4. Select the request, choose **Assign DNS** from More top menu and select the required DNS account.
5. In cases where you do not have a **DNS** account configured or have not opted for it when raising the certificate request, PAM360 provides an option for automating DNS-01 challenge verification through **Agent Mapping.**
6. Click on the **Agent Mapping** icon present to the left side of the request. Agent mapping is a one-time configuration.

Agent Mapping

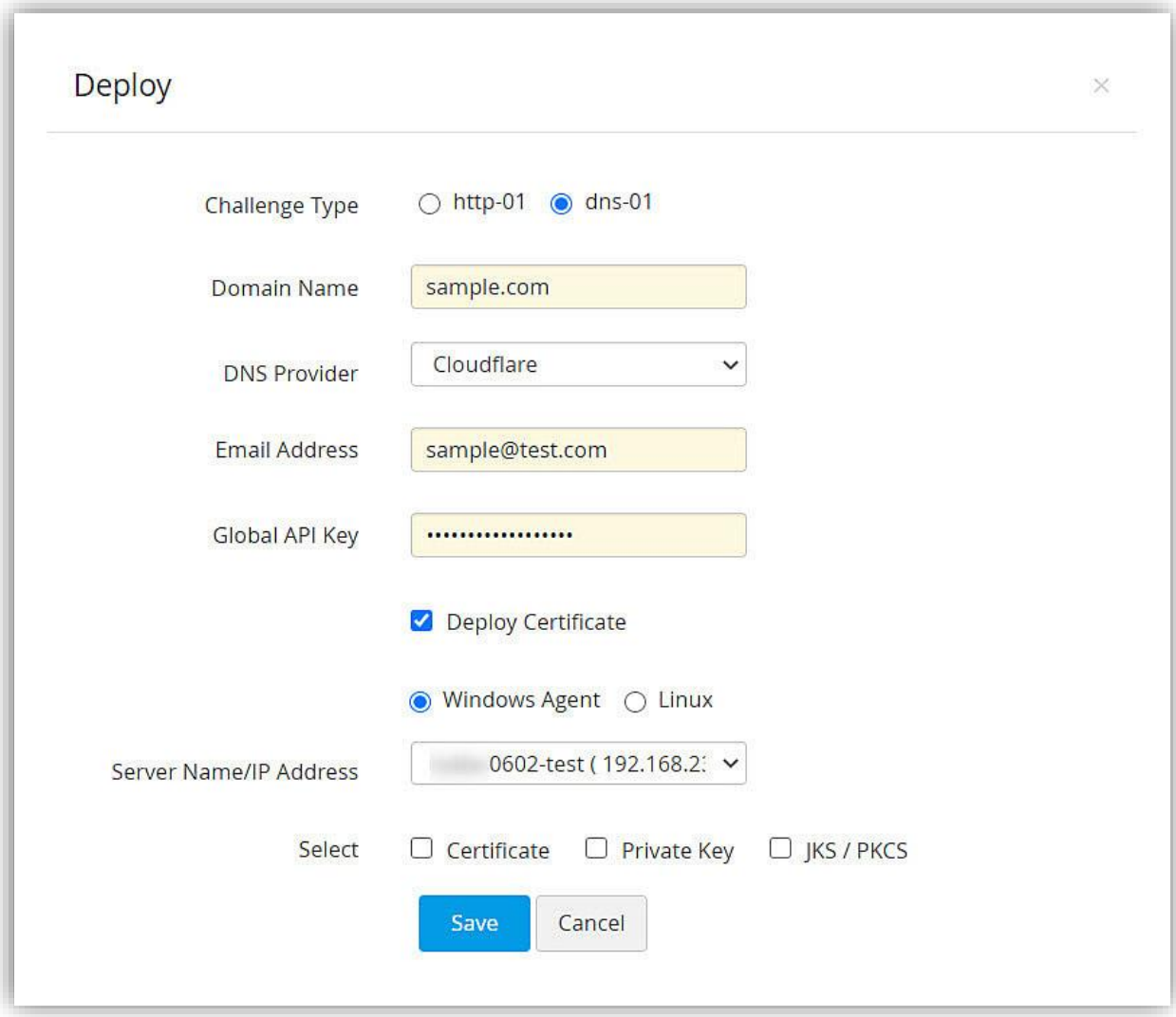
In the **Deploy** window that opens, carry out the following operations to map and save your end-

server details in PAM360.

1. Choose your DNS provider. For Azure DNS, provide the required details—**Subscription ID**, **Directory ID**, **Application ID**, **Application Key** and **Resource Group Name**.



2. For Cloudflare DNS, enter the email address associated with your Cloudflare account and the **Global API key.**



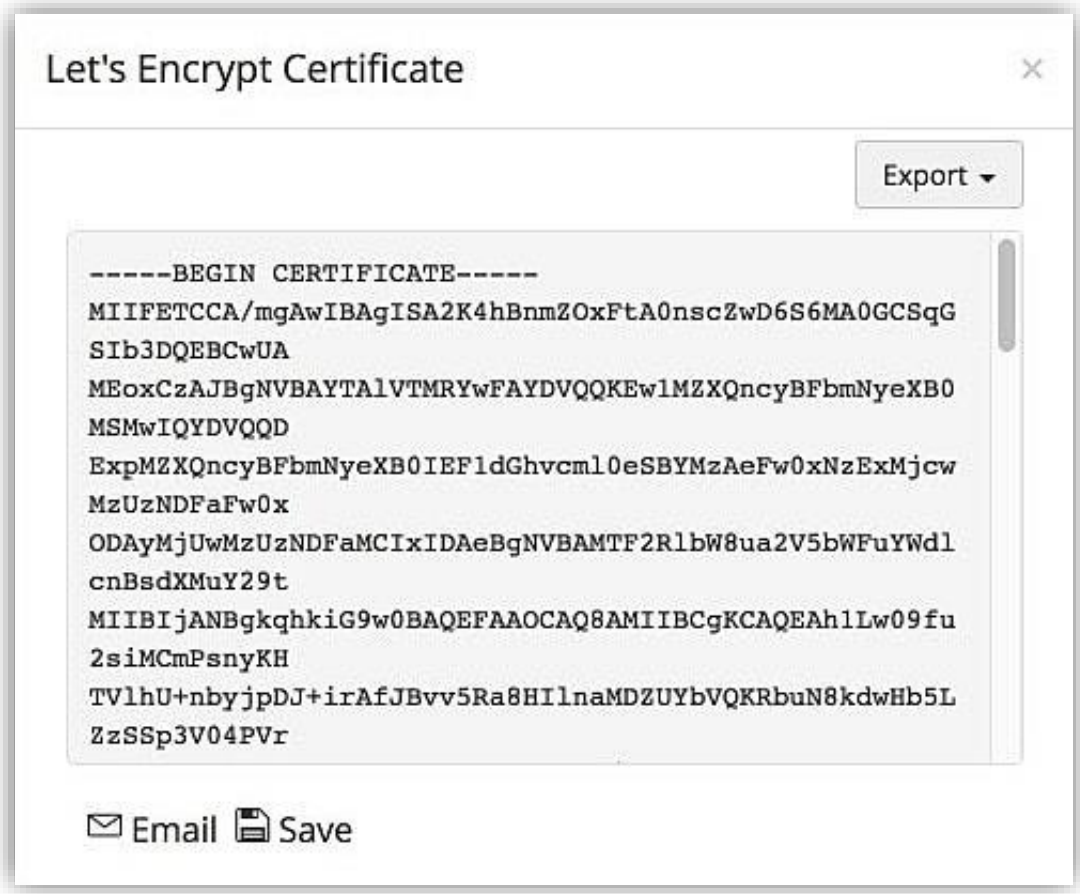
3. For Amazon Route 53 DNS, enter the **Access Key ID** and **Secret** associated with your AWS account.
4. Enable the **Deploy Certificate** check-box to automate deployment of the certificate to their corresponding end-servers after domain validation and after successive renewals.
5. For Linux end-servers provide the required details, while for Windows end-servers download and install the Windows agent using the same procedure as mentioned for http-01 challenge.
6. After filling in the details, click **Save.** The end-server details are successfully mapped and stored in PAM360, which you can view or edit from **Manage >> Deploy** tab.

Notes:

- You can request and acquire certificates only for **public domains** using Let's Encrypt integration.
- The handling of challenges can also be done manually without automation. Copy and paste the challenge values / text records manually in your domain server. Then in the PAM360 server, navigate to **Pending Requests** page and click **Verify.** The challenge is verified and certificate is issued.
- PAM360 automates challenge verification using **DNS** for a certificate request only when **Agent mapping** is not available. Challenge verification is automated through agents, if agent details are available in **Manage >> Deploy tab.**
- Currently, PAM360 agents are only available for Windows servers.
- If you have chosen Global DNS configuration for RFC2136 DNS update, the domain name itself acts as the zone name (Global DNS configuration is possible only if you are using the same **Key Secret** for all zones). Whereas, if you have chosen domain-agent mapping, you have to provide the Zone name, Key Name, and Key Secret for each domain separately.

5. Procuring and Saving the Certificate

1. On successful verification, Let's Encrypt issues the requested certificate.
2. The window automatically redirects to a page which displays the certificate and its status (status is marked Available, if the challenge verification is successful and Failed if the challenge verification fails).
3. Click the Available button to save the certificate in PAM360 repository, e-mail or export it.
4. If the challenge fails, click New challenge ( ) to obtain another set of challenges and repeat the above process.
5. On saving, the certificate gets added to the PAM360 repository which can be viewed from the **Certificates>> Certificates** tab.



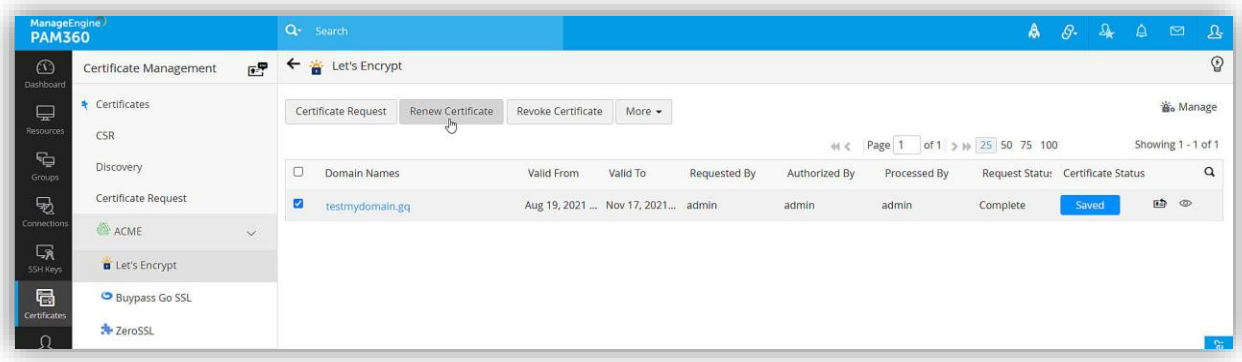
6. Renewing Certificates

Certificates issued by Let's Encrypt have a life-time of ninety days after which they are not valid. Also, as mentioned above, the domain authentication validity period is sixty days, which means that the user has to fulfill the challenges once in every sixty days in order to prove his ownership of the domain.

Certificate renewals can be carried out manually or automatically through automatic domain validation. To renew a certificate manually,

1. Navigate to **Certificates >> Let's Encrypt**.
2. Select the certificate that you want to renew and click Renew Certificate button.
3. The certificate is renewed and the Certificate Status bar displays Renewed.
4. Click on it to save the renewed version of the certificate to PAM360 certificate repository.
5. History on renewal can be inferred by clicking on the certificate history button from the **Certificates >> Certificates** tab.

Note: The certificate should be saved after renewal in order to be updated in the certificate repository. Else, only the old version of the certificate will continue to remain in repository.



6.1 Automatic Renewals through Automatic Domain Validation

If agent mapping had been configured, the certificate renewal process is done automatically without manual intervention. All the certificates in your organization procured from Let's Encrypt is automatically renewed after every 75 days. i.e., 15 days before its expiry and a notification is sent to the account holder's e-mail address.

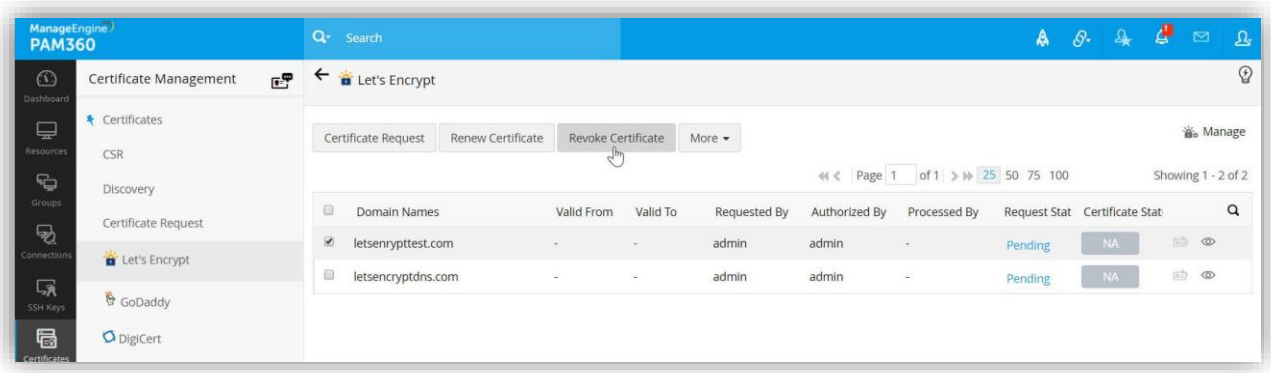
Note: Automatic renewals are applicable only for those certificates saved in PAM360 repository. i.e., after procuring a certificate from Let's Encrypt, you have to save it in order for the automatic renewal to take effect.

7. Revoking Certificates

Revoking a certificate renders the certificate invalid and immediately removes the HTTPS from the website.

To revoke a certificate,

1. Navigate to **Certificates >> Let's Encrypt** tab.
2. Select a certificate you want to revoke and click **Revoke Certificate**.
3. The certificate is revoked and is no longer valid.

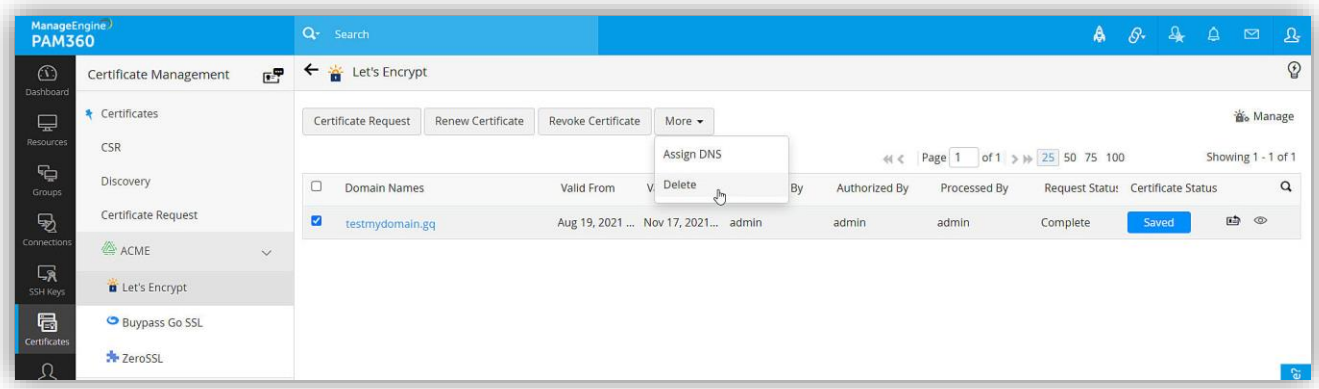


8. Deleting Certificates

Deleting a certificate removes the certificate from PAM360 repository, but the certificate still remains valid.

To delete a certificate,

1. Navigate to **Certificates >> Let's Encrypt** tab.
2. Select the certificate you want to delete and click **Delete**.
3. The certificate is deleted from the PAM360 database.



9. About Let's Encrypt

Let's Encrypt is a free, automated and open Certificate Authority developed by the Internet Security Research group (ISRG) with a main motive to reduce the complexity involved in establishing HTTPS connection and smoothen the overall certificate installation process. Till date, Let's Encrypt issues only domain validated certificates. Organization validation and extended validation are not available and are not being planned to be distributed anytime in the near future. All certificates issued by Let's Encrypt have a life time of ninety days after which they are not valid. Also, the domain authentication validity for a certificate is sixty days.

i.e., for every domain you secure, you'll have to fulfill the challenges once in sixty days in order to prove your ownership of the domain. The main purpose of domain validation is to ensure security and Let's Encrypt is planning to reduce this domain authentication validity period to seven days.For more information about Let's Encrypt, click here.

Integrating PAM360 with GoDaddy SSL Certificate Authority

PAM360 facilitates integration with GoDaddy SSL certificate authority (CA) and helps you achieve an end-to-end life cycle management of GoDaddy certificates installed on your domains from a single interface. This document discusses the steps you should follow to establish connection with your GoDaddy account, acquire, deploy, renew and perform all certificate management-related operations from PAM360.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to GoDaddy's CA Services.

URL: https://api.godaddy.com/

Port: 443

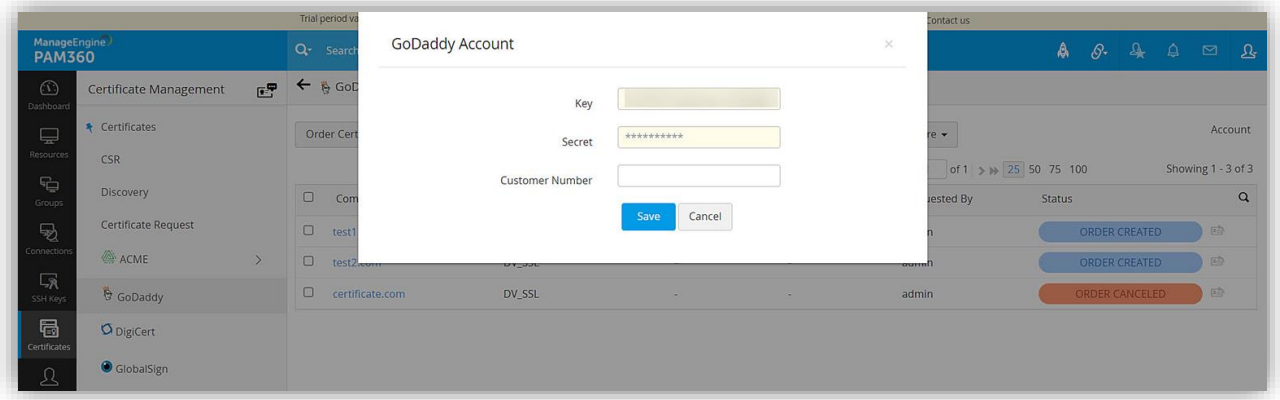
Follow the step-by-step procedure below to integrate GoDaddy with PAM360:

1. **Configure GoDaddy API credentials in PAM360**
2. **Place a certificate order**
3. **Domain validation through challenge verification**
4. **Certificate issue**
5. **Renew, revoke and delete certificates**
6. **Import existing certificates**

1. Configure GoDaddy API Credentials in PAM360

To begin managing the lifecycles of certificates issued by GoDaddy CA from PAM360, you have to initially set up a connection with your GoDaddy account by providing your API key details generated from the website. To generate your API key,

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Login to your GoDaddy account if you aren't logged in already.
3. Once you log in, you'll be redirected to the API keys page where you can create and manage API keys. Click **Create New API key.**
4. Provide your application name, choose the environment type as **Production,** and click **Next.**
5. The API key and its secret is generated. Copy and save the secret in a secure location, for it will not be displayed again.
6. Now, navigate to PAM360 and switch to **Certificates >> GoDaddy** tab. Click on **Account** on the top-right corner.
7. Provide the API key and secret in the pop up that appears and click **Save.**



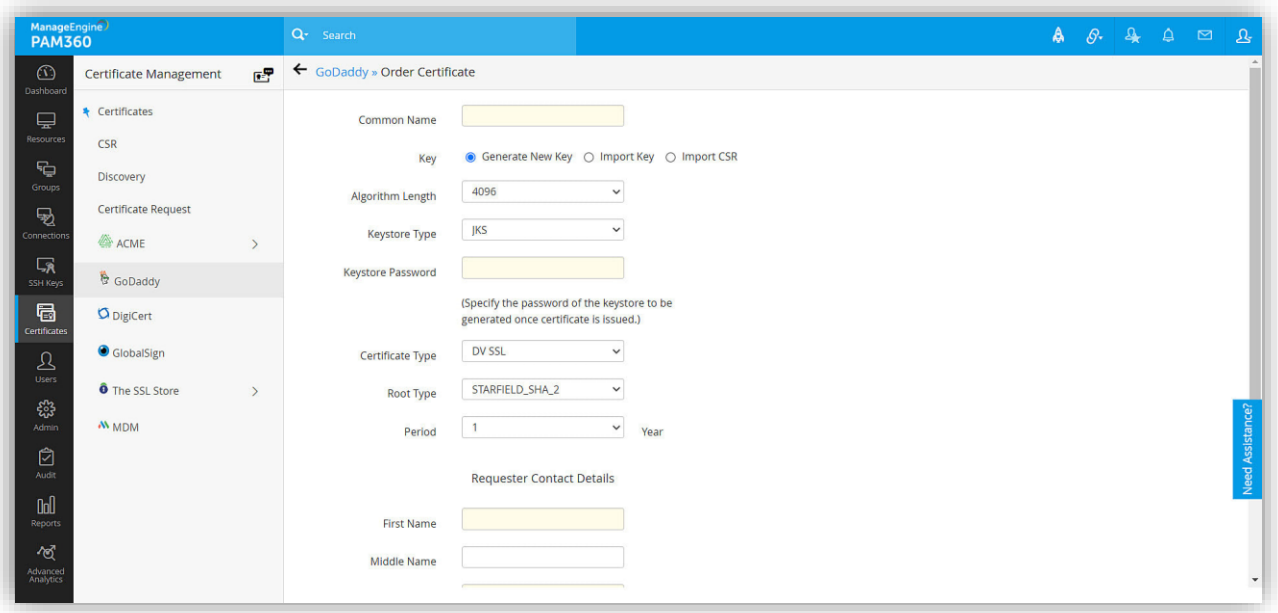
8. The key details are stored in PAM360. The account configuration is a one-time process so you needn't provide your API details every time you place a certificate order.

2. Place a Certificate Order

After setting up the account, you need to acquire SSL certificates from GoDaddy before placing a certificate order from PAM360.

1. To buy SSL from GoDaddy, go to the GoDaddy web security portal and buy the certificates of your choice from **SSL Certificates.** This will just add the desired SSL product to your GoDaddy account as a credit; the SSL certificates won't be available for use.
2. After purchasing the SSL certificates, you can set up the certificates in PAM360 by creating a certificate request, and importing the certificates into PAM360.

3. To do so, navigate to **Certificates >> GoDaddy**, and click on **Certificate Order**.



4. Fill in the required details and click **Create.**

> **Note:** When raising certificate requests from PAM360, you can only raise as many requests as the number of set-up certificates purchased from GoDaddy.

3. Domain Validation through Challenge Verification

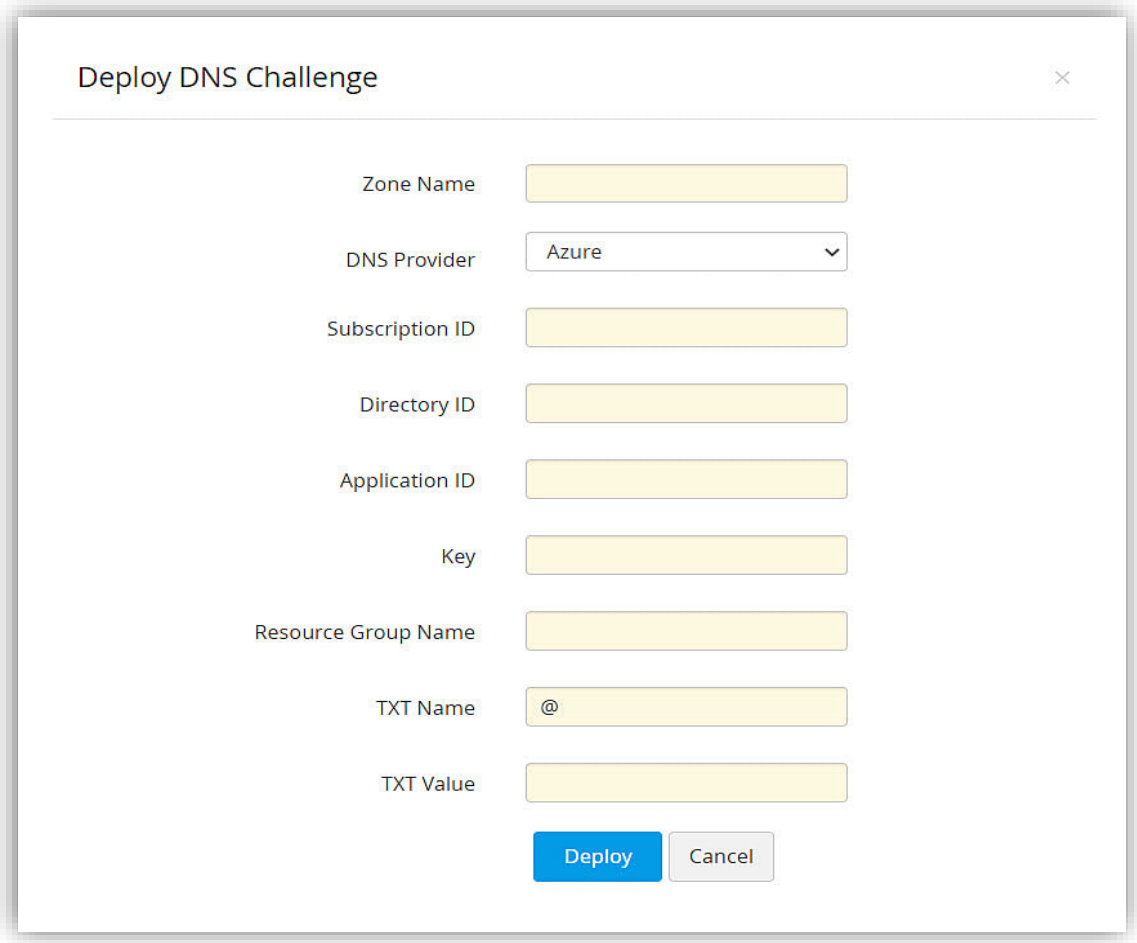
Once you have placed the certificate order, you need to validate your ownership of the domain by fulfilling certain challenges put forth by GoDaddy CA. The challenge IDs are mailed to requester's as well as the domain administrator's email IDs. To prove your ownership of the domain and acquire the SSL certificate,

1. Open the email from GoDaddy consisting of domain verification challenge details.
2. GoDaddy offers two methods to prove your domain ownership, out of which you've to choose one based on the type of your certificate request and your environment.
    i. **HTML page-** Upload an HTML page with the challenge ID provided in your domain server, to a distinct directory of the website for the common name in your request.

> **Note:** This validation method is not available for Wildcard SSL certificate requests.

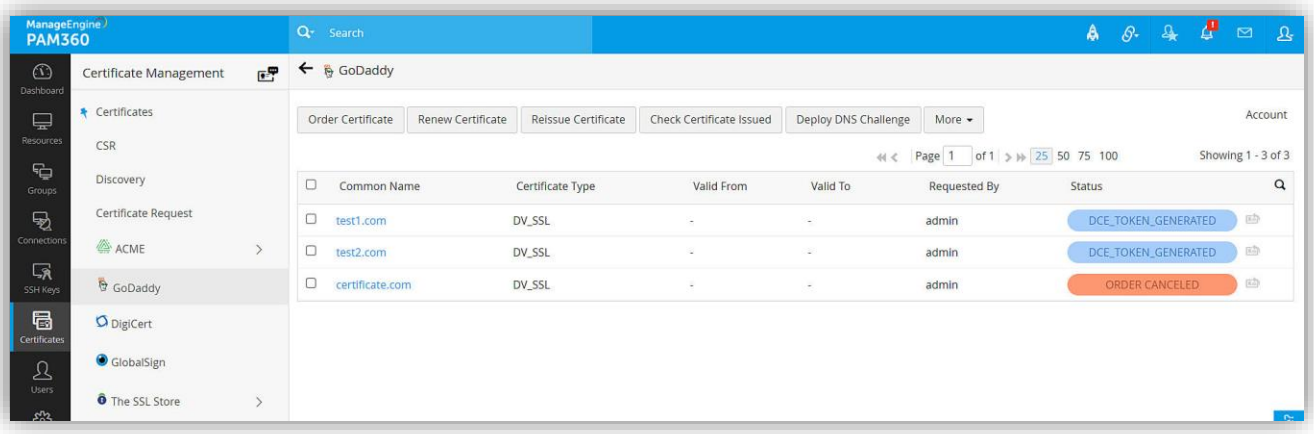
ii. **DNS record** - Create a TXT record with the challenge ID in your domain name's zone (DNS) file.

3. After making the above updates, click on the verification link sent to your email ID. On successful validation of your domain, GoDaddy certificate authority issues the certificate.
4. For domain validation through DNS-based challenge verification, you can configure your DNS details (supported for Azure DNS, Cloudflare DNS, Amazon Route 53, RFC2136 Update, ClouDNS, and GoDaddy DNS) and deploy the challenge ID directly from PAM360 using the **Deploy DNS Challenge** option. Click here for a more detailed explanation of the instructions for domain control challenge verification.



4. Certificate Issue

After performing the operations on your domain server and submitting the domain validation, navigate to **Certificates** and click **Check Certificate Availability** icon beside the corresponding certificate request. If your domain verification is successful, GoDaddy issues the certificate which is fetched by PAM360 and is added to the centralized certificate repository.



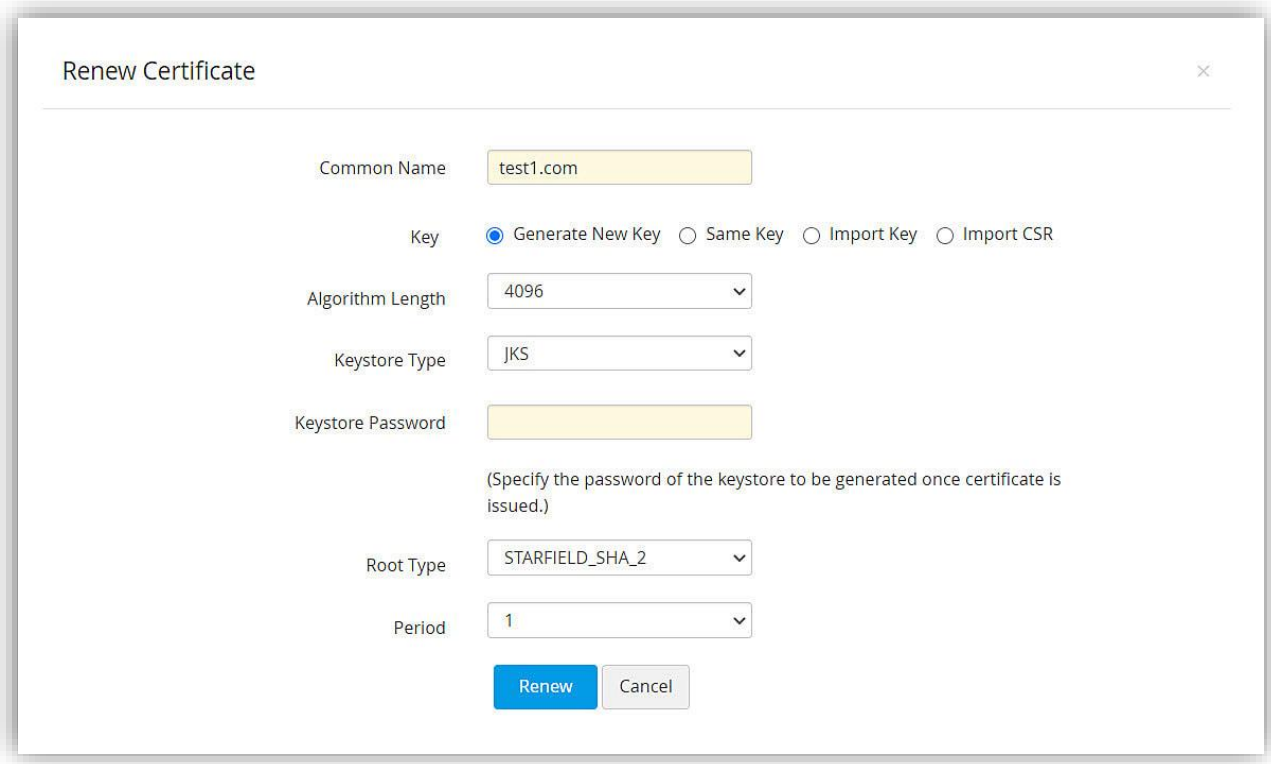
Note: The certificate is automatically added to PAM360 repository only if you have the required license count. If not, renew your PAM360 license and then attempt to add the issued certificate to the repository.

5. Renew, Revoke and Delete Certificates

You can renew, revoke, or request reissue for certificates, and cancel certificate orders from PAM360.

To renew a certificate,

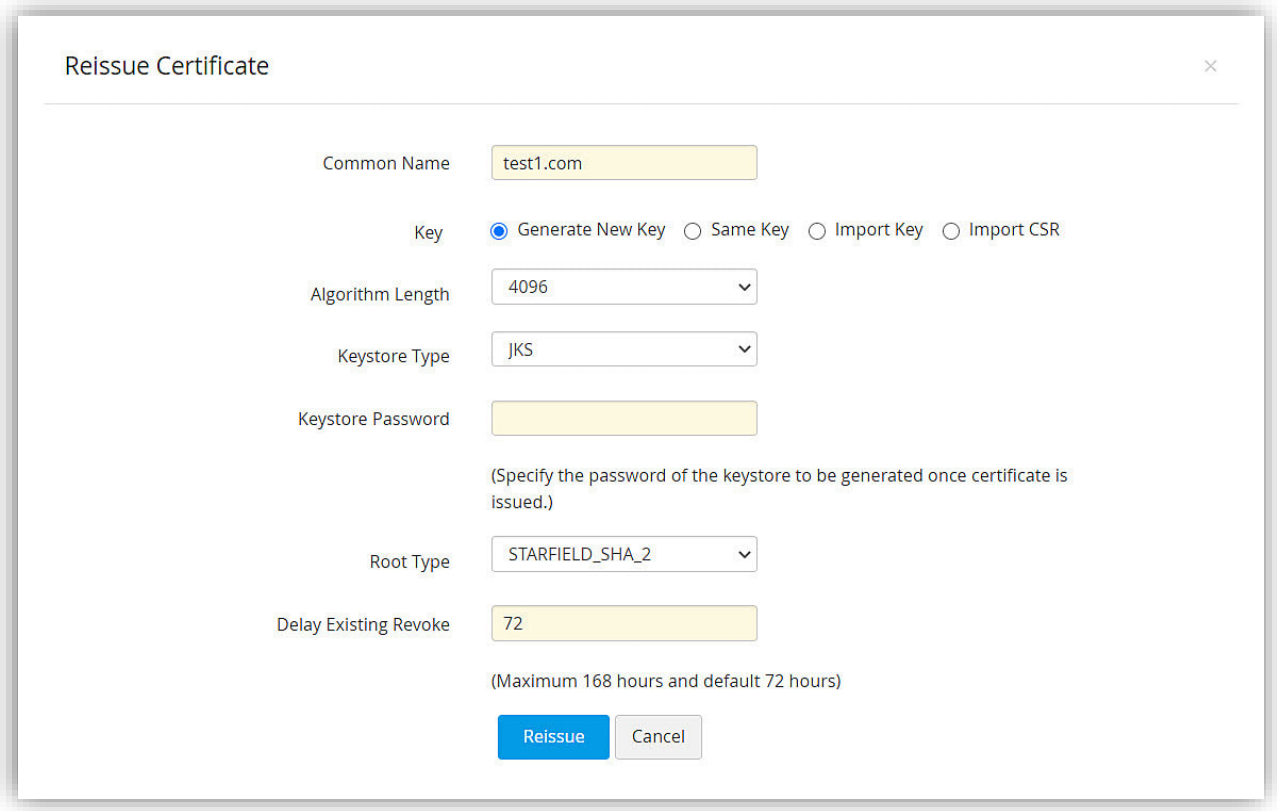
1. Navigate to **Certificates >> GoDaddy** tab.
2. Select the required certificate and click **Renew Certificate** from the top menu.



3. You have to prove your ownership of the domain before every renewal by fulfilling the challenges put forth by GoDaddy CA. The challenges are mailed to the requester's and domain administrator's email IDs.
4. On successful validation, certificate is issued and is automatically added to PAM360's certificate repository.

To request for a certificate reissue,

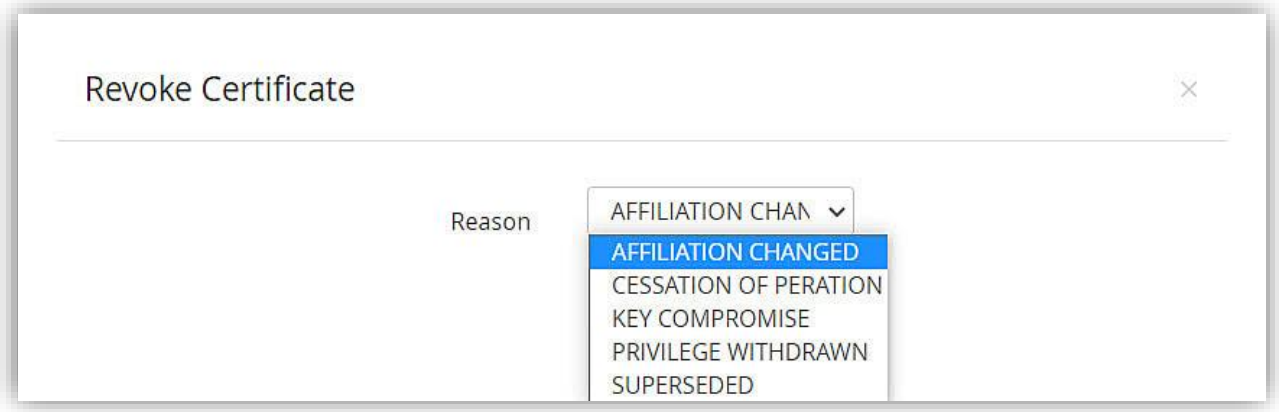
1. Navigate to **Certificates >> GoDaddy** tab.
2. Select the required certificate and click **Reissue Certificate** from the top menu.



3. Here again, you have to prove your ownership of the domain before fulfilling the challenges put forth by GoDaddy CA. The challenges are mailed to the requester's and domain administrator's email IDs.
4. On successful validation, the certificate is reissued and is automatically added to PAM360 certificate repository.

To revoke a certificate,

1. Navigate to **Certificates >> GoDaddy** tab.
2. Select the required certificate and click **Revoke Certificate** from the **More** drop down menu.



3. Confirm the action by clicking **Revoke** after choosing a valid reason from the dropdown. Switch to the **Certificates** tab and delete the certificate to permanently remove it from PAM360's repository.

> **Note:** Revoking a certificate will remove the certificate as well as the corresponding SSL bought from GoDaddy website, and you won't be able to request another certificate for the same SSL. So, it's advised to use 'Reissue' instead of 'Revoke'.

To delete a certificate request from PAM360,

1. Navigate to **Certificates >> GoDaddy** tab.
2. Select the required certificate and click **Delete** from the **More** drop-down menu.

To cancel a certificate order from PAM360,

1. Navigate to **Certificates >> GoDaddy** tab.
2. Select the required certificate and click **Cancel Order** from the **More** drop-down menu.

6. Import Existing Certificates

PAM360 allows you to import existing certificates from GoDaddy which you may have ordered before integrating with PAM360. Using this option, you can import previous GoDaddy certificates into the Certificates >> Certificates tab and manage them from PAM360.

Follow the below steps:

1. Navigate to **Certificates >> GoDaddy** tab.
2. Click **More >> Import Existing Certificates**. In the pop up, you can choose to exclude the expired and revoked certificates.
3. Click **Import**.

The imported certificates will be added to the **Certificates >> Certificates** tab. Please note that these certificates will not be present under the GoDaddy certificates tab.

Integrating PAM360 with The SSL StoreTM Certificate Authority

PAM360 facilitates end-to-end life cycle management of certificates obtained from trusted certificate authorities (CAs) by enabling users to acquire, consolidate, deploy, renew and track certificates issued by commercial CAs from a single interface.

With PAM360's seamless API-based integration with The SSL Store™—one of the largest platinum partners of world's leading CAs—you will have the option to acquire and manage certificates from the following third-party CAs directly using PAM360: **Sectigo (formerly Comodo), Symantec, Thawte, Geotrust,** and **RapidSSL**.

Before you proceed with the integration, complete the following step as a prerequisite:

> **Prerequisite**
>
> Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to the SSL Store's CA Services.
>
> **URL:** https://api.thesslstore.com/rest/
>
> **Port:** 443

Follow the steps below to place certificate orders, acquire, consolidate, deploy and manage trusted third-party CA certificates from PAM360.

1. Configuring API authentication credentials in PAM360
2. Placing a certificate order

   2.1 Configuring DNS account
3. Domain control validation, certificate issue and deployment
4. Renewing, reissuing and deleting certificate orders

1. Configuring API Authentication Credentials in PAM360

The first step to request and manage third-party CA certificates from PAM360 is to sign up for an **exclusive enterprise account** at The SSL Store™ portal and configure the API credentials generated subsequently in PAM360's interface. To set up an Enterprise account with The SSL Store™,

1. Navigate to this enterprise sign up link in The SSL Store™ website. Proceed through the sign up link for Key Manager Plus.
2. Fill in your personal details and organization details as requested, and click **Continue**.
3. You will then be taken to the **Setup Payment** section where you need to configure a payment method, and provide the payment details and billing information.
4. After providing the details, click **Continue**.
5. You will be redirected to the **Confirmation/Token** section where the API credentials (Partner ID and Token) are displayed. Copy and save the credentials in a secure location.
6. Now, switch to the PAM360 server and navigate to **Certificates >> The SSL Store™** tab. Click **Manage** in the top-right corner of the window.
7. Under the **Accounts** tab, provide the generated partner code and token, and click **Save**.
8. The details are stored in PAM360. Configuring API authentication credentials is a one-time process. You do not need to provide the details every time you place a certificate order.

2. Placing a Certificate Order

Once you have configured your API authentication credentials, you can leverage The SSL Store™'s API to generate certificate signing requests (CSRs), place orders, procure, and manage certificates from any of the following certificate authorities directly from PAM360: **Sectigo, Symantec, Thawte, GeoTrust,** and **RapidSSL**.

To generate a CSR and place a certificate order,

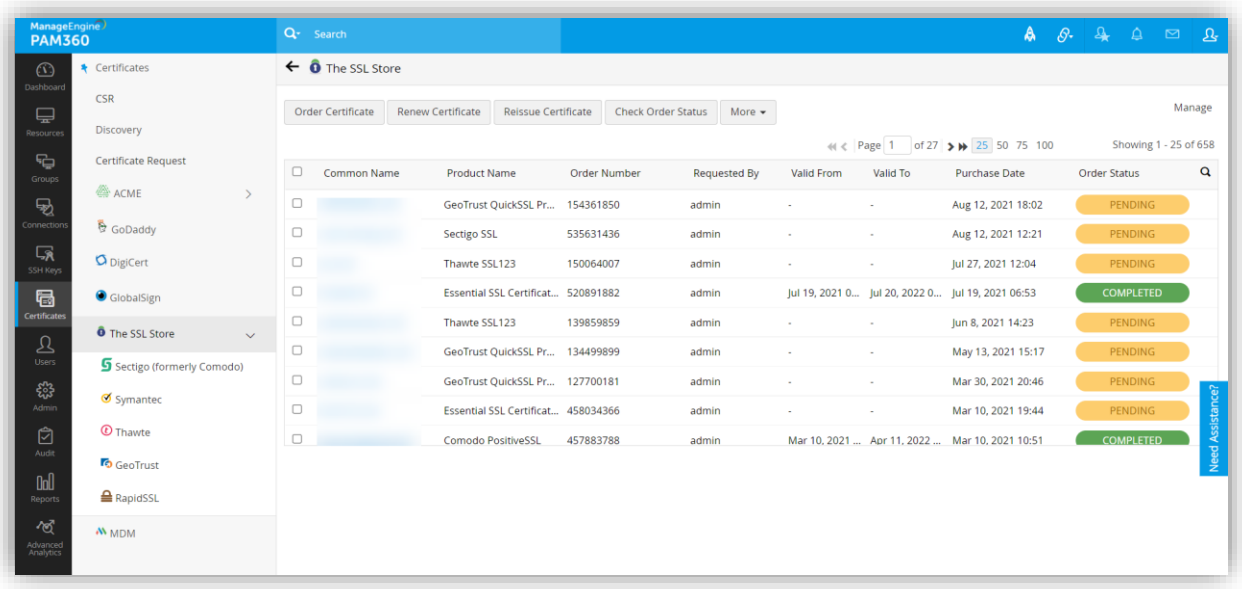
1. Navigate to the **Certificates** tab >> **The SSL store™**.
2. Click **Order Certificate**.
3. In the window that opens, choose the vendor, validation type, product name, domain validation type and validity.
4. PAM360 supports all the three domain control validation methods: DNS-based, file-

based and email validation.

5. Then, provide the common name, algorithm length, keystore type, keystore password, number of servers in which the certificate will be deployed, server type and the approver's email IDs. Users also have the option to import and use an already existing CSR or private key.
6. The approver email ID is the email ID to which Domain Control Validation (DCV) verification mail will be sent. The approver email ID should take either of the following formats:
    - <admin@domain>, <administrator@domain>, <hostmaster@domain>, <webmaster@domain> or <postmaster@domain>
    - Any administrator, registrant, tech or zone contact email address that appears on the domain's WHOIS record and is visible to the CA system.
7. Then, provide the organization details (applicable for organization validation and extended validation order types only), administrator contact details and contact details of the technician placing the certificate order.
8. After filling in the details, click **Create**.
9. You will be taken to a window where you can see the list of certificate orders placed along with their statuses displayed to the right of the table view.

Note:

- PAM360 allows you to import the already existing certificate orders placed within your account from The SSL Store™ and track their statuses. Click **Import Existing Orders** from the **More** top menu to import the existing open orders into **PAM360.**
- Also, you can preconfigure your organization details under **Manage** to refrain from providing it every time you place an OV / EV certificate order.



2.1 Configuring your DNS account

If you are opting for DNS-based domain validation in the certificate order, you should configure the DNS account in PAM360 and specify it in the **DNS** field in the order to automate the challenge verification procedure. To configure your DNS account,

1. Navigate to **Certificates >> The SSL Store™ >> Manage**
2. Switch to the **DNS** tab. Click **Add** and in the pop-up that opens, choose the DNS provider.
3. Here, you can add a maximum of one DNS account for each supported DNS provider. PAM360 currently supports automatic domain control validation for Azure, Cloudflare DNS, Amazon route 53 DNS, RFC2136 DNS update (nsupdate), GoDaddy DNS, ClouDNS.

2.1.1 For Azure DNS

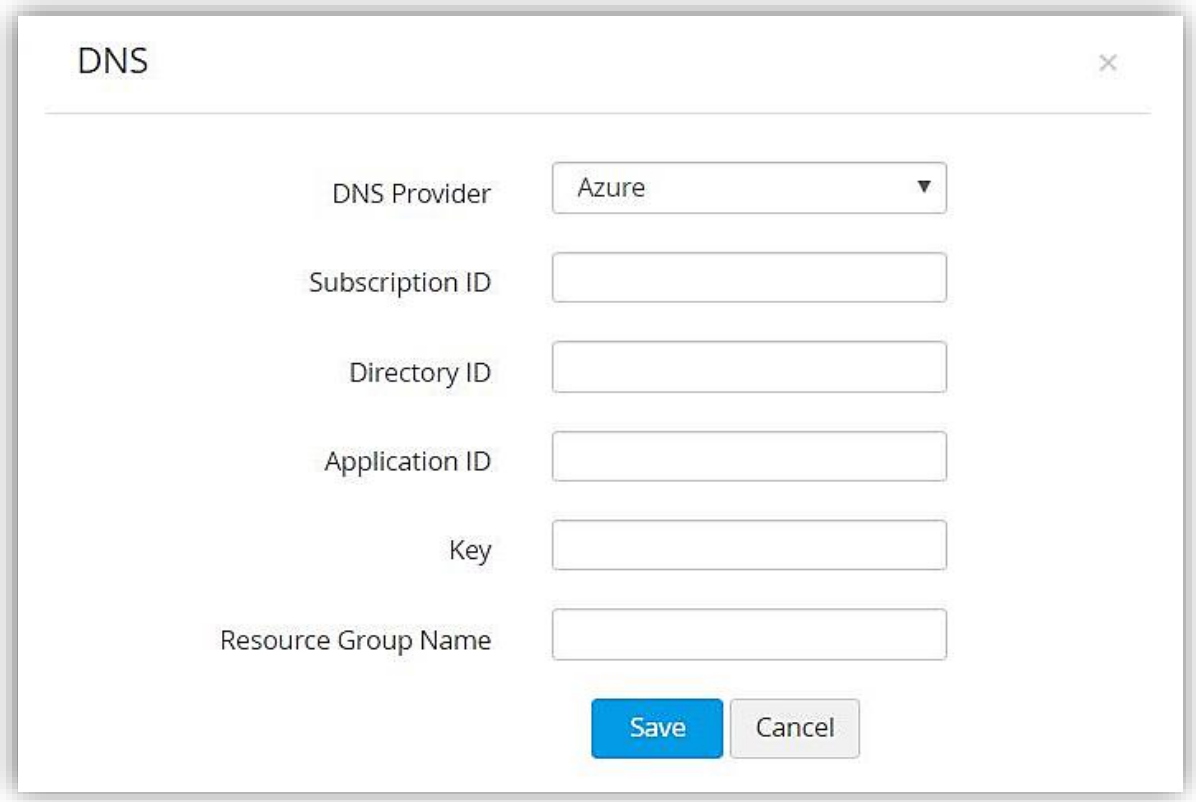
1. Provide the **Subscription ID**, which is available in the Overview page of the Azure DNS zone.
2. Provide the **Directory ID**, which is available in **Azure Active Directory >> Properties.**
3. If you have an already existing Azure application, provide its **Application ID** and Key.
4. If not, follow the steps mentioned below to create the Azure application and key, and give the application access to the DNS zones for making API calls.

Follow the below steps to create the Azure application and key from the **Azure console**:

1. Navigate to **App registrations** >> **New application registration**.
2. Provide the application name, select the application type Web app / API and provide the sign-on URL. Click **Create**.
3. After successful creation, you are directed to a window that displays the Application ID.
4. To get the application key, navigate to **Keys** and create a key.
5. Provide the key description, duration and click **Save**.
6. Once the key is saved, key value is displayed. Copy and save the key value for future references.

To give the application access to DNS zones:

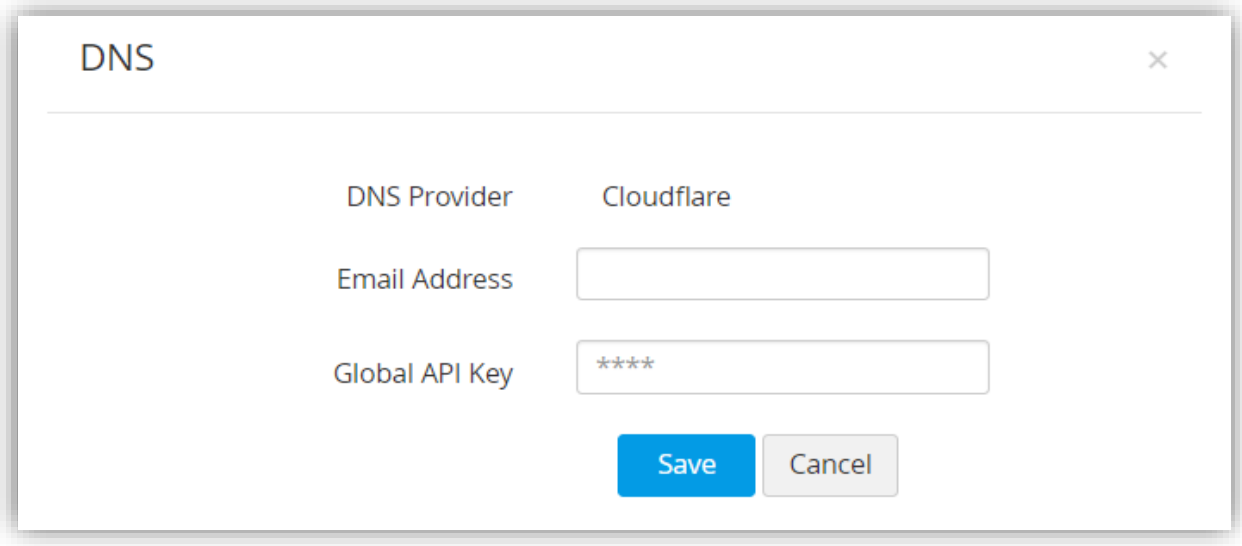
1. Navigate to the resource group where all DNS zones are created or switch to a specific DNS zone.
2. Switch to **Access Control (IAM)** and click **Add**.
3. Choose the role as **Contributor**, assign access to Azure AD user, group or application, search and select the application created in Azure Directory and click **Save**.
4. The created Azure application is now given access to DNS zones for making API calls.
5. Now, enter the **Resource Group Name**, which is the group name in which you have created the DNS zone and click **Save**.
6. Your DNS account details are saved and listed under **Manage >> DNS.**



2.1.2 For Cloudflare DNS

1. In the **Email address** field, specify the email address associated with the Cloudflare account.
2. For Global API Key, use the 'Generate API' key option in the domain overview page of the Cloudflare DNS to generate the key and paste the value in this field.
3. Click **Save**. Your DNS account details will be saved and listed under **Manage >> DNS**.

> **Note:** For DNS based domain validation type, if you are going to specify an already configured DNS account in the certificate order for domain control validation, make sure its status is marked **Enabled** under Manage >> DNS.

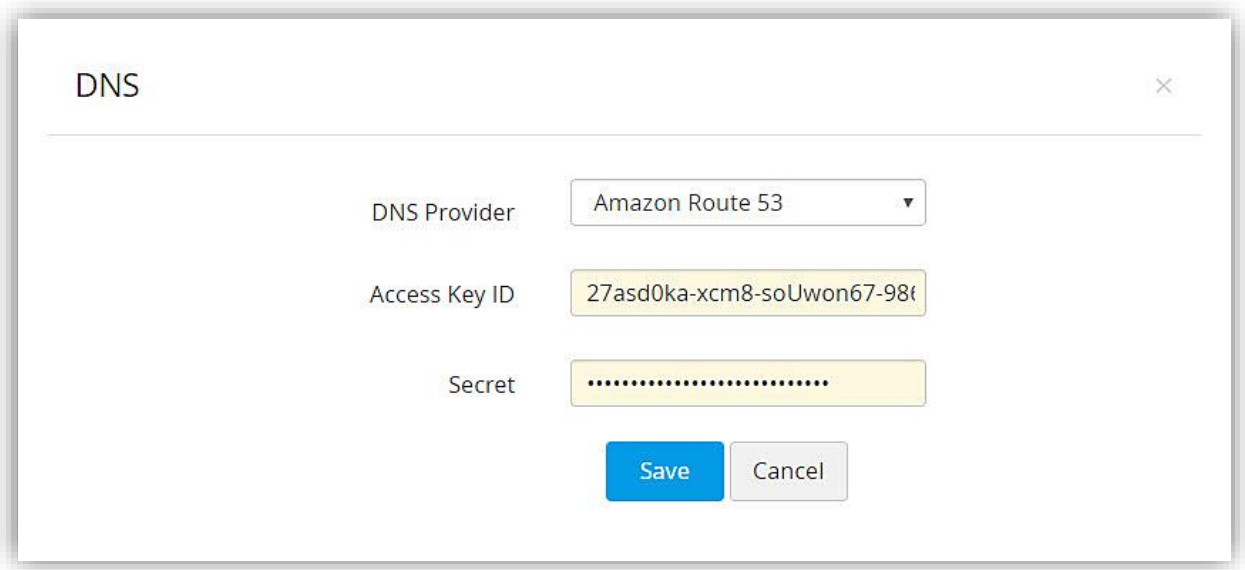


2.1.3 For AWS Route 53 DNS

1. Generate and specify the **Access Key ID** and **Secret** associated with your AWS account.
2. If you do not have an AWS account, create one and generate the Access Key ID and Secret by following the steps given below:
    i. Login to the AWS console and navigate to **IAM Services** >> **Users**.
    ii. Click **Add user**.
    iii. Provide the user name and select the access type as **Programmatic access**.
    iv. Switch to the next tab, click **Attach existing policies** directly under **Set Permissions** and search for "**AmazonRoute53FullAccess**".
    v. Assign the policy that is listed and switch to the next tab.
    vi. In the tags section, add appropriate tags (optional) and switch to the next tab.
    vii. Review all the information entered and click **Create user**.
    viii. The user account is created and subsequently, an access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.
3. If you already have an AWS user account, you have to grant "**AmazonRoute53FullAccess**" permission to the user and generate the access key if the user doesn't have one. And if the user account has an access key associated already, it is just enough to ensure the required permission is granted.

To grant the required permissions,

1. Navigate to the **Permissions** tab, select the required user account and click **Add Permission**.
2. Click **Attach existing policies** directly under **Set Permissions** and search for "**AmazonRoute53FullAccess**".
3. Assign the listed policy and hit **Save**.
4. To generate the access key,
5. Select the particular user account and navigate to the **Security Credentials** tab.
6. In the window that opens, click **Create access** key.
7. An access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.

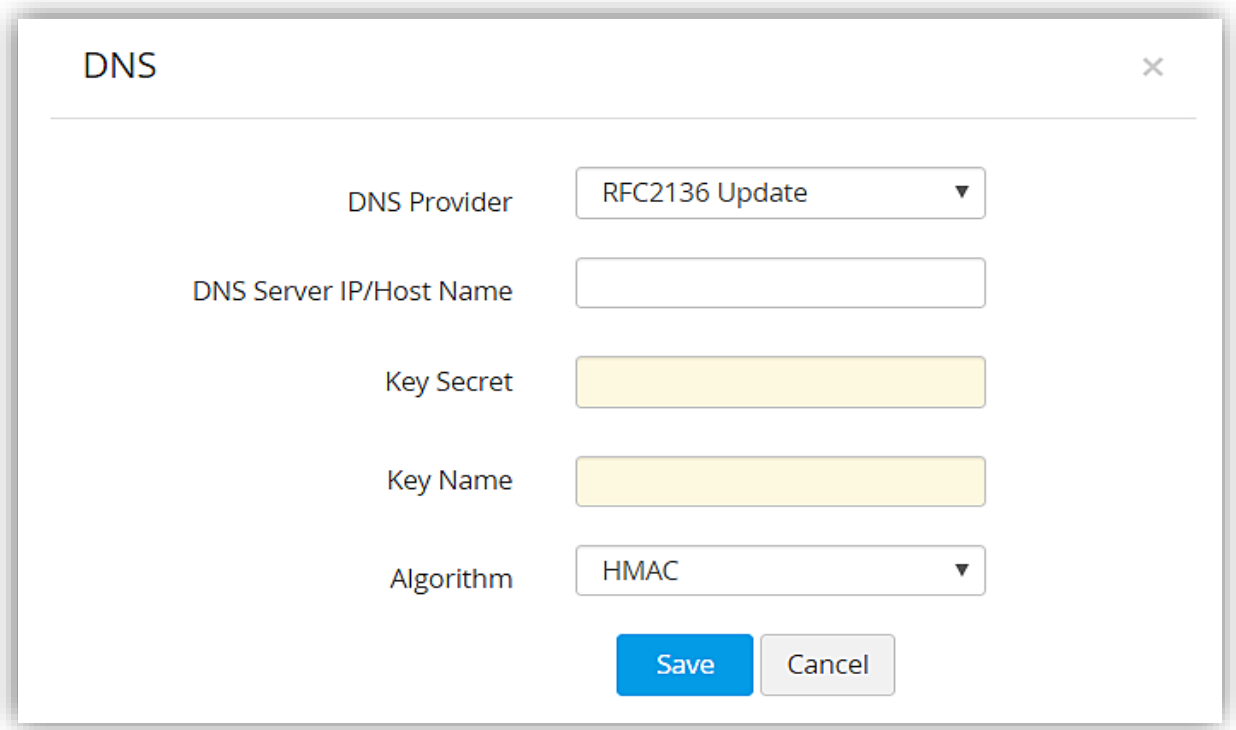


2.1.4 RFC2136 DNS Update

If you are using open source DNS servers such as Bind, PowerDNS etc., that support RFC2136 DNS update, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

1. The DNS Server IP / Hostname represents the server name / IP address in which the DNS server is installed or running.
2. The server details are found in the server installation directory. For instance, in the case of Bind9 DNS server, you can find these in the file named.local.conf in the server installation directory.

3. Provide the **Key Secret**, which is the key content found in the server installation directory.
4. Provide a name for the key, choose the signature algorithm and click **Save**.



2.1.5 GoDaddy DNS

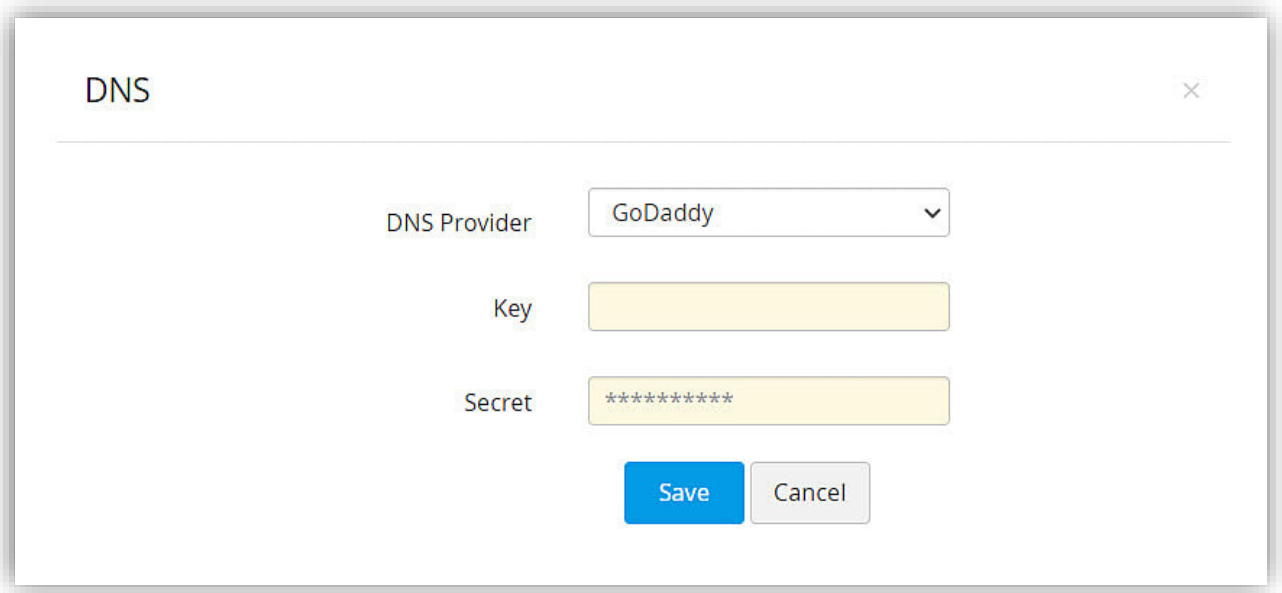
If you are using GoDaddy DNS for DNS validation, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

Steps to Obtain GoDaddy API Credentials:

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Log in to your GoDaddy account if you aren't logged in already.
3. Once you log in, you will be redirected to the API keys page where you can create and manage API keys. Click **Create New API** key.
4. Provide your application name, choose the environment type as **Production** and click **Next**.
5. The API key and its secret is generated. Copy and save the secret in a secure location, as it will not be displayed again.

Now, in the PAM360 interface, follow the below steps to add GoDaddy DNS to The SSL Store certificate repository:

1. Navigate to **Certificates >> The SSL Store** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **GoDaddy** from the DNS Provider drop-down menu.
4. Enter the **Key** and **Secret** that was previously generated from the GoDaddy portal. Click **Save**.



2.1.6 ClouDNS

If you are using ClouDNS for DNS validation, follow the steps below to automate the DNS-based domain control validation procedure using PAM360:

Steps to Obtain ClouDNS API Credentials:

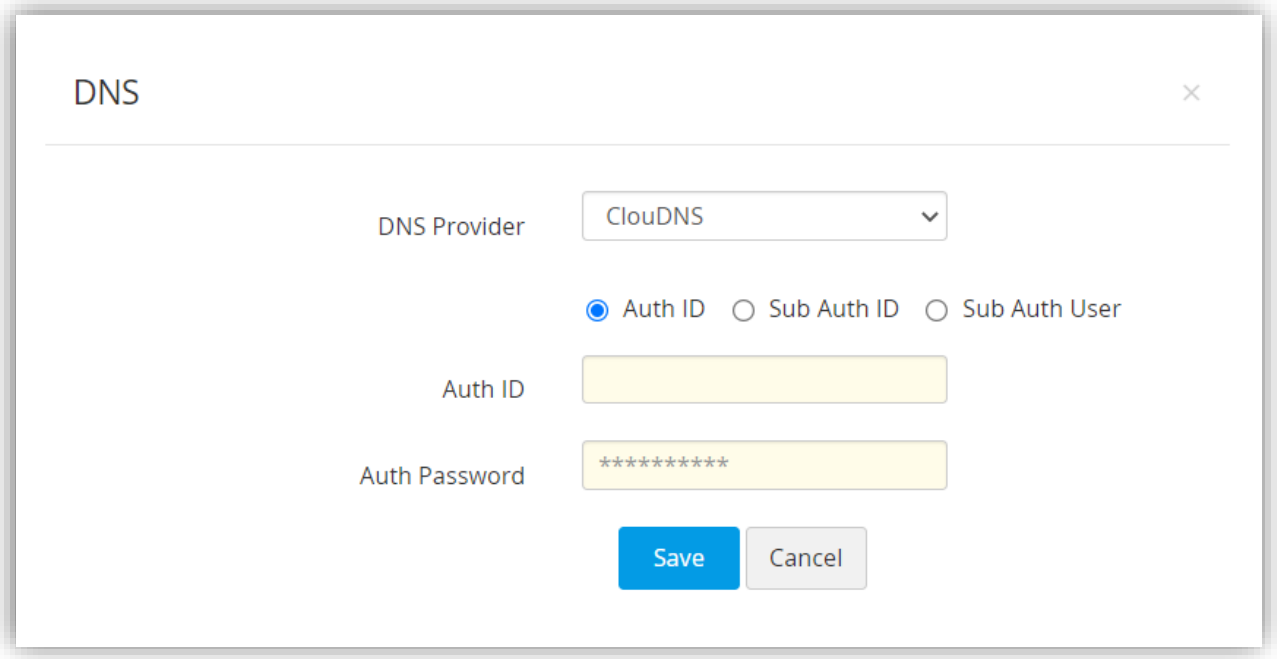
1. Login to your ClouDNS account and go to **Reseller API.**
2. If you have already created an API user id, you will find it under **API Users**. If not, click **Create API** to generate a new one.

Click here to learn more about ClouDNS API Auth IDs.

Now, in the PAM360 interface, follow the below steps to add ClouDNS to SSL Store CA:

1. Navigate to **Certificates >> SSL Store** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **ClouDNS** from the **DNS Provider** drop-down.

4. Choose one of the following options: **Auth ID, Sub Auth ID, Sub Auth User.**
5. Enter the chosen ClouDNS Auth ID, its respective **Auth Password**, and click **Save**.



3. Domain Validation, Certificate Issue, and Deployment

Prerequisite

If the end server in which you're deploying the challenge file is a Windows machine, follow the below steps to install the Windows agent:

1. Navigate to **Admin >> PAM360 Agents** and click **Windows Agent** under the required version: 32-bit or 64-bit.
2. Execute the following commands:

Installing PAM360 agent for Windows server:

To install PAM360 agent as a Windows service

1. Open the command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **AgentInstaller.exe install <Agent Key copied from the PAM360 UI>**.

To stop the agent and uninstall the Windows service

1. Open the command prompt and navigate to the PAM360 agent installation directory.
2. Execute the command **AgentInstaller.exe stop**.

Once the certificate authority receives your order, you will have to go through a process called **Domain control validation** (DCV) and prove your ownership over the domain upon the completion of which you will receive the certificate. PAM360 supports all the three DCV methods:

1. E-mail based DCV
2. File or HTTP based DCV
3. DNS based DCV

3.1 Email-based Domain Control Validation

1. In email based domain control validation, the certificate authority sends a verification email to the approver email ID specified when placing the certificate order.
2. This email will guide you through the steps that need to be performed in order to complete the domain control validation procedure.
3. After completing the steps, navigate to the PAM360 server, and switch to **Certificates>>The SSL Store™** tab.
4. Select the order and click check Order Status from the top menu.
5. On successful verification, the certificate authority issues the certificate which is

fetched and added to PAM360's secure repository. To access the certificate, navigate to the **Certificates** tab.

6. From here, deploy the certificate to necessary end-point servers such as a Certificate Store or an IIS server directly from PAM360.

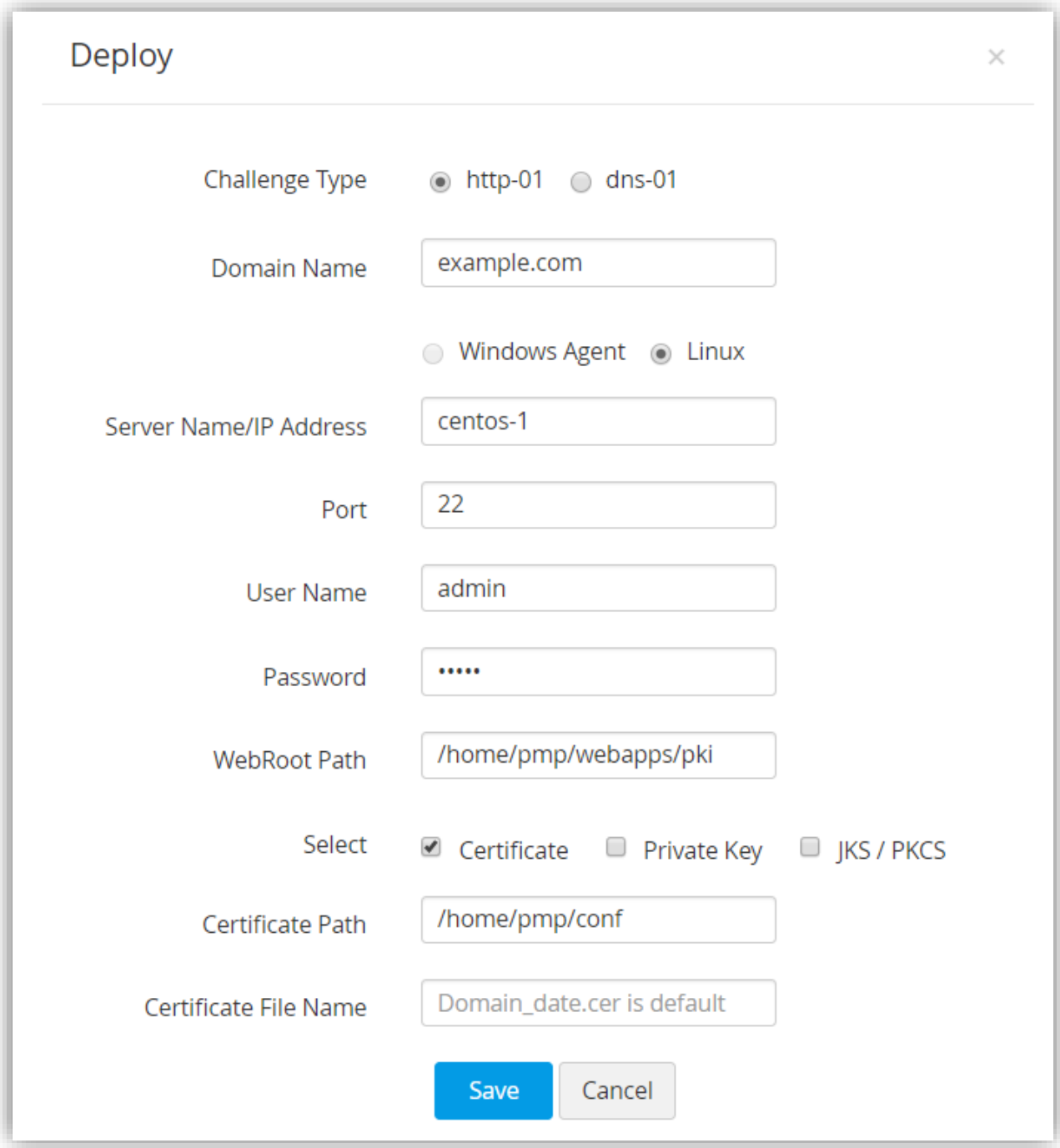
Click here for more details on certificate deployment.

3.2 File/HTTP-based Domain Control Validation

- If you have opted file / HTTP based domain control validation, a challenge file is displayed on creating the order.
- Navigate to the domain server, create the path specified and deploy the challenge file in that path.

This entire process of deploying the challenge file in the end-point server can be automated from PAM360. This can be achieved by configuring the server details in the Deploy tab under Manage. To automate domain control validation,

1. Navigate to **Certificates>>The SSL Store™ >> Manage.**
2. Switch to the **Deploy** tab and click **Add**.
3. In the pop-up that opens, choose the challenge type as **'http-01'** , specify the domain name, choose the server type (Windows or Linux) and enter the server details. Click **Save**.
4. The challenge file is automatically deployed to the corresponding end-server in the specified path.



5. Once you have deployed the challenge file, navigate to the PAM360 server, switch to **The SSL Store™** tab, choose the order and click **Check Order Status** from the top menu.
6. On successful domain validation, the certificate authority issues the certificate which is fetched, added to the **Certificates** tab in PAM360 and is also deployed in the specified path of the server configured earlier under **Manage** >> **Deploy**.

3.3 DNS-based Domain Control Validation

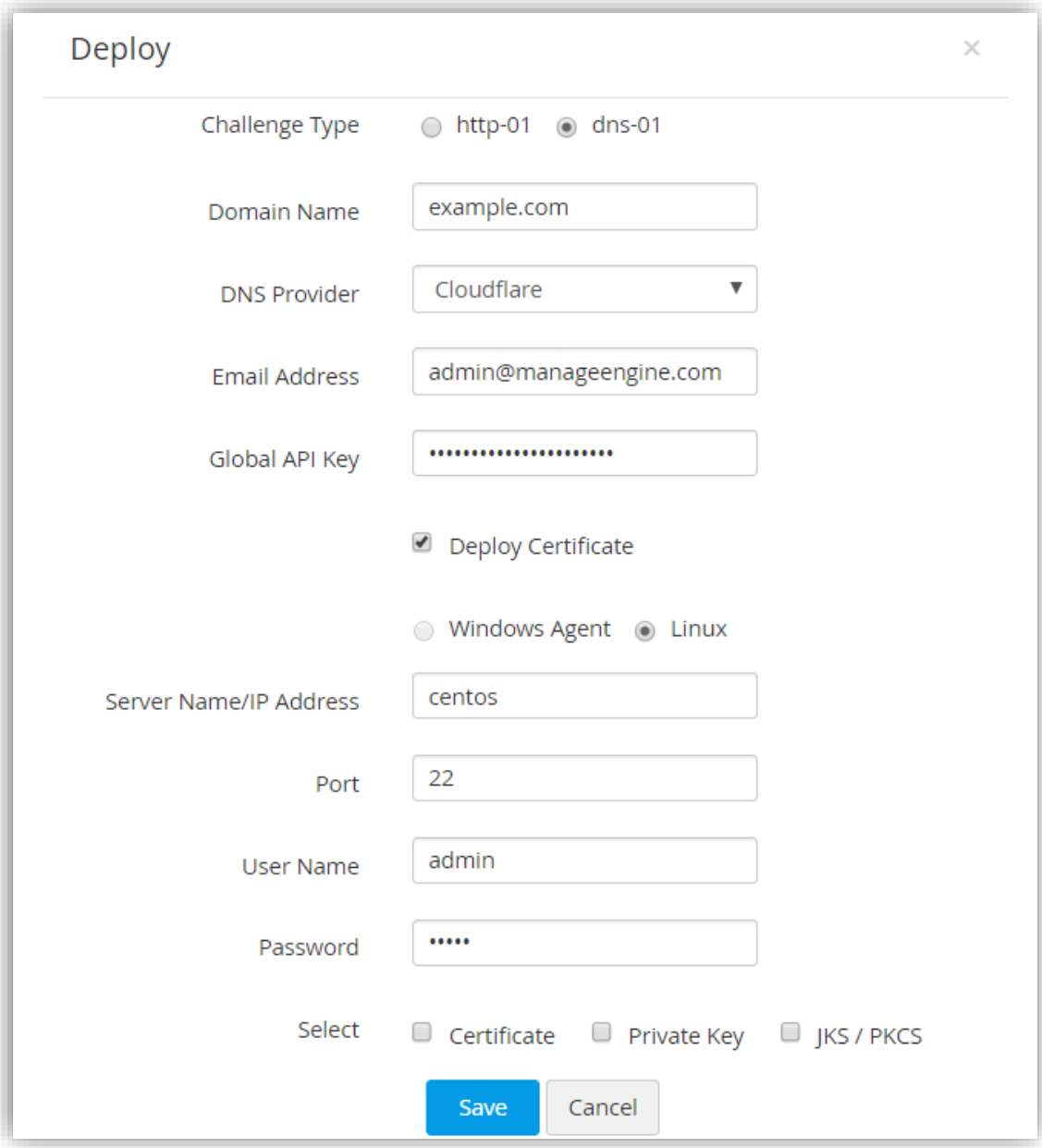
1. If you have opted for DNS based domain control validation, a DNS challenge value and

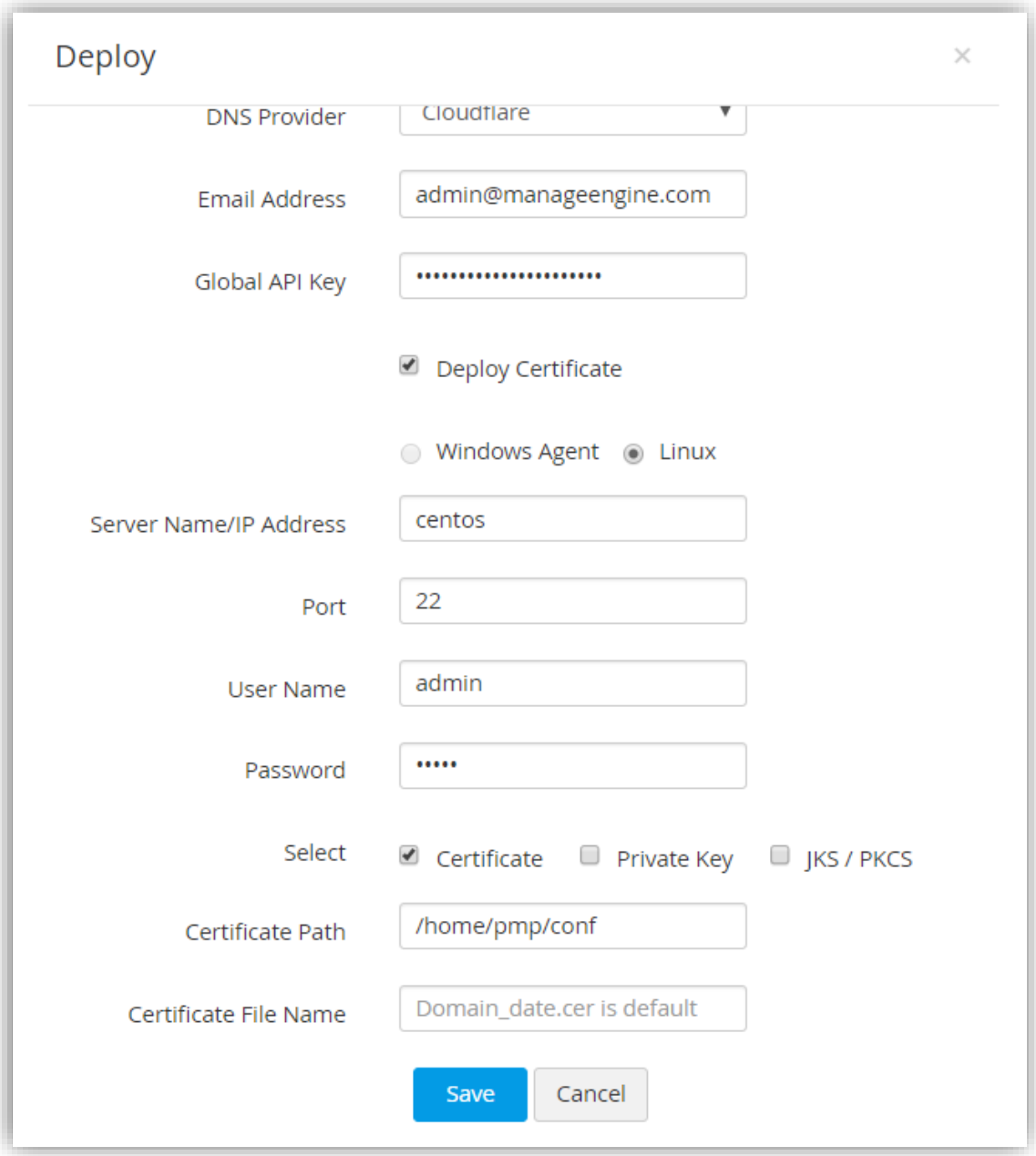
text record are displayed on creating the order.

2. Copy and paste the text records manually in the domain server.

Similar to the HTTP challenge, the entire challenge verification process can be automated from PAM360. This can be achieved by configuring the server details in the **Deploy** tab under **Manage**. To automate domain control validation,

1. Navigate to **Certificates >> The SSL Store™ >> Manage**.
2. If the end-server is a Windows machine, initially download and install the PAM360 agent for Windows server from the Windows Agents tab using the steps mentioned in the previous section.
3. Switch to the **Deploy** tab and click **Add**.
4. In the pop-up that opens, choose the challenge type as **'dns-01'**, specify the domain name, choose the DNS provider (Azure, Cloudflare DNS, Amazon route 53 DNS, RFC2136 DNS update (nsupdate), GoDaddy DNS, ClouDNS) and enter the server details.
5. Check 'Certificate' option to deploy the certificate to the end-server after procurement. Click **Save**.
6. The DNS challenge values and text records are automatically created in the corresponding DNS servers.


Deploy
Challenge Type
http-01
dns-01
Domain Name
example.com
DNS Provider
Cloudflare
Email Address
admin@manageengine.com
Global API Key
Deploy Certificate
Windows Agent
Linux
Server Name/IP Address
centos
Port
22
User Name
admin
Password
Select
Certificate
Private Key
JKS / PKCS
Save
Cancel



7. Once the challenges have been filled, navigate to the PAM360 server, switch to **Certificates >> The SSL Store™** tab, choose the order and click Order Status from the top menu.
8. On successful domain validation, the certificate authority issues the certificate which is fetched and automatically added to PAM360's certificate repository. To access the certificate, navigate to the **Certificates** tab.
9. From here, deploy the certificate to the necessary end-point servers such as a Certificate Store or an IIS server directly from PAM360. Click here for more details on certificate deployment.

10. Also, the certificate is automatically deployed to its corresponding end-server after issue, if you have enabled the Deploy Certificate option at the time of configuring server details under **Manage >> Deploy**.

Notes:

1. For DNS-based domain control validation, if you had chosen a DNS account configured under **Manage >> DNS** when placing the order, PAM360 automates challenge verification using that account. Instead, if you have already configured the domain and server details under **Manage >> Deploy**, the challenge verification, and subsequently the deployment of certificates is carried out for that specific domain and server alone.
2. For RFC2136 DNS update, if you have chosen Global DNS configuration, the domain name itself acts as the zone name (Global DNS configuration is possible only if you are using the same **Key Secret** for all zones). Whereas, if you have chosen domain-agent mapping, you have to provide the Zone name, Key Name, and Key Secret for each domain separately.

4. Renewing, Reissuing & Deleting Certificate Orders

You can renew, request reissue or delete certificate orders placed to third-party certificate authorities from PAM360.

To renew a certificate,

1. Navigate to **Certificate >> The SSL Store™**
2. Select the required order and click **Renew Certificate** from the top menu.
3. Complete the domain control validation (DCV) procedure if necessary.
4. On successful validation, the certificate is issued and the new version is automatically updated in the **Certificates** tab.

Note: You can request a reissue only for those certificates requested from PAM360 and not for the imported orders.

To delete a certificate request, follow the below steps

1. Navigate to **Certificates >> The SSL Store™**.
2. Select the required certificate and click **Delete** from the **More** menu.
3. The certificate request is deleted from PAM360.

Note: When a certificate request is deleted, it is removed only from PAM360. You can find the order in The SSL Store™ website for your account and import it into PAM360 if needed using **The SSL Store™ >> More >> Import** option.

Disclaimer: The procurement of public CA certificates from PAM360 can be successfully completed only if the user has signed up for an exclusive enterprise account with The SSL Store™. PAM360 imports certificates after issue using The SSL Store™'s API for providing better PKI management functionality. All personal information (including payment details) is collected and processed by The SSL Store™ and ManageEngine is not responsible for any payment related issues. Please contact The SSL Store™ technical support team if you face any difficulties with payment and procurement of certificates from public CAs affiliated with The SSL Store™ using PAM360.

Integrating PAM360 with DigiCert SSL Certificate Authority

PAM360 integrates with DigiCert certificate signing authority, allowing enterprises to automate the end-to-end management of web server certificates signed and issued by DigiCert, from a centralized platform. This document discusses the steps to manage the lifecycle of SSL certificates issued by DigiCert, directly from PAM360's web interface; these operations include importing existing orders, certificate requests, provisioning, deployment, and renewal of certificates.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to DigiCert's CA Services.

URL: https://www.digicert.com/services/v2/

Port: 443

Follow the step-by-step procedure below to integrate DigiCert with PAM360:

1. Configuring DigiCert CertCentral API Key Details
2. Pre-validating Organizations/Domains in DigiCert CertCentral
3. Importing Existing Orders
4. Creating a Certificate Order
5. Issuing Certificates
6. Managing Certificates

1. Configuring DigiCert CertCentral API Key Details

To request and manage DigiCert certificates from PAM360, you need to link your PAM360 account with your DigiCert CertCentral account. To achieve this, you must apply your CertCentral API key details in PAM360.

Case 1: Steps to Generate API Key in DigiCert CertCentral

If you do not have a DigiCert account already, follow the steps below to sign up for a new account:

1. Go to DigiCert's sign up page and fill in the required details.
2. Once the account is created, navigate to DigiCert's login page and log into the CertCentral portal using your DigiCert credentials.
3. Once logged in, generate your CertCentral API key by following the below steps.
    i. Go to **Automation** on the left pane of the CertCentral portal and click **Add API Key**.
    ii. In the window that opens, enter a Name and Description for the API key, assign a User. The user assigned should have admin privileges in digicert.
    iii. Click **Add**.
    iv. A new API key is generated and displayed in a different window. Copy the key and store it in a secure location, for it will not be displayed again.
    v. Click here for more about CertCentral account creation and API key generation process.
4. Once you have generated the API key, login to PAM360 and navigate to Certificates >> DigiCert.
5. You will be prompted to enter the API key. Provide the key details and click Save. (Remember, applying the API key in PAM360 is a one-time operation)

Now the key is saved and your CertCentral account is successfully linked to your PAM360 account.

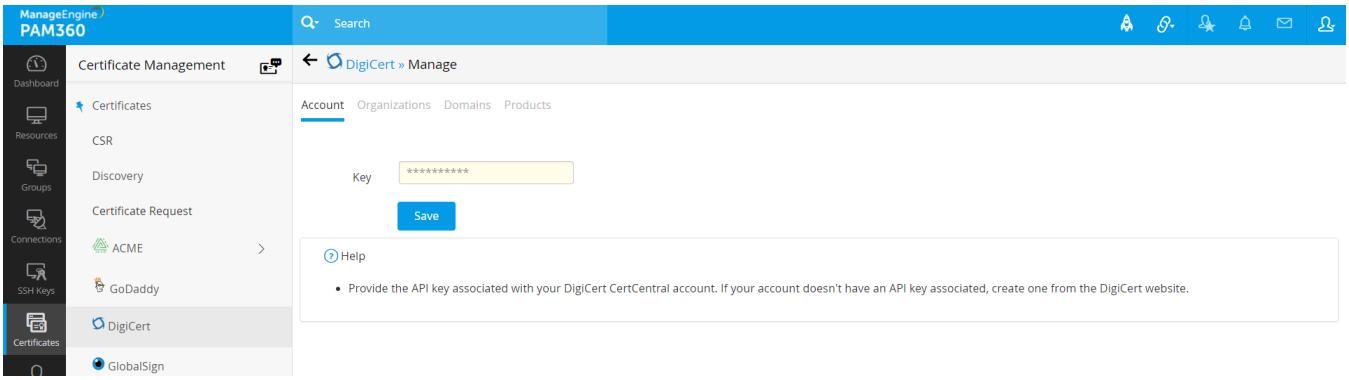
Case 2: You have a DigiCert account

If you have an account with DigiCert CertCentral already, all you have to do is generate your API key from the CertCentral portal and provide it in PAM360.

1. Login to your CertCentral account, and generate the API key using the steps mentioned above.
2. Once you have generated the API key, switch to PAM360 interface, navigate to **Certificates >> DigiCert**.
3. Click **Add**. Provide the **API key Name, Key** and click **Save**. This is a one-time operation.

4. The key is saved. Your CertCentral account is now successfully linked with your PAM360 account.

To delete an API key, select the key(s) you wish to delete and click Delete from the top pane. In the pop-up that appears, click **OK**.



2. Pre-validating Organizations/Domains in DigiCert CertCentral

(To be performed in the DigiCert CertCentral portal)

Before placing orders for DigiCert certificates from PAM360, you must have your domains/organizations pre-validated from the DigiCert CertCentral portal. Once the pre-validation process is complete, you can proceed with certificate issuance and renewals for those domains/organizations. Read more about the pre-validation process in the CertCentral user guide.

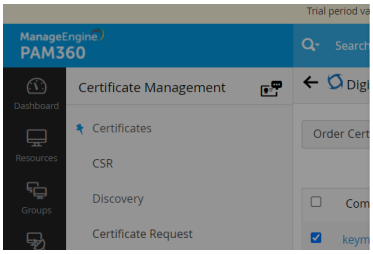
3. Importing Existing Orders

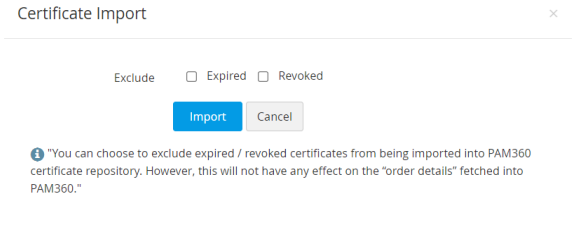
The next step is to import all certificate orders from your CertCentral portal into the PAM360 repository. Follow the below steps:

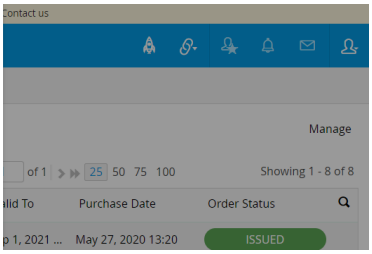
1. Navigate to **Certificates >> DigiCert** tab.
2. Click **Import Existing Orders** from the **More** drop down in the top bar.
3. Select the **Expired** or **Revoked** option to exclude the expired or revoked certificates from getting added to the PAM360 certificate repository during import. This can save the license count for SSL certificates in your installation without affecting the number of order details fetched into PAM360.

4. Once the required option is selected, click **Import**.

All the existing certificate orders associated with your DigiCert CertCentral account will be imported into the PAM360 repository.





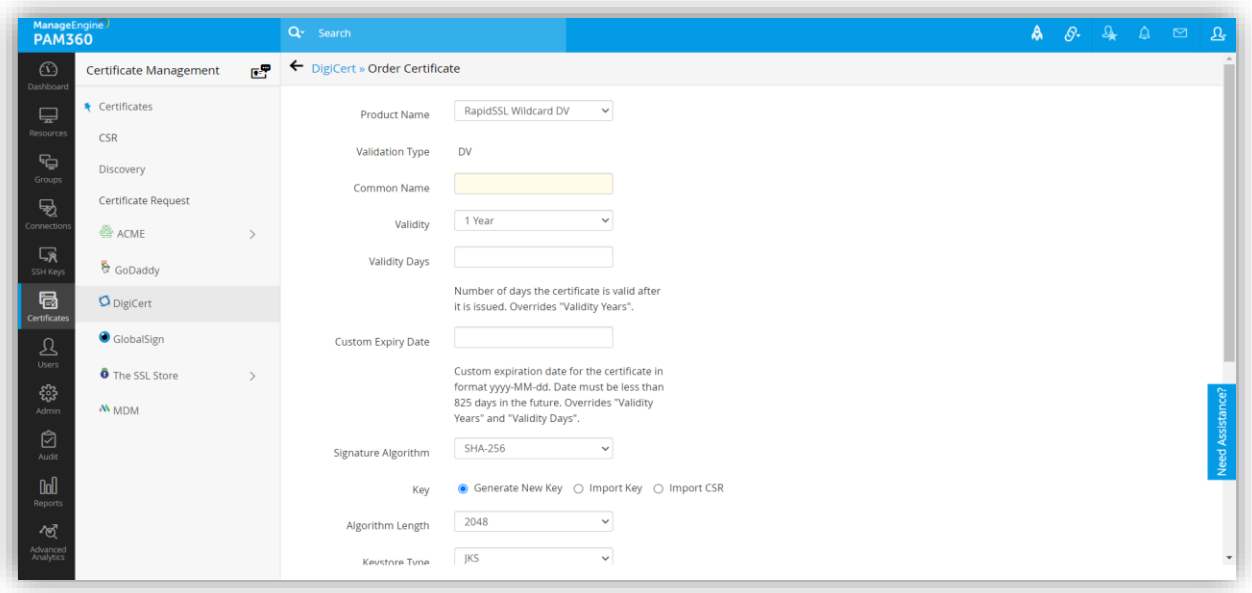


4. Creating a Certificate Order

Once you have successfully linked your CertCentral account to your PAM360 account by providing the API key details, you can place orders for DigiCert SSL/TLS certificates directly from the PAM360 interface.

Follow the below steps to place a new certificate order:

1. Navigate to **Certificates >> DigiCert** and click **Order Certificate.**
2. In the **Order Certificate** window, choose the **Product Name**, **Validity**, **Signature Algorithm**, Algorithm Length, **Keystore Type**, **Server Platform, Payment Method** and **Organization**.
3. Enter the **Common Name**. You can also specify the **Validity** in number of days, or enter a **Custom Expiration Date**.
4. After filling in the details, click **Create**.



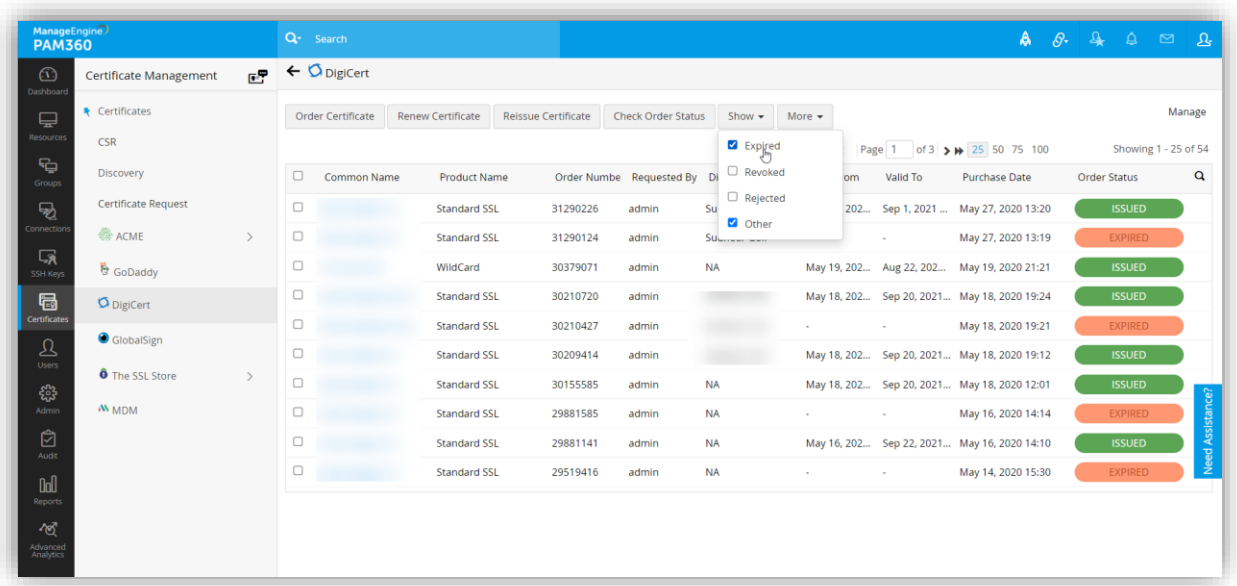
Notes:

- Product name, payment, and organization fields are fetched and displayed according to the permissions provided in the CertCentral portal.
- For certificate validity, the value given for **Custom Expiry Date** overrides the values given for **Validity Days** and **Validity** in years. The value given for **Validity Days** overrides the value given for **Validity**.
- The payment for orders placed from PAM360 is handled by the CertCentral portal. If you face any issues with the payment, please contact the CertCentral customer support team.

5. Issuing Certificates

1. Once a certificate order is successfully created, you can view it under **Certificates >> DigiCert** tab along with the certificate order status.
2. To track the certificate availability for an order, select the order and click **Check Order Status** from the top bar. The order status is checked automatically through a schedule every day. During the scheduled check if the certificate is available, it is fetched and added to the PAM360 certificate repository.
3. To track the validation status for domains/organizations from PAM360, choose an order and click **More >> Check Validation Status** from the top menu.

4. To filter your order view according to the order status, click the **Show** drop-down from the top menu and select from the options **Expired**, **Revoked**, or **Rejected** to customize your repository display. For other statuses such as **Issued** or **Pending**, select the **Other** option.



> **Note:** Certificates issued are automatically added to the PAM360 repository only if you have the required license count. If not, you need to purchase an add-on for more keys and certificates before attempting to import new certificates.

6. Managing Certificates

Follow the below steps to renew, revoke, delete or request reissue for certificates or cancel certificate orders from PAM360.

Navigate to **Certificates >> DigiCert**.

6.1 Renewing a Certificate

1. Select the required certificate and click **Renew Certificate** from the top bar.
2. Ensure that you have the domain(s) / organization pre-validated from CertCentral portal before requesting for a renewal.
3. On successful validation, certificate is issued and automatically added to the PAM360 certificate repository.

6.2 Requesting for a Certificate Reissue

1. Select the required certificate and click **Reissue Certificate** from the top bar.
2. Ensure that you have the domain(s) / organization pre-validated from CertCentral portal before requesting for a certificate reissue.
3. On successful validation, the certificate is reissued and automatically added to the PAM360 certificate repository.

6.3 Revoking a Certificate

1. Select the required certificate and click **Revoke Certificate** from the **More** dropdown in the top bar.
2. The certificate is revoked. Switch to **Certificates** tab and delete the certificate to remove it from the PAM360 repository.

6.4 Deleting a Certificate Request

1. Select the required order and click **Delete** from the **More** dropdown in the top bar.
2. The certificate request is deleted from PAM360.

6.5 Canceling a Certificate Order

1. Select the required order and click **Cancel Order** from the **More** dropdown in the top bar.
2. The certificate order is canceled.

Integrating PAM360 with GlobalSign SSL Certificate Authority

PAM360 facilitates integration with GlobalSign Certificate Authority (CA), making it possible for enterprises to automate the end-to-end management of web server certificates signed and issued by GlobalSign from a centralized platform. This document discusses the steps to manage the entire lifecycle of SSL certificates issued by GlobalSign, directly from the PAM360 web interface—right from importing existing orders, certificate request and provisioning, to deployment, renewal and thereupon.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to the GlobalSign's CA Services.

URL: https://system.globalsign.com/kb/ws/v1

Port: 443

1. **Steps to add GlobalSign account into PAM360**
2. **Placing a certificate order**
3. **Domain Control Validation, Certificate Issue & Deployment**
4. **Managing SSL Certificates Issued by GlobalSign CA**

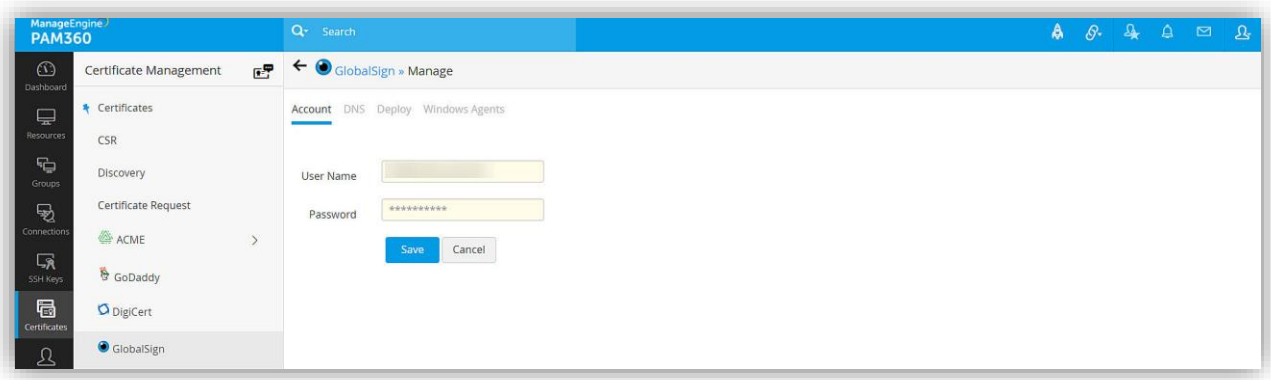
1. Steps to Add GlobalSign Account into PAM360

Follow the below steps to add your GlobalSign account into PAM360:

1. Navigate to **Certificates >> GlobalSign** and enter your GlobalSign credentials for authentication.
2. Once your GlobalSign account is verified and added, you may proceed with the below

steps.

3. If the GlobalSign account fails to get added to PAM360, contact the GlobalSign support, get an exception for the user's IP address and try again.
4. In case of account add failure, the IP address will be available in the **Audit** section.



2. Placing a Certificate Order

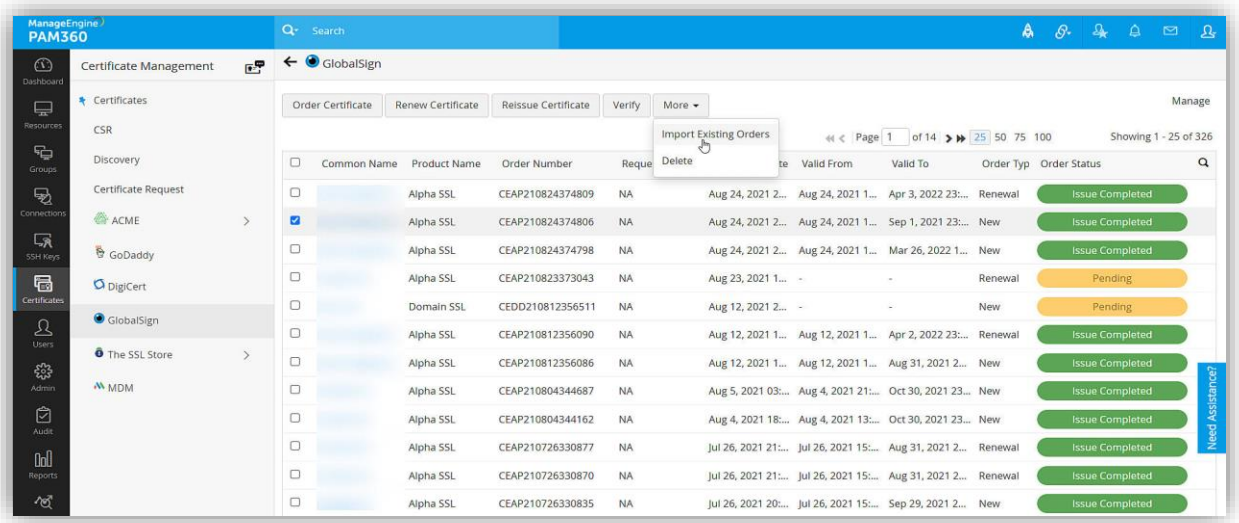
Once you have configured your GlobalSign credentials, you can now leverage GlobalSign's API to generate certificate signing requests (CSRs), place orders, procure, and manage certificates directly from PAM360.

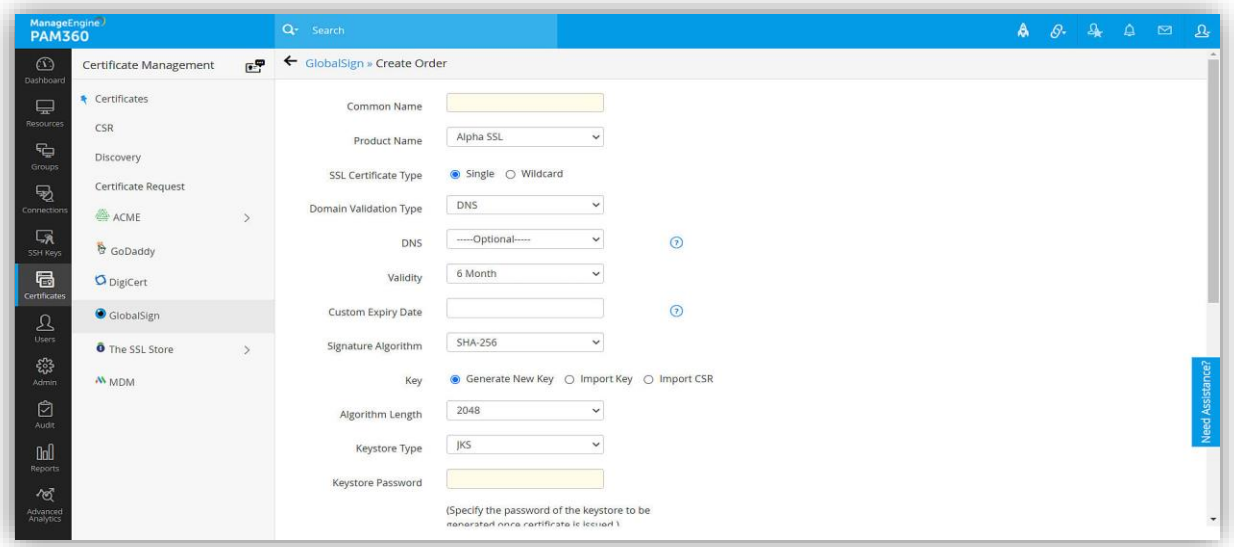
To generate a CSR and place a certificate order,

1. Navigate to the **Certificates >> GlobalSign.**
2. Click **Order Certificate.**
3. In the window that opens, enter the **Common Name, Product Name**, **SSL Certificate Type**, **Domain Validation type** and **Validity**.
4. PAM360 supports all the three domain control validation methods: DNS-based, file-based and email validation.
5. Then provide the SSL certificate type, signature algorithm, algorithm length, keystore type, keystore password, primary and secondary contact details. Users also have the option to import and use an already existing CSR or private key.
6. If the Product Name is chosen as Domain SSL, enter the SSL Certificate Type as **Single/Wildcard**.
7. For any Product Name other than Domain SSL, provide the UCC SAN and validity for the same.

8. The approver email ID is the email ID to which Domain Control Validation (DCV) verification mail will be sent. The approver email ID should take either of the following formats:
    - **<admin@domain>, <administrator@domain>, <hostmaster@domain>, <webmaster@domain> or <postmaster@domain>**
    - Any administrator, registrant, tech or zone contact email address that appears on the domain's WHOIS record and is visible to the CA system.
9. Then, provide the organization details (applicable for organization validation and extended validation order types only), administrator contact details and contact details of the technician placing the certificate order.
10. After filling in the details, click **Create**.
11. You will be taken to a window where you can see the list of certificate orders placed along with their statuses displayed to the right of the table view.

Note: PAM360 allows you to import the already existing certificate orders placed within your account from GlobalSign and track their statuses. Click **Import Existing Orders** from the **More** top menu to import the existing open orders into PAM360.

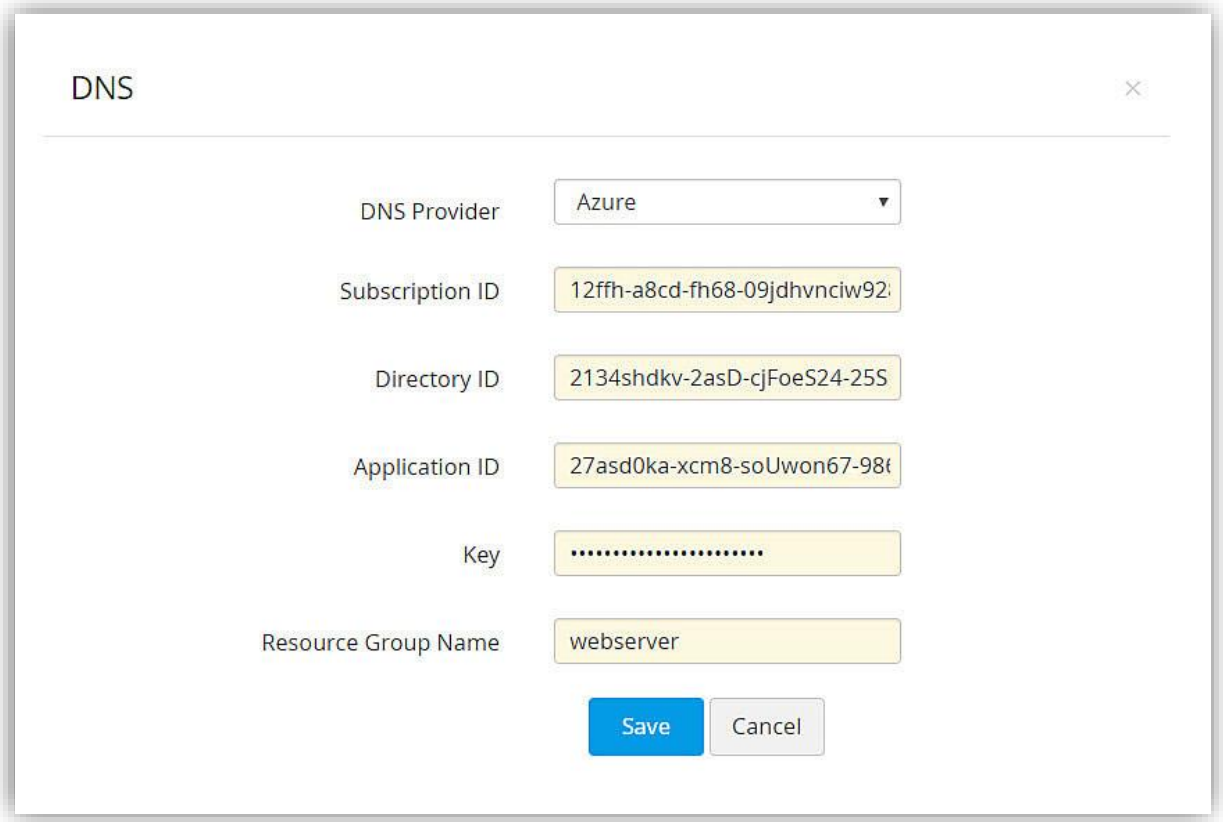




2.1 Configuring your DNS Account

If you are opting for DNS based domain validation in the certificate order, you should configure the DNS account in PAM360 and specify it in the 'DNS' field in the order for automating the challenge verification procedure. To configure your DNS account,

1. Navigate to **GlobalSign >> Manage.**
2. Switch to the **DNS** tab.
3. Here, you can add a maximum of one DNS account for each DNS provider supported. PAM360 currently supports automatic domain control validation for Azure, Cloudflare, Amazon Route 53 DNS, RFC2136 DNS update, ClouDNS, and GoDaddy DNS.
4. Click **Add**. In the pop-up that opens, choose the DNS provider.



2.1.1 Azure DNS

1. Provide the Subscription ID, which is available in the Overview page of the Azure DNS zone.
2. Provide the Directory ID, which is available in **Azure Active Directory >> Properties.**
3. If you have an already existing Azure application, provide its Application ID and Key.
4. If not, follow the steps mentioned below to create the Azure application and key, and give the application access to the DNS zones for making API calls.
5. To create the Azure application and key,
    i. Navigate to **App registrations >> New application registration**.
    ii. Provide the application name, select the application type Web app / API and provide the sign-on URL. Click **Create**.
    iii. After successful creation, you are directed to a window that displays the Application ID.
    iv. To get the application key, navigate to Keys and create a key.
    v. Provide the key description, duration and click **Save**.
    vi. Once the key is saved, key value is displayed. Copy and save the key value for future references.
6. To give the application access to DNS zones,

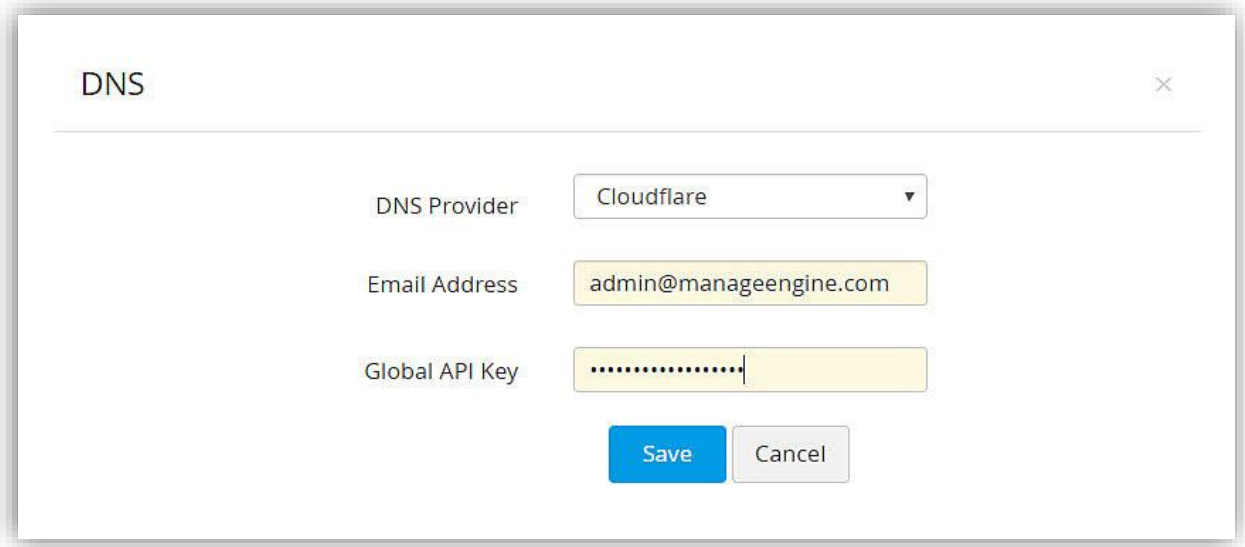
i. Navigate to the resource group where all DNS zones are created or switch to a specific DNS zone.
ii. Switch to Access Control (IAM) and click **Add**.
iii. Choose the role as Contributor, assign access to Azure AD user, group or application, search and select the application created in Azure Directory and click Save.
iv. The created Azure application is now given access to DNS zones for making API calls.

7. Finally, enter the Resource Group Name, which is the group name in which you have created the DNS zone and click **Save.**
8. Your DNS account details are saved and listed under **Manage >> DNS**.

2.1.2 Cloudflare DNS

1. In the Email address field, specify the email address associated with the Cloudflare account.
2. For Global API Key, use the 'Generate API' key option in the domain overview page of the Cloudflare DNS to generate the key and paste the value in this field.
3. Click **Save**. Your DNS account details are saved and listed under **Manage >> DNS**.

> **Note:** For DNS based domain validation type, if you are going to specify an already configured DNS account in the certificate order for domain control validation, make sure its status is marked Enabled under **Manage >> DNS**.



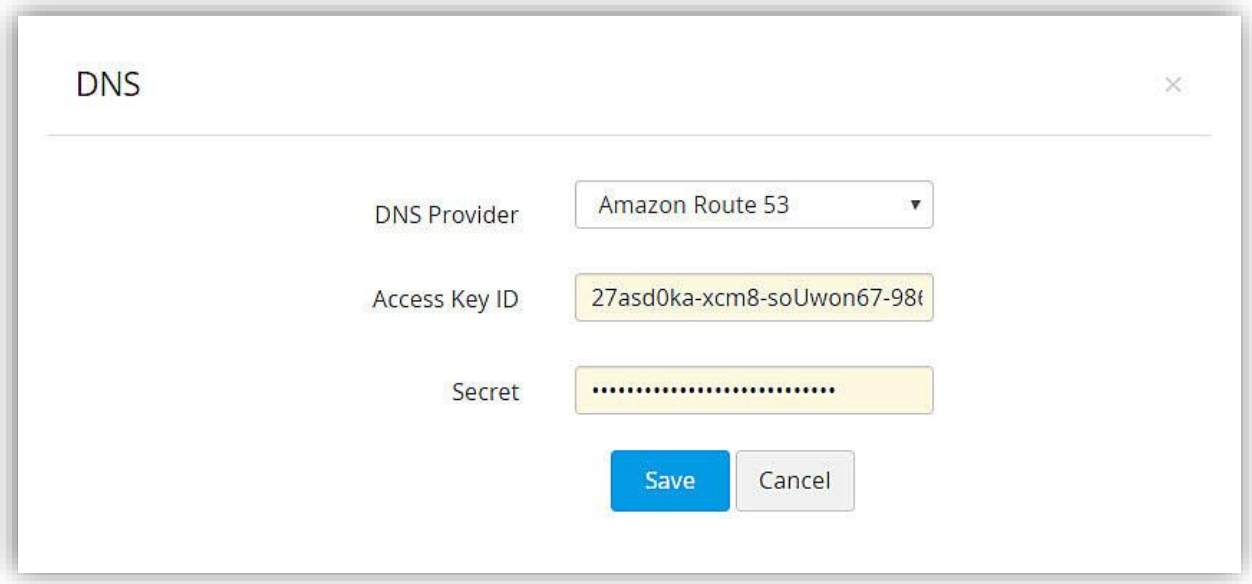
2.1.3 AWS Route 53 DNS

1. Generate and specify the Access Key ID and Secret associated with your AWS account.
2. If you do not have an AWS account, create one and generate the Access Key ID and Secret by following the steps given below:
    i. Login to the AWS console and navigate to IAM Services >> Users.
    ii. Click Add user.
    iii. Provide the user name and select the access type as Programmatic access.
    iv. Switch to the next tab, click Attach existing policies directly under Set Permissions and search for "AmazonRoute53FullAccess".
    v. Assign the policy that is listed and switch to the next tab.
    vi. In the tags section, add appropriate tags (optional) and switch to the next tab.
    vii. Review all the information entered and click Create user.
    viii. The user account is created and subsequently, an access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.
3. If you already have an AWS user account, you have to grant "**AmazonRoute53FullAccess**" permission to the user and generate the access key if the user doesn't have one. And if the user account has an access key associated already, it is just enough to ensure the required permission is granted.

To grant the required permissions, follow the below steps:

1. Navigate to the **Permissions** tab, select the required user account and click **Add Permission**.
2. Click **Attach** existing policies directly under **Set Permissions** and search for "**AmazonRoute53FullAccess**".
3. Assign the listed policy and hit **Save**.
4. To generate the access key,
    i. Select the particular user account and navigate to the **Security Credentials** tab.
    ii. In the window that opens, click **Create access key**.
    iii. An access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.

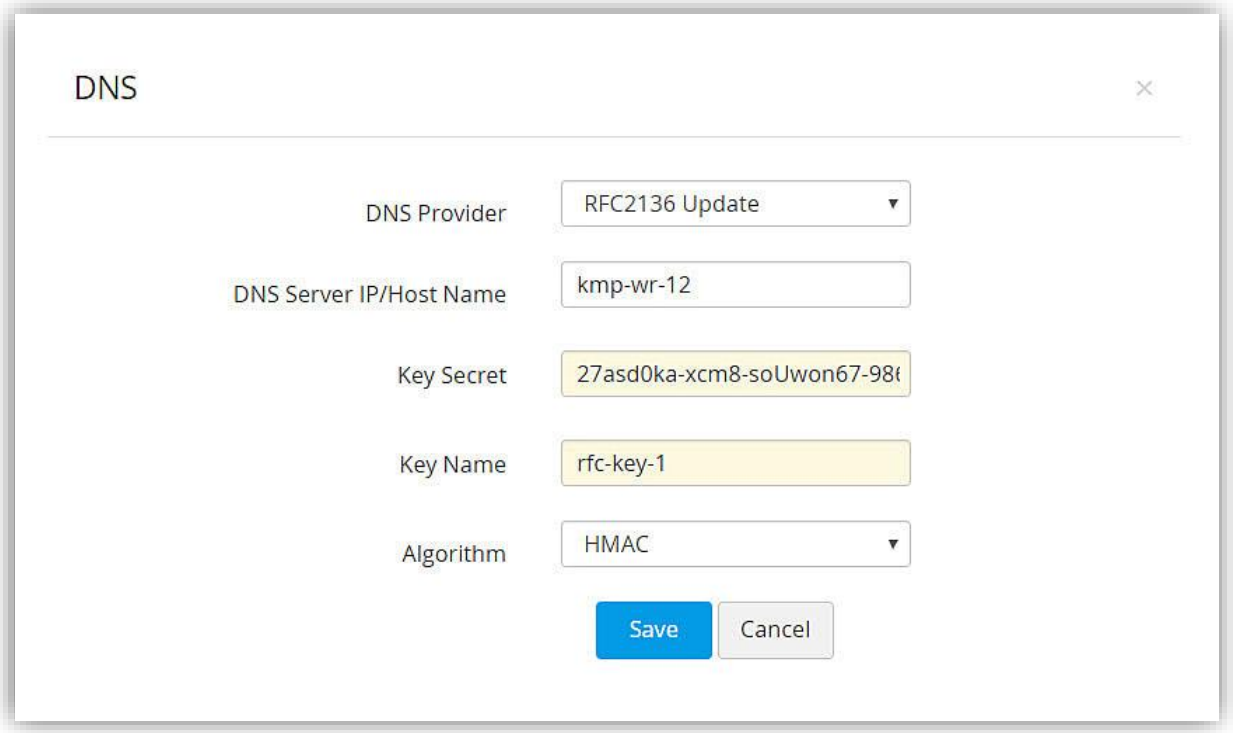
In the PAM360 interface, go to the **Certificates** tab, **Manage >> DNS** and enter the following details for Amazon Route 53:



2.1.4 RFC2136 DNS Update

If you are using open source DNS servers such as Bind, PowerDNS etc., that support RFC2136 DNS update, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

1. The DNS Server IP / Hostname represents the server name / IP address in which the DNS server is installed or running.
2. These details are usually found in the server installation directory. For instance, in the case of Bind9 DNS server, you can find these in the file named .local.conf in the server installation directory.
3. Provide the **Key Secret**, which is nothing but the key content found in the server installation directory.
4. Provide a name for the key, and choose the signature algorithm.
5. Click **Save**.



2.1.5 GoDaddy DNS

If you are using GoDaddy DNS for DNS validation, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

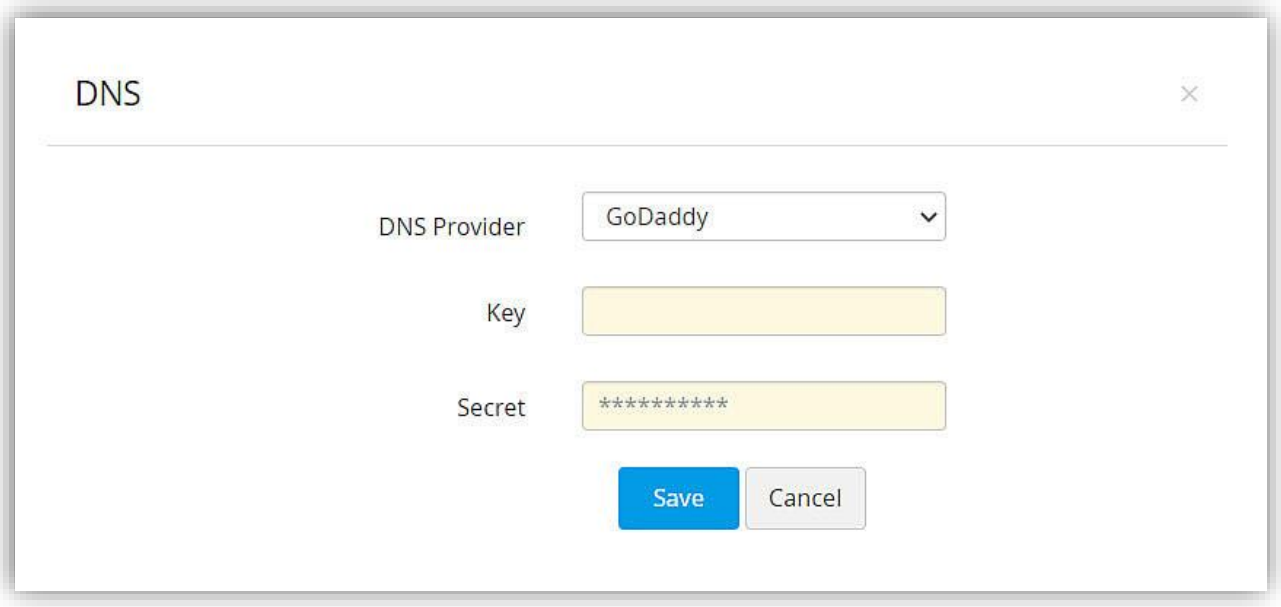
Steps to Obtain GoDaddy API Credentials:

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Log in to your GoDaddy account if you aren't logged in already.
3. Once you log in, you will be redirected to the API keys page where you can create and manage API keys. Click **Create New API** key.
4. Provide your application name, choose the environment type as **Production** and click **Next**.
5. The API key and its secret is generated. Copy and save the secret in a secure location, as it will not be displayed again.

Now, in the PAM360 interface, follow the below steps to add GoDaddy DNS to GlobalSign certificate repository:

1. Navigate to **Certificates >> GlobalSign** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.

3. Choose **GoDaddy** from the DNS Provider drop-down menu.
4. Enter the **Key** and **Secret** that was previously generated from the GoDaddy portal. Click **Save**.



2.1.6 ClouDNS

If you are using ClouDNS for DNS validation, follow the steps below to automate the DNS-based domain control validation procedure using PAM360:

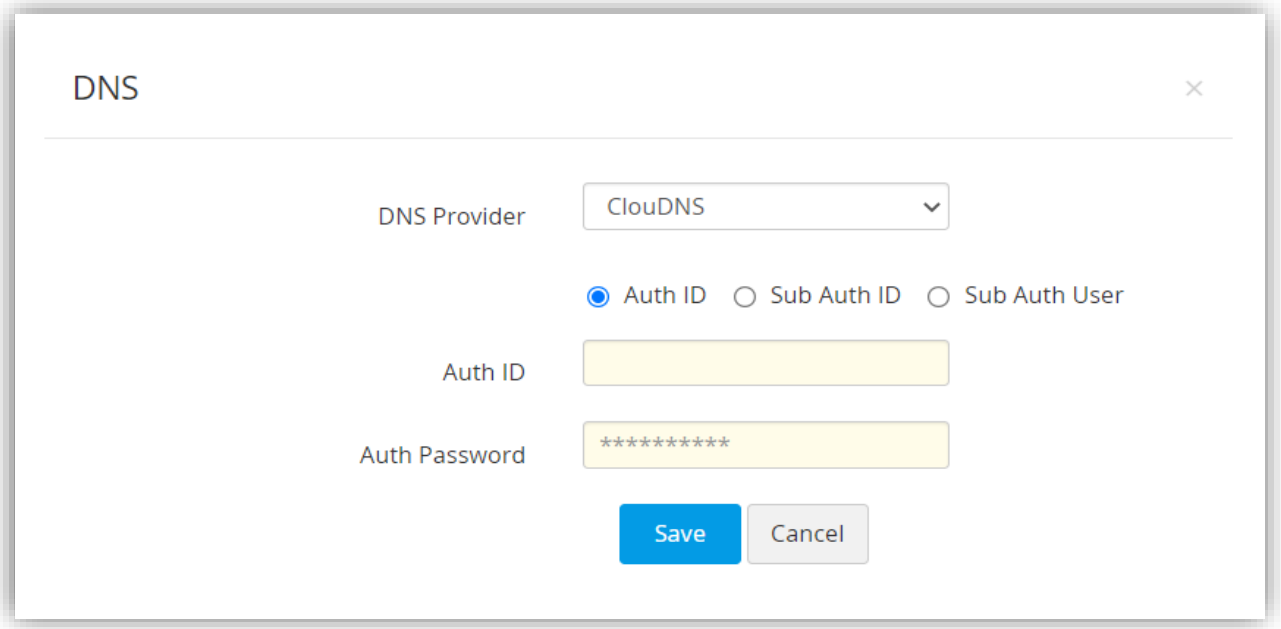
Steps to Obtain ClouDNS API Credentials:

1. Login to your ClouDNS account and go to **Reseller API.**
2. If you have already created an API user id, you will find it under **API Users**. If not, click **Create API** to generate a new one.

Click here to learn more about ClouDNS API Auth IDs.

Now, in the PAM360 interface, follow the below steps to add ClouDNS to GlobalSign CA:

1. Navigate to **Certificates >> GlobalSign** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **ClouDNS** from the **DNS Provider** drop-down.
4. Choose one of the following options: **Auth ID, Sub Auth ID, Sub Auth User.**
5. Enter the chosen ClouDNS Auth ID, its respective **Auth Password**, and click **Save**.



3. Domain Control Validation, Certificate Issue and Deployment

Once the certificate authority receives your order, you will have to go through a process called Domain control validation (DCV) and prove your ownership over the domain upon the completion of which you will receive the certificate. PAM360 supports all the three DCV methods:

1. E-mail based DCV
2. File or HTTP based DCV
3. DNS based DCV

3.1 E-mail based Domain Control Validation

1. In email based domain control validation, the certificate authority sends a verification email to the approver email ID specified when placing the certificate order.
2. This email will guide you through the steps that need to be performed in order to complete the domain control validation procedure.
3. After completing the steps, navigate to the PAM360 server, and switch to the GlobalSign tab.
4. Select the order and click **Verify** from the top menu.

5. On successful verification, the certificate authority issues the certificate which is fetched and added to PAM360's secure repository. You can access the certificate from the **Certificates >> Certificates** tab.
6. From here, you can deploy the certificate to necessary end-point servers such as a Certificate Store or an IIS server directly from PAM360.

Click here for more details on certificate deployment.

3.2 File / HTTP based Domain Control Validation

1. If you have opted file / HTTP based domain control validation, a challenge file is displayed on creating the order.
2. Navigate to the domain server, create the path specified and deploy the challenge file in that path.

This entire process of deploying the challenge file in the end-point server can be automated from PAM360. This can be achieved by configuring the server details in the **Deploy** tab under **Manage**. If the end-server is a Windows machine, complete the below procedure before proceeding:

Prerequisite:

If the end-server is a Windows machine, download and install the Key Manager Plus agent for Windows from **Certificates >> Discovery >> Agent** and then follow the below steps:

To install Key Manager Plus agent and start as a Windows service:

- Open the command prompt and navigate to the PAM360 installation directory.
- Execute the command '**AgentInstaller.exe start**.'

To stop the agent and uninstall the Windows service:

- Open the command prompt and navigate to the PAM360 installation directory.
- Execute the command '**AgentInstaller.exe stop**.'

To automate domain control validation, follow the below steps:

1. Switch to **GlobalSign >> Manage.**
2. Go to the **Deploy** tab and click **Add**.
3. In the pop-up that opens, choose the challenge type as 'http-01', specify the domain name, choose the server type (Windows or Linux) and enter the server details. Click **Save**.
4. The challenge file is automatically deployed to the corresponding end-server in the specified path.
5. Once you have deployed the challenge file, navigate to the PAM360 server, switch to the **GlobalSign** tab, choose the order and click **Verify** from the top menu.
6. On successful domain validation, the certificate authority issues the certificate which is fetched, added to PAM360 certificate repository (**Certificates >> Certificates**).

3.3 DNS based Domain Control Validation

1. If you have opted DNS based domain control validation, a DNS challenge value and text record are displayed on creating the order.
2. Copy and paste the text records manually in the domain server.

Similar to the HTTP challenge, the entire challenge verification process can be automated from PAM360. This can be achieved by configuring the server details in the Deploy tab under Manage. To automate domain control validation, follow the below steps:

1. Switch to **GlobalSign >> Manage**.
2. If the end-server is a Windows machine, download and install the PAM360 agent for Windows using the steps mentioned in the prerequisite section.
3. Switch to the **Deploy** tab and click **Add**.
4. In the pop-up that opens, choose the challenge type as 'dns-01', specify the domain name, choose the DNS provider (Azure, Cloudflare, Amazon Route 53 DNS, RFC2136 DNS update, ClouDNS, and GoDaddy DNS.) and enter the server details.
5. Check **'Deploy Certificate'** option to deploy the certificate to the end-server after procurement. Click **Save**.
6. The DNS challenge values and text records are automatically created in the corresponding DNS servers.
7. Once the challenges have been fulfilled, navigate to the PAM360 server, switch to the

GlobalSign tab, choose the order and click **Verify** from the top menu.

8. On successful domain validation, the certificate authority issues the certificate which is fetched and automatically added to PAM360 certificate repository. You can access the certificate from the **Certificates >> Certificates** tab.
9. From here, you can deploy the certificate to the necessary end-point servers such as a Certificate Store or an IIS server directly from PAM360. Click here for more details on certificate deployment.

Notes:

1. For DNS based domain control validation, if you had chosen a DNS account configured under **Manage >> DNS** when placing the order, PAM360 automates challenge verification using that account. Instead, if you have already configured the domain and server details under **Manage >> Deploy**, the challenge verification, and subsequently the deployment of certificates is carried out for that specific domain and server alone.
2. For RFC2136 DNS update, if you have opted Global DNS configuration, the domain name itself acts as the zone name (Global DNS configuration is possible only if you are using the same Key Secret for all zones). Whereas, if you have opted domain-agent mapping, you have to provide the Zone name, Key Name, and Key Secret for each domain separately.

4. Managing SSL Certificates Issued by GlobalSign CA

You can renew, request reissue or delete certificate orders placed to third-party certificate authorities from PAM360.

4.1 Renewing certificates

1. Navigate to **Certificates >> GlobalSign**
2. Select the required order and click **Renew Certificate** from the top menu.
3. Complete the domain control validation (DCV) procedure if necessary.
4. On successful validation, the certificate is issued and the new version is automatically updated in **Certificates >> Certificates** tab.

Certificate renewal is allowed only 90 days before the expiry date of the selected certificate.

4.2 Requesting for a certificate reissue

1. Navigate to **Certificates >> GlobalSign**.
2. Select the required order and click **Reissue Certificate** from the top menu.
3. The certificate is reissued and automatically updated in the **Certificates >> Certificates** tab.

4.3 Verifying a certificate request

1. Navigate to **Certificates >> GlobalSign**.
2. Select a certificate order which is pending in PAM360 and click **Verify** from the top menu
3. If the selected certificate is a **Domain Validation** certificate, then PAM360 will perform Domain Verification and URL Verification with GlobalSign and issue the certificate once the verification is complete. The issued certificate will be added to the SSL certificate repository in PAM360.
4. If the selected certificate is not a Domain Validation certificate, then PAM360 will fetch the status of the certificate alone from GlobalSign.

4.4 Deleting a certificate request

1. Navigate to **Certificates >> GlobalSign**
2. Select the required certificate and click **Delete** from the **More** top menu.
3. The certificate request is deleted from PAM360.

> **Note:** When a certificate request is deleted, it is removed only from PAM360. You can find the order being open in the GlobalSign website for your account and you can import it into PAM360 if needed using **GlobalSign >> More >> Import Existing Orders**.

Integration with Buypass Go SSL

PAM360 facilitates integration with Buypass Go SSL — the certificate authority (CA) that uses the Automatic Certificate Management Environment (ACME) protocol to provide secure SSL certificates free of cost. This integration with Buypass Go SSL helps you achieve an end-to-end life cycle management of Buypass Go SSL certificates installed on your domains from a single interface. This document discusses the steps you should follow to establish a connection with your Buypass Go SSL account, acquire, deploy, renew and perform all certificate management related operations from PAM360.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to Buypass Go SSL's CA Services.

Production URL: https://api.buypass.com/acme/directory

Staging URL: https://api.test4.buypass.no/acme/directory

Port: 443

Follow the step-by-step procedure below to integrate Buypass Go SSL with PAM360:

1. Create a Buypass Go SSL Account
2. Raise a Certificate Request
3. Buypass Go SSL Challenge Verification
4. Procure and Save the Certificate
5. Renew Certificates
6. Revoke Certificates
7. Delete Certificates

1. Create a Buypass Go SSL Account

To begin the process of requesting SSL certificates from Buypass Go SSL, you must create an account. This is a one-time process and can be done directly from the PAM360 interface.

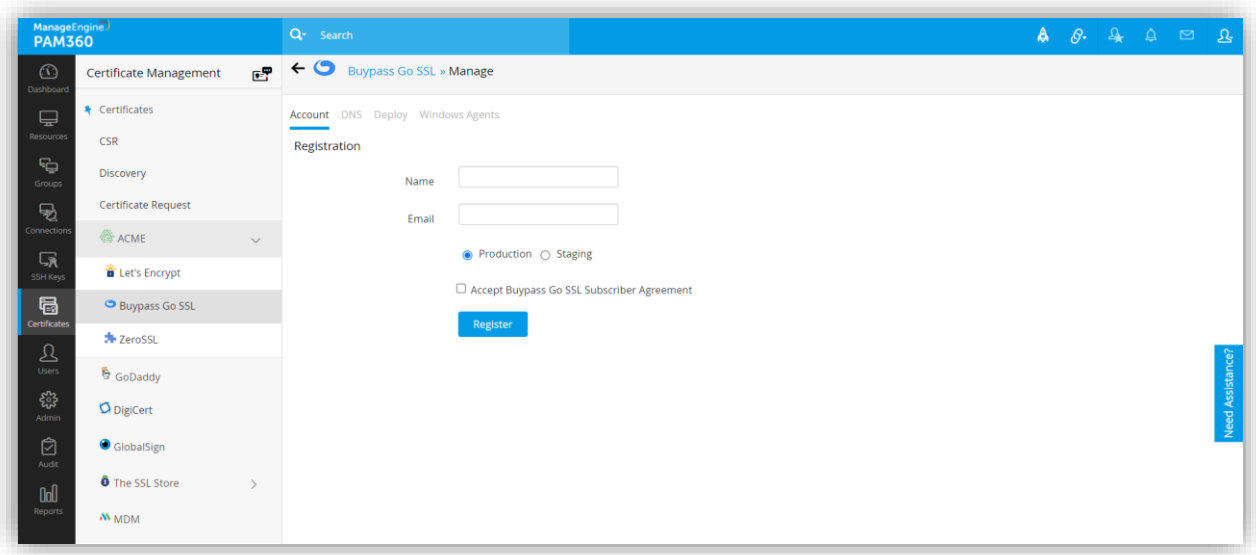
1. To create a Buypass Go SSL account, navigate to the **Certificates** tab, click the **ACME** drop-down and select **Buypass Go SSL**.
2. Click **Manage**. Under the **Account** tab, click **New Registration**.
3. In the pop-up, enter an account name and a valid e-mail address. Choose **Production** or **Staging**, based on your requirement.
4. Click the checkbox to accept the Buypass Go SSL Subscriber Agreement.
5. Click **Register**. Now, an account with Buypass Go SSL is created.

Once your account is created, you can update the account email address, delete it from PAM360, or deactivate the account entirely. Please note that deleting the account only removes it from PAM360. Even if you delete the account here, it will still be active in the Buypass Go SSL portal. To add the same account back to PAM360, export the key and use the **Add Account** option with the same details used before.

However, if you select the **Deactivate** option while deleting the account, then the Buypass Go SSL account will be removed completely and you cannot add it back to PAM360 with the same details.

Notes:

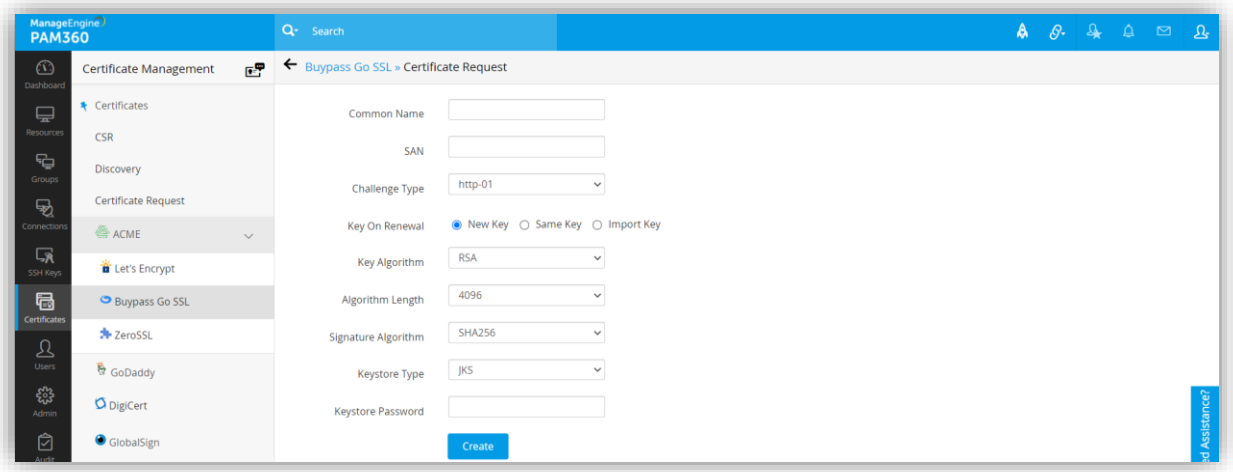
1. Only the users who are assigned with the 'ACME' role under 'SSH Keys and Certificates' user roles can perform the above operation. Go to **Admin >> Customization >> Roles** to activate this user role.
2. Only one Buypass Go SSL account can be created from PAM360.



2. Raise a Certificate Request

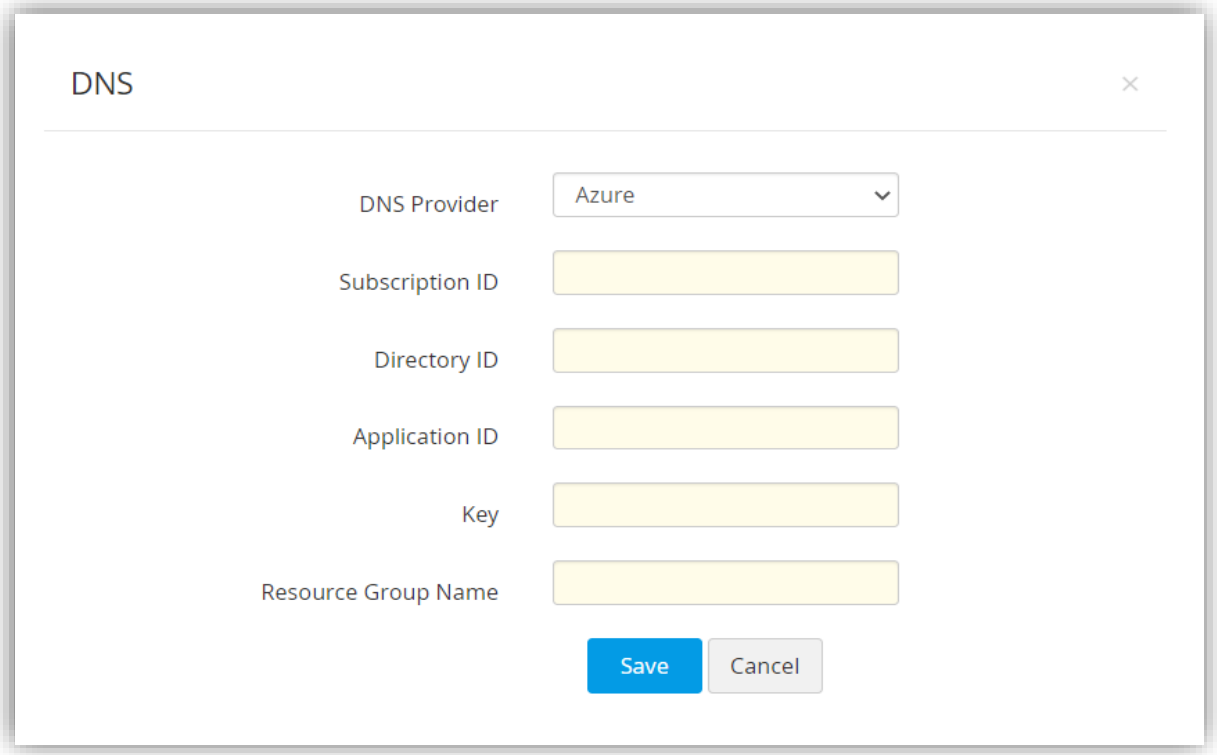
Once your Buypass Go SSL account is registered, you can proceed with raising certificate requests to the CA. To complete a certificate request, you will be presented with a challenge verification to fulfill in order to validate your domain and issue the certificate you have requested.

1. Navigate to **Certificates >> Acme >> Buypass Go SSL.**
2. Click **Certificate Request.** Fill in the domain name, select the challenge type, choose the key algorithm, algorithm length, signature algorithm, keystore type, enter the keystore password and click **Create**.
3. For dns-01 challenge type, you can choose and assign a DNS account from the drop-down if you have already configured your DNS credentials. This will be used for automatic challenge verification for all the domains specified in the request.
4. Also, you have options to change the private key whenever the certificate is renewed.
5. If you need to change the key, use **New Key**. This option will generate a new key every time the certificate is renewed.
6. If you want to retain the same key on renewal, use the **Same Key** option.
7. To use your own key, use the **Import Key** option. This key will be used for the first time when the certificate is generated and also for subsequent renewals.



To configure your DNS account, follow the below steps:

1. Navigate to **Buypass Go SSL >> Manage.** Switch to the **DNS** tab.
2. Here, you can add a maximum of one DNS account for each DNS provider supported. PAM360 currently supports automatic challenge verification for Azure DNS, CloudFlare DNS, and Amazon Route 53 DNS, RFC2136 DNS update (nsupdate), GoDaddy DNS, and ClouDNS. Click Add.
3. In the pop-up that opens, choose the DNS provider.



2.1 Azure DNS

1. Provide the Subscription ID, which is available in the Overview page of the Azure DNS zone.
2. Provide the Directory ID, which is available in Azure Active Directory >> Properties.
3. If you have an already existing Azure application, provide its Application ID and Key.
4. If not, follow the steps mentioned in this document to create the Azure application and key, and give the application access to the DNS zones for making API calls.
5. Finally, enter the Resource Group Name, which is the group name in which you have created the DNS zone and click Save.
6. Your DNS account details are saved and listed under Manage >> DNS.

2.2 Cloudflare DNS

1. In the Email address field, specify the email address associated with the Cloudflare account.
2. For Global API Key, use the **Generate API** key option in the domain overview page of the Cloudflare DNS to generate the key and paste the value in this field. Click Save.
3. Your DNS account details are saved and listed under **Manage >> DNS**.

2.3 AWS Route 53 DNS

Generate and specify the Access Key ID and Secret associated with your AWS account. If you do not have an AWS account, create one and generate the Access Key ID and Secret by following the steps given below:

1. Login to the AWS console and navigate to **IAM Services >> Users**. Click **Add user.**
2. Provide the user name and select the access type as **Programmatic access**.
3. Switch to the next tab, click Attach existing policies directly under Set Permissions and search for "AmazonRoute53FullAccess".
4. Assign the policy that is listed and switch to the next tab. In the tags section, add appropriate tags (optional) and switch to the next tab.
5. Review all the information entered and click Create user.
6. The user account is created and subsequently, an access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.

7. If you already have an AWS user account, you have to grant "AmazonRoute53FullAccess" permission to the user and generate the access key if the user doesn't have one. if the user account has an access key associated already, it is just enough to ensure the required permission is granted.

To grant the required permissions:

1. Navigate to the **Permissions** tab, select the required user account and click **Add Permission**.
2. Click Attach existing policies directly under Set Permissions and search for "AmazonRoute53FullAccess".
3. Assign the listed policy and hit Save.
4. To generate the access key,
5. Select the particular user account and navigate to the Security Credentials tab.
6. In the window that opens, click Create access key.
7. An access key ID and a secret is generated. Copy and save the key ID and secret in a secure location as it will not be displayed again.

2.4 RFC2136 DNS Update

If you are using open source DNS servers such as Bind, PowerDNS etc., that support RFC2136 DNS update, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

1. Mention the DNS Server IP / Hostname represents the server name / IP address in which the DNS server is installed or running.
2. These details are usually found in the server installation directory. For instance, in the case of Bind9 DNS server, you can find these in the file named .local.conf in the server installation directory.
3. Provide the **Key Secret**, which is nothing but the key content found in the server installation directory.
4. Provide a name for the key, and choose the signature algorithm.
5. Click **Save**.

2.5 GoDaddy DNS

If you are using GoDaddy DNS for DNS validation, follow the steps below to automate DNS-based domain control validation procedure using PAM360:
Steps to Obtain GoDaddy API Credentials:

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Log in to your GoDaddy account if you aren't logged in already.
3. Once you log in, you will be redirected to the API keys page where you can create and manage API keys.
4. Click Create New API key.
5. Provide your application name, choose the environment type as Production and click Next.
6. The API key and its secret is generated. Copy and save the secret in a secure location, as it will not be displayed again.

Now, in PAM360 interface, follow the below steps to add GoDaddy DNS to Buypass Go SSL CA:

1. Navigate to **Certificates >> Acme >> Buypass Go SSL** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**. Choose **GoDaddy** from the DNS Provider dropdown.
3. Enter the Key and Secret that was previously generated from the GoDaddy portal.
4. Click **Save**.

2.6 ClouDNS

If you are using ClouDNS for DNS validation, follow the steps below to automate the DNS-based domain control validation procedure using PAM360:
Steps to Obtain ClouDNS API Credentials:

1. Login to your **ClouDNS** account and go to **Reseller API**.
2. If you have already created an API user id, you will find it under API Users. If not, click Create API to generate a new one.
3. Click here to learn more about ClouDNS API Auth IDs.

Now, in the PAM360 interface, follow the below steps to add ClouDNS to Buypass Go SSL CA:

1. Navigate to **Certificates >> Acme >> Buypass Go SSL** and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **ClouDNS** from the DNS Provider dropdown.
4. Choose one of the following options: Auth ID, Sub Auth ID, Sub Auth User.
5. Enter the chosen ClouDNS Auth ID, its respective Auth Password, and click **Save**.

Notes:

1. One certificate can secure up to 5 domains. You can enter a maximum of 5 names in the 'domain name' field out of which the first name is considered as the common name and the rest are treated as Subject Alternative Names (SAN).
2. Buypass Go SSL has a rate limit of 20 certificates every 7 days for base domains. It supports upto 5 requests every 7 days for obtaining duplicate certificates.
3. Buypass Go SSL does not support wildcard certificates.
4. PAM360 integration with Buypass Go SSL supports encryption via RSA and EC algorithms.
5. PAM360 supports http-01 and dns-01 based domain validations. Choose the challenge type based on your requirements.
6. For dns-01 based domain validation, if you are using your configured DNS account for challenge verification, make sure that the status of the chosen DNS account is marked Enabled under Manage >> DNS.
7. Option to change the private key currently works only with the RSA key algorithm.

3. Buypass Go SSL Challenge Verification

PAM360 expedites domain validation through automatic verification of HTTP-01 and DNS-01 challenges (currently Azure, Cloudflare, Amazon Route 53, RFC2136 DNS update, GoDaddy DNS, ClouDNS). For the automation to take effect, you have to initially map the end-server details to PAM360, which is a one-time process.

3.1 Domain validation through HTTP-01 challenge verification

For domain validation through http-01 challenge,

1. A window opens displaying the challenge to be fulfilled.
2. Click the **Agent mapping** icon.
3. A pop up will open. If the domain server is a Linux machine, fill in the required details and click **Save**.

If the domain server is a Windows machine, download and install the Key Manager Plus agent for Windows server using the steps mentioned below:

1. Downloading Key Manager Plus agent for Windows servers:
2. The Key Manager Plus agent package is a zip file comprising of the necessary executables, configuration files required for automatic verification of Buypass Go SSL challenges through automatic domain validation. Unzip the folder and install the agent on your Windows domain server after download. To download the agent,
3. Navigate to **Certificates >> ACME >> Buypass Go SSL** tab, and click **Manage** button in the top right corner.
4. Switch to the **Windows agents** tab.
5. Download the Key Manager Plus agent from the top right corner of the window based on your server compatibility (32 bit or 64 bit).

Installing Key Manager Plus agents for Windows server:

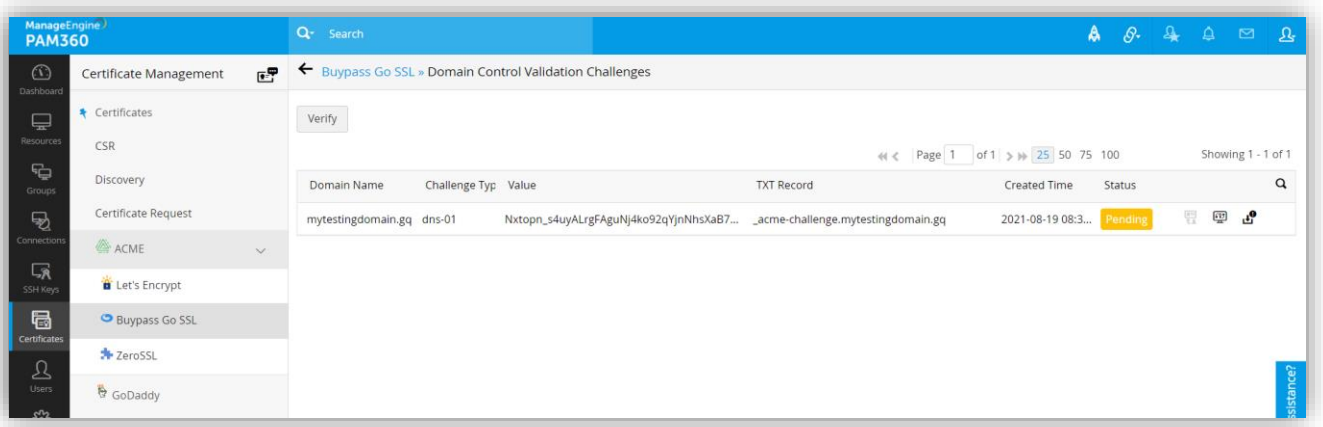
1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command 'AgentInstaller.exe start.'

To stop the agent and uninstall the Windows service,

1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command 'AgentInstaller.exe stop.'

3. If the domain server is a Windows machine, download and install the Windows agent on the domain server. Navigate to **Manage >> Windows agents**, download and install the agent on the domain server.
4. Once, the above agent mapping settings are configured (agent mapping is a one-time configuration), PAM360 automatically handles the verification of challenges presented by Buypass Go SSL.

After configuring agent mapping, click **Pending** on the pending requests and click Verify. The challenge is verified and certificate request is submitted to Buypass Go SSL CA.



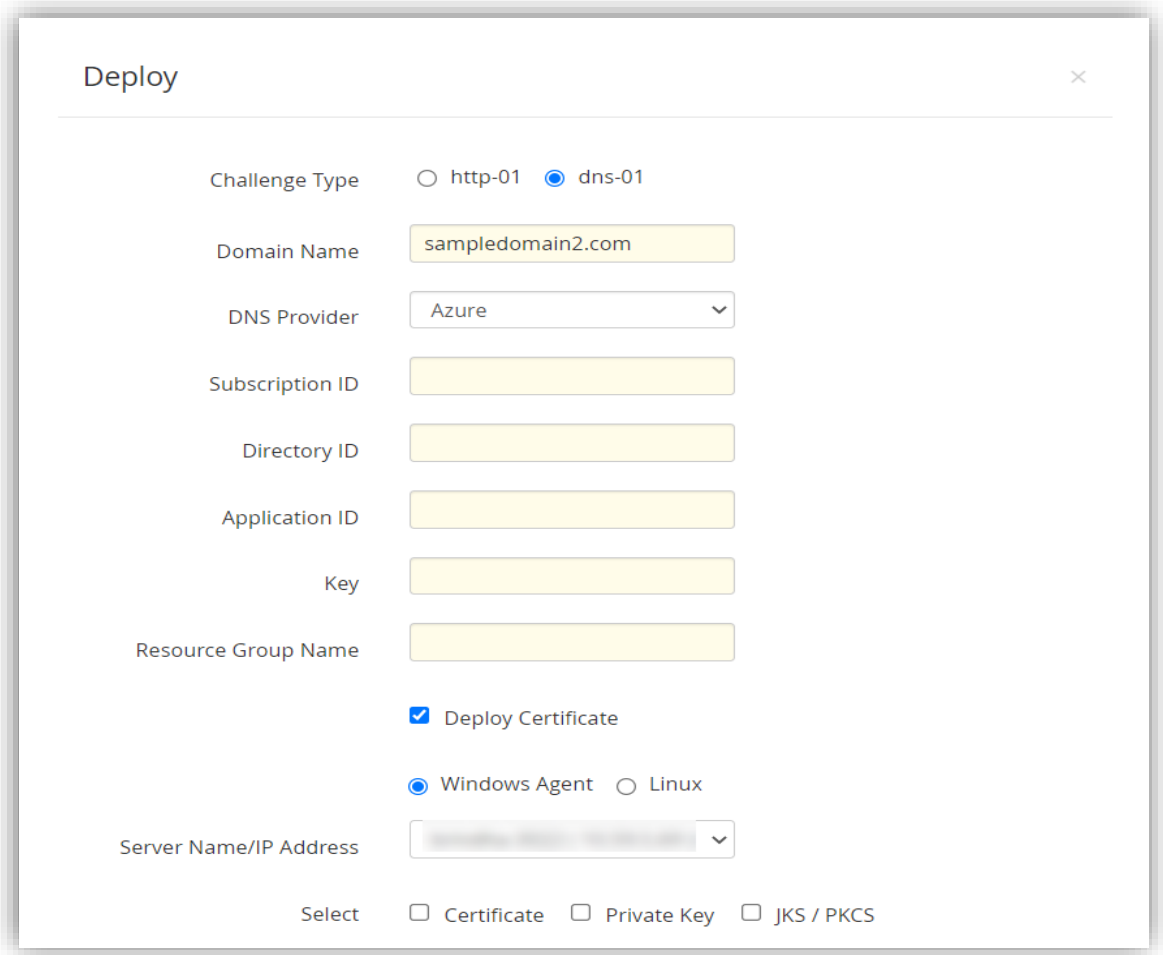
3.2 Domain validation through DNS-01 challenge verification

For DNS-01 challenge verification from PAM360,

1. Switch to the **Buypass Go SSL** tab and click on the request status (Pending) corresponding to the certificate request.
2. You'll be directed to a window that displays the DNS challenge value and TXT record.
3. If you have already configured your DNS account details and have opted for DNS while creating the certificate request, you can assign the DNS account to the request.
4. Select the request, choose **Assign DNS** from More top menu and select the required DNS account.
5. In cases where you do not have a DNS account configured or have not opted for it when raising the certificate request, PAM360 provides an option for automating DNS-01 challenge verification through Agent Mapping.
6. Click on the Agent Mapping icon available to the left side of the request. Agent mapping is a one-time configuration.

Agent Mapping

1. In the Deploy window that opens, carry out the following operations to map and save your end-server details in PAM360.
2. Choose your DNS provider. For Azure DNS, provide the required details—subscription ID, directory ID, application ID, application key and resource group name.
3. For Cloudflare DNS, enter the email address associated with your Cloudflare account and the Global API key.
4. For Amazon Route 53 DNS, enter the Access Key ID and Secret associated with your AWS account.
5. Enable the Deploy Certificate check-box to automate deployment of the certificate to their corresponding end-servers after domain validation and after successive renewals.
6. For Linux end-servers provide the required details, while for Windows end-servers download and install the Windows agent using the same procedure as mentioned for http-01 challenge.
7. After filling in the details, click **Save**. The end-server details are successfully mapped and stored in PAM360, which you can view or edit from **Manage >> Deploy** tab.



Notes:

1. You can request and acquire certificates only for public domains using Buypass Go SSL integration.
2. The handling of challenges can also be done manually without automation. Copy and paste the challenge values / text records manually in your domain server. Then in the PAM360 server, navigate to Pending Requests page and click Verify. The challenge is verified and certificate is issued.
3. PAM360 automates challenge verification using DNS for a certificate request only when Agent mapping is not available. Challenge verification is automated through agents, if agent details are available in **Manage >> Deploy** tab.
4. Currently, Key Manager Plus agents are only available for Windows servers.
5. For RFC2136 DNS update, if you have opted Global DNS configuration, the domain name itself acts as the zone name (Global DNS configuration is possible only if you are using the same Key Secret for all zones). Whereas, if you have opted domain-agent mapping, you have to provide the Zone name, Key Name, and Key Secret for each domain separately.

4. Procure and Save the Certificate

On successful verification, Buypass Go SSL issues the requested certificate.

1. The window automatically redirects to a page which displays the certificate and its status (status is marked Available, if the challenge verification is successful and Failed if the challenge verification fails).
2. Click the Available button to save the certificate in PAM360 repository, e-mail or export it.
3. If the challenge fails, click New challenge to obtain another set of challenges and repeat the above process.

4. On saving, the certificate gets added to the PAM360 repository which can be viewed from the **SSL >> Certificates** tab.

5. Renew Certificates

Certificates issued by Buypass Go SSL have a life-time of 180 days after which they are not valid. Certificate renewals can be carried out manually or automatically through automatic domain validation. To renew a certificate manually,

1. Navigate to **Certificates >> ACME >> Buypass Go SSL**.
2. Select the certificate that you want to renew and click **Renew Certificate** button.
3. The certificate is renewed and the Certificate Status bar displays Renewed.
4. Click on it to save the renewed version of the certificate to the PAM360 certificate repository.

> **Note:** The certificate should be saved after renewal in order to be updated in the certificate repository. Else, only the old version of the certificate will continue to remain in repository.

Automatic Renewals through Automatic Domain Validation

If agent mapping had been configured, the certificate renewal process is done automatically without manual intervention. All the certificates in your organization procured from Buypass Go SSL is automatically renewed 15 days before its expiry and a notification is sent to the account holder's e-mail address.

> **Note:** Automatic renewals are applicable only for those certificates saved in PAM360 repository. i.e., after procuring a certificate from Buypass Go SSL, you have to save it in order for the automatic renewal to take effect.

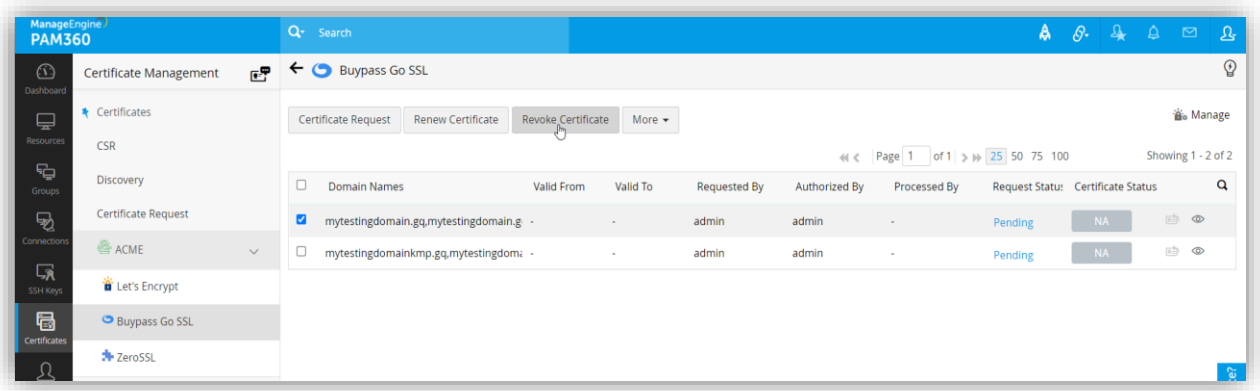
6. Revoke Certificates

Revoking a certificate renders the certificate invalid and immediately removes the HTTPS from

the website.

To revoke a certificate,

1. Navigate to **Certificates >> ACME >> Buypass Go SSL** tab.
2. Select a certificate you want to revoke and click **Revoke Certificate**.
3. The certificate is revoked and is no longer valid.

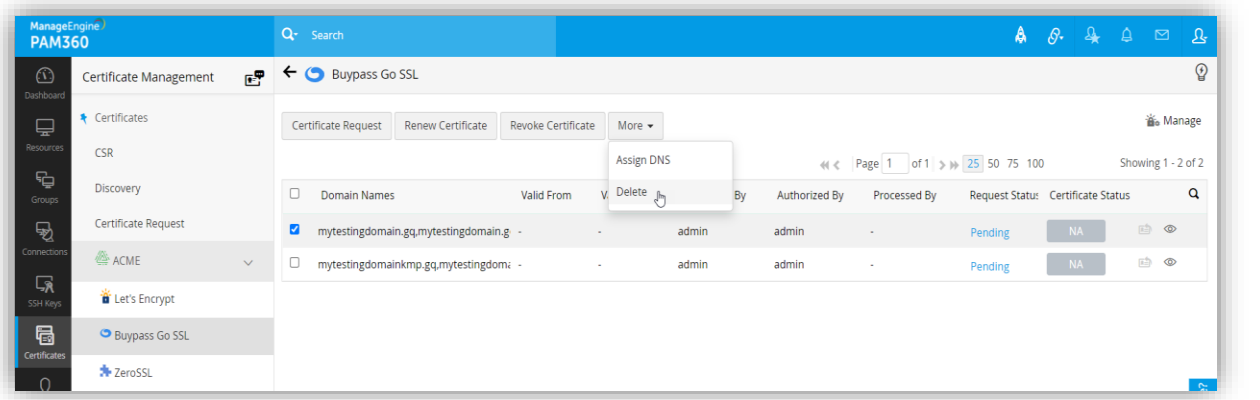


7. Delete Certificates

Deleting a certificate removes the certificate from PAM360 repository, but the certificate still remains valid.

To delete a certificate,

1. Navigate to **Certificates >> Acme >> Buypass Go SSL** tab.
2. Select the certificate you want to delete and click **More >> Delete.**
3. The certificate is deleted from the PAM360 database.



Integration with ZeroSSL

PAM360 facilitates integration with ZeroSSL — the certificate authority (CA) that uses the Automatic Certificate Management Environment (ACME) protocol to provide secure SSL certificates free of cost. This integration helps you achieve an end-to-end life cycle management of ZeroSSL certificates installed on your domains from a single interface. This document discusses the steps you should follow to establish a connection with your ZeroSSL account, acquire, deploy, renew and perform all certificate management related operations from PAM360.

Before you proceed with the integration, complete the following step as a prerequisite:

Prerequisite

Add the following base URL and port as an exception in your firewall or proxy to ensure PAM360 is able to connect to ZeroSSL's CA Services.

URL: https://acme.zerossl.com/v2/DV90

Port: 443

Follow the step-by-step procedure below to integrate ZeroSSL with PAM360:

1. **Create a ZeroSSL Account**
2. **Raise a Certificate Request**
3. **ZeroSSL Challenge Verification**
4. **Procure and Save the Certificate**
5. **Renew Certificates**
6. **Revoke Certificates**
7. **Delete Certificates**

1. Create a ZeroSSL Account

To begin the process of requesting SSL certificates from ZeroSSL, you must create an

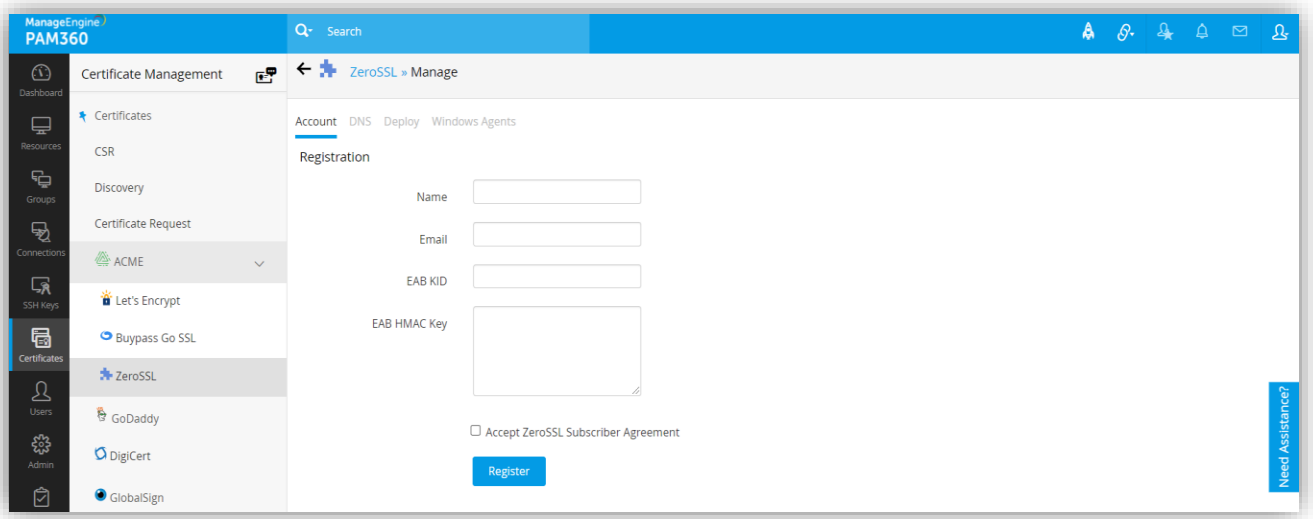
account. This is a one-time process and can be done directly from the PAM360 interface.

1. To create a ZeroSSL account, navigate to the **Certificates** tab, click the **ACME** drop-down and select **ZeroSSL**.
2. Click **Manage**. Under the **Account** tab, click **New Registration**.
3. In the pop-up, enter an account name and a valid e-mail address. Enter your **EAB KID** and **EAB HMAC Key.** Click here to generate EAB KID and HMAC Key for your account, if you don't have one already.
4. Click the checkbox to accept the ZeroSSL Subscriber Agreement.
5. Click **Register**. Now, an account with ZeroSSL is created.

Once your account is created, you can update the account email address, delete it from PAM360, or deactivate the account entirely. Please note that deleting the account only removes it from PAM360. Even if you delete the account here, it will still be active in the ZeroSSL portal. To add the same account back to PAM360, export the key and use the **Add Account** option with the same details used before. However, if you select the **Deactivate** option while deleting the account, then the ZeroSSL account will be removed completely and you cannot add it back to PAM360 with the same details.

Notes:

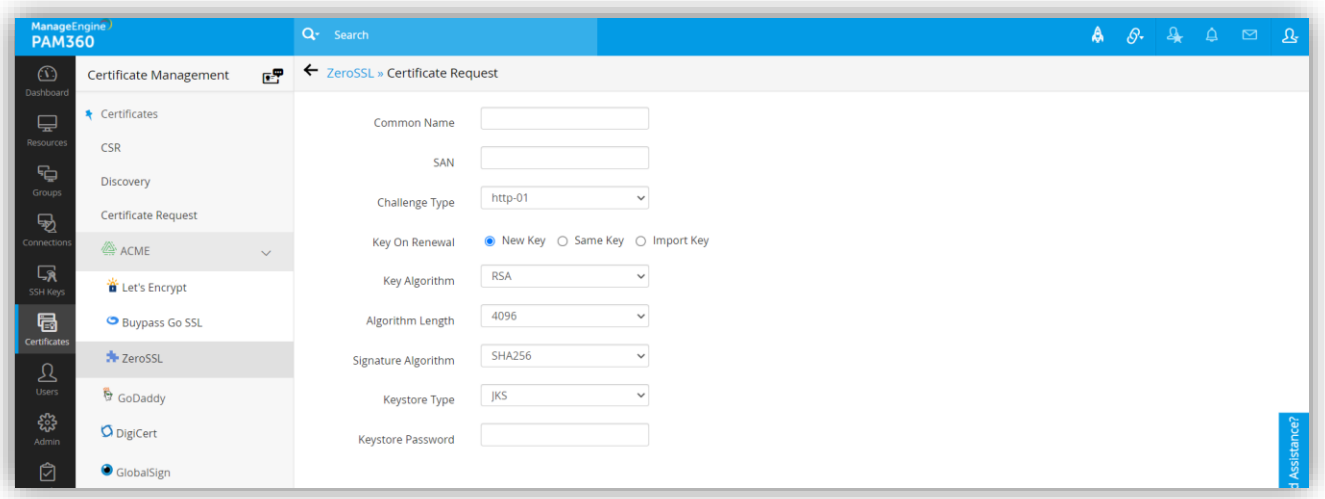
1. Please note that for each new account registration, a new EAB KID has to be created. After successfully registering for an account, the same EAB HMAC key cannot be used again. Click here to read the ZeroSSL document for more details.
2. Only the users who are assigned with the 'ACME' role under 'SSH Keys and Certificates' user roles can perform the above operation. Go to **Admin >> Customization >> Roles** to activate this user role.
3. Only one ZeroSSL account can be created from PAM360.



2. Raise a Certificate Request

Once your ZeroSSL account is registered, you can proceed with raising certificate requests to the CA. To complete a certificate request, you will be presented with a challenge verification to fulfill in order to validate your domain and issue the certificate you have requested.

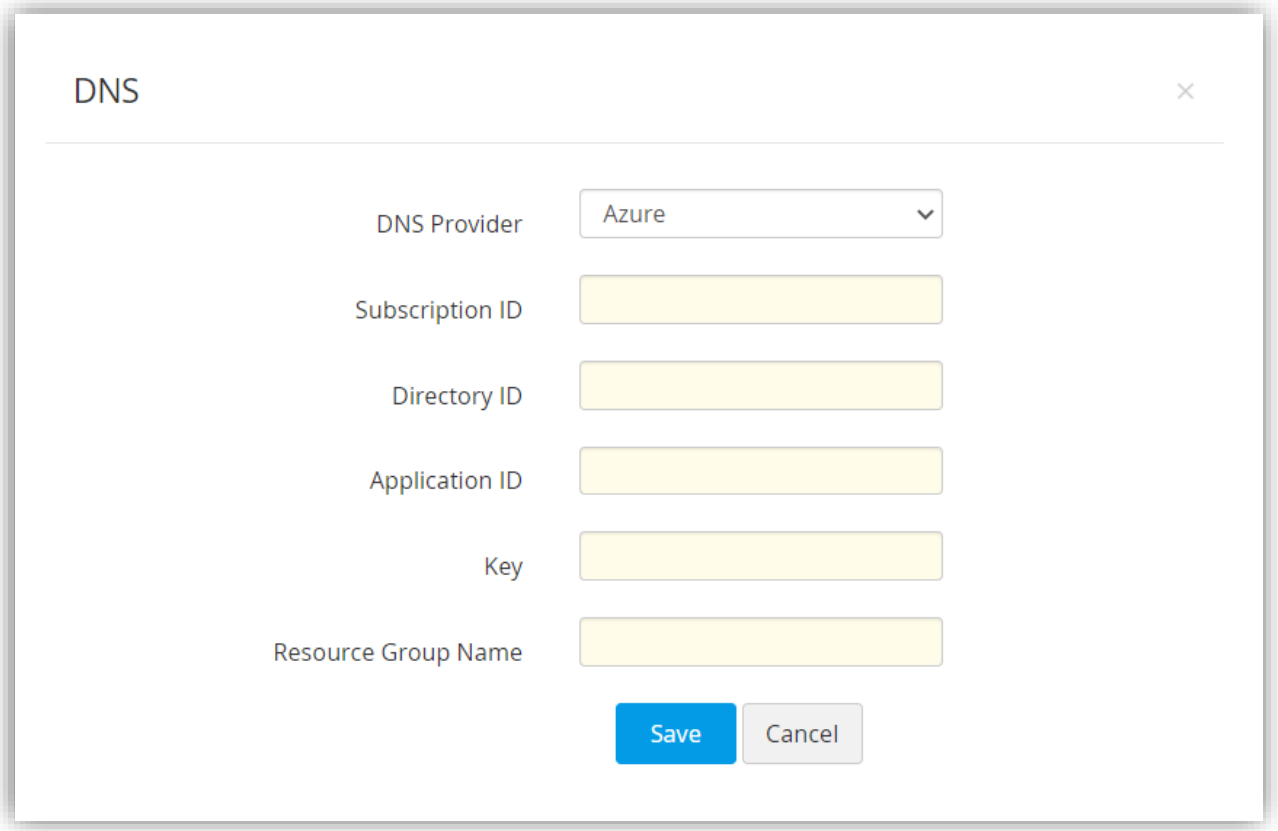
1. Navigate to **Certificates >> ACME >> ZeroSSL.**
2. Click **Certificate Request.** Fill in the domain name, select the challenge type, choose the key algorithm, algorithm length, signature algorithm, keystore type, enter the keystore password and click **Create**.
3. For dns-01 challenge type, you can choose and assign a DNS account from the drop-down if you have already configured your DNS credentials. This will be used for automatic challenge verification for all the domains specified in the request.
4. Also, you have options to change the private key whenever the certificate is renewed.
    a. If you need to change the key, use **New Key**. This option will generate a new key every time the certificate is renewed.
    b. If you want to retain the same key on renewal, use the **Same Key** option.
    c. To use your own key, use the **Import Key** option. This key will be used for the first time when the certificate is generated and also for subsequent renewals.



Note: PAM360 supports wildcard certificate requests for DNS based challenges. For wildcard certificate requests, enter the common name in the format *.domainname.com

To configure your DNS account, follow the below steps:

1. Navigate to **ZeroSSL >> Manage.** Switch to the **DNS** tab.
2. Here, you can add a maximum of one DNS account for each DNS provider supported. PAM360 currently supports automatic challenge verification for Azure DNS, CloudFlare DNS, and Amazon Route 53 DNS, RFC2136 DNS update (nsupdate), GoDaddy DNS, and ClouDNS. Click Add.
3. In the pop-up that opens, choose the DNS provider.



2.1 Azure DNS

1. Provide the Subscription ID, which is available in the Overview page of the Azure DNS zone.
2. Provide the Directory ID, which is available in Azure Active Directory >> Properties.
3. If you have an already existing Azure application, provide its Application ID and Key.
4. If not, follow the steps mentioned in this document to create the Azure application and key, and give the application access to the DNS zones for making API calls.
5. Finally, enter the Resource Group Name, which is the group name in which you have created the DNS zone and click Save.
6. Your DNS account details are saved and listed under **Manage >> DNS**.

2.2 Cloudflare DNS

1. In the Email address field, specify the email address associated with the Cloudflare account.
2. For Global API Key, use the **Generate API** key option in the domain overview page of the Cloudflare DNS to generate the key and paste the value in this field. Click Save.

3. Your DNS account details are saved and listed under **Manage >> DNS**.

2.3 AWS Route 53 DNS

Generate and specify the Access Key ID and Secret associated with your AWS account. If you do not have an AWS account, create one and generate the Access Key ID and Secret by following the steps given below:

1. Login to the AWS console and navigate to **IAM Services >> Users**. Click **Add user.**
2. Provide the user name and select the access type as **Programmatic access**.
3. Switch to the next tab, click Attach existing policies directly under Set Permissions and search for "AmazonRoute53FullAccess".
4. Assign the policy that is listed and switch to the next tab. In the tags section, add appropriate tags (optional) and switch to the next tab.
5. Review all the information entered and click Create user.
6. The user account is created and subsequently, an access key ID and a secret is generated. Copy and save the key ID and secret in a secure location for it will not be displayed again.
7. If you already have an AWS user account, you have to grant "AmazonRoute53FullAccess" permission to the user and generate the access key if the user doesn't have one. if the user account has an access key associated already, it is just enough to ensure the required permission is granted.

To grant the required permissions:

1. Navigate to the **Permissions** tab, select the required user account and click **Add Permission**.
2. Click Attach existing policies directly under Set Permissions and search for "AmazonRoute53FullAccess".
3. Assign the listed policy and hit Save.
4. To generate the access key,
5. Select the particular user account and navigate to the Security Credentials tab.
6. In the window that opens, click Create access key.
7. An access key ID and a secret is generated. Copy and save the key ID and secret in a

secure location as it will not be displayed again.

2.4 RFC2136 DNS Update

If you are using open source DNS servers such as Bind, PowerDNS etc., that support RFC2136 DNS update, follow the steps below to automate DNS-based domain control validation procedure using PAM360.

1. Mention the DNS Server IP / Hostname represents the server name / IP address in which the DNS server is installed or running.
2. These details are usually found in the server installation directory. For instance, in the case of Bind9 DNS server, you can find these in the file named.local.conf in the server installation directory.
3. Provide the **Key Secret**, which is nothing but the key content found in the server installation directory.
4. Provide a name for the key, and choose the signature algorithm.
5. Click **Save**.

2.5 GoDaddy DNS

If you are using GoDaddy DNS for DNS validation, follow the steps below to automate DNS-based domain control validation procedure using PAM360:
Steps to Obtain GoDaddy API Credentials:

1. Go to the GoDaddy developer portal and switch to the API keys tab.
2. Log in to your GoDaddy account if you aren't logged in already.
3. Once you log in, you will be redirected to the API keys page where you can create and manage API keys.
4. Click Create New API key.
5. Provide your application name, choose the environment type as Production and click Next.
6. The API key and its secret is generated. Copy and save the secret in a secure location, as it will not be displayed again.

Now, in PAM360 interface, follow the below steps to add GoDaddy DNS to ZeroSSL CA:

1. Navigate to **Certificates >> Acme >> ZeroSSL** and click **Manage** from the right most corner.

2. Switch to the **DNS** tab and click **Add**. Choose **GoDaddy** from the DNS Provider drop-down.
3. Enter the Key and Secret that was previously generated from the GoDaddy portal.
4. Click **Save**.

2.6 ClouDNS

If you are using ClouDNS for DNS validation, follow the steps below to automate the DNS-based domain control validation procedure using PAM360:
Steps to Obtain ClouDNS API Credentials:

1. Login to your **ClouDNS** account and go to **Reseller API**.
2. If you have already created an API user id, you will find it under API Users. If not, click Create API to generate a new one.
3. Click here to learn more about ClouDNS API Auth IDs.

Now, in the PAM360 interface, follow the below steps to add ClouDNS to ZeroSSL CA:

1. Navigate to **Certificates >> Acme >>** ZeroSSL and click **Manage** from the right most corner.
2. Switch to the **DNS** tab and click **Add**.
3. Choose **ClouDNS** from the DNS Provider drop-down.
4. Choose one of the following options: Auth ID, Sub Auth ID, Sub Auth User.
5. Enter the chosen ClouDNS Auth ID, its respective Auth Password, and click **Save**.

Notes:

a. ZeroSSL offers multi-domain certificates as well as wildcard certificates.

b. PAM360 integration with ZeroSSL supports encryption via RSA and EC algorithms.

c. PAM360 supports http-01 and dns-01 based domain validations. Choose the challenge type based on your requirements.

d. For dns-01 based domain validation, if you are using your configured DNS account for challenge verification, make sure that the status of the chosen DNS account is marked Enabled under Manage >> DNS.

e. Option to change the private key currently works only with the RSA key algorithm.

3. ZeroSSL Challenge Verification

PAM360 expedites domain validation through automatic verification of HTTP-01 and DNS-01 challenges (currently Azure, Cloudflare, Amazon Route 53, RFC2136 DNS update, GoDaddy DNS, ClouDNS). For the automation to take effect, you have to initially map the end-server details to PAM360, which is a one-time process.

3.1 Domain validation through HTTP-01 challenge verification

For domain validation through http-01 challenge,

1. A window opens displaying the challenge to be fulfilled.
2. Click the Agent mapping icon.
3. A pop up will open. If the domain server is a Linux machine, fill in the required details and click Save.

If the domain server is a Windows machine, download and install the Key Manager Plus agent for Windows server using the steps mentioned below:

1. Downloading Key Manager Plus agent for Windows servers:
2. The Key Manager Plus agent package is a zip file comprising of the necessary

executables, configuration files required for automatic verification of ZeroSSL challenges through automatic domain validation. Unzip the folder and install the agent on your Windows domain server after download. To download the agent,

3. Navigate to **Certificates >> ACME >> ZeroSSL** tab, and click **Manage** button in the top right corner.
4. Switch to the **Windows agents** tab.
5. Download the Key Manager Plus agent from the top right corner of the window based on your server compatibility (32 bit or 64 bit).

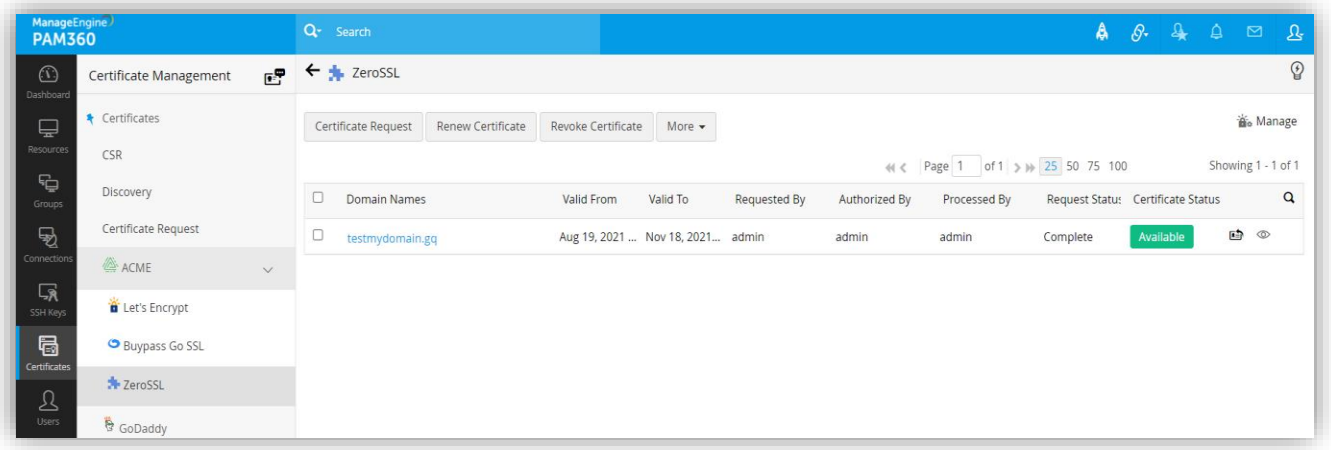
Installing Key Manager Plus agents for Windows server:

1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command 'AgentInstaller.exe start.'

To stop the agent and uninstall the Windows service,

1. Open the command prompt and navigate to the PAM360 installation directory.
2. Execute the command 'AgentInstaller.exe stop.'
3. If the domain server is a Windows machine, download and install the Windows agent on the domain server. Navigate to Manage >> Windows agents, download and install the agent on the domain server.
4. Once, the above agent mapping settings are configured (agent mapping is a one-time configuration), PAM360 automatically handles the verification of challenges presented by ZeroSSL.

After configuring agent mapping, click **Pending** on the pending requests and click Verify. The challenge is verified and certificate request is submitted to ZeroSSL CA.



3.2 Domain validation through DNS-01 challenge verification

For DNS-01 challenge verification from PAM360,

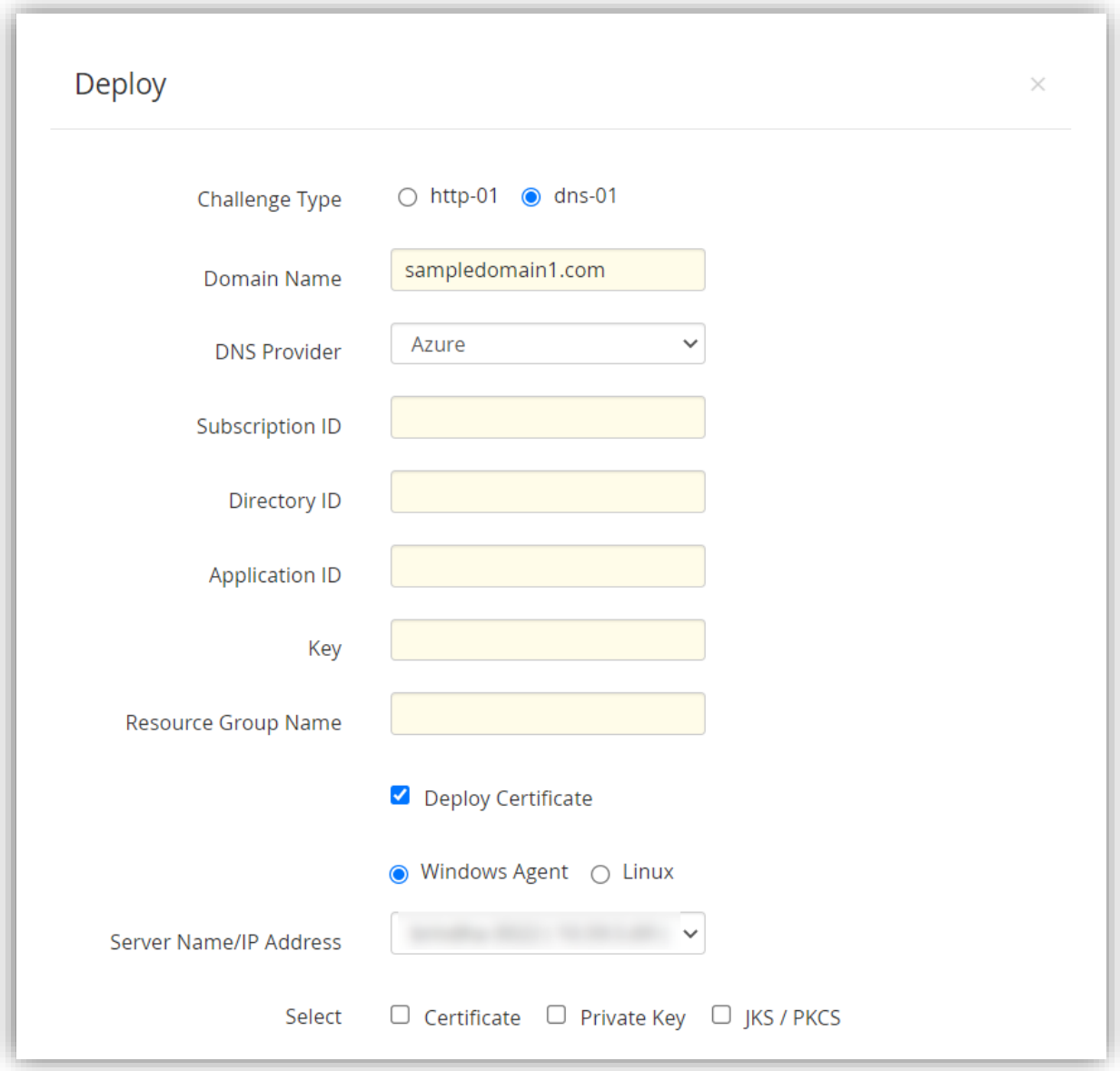
1. Switch to the **ZeroSSL** tab and click on the request status (Pending) corresponding to the certificate request.
2. You'll be directed to a window that displays the DNS challenge value and TXT record.
3. If you have already configured your DNS account details and have opted for DNS while creating the certificate request, you can assign the DNS account to the request.
4. Select the request, choose **Assign DNS** from More top menu and select the required DNS account.
5. In cases where you do not have a DNS account configured or have not opted for it when raising the certificate request, PAM360 provides an option for automating DNS-01 challenge verification through Agent Mapping.
6. Click on the Agent Mapping icon available to the left side of the request. Agent mapping is a one-time configuration.

Agent Mapping

1. In the Deploy window that opens, carry out the following operations to map and save your end-server details in PAM360.
2. Choose your DNS provider. For Azure DNS, provide the required details—subscription ID, directory ID, application ID, application key and resource group name.
3. For Cloudflare DNS, enter the email address associated with your Cloudflare account

and the Global API key.

4. For Amazon Route 53 DNS, enter the Access Key ID and Secret associated with your AWS account.
5. Enable the Deploy Certificate check-box to automate deployment of the certificate to their corresponding end-servers after domain validation and after successive renewals.
6. For Linux end-servers provide the required details, while for Windows end-servers download and install the Windows agent using the same procedure as mentioned for http-01 challenge.
7. After filling in the details, click **Save**. The end-server details are successfully mapped and stored in PAM360, which you can view or edit from **Manage >> Deploy** tab.



Notes:

a. You can request and acquire certificates only for public domains using ZeroSSL integration.

b. The handling of challenges can also be done manually without automation. Copy and paste the challenge values / text records manually in your domain server. Then in the PAM360 server, navigate to Pending Requests page and click Verify. The challenge is verified and certificate is issued.

c. PAM360 automates challenge verification using DNS for a certificate request only when Agent mapping is not available. Challenge verification is automated through agents, if agent details are available in **Manage >> Deploy** tab.

d. Currently, Key Manager Plus agents are only available for Windows servers.

e. For RFC2136 DNS update, if you have opted Global DNS configuration, the domain name itself acts as the zone name (Global DNS configuration is possible only if you are using the same Key Secret for all zones). Whereas, if you have opted domain-agent mapping, you have to provide the Zone name, Key Name, and Key Secret for each domain separately.

4. Procure and Save the Certificate

On successful verification, ZeroSSL issues the requested certificate.

1. The window automatically redirects to a page which displays the certificate and its status (status is marked Available, if the challenge verification is successful and Failed if the challenge verification fails).
2. Click the Available button to save the certificate in PAM360 repository, e-mail or export it.
3. If the challenge fails, click New challenge to obtain another set of challenges and repeat the above process.
4. On saving, the certificate gets added to the PAM360 repository which can be viewed from the **SSL >> Certificates** tab.

5. Renew Certificates

Certificates issued by ZeroSSL have a life-time of 90 days after which they are not valid. Certificate renewals can be carried out manually or automatically through automatic domain validation. To renew a certificate manually,

1. Navigate to **Certificates >> ACME >> ZeroSSL**.
2. Select the certificate that you want to renew and click **Renew Certificate** button.
3. The certificate is renewed and the Certificate Status bar displays Renewed.
4. Click on it to save the renewed version of the certificate to the PAM360 certificate repository.

> **Note:** The certificate should be saved after renewal in order to be updated in the certificate repository. Else, only the old version of the certificate will continue to remain in repository.

Automatic Renewals through Automatic Domain Validation

If agent mapping had been configured, the certificate renewal process is done automatically without manual intervention. All the certificates in your organization procured from ZeroSSL is automatically renewed 15 days before its expiry and a notification is sent to the account holder's e-mail address.

> **Note**: Automatic renewals are applicable only for those certificates saved in PAM360 repository. i.e., after procuring a certificate from ZeroSSL, you have to save it in order for the automatic renewal to take effect.

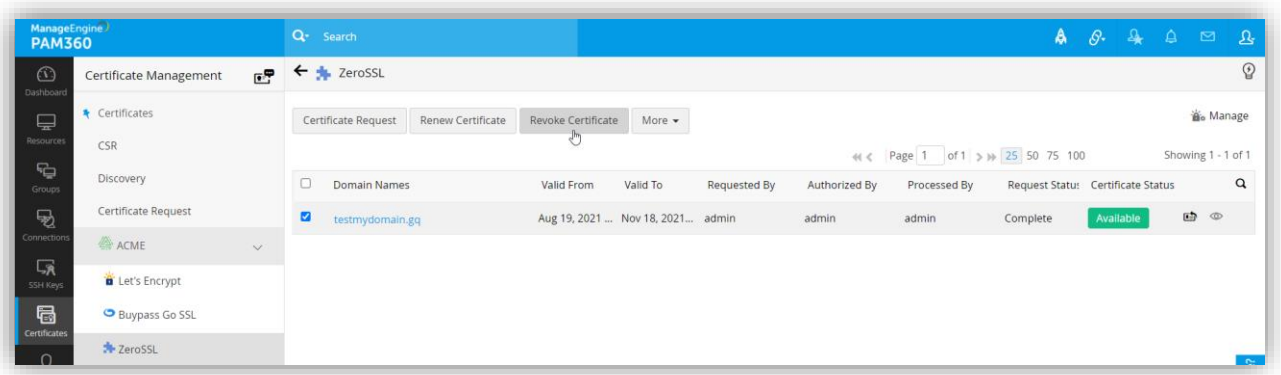
6. Revoke Certificates

Revoking a certificate renders the certificate invalid and immediately removes the HTTPS from the website.

To revoke a certificate,

1. Navigate to **Certificates >> Acme >> ZeroSSL** tab.

2. Select a certificate you want to revoke and click **Revoke Certificate**.
3. The certificate is revoked and is no longer valid.

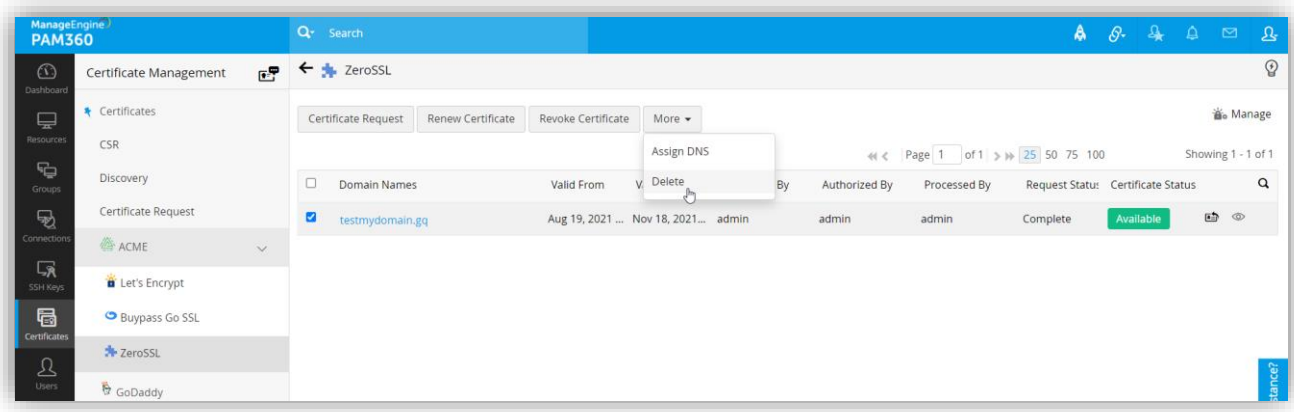


7. Delete Certificates

Deleting a certificate removes the certificate from PAM360 repository, but the certificate still remains valid.

To delete a certificate,

1. Navigate to **Certificates >> Acme >> ZeroSSL** tab.
2. Select the certificate you want to delete and click **More >> Delete.**
3. The certificate is deleted from the PAM360 database.



Integration with AWS-ACM Certificate Manager

PAM360 now integrates with AWS Certificate Manager (ACM) — an SSL certificate manager and private certificate authority. This integration enables you to request and obtain certificates from AWS-ACM into PAM360. In addition, you can deploy certificates from PAM360 to the AWS-ACM repository.

It also allows you to renew certificate requests and automate the end-to-end lifecycle management of SSL/TLS certificates issued and managed by ACM, directly from the PAM360 web interface.

1. How does the PAM360 – AWS-ACM Integration Work?
2. AWS-ACM Certificate Discovery
3. Deploying Certificates to AWS-ACM
4. Requesting Certificates from AWS-ACM
5. Domain Validation, Certificate Issue, and Deployment
6. Renewing, Revoking, Deleting & Fetching Private Key of Certificates

1. How does the PAM360 – AWS-ACM Integration Work?

Through PAM360's certificate discovery feature, import AWS-ACM certificates into the PAM360 repository. Once discovery is done, PAM360 displays all the AWS certificates deployed to all regions under the AWS tab. Click here to learn more about the supported regions in AWS.

There are two types of certificates in AWS-ACM: Public and Private Certificates. AWS-ACM allows you to use public certificates provided by ACM or certificates that are imported into ACM. If you use ACM Private CA to create a CA, ACM can issue certificates and automate certificate renewals from that private CA.

PAM360 allows you to create new certificates and manage them in the product. AWS-ACM does not support the creation of new certificates. However, you can create, request, and import certificates from PAM360 into AWS-ACM and manage them from the AWS Management Console. Click here to learn more about importing certificates into AWS-ACM.

Prerequisites

To perform the AWS-ACM integration, administrators require the following user role permissions in AWS-ACM: AWSCertificateManagerFullAccess - This policy provides full access to all ACM actions and resources. Click here to read more about the user role policies in AWS.

This integration requires **API AccessKey** and **SecretKey**. These credentials are also required to perform AWS certificate discovery to import AWS-ACM certificates into PAM360.

2. AWS-ACM Certificate Discovery

PAM360 enables you to discover, import, and configure expiry notifications for SSL certificates hosted in the following Amazon Web Services: AWS Certificate Manager (ACM) and AWS Identity and Access Management (IAM). Click here for detailed steps on how to discover AWS-ACM certificates.

Note: When you perform any operation on the AWS certificates added before PAM360 build 6200, PAM360 automatically performs certificate rediscovery and re-populates the data in the table to get the Amazon Resource Name (ARN) ID. Please note that this automatic rediscovery happens only from PAM360 build 6200 onwards.

In the **Certificates >> AWS** tab, Public Certificates requested from Amazon are marked as **Amazon Issued**, Private Certificates are marked as Private and certificates are that imported from PAM360 to AWS-ACM are marked as **Imported**.

3. Deploying Certificates to AWS-ACM

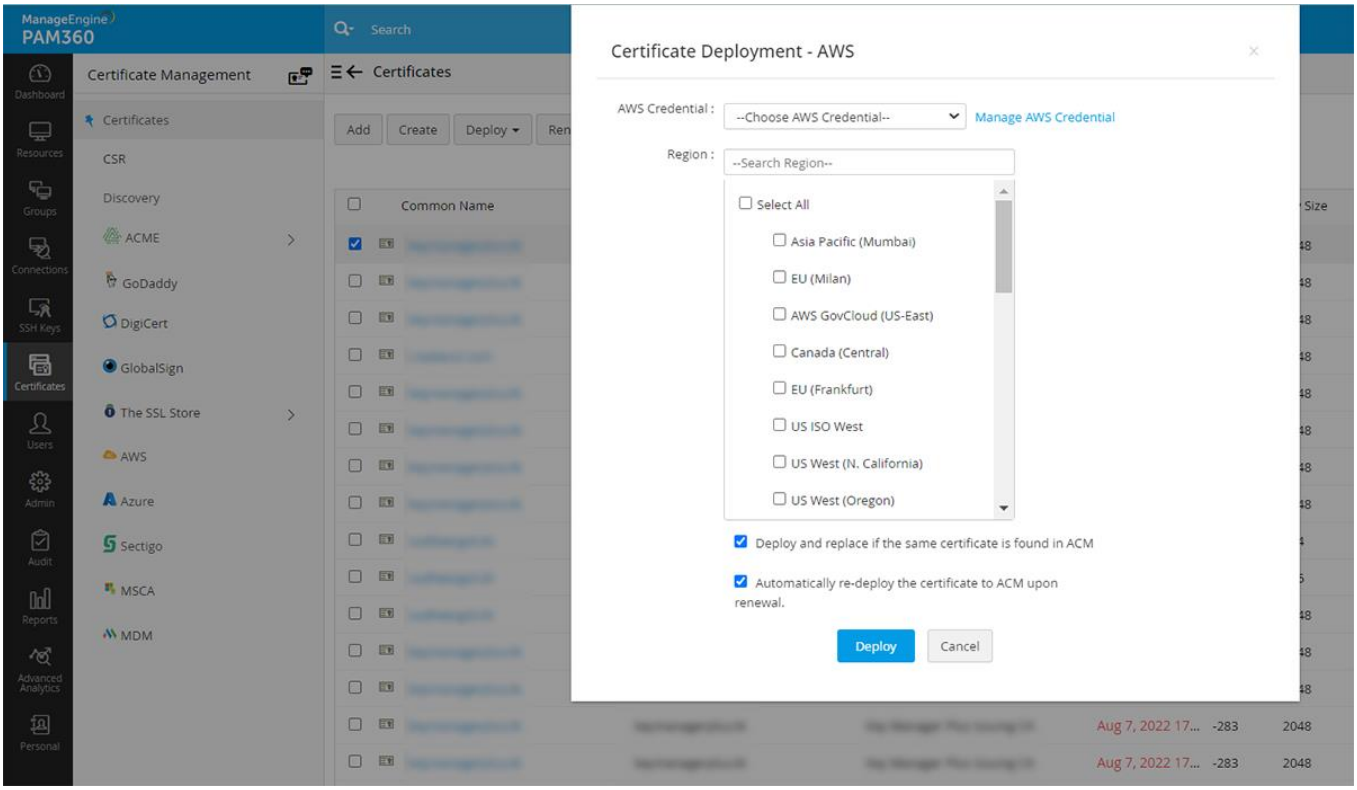
PAM360's integration with AWS-ACM facilitates you to deploy certificates to the AWS-ACM and manage them from their console. To deploy certificates to AWS-ACM, follow the below steps:

1. Navigate to **Certificates >> Certificates**.
2. Select the required AWS certificate and click **Deploy >> AWS-ACM** from the top menu.
3. In the dialog box that appears, choose the following attributes:

i. **AWS Credential** from the dropdown.

ii. Select one or more **Regions** using the checkboxes.

Certificates can be deployed to all the supported regions provided the private keys are available.



Deploy and replace if the same certificate is found in ACM: If you wish to replace the certificate in ACM after deployment, in case it turns out to be a duplicate, select this option.

Automatically re-deploy the certificate to ACM upon renewal: Select this option to automatically re-deploy the certificate to ACM every time it is renewed so that the certificate in PAM360 and AWS-ACM are always in sync.

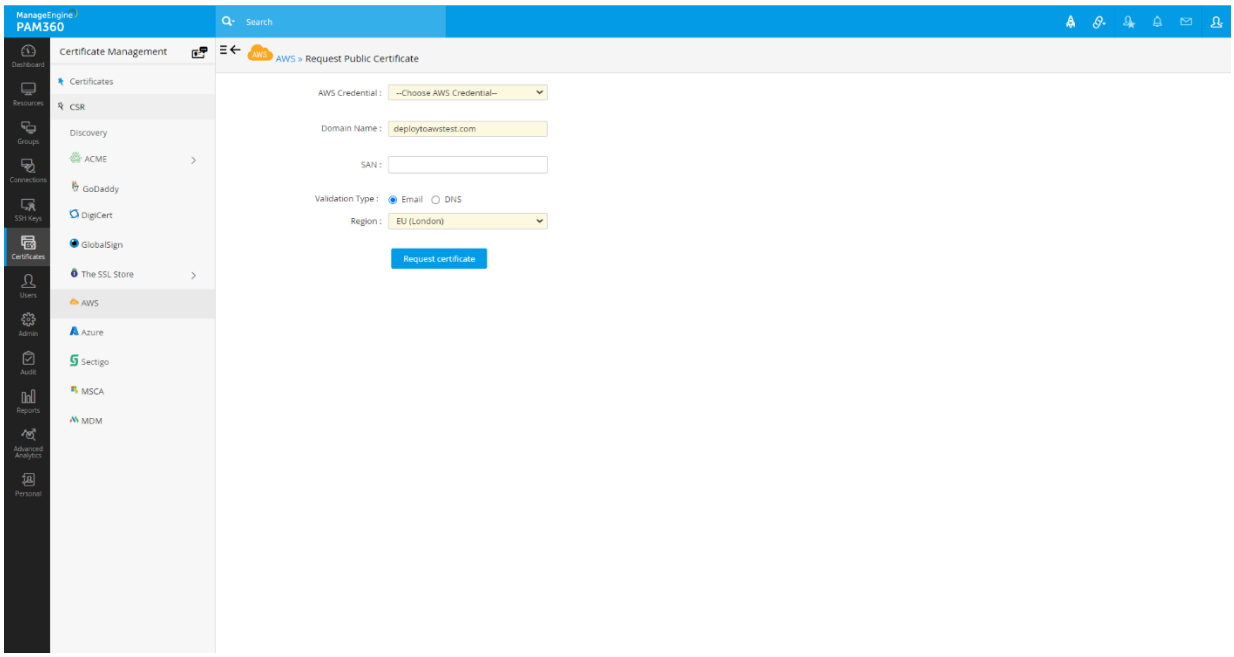
If there is a mismatch in the deployed certificates, they will be marked in red in the AWS tab in PAM360.

4. Requesting Certificates from AWS-ACM

PAM360 allows you to request both Public and Private certificates from AWS-ACM and manage them from the PAM360 interface.

4.1 Request Public Certificates

1. Navigate to **'Certificates >> AWS'**.
2. Click the **Request Certificate** dropdown and click **Public Certificate**.



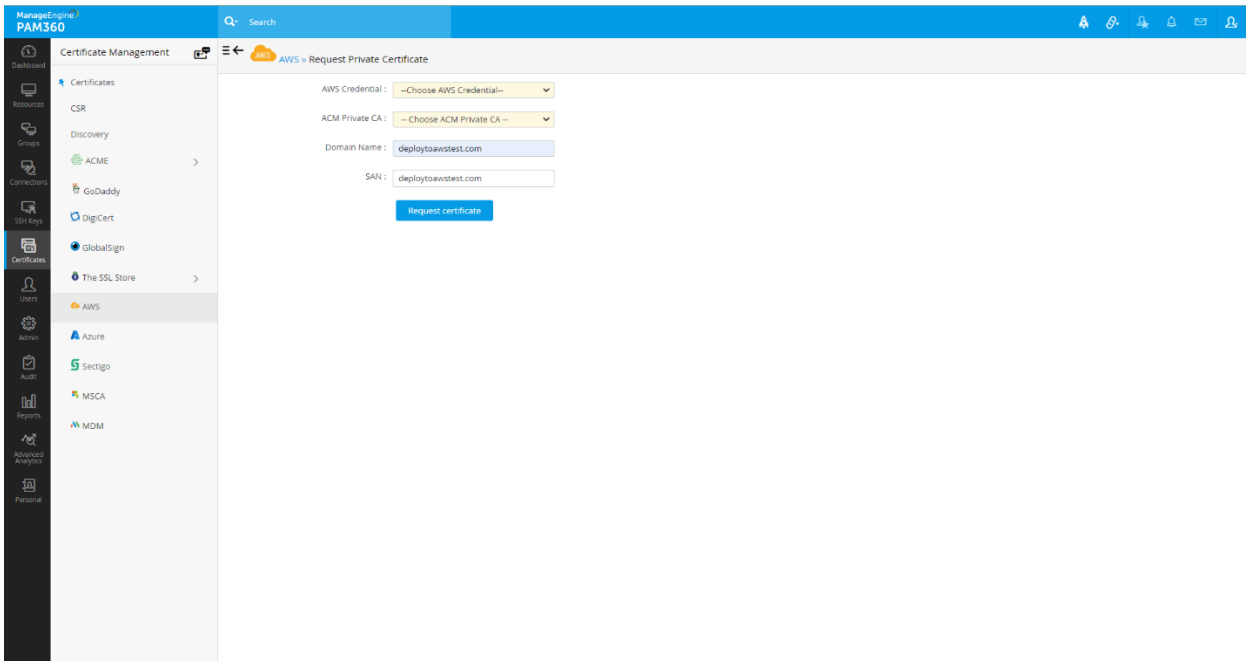
In the page that appears, fill in the following attributes:

1. Select your **AWS Credential** from the dropdown.
2. Enter the **Domain Name** and **SAN**.
3. Choose a Validation Type: **Email** or **DNS**.
4. Click the **Region** from the dropdown.

Now, click **Request Certificate**. The certificate matching the credentials you have provided will be imported into PAM360. Please note that Public Certificates from AWS-ACM do not have a private key.

4.2 Request Private Certificate

1. Navigate to 'Certificates >> AWS'.
2. Click the Request Certificate drop-down and click Private Certificate.



In the page that appears, fill in the following attributes:

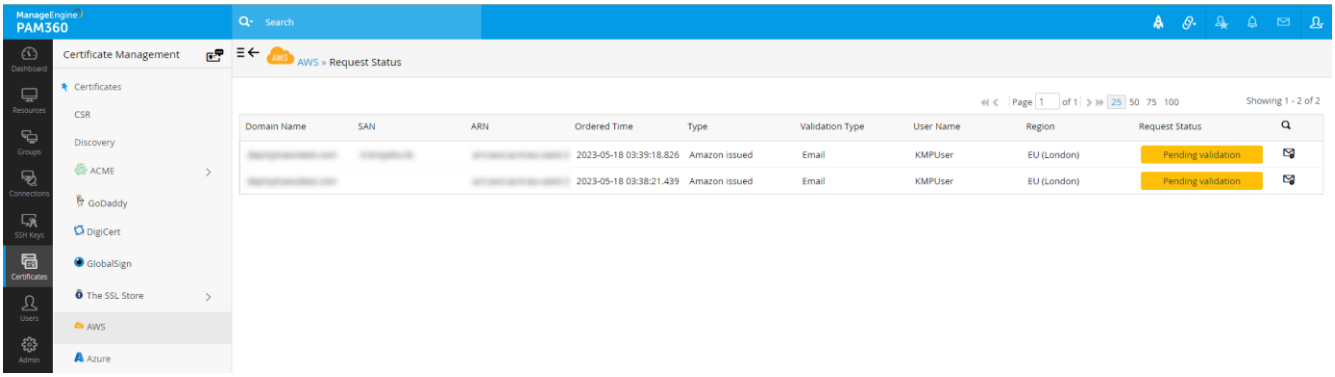
1. Select your **AWS Credential** from the dropdown.
2. Select an **ACM Private CA** from the dropdown.
3. Enter the **Domain Name** and **SAN**.

Now, click **Request Certificate**. The requested certificates will be issued and added to the repository upon validation.

4.3 Request Status

Once you request certificates from AWS-ACM, click the Request Status option from the top menu to view and validate the status of the certificates.

In this page, you can view the request, renewal, and domain validation status of both private and public certificates. Once a certificate request is created, the status of the certificate will appear in this table as Pending Validation/Deploy Challenge/Sync Records.



If you have configured DNS-based challenge verification, click the status to deploy the challenge. The status will change to Deploy Challenge and the validation process will begin. Once it is complete, the status changes to Issued.

5. Domain Validation, Certificate Issue, and Deployment

Once the certificate authority receives your order, you will have to go through a process called domain validation and prove your ownership over the domain upon the completion of which you will receive the certificate. PAM360 supports all the two validation methods:

1. Email Validation
2. DNS Validation

5.1 Email Validation

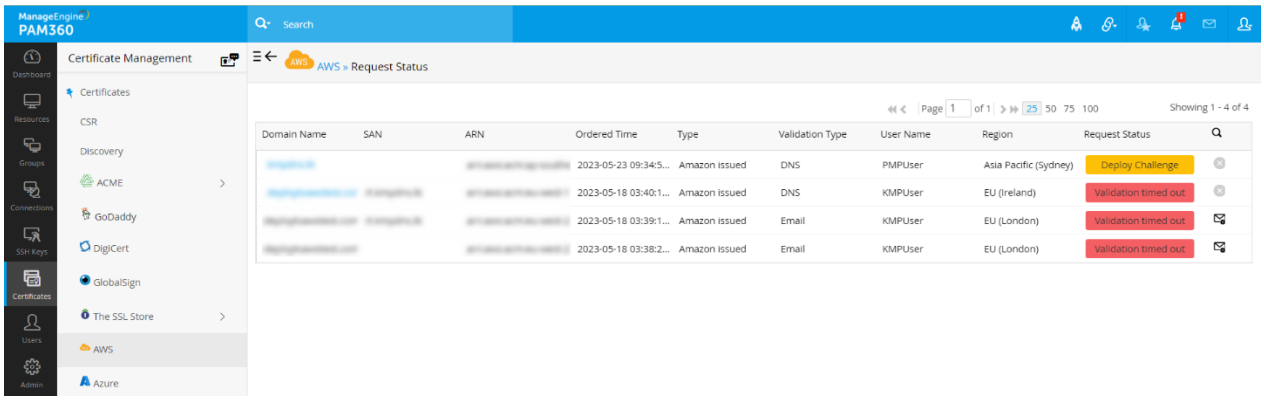
1. In email validation, the certificate authority sends a verification email to the approver email ID specified when placing the certificate order.
2. This email will guide you through the steps that need to be performed to complete the validation procedure. Go to verify option and verify via email. Go to request status and click pending validation to obtain the certificates.
3. After completing the steps, navigate to the PAM360 server, and switch to the AWS tab.
4. Upon successful verification, the certificate authority issues the certificate which is fetched and added to PAM360's secure repository. You can access the certificate from the **Certificates >> Certificates** tab.

Click here for more details on certificate deployment.

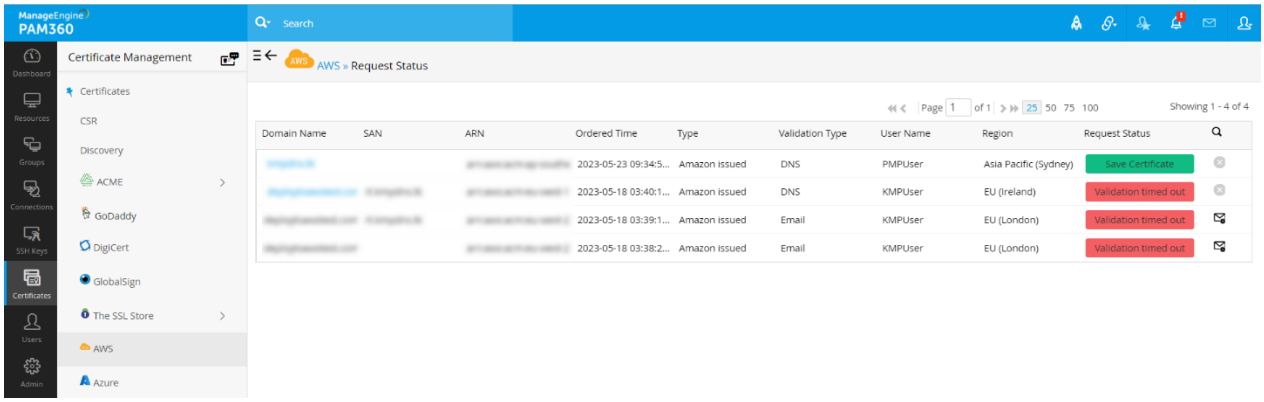
5.2 DNS Validation

If you have opted for DNS validation when ordering a public certificate with a provided details of the DNS:

1. Go to the **Request Status** page and click the **Deploy Challenge** option to create the DNS record.



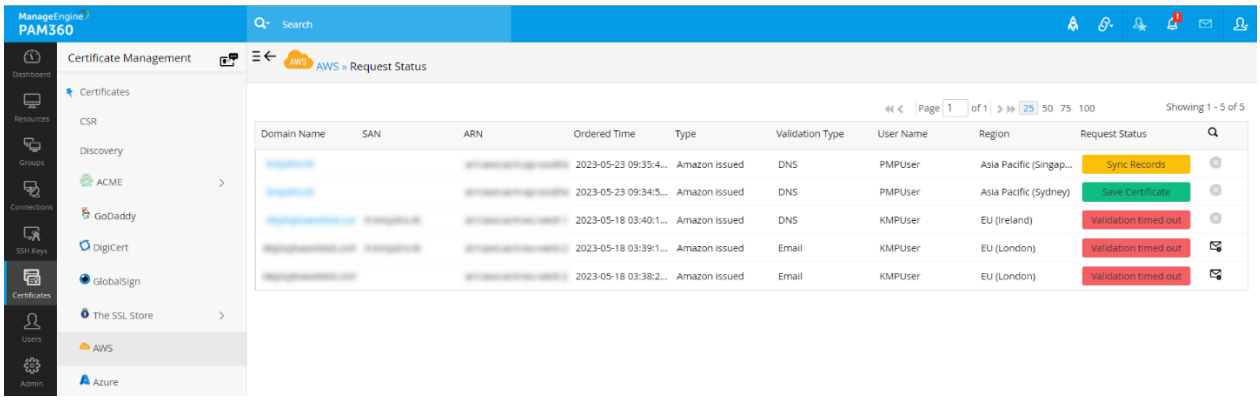
2. The DNS challenge values and text records are automatically deployed in the corresponding DNS servers post the above action.
3. Upon successful DNS validation, the certificate authority issues the certificate.



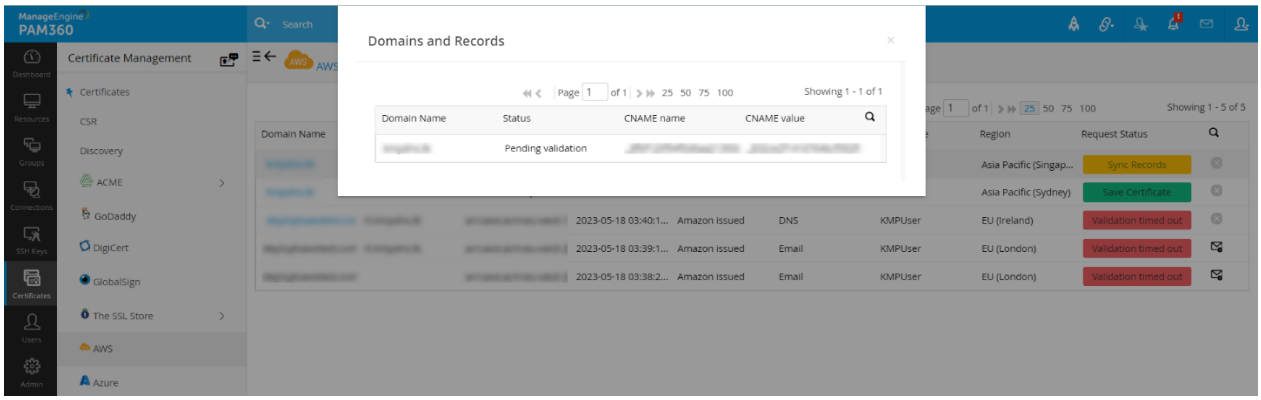
4. Once the certificate is issued, the status will change accordingly, and you can access the certificate from the **Certificates >> Certificates** tab.

If you have opted for DNS validation when ordering a public certificate without the DNS details:

1. Go to the **Request Status** page and click the **Sync Records** option to create the DNS record.



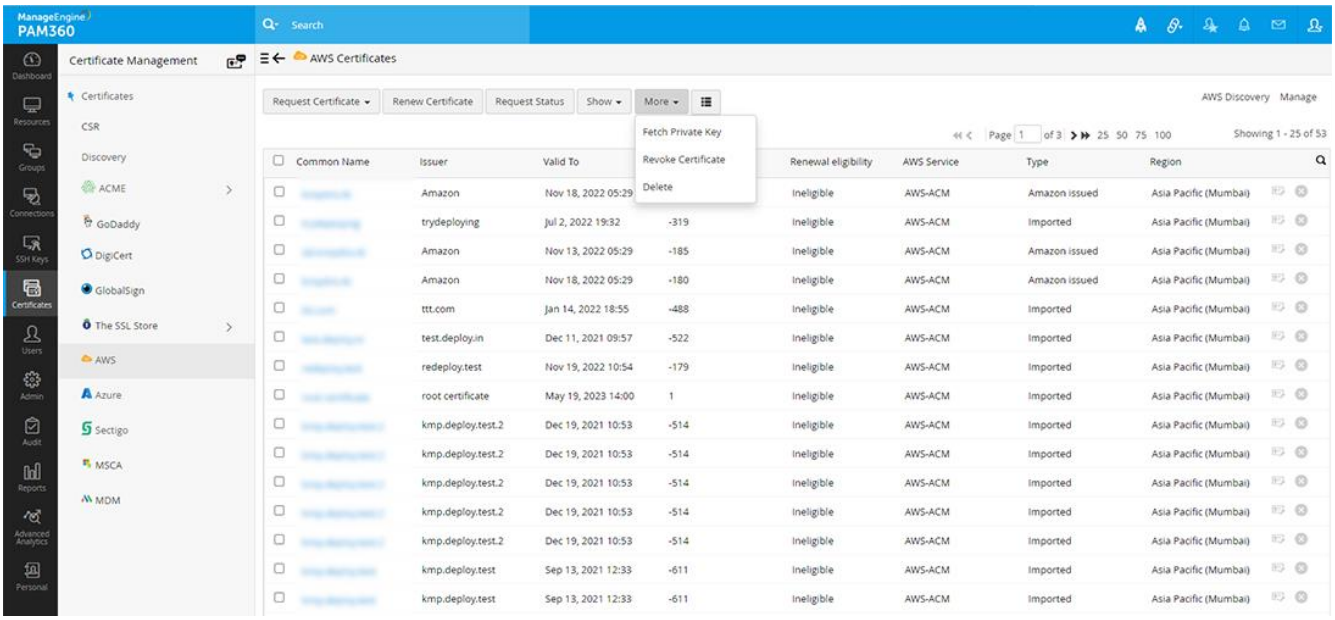
2. The DNS challenge value and text record will be displayed in a pop-up. Copy and paste the text records manually into the domain server.



3. You can sync the order's current status by clicking on the button under **Request Status** for that particular order.
4. Upon successful DNS validation, the certificate authority issues the certificate and you can access the certificate from the **Certificates >> Certificates** tab.

6. Renewing, Revoking, Deleting & Fetching Private Key of Certificates

PAM360 allows you to renew Private certificates. When a certificate renewal is requested from PAM360, the renewed certificate will be retrieved from AWS-ACM. However, if you renew a certificate in AWS-ACM, it is not automatically updated in PAM360. To fix the mismatch, rediscover the certificates in PAM360 and re-populate the data.



6.1 Renewing the Certificates

1. Navigate to **'Certificates >> AWS'**.
2. Select the required order and click **Renew Certificate** from the top menu.

3. Complete the DNS validation procedure if necessary.
4. On successful validation, the certificate is issued and the new version is automatically updated in the **Certificates >> AWS** tab.

Please note that only the certificates that satisfy all criteria mentioned here will be renewed. Click here to read about AWS's eligibility criteria for certificate renewal.

6.2 Revoking the Certificate Request

1. Navigate to **'Certificates >> AWS'**.
2. Select the certificate that needs to be revoked and click **More >> Revoke Certificate**.

Please note that the revoke option applies only to Private Certificates in AWS-ACM.
Revoking a certificate request removes the certificate entry from PAM360 only.

6.3 Fetching the Private Key

To fetch the private key of a Private Certificate, follow the below steps:

1. Navigate to **'Certificates >> AWS'**.
2. Select the required Private Certificate and click **More >> Fetch Private Key** from the top menu.

This operation fetches the private key of the selected private certificate from AWS-ACM.
Please note that is a paid option and might incur costs as per your AWS-ACM license.

6.4 Deleting the Certificate from the PAM360 Interface

1. Navigate to **'Certificates >> AWS'**.
2. Select the required certificate and click **More >> Delete** from the top menu.
3. The certificate request is deleted from the AWS tab.

Please note that using the Delete option simply removes the certificate from the PAM360 interface, you can no longer manage it from the product. However, it does not delete the certificate from AWS-ACM - the certificate can still be viewed and managed from the AWS console.

Integration with Azure Key Vault

PAM360 integrates with Microsoft Azure Key Vault — a cloud service for managing SSL certificates. This integration enables users to request, renew, and manage the SSL certificates stored in the Azure Key Vault by importing them into the PAM360 repository. You can automatically renew certificate requests and automate the end-to-end lifecycle management of SSL/TLS certificates stored and managed in the Azure Key Vault, directly from the PAM360 web interface.

1. How does the PAM360 - Azure Key Vault Integration Work?
2. Importing Azure Key Vaults
3. Discovering Certificates from Azure Key Vaults
4. Creating a Certificate Request
5. Renewing, Deleting, Filtering all Versions of Certificates

1. How does the PAM360 – Azure Key Vault Integration Work?

Let's say you manage a number of Key Vaults in the Azure portal and each of those Key Vaults contains a number of SSL certificates. PAM360 lets you add your Azure credentials in the product and then automatically imports the Key Vaults corresponding to your Azure credentials into the PAM360 repository. Once your Key Vaults are added, you may discover the certificates that are stored in the Key Vaults using the discovery operation. PAM360 allows you to create new certificate requests and renew the existing certificates that are both created in PAM360 and imported from Azure Key Vault. You can import and manage different versions of the same certificate from the Key Vaults.

Prerequisites:

1. To perform the PAM360 - Azure Key Vault integration, the following Azure Credentials are required: Application/client ID, Directory/tenant ID, Subscription ID, and client secret.

2. You must provide API Access permission to the Key Vault from which you wish to import certificates into PAM360. The Key Vaults you are importing into PAM360 must also have the following permissions: Key permissions, Secret permissions, Certificate permissions under Access Policies.

3. The Key Vault owner must have permission to list the key vaults. To grant this, go to **Access Control (IAM) >> Add >> Add role assignment** and select Assign access to as User, group, or service principal.

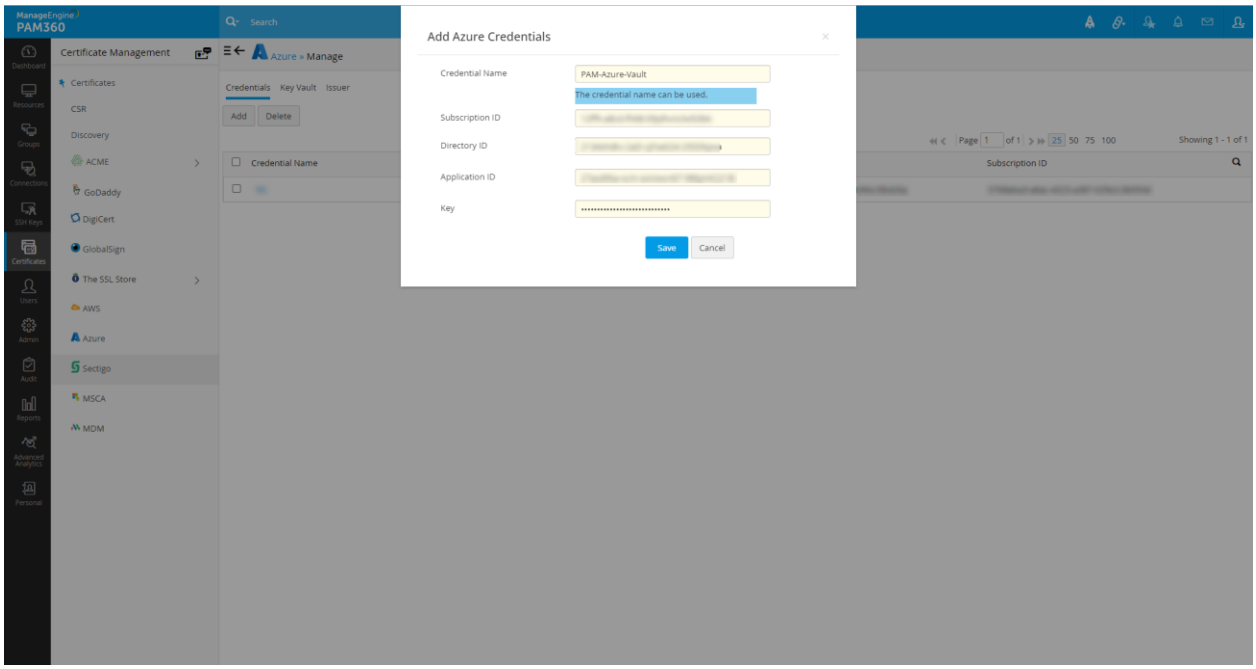
2. Importing Azure Key Vaults

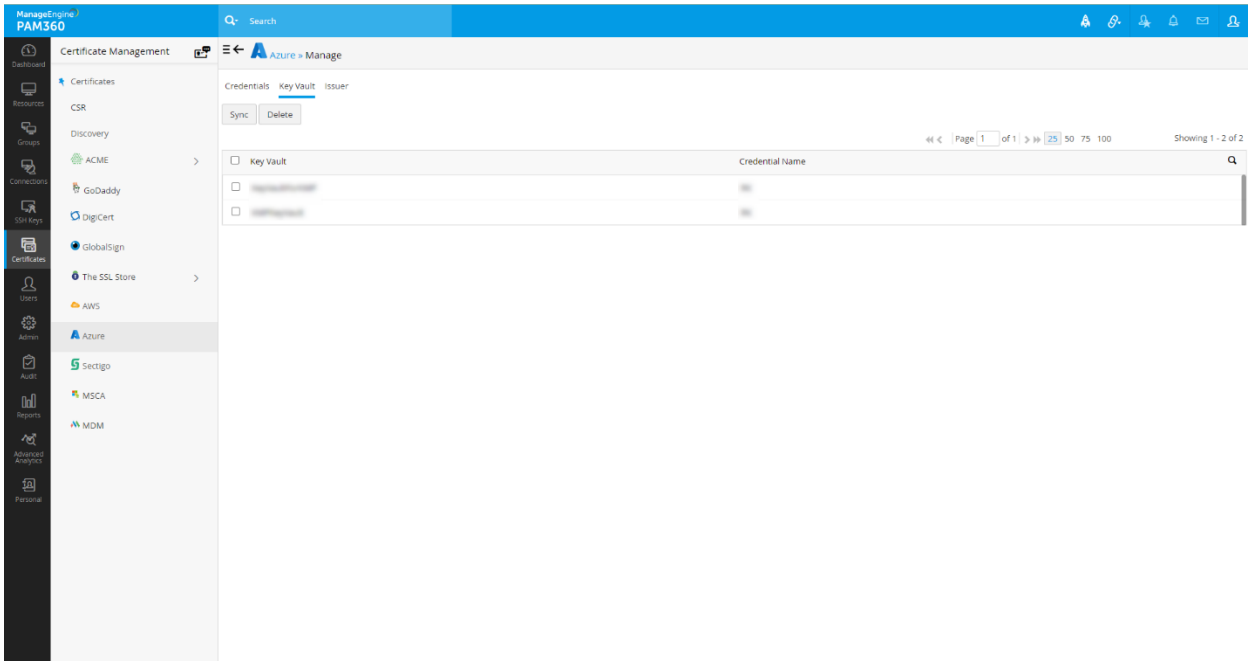
To begin importing Key Vaults and their corresponding certificates from the Azure portal, you must add your Azure credentials in the PAM360 interface.

2.1 Adding Azure Credentials

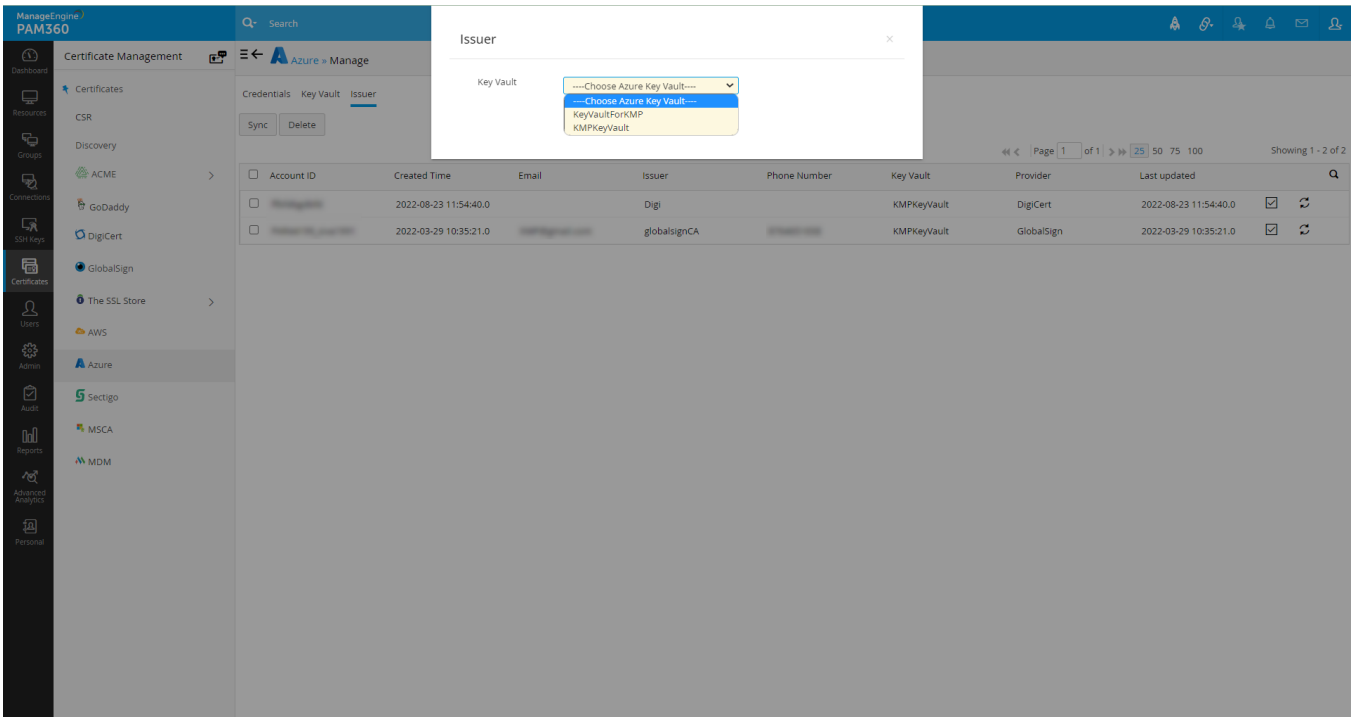
To import all key vaults that are being managed in the Azure portal, you must add your Azure credentials in PAM360. Follow the below steps:

1. Navigate to **'Certificates >> Azure'**.
2. Go to **Manage** and click **Add**.
3. In the **Add Azure Credentials** pop-up, enter the following attributes:
    a. Credential Name - enter a unique credential name
    b. Subscription ID
    c. Directory ID
    d. Application ID
    e. Key
4. Click **Save**.





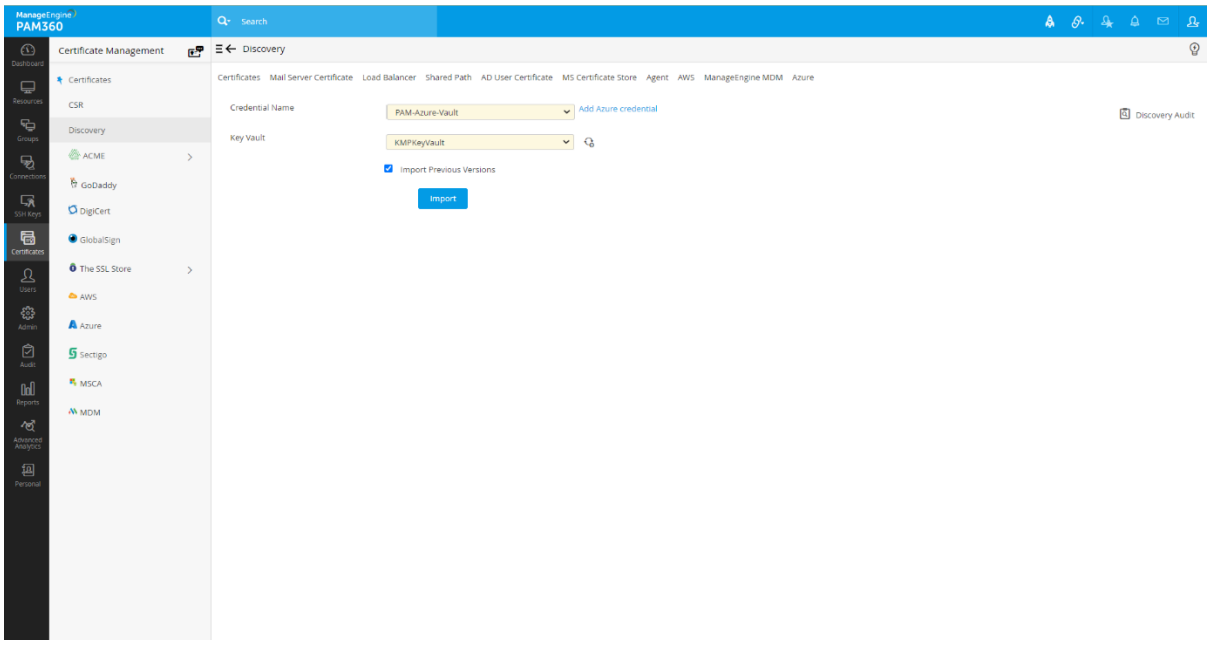
Once your credentials are saved, all the key vaults that are related to the saved credential will be automatically imported into PAM360. All the imported vaults will be visible under the Key Vault tab. In case the key vaults are not imported, click the **Sync** button to manually kick-start the process. If you have any Issuer IDs saved in your Azure portal, press **Sync** and choose a Key Vault from the pop-up that appears. Now all the issuer certificates from the selected Key Vault will be listed under the **Issuer** tab.



3. Discovering Certificates from Azure Key Vaults

PAM360 enables you to discover, import, and configure expiry notifications for SSL certificates managed in the Azure portal.

1. Navigate to **'Certificates >> Discovery >> Azure'**.
2. Choose the following attributes from the dropdowns:
   a. **Credential Name** - The Azure credential from which you wish to import key vaults.
   b. **Key Vault** - Choose the required key vault from which you wish to import certificates. In case you find that the certificates list is not fully updated, click the sync icon available beside the Key Vault drop-down to manually sync the certificate list from the Azure portal.
   c. Select the **Import Previous Versions** option to import all available versions of the certificates in the key vault. Click **Import**.



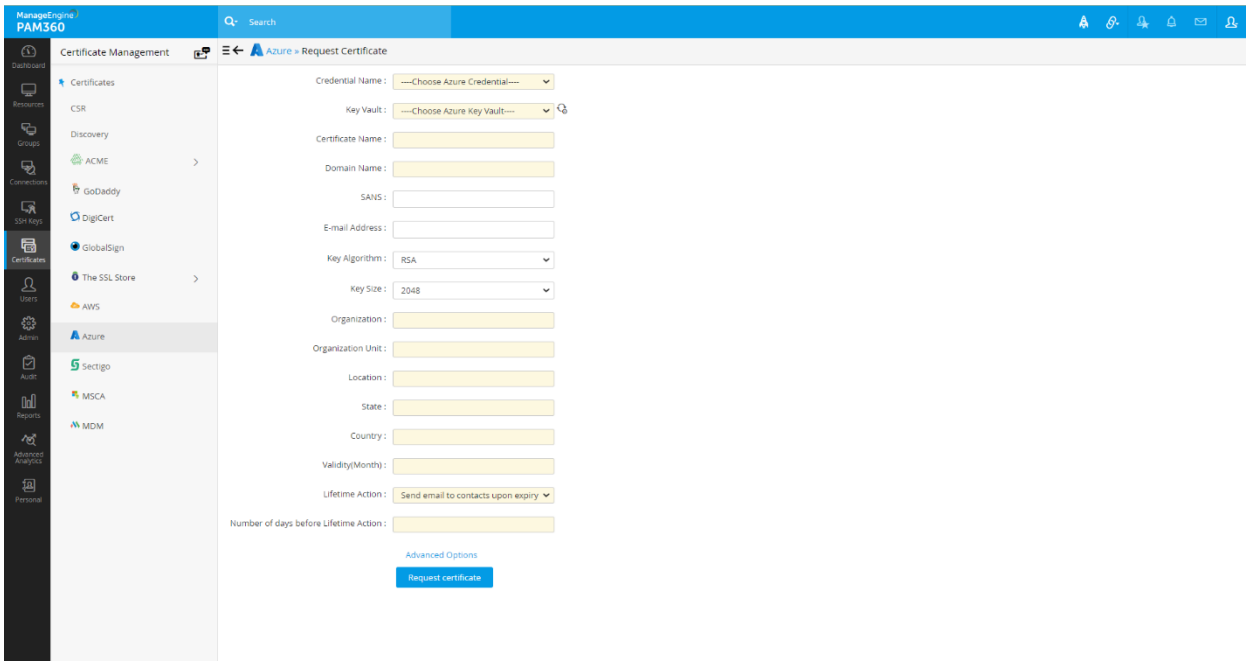
Now all the certificates from the selected Azure Key Vault will be imported and populated in the **Azure** tab.

> **Note:** Please note that every version of a certificate will be considered as an individual certificate in PAM360 and therefore will impact your license count.

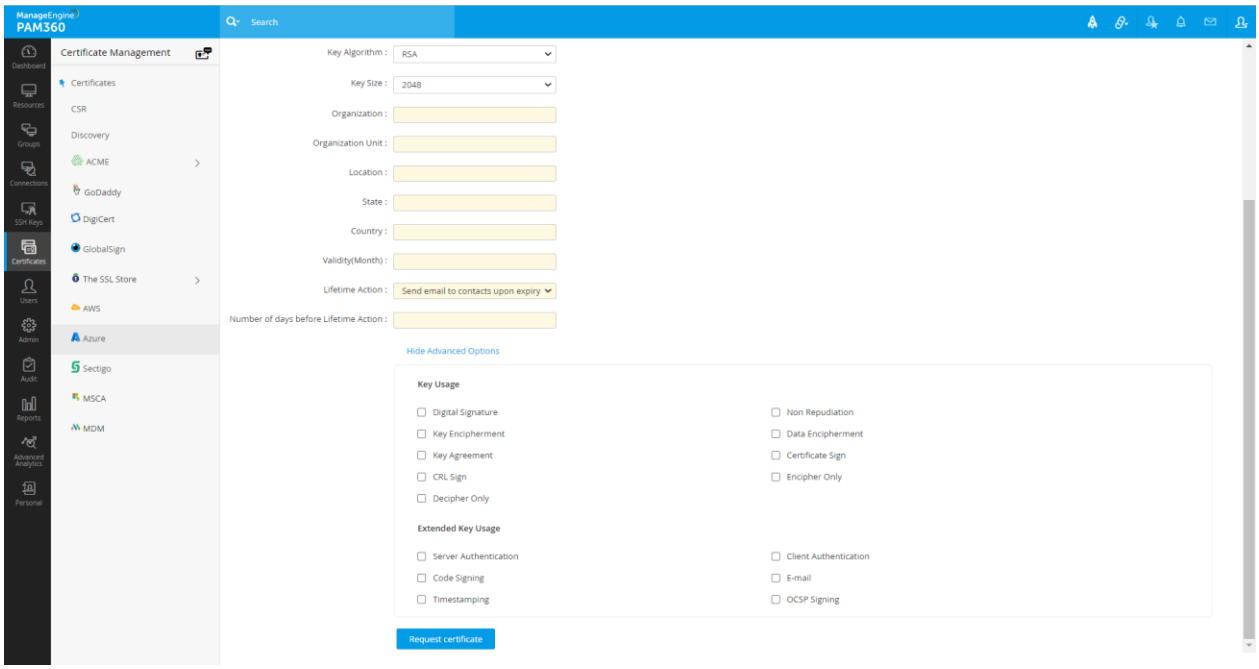
4. Creating a Certificate Request

PAM360 allows you to create SSL certificate requests for your Azure credential in the Azure key vault that you require. You can even create new versions of existing certificates by providing the same certificate name. All the certificate requests created in PAM360 will be automatically updated in the Azure portal. Follow the below steps:

1. Navigate to **'Certificates >> Azure'** and click **Request Certificate**.
2. Choose your **Azure Credential** and the required key vault from the dropdown.
3. Provide attributes such as the certificate name, domain name, SANs - You can add multiple SAN values separated by a comma.
4. Enter an email address, choose a **Key Algorithm** and **Key Size** from the dropdowns and enter location details.
5. Enter the certificate validity in months and choose a **Lifetime Action** from the drop-down. You can choose to either auto renew the certificate upon expiry or choose to send an email notification to your certificate contacts in the Azure portal.
6. Enter the number of days before which the chosen Lifetime Action must be invoked.



7. To add optional properties to the new certificate, click **Advanced Options** to expand the menu. Here, there are two categories of options, **Key Usage** and **Extended Key Usage**. Select the required options to set the preferred flags for the certificate to denote the purpose for which the new certificate may be used. The Key Usage options include Non Repudiation, Digital Signature, Data or Key Encipherment, Server/Client Authentication etc. You can choose the properties and mark them as critical by selecting the checkbox.

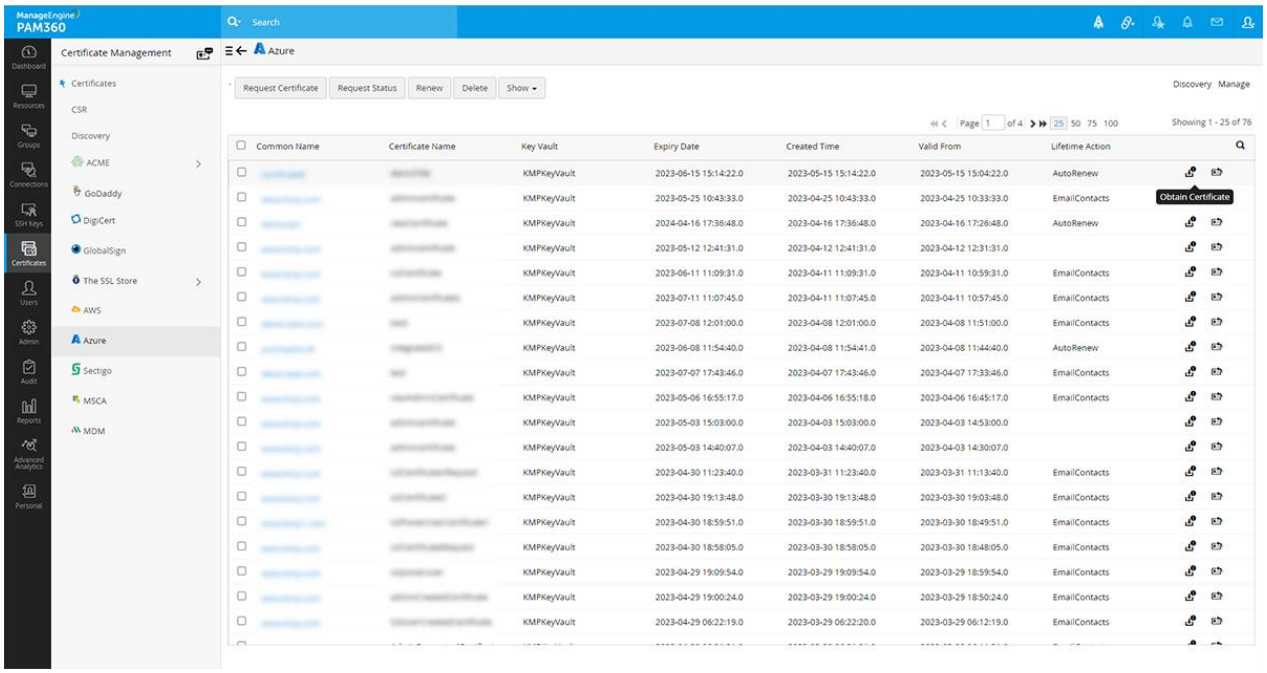


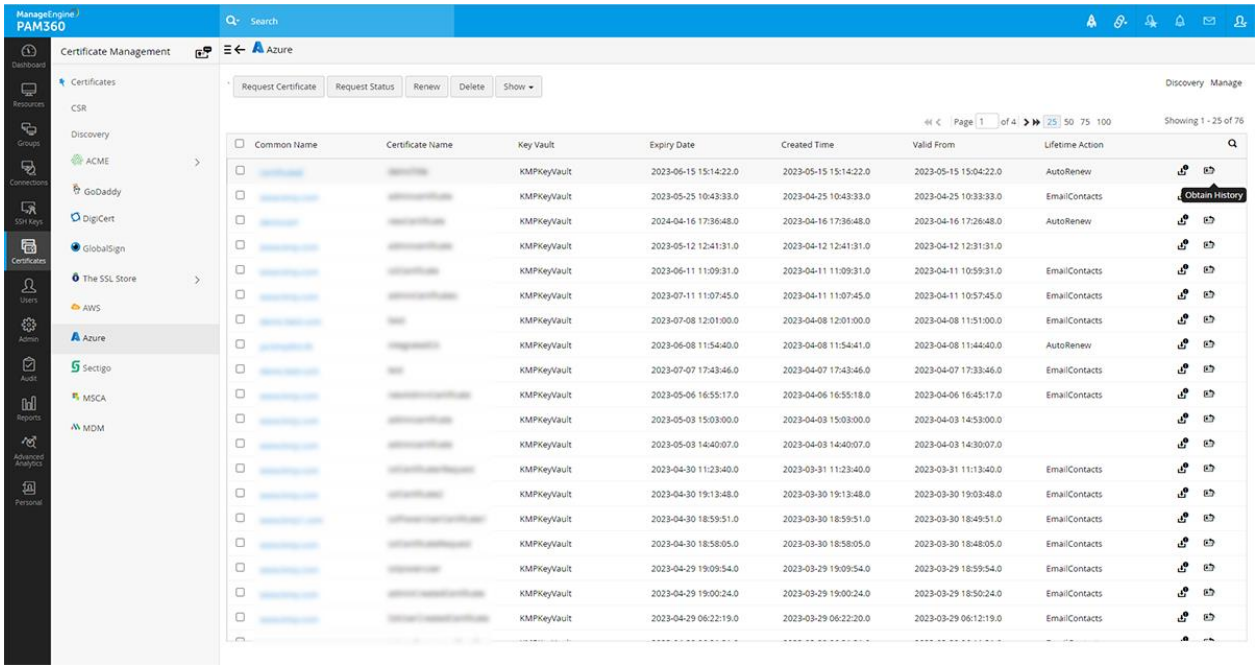
8. After adding all the details, click **Request Certificate**. A new certificate request is created in both PAM360 and the Azure portal.

Once the request is created, go to the **Request Status** tab to view the status and other details pertaining to a certificate. To obtain the latest certificate from your request, click the **Obtain**

Certificate option available beside the certificate. The following operations can be done on the certificates being managed from the Azure tab:

1. **Obtain Certificate** - This option retrieves the selected certificate from the Azure portal.
2. **Obtain History** - This option retrieves all the versions of the selected certificate from the Azure portal.



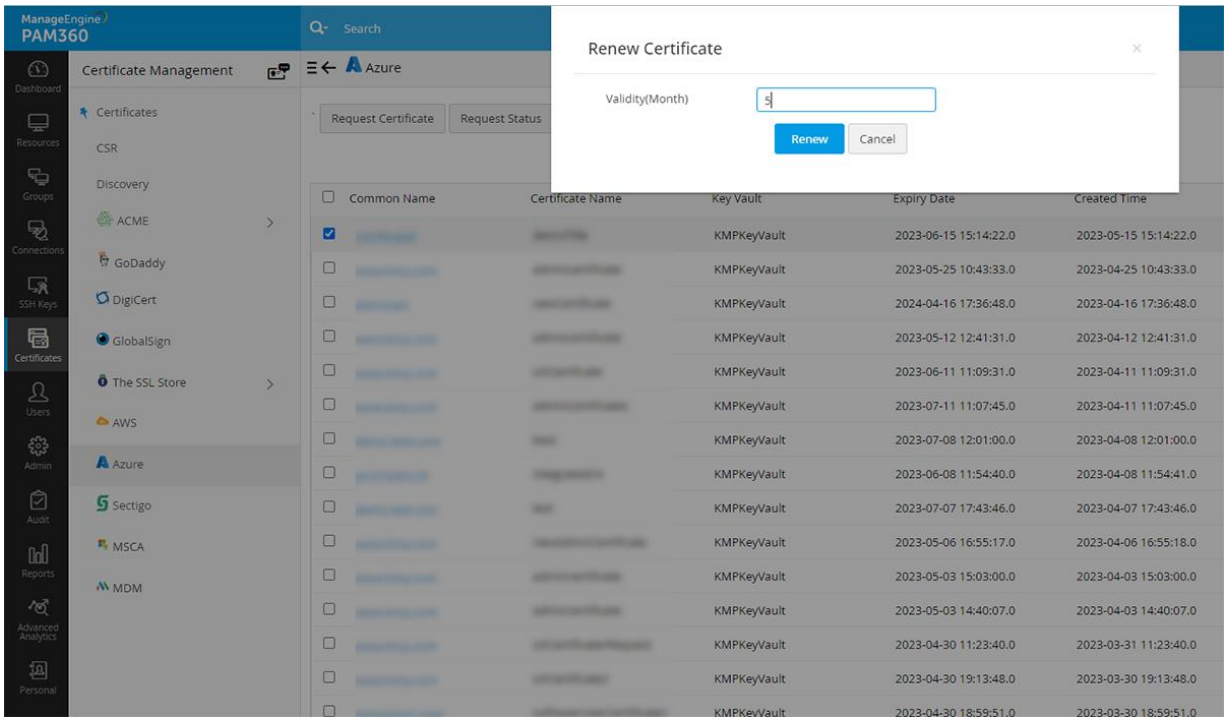


5. Renewing, Deleting, Filtering all Versions of Certificates

5.1 Renewing Certificates

PAM360 allows you to renew Azure certificates right from the PAM360 interface.

1. Select a certificate that you wish to renew and click the Renew option at the top.
2. Enter the validity in months and click Renew. The certificate will be renewed with the specified validity period and will be updated in both PAM360 and the Azure portal.



Notes: Please note that you cannot renew the following certificates:

1. Certificates that were issued by a third-party issuer and are currently being managed in the Azure Portal.

2. Previous versions of existing certificates.

5.2 Deleting Certificates

To delete certificates:

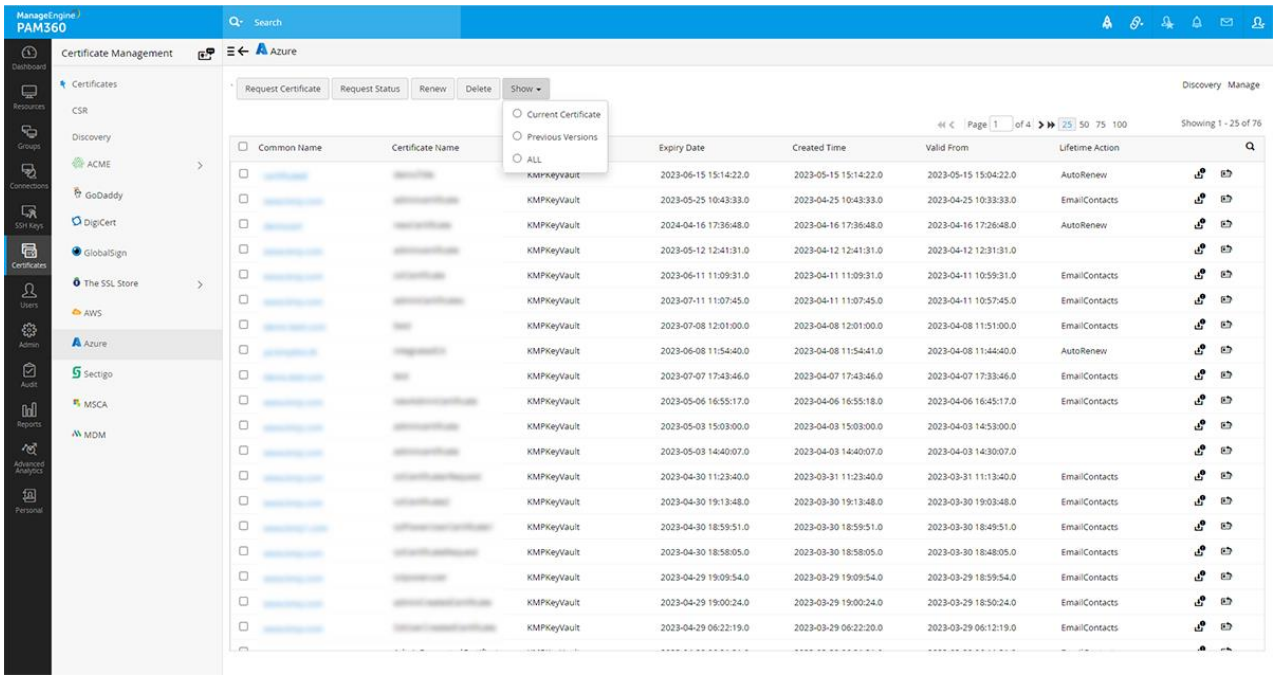
1. Select one or more certificates using the checkboxes.
2. Click **Delete** from the top.

Note: Please note that the certificate will be deleted only from the PAM360 interface and this operation will not impact the certificate's status in the Azure portal.

5.3 Filtering Certificates

To filter versions of certificates, click the Show drop-down and choose from the options:

1. **Current Certificate** - This option will display only the current versions of the certificates.
2. **Previous Versions** - This option will display older versions of the available certificates.
3. **All** - This option will display all versions of the available certificates.



Integration with Sectigo Certificate Manager

PAM360 integrates with Sectigo Certificate Manager (SCM), a PKI management platform that specializes in managing SSL/TLS certificates, SSH keys, and various other digital identities. The integration leverages SCM's API and allows PAM360 to act as a centralized platform where you can import and manage SSL/TLS certificates from the SCM. Automate the lifecycle management of these certificates through diverse operations that are supported by the integration.

In this document, you will learn the steps to manage the lifecycle of SSL/TLS certificates issued by the SCM, which includes importing existing orders, creating new certificate requests, deployment, and renewal of certificates.

Prerequisite:

Add the following base URL and port as an exception in your firewall/proxy to permit PAM360 to connect to the SCM.

URL: https://cert-manager.com/api

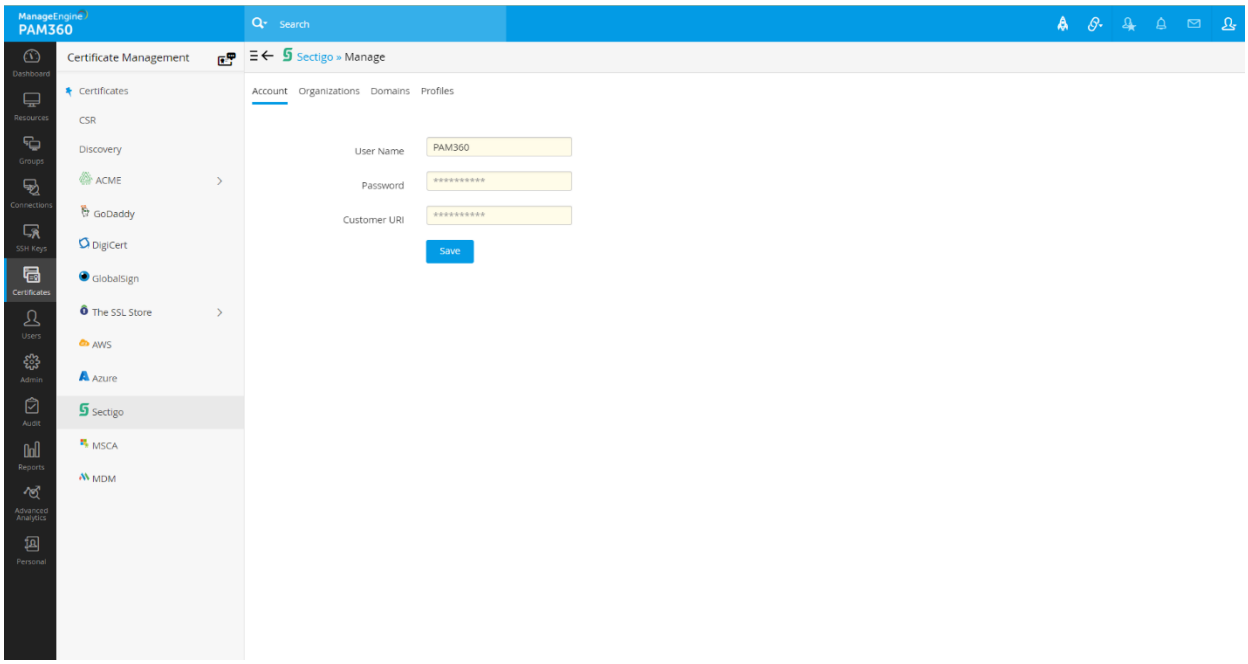
Port: 443

1. **Set up Sectigo Certificate Manager details in PAM360**
2. **Import existing orders**
3. **Create a new certificate order**
4. **Certificate issue**
5. **Renew, reissue, revoke, and delete certificates**

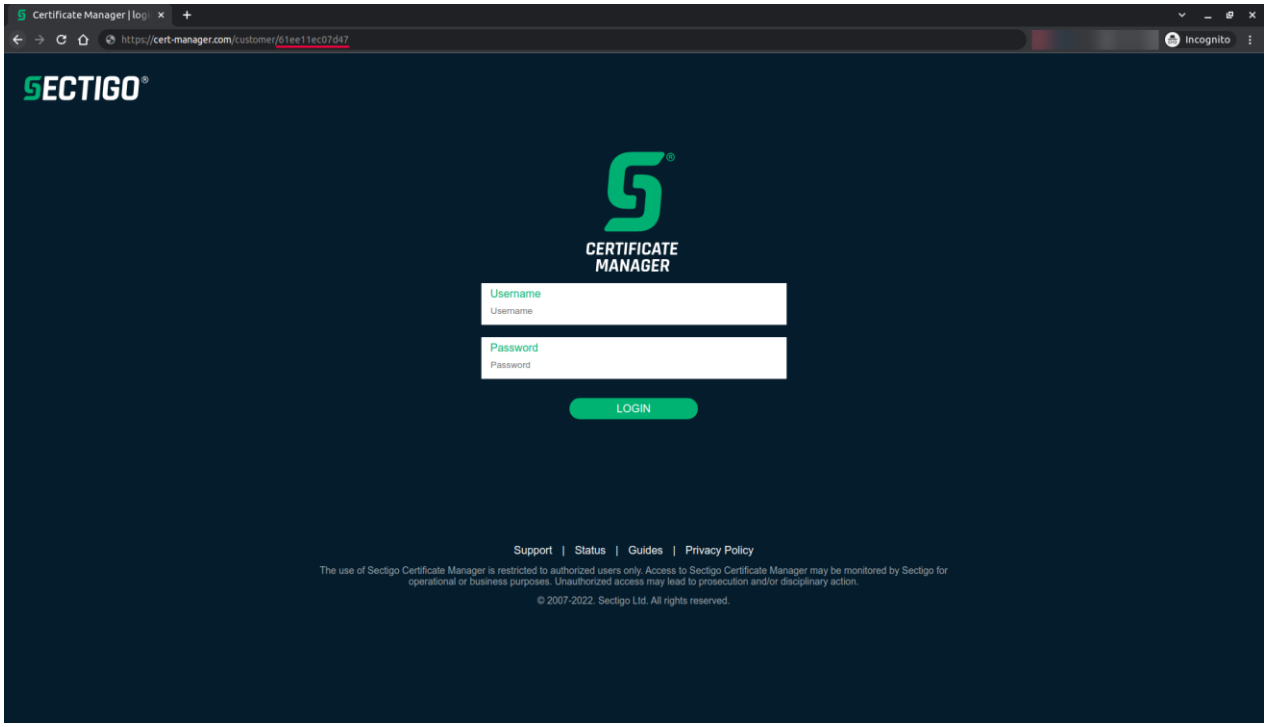
1. Set up Sectigo Certificate Manager Details in PAM360

To begin managing SSL certificates issued by Sectigo from PAM360, you must add your SCM account in PAM360 and link your unique Customer URI. If you do not have an SCM account, contact the Sectigo team to sign up and get your login credentials and the Customer URI. If you have an SCM account, follow the below steps to link your account with PAM360 and begin the integration process.

1. Log into the PAM360 web interface, navigate to **'Certificates >> Sectigo'** and click **Manage**.



2. Under **Account**, enter your SCM User Name, Password, your unique Customer URI and click **Save**. This is a one-time operation. You can find your Customer URI suffixed in the SCM login URL as shown below:

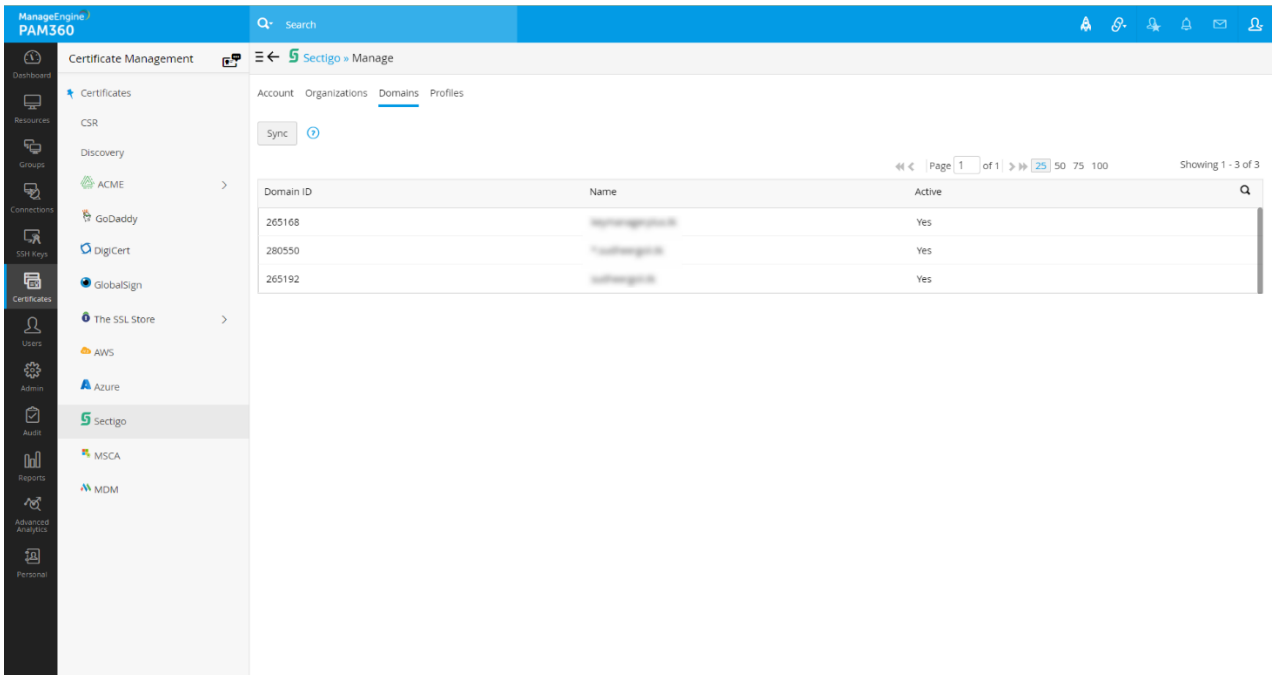


3. The SCM account details are saved and it is now successfully linked to your PAM360 account.

Important Notes:

1. For this integration to work as expected, the SCM account you are using must have the MRAO Admin user role in the Sectigo portal.
2. The user profile under the SCM account you are using must contain pre-validated domains and organizations. To send certificate requests, PAM360 fetches the existing domains, organizations, and certificate profiles from the SCM. Since the SCM issues certificates based on certificate profiles and pre-validated domains, this step is vital to ensure success of the integration.

4. Once the integration is complete, all the organizations, domains, and certificate profiles listed in your SCM account will be imported into PAM360 and displayed under individual tabs, along with their ID and status. This information is updated once a week through an automated schedule. To manually sync your account, click the **Sync** option available under each tab.

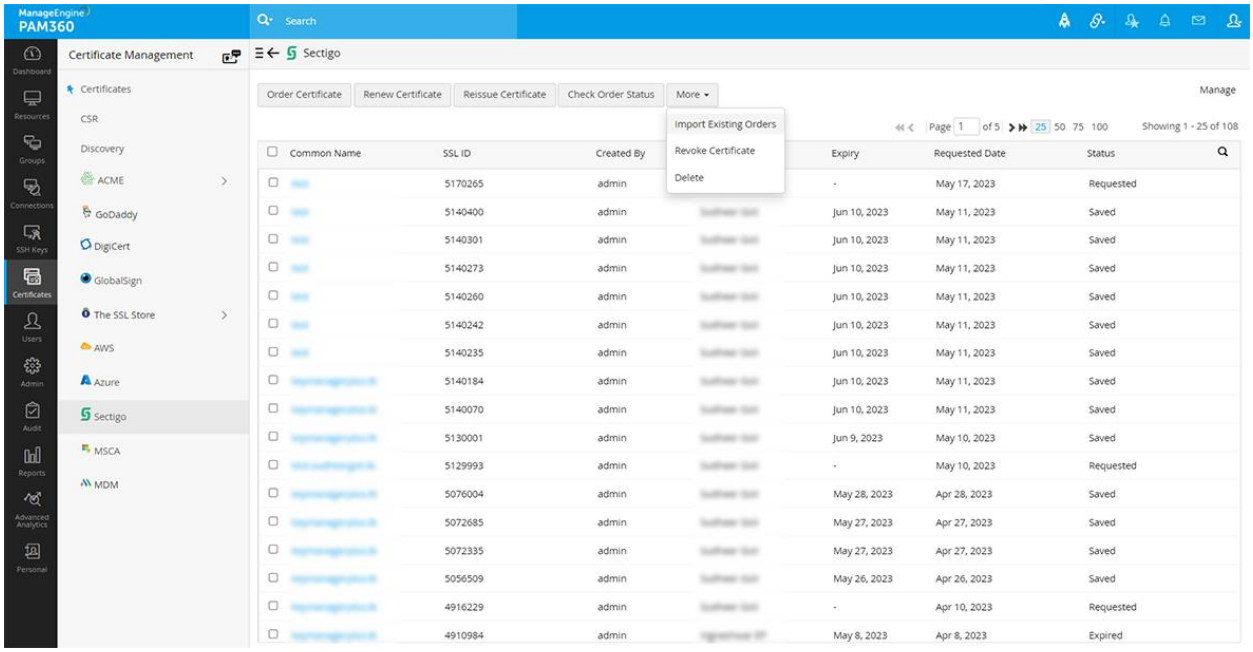


2. Import Existing Orders

If you have an active SCM account, you likely have existing certificate orders that can be managed using the Sectigo Certificate Manager. Apart from creating new certificate orders,

you can also import all the existing orders from the SCM portal and manage them from the PAM360 interface.

1. Navigate to the **'Certificates >> Sectigo'** tab in PAM360.
2. Click **More >> Import Existing Orders** from the top menu.

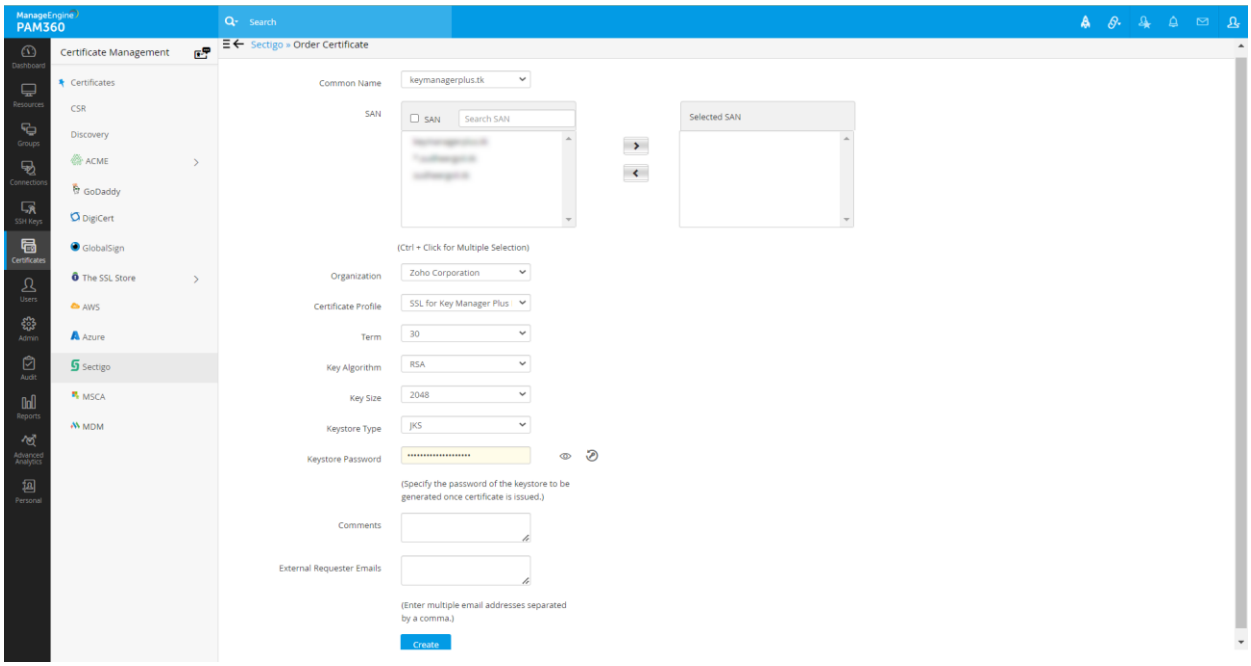


3. Select the required option and click **Import**.
4. All the existing certificate orders associated with your SCM account are imported into PAM360.

3. Create a New Certificate Order

Once you have successfully linked your SCM account with PAM360, you can start creating new certificate orders directly from PAM360. To place a new certificate order:

1. Navigate to the **'Certificates >> Sectigo'** tab and click **Order Certificate**.
2. In the window that opens, enter the following attributes: Common Name, SAN, Organization, Certificate Profile, Term, Key Algorithm, Key Size, Keystore Type, Keystore Password, Comments, and External Requester Emails.

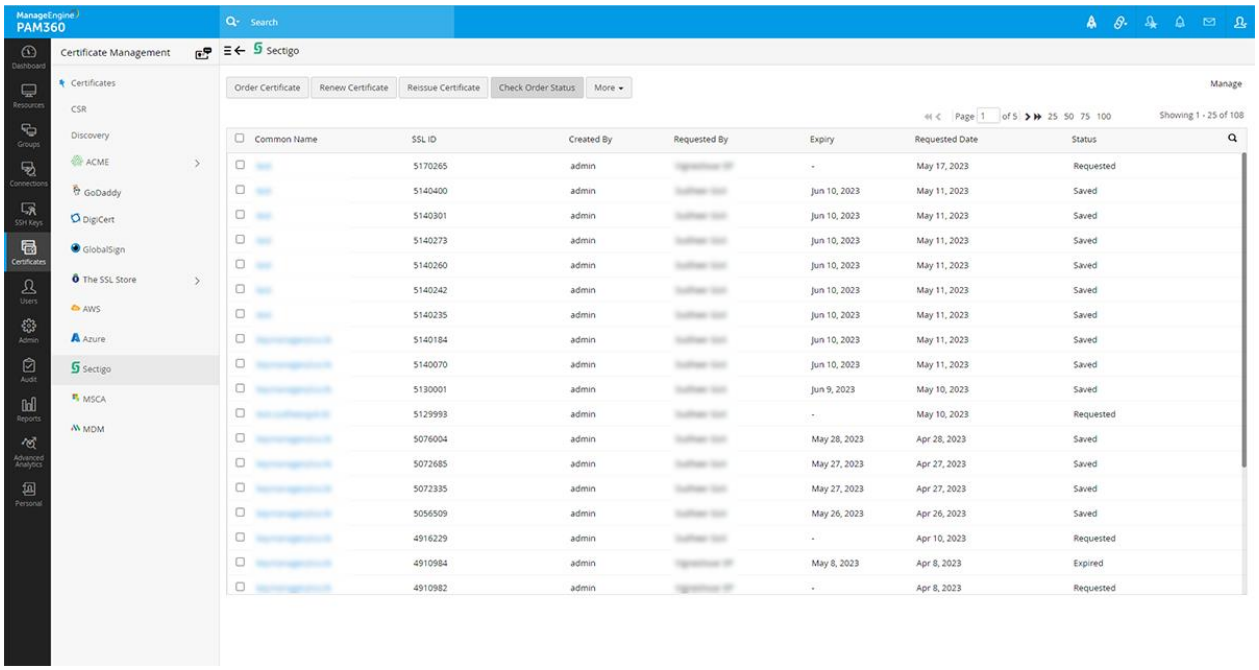


3. Ensure that you have selected the appropriate **Certificate Profile**. Also, ensure that the comment does not exceed 1024 characters.
4. Verify your details and click **Create**.

> **Note:** If you find any mismatch in the SCM-related details that are displayed here, please verify the details in the Sectigo portal and then perform a manual sync under **Sectigo >> Manage** in the PAM360 interface to refresh the details.

4. Certificate Issue

1. Once a certificate order is successfully created, you can view it under the **Certificates >> Sectigo** tab with its status displayed to the right.
2. To track the certificate availability for an order, select the order and click **Check Order Status** from the top menu.



3. Once a certificate is issued, it is fetched and added to the PAM360 certificate repository. You will be able to view it under **Certificates >> Certificates**.
4. Typically, the status of your certificate orders is checked automatically every day through a schedule. This way, whenever a certificate is available, it is fetched and added to PAM360 certificate repository.

> **Note:** Please note that the certificates that are issued are automatically added to PAM360 only if you have the required license count. If not, you must renew your PAM360 license before attempting to import any certificates.

5. Renew, Reissue, Revoke, and Delete Certificates

You can renew, revoke, delete or request reissue for certificates or cancel certificate orders from PAM360.

5.1 Renew a Certificate

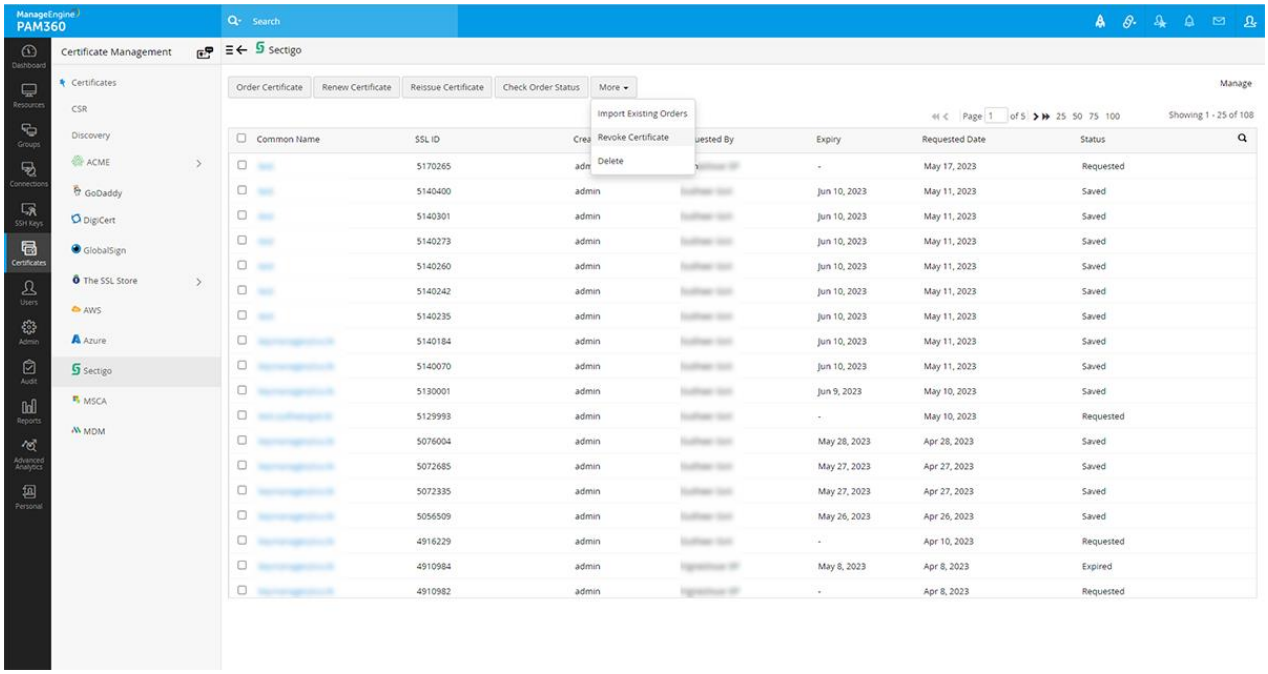
1. Navigate to **'Certificates >> Sectigo'**.
2. Select the required certificate and click **Renew Certificate** from the top menu.
3. Upon successful validation, the certificate is issued and will be automatically added to the PAM360 certificate repository.

5.2 Reissue a Certificate

1. Navigate to **'Certificates >> Sectigo'**.
2. Select the required certificate and click **Reissue Certificate** from the top menu.
3. Upon successful validation, the certificate is issued and will be automatically added to the PAM360 certificate repository.

5.3 Revoke a Certificate

1. Navigate to **'Certificates >> Sectigo'**.
2. Select the required certificate and click **More >> Revoke Certificate** from the top menu.
3. The certificate is revoked. Go to the **Certificates >> Certificates** tab and delete the certificate to remove it from the PAM360 repository.



5.4 Delete a Certificate

1. Navigate to **'Certificates >> Sectigo'** tab.
2. Select the required order and click **More >> Delete** from the top menu.
3. The certificate request is deleted from PAM360.

> **Note:** Please note that using the **Delete** option only removes the certificate from the PAM360 interface, and you can no longer manage it from the product. However, it does not delete the certificate request from the SCM—the certificate can still be viewed and managed from the SCM portal.

Manage Certificates using Microsoft Certificate Authority (MSCA)

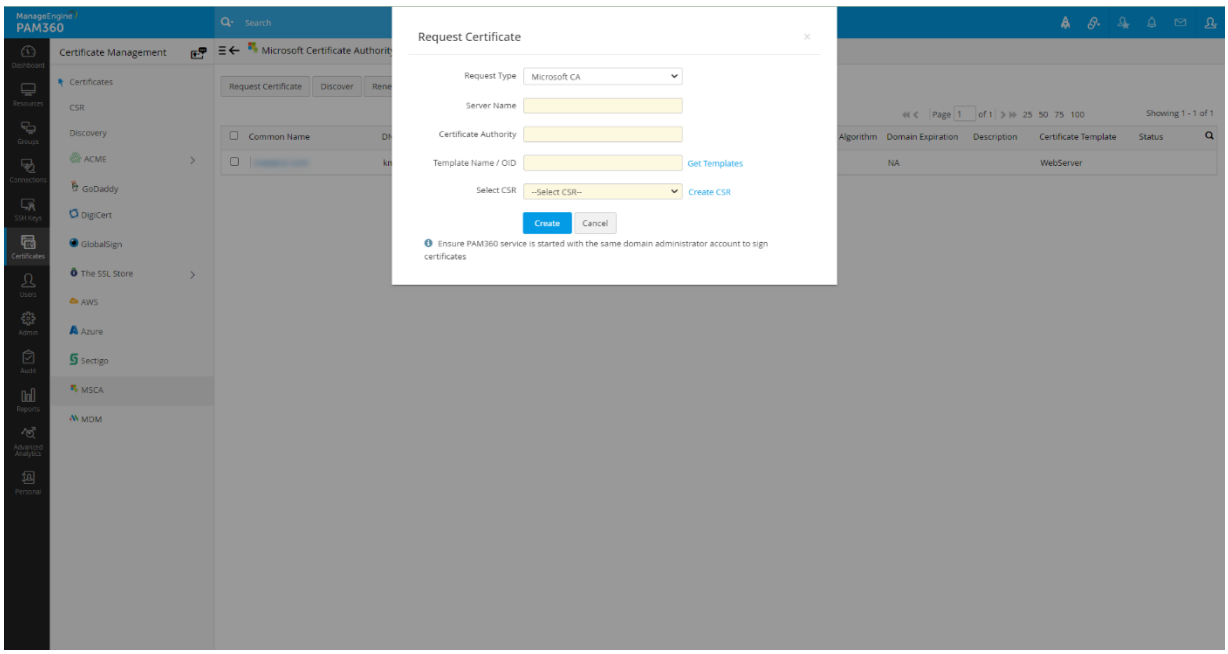
PAM360 allows users to discover and import certificates from Microsoft Certificate Authority. By the end of this document, you will have learned the following:

1. Request Certificate
2. Discover Certificate
3. Renew Certificate
4. Export Certificate
5. Revoke Certificate
6. Delete Certificate

Navigate to **'Certificates >> MSCA'**. All the certificates related to MSCA will be displayed here.

1. Request Certificate

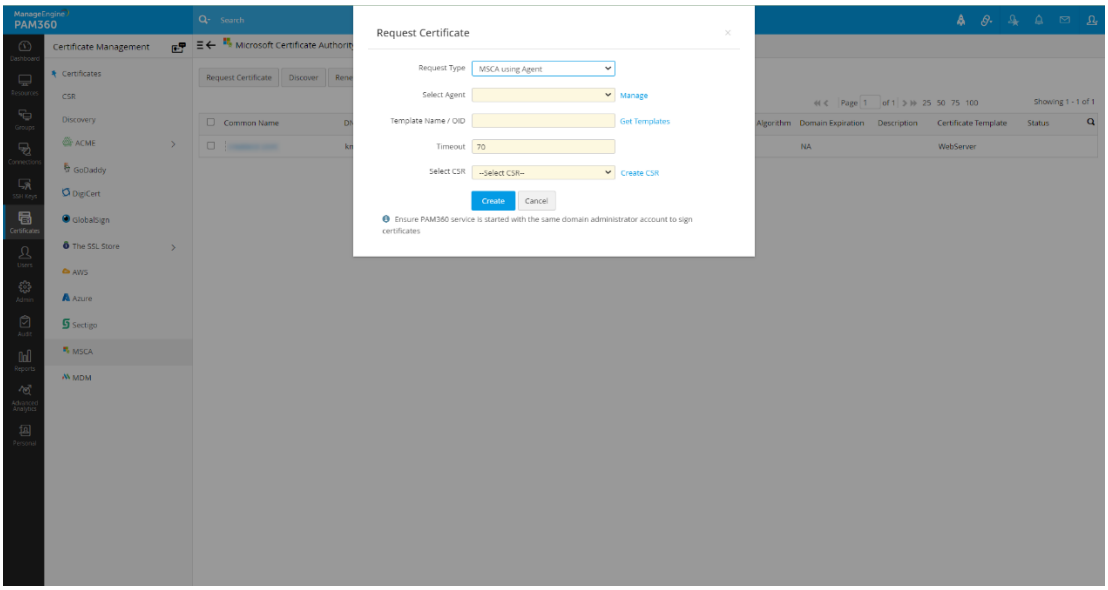
1. Click **Request Certificate** from the top pane.
2. In the pop-up that appears:
   a. Select the **Request Type** as **Microsoft CA** or **MSCA using Agent**.
   b. If you choose **Microsoft CA**, mention the **Server Name** that runs the internal CA and also the **Certificate Authority** name.



c. If you choose **MSCA using Agent**,

i. Select the **Agent** from the list available in the dropdown. You can also **Manage** the agent by clicking the link beside the dropdown. To know more about managing the agent, click here.

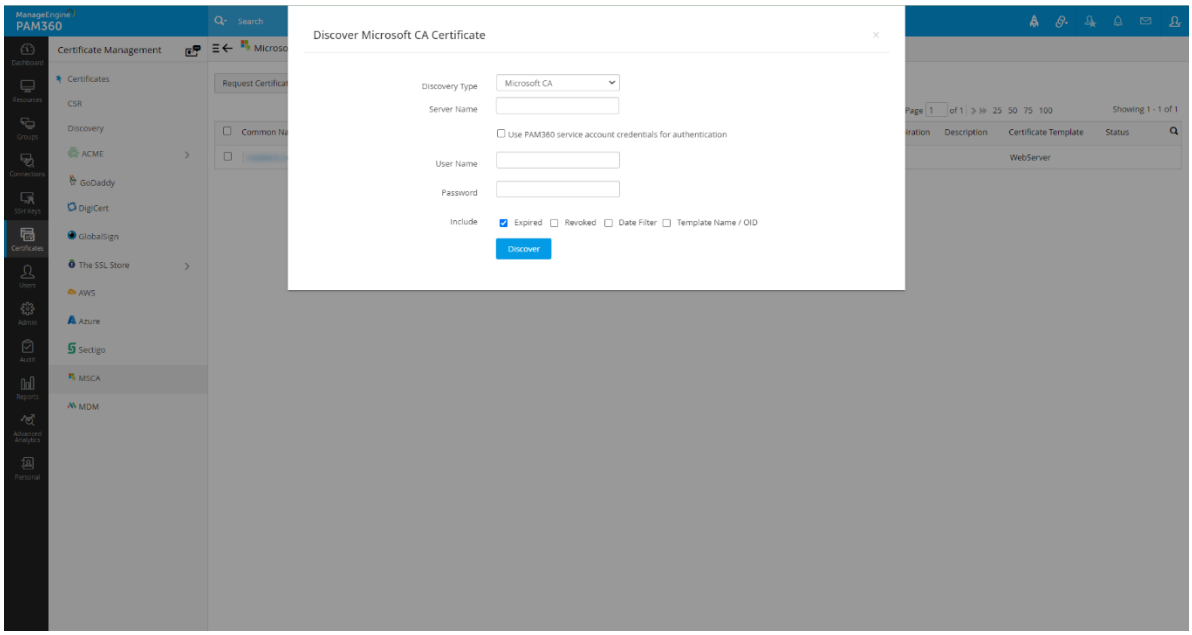
ii. Mention the **Agent Time out** in seconds within which the agent should respond. If the agent doesn't respond within the time-out period, the operation will be audited as failed.

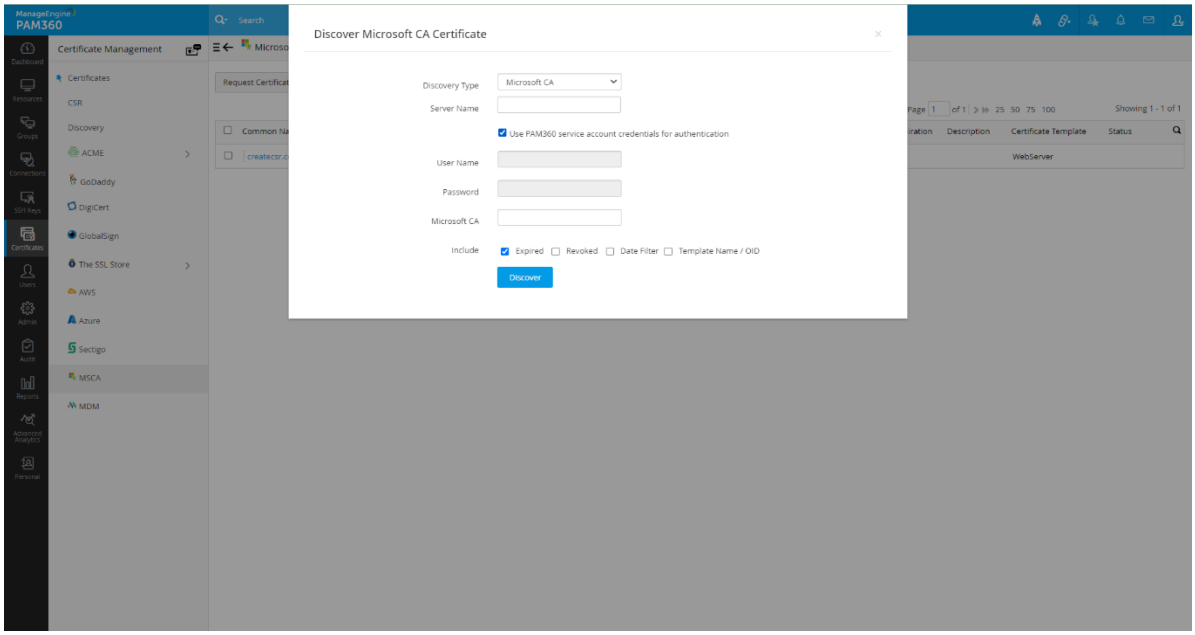


3. Select the **Template Name / OID** based on your requirement or select any of the pre-defined templates by clicking the **Get Templates** link.
4. Select the **CSR** from the dropdown or click the **Create CSR** link to create new CSR and click **Create**.

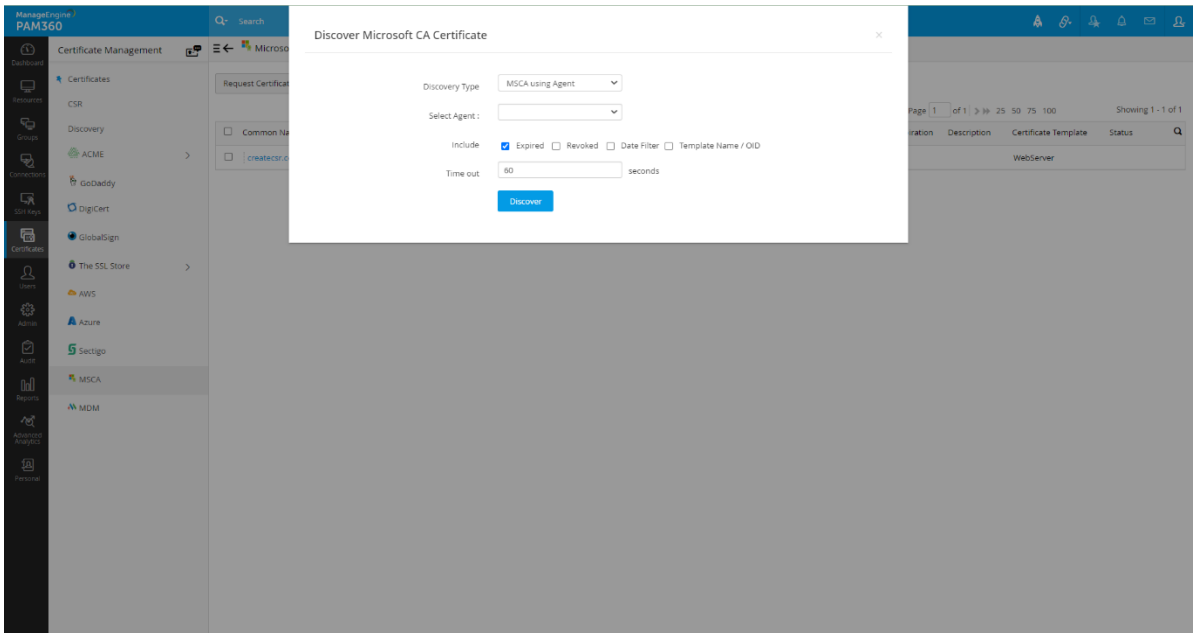
2. Discover Certificate

1. Click **Discover** from the top pane.
2. In the pop-up that appears:
   a. Select the **Discovery Type** as **Microsoft CA** or **MSCA using Agent**.
   b. If you choose to discover certificates issued by a particular MSCA, select **Discovery Type** as **Microsoft CA**.
   c. Enter the **Server Name**, required credentials, or choose **Use PAM360 service account credentials for authentication** and mention the **Microsoft CA**.





d. If you choose the **Discovery Type** as **MSCA using Agent**, Select the Agent from the dropdown and mention the agent **Time out** in seconds within which the agent should respond.



e. You can also choose to **Include** the **Expired** and/or **Revoked certificates**.

f. If you choose to **Include** the **Date Filter**, select the from and to dates.

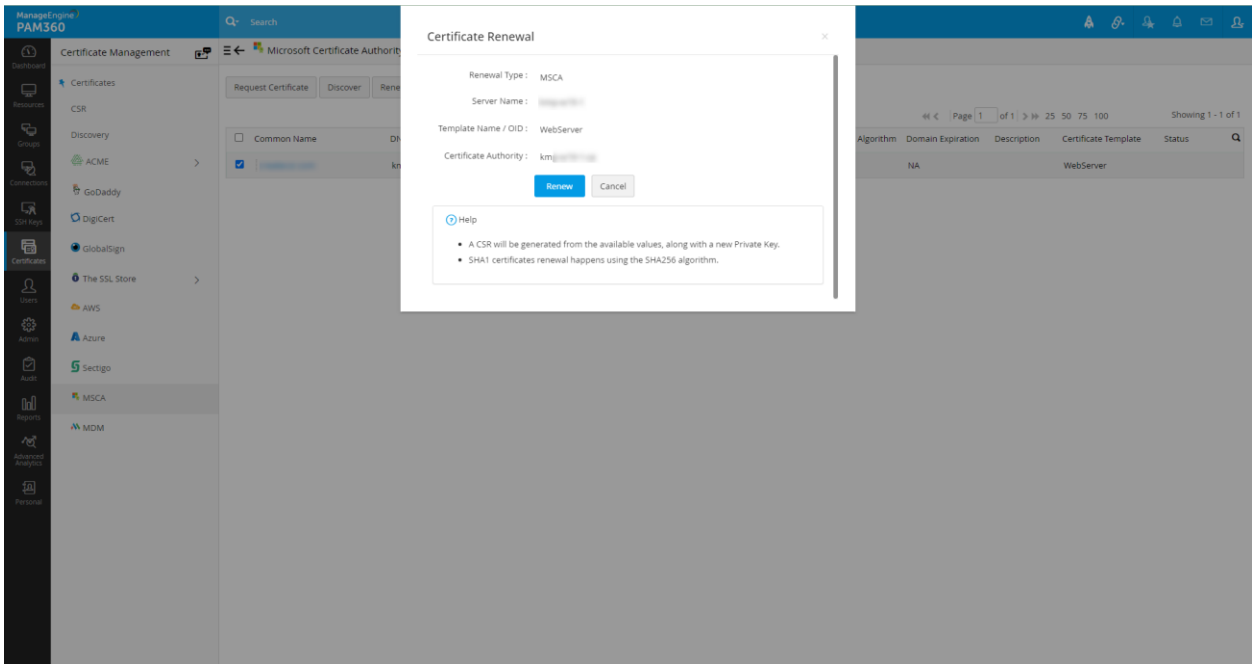
g. If you choose to **Include** the **Template Name / OID**, select the **Template Name / OID** based on your requirement or select any of the pre-defined templates by clicking the **Get Template** link.

h. Click **Discover**.

3. You can view the discovered certificates in **Certificates >> Certificates** Tab.

3. Renew Certificate

1. Select a certificate and click Renew at the top.
2. If the certificate does not have a private key, PAM360 allows you to create a new private key. Click OK in the pop-up that appears.
3. Attributes such as Renewal Type, Server Name, Template Name / OID, Certificate Authority will be auto populated from the certificate details. The Server Name is the name of the Microsoft CA server which signed the certificate. Certificate Authority is the CA service that runs in the specified Microsoft CA server.



4. For certificates signed by Microsoft CA directly or using the SSL agent (KMP agent), validity days will be taken from the Microsoft CA server and therefore it cannot be entered manually during renewal. These types of certificates will be renewed only till the date specified in the Microsoft CA server.

Notes:

i. During the renewal process, a CSR will be generated from the available values, along with a new Private Key.
ii. SHA1 certificates will be renewed using the SHA256 algorithm.

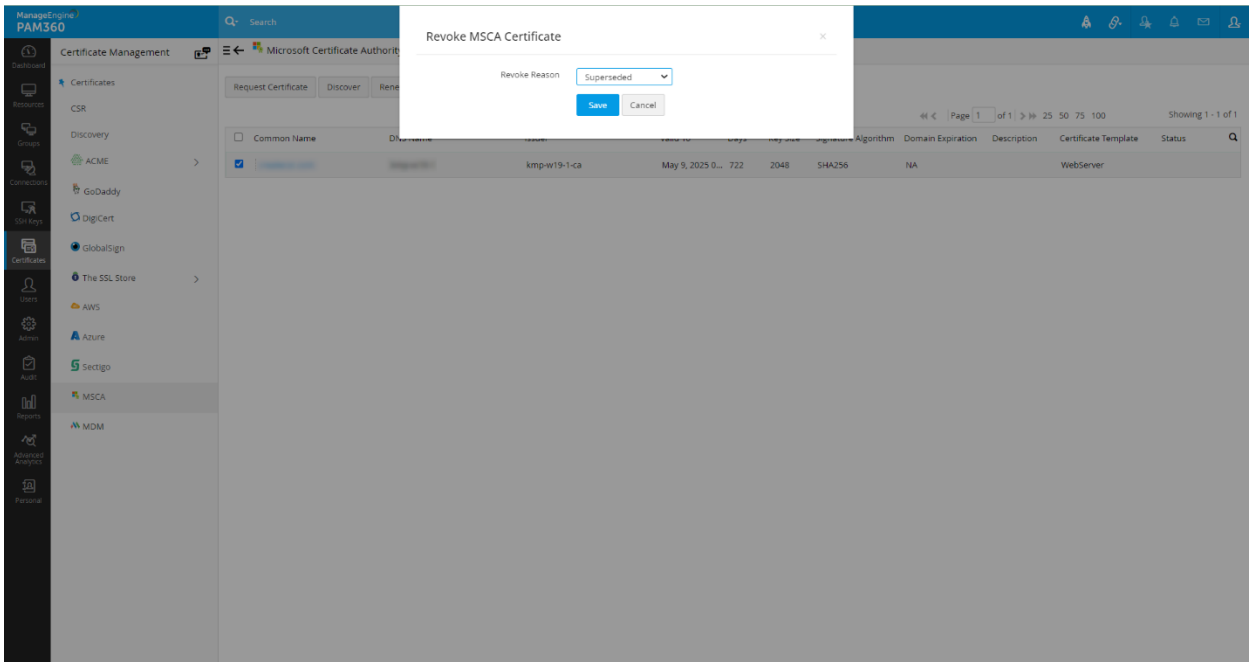
PAM360 also allows you to set up auto-renewal for certificates. To know how to auto renew certificates in PAM360, click here.

4. Export Certificate

1. PAM360 allows you to export the following certificate types: .cer, .crt, .pem, .der, .p7b, .pfx, .p12, .pkcs12, .jks, .keystore.
2. In the MSCA certificates window, click the certificate you want to export.
3. In the **Certificate Details** window, click **Export** on the top right corner and select the required format in the which you want to export the certificate.
4. The certificate will be downloaded to your machine in the selected format.

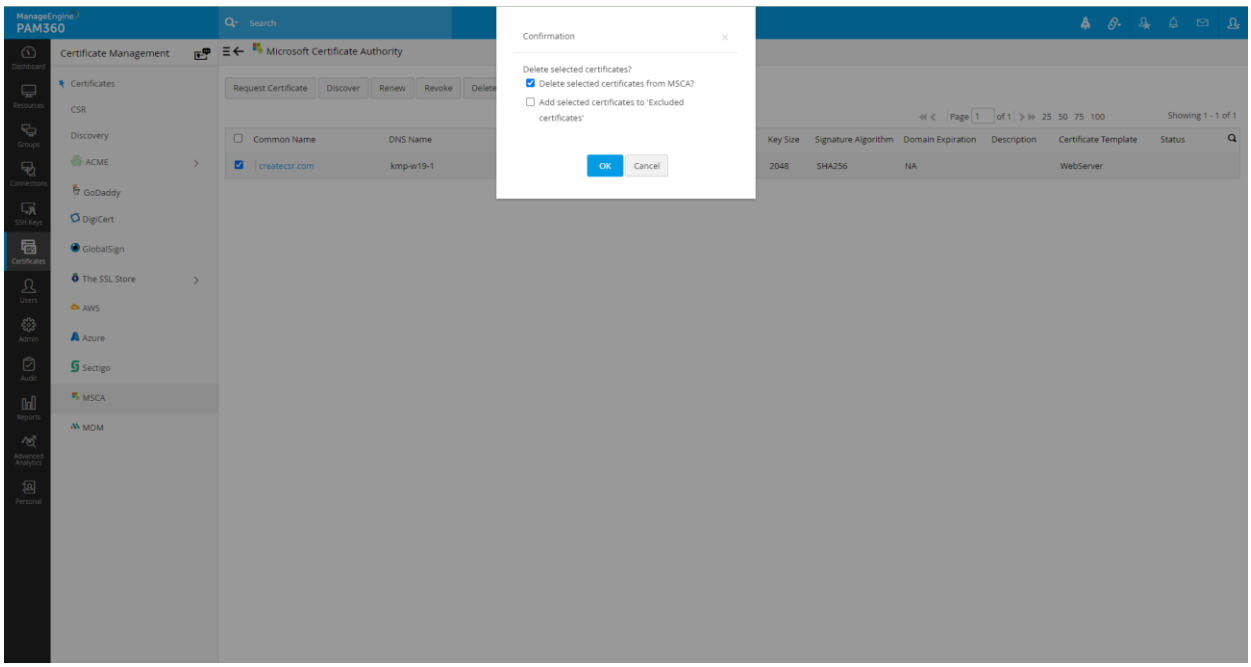
5. Revoke Certificates

1. Select the required certificates and click **Revoke** at the top.
2. In the pop up that appears, mention the **Revoke Reason** from the dropdown and click **Save**.



6. Delete Certificate

1. Select the required certificates and click **Delete** at the top.
2. In the pop up that appears, select if you want to **Delete selected certificates from MSCA?** and/or **Add selected certificates to 'Excluded certificates'** and click **OK**.



Integration with ManageEngine Mobile Device Manager Plus (MDM)

PAM360 integrates with ManageEngine Mobile Device Manager Plus (MDM); this integration is achieved through the ManageEngine MDM APIs. Once the integration is done, you can discover and import SSL certificates from the devices managed through your MDM server and store the SSL certificates in the PAM360 repository. You can also deploy SSL certificates from PAM360 to the mobile devices listed in your MDM environment. All the imported SSL certificates are stored in the PAM360 repository, from where you can filter the view based on the OS type such as iOS, Android, Windows, Chrome OS, Mac OS, and Apple tvOS. In addition to that, PAM360 allows you to export instant and periodically scheduled reports of the MDM certificates that are managed in the certificate repository within a selected time period.

> **Note:** The PAM360 - ManageEngine MDM integration works with **MDM release version 10.1.2011.02 and above** only.

1. **Prerequisite**
2. **Discover SSL Certificates from ManageEngine MDM**
3. **Import and Deploy SSL Certificates**
4. **Create MDM Certificates Report**

1. Prerequisite

The PAM360 - ManageEngine MDM integration requires a valid API key with the necessary permissions. To generate the API server key, follow the below steps in the **ManageEngine MDM portal**:

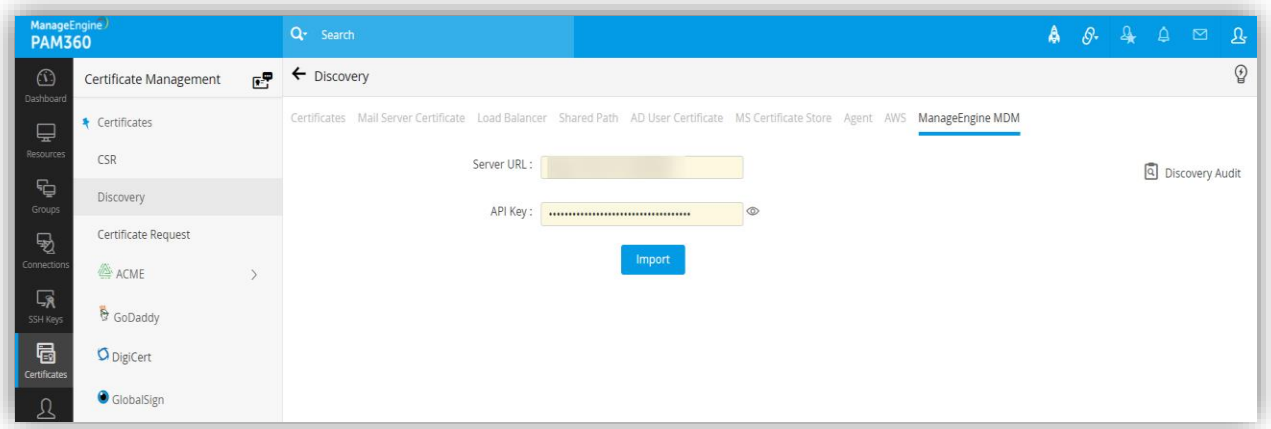
1. Navigate to **Admin** and click **Generate Key** under **API Key Generation**.
2. In the pop-up, choose **Third-party App** as the **Application**, enter a **Service Name**, and under **Permissions**, select the following: **CertMgmt (read and write), Devices (read and write), Profiles (read and write).**

3. Click **Generate Key**. Once the new API key is generated, use the copy icon to copy it. This key is necessary to perform certificate discovery in the following discovery steps.

2. Discover SSL Certificates from ManageEngine MDM

Once you have the API server key from the MDM portal, follow the below steps in the PAM360 interface to discover SSL certificates from the devices managed in MDM:

1. Navigate to **Certificates >> Discovery >> ManageEngine MDM**.
2. Specify the URL of the ManageEngine MDM server and enter the newly generated API Key.
3. Click **Import From MDM**. PAM360 will establish a secure connection with the MDM server and start importing SSL certificates into the repository.
4. Click **Discovery Audit** to view the status of the import.



Alternatively, you can also discover and import certificates through the **Manage** option under **Certificates >> MDM**. This is explained in detail under the subsequent steps.

3. Import and Deploy SSL Certificates

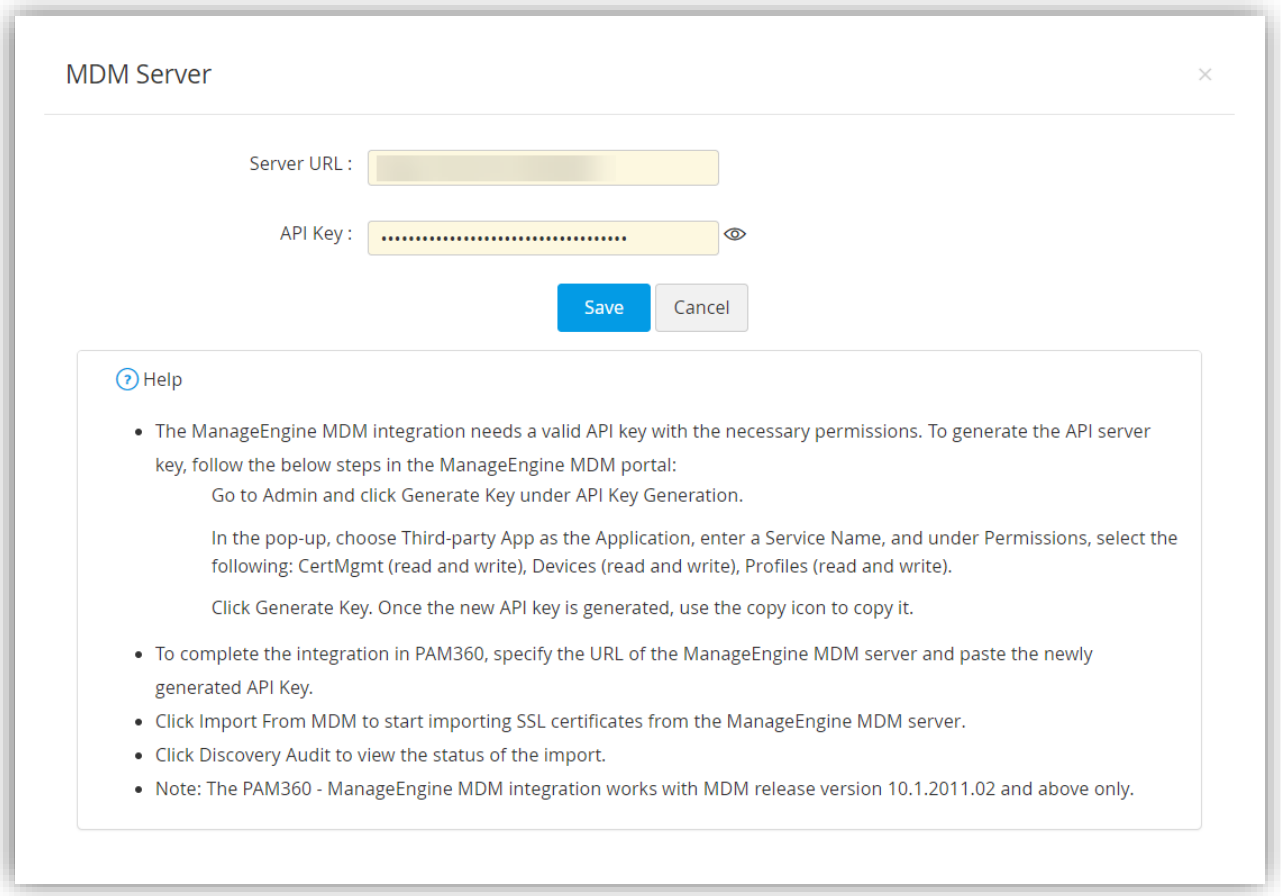
All the SSL certificates discovered from the MDM server are stored in the certificate repository and you can access them from the **SSL >> ManageEngine MDM**. The ManageEngine MDM tab displays certificate attributes such as the Common Name, Device Name, Issuer, Date of Expiry, Signature Algorithm, and Serial Number. Using the Show drop-down, you can filter the view of the SSL certificates based on the following OS types: iOS, Android, Windows, Chrome OS, Mac OS, and Apple tvOS.

From the ManageEngine MDM tab, you can import, deploy, and manage the SSL certificates discovered from the MDM portal.

3.1 Import SSL Certificates

Follow the below steps to import certificates from the MDM server:

1. If you have not previously discovered certificates through the Discovery tab, navigate to **Certificates >> MDM** and click **Manage**.
2. In the pop-up that appears, enter the server URL, API server key, and click **Save**.
3. Click **Import** to fetch certificates from the devices in your MDM server.



However, if you have already discovered certificates via the **Discovery** tab, you can skip this step as your certificates will already be available in PAM360.

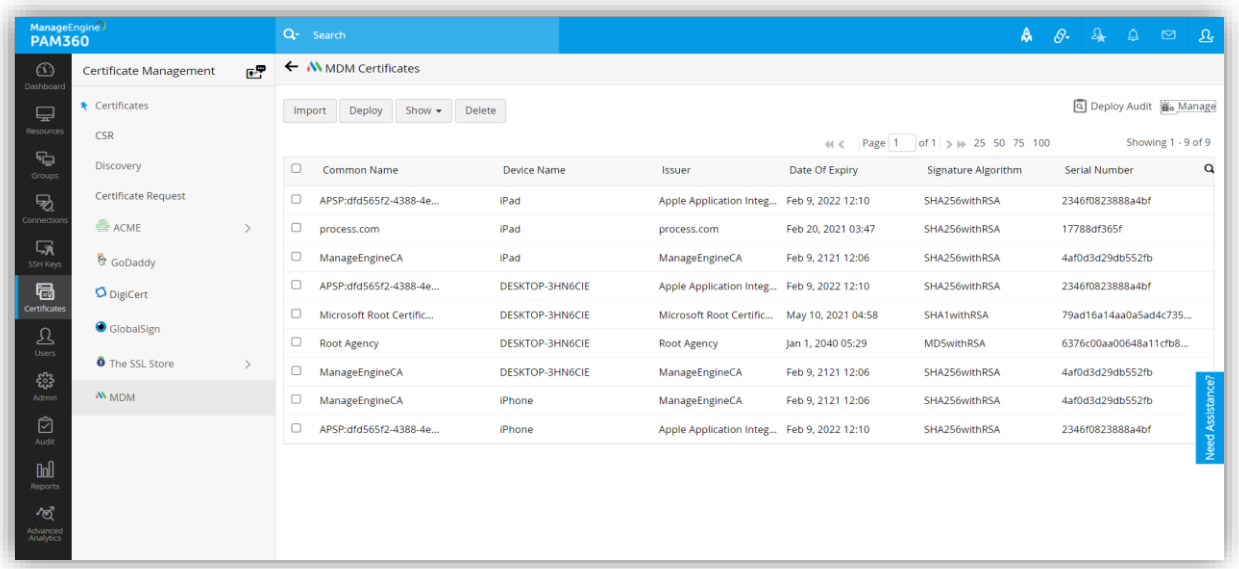
3.2 Deploy SSL Certificates

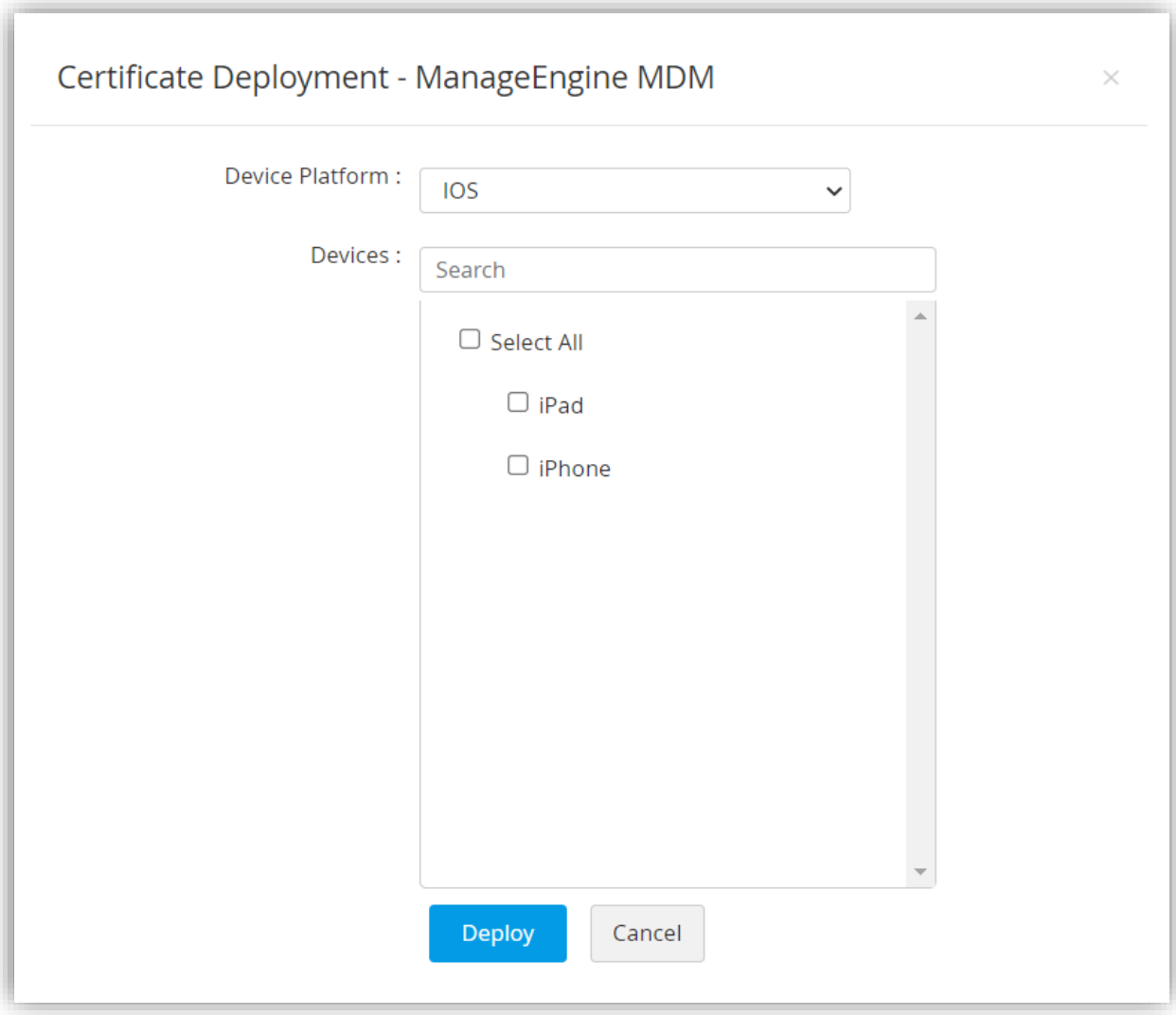
PAM360 allows you to deploy SSL certificates to the various devices in your MDM server. Follow the below steps:

1. Navigate to **Certificates >> MDM**.
2. Select one or more certificates from the certificates list and click **Deploy**.

3. In the pop-up that appears, choose a **Device Platform**, select the required devices from the list of devices associated with your MDM server. Use the checkboxes and select **Certificate** and/or **JKS/PKCS** based on your requirement. Click **Deploy**.
4. To get the deployment status, go to **Deploy Audit** and click the **Get Status** option.

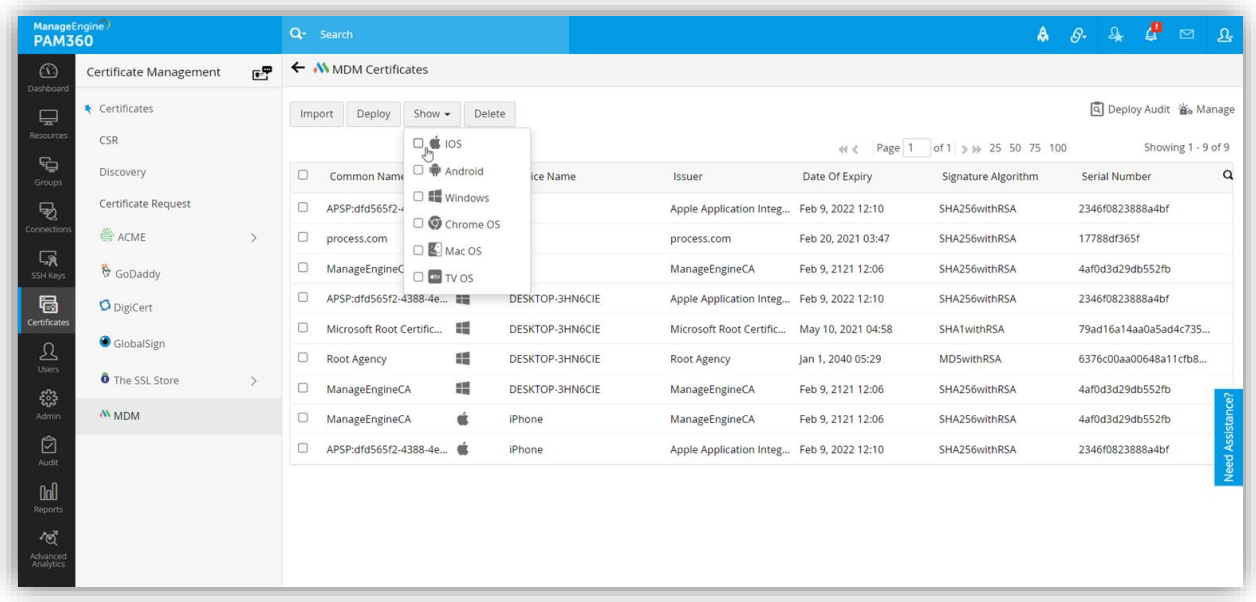
Note that the deployment status will not be updated instantly, as ManageEngine MDM puts deployment requests on a queue until the selected device is online. Click the **Get Status** option whenever you need to get the updated deployment status.





3.3 Show and Delete Certificates

1. You can filter the certificates view using the **Show** option. Click the **Show** drop-down and choose the required OS types from the list. The certificates in the table view will be filtered as per your selection.
2. To delete certificates from the table view, select the required certificates using the checkboxes and click **Delete** from the menu. Click **Confirm** in the confirmation dialog box.



4. Create MDM Certificates Report

PAM360 offers a provision to export reports of the MDM certificates managed in the PAM360 repository within a selected period. This report provides detailed information on the MDM certificates managed via PAM360. Additionally, you can schedule periodic generation of MDM certificate reports.

Follow the below steps to create the MDM Certificates Report:

1. Navigate to the **Reports** tab and click **MDM Certificates Report** under **SSL Reports**.
2. This report includes details such as: **Common Name, Device Name, Issuer, Date of Expiry, Signature Algorithm, and Serial Number.**
3. Click the **Show** dropdown to filter the report view based on the OS type.
4. Click the **Date Filter** and choose a time period to view certificates imported within the specified dates.
5. Click the **Export** dropdown to export this report in PDF & CSV formats, or send via email to the specified recipients.

Click here to learn more about Reports in PAM360.

Follow the below steps to schedule periodic generation of the MDM certificates report:

1. Go to the **Admin >> SSH/SSL Config >> Schedules** tab.
2. Add a **Schedule Name** and choose the **Schedule Type** as **Report.**

3. Under **Report Type**, choose **MDM Certificates Report**.
4. Enter a preferred recurrence type, date and time.
5. Choose a report format and click **Save**.

Once the schedule is created, PAM360 will periodically generate the MDM Certificates Report on the specified date and time.

Click here to learn more about Schedules in PAM360.

Share SSL Certificates with Users

PAM360 allows you to share your certificates or certificate groups with users and user groups. When you share a certificate, all the details of that certificate will be naturally shared. In general, every user will have access to the certificates they own and also to those that are shared with them.

A user with whom a certificate is shared can also export and access its private key, but only after raising a request for the same with the certificate's owner and getting approval. However, the approval grants the permission only for export; any other operation involving the private key will not be available for the user.

What you can share with other users and user groups?

You can share

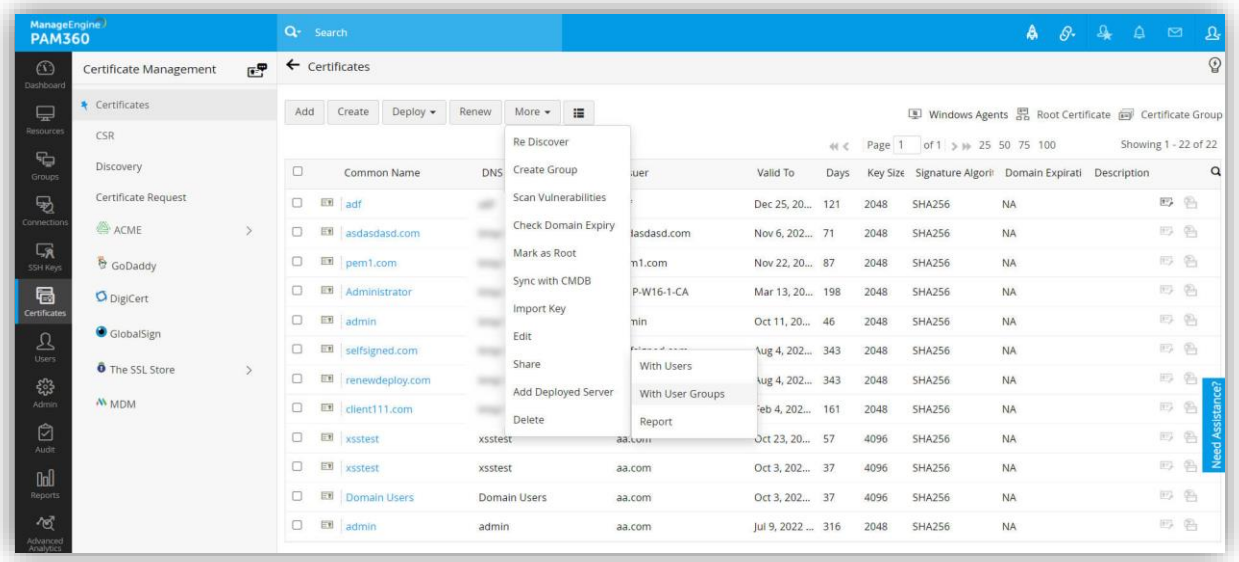
- An owned certificate to a user or user group.
- An owned certificate group to a user or user group.

In this section you will learn to:

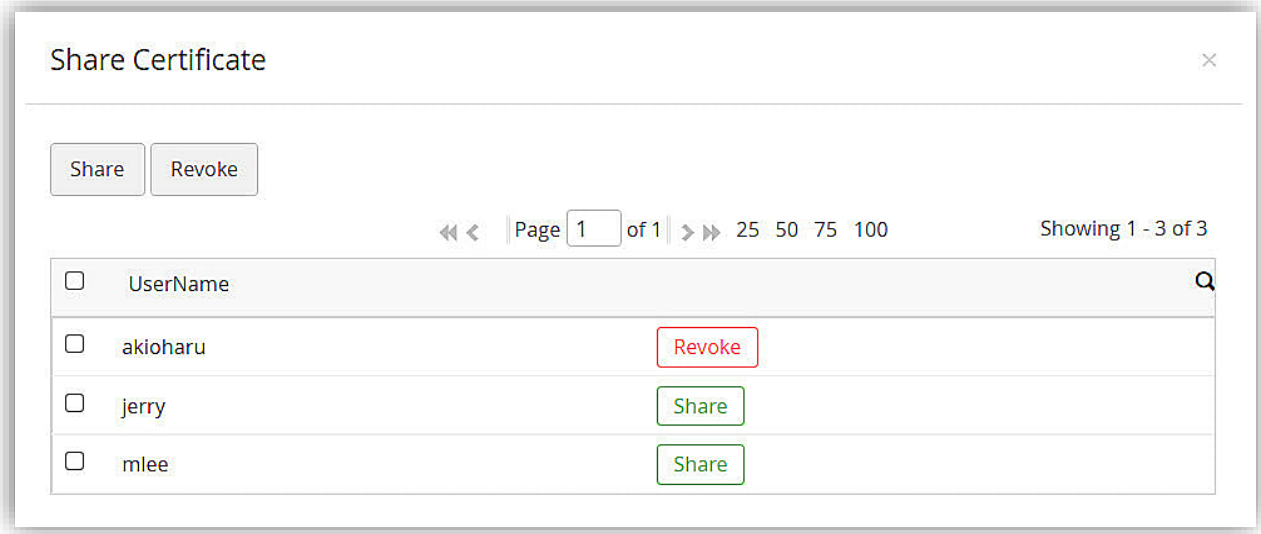
1. Sharing a Certificate with Users / User Groups
2. Sharing a Certificate Group with Users / User Groups
3. Sharing Certificates
4. Requesting a Certificate's Private Key from the Owner of the Certificate

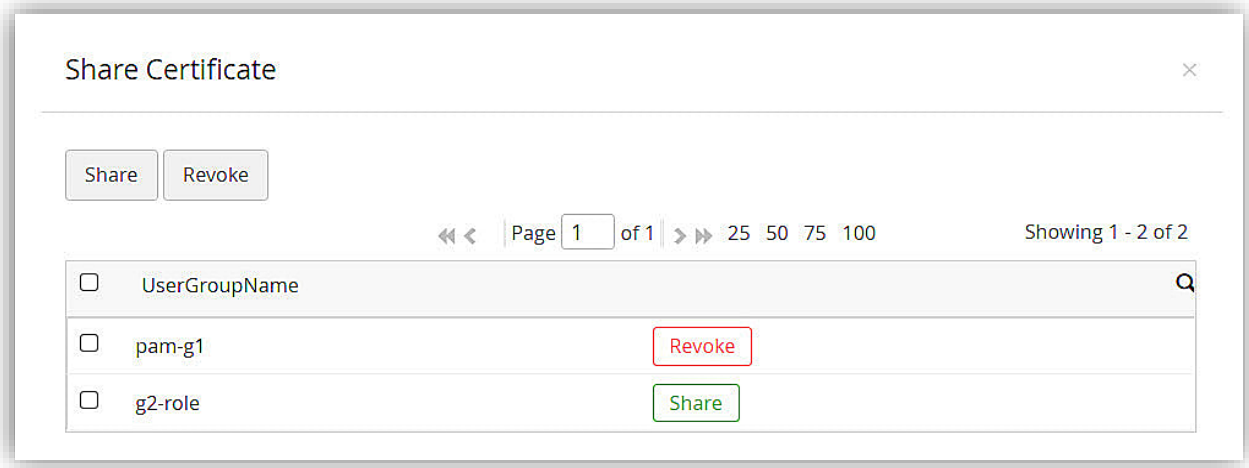
1. Sharing a Certificate with Users / User Groups

1. Navigate to the **Certificates** tab.
2. Select the particular certificate to be shared.



3. Click on the **More** action button at the top and select the required option from the dropdown menu—either **Share With Users** or **Share With User Groups**, depending on your need.



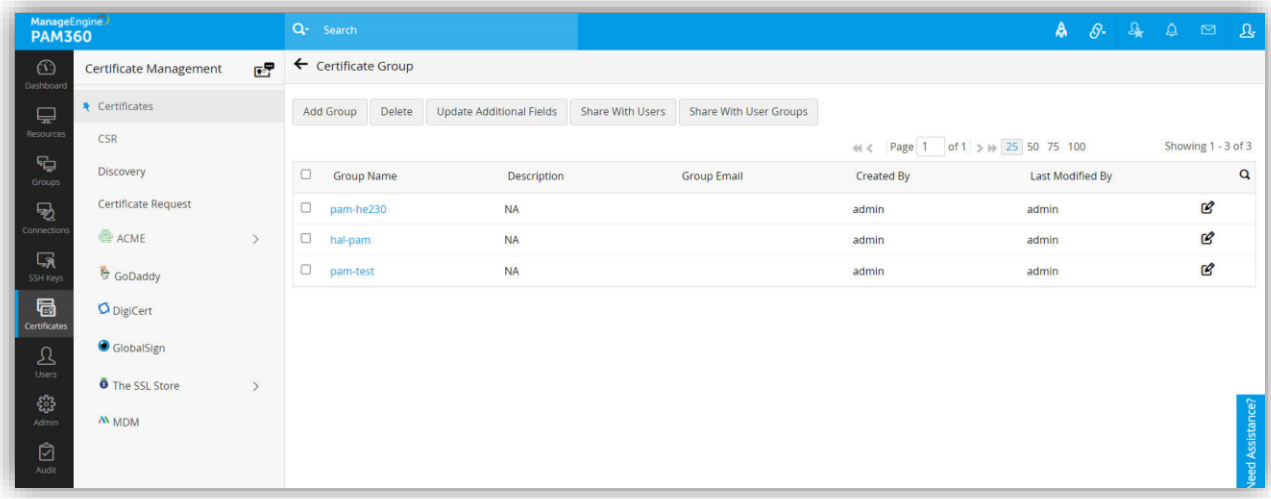


4. In the new window that opens, choose the user(s) or user group(s) whom you want to share the certificate with and click **Share**. Once shared, the access to the certificates can be revoked any time from the same window.

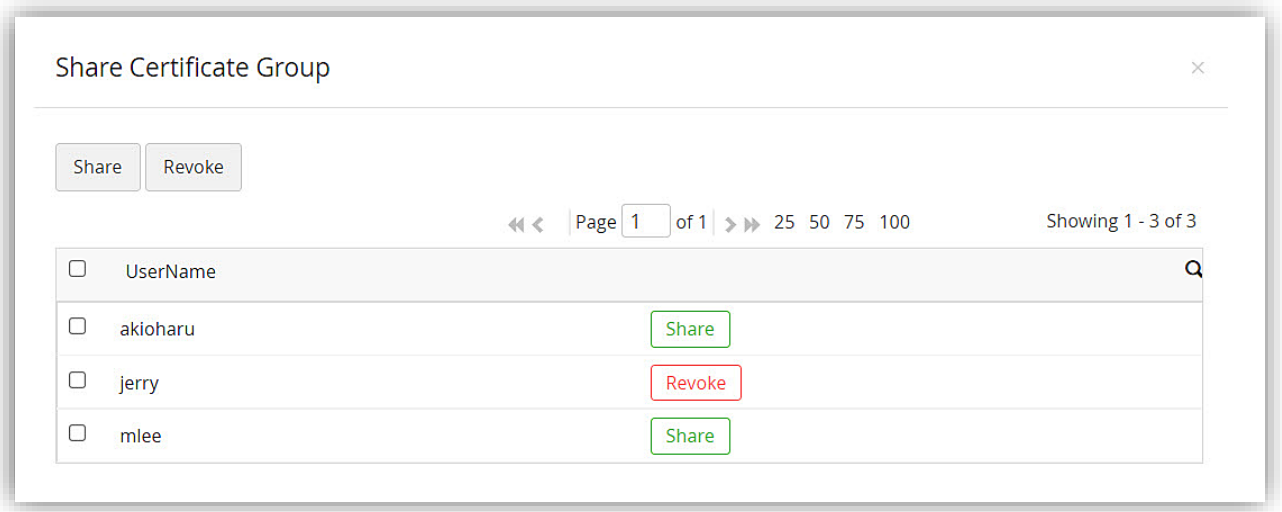
> **Note:** When you share a particular certificate with a user group, it will be visible to all members of that user group, provided that their role includes the privilege to access SSL certificates.

2. Sharing a Certificate Group with Users / User Groups

1. Navigate to the **Certificates** tab.
2. Click on **Certificate Group** on the top-right corner.
3. Select the required certificate group that you want to share.



4. Depending on whether you need to share the certificate group with user(s) or user group(s), select the required option—either **Share With Users** or **Share With User Groups.**
5. In the new window that opens, choose the user(s) or user group(s) whom you want to share the certificate with and click **Share**. Once shared, the access to the certificates can be revoked any time from the same window.



Note: Since only owned certificates can be shared, certificate groups can be created only with owned certificates. When you share a particular certificate group with a user group, the details of all respective certificates belonging to the certificate group would be visible to all the members of the user group, provided that their role includes the privilege to access SSL certificates.

3. Sharing Certificates

PAM360 allows users to modify the access level to the shared certificates globally. This allows the user to give **view/ modify** permission to the users under the selected roles with whom the certificates are shared. To do this,

1. Navigate to **Admin >> SSH/SSL Config >> Certificate Sharing.**
2. In the **Certificate Sharing** window, move the user roles accordingly to grant **View** or **Manage** permission to certificates for those user roles.
3. Select the checkbox to **Share the renewed certificate with users who have access.**

4. Click **Save.**

Now, the users to whom the certificates are shared will have the appropriate permission.

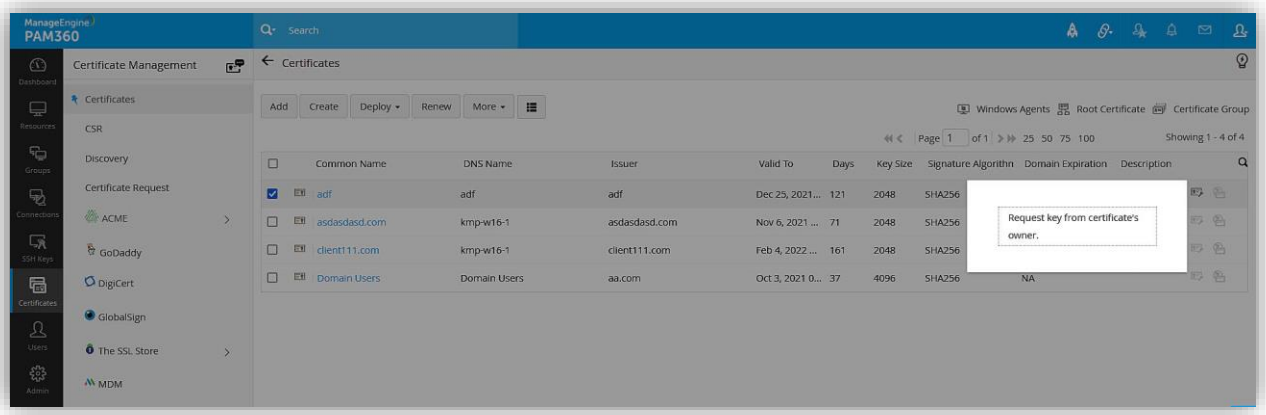
4. Requesting a Certificate's Private Key from the Owner of the Certificate

When a certificate is shared with you, you can carry out the operations that doesn't involve the private key of the certificate. These include:

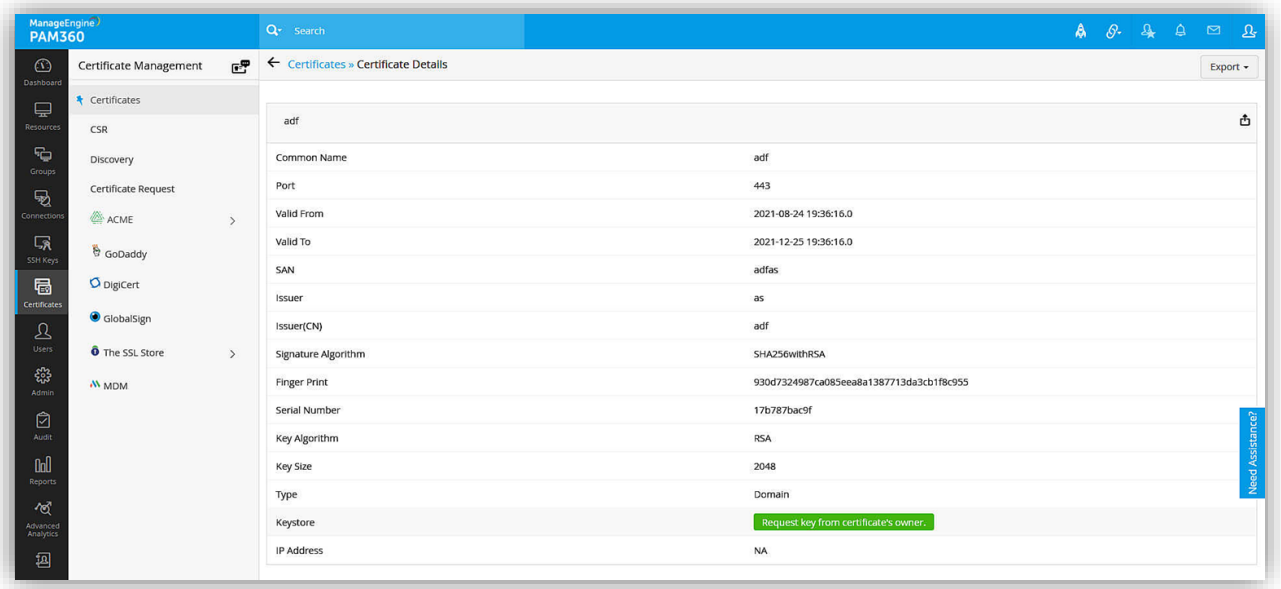
- View certificate details like expiry, key size, algorithm, length, and DNS name
- Scan vulnerabilities
- Check domain expiry
- Edit
- Sync with CMDB, and
- Export the certificate

In addition to these, you can request the certificate's private key from the owner of the certificate. To do so,

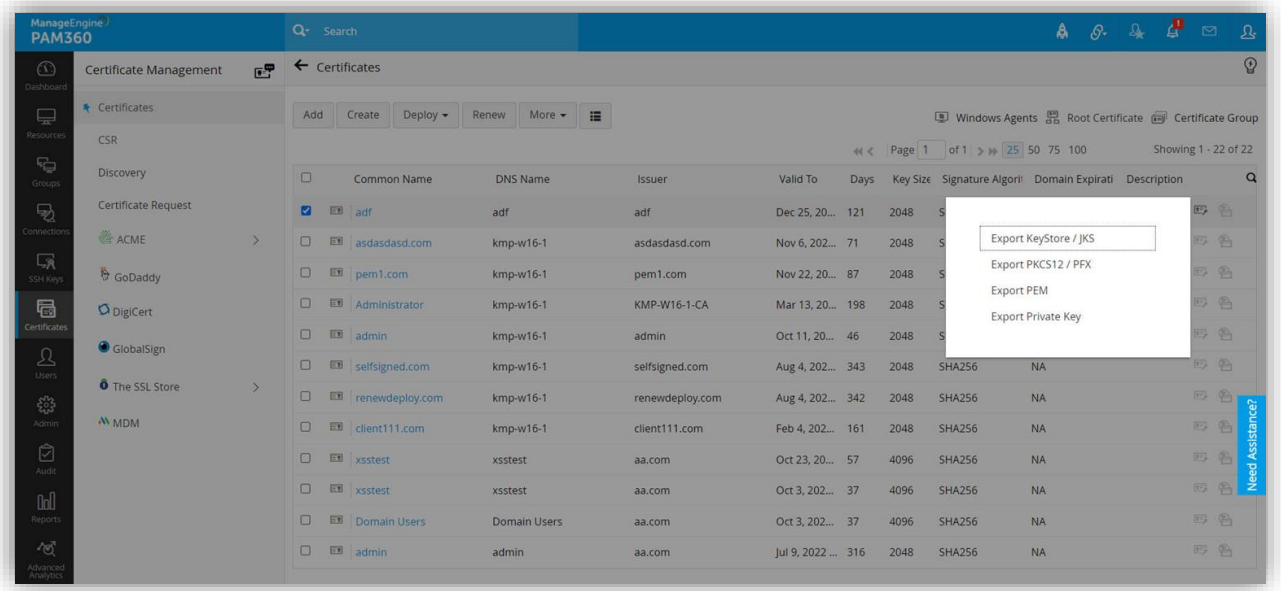
1. Navigate to **Certificates**, select the shared certificate from the list, and click on **Request key from certificate's owner** from the **Keystore** icon beside the certificate.



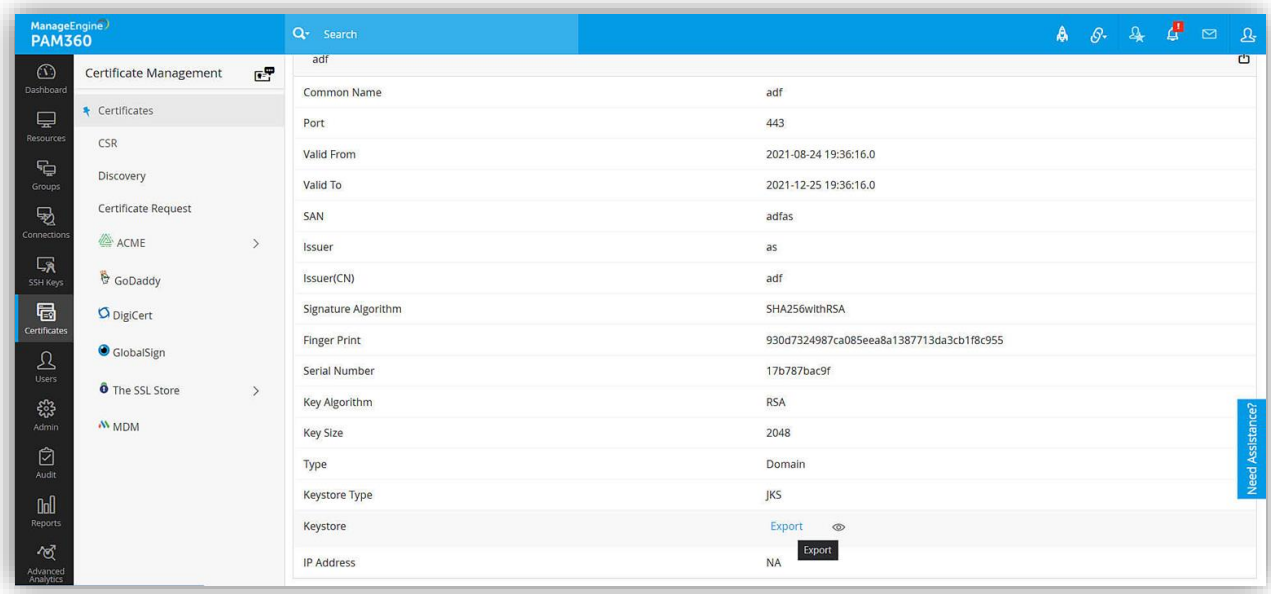
2. You can also request the private key by clicking on the shared certificate, and then clicking on **Request key from certificate's owner** from the 'Certificate Details' window.



3. The owner of the certificate will be notified of the request through PAM360 and email. Upon approval, you can export the private key from the **Certificates** tab **only once.**
4. To export the private key, navigate to **Certificates**, select the shared certificate, and then click on **Export Private Key** from the 'Keystore' icon beside the certificate.



5. Alternatively, you can export the private key by clicking on the shared certificate, and then clicking on the **Export** button beside **Keystore** from the '**Certificate Details**' window.



Note: As mentioned above, you can export the private key of a shared certificate **only once** after approval from its owner. You need to request the private key from the certificate's owner if you want to export it again.

Deploy SSL Certificates to Target Web Servers

In general, SSL certificates procured from Certificate Authorities (CAs) are stored in a repository and then manually deployed on appropriate target systems. PAM360 deploys the certificates from the repository on the correct target systems automatically. You can use PAM360 to deploy the certificates on the various systems individually, or in bulk, based on your requirements. Also, you can use the Key Manager Plus agent to deploy certificates on servers that reside in demilitarized zones outside of the domain where the PAM360 server is present.

1. Steps to Deploy Certificates on Different Target Systems

1.1 Deploying certificates to a Windows server

1.2 Deploying certificates to MS Certificate store

1.3 Deploying certificates to Internet Information Services (IIS)

1.4 IIS Binding

1.5 Deploying certificates to a Linux server

1.6 Deploying Certificates to a Browser

1.7 Deploying Certificates to ManageEngine MDM

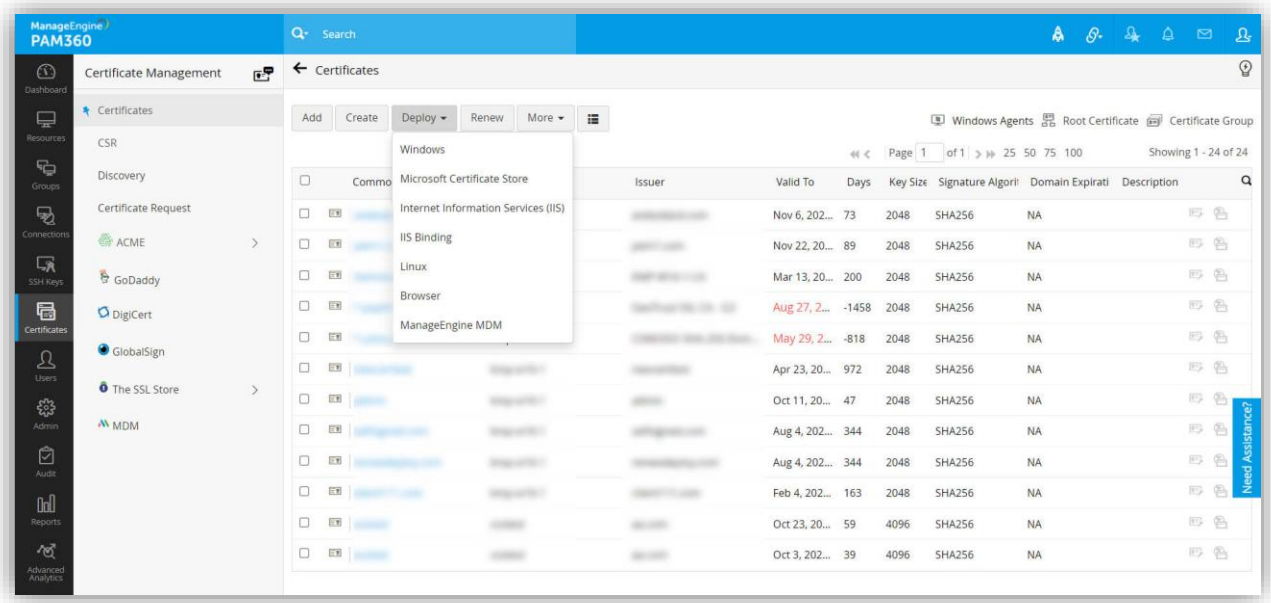
1.8 Deploying Certificates to AWS-ACM

1.9 Deploying Certificates to Load Balancer

1. Steps to Deploy Certificates on Different Target Systems

Using PAM360, you can directly deploy selected SSL certificates onto target servers. To deploy an SSL certificate to a target server:

1. Navigate to **Certificates >> Certificates**.
2. Select the certificates that you want to deploy to target servers by clicking on the check boxes beside them.
3. Click **Deploy**.
4. In the **Certificate Deployment** window that opens, select the server type (**Windows, MS Certificate Store, IIS, Linux**) and provide the required details. The certificates are deployed to the specified servers in the specified path.

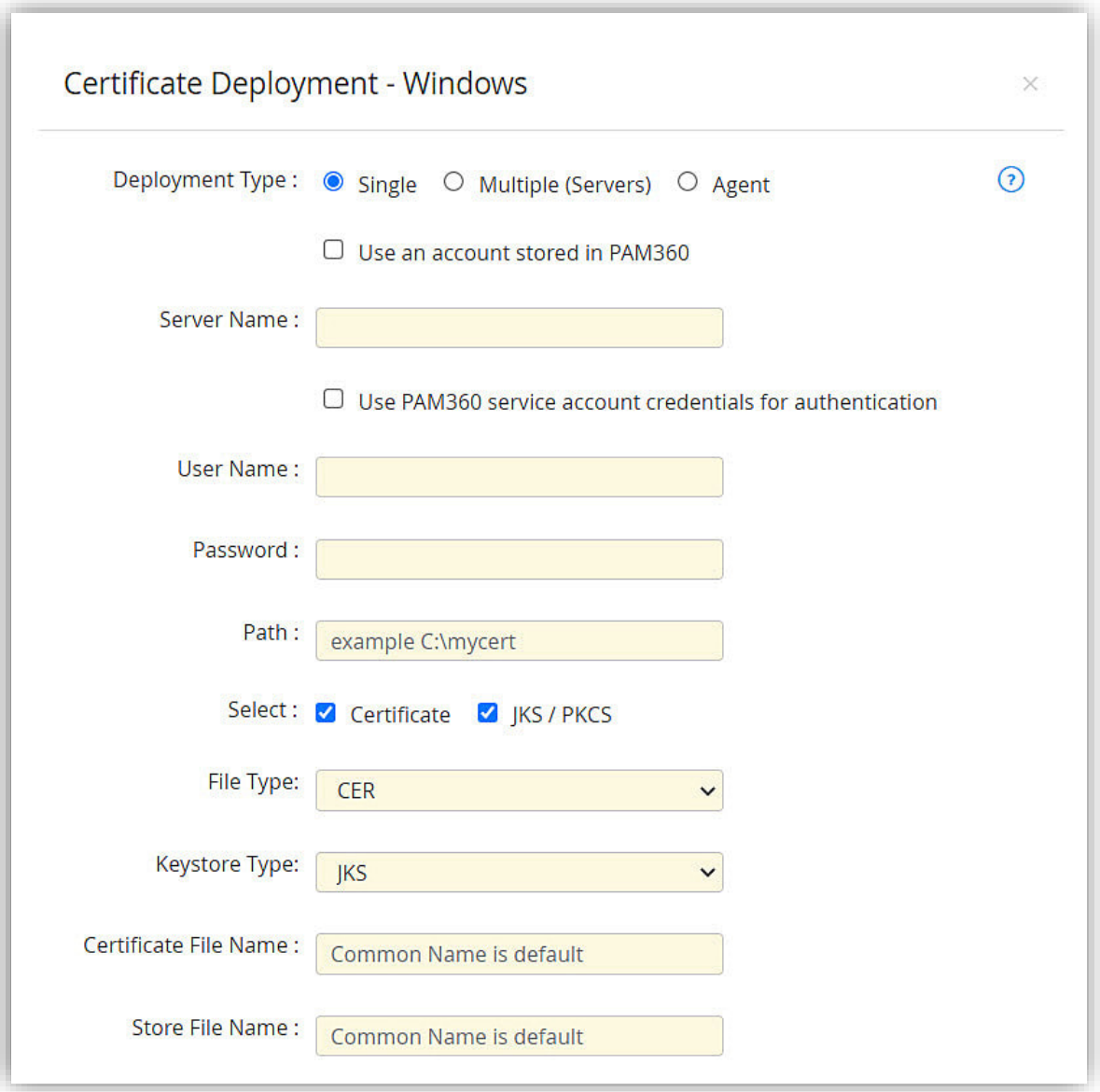


1.1 Deploying Certificates to a Windows Server

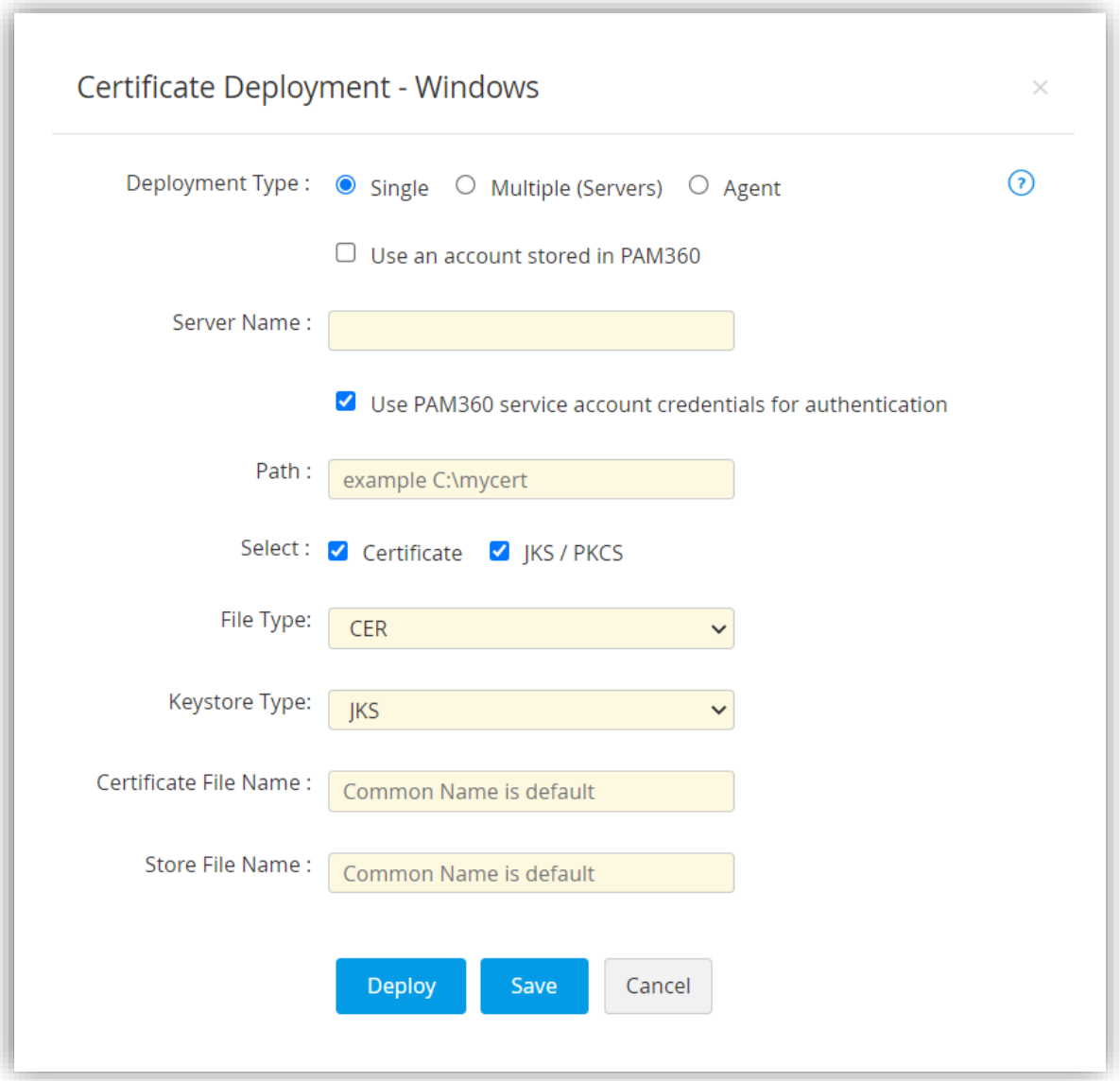
Notes:

1. For deploying certificates on Windows systems, MS Certificate Store and Internet Information Services (IIS), use your domain administrator account as the service login account of PAM360.
2. If you are using a domain service account to run PAM360, ensure you already have it configured in your local admin group.

1. To deploy certificates on Windows server, choose the server type as **Windows**.
2. Select the **Deployment Type** as **Single, Multiple** (servers) or **Agent** as per your need.
    i. For single server deployment, provide the required details: **Server Name, User Name, Password, Path, File Type** and **Certificate File Name.** ou can optionally enable **Certificate** to choose the **File Type** and mention the **Certificate File Name** or/and enable **JKS/PKCS** to choose the **Keystore Type** and mention the **Store File Name.**



ii. If you select the checkbox **Use PAM360 service account credentials for authentication**, you need not provide the username and password separately, as the service account credentials used for PAM360 will be used here too.



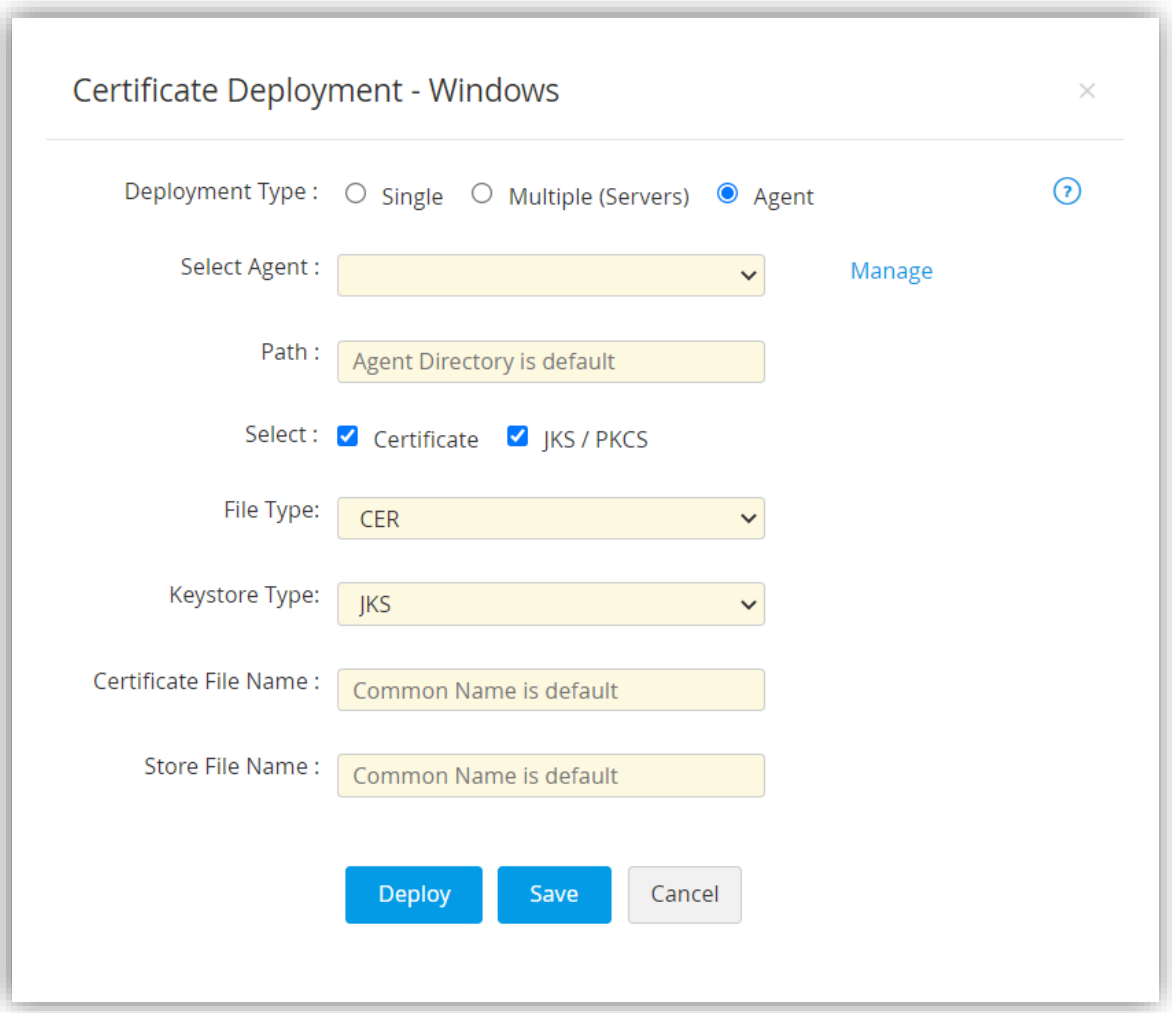
iii. If you select the checkbox **Use an account stored in PAM360**, you need not provide the password as PAM360 will take the user account details directly from the database.

iv. For certificate deployment on **Multiple** servers, upload a **.csv** file comprising the following details: **Server Name, User Name, Password, Path, Certificate file name** (optional), **Keystore File Name** (optional) and **File Type.** You can optionally enable **Certificate** to choose the **File Type** or/and enable **JKS/PKCS** to choose the **Keystore Type.**

v. If you choose the **Deployment Type** as **Agent**, choose the host name of the PAM360 agent from the **Select Agent** drop-down, enter the destination file path in the agent machine. If a destination path is not mentioned, the agent installation path will be taken as default. You can optionally enable **Certificate** to choose the

File Type and mention the **Certificate File Name** or/and enable **JKS/PKCS** to choose the **Keystore Type** and mention the **Store File Name.**

vi. Click **Save** to save the details.



3. Now, click **Deploy**.

The certificate is deployed to the specified server/agent in the specified path.

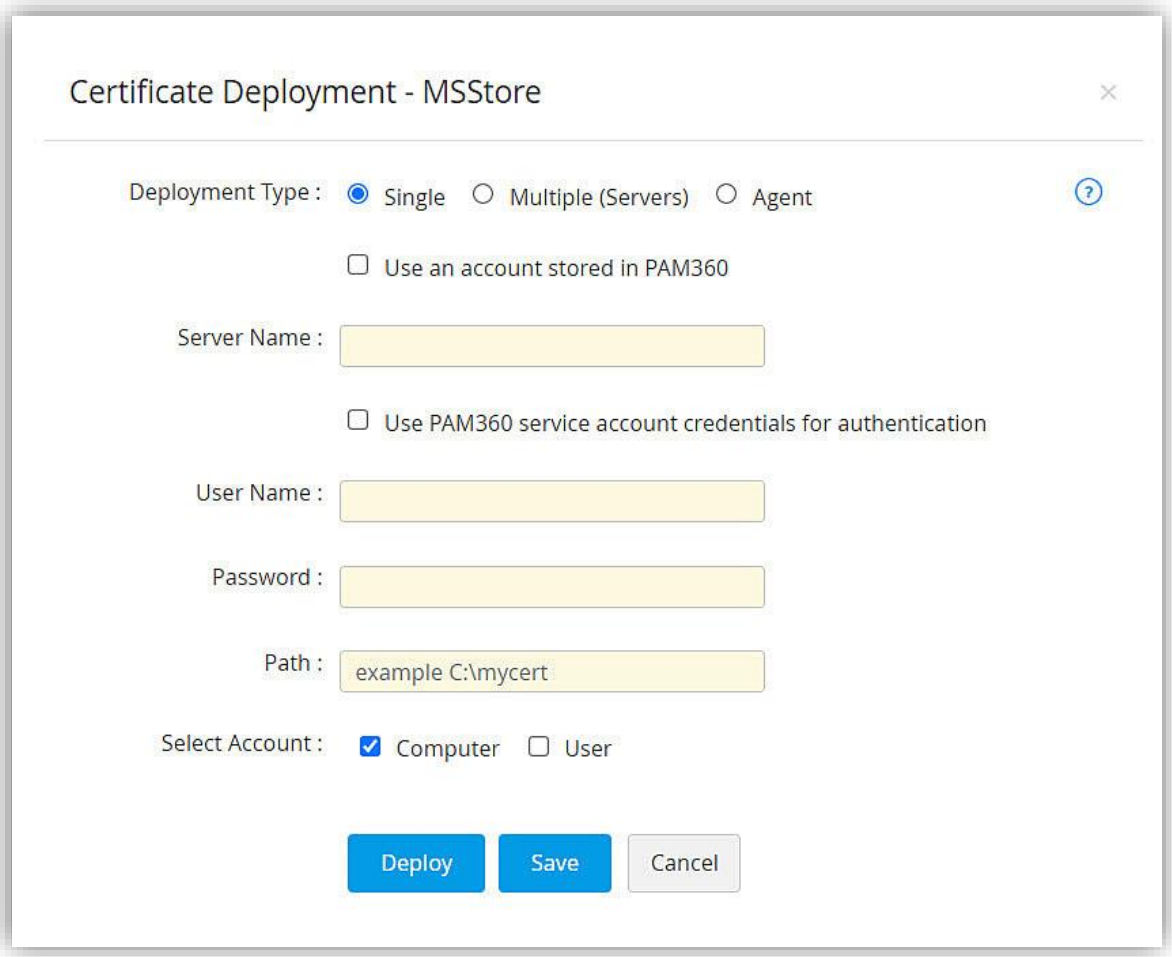
Note: For file-based deployment, if the Certificate and Keystore file names are not provided, or if multiple certificates are selected for deployment, the Common Name will be used as the file name.

1.2 Deploying Certificates to MS Certificate Store

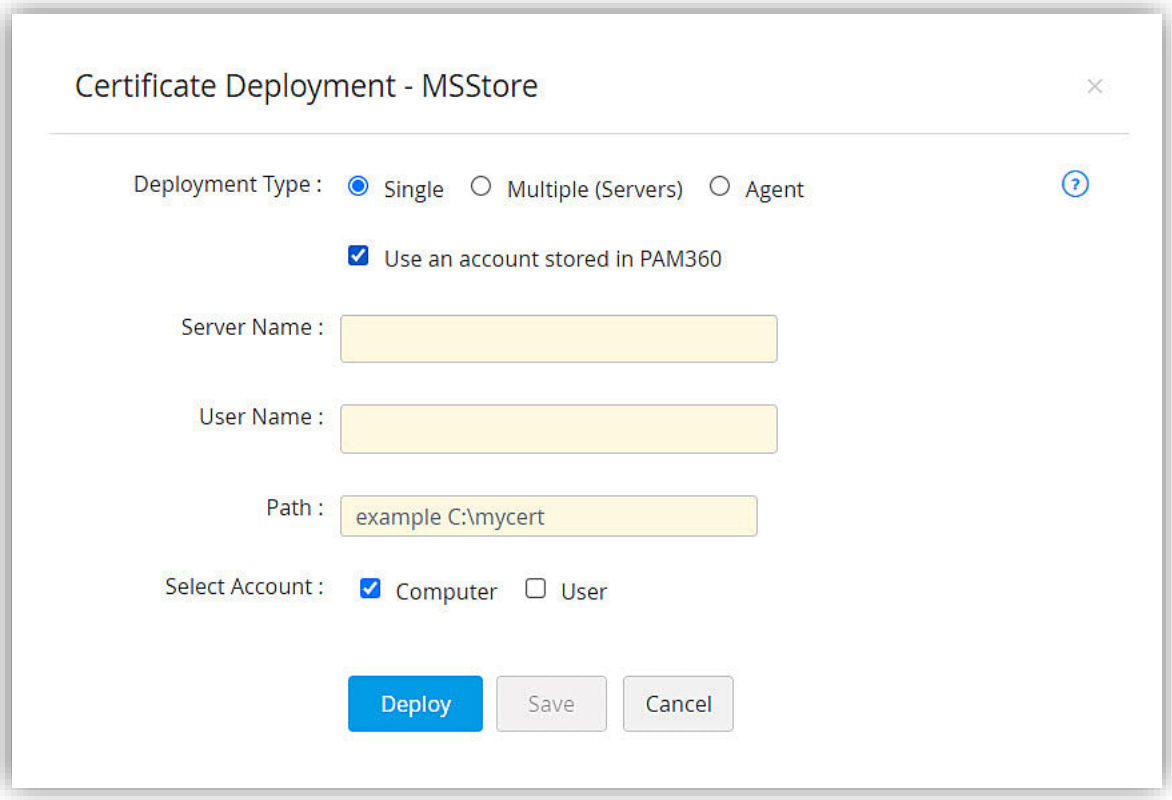
1. To deploy certificates to **MS Certificate store**, choose the server type as **Microsoft Certificate Store**.

2. Select the **Deployment Type** as **Single, Multiple** or **Agent** as per your need.

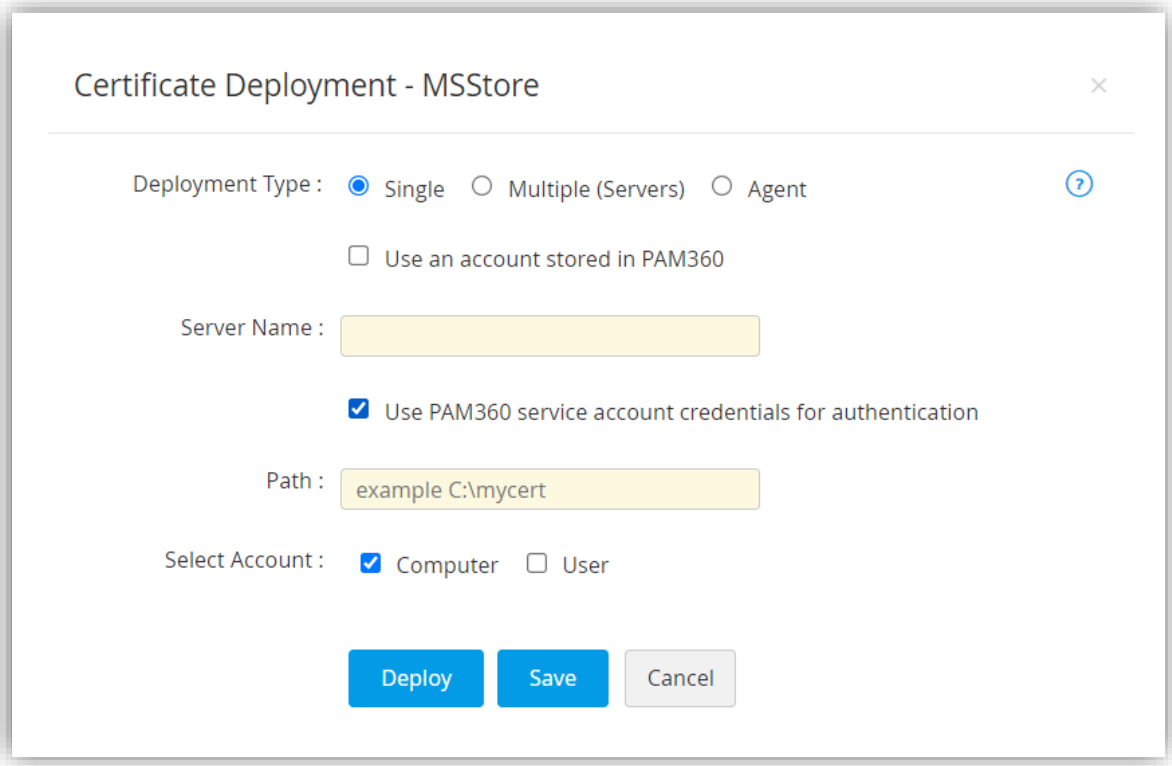
   i. For **Single** deployment, provide the required details: **Server Name, User Name, Password, Path.**



   ii. If you select the checkbox **Use an account stored in PAM360,** you need not provide the password as PAM360 will take the user account details directly from the database.



iii. If you select the checkbox **Use PAM360 service account credentials for authentication**, you need not provide the username and password as PAM360 will take the user account details directly from the database.

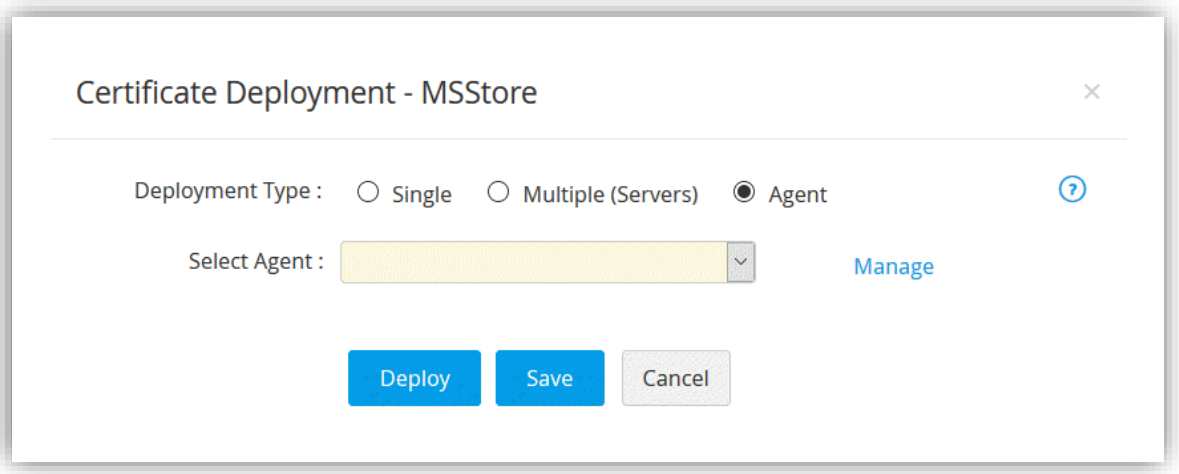


iv. For certificate deployment on **Multiple** servers, upload a .csv file comprising the following details: **Server Name, User Name, Password, Path**.

v. Select **Computer** and/or **User account** to deploy the certificate to the selected account.

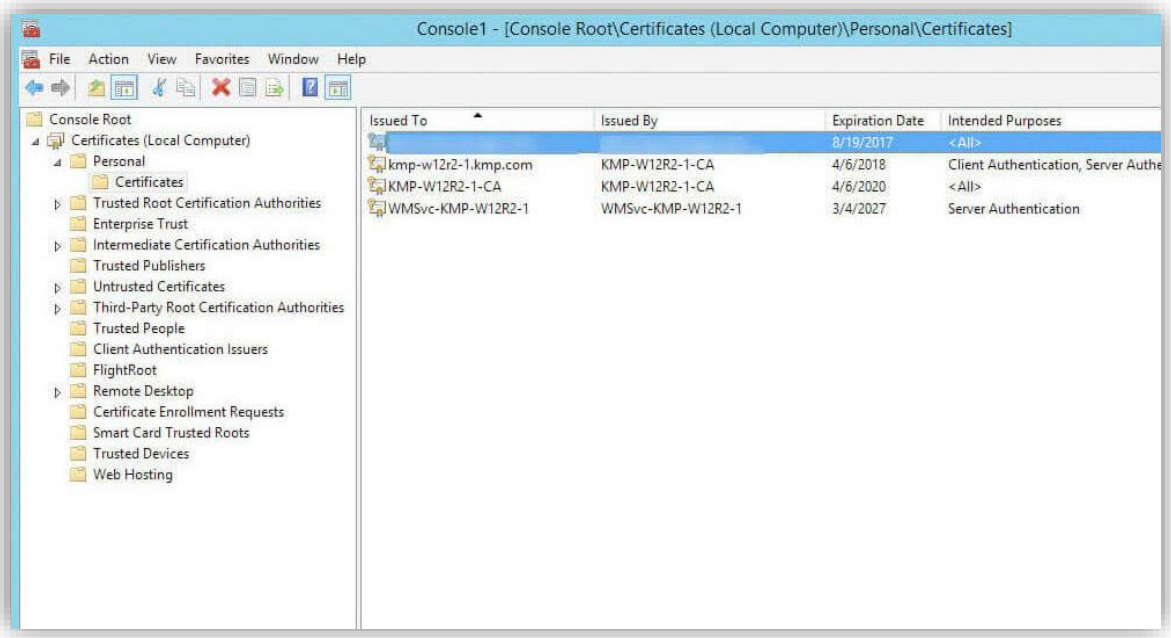
> **Note:** For Agent deployment, the latest version of PAM360 agent (5900) should run in the user account to which the certificates are to be deployed.

vi. If you choose the Deployment Type as **Agent**, choose the host name of the PAM360 agent from the **Select Agent** drop-down and click **Save** to save the agent details.

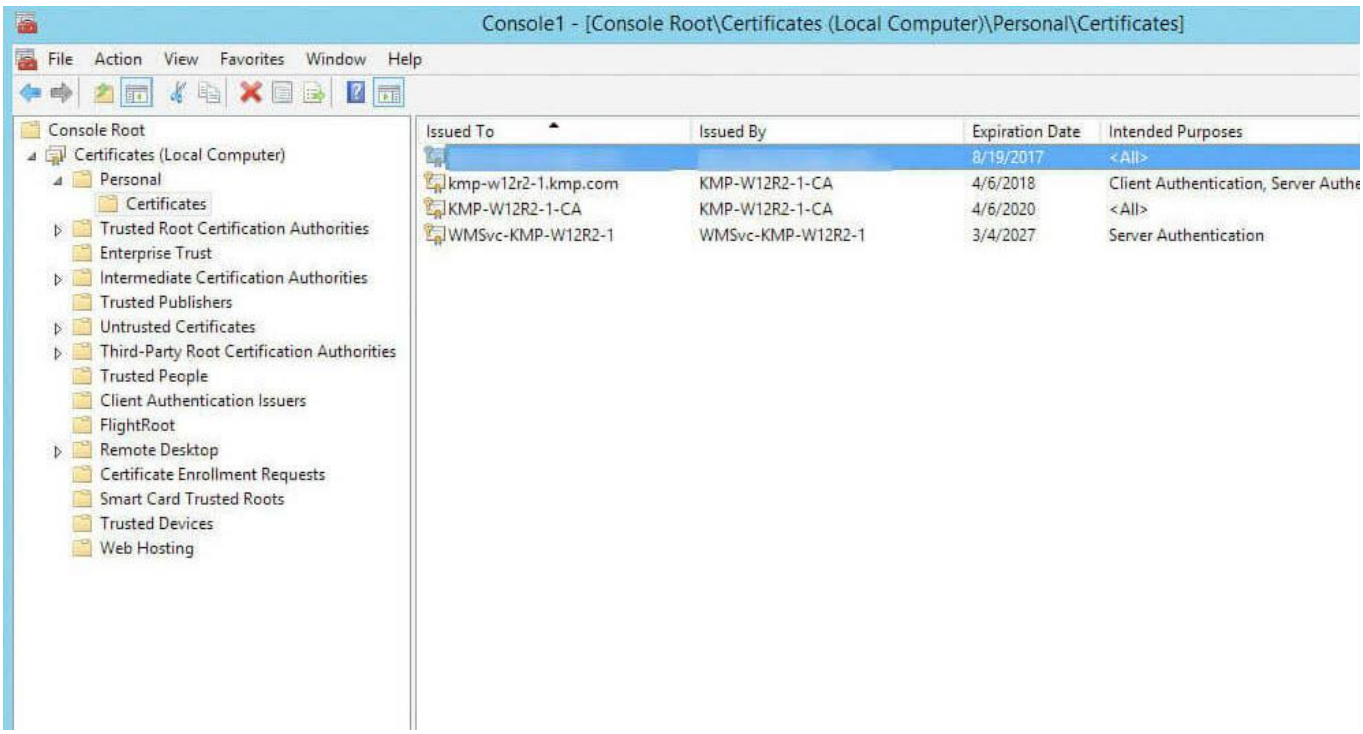


vii. Now, select **Enable PrivateKey Export from MS Store after deployment** to export private key from the certificate store.

viii. Cliick **Save** to save the agent details. After providing the details, click **Deploy**.



The selected certificates are deployed to **Personal Certificates**.

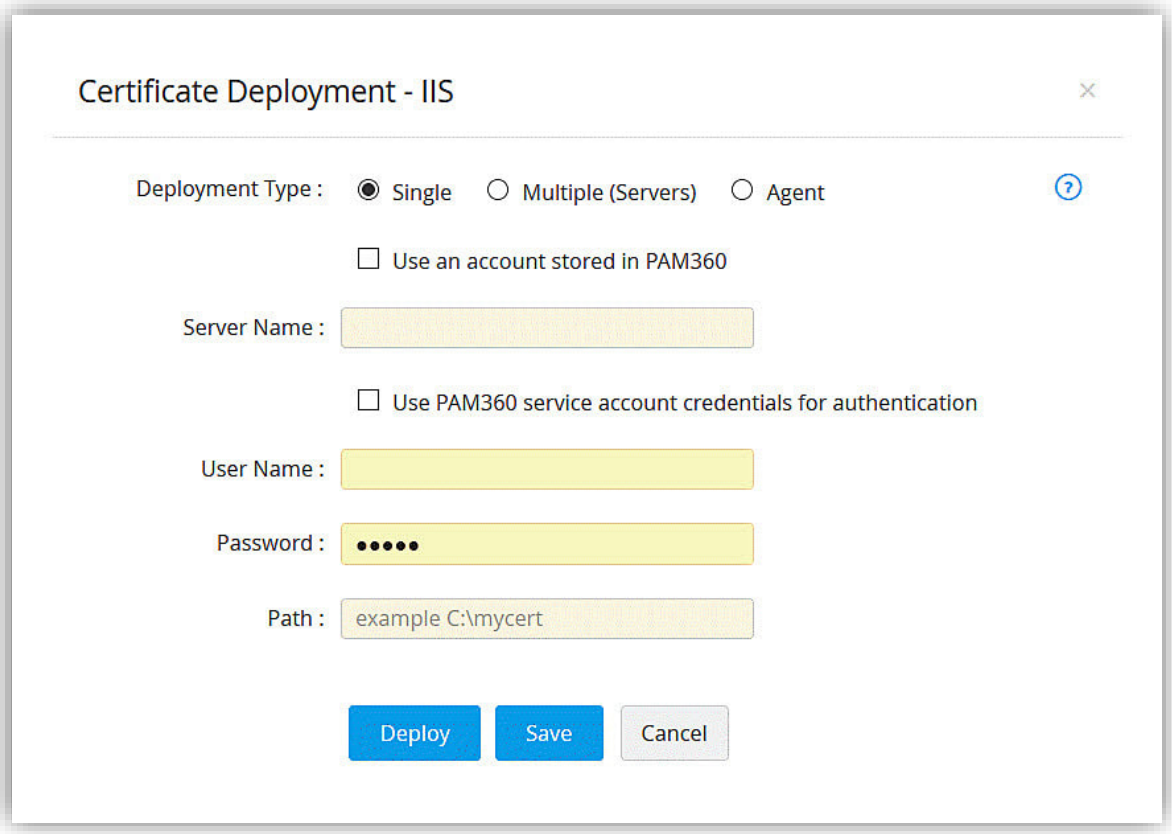


1.3 Deploying Certificates to Internet Information Services (IIS)

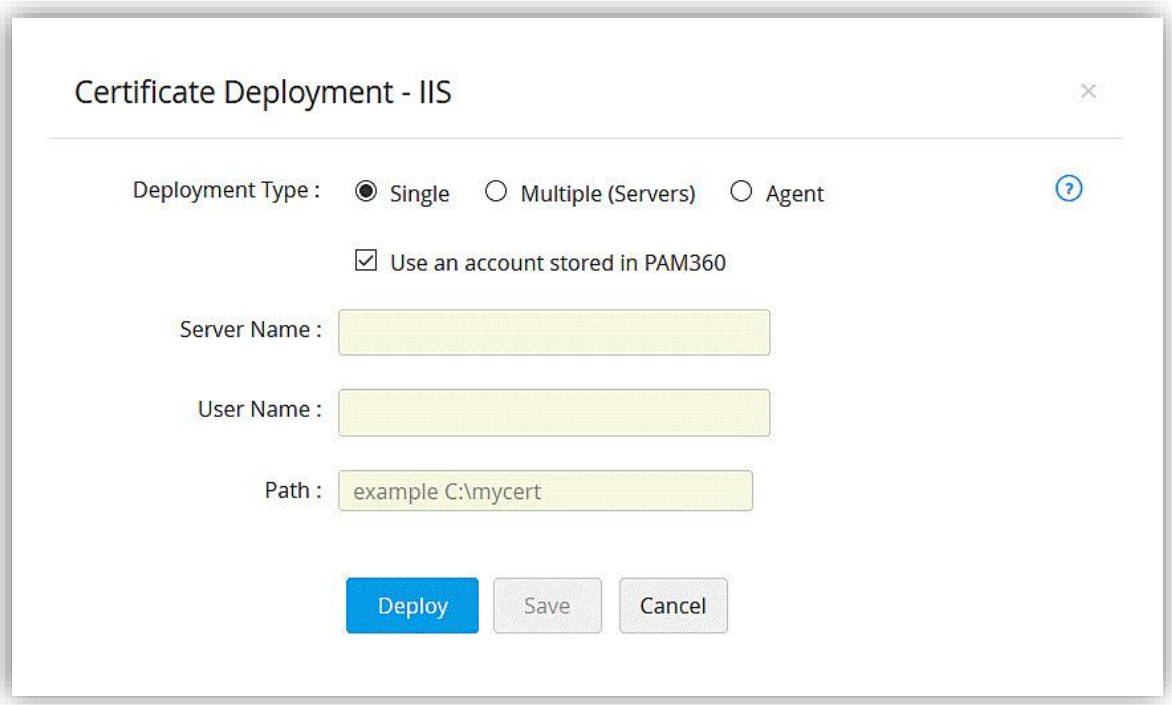
Follow the below steps to deploy a certificate on the IIS server. However, this procedure will only deploy the certificate to the server; IIS binding must be done separately.

1. To deploy certificates to Internet Information Services (IIS), choose the server type as **IIS**.
2. Select the **Deployment Type** as **Single, Multiple** or **Agent** as per your need.

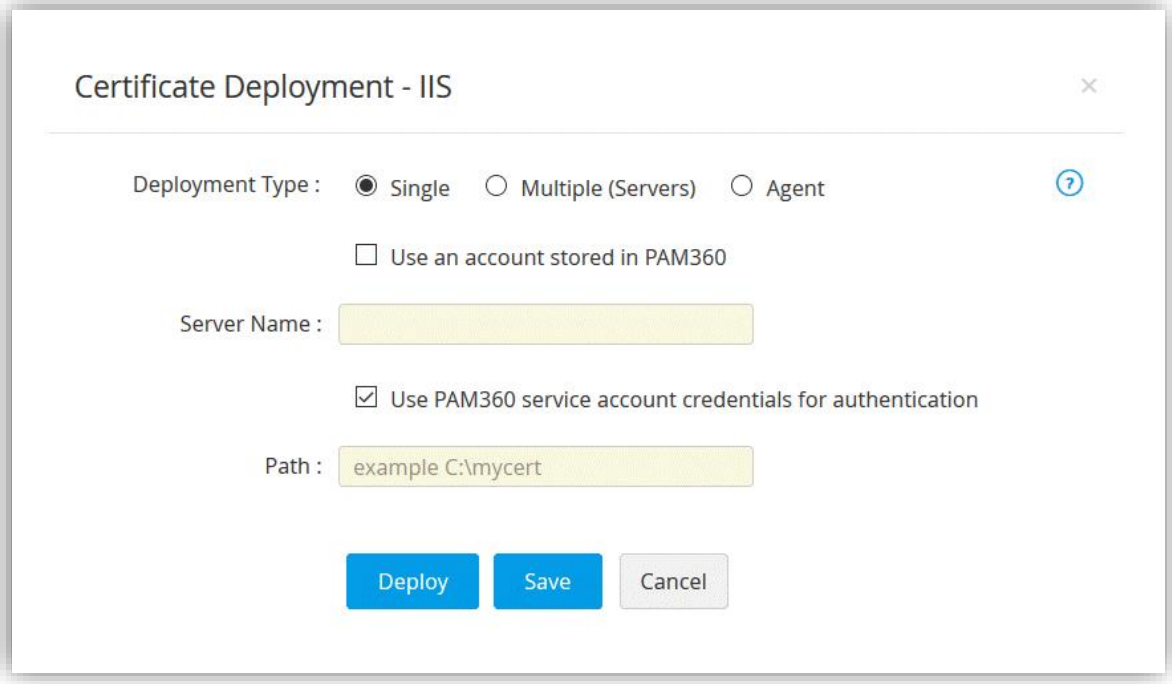
i. For **Single** deployment, provide the required details: **Server Name, User Name, Password, Path.**



ii. If you select the checkbox **Use an account stored in PAM360,** you need not provide the password as PAM360 will take the user account details directly from the database.



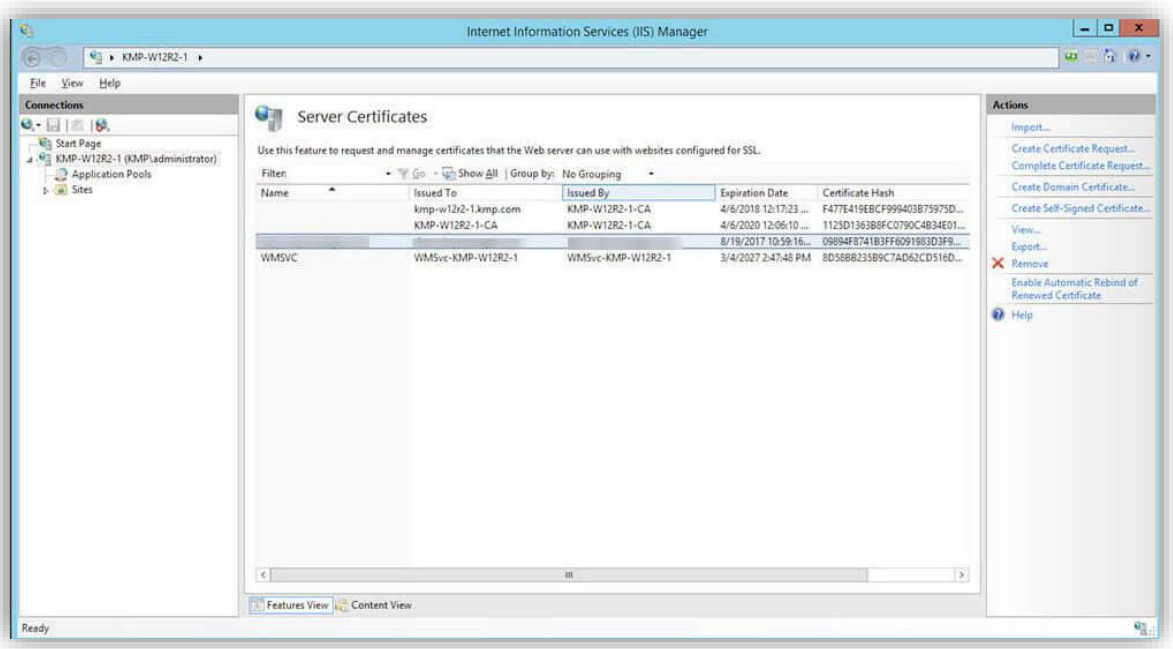
iii. If you select the checkbox **Use PAM360 service account credentials for authentication**, you need not provide the username and password as PAM360 will take the user account details directly from the database.



iv. For certificate deployment on **Multiple** servers, upload a .csv file comprising the following details: **Server Name, User Name, Password, Path.**

v. If you choose the Deployment Type as **Agent**, choose the host name of the PAM360 agent from the **Select Agent** dropdown and click **Save** to save the agent details.

vi. After providing the details, click **Deploy**.

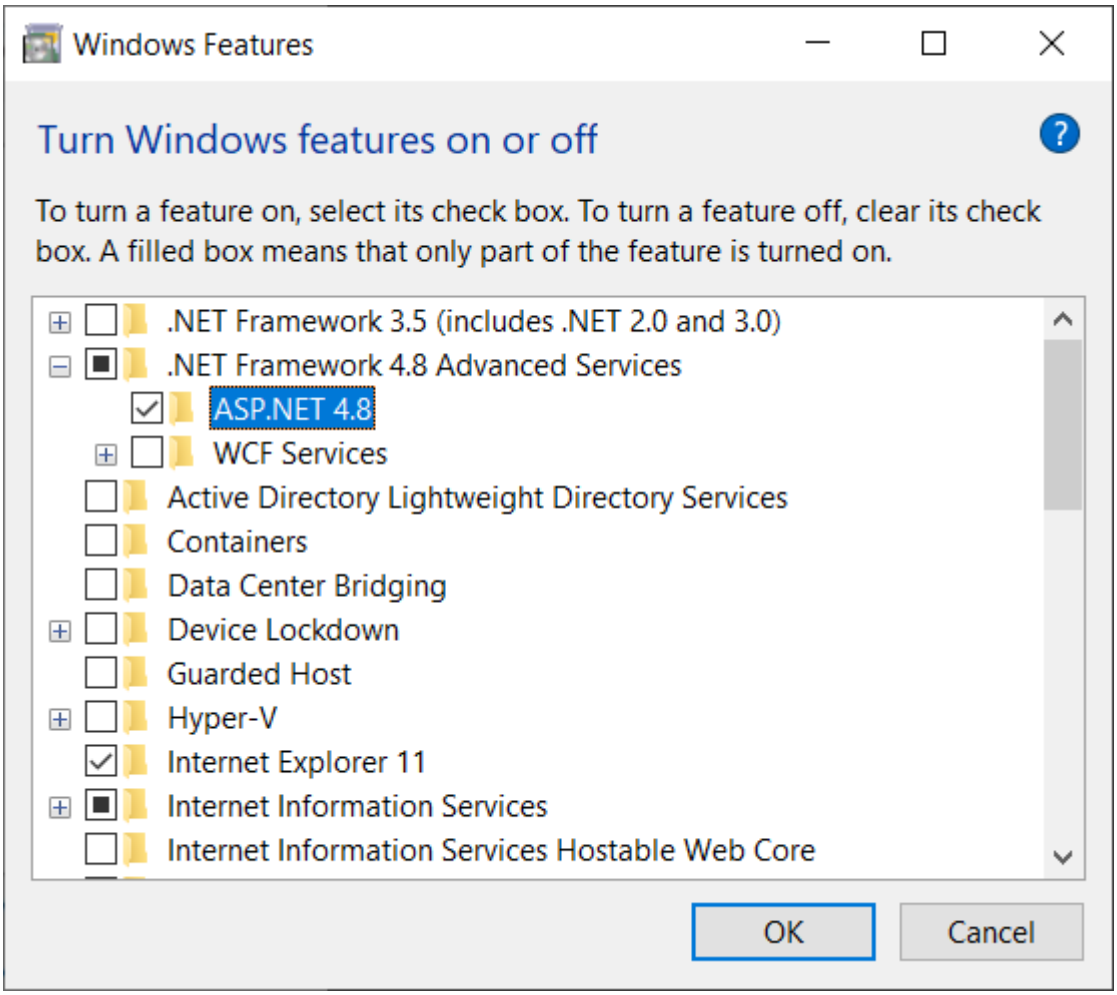


The certificate(s) are deployed to Server certificates of the specified server(s).

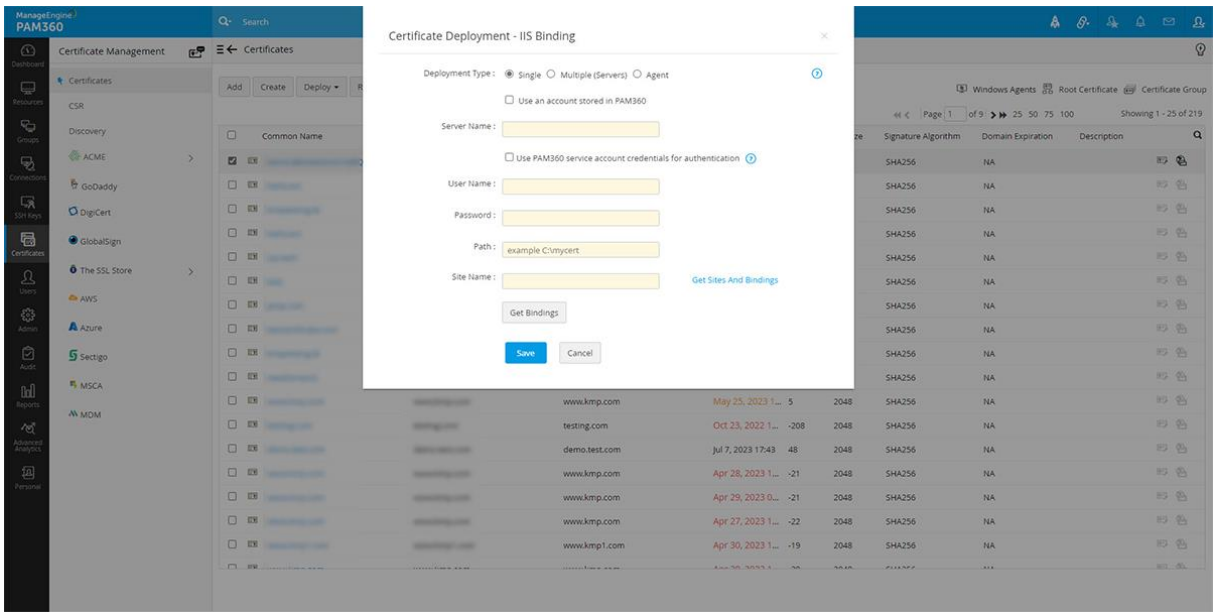
1.4 IIS Binding

Follow the below steps to deploy a certificate to the IIS server and bind the certificate to a site running in that server.

> **Note:** IIS Binding for the Deployment Type **Single** works only if the IIS server and PAM360 are in the same domain, which has **.Net Framework version 4 or above** enabled. However, if an IIS Server resides in a demilitarized zone, choose the Deployment Type as **Agent** and proceed with the steps for the same given below.



1. To deploy certificates on a Microsoft IIS server and perform IIS binding, choose the server type as **IIS Binding.**
2. Select the **Deployment Type** as **Single** or **Agent** as per your need.
    i. If you choose the deployment type as **Single**, enter the required details: **Server Name, User Name, Password, Path, Site Name.**

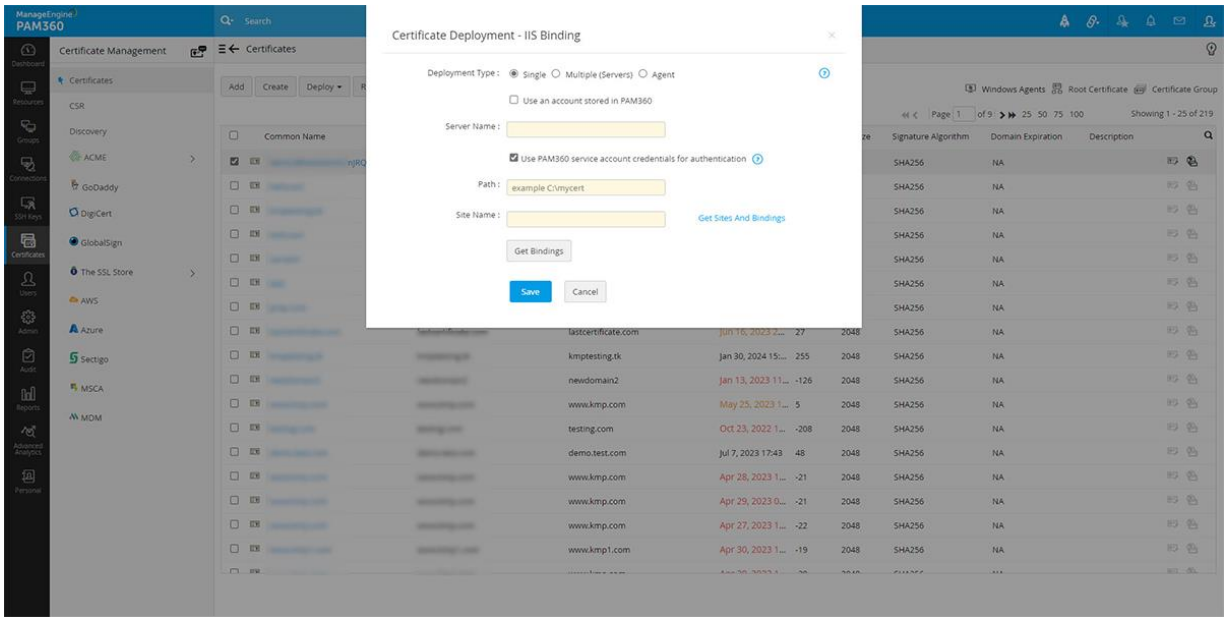


ii. Specify the name of a valid IIS server to which the certificate needs to be deployed, and provide the user account credentials.

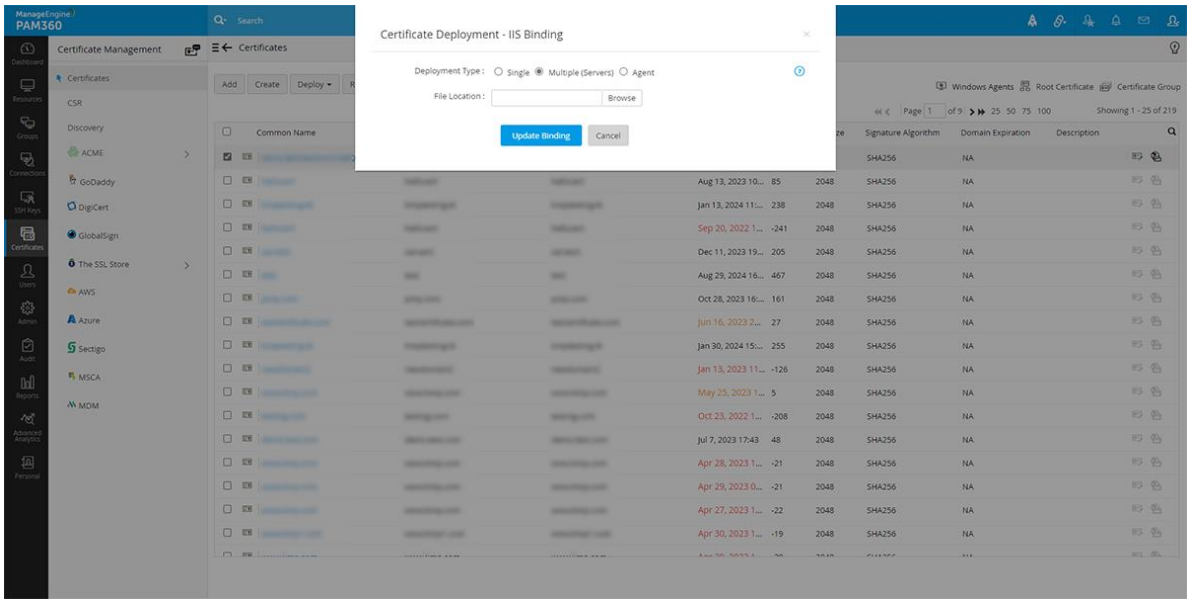
iii. Specify a path in the server where the certificate must be placed.

iv. If you select the checkbox **Use an account stored in PAM360,** you need not provide the password as PAM360 will take the user account details directly from the database.

v. If you select the checkbox **Use PAM360 service account credentials for authentication**, you need not provide the username and password as PAM360 will take the user account details directly from the database.



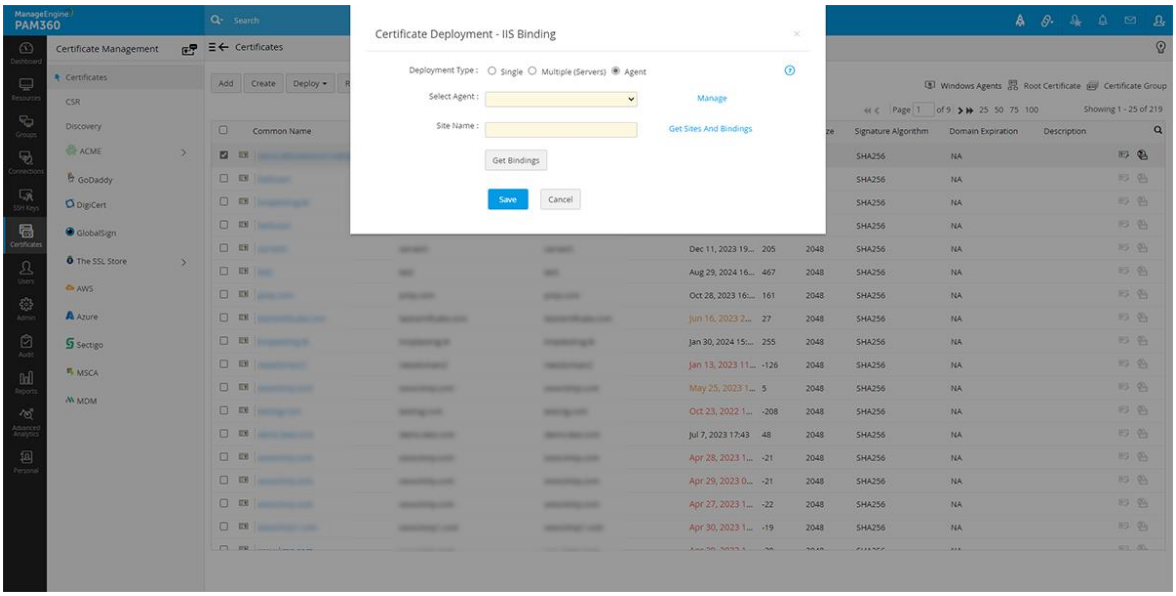
vi. If the IIS Server resides in a demilitarized zone, choose the **Deployment Type** as **Agent**. Select an agent from the drop-down. Click **Get Sites And Bindings** to list all sites and their respective bindings available in the selected server. Enter the name of a site in the **Site Name** field, click **Get Bindings** to list all the bindings available for that site.



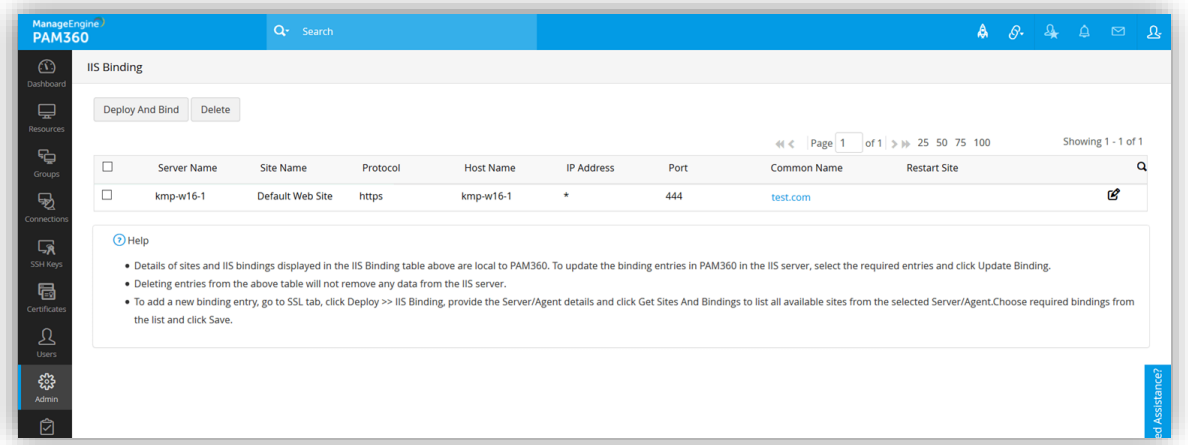
You can login using three different ways: with Credentials, using Service Authentication, or using Agent. Upload the file with the content in the following format:

a. For Single certificate selection,
b. <servername>, <CREDENTIALS>, <site name>, <binding information>, <server credentials>, <temp path>
c. (and/or)
d. <servername>, <SERVICE_AUTH>, <site name>, <binding information>, <temp path>
e. (and/or)
f. <servername>, <AGENT>, <site name>, <binding information>
g. For Multiple certificate selection, include <domain name> in the above format
h. Example: testServer,CREDENTIALS,test.com,Default Web Site,*:443:myhost,testUSer,testPwd,C:\
i. For Multiple certificates with same common name, include <domain name> along with the <serial number> in the above format.
j. Example: testServer,SERVICE_AUTH,test.com,se123245d,Default Web Site,*:443:myhost,C:\

vii. If the IIS Server resides in a demilitarized zone, choose the **Deployment Type** as **Agent**. Select an agent from the dropdown. Click **Get Sites And Bindings** to list all sites and their respective bindings available in the selected server. Enter the name of a site in the **Site Name** field, click **Get Bindings** to list all the bindings available for that site.



viii. Here, to add new bindings, click **Add New Bindings** and enter attributes such as **Host Name, Port, IP Address**, and select a certificate. The newly added bindings will be visible under **Admin >> SSH/SSL >> IIS Binding.** The new site bindings added in PAM360 will not reflect in the IIS server until they are deployed to the server using the **Deploy and Bind** option.



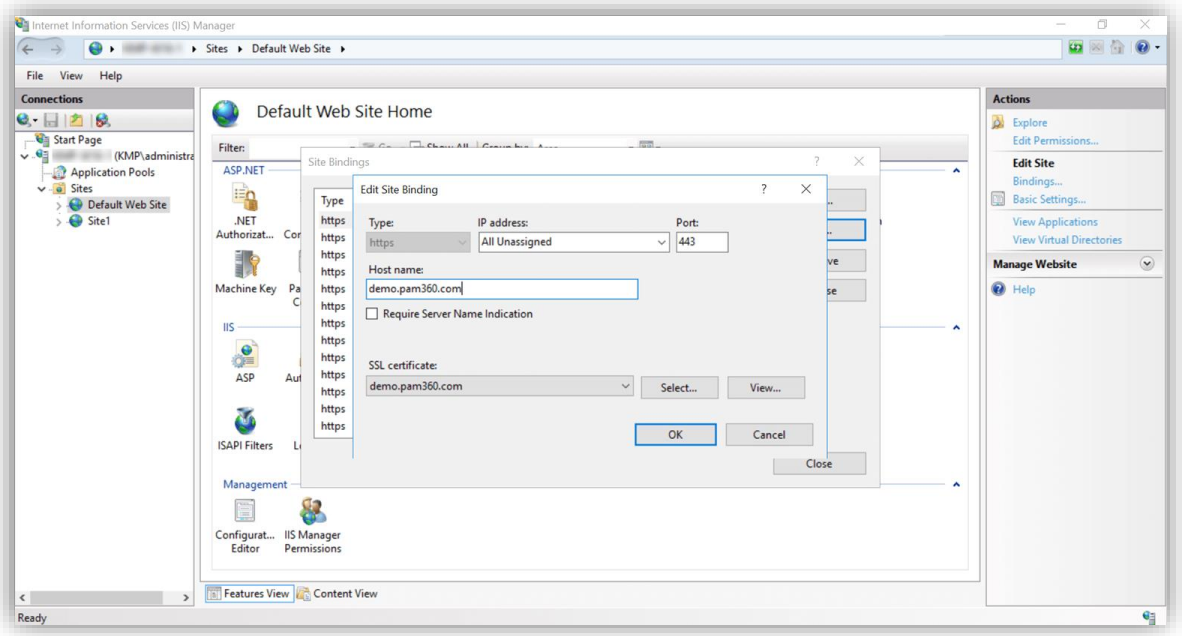
ix. To populate the list of sites associated with the IIS server, click **Get Site Names** and choose a site from the drop-down. To enter a site name manually in the **SiteName** field, click **Hide List,** type in the site name and click the **Get Bindings** option.

x. Enter the **Host Name**, **IP Address** and **Port** of the site manually.

xi. Select the **Restart Site** option to restart the site automatically.

xii. Click **Add Binding/Update Binding** to deploy the certificate at the path specified in your IIS server and complete IIS site binding.

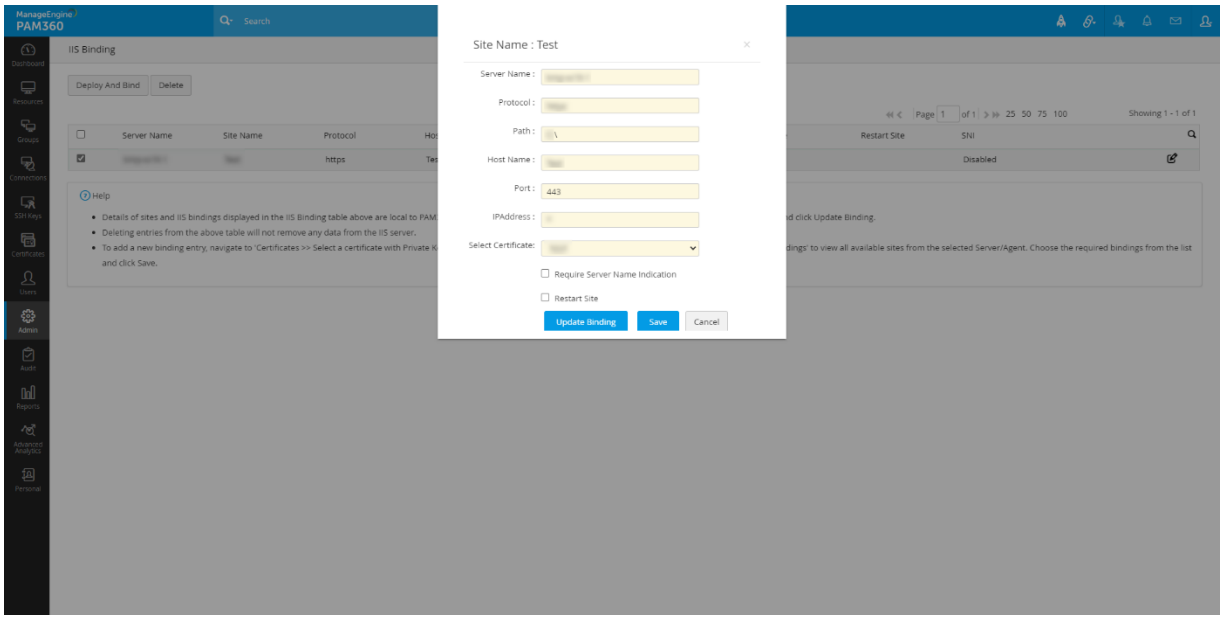
xiii. To update multiple bindings, select the required bindings from the list, click **Save**. Go to **Admin >> SSH/SSL >> IIS Binding,** select the bindings and click **Deploy and Bind.**



xiv. To save the specified details and deploy the certificate later, click **Save**. The server details and the respective site details will be available under **Admin >> SSH/SSL >> IIS Binding.**

xv. To edit the binding details, click the **Edit** icon beside a server. In the window that opens, modify any of the given details and click **Save**. Now, select the server name and click **Deploy And Bind** from the top bar. The selected certificate will be deployed on the servers and the IIS binding will be updated in the IIS server.

xvi. Details of sites and IIS bindings displayed in the IIS Binding table above are local to PAM360. To update the binding entries here with the entries from IIS server, select the required entries and click **Update Binding**.

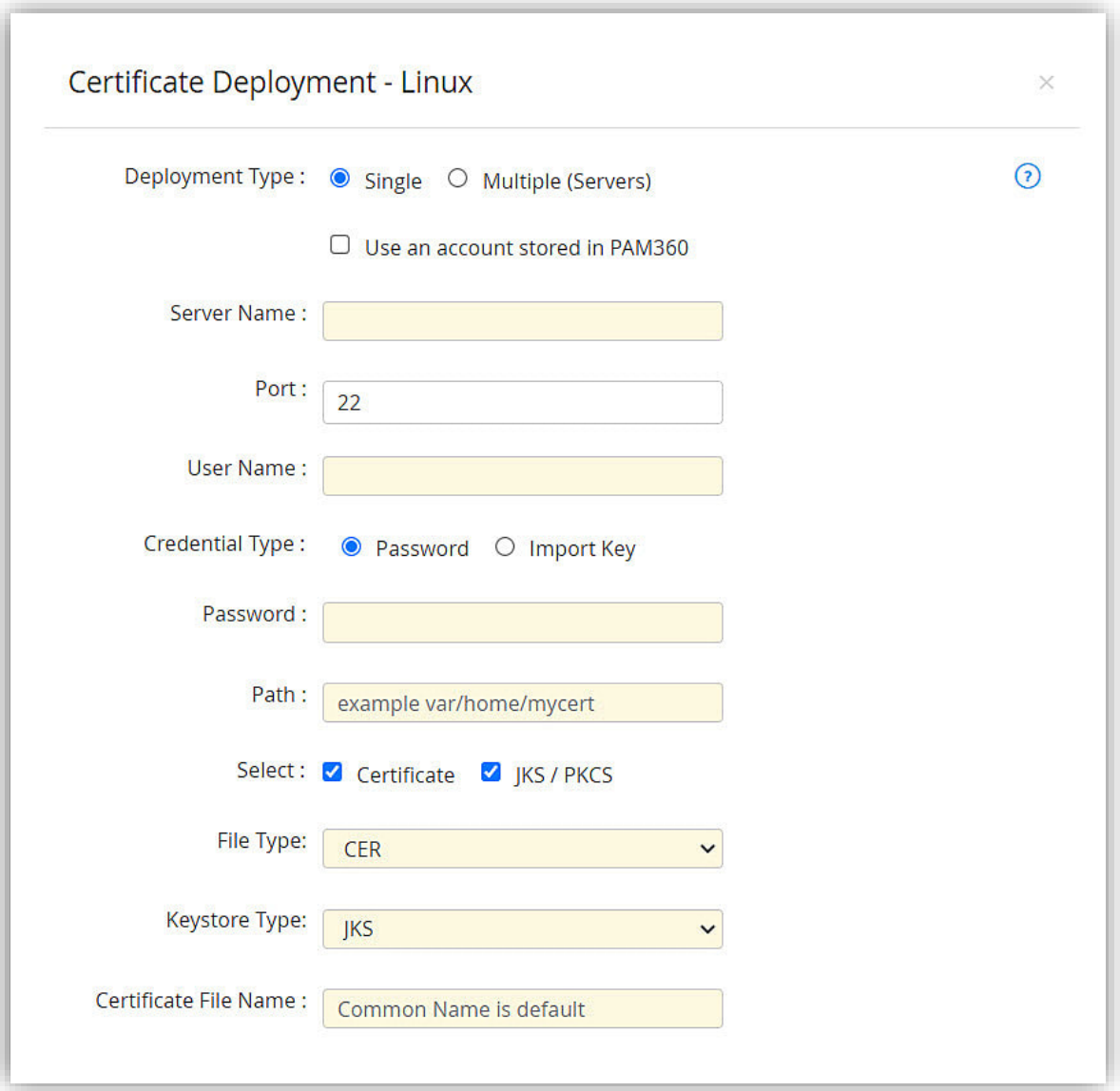


xvii. Deleting entries from the above table will not remove any data from the IIS server.

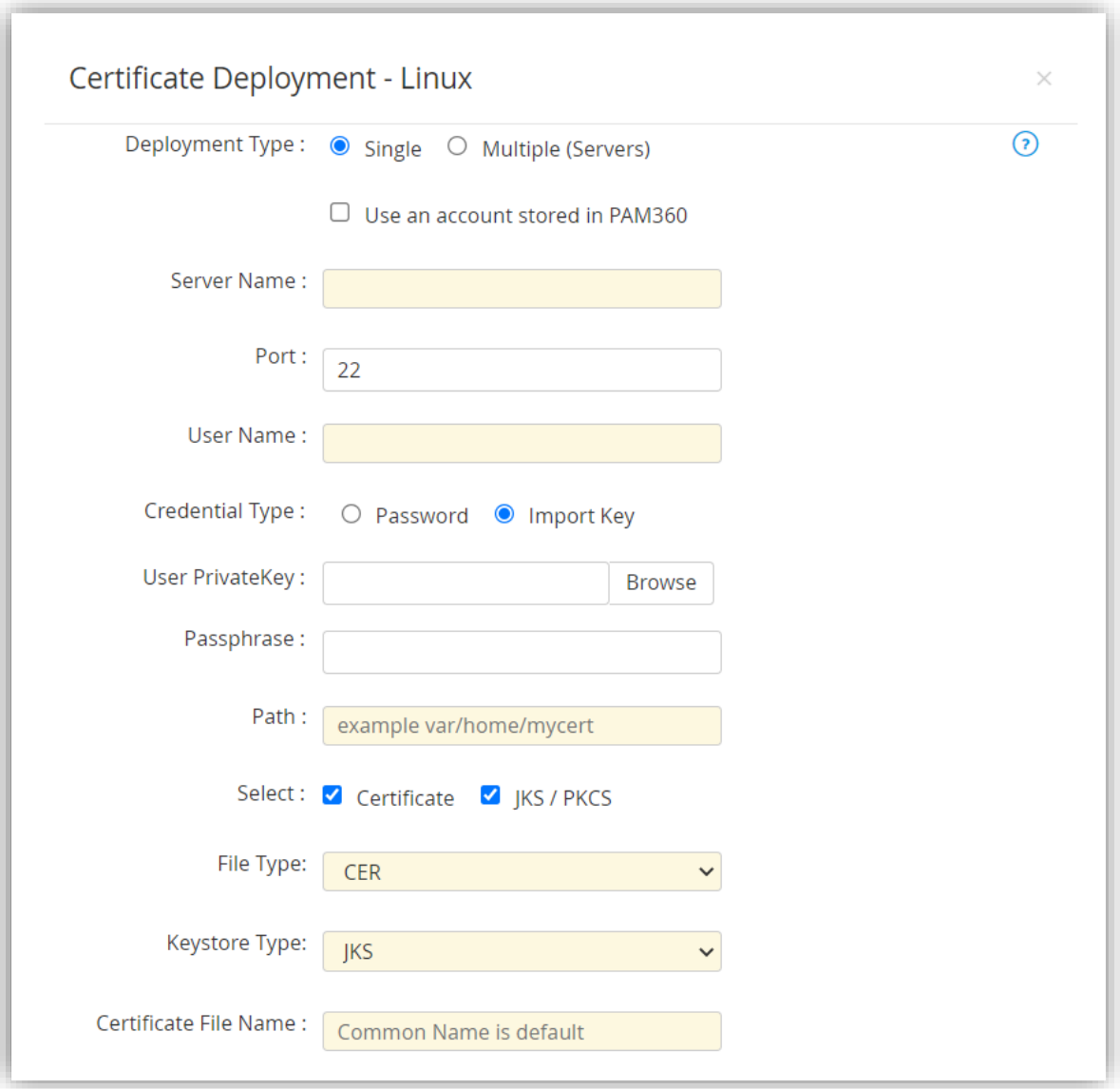
1.5 Deploying Certificates to a Linux Server

1. To deploy certificates to a Linux server, choose the server type as **Linux**.
2. Select the **Deployment Type** as **Single** or **Multiple** as per your need.

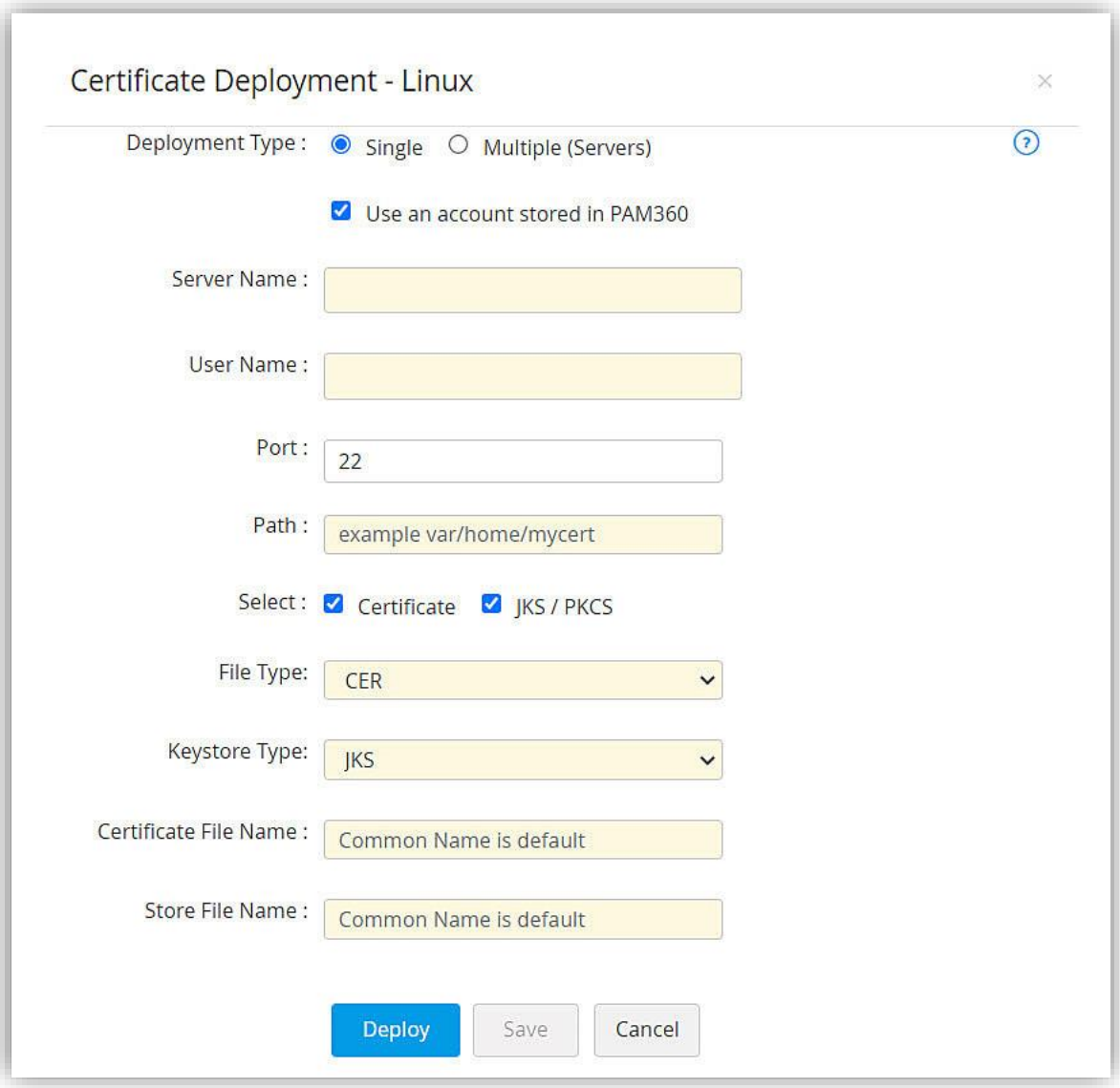
    i. For **Single** server deployment, provide the required details: **Server Name, Port** (port 22 is assigned by default), **User Name, Password, Path.** You can optionally enable **Certificate** to choose the **File Type** and mention the **Certificate File Name** or/and enable **JKS/PKCS** to choose the **Keystore Type** and mention the **Store File Name.**



ii. You can opt for a key-based authentication for password-less servers by choosing the **Import Key** credential type. Upload the private key associated with the required user account in the target server and provide the key passphrase.



iii. If you select the checkbox **Use an account stored in PAM360**, you need not provide the password as PAM360 will take the user account details directly from the database.



iv. For certificate deployment on **Multiple** servers, upload a **.csv** file comprising the following details: **Server Name, User Name, Password, Path, Certificate file name** (optional), **Keystore File Name**(optional). You can optionally enable **Certificate** to choose the **File Type** or/and enable **JKS/PKCS** to choose the **Keystore Type.**

v. You can also opt for a key-based authentication for password-less servers by choosing the **Import Key** credential type. Upload the **Private Key** associated with the required user account in the target system and provide the key **Passphrase.**

3. After providing the details, click **Deploy.**

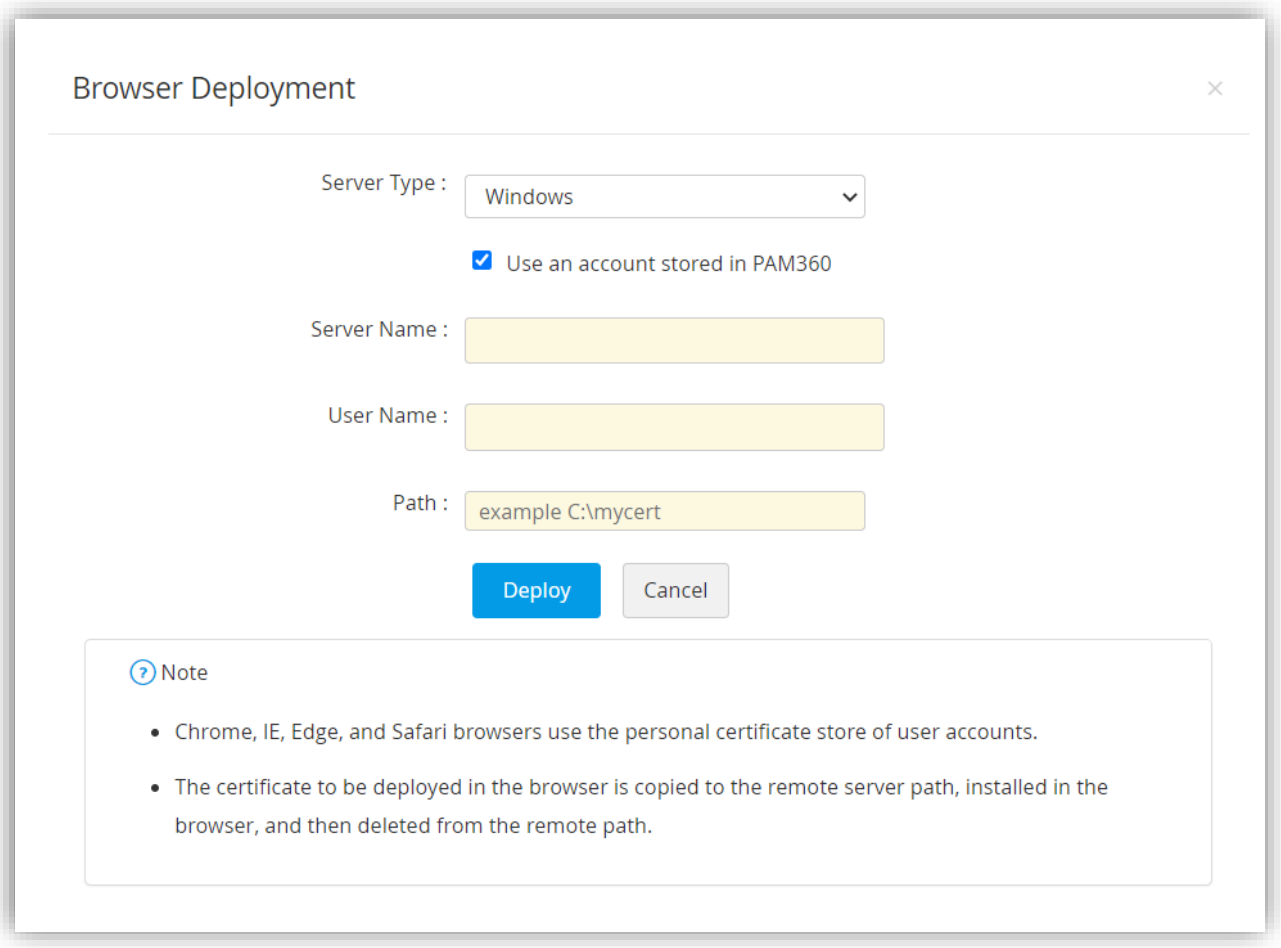
The certificate is deployed to the specified server in the specified path.

Notes:

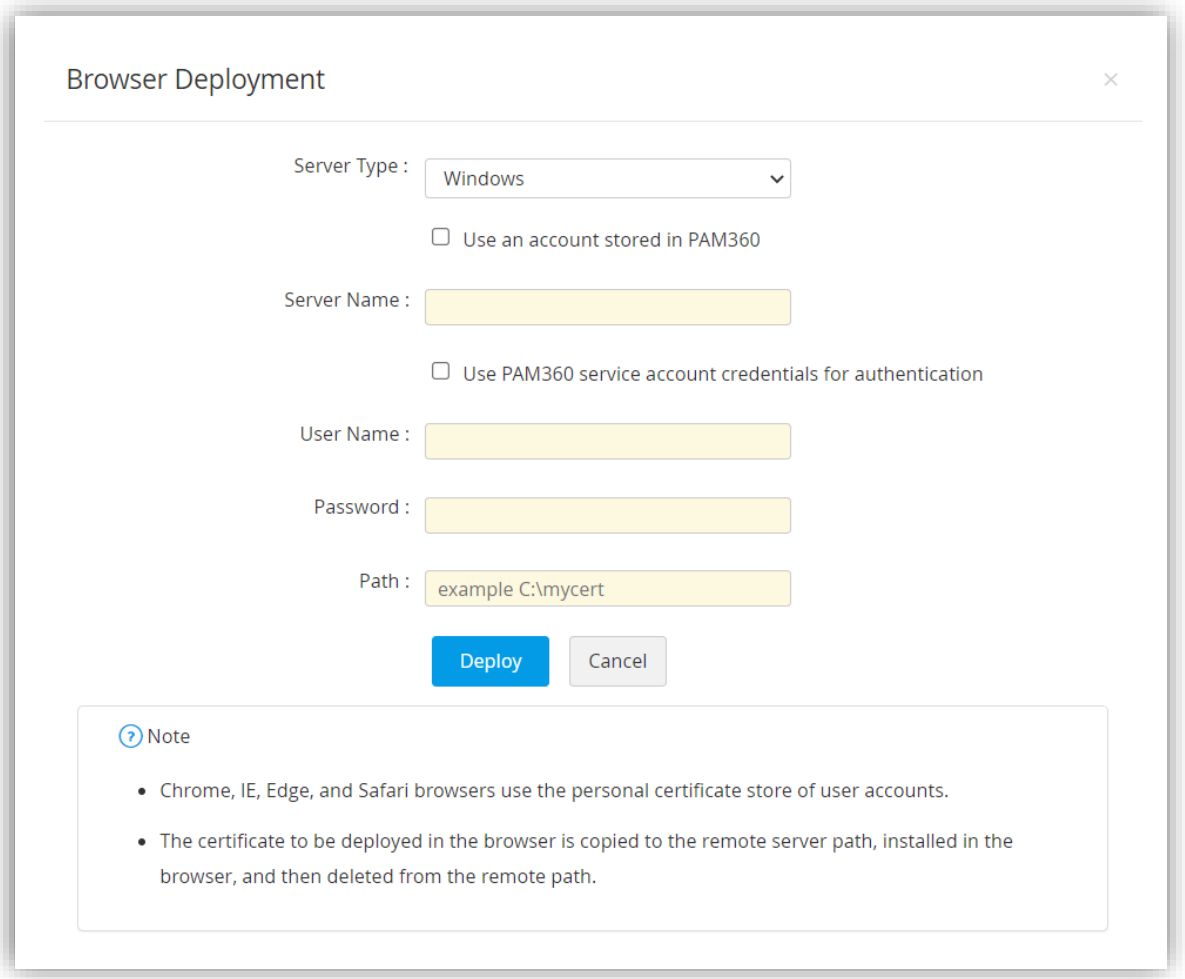
1. Key-based authentication option is available for single deployment type only.
2. The private key uploaded during key-based authentication is for one-time use only and is not stored anywhere in the PAM360 database. If you wish to add it to the PAM360 repository, use the **Import Keys** option from the **SSH Keys** tab to do it manually.

1.6 Deploying Certificates to a Browser

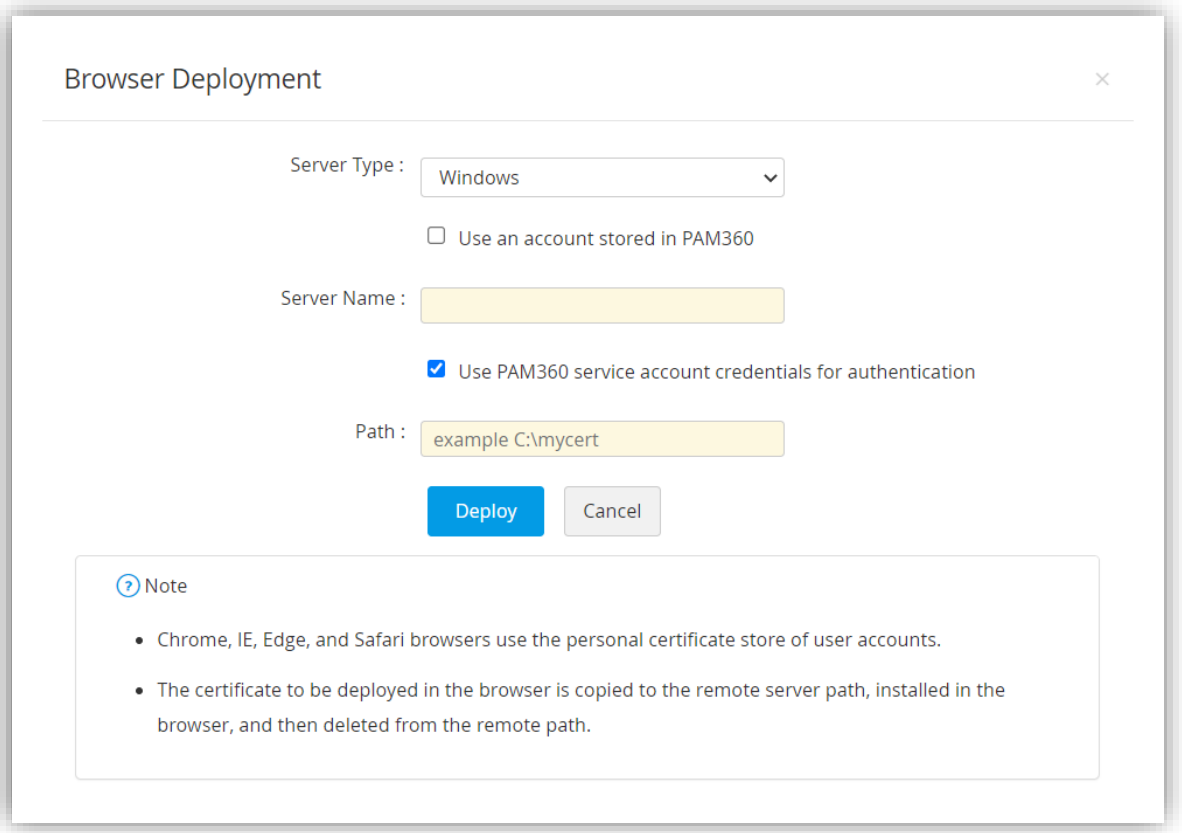
1. To deploy certificates on a browser, choose the deploy type as **Browser.**
2. Select the **Server Type** as **Windows, Linux** or **Mac OS** as per your need.
3. If you select the checkbox **Use an account stored in PAM360**, you need not provide the password as PAM360 will take the user account details directly from the database.



4. If the server type is **Windows,**
    i. Mention the **Server Name, User Name, Password** and **Path.**

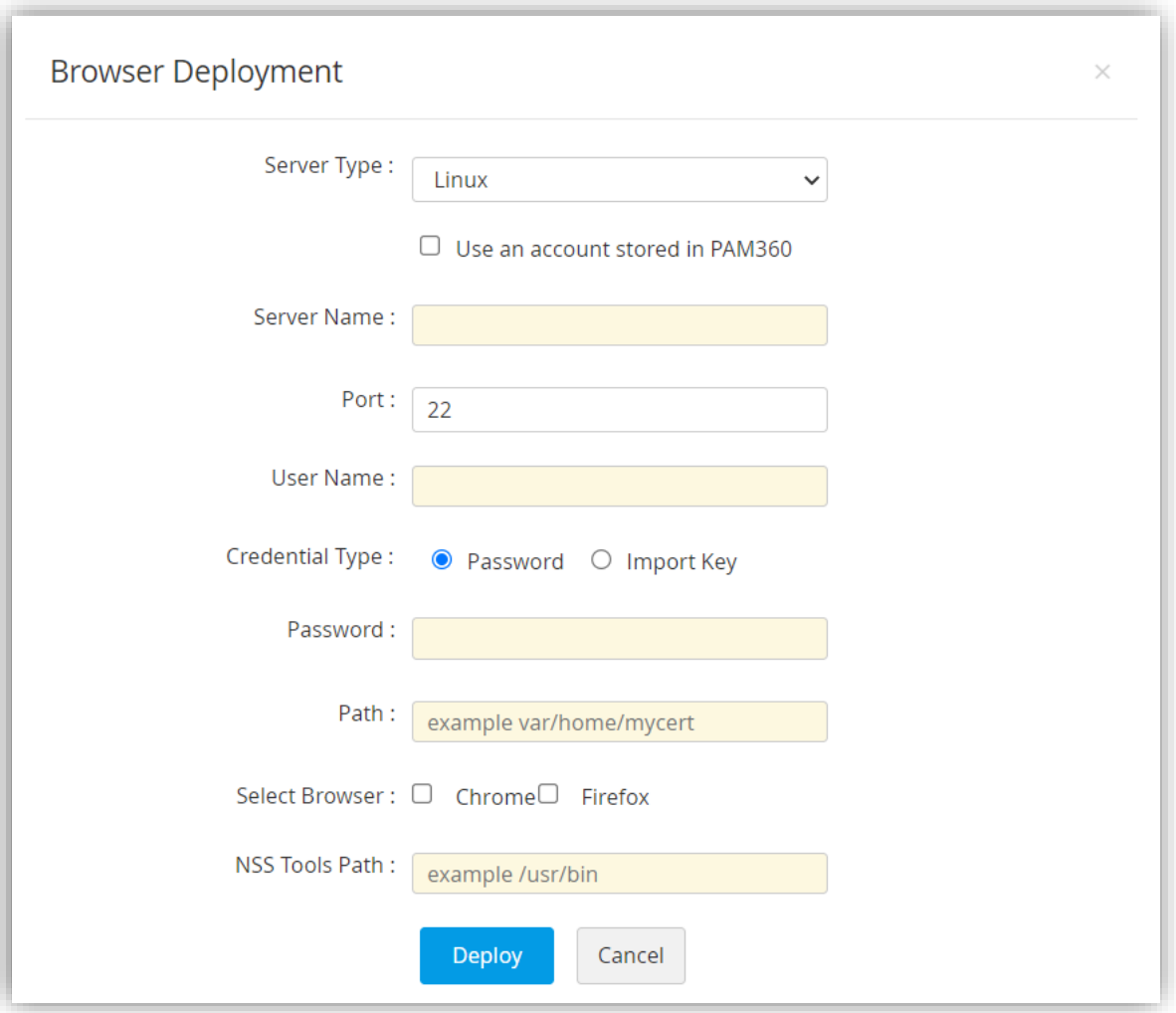


ii. If you select the checkbox **Use PAM360 service account credentials for authentication**, you need not provide the **User Name** and **Password** separately, as the service account credentials used for PAM360 will be used here too.



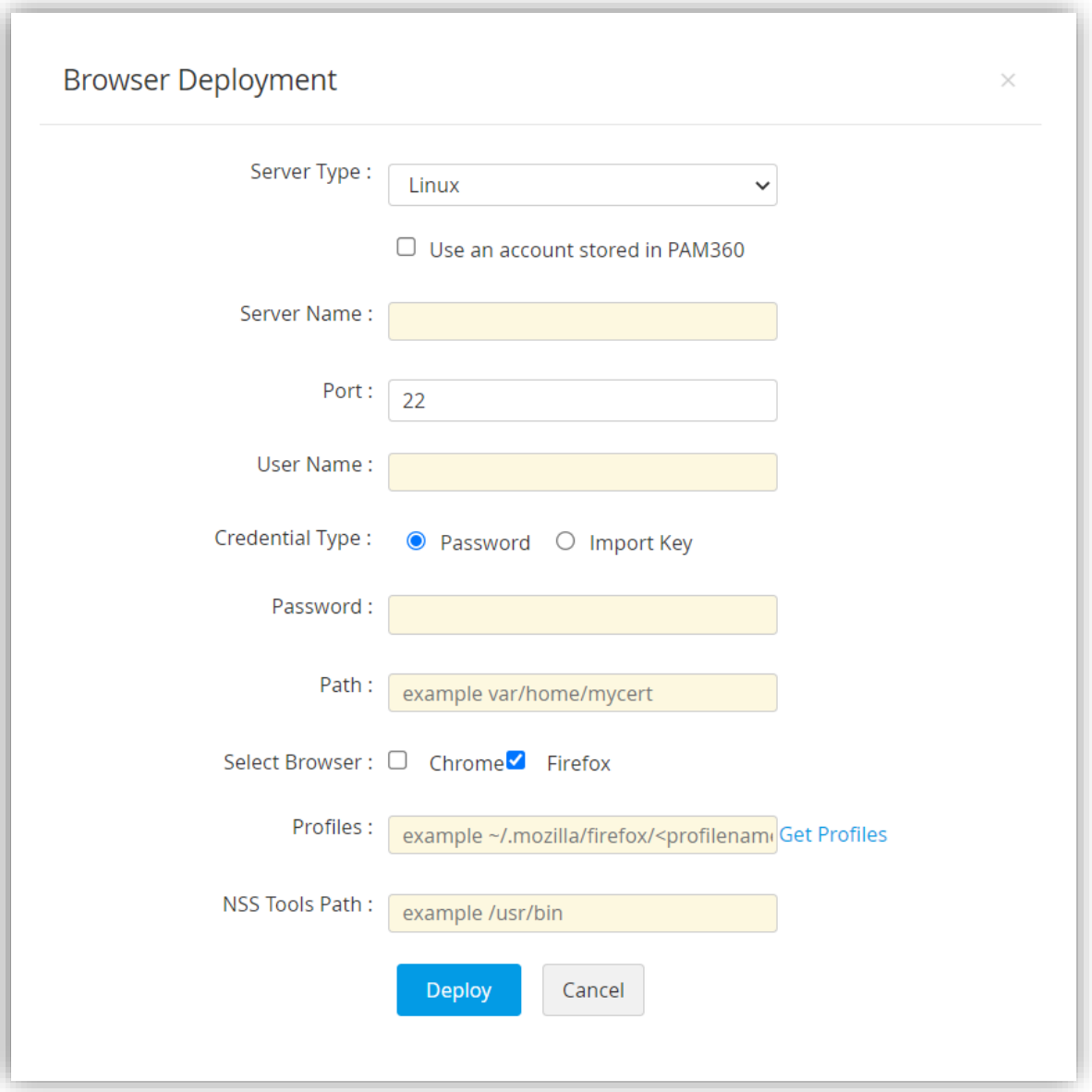
5. If the server type is **Linux,**

    i. Enter the **Server Name, Port, User Name, Password** and **Path.**



ii. Select the required **Browser(s)** (**Firefox** or/and **Chrome**) where the certificate is to be deployed.

iii. If you select **Firefox**, mention the **Profile** name. Click **Get Profiles** to choose from available profiles.



Note:

Get Profiles option gets all profiles path from profiles.ini file from the following location:

Windows: APPDATA\Mozilla\Firefox\profiles.ini

Linux: $HOME/.mozilla/firefox/profiles.ini

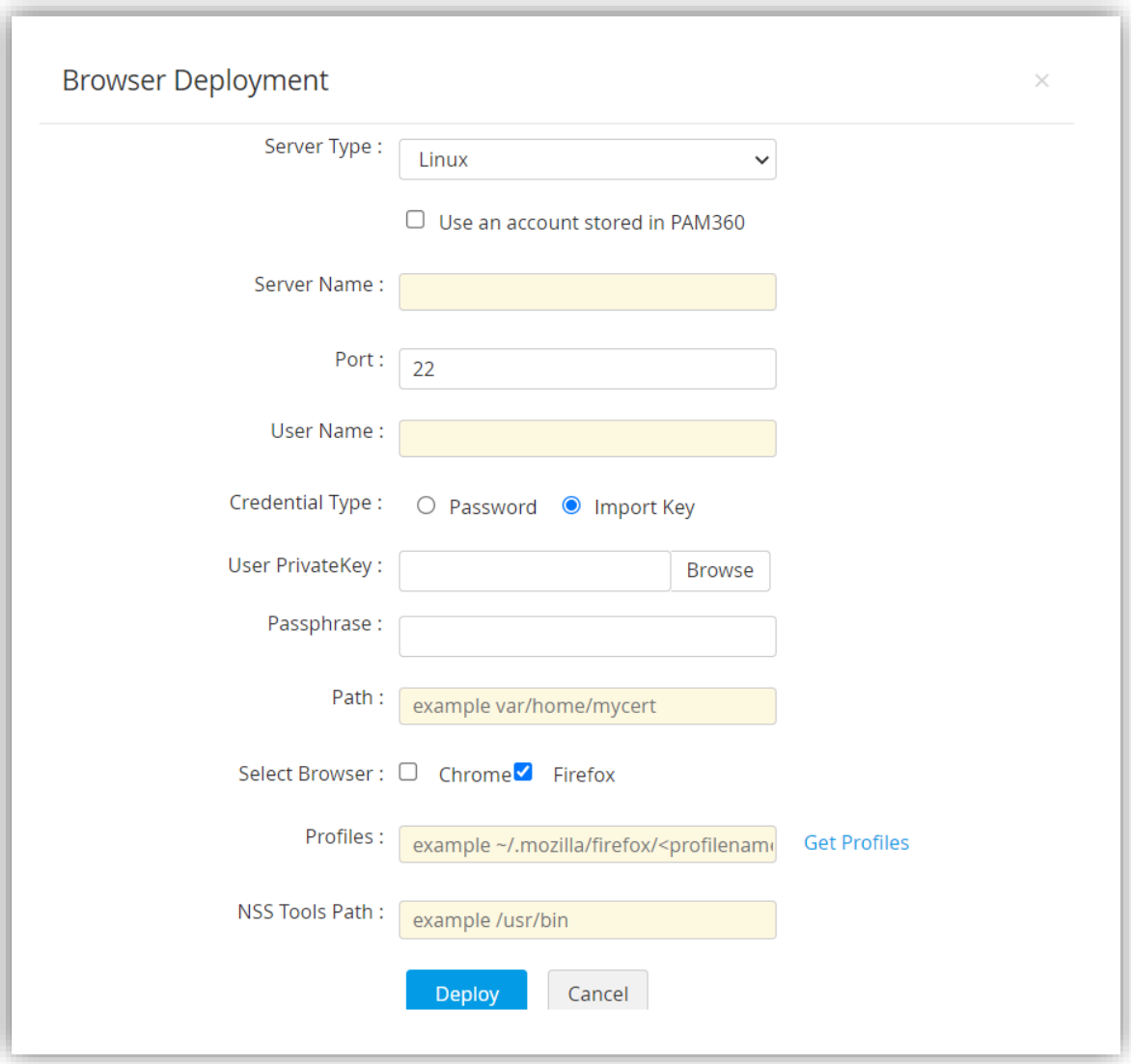
Mac: $HOME/Library/Application Support/Firefox/profiles.ini

iv. Mention the **NSS Tools Path.**

Notes:

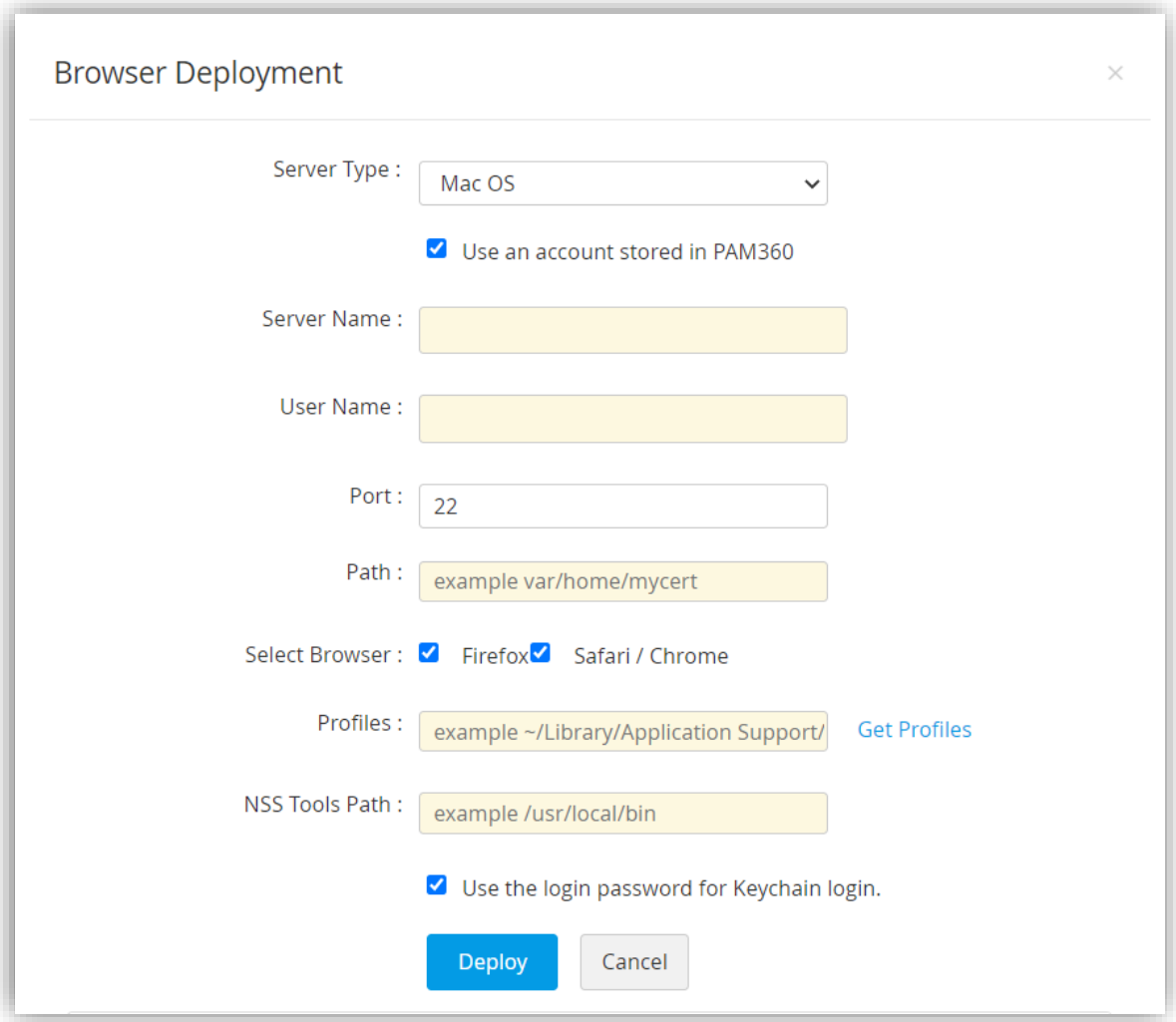
1. In Linux, Chrome and Firefox use NSS shared DB to manage the certificates. This NSS tool can be installed using the following command: sudo apt-get install libnss3-tools.
2. For Chrome, the certificate is deployed in NSS DB in the following path: $HOME/.pki/nssdb.
3. For Firefox, Profiles folder contains the NSS DB to manage certificates.

v. You can also opt for a key-based authentication for password-less servers by choosing the **Import Key** credential type. Upload the **User PrivateKey** associated with the required user account in the target system and provide the key passphrase.



6. If the server type is **Mac OS,**
    i. Enter the **Server Name, Port, User Name, Password** and **Path.**
    ii. Select the required **Browser(s)** (**Firefox** or/and **Safari/Chrome**) where the certificate is to be deployed.
    iii. If you select **Firefox**, mention the **Profile** nameand **NSS Tools Path.** Click **Get Profiles** to choose from available profiles.
    iv. If you select **Safari/Chrome** you can choose to **Use the login password for Keychain login** or mention the Login Keychain Password.

    Note: For Safari and Chrome, Mac OS uses System Keychain to manage certificates. For Firefox, NSS DB from profiles manages the certificates. To install NSS utils, use the following command: brew install nss.



7. Click **Deploy.**

Now, you have successfully deployed the certificate to the selected browsers.

1.7 Deploying Certificates to ManageEngine MDM

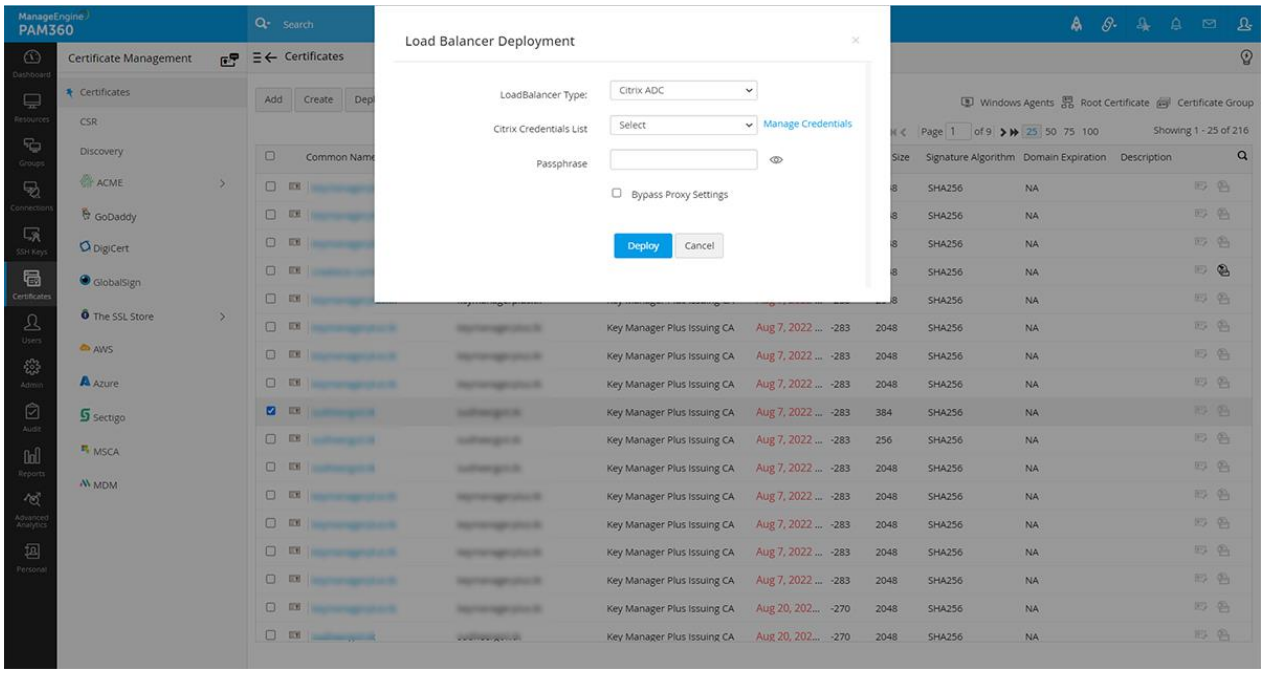
To learn about deploying certificates to ManageEngine MDM, click here.

1.8 Deploying Certificates to AWS-ACM

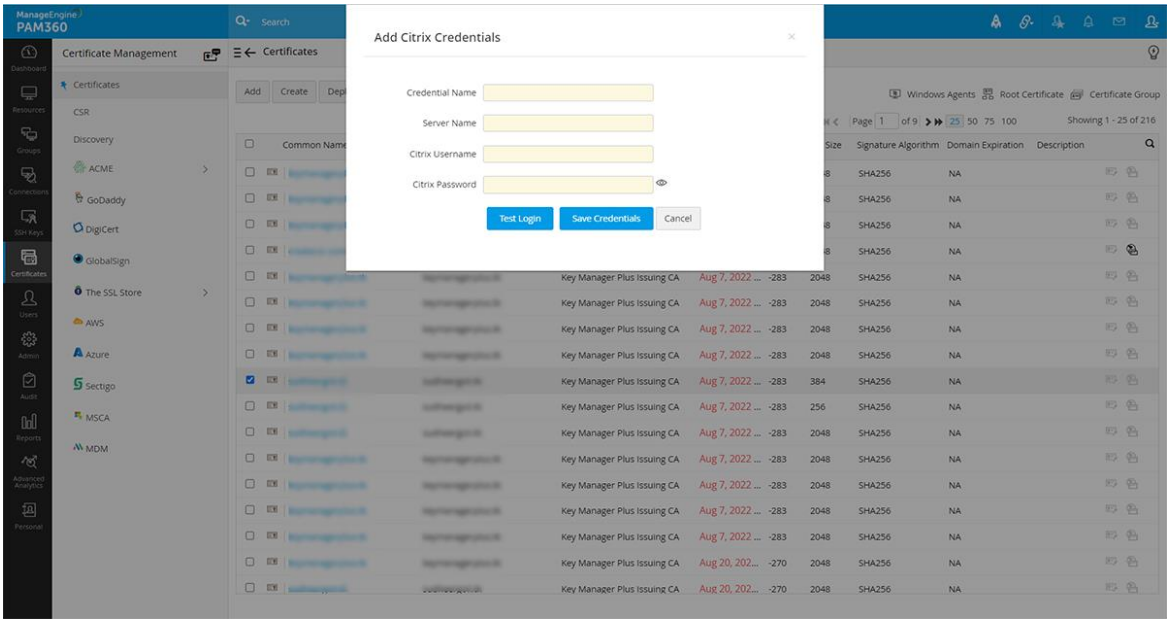
To learn about deploying certificates to AWS-ACM, click here.

1.9 Deploying Certificates to Load Balancer

1. To deploy certificates on a LoadBalancer, choose the deploy type as **Load Balancer**.
2. In the pop-up that appears, select the **Citrix ADC** as the **Load Balancer Type**.
3. Select the required **Citrix Credential List** from the dropdown.



4. Click **Manage Credentials** to add or delete a credential.
    i. In the pop-up that appears, click to **Add** and mention the **Credential Name, Server Name, Citrix Username** and **Citrix Password**.
    ii. Click **Test Login** to test the credential and click **Save Credentials**.
    iii. To delete a credential, select a credential you want to delete and click **Delete** and in the pop-up that appears click **OK**.



5. Enter the **Citrix Password** and a **Passphrase**. You can also use the Generate Password icon to generate a secure passphrase.
6. During Citrix load balancer discovery using REST API, you can choose to bypass your proxy server settings by selecting the **Bypass Proxy Settings** checkbox. This option

allows you to bypass the proxy server you have enabled under **Admin settings** directly perform Citrix load balancer discovery through the internet.

7. Select **Service Deploy**. In the pop-up that appears, select the services to deploy the load balancer and click **Select Services**.
8. Select **Virtual Server Deploy**. In the pop-up that appears, select the virtual servers to deploy the load balancer and click **Select Virtual Servers**.
9. Click **Deploy**.

Now, you have successfully deployed the certificate to the selected LoadBalancer.

SSL Vulnerability

PAM360 scans SSL certificates in its repository and flags certificates that are prone to any vulnerability. This way, users are kept informed of certificates / server configurations that are insecure. Users can then take necessary remedial measures to replace or change the SSL certificates or server configurations. PAM360 scans your SSL environment for the following categories of vulnerability.

1. SSL Certificate Revocation Status
    1.1 Certificate Revocation List (CRL)
    1.2 Online Certificate Service Protocol (OCSP) Revocation Status
2. SSL End-Server Vulnerability
    2.1 Heartbleed Bug
    2.2 POODLE SSL
    2.3 SSL 3.0 Enabled
    2.4 Weak Cipher Suites
3. Key Takeaways
4. SSL Vulnerability Scan

1. SSL Certificate Revocation Status

This check is performed to get information about the revocation status of a selected certificate. If the certificate for any of your domains in use is revoked, you have to take steps to replace it immediately. Revocation status for a certificate is obtained using two methods.

1.1 Certificate Revocation List (CRL)

i. Error:

The selected certificate is revoked and can no longer be trusted.

ii. What's the issue?

Certificate Revocation List (CRL) is a list of SSL certificates that are revoked by the Certificate

Authorities (CAs) before their expiration date. Certificates are revoked because of various reasons such as mis-issuances, private key compromise, CA compromise etc., CRLs are a kind of blacklist used by browsers to verify the validity of a certificate. Such tests are essential because, SSL certificates are the means by which browsers and users trust your identity and an invalid SSL certificate brings down their trust for your organization.

PAM360 checks CRL revocation status for your certificates and flags certificates that have been revoked.

Learn more about CRL

1.2 Online Certificate Service Protocol (OCSP) Revocation Status

i. Error:

The selected certificate is revoked and can no longer be trusted.

ii. What's the issue?

Online Certificate Service Protocol (OCSP) is an internet protocol used for obtaining the revocation status of a digital certificate. Web browsers send the certificate in question to the respective Certificate Authority (CA). The CA then returns the response - 'valid', 'revoked' or 'unknown'.

PAM360 checks OCSP revocation status for your certificates and flags certificates that have been revoked.

Learn more about OCSP revocation

iii. Workaround:

If any of the above tests render positive for certificate revocation, you have to immediately replace the particular certificate. Failing to do so might cause browsers to throw security errors for your website.

You can replace the revoked certificates with new certificates from trusted third parties directly from PAM360. Refer to the detailed help section to learn more about certificate request and deployment using PAM360.

2. SSL End-Server Vulnerability

End-server vulnerability is caused due to improper configuration of SSL protocol in your domain server. PAM360 tests your domain servers for the following end-server vulnerability.

2.1 Heartbleed Bug

i. Error:

The selected server is prone to Heartbleed vulnerability.

ii. What's the issue?

Heartbleed bug is a vulnerability in the OpenSSL, a popular open source cryptographic library that helps in the implementation of SSL and TLS protocols. This bug allows attackers to steal private keys attached to SSL certificates, usernames, passwords and other sensitive data without leaving a trace.

PAM360 checks your domain servers for Heartbleed bug vulnerability and flags the affected servers.

Learn more about Heartbleed bug

iii. Workaround

Patch your OpenSSL software. Replace the vulnerable versions with safe versions of the software.

2.2 POODLE SSL

i. Error:

The selected server is prone to POODLE attack.

ii. What's the issue?

The POODLE is a form of a man-in-the-middle attack that exploits the vulnerability in the CBC encryption scheme as implemented in the SSL 3.0 protocol. Though POODLE is not as serious as the Heatbleed vulnerability, best practices recommend you discover and mitigate the problem as quickly as possible.

PAM360 scans your servers and flags servers that are vulnerable to POODLE attack.

Learn more about POODLE

iii. Workaround:

Disable SSL 3.0 protocol and enable TLS protocols (1.0, 1.1 and 1.2) on the client-side. It's to be noted that by default, PAM360 disables SSL 3.0 protocol on the PAM360 server.

2.3 SSL 3.0 Enabled

i. Error

The selected server exploits the outdated SSL 3.0 protocol, which is prone to known vulnerabilities.

ii. What's the issue?

It has been discovered that SSL 3.0 protocol has a flaw in its design that makes it vulnerable to man-in-the-middle attacks. If you have a public facing website dealing with payments, you should immediately discover all servers that exploit SSL 3.0 and upgrade to TLS version.

PAM360 scans servers in your network and flags all servers that make use of this protocol.

Learn more about SSL 3.0 vulnerability

iii. Workaround:

Disable SSL 3.0 protocol and enable TLS protocols (1.0, 1.1 and 1.2) on the client-side. It's to be noted that by default, PAM360 disables SSL 3.0 protocol on the PAM360 server.

2.4 Weak Cipher Suites

i. Error:

The selected server exploits weak SSL ciphers, which is a medium risk vulnerability.

ii. What's the issue?

Many organizations knowingly or unknowingly exploit weak SSL protocols and cipher suites in their domain servers which makes their website vulnerable to various MITM attacks. To play safe, they have to identify those weak ciphers, disable them and re-configure the domain servers. By default, SSL 3.0 is disabled on PAM360 server, which is a weak SSL protocol. In

addition, PAM360 scans the end-point servers and flags the weak ciphers used in the TLS (1.0,1.1 and 1.2) protocol.

iii. Workaround:

Disable weak cipher suites and re-configure your domain server.

3. Key Takeaways

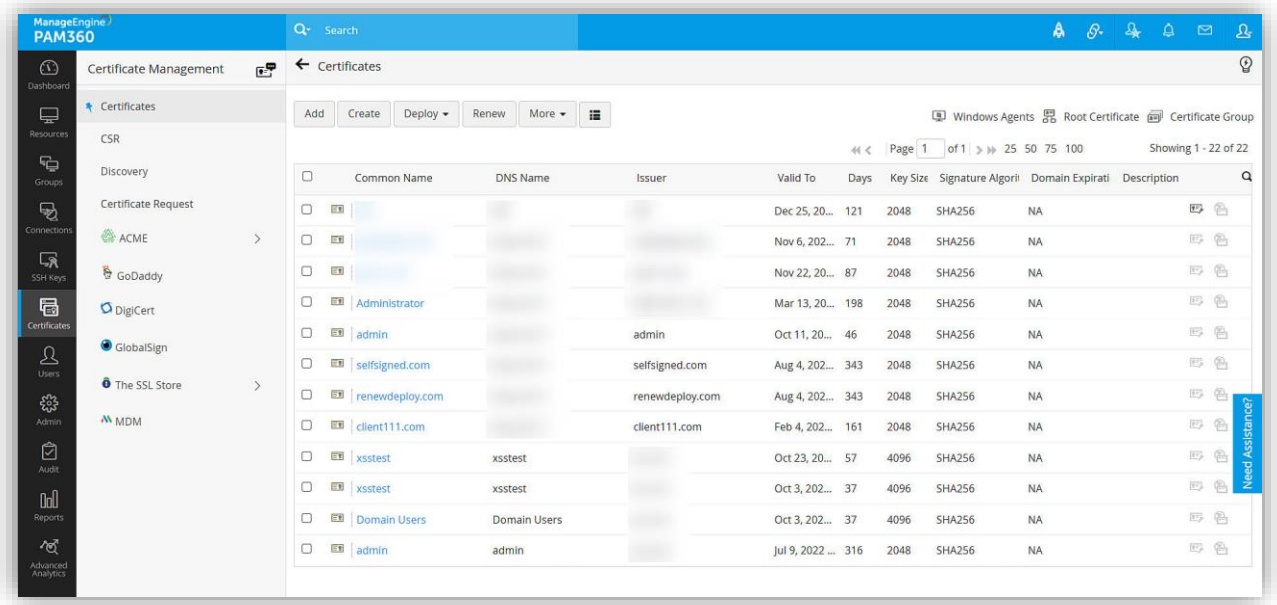
Here's a quick summary on how PAM360 scans your domain servers for vulnerability.

1. PAM360 initially scans the domain servers (to which the selected SSL certificate is deployed) and flags the weak ciphers.
2. Your domain server is scanned for HEARTBLEED and POODLE vulnerability, followed by CRL and OCSP revocation statuses.
3. When one or more of the above vulnerability checks renders a positive result, PAM360 flags the particular certificate as vulnerable.
4. Also, you can schedule automatic periodic vulnerability checks for your SSL certificates using PAM360 and opt an e-mail notification to the administrators as and when the tests are completed.
5. PAM360 provides dedicated, comprehensive, periodic reports on SSL vulnerability.

4. SSL Vulnerability Scan

To perform the SSL vulnerability check on your domain server, follow the below steps:

1. Navigate to **Certificates >> Certificates.**
2. Click on **Vulnerability** icon ( ) present to the left of the required certificate.
3. You will be redirected to a window which displays the certificates and the list of servers in which it is deployed.



4. Click **Scan**. If you want to perform the vulnerability scan on SANs also, enable Include SAN check box. If you want to perform this scan only for the servers in which the particular certificate is deployed (as discovered by PAM360), enable **Only deployed servers** check box.
5. PAM360 runs the scan and displays the results in a separate window. It comprises of the following details:

    i. IP address, Port corresponding to the domain server

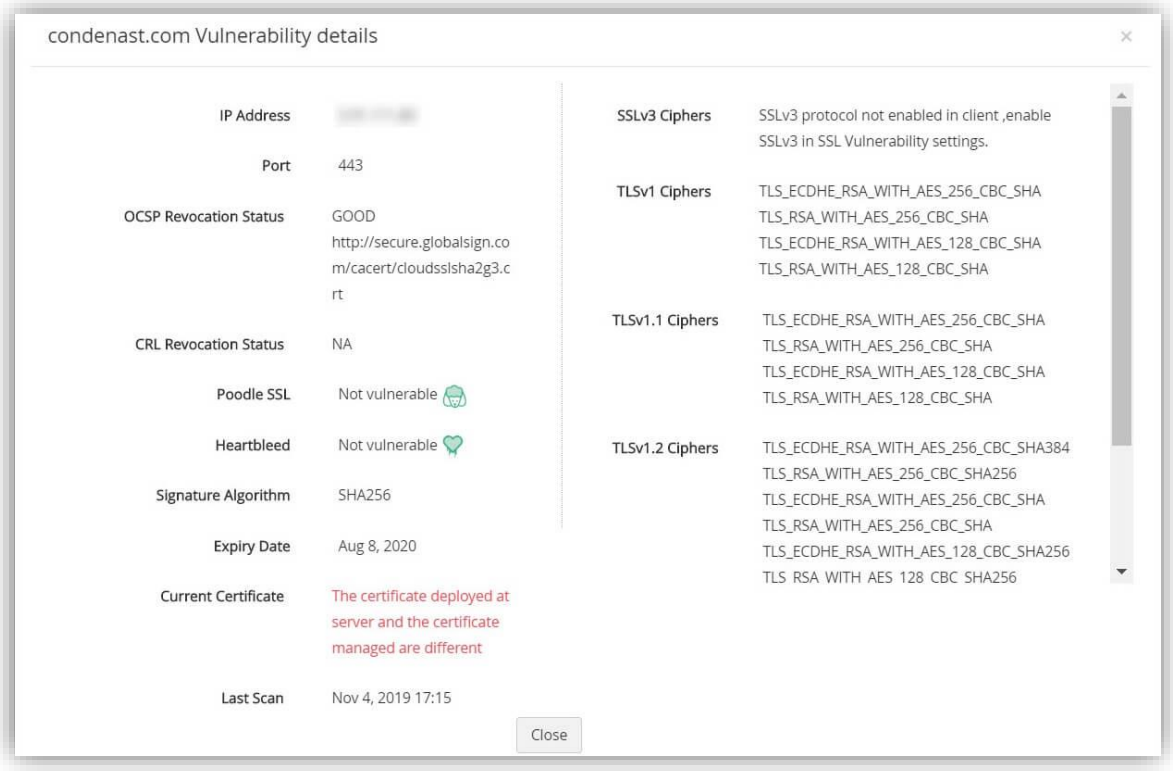
    ii. CRL, OCSP revocation statuses

    iii. POODLE SSL, HEARTBLEED vulnerability status

    iv. Information on whether the current version of the certificate (version of certificate being scanned) is deployed on domain servers

    v. List of insecure ciphers in SSL 3.0 and TLS (1.0, 1.1, 1.2) protocols in the domain server

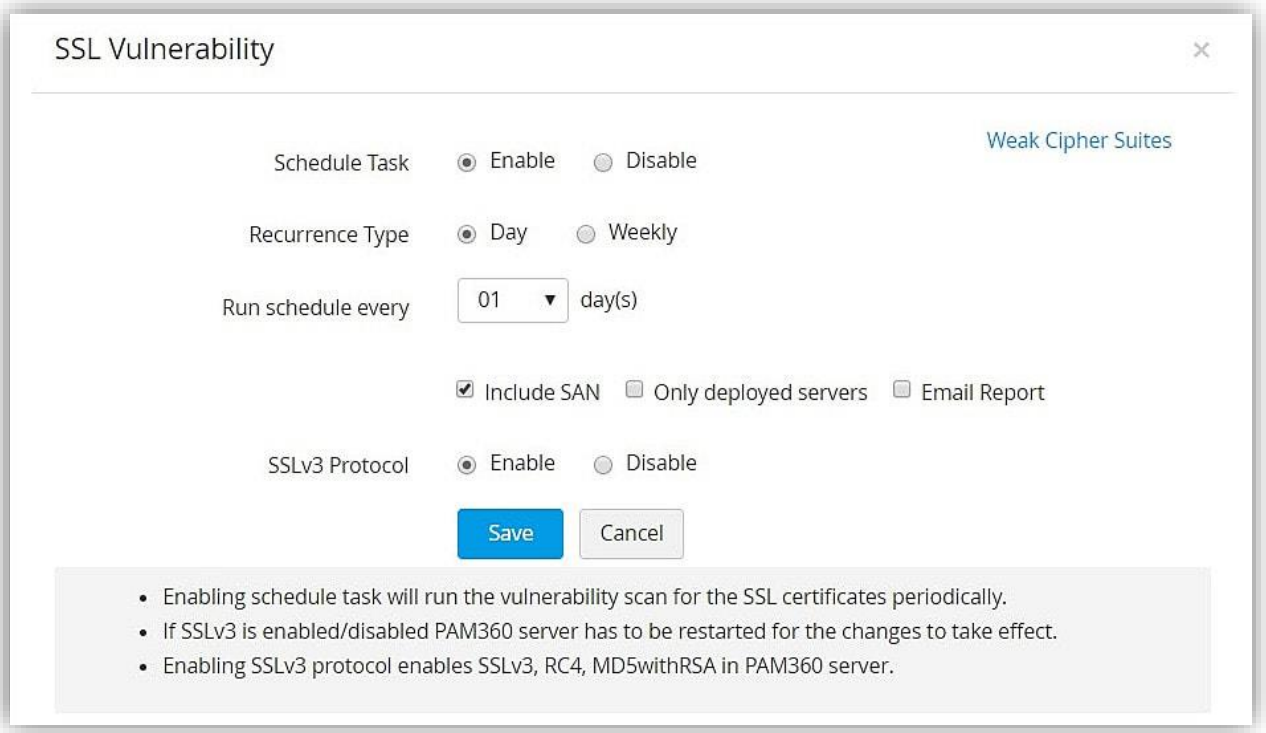
Note: By default, SSL 3.0 protocol is disabled in PAM360 server for security purposes. To scan SSL 3.0 protocol on your domain servers, you have to first enable SSL 3.0 protocol on PAM360 server and then restart the server.



6. Click **Export** to export the report in the form of PDF or e-mail to specific mail ids for better interpretation.

To schedule automatic vulnerability scan,

1. Navigate to **Admin >> SSH/SSL >> SSL Vulnerability**
2. Enable scheduled task by selecting the **Enable** radio button.
3. Choose the recurrence type and specify the time interval
4. You can opt to receive e-mail notifications to specific email ids after every scan by enabling the Enable Report check box
5. To enable scanning SSL 3.0 protocol in domain servers, enable the same in PAM360 server by choosing the enable option.
6. Click **Save**. The scheduled task is saved and vulnerability scan is carried out as per the scheduled time interval.



Notes:

- The above technique is used to perform vulnerability scan for all certificates in the PAM360 repository. To run the scan only for selected certificates, you can do so from the **Admin >> SSH/SSL >> Schedules tab**. Refer to the help section on schedules to learn how to schedule vulnerability scan for selected certificates.
- To view the data generated from the SSL vulnerability scans, go to the **Dashboard** tab >> **Keys Dashboard** >> **Vulnerabilites** widget.
- PAM360 generates instant, comprehensive reports on SSL Vulnerability for better interpretation, which can be accessed from Reports tab. To learn more, refer to the detailed help section on reports.

SSH and SSL Audit and Reports

1. Audits

   1.1 Viewing Audit Records

   1.2 Classified Audit Records

   1.3 Configuring SNMP traps and Syslog settings

   1.4 Key Audit Notifications

   1.5 Purging audit trails

2. SSH and SSL Reports

   2.1 Viewing Reports

   2.2 Exporting Reports

   2.3 Selecting Reporting Period

   2.4 Creating Scheduled Tasks

1. Audits

PAM360 comes with an efficient auditing mechanism, which records all activities performed in the product. The audit trails capture information on 'who' performed 'what' operation and 'when'. While the Password users in PAM360 can only view the audit records for their actions, the administrators can view the audit records pertaining to all users.

1.1 Viewing Audit Records

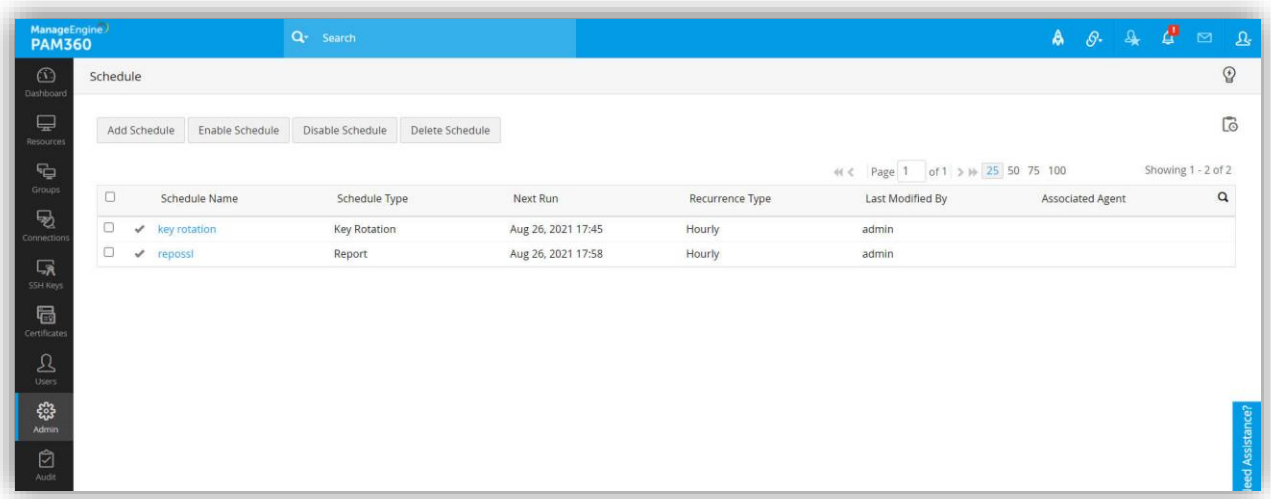
The last five entries in the audits can be viewed instantly from the **Operation Audit** of the Keys Dashboard page. You can view the full audit records by navigating to Audit >>**Keys/Certificate Audit.** You can apply filters and selectively view the required records. By clicking on the search icon in the right top corner of the audit table, you can invoke text boxes to search and selectively view required records. The Certificates related audits of all the users will be available under **Audit >> Certificate Audit.** The Certificate Audit is not user-specific, which means the audits related to the certificates can be viewed by the administrator(s). Whereas Keys Audit, which is available under **Audit >> Keys Audit** contains both the Certificates and SSH Keys related audits is user-specific, which means only that particular user will have access to those audits.

Audit trails have been classified into the following categories:

- **Key Association Audit**
- **Key Rotation Audit**
- **Schedule Audit**

1.2 Classified Audit Records in Respective Pages

1. Navigate to **SSH Keys >> Key Rotation Audit** to view the records of all SSH key rotation operations executed from PAM360.
2. Navigate to **SSH Keys >> Key Association Audit** to view the record of all SSH key association operations executed using PAM360.
3. The **Schedules** tab contains audit trails related to various scheduled tasks created in PAM360, including scheduled key rotation and discovery, and report generation operation. To view, navigate to **Admin >> SSH/SSL Config >> Schedules** and click on the **Schedule Audit** icon in the top-right corner of the tab. You can even drill-down the task execution result.

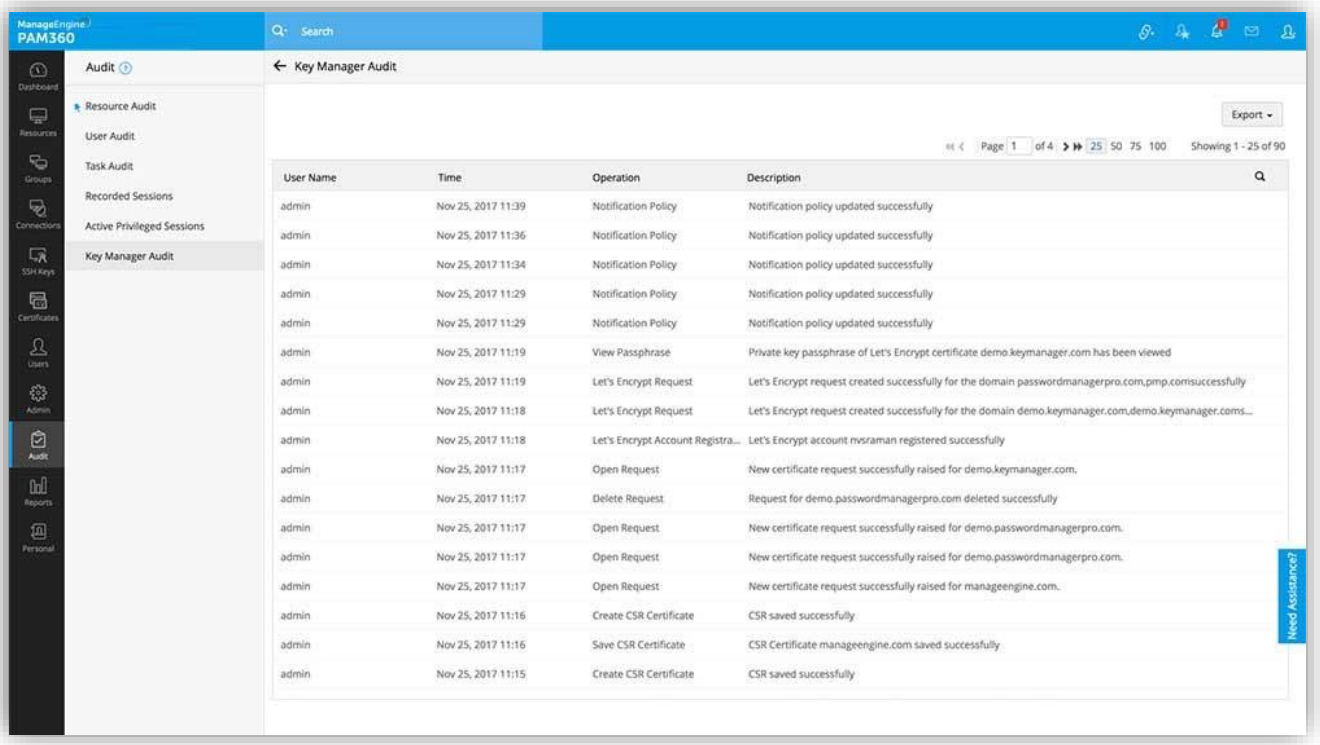


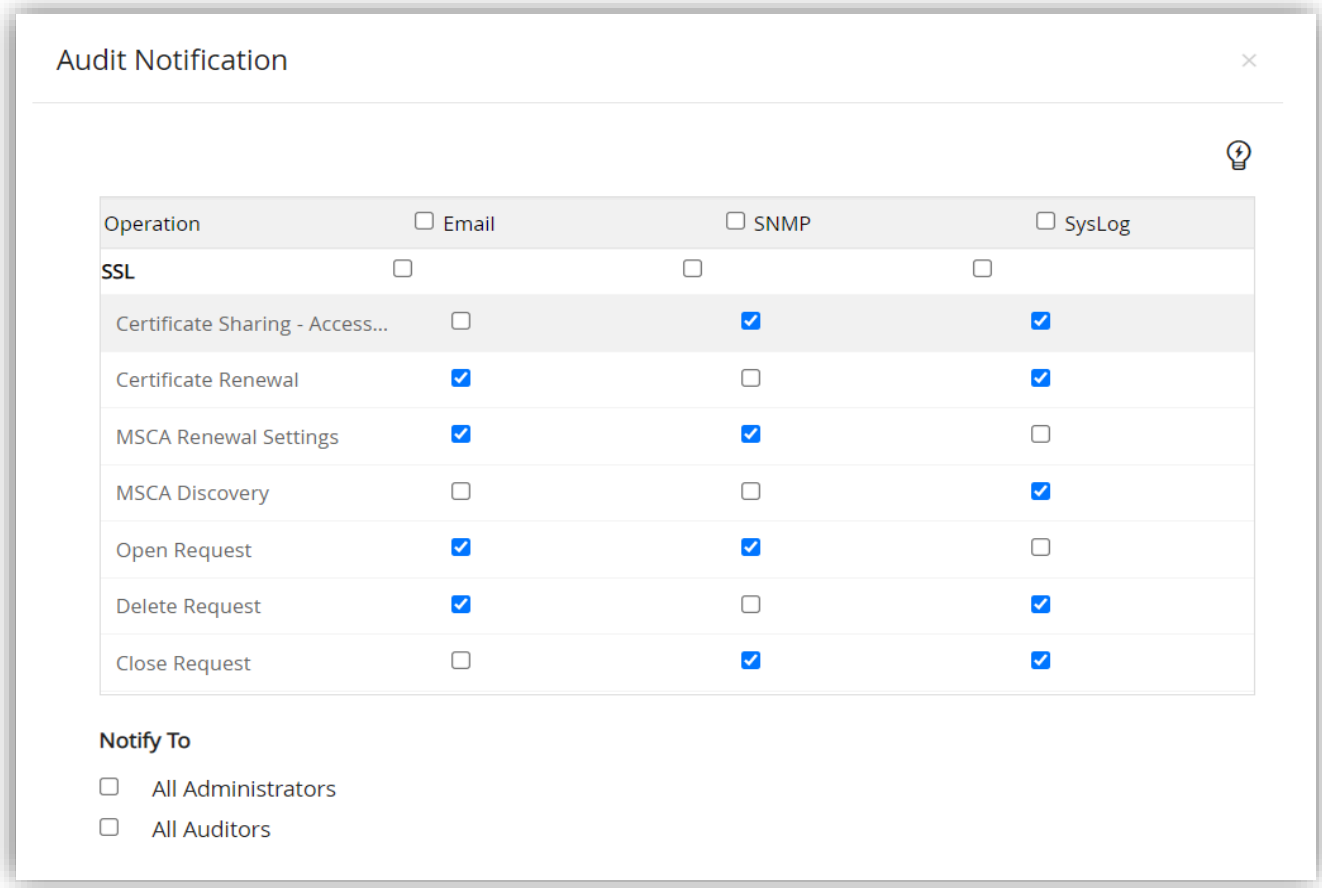
1.3 Configuring SNMP traps and Syslog settings

You can configure PAM360 to send SNMP traps and/or Syslog messages to other management systems, for the various operations that take place within PAM360. To configure, navigate to **Admin >> Integration >> SNMP Traps/Syslog Settings.** Here you need to provide basic information such as Hostname, Port to get the SNMP Traps or Syslog messages set up.

1.4 Key Audit Notifications

You can send notifications for key audit operations performed in PAM360 by navigating to **Audit >> Key Audit >> Audit Actions >> Configure Keys Audit.** Here, you will have the option to send the notifications as email, SNMP traps, or Syslog settings. You can choose which key-related operations you want to create an alert for and send the notifications to all administrators, all auditors or specific users and user groups.





1.5 Purging audit trails

By navigating to **Audit Actions >> Purge Audit trails** under **Keys Audit/Certificate Audit**, you can specify the number of days after which the audit records must be purged for various key-related operations such as operation, discovery, association, rotation, and schedule.

2. SSH and SSL Reports

PAM360 presents the information on the entire SSH key and SSL certificate management process in your enterprise in the form of comprehensive reports. The status and summaries of the different activities such as public key deployment, private key rotation, access to servers, list of all SSH users and their key association, list of SSL certificate, SSL validity, etc. are provided in the form of tables and graphs, which assist the IT administrators to make a well-informed decision on SSH key and SSL certificate management.

2.1 Viewing Reports

You can view the reports from the Reports tab in the GUI. PAM360 provides the following reports:

SSH Reports

1. **Private Key Report** – View a detailed report of the SSH keys generated or imported via PAM360.
2. **Private Key Rotation Report** – View a detailed report of the SSH key rotations executed using PAM360.
3. **Public Key Deployment Report** – View a detailed report of SSH keys that are deployed in the target systems.
4. **PGP Keys Report –** View a detailed report of all the PGP keys stored and managed in PAM360.

SSL Reports

1. **SSL Certificate Report** – View a detailed list of all SSL certificates imported, discovered, and created using PAM360.
2. **SSL Request Report** – View a detailed report on all the certificate requests raised from PAM360.
3. **SSL Expiry Report** – You can directly apply an expiry filter when selecting this report. A detailed report of the certificates with expiry information relevant to your selection, are displayed.
4. **Wildcard SSL Certificates Report** - This report provides a detailed view of the wildcard SSL certificates in use and also the servers in which the certificates are deployed.
5. **Deployed Servers Report** – This report provides a detailed view of those certificates that are deployed in more than one server.
6. **AD User Certificates Report** – View a detailed list of all the certificates mapped to user accounts in Active Directory.
7. **SHA1 Certificates Report** – This report provides a detailed view of all the SHA-1 certificates deployed in the organization.
8. **Deployment Report** – This report provides information on the certificates deployed through PAM360.
9. **Let's Encrypt Report** – Details on the status of certificate requests submitted to Let's Encrypt CA.
10. **Let's Encrypt Certificates Report** – This report is a subset of SSL certificate report, that provides a detailed view of certificates procured from Let's Encrypt CA.
11. **SSL Vulnerability Report** – This report provides detailed information on vulnerability scan performed on SSL certificates stored in PAM360 repository.

12. **Microsoft Certificate Authority Auto Renewal Report** - This report provides details on attempted / successful auto-renewals of certificates issued by Local certificate authority, invoked from PAM360.
13. **Certificate Sign Report** - This report provides a detailed list of certificates that are signed—either using Microsoft Certificate Authority or based on a root certificate—from Key Manager Plus.
14. **GlobalSign Orders Report** – This report is a subset of SSL certificate report; it provides a detailed view of certificate orders requested from GlobalSign CA. Use the Date Filter to view orders within a particular time period. The contents of this report can be exported in the PDF, CSV formats or sent as an Email to the specified recipients.
15. **Certificate Renewal Report** – This report provides details on attempted/successful auto-renewals of certificates issued by Local CA, certificates issued/renewed from third-party CA, Certificates issued by MSCA using agent and self-signed certificate renewal, invoked from PAM360.
16. **Buypass Go SSL Certificates Report** – This report provides details on the status of the certificate requests submitted to Buypass Go SSL CA. It displays vital details such as the Common Name, DNS Name, Issuer, Validity, and Creation time. Use the Date Filter to view orders submitted within a specific time period. You can export this report in PDF & CSV formats, or send via email to the specified recipients.
17. **ZeroSSL Certificates Report** – This report provides details on the status of the certificate requests submitted to the ZeroSSL CA. The attributes displayed in the report includes: Common Name, DNS Name, Issuer, Validity, and Creation time. Use the Date Filter to view orders submitted within a specific time period. You can export this report in PDF & CSV formats, or send via email to the specified recipients.
18. **MDM Certificates Report** – This report provides detailed information on the MDM certificates managed via PAM360. This report includes details such as: Common Name, Device Name, Issuer, Date of Expiry, Signature Algorithm, and Serial Number. Use the Show dropdown to filter the report view based on the OS type. Use the Date Filter to view certificates imported within a specific time period. You can export this report in PDF & CSV formats, or send via Email to the specified recipients.
19. **Certificates Sync Status Report** – This report provides a detailed view of the sync status of SSL certificates that are deployed to multiple servers through PAM360.
20. **Azure Certificate Report** – This report provides detailed information on the certificates from the Azure portal that is managed via PAM360. This report contains details such as Certificate Name, Domain Name, Key Vault, Issuer, Expiry Date, Created

Time, Valid From, and Lifetime Action. Use the Date Filter to view certificates imported within a specific time period. You can export this report in PDF & CSV formats or send it via Email to the specified recipients.

21. **Load Balancer Certificate Report** – This report provides you with the list of certificates deployed to the load balancer with the relevant information such as Common Name, Server Name, Credential Name, Load Balancer Type, Services, Virtual Servers, and Last Synced. You can export this report in different formats available in the Export drop-down at the top.
22. **Azure Certificates Request Report** - This report provides details on the status of the certificate requests submitted to Azure Key Vault. It displays important information such as Certificate Name, Domain Name, Key Vault, Issuer, Expiry Date, Created Time, Valid From, Last Updated, and Lifetime Action.
23. **AWS Certificate Request Report** – This report provides details on the status of the certificate requests submitted to AWS-ACM. You can export this report in the available types with important information such as Domain Name, SAN, ARN, Ordered Time, ACM, Region, and Renewed On.
24. **AWS Certificate Report** – This report provides detailed information on the certificates obtained from the AWS-ACM and managed via PAM360. Select the required report criteria from the Column Chooser before exporting the report in the desired format.
25. **MSCA Certificates Report** – This report provides the entire list of SSL certificates provided by the Microsoft Certificate Authority and managed via PAM360. It displays important information such as Common Name, DNS Name, Issuer, Valid To, Key Size, Description, etc. Use the Column Chooser to display the required information and to export the report in the available formats.
26. **MSCA Revoke and Delete Report** – This report list the certificates revoked and deleted by the MSCA. It displays information such as Common Name, Certificate Authority, Certificate Template, pki.msca.revokedBy, pki.msca.revokeReason, pki.msca.deletedOn, pki.msca.deleteStatus, etc. You can select the required criteria from the Column Chooser at the top pane before exporting the report in the desired type.
27. **Sectigo Certificate Report** – This report provides the SSL certificates list imported from SCM or created by SCM and managed via PAM360. You can export this report in PDF & CSV formats or send it via Email to the specified recipients.

2.2 Exporting Reports

You can export the reports generated in PAM360 as a CSV or PDF and also email the reports.

To export a report:

1. Select any report from those enumerated in the Reports tab in the GUI.
2. Click the Export button in the top-right corner of the window.
3. Select any of the options from the drop-down list.
    - **PDF** – Export the report as a PDF file to the system.
    - **CSV** – Export the report as a CSV file to the system.
    - **Email** – Export the report via mail. Specify the email addresses of the users you wish to provide the reports.

2.3 Selecting Reporting Period

You can apply date filters and generate reports for a specified time period alone. To filter the reports by date:

1. Select any report (except SSH users report) from those enumerated in the Reports tab in the GUI.
2. Click the Date filter in the top-right corner of the window.
3. Specify the from and to date of the time period within which you wish to view reports.
4. Click **Save.**

> **Note:** Use the Export feature with the Date Filter applied to export the data only reported within the time period specified.

2.4 Creating Scheduled Tasks for Automatic Report Generation

You can create scheduled tasks for generating reports automatically. The reports will also be emailed to you or to any number of recipients as required.

To schedule report generation:

1. Navigate to **Admin >> SSH/SSL Config >> Schedules.**

2. Click the **Add Schedule** button.
3. In the Add Schedule window, enter a name for the schedule and select the type of schedule as **Report.**
4. Select the report type. All the reports selected here will be sent via email.
5. Specify the periodicity for report generation **- hourly, daily, weekly, monthly** or **once only.** Specify when you want to start the report generation operation. Set the starting time, date, or day corresponding to the option chosen.
6. Enter the email addresses of the users you wish to provide the report.
7. Click **Save.**

You will get a message confirming addition of a new schedule.

SSH/SSL Admin Settings

PAM360 allows you to enable notifications for various operations such as SSL key expiry, failed SSH key rotation, certificate management, PGP key expiry, etc. In addition, PAM360 allows you to retain or overwrite existing keys. Here in this document you will learn about the following topics:

1. **Managing Notifications**
2. **SSH Policy Configuration**

1. Managing Notifications

You can set up to get notified via email, syslog messages in any of the following cases:

1. If SSL certificates are expiring within a specified number of days.
2. If domain names are about to expire within a specified number of days.
3. If SSH keys are not rotated for more than a specified number of days.
4. For certificate management operations performed from within the application.
5. If PGP keys are expiring within a specified number of days. To learn more about PGP keys, click here.

> **Note:** Notifications regarding PGP key expiration will be sent via email only.

To configure notifications:

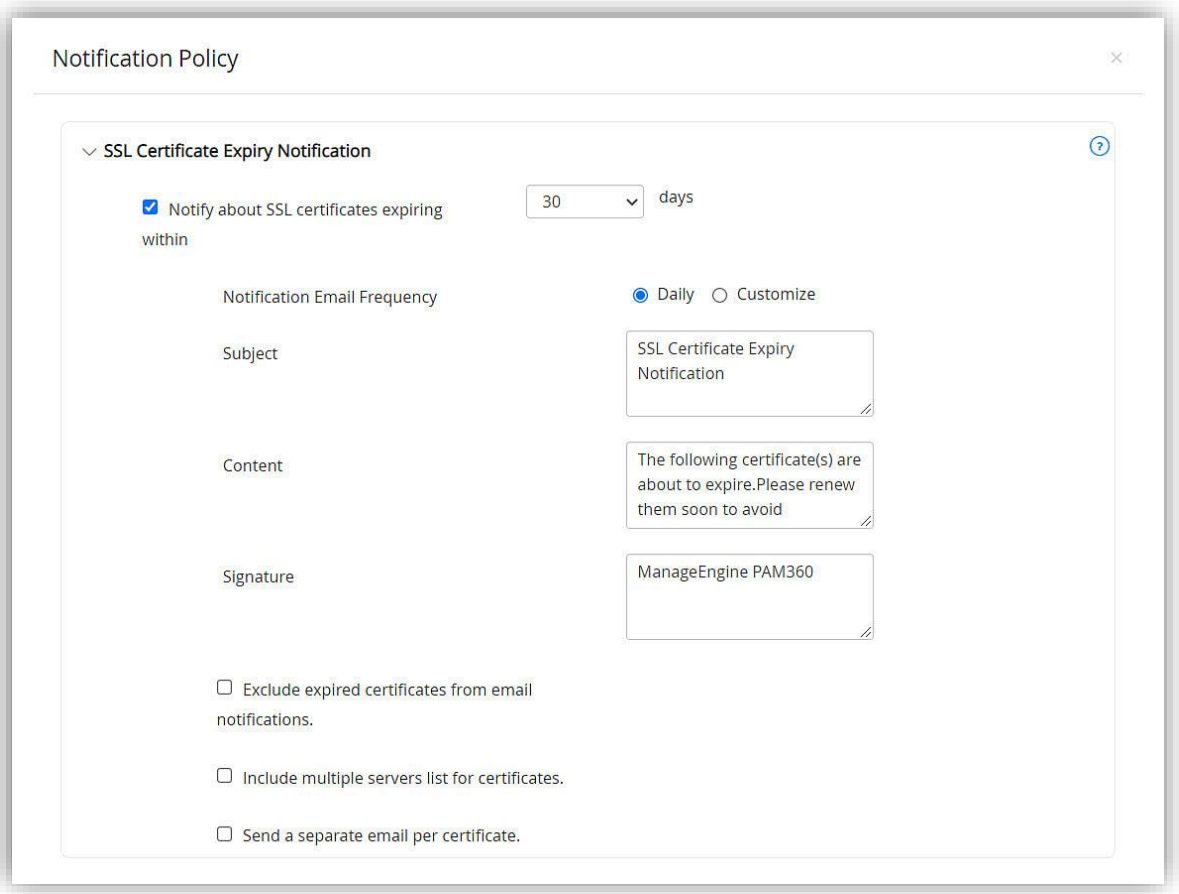
1. Navigate to the **Admin >> SSH/SSL Config >> Notification Settings**.
2. To enable SSL certificate expiry notifications, select the **Notify about SSL certificates expiring within** checkbox. Choose a value for days. You will get notified about only those certificates whose expiry dates fall within the period (number of days) you enter.
3. **Notification Email Frequency:** Choose to receive notifications either **Daily** or **Customize** your notifications.
    i. If you choose to **Customize**, set the **Interval** (in days) to notify about the to-be-expired certificates.
    ii. Select the **Email certificates on every schedule if expiry is less than** option if you

want to receive notifications on all schedules irrespective of the above-set interval.

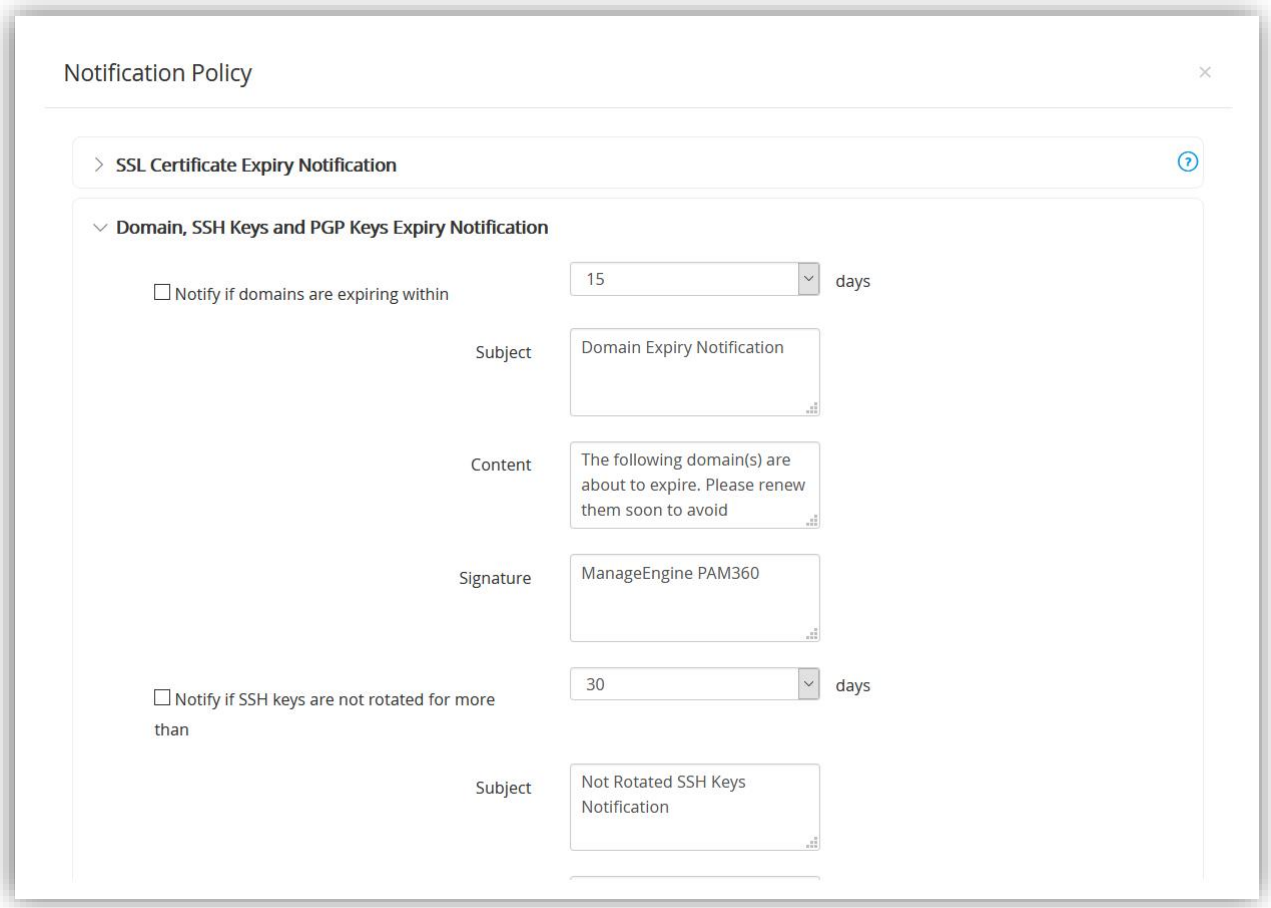
iii. Select **Exclude expired certificates from email notifications** to not get notified about expired certificates.

iv. Select **Include multiple servers list for certificates** to get the details about the list of servers where the certificates are placed/deployed.

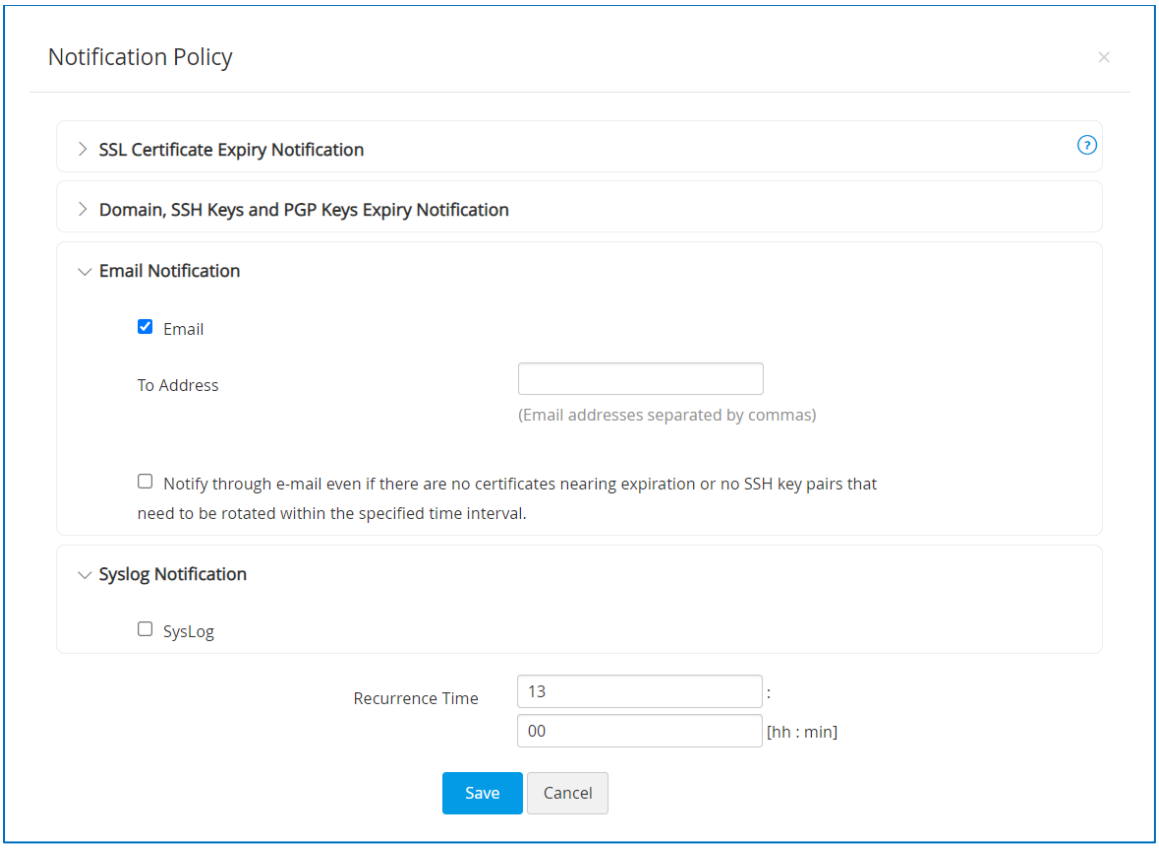
v. Select **Send a separate email per certificate** if you want to customize each email. You can mention the **Subject** and/or **Select the attributes to add in the subject** of the expiry notification.



4. You can also choose to get notifications regarding domain name expiration, PGP key expiration or SSH key rotation failure for the configured time period or both by selecting the respective check-boxes. Expiring SSL certificates, and the SSH keys that were not rotated within the specified days are notified during the mentioned **Recurrence Time.**



5. You are also allowed to edit the **Subject, Content and Signature** of your email-notifications.
6. You can choose to be notified in two ways:
    i. **E-mail** – Enter the **To Addresses.** If you have not configured your mail-server settings, do it from the Mail Server Settings tab.



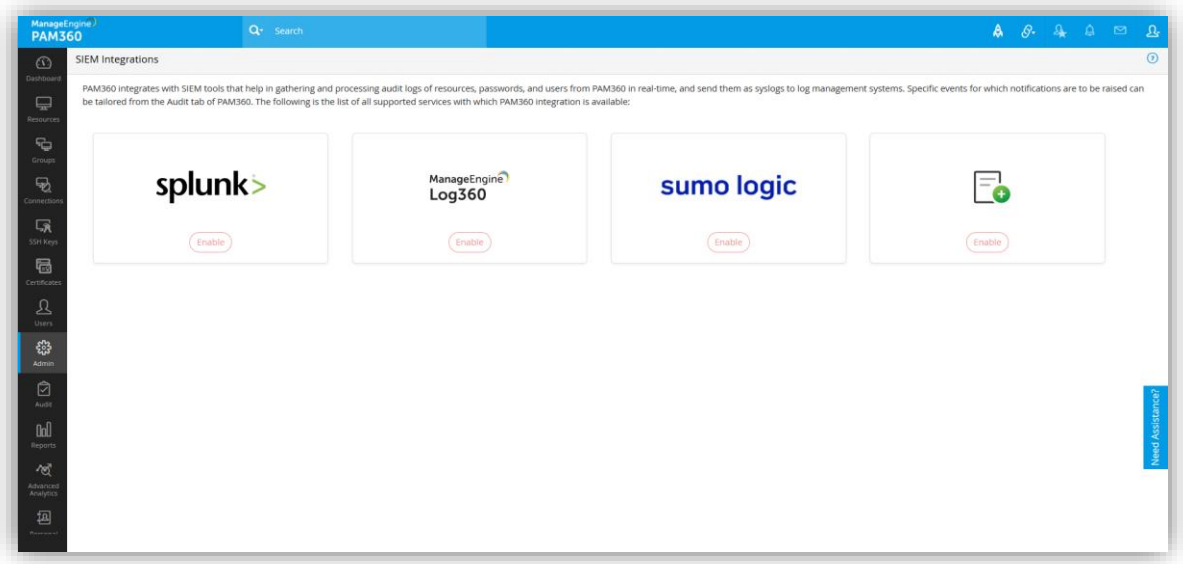
ii. **Syslog** – Navigate to **Admin >> Integration >> SIEM Integration** and select the required integration to mention the IP address of the server and the port to which the syslog is to be delivered. To learn more about SIEM integration, click here. Refer to the Syslog format given below:

a. **SSH**

<190> Key_Name:172.21.147.130_test123_id Days_Exceeded:0 Modified_On:2016-02-16 17:41:24.008

b. **SSL**

<190> Parent_Domain: manageengine.com Included_Domain: pam360.com Days_to_Expire: 100 Expire_Date: 5.08.2017



7. After filling in the details, click **Save.**

> **Note:** The number of days specified in the SSH key rotation and SSL certificate expiry notification policy will be applied to the dashboard settings also.

2. SSH Policy Configuration

PAM360 allows you to create a high level policy on SSH keys management. when PAM360 creates new keys, you can specify whether to retain (ie. to be appended to the existing ones) or overwrite the existing keys. Overwriting will remove the existing keys and allows you to have a fresh start. Your SSH environment will have only the keys that were generated by the PAM360. PAM360 carries out these changes in the authorized_keys file directly.

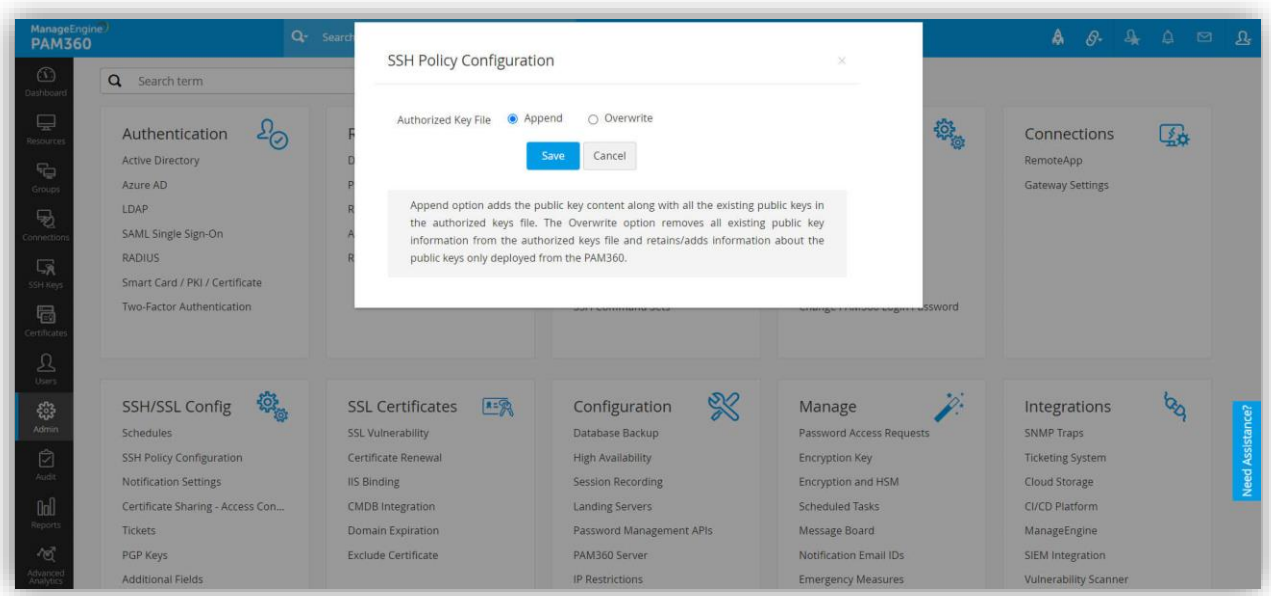
From the SSH Policy, you can set the option for adding keys to the authorized_keys file. You can choose from:

1. **Append** – Allows you to retain existing keys as well the new ones deployed by PAM360.
2. **Overwrite** – Removes all existing public key information from the authorized keys file and retains the public keys deployed from PAM360 only. This is what we call as clean start.

To change the policy configuration:

1. Navigate to the **Admin >> SSH/SSL Config >> SSH Policy Configuration.**
2. Select to either **Append** or **Overwrite** the keys.

3. Click **Save.**



You will get a confirmation that the SSH policy settings have been updated.

Manage SSH/SSL Schedules

A schedule is a basic time-management tool that consists of list of activities that are intended to take place at a certain time or as a sequence of event. You can create scheduled tasks to automatically carry out operations such as SSH resources and SSL certificates discovery, key rotation, and report generation at periodic intervals.

1. **Add Schedules**
2. **Edit Schedules**
3. **Enable/Disable Schedules**
4. **Delete Schedules**

1. Add Schedules

1. Navigate to the **Admin >> SSH/SSL Config >> Schedule.**
2. Click the **Add Schedule** button.
3. Select the type of schedule. You have six options:

i. Key Rotation

Schedule the rotation of SSH keys assigned to user accounts.

1. Select the keys that are to be scheduled for rotation. If keys are not assigned but are scheduled to rotate, schedule rotation will fail and an error message will be displayed in the **Audit** tab in the GUI.
2. Automatically push the key files (private key, public key or both the private and public keys) onto its associated users by enabling the '**Push private key file to remote user account**' and/or '**Push public key file to remote user account**' option, instead of pushing the key files manually after every scheduled rotation.
3. Here, you can also select to **Use keyname as filename.**

ii. SSL Discovery

Schedule the discovery of SSL certificates using this option. Specify the start and end IP addresses and the ports to be checked for deployed SSL certificates.

1. Select **Discover by IP Address Range** to specify the **StartIP** and **End IP** addresses.
2. Select **Subnet** to mention the **IP Address** and the **ports** to be checked for deployed SSL certificates. You can also select **From file** to upload a schedule.
3. Select the **Bypass Proxy Settings** checkbox to bypass proxy server settings during the discovery operation. This option is applicable for the **IP Address Range**, **Subnet** and **From File** modes only.
4. If you select **Load Balancer**, enter the **Server Name, Port, User Name, Credential Type, Password** and **Path.** Choose the required load balancer from the **Type** drop-down: **General, BIG-IP F5,** or **Citrix.** To perform Citrix discovery using the Citrix REST API commands, select the checkbox **Use REST API (By default PAM360 uses CLI commands for discovery and fetching certificates).**
5. Choose the **Shared Path - Windows** option to schedule a discovery operation for a specific directory path.
6. Select the **Agent** checkbox to schedule an SSL discovery through the PAM360 agent. You can perform two modes of discovery through the agent: **IP Address Range** and **Shared Path - Windows.**

iii. AD User Certificate Discovery

Schedule the discovery of SSL certificates from active directory—the certificates belonging to various users in Active Directory could be fetched into PAM360 using this option.

1. Select the **Domain Name** or click **New Domain** to add a **New Domain Name.**
2. Mention the **Primary** and **Secondary Domain Controller.**
3. Select the **Connection Mode (No SSL / SSL)** and enter the user credentials.
4. Click **Fetch Groups & OUs** and select the required user accounts / OUs in which certificate discovery has to be performed.

iv. MS Certificate Store Discovery

Schedule the discovery of SSL certificates from Microsoft Certificate Store and certificates issued by Microsoft Certificate Authority using this option.

1. Enable **Agent** to select the required agent from the list of available agents and mention the **Time out** in seconds or specify the **Server Credentials.**

2. Enter the user credentials or select the checkbox to **Use PAM360 service account credentials for authentication.**
3. For certificates issued by Microsoft Certificate Authority, you can fine tune your discovery based on certificate issue date, certificate revocation / expiration statuses, and certificate templates.

v. AWS Discovery

1. Choose the appropriate **AWS Credentials** from the dropdown. To add new credentials, navigate to the **Certificates >> AWS >> Manage**.
2. Choose the required AWS Service from which certificates need to be imported: **ACM or IAM**.
3. To import certificates from ACM, select **ACM** under AWS service and choose the service Region. To import certificates from **IAM**, specify the required AWS User Name(s) or use the **List AWSUserNames** option to retrieve the usernames. Choose the required usernames.

vi. SSL Vulnerability

Schedule periodic vulnerability scan on selected or all SSL certificates in PAM360 repository. Select the certificates on which the vulnerability scan is to be performed at regular intervals of time, and specify an e-mail id to which notification is to be sent after every scan.

vii. SSL Expiry

Schedule expiry alert notifications for SSL certificates.

1. Select the **Specific Certificates** or **Certificate Groups** that are to be tracked for expiry.
2. Schedule the scan at required intervals of time and specify the number of days to expiry before which the email notification should be sent.
3. Select the following options to tailor the scan results that are sent in email. The following preferences are saved only for email and will not change how scheduled scan results appear in the **Audit:**

i. Choose to receive notifications either **On Every Scedule** or **Customize** your notifications.

ii. If you choose to **Customize**, set the Interval (in days) to notify about the to-be-expired certificates.

iii. Enable the **Email certificates on every schedule if expiry is less than** option if you want to receive notifications on all schedules irrespective of the above-set interval.

iv. **Include auto-renewal certificates in email notification -** Certificates that will be auto renewed will be included in the email notifications.

v. **Exclude expired certificates from email notifications** - Certificates that are already expired in the repository will be excluded from the email notifications.

vi. **Send a separate email per certificate** - Every expired certificate will be sent as a separate email.

viii. Reports

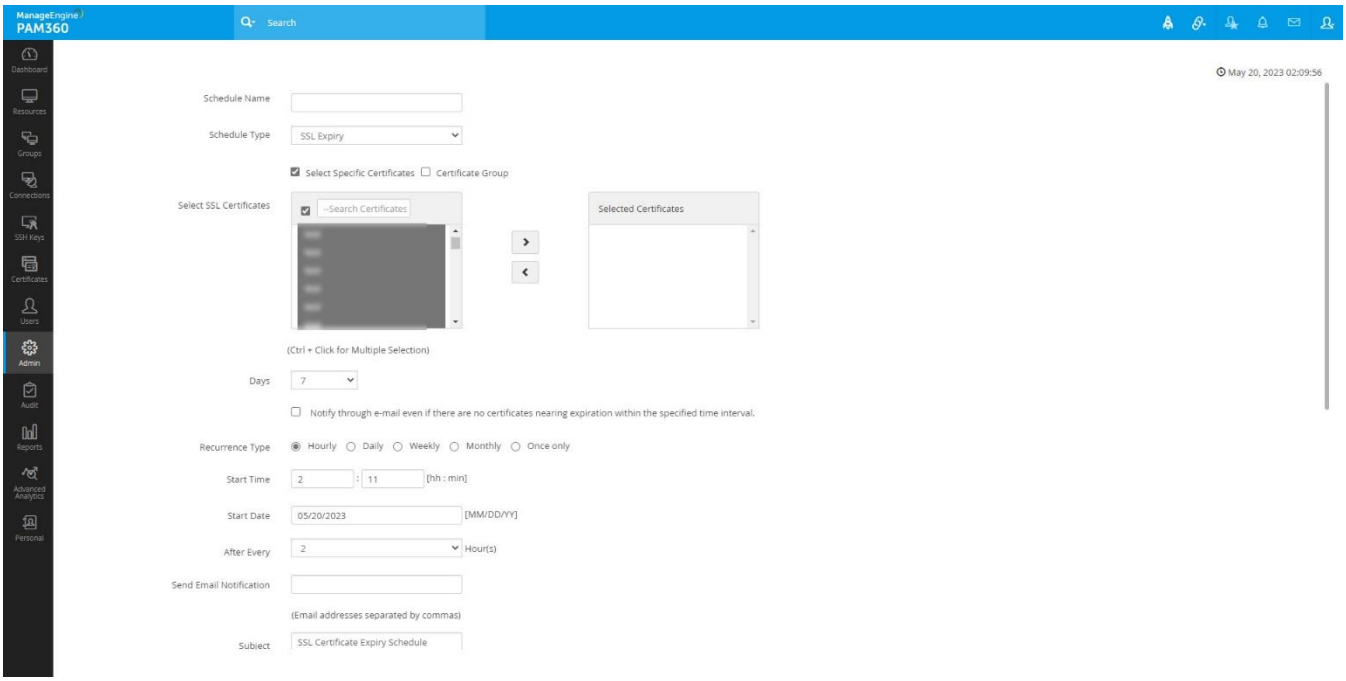
Schedule the reports to be generated and sent to the email address specified. All the reports generated by PAM360 can be scheduled to be sent to email addresses using this option. You can **Select Specific Certificates** or **Certificate groups** and move the required certificates to the **Selected Certificates** column using the arrow keys to generate reports for selected certificates under **SSL Certificate Report** type.

Scheduling Options

1. Select the recurrence type as - **hourly, daily, weekly, monthly**, or **once only**. Set the **starting time**, **date**, or **day**, corresponding to the option chosen.
2. Enter the email addresses of the users to be notified. The server authentication settings can be specified in the **Settings >> Mail Server Settings** tab in the GUI.
3. Customize the notification emails by adding an email subject of your choice. To tailor the body of the email further, add custom email content, and a unique signature.

Click **Save**. Now, you have successfully added a new schedule.

To execute a schedule, go to the **Schedule** window and click the **execute schedule icon** beside the respective schedule name.



Note: The result of the schedule execution will get updated in the Schedule audit and also in the respective operation audits.

2. Edit Schedules

1. Navigate to **Admin >> SSH/SSL >> Schedule.**
2. Click the name of the schedule you would like to edit.
3. You will be redirected to the Edit Schedule window. You can edit all the details of the schedule except its name and type.
4. Click the **Update** button to save any modifications.

3. Enable/Disable Schedules

The schedules can be enabled or disabled anytime. Use the disable option to stop the execution of a schedule temporarily without deleting it. When re-enabled, the schedule again starts its periodic execution.

1. Navigate to **Admin >> SSH/SSL >> Schedule.**
2. Select the schedules and click the **Enable Schedule** or **Disable Schedule** button. You will get a confirmation that the schedule has been enabled or disabled successfully.

Note: The schedules set to run only once cannot be enabled if they have already been executed. Modify the schedule to enable it.

4. Delete Schedules

1. Navigate to **Admin >> SSH/SSL >> Schedule.**
2. Select the schedules to be deleted.
3. Click the **Delete Schedule** button.
4. Click **Ok** in the confirmation pop-up window.

You will get confirmation that the schedules have been deleted successfully.

Ticketing System Integration for SSL Certificates

PAM360 integrates with enterprise ticketing systems to automatically create service requests for vulnerable or expiring SSL certificates. The integration ensures that periodic tickets are created in the ticketing system to alert the technicians and take timely action to reduce the security threats posed by expiring or vulnerable SSL certificates. The frequency of service request creation for expiring and vulnerable tickets will be governed by the notification policies set for the same by the user.

1. How does the Ticketing System Integration for SSL Certificates work?
    1.1 SSL Expiry
    1.2 SSL Vulnerability
2. Steps to integrate ticketing systems with PAM360
    2.1 ServiceDesk Plus
    2.2 ServiceNow

1. How does the Ticketing System Integration for SSL Certificates Work?

PAM360 allows you to set up periodic notifications, in the form of emails or syslog messages, to check for expiring or vulnerable SSL certificates in the repository.

To enable the ticketing system for SSL certificates, enter the server URL of the machine where the ticketing system is running in PAM360 and ensure that the ticketing system host is accessible by the PAM360 server.

Once ticketing system for SSL certificates is enabled, PAM360 will create tickets in the ticketing environment automatically, whenever the notifications for expiring/vulnerable SSL certificates are triggered during a scheduled or a manual vulnerability check.

Prerequisite

Tickets are created in the ticketing environment based on the notification policy set for SSL certificates that are expiring and/or deemed as vulnerable in PAM360. Click here to learn more about how to set up notifications for the same.

1.1 SSL Expiry

The SSL expiry ticket is created as part of the default expiry notifications sent by PAM360, as well as the scheduled SSL expiry reports. The notifications are triggered whenever a scheduled expiry report or default expiry notification task is run in PAM360.

1. You can set up a schedule for notifications regarding expiring SSL tickets in **Admin >> SSH/SSL >> Notification Settings**. To enable SSL certificate expiry notifications, select the '**Notify about SSL certificates expiring within**' checkbox. Choose a value for days. You will be notified about only those certificates whose expiry dates fall within the period (number of days) you enter. Customize the frequency of the notifications as per requirement. Once the schedule is set, PAM360 will collate a list of expiring certificates falling under the specified number of days.
2. For each SSL certificate, PAM360 will check if an expiry ticket is already created in the ticketing environment. If not, a new ticket will be opened. The new ticket will contain details such as the Ticket Number, Status, IP Address, Certificate Serial Number for which the ticket is created locally.
3. If a ticket already exists, the status of the ticket will be checked. If the status of the ticket is Open, In Progress, or On Hold, PAM360 will not create a new ticket. However, if the status is Resolved, Canceled, or Closed, PAM360 will re-open the ticket until the corresponding SSL certificate in renewed and updated in the PAM360 repository.
4. Tickets created by PAM360 will be flagged as 'High Priority'.

1.2 SSL Vulnerability

The SSL vulnerability ticket is created as part of the default schedule for vulnerability scan done by PAM360, as well as manual scans. A ticket will be created for each vulnerability, detected during the vulnerability scan.

1. You can set up a schedule for vulnerability scans in **Admin >> SSH/SSL >> SSL Vulnerability.** Configure the recurrence type to set up the scan to run daily or weekly.
2. First, PAM360 will check if a vulnerability ticket already exists in the ticketing

environment using the certificate serial number, Domain Name, and IP Address. If a ticket is already created, the status of the ticket will be retrieved.

3. If the ticket status is Open, In Progress, or On Hold, PAM360 will simply add the latest scan results to the ticket. If the ticket status is Resolved, Canceled, or Closed, but vulnerabilities are still found in the scan results, then PAM360 will reopen the ticket and add the latest scan results to it.
4. If no ticket is corresponding to particular server vulnerability is available in the ticketing environment, PAM360 will create a new ticket.
5. In the ticketing system, a separate ticket is created for each domain - IP vulnerability combination. For example, consider a certificate with common name example.com and SAN namely test.example.com, used for two different IP addresses as follows:
    - example.com at IP location 192.168.0.23
    - test.example.com at IP location 192.168.205.35

    If vulnerabilities found at both locations, then two tickets will be created for example.com@192.168.0.23 and for test.example.com@192.168.205.35. Even though the certificate used is the same, since the servers' locations are different, they will be considered as two different vulnerabilities.
6. Tickets created by PAM360 will be flagged as **High Priority**.

> **Note:** The vulnerability tickets will only contain details of weak ciphers found during the scan i.e., the ticket will not list the health of other ciphers available in that particular server if they are not found to be vulnerable.

2. Steps to Integrate Ticketing Systems with PAM360

Listed below are the ticketing systems currently supported by PAM360:

1. ServiceDesk Plus (on-premise)
2. ServiceNow

2.1 ServiceDesk Plus

1. Navigate to **Admin>> SSH/SSL >> Tickets** and choose **Enable.**
2. Under Help Desks, click **ServiceDesk Plus.**
3. Enter the ServiceDesk Plus **Technician Key** (API Token) and **Server URL** where the

ServiceDesk Plus host is running.

4. Select the **Template Name**.

   [or]

   Click **Fetch Templates** to bring in all the available templates from ServiceDesk Plus. Now, select a template that contains default fields while ensuring that it does not have any mandatory custom fields, failing which will fail ticket creation.

5. Under **Create Tickets**, select **Create ticket for SSL certificate expiry** or **Create ticket for SSL vulnerabilities** or both, based on your requirement. Click **Save**.

2.1.1 Format for SSL Expiry tickets in ServiceDesk Plus

Subject: SSL Certificate <common name> expiry

Description:

The SSL Certificate <common name> expiring soon, please take care

Common Name: <common name>

Expiry Date: Feb 25, 2020

Scanned by: PAM360 running at https://<PAM server-url>:<port>

2.1.2 Format for SSL Vulnerability tickets in ServiceDesk Plus

Subject: Vulnerabilities for <domain name>

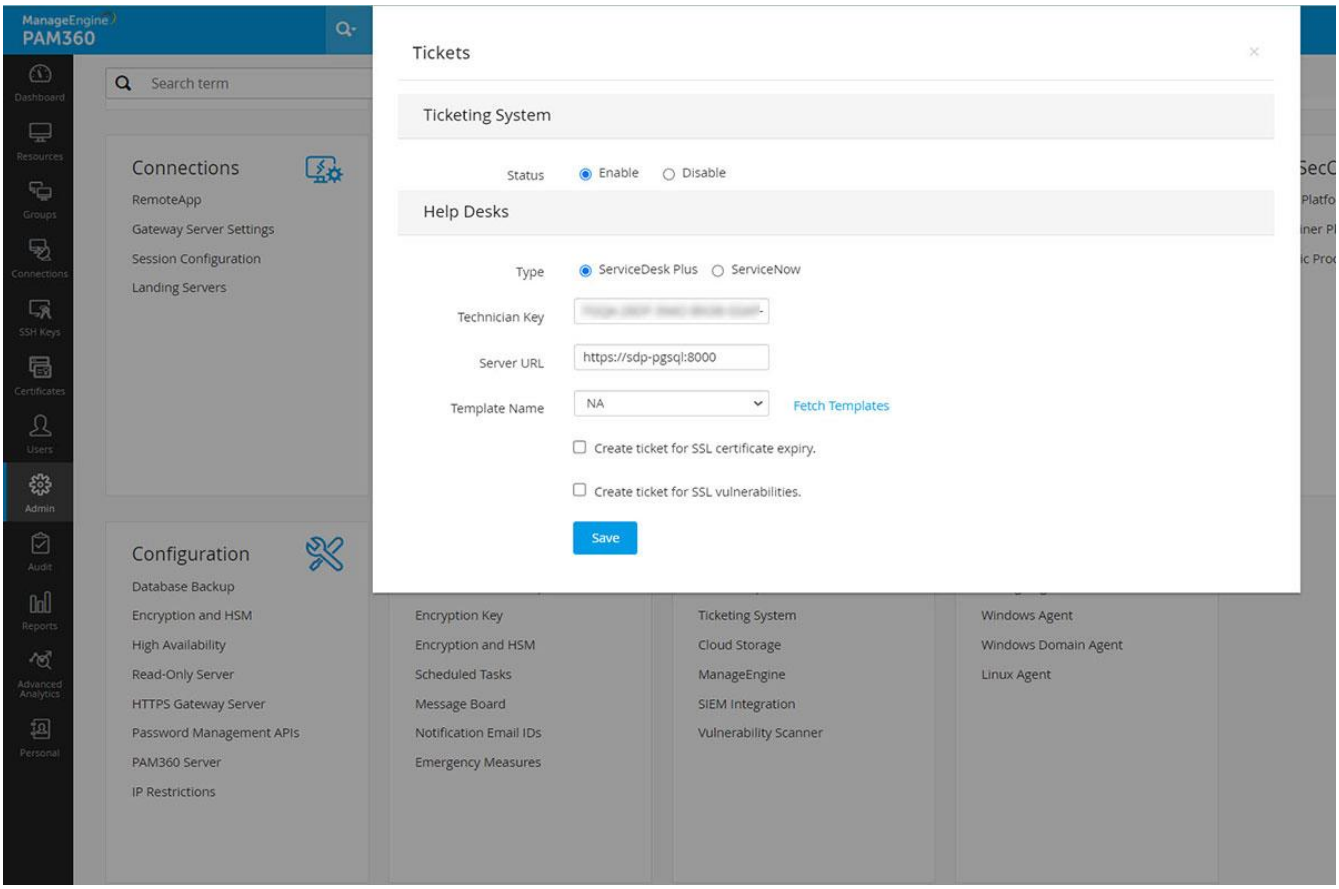
Description:

<Domain Name> (this could be the SAN)
<Common Name> (certificate common name)
<IP Address>
Weak ciphers in use, which should be removed
<Names of the ciphers found to be weak>

If any vulnerabilities such as **OCSP, CRL, HeartBleed**, or **Poodle** are found, then the corresponding Signature Algorithm and expiry date information will also be added here.

Scan Time:

Scanned by: PAM360 running at https://<PAM server-url>:<port>



2.2 ServiceNow

1. Navigate to **Admin>> SSH/SSL >> Tickets** and choose **Enable**
2. Under Help Desks, click **ServiceNow**
3. Enter the ServiceNow **User Name**, **Password**, **Server URL** where the ServiceNow host is running.
4. Click to **Fetch Columns** from ServiceNow. The fetched columns will be displayed under additional fields. Now, select the fetched columns from additional fields and associate it with an existing column in PAM360. This allows users to add additional information to the tickets created in ServiceNow.
5. Under **Create Tickets**, select **Create ticket for SSL certificate expiry** or **Create ticket for SSL vulnerabilities or both**, based on your requirement. Click **Save**.

2.2.1 Format for SSL Vulnerability tickets in ServiceNow

Short Description: SSL Certificate <common name> expiry

Additional Comments:

The SSL Certificate <common name> expiring soon, please take care

Common Name: <common name>

Expiry Date: Feb 25,2020

Scanned by: PAM360 running at https://<PAM server-url>:<port>

2.2.2 Format for SSL Vulnerability tickets in ServiceNow

Short Description: Vulnerabilities for <domain name>

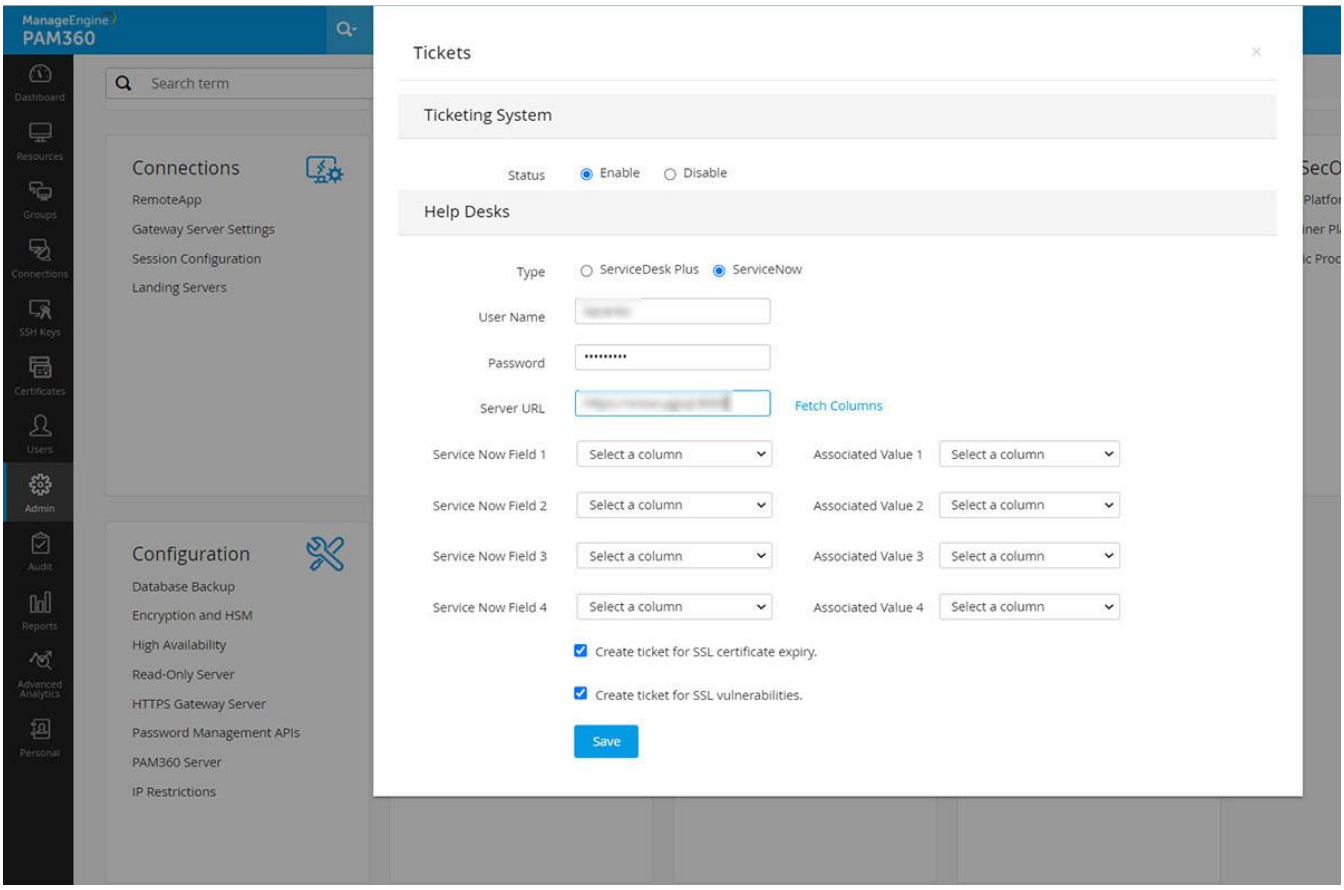
Additional Comments:

<Domain Name>(this could be the SAN)
<Common Name> (certificate common name)
<IP Address>
Weak ciphers in use, which should be removed
<Names of the ciphers found to be weak>

If any vulnerabilities such as **OCSP, CRL, HeartBleed,** or **Poodle** are found, then the corresponding Signature Algorithm and expiry date information will also be added here.

Scan Time:

Scanned by: PAM360 running at https://<PAM server-url>:<port>



Integration with Service Desk Plus' CMDB

PAM360 provides the option to integrate with ManageEngine Service Desk Plus's configuration management database (CMDB). This integration enables you to export SSL certificate details from PAM360's repository to Service Desk Plus's CMDB thereby allowing administrators to monitor the usage, expiry and other aspects of SSL certificates across the organization directly from Service Desk Plus interface.

At the end of this section, you will have learned the following:

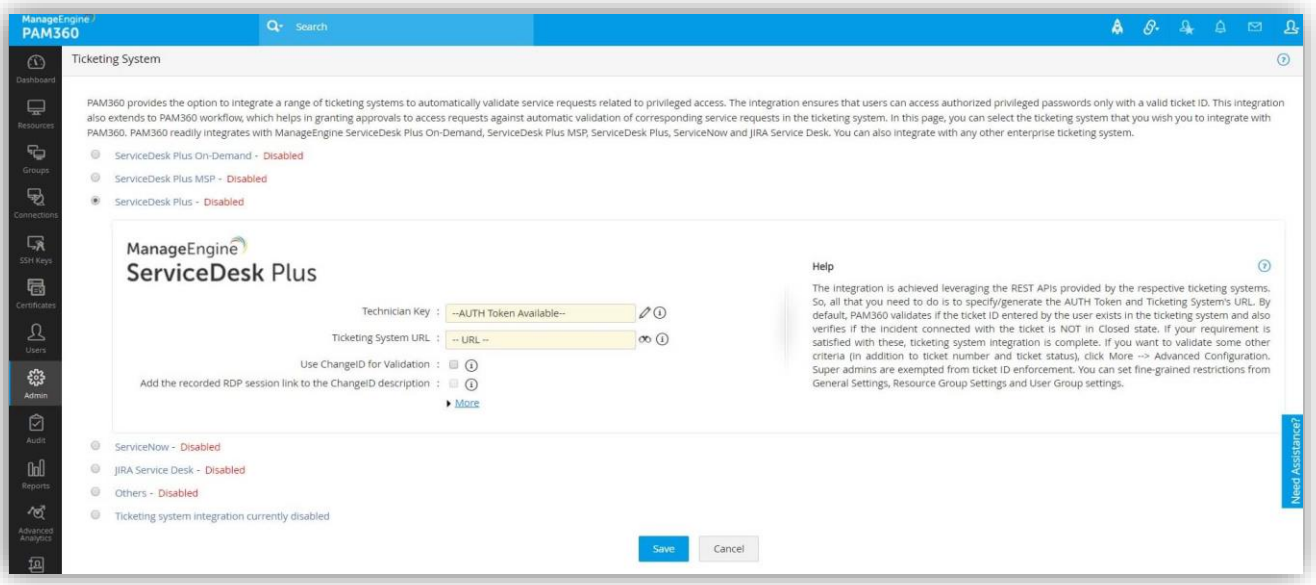
1. How does this Integration Work?
2. Creating CI type in SDP's CMDB
3. Enabling Certificate Sync
4. Deleting Certificates from CMDB

1. How does this Integration Work?

To export SSL certificates from PAM360 to Service Desk Plus's (SDP) CMDB, you have to first provide the server details where SDP instance is running and the user account details (technician key). Once the integration takes effect, a new parent CI type and a corresponding child CI type will be created in Service Desk Plus which will house all the certificates exported from PAM360's repository. You can also export SSL certificates from PAM360 into an already existing CI type in SDP by appropriately mapping the certificate attributes to that of the existing CI. Exporting certificates into CMDB renders visibility over SSL environment and allows administrators manage all IT assets from a single, central repository.

> **Prerequisite:** Before proceeding to set up CMDB integration, PAM360 requires the details of the server in which ServiceDesk Plus is running and the technician key.

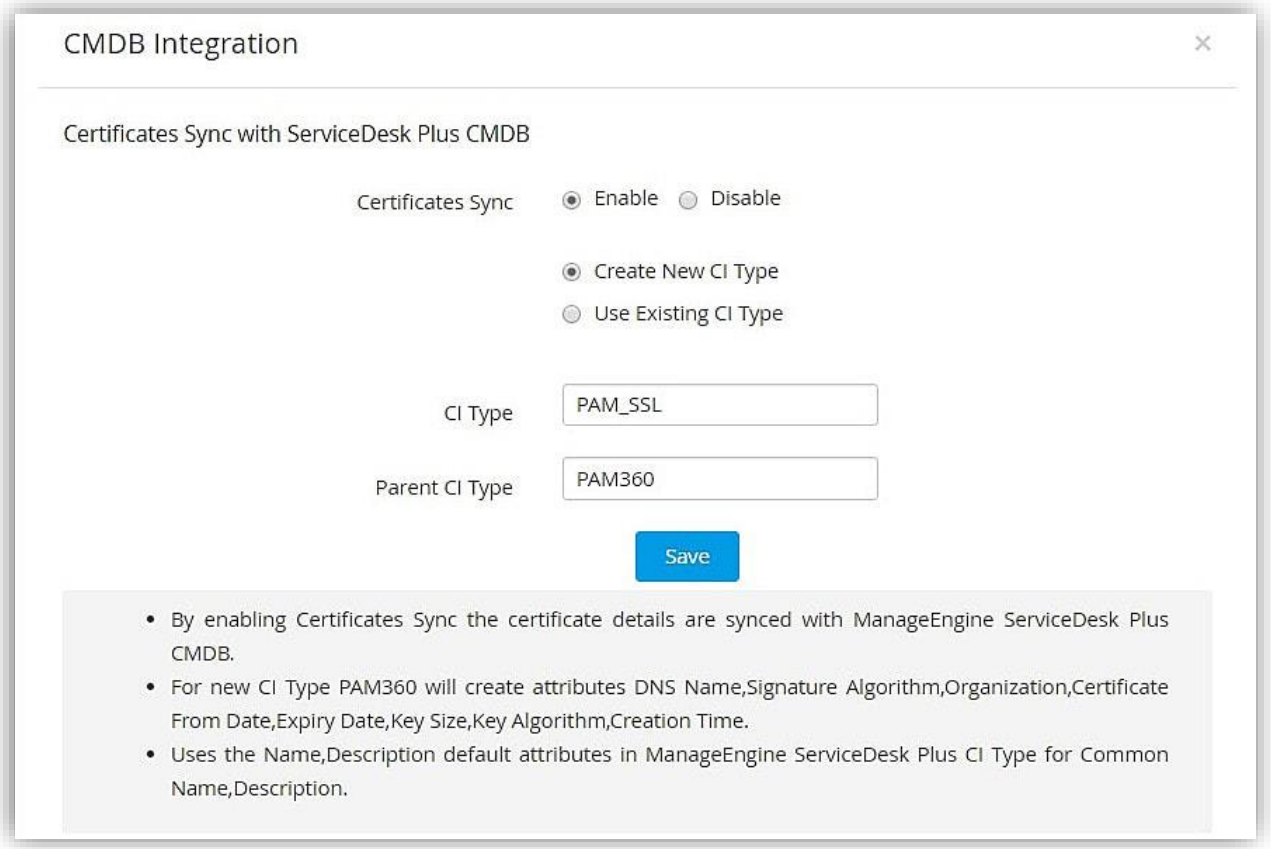
To provide the above details, go to **Admin >> Integration >> Ticketing System Integration**. In the page that loads, enable ServiceDesk Plus integration and enter the details. The technician key should be generated from SDP's interface and the user account for which the key is generated should have SDAdmin privilege in SDP.



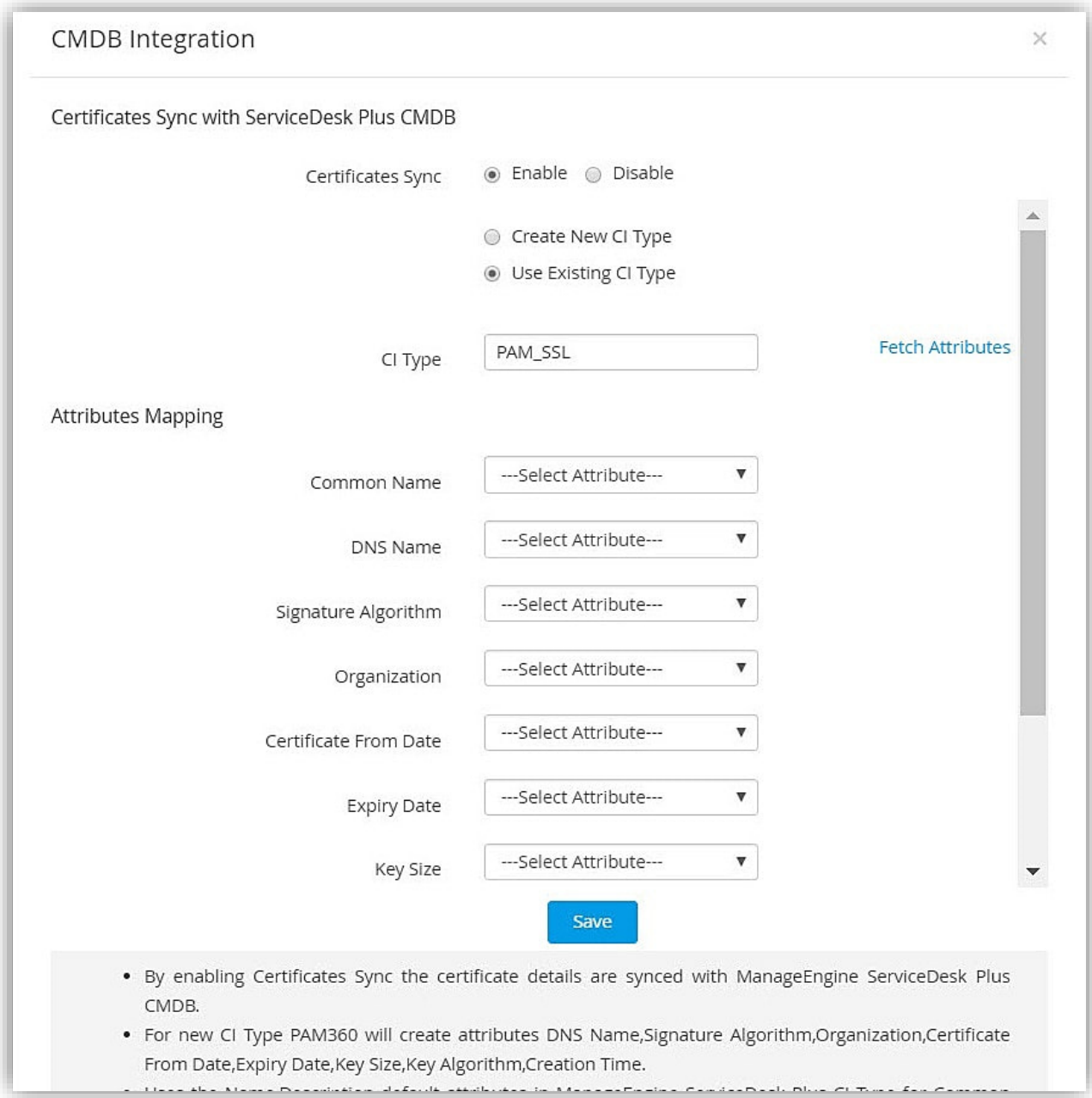
2. Creating CI type in SDP's CMDB

After providing SDP server configuration details, the next step is creating a new CI type in SDP's CMDB or use an already existing CI type in SDP's CMDB to export certificates from PAM360's repository. To create a CI type,

1. Navigate to **Admin >> SSH/SSL >> CMDB Integration** in PAM360's interface.
2. In the dialog box that opens, click **'Enable'** beside Certificate Sync option.
3. You can either choose to create a new configuration item (CI) type in SDP or export certificates into an already existing CI type.
4. To create a new CI type, select **'Create New CI Type'** option, provide a name for the CI type and an optional parent CI name. By default, child CI type PAM360_SSL is created under the parent CI type PAM360. You can choose to modify the names according to your requirements.



5. Click **Save.** A new CI type in created in SDP's CMDB consisting of the following attributes: Common name, DNS name, signature algorithm, organization, certificate from date, expiry date, key size, key algorithm, creation time and description. All the SSL certificates from PAM360's repository will them be exported to SDP's CMDB.
6. To export certificates into an already existing CI type in SDP, select **Use Existing CI Type** option and specify its name.
7. Click **Fetch attributes** to fetch the attributes of the existing CI type.
8. You then have to map the certificate attributes available in PAM360 (common name, DNS name etc.,) with the attributes of the chosen CI type by choosing appropriate options from the **Select Attribute** dropdown.
9. After the mapping is done, click **Save.** All the certificates from PAM360's repository will be exported to SDP's CMDB.



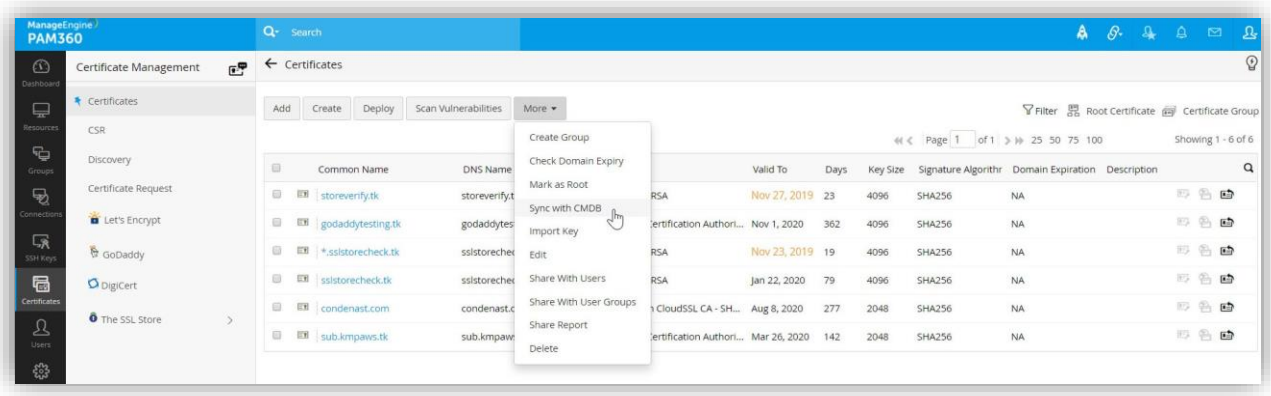
3. Enabling Certificate Sync

To enable certificate synchronization with SDP's CMDB,

1. Navigate to **SSH/SSL >> CMDB Integration** in PAM360's interface.
2. Switch to CMDB tab and click **'Enable'** besides Certificates Sync. All certificates in PAM360 are synced with SDP's CMDB. Also, certificates that are added to PAM360 in future will be automatically exported and synchronized with SDP's CMDB.

In addition, you can choose to sync certificates manually whenever you want by carrying out the below steps:

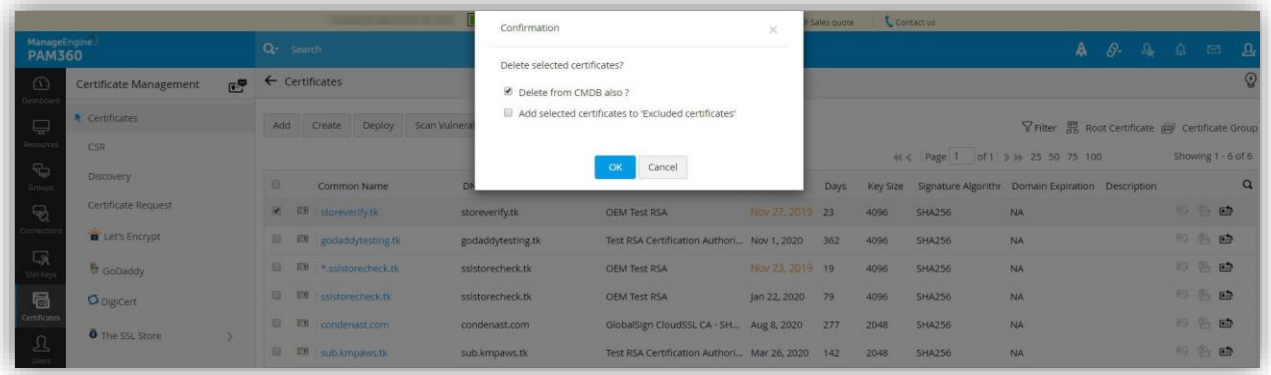
1. Navigate to **Certificates** tab and click the **More** option available above the table view.
2. Select **Sync with CMDB** from the dropdown menu. All the certificates in PAM360's repository will be synced with SDP's CMDB.



4. Deleting Certificates from CMDB

Similarly, when you delete unwanted certificates from PAM360's repository, the certificate gets deleted from SDP's CMDB also.

1. Navigate to **Certificates** tab.
2. Select the certificate(s) that you wish to delete. Click the **More** option available above the table view and select **Delete** from the dropdown menu.
3. A dialog box will appear asking you to confirm the deletion of certificate from CMDB also.
4. Enable the check-box and click **Ok.** The selected certificates are deleted from PAM360 and SDP's CMDB.



Manage PGP Keys

PAM360 allows you to create and manage Pretty Good Privacy (PGP) keys from the PAM360 web interface. The PGP keys are used to encrypt texts, emails, signing files, etc. PGP keys work as a key pair as they have a Master Key with a Sub Key bound to it. While creating a PGP key in PAM360, you can assign operations for the Master Key and the Sub Key individually, eg., signing and certifying to the Master Key and authentication and encryption to the Sub Key.

The PGP keys created are saved in the product key repository to secure and centralize their management. You may add a detailed description to the keys referring to their usage instances which helps you search and locate the keys faster. Also, there are provisions to edit the key description, view the passphrase, store them in an organized manner, or export the keys to your system or email address. Apart from the above, PAM360 provides detailed reports on the creation of PGP keys and operations performed on them such as export, edit, delete, etc. Each of the above operations will be logged into the **Audit** section of PAM360. You may also set up email notifications to get notified about the expiration of the PGP keys.

Refer to the sections below to learn more about each operation you can perform on the keys from the **PGP Keys** tab.

1. **Create PGP Key**
2. **Edit Key**
3. **Export Key**
4. **Email Key**
5. **Show Passphrase**
6. **Delete Key(s)**

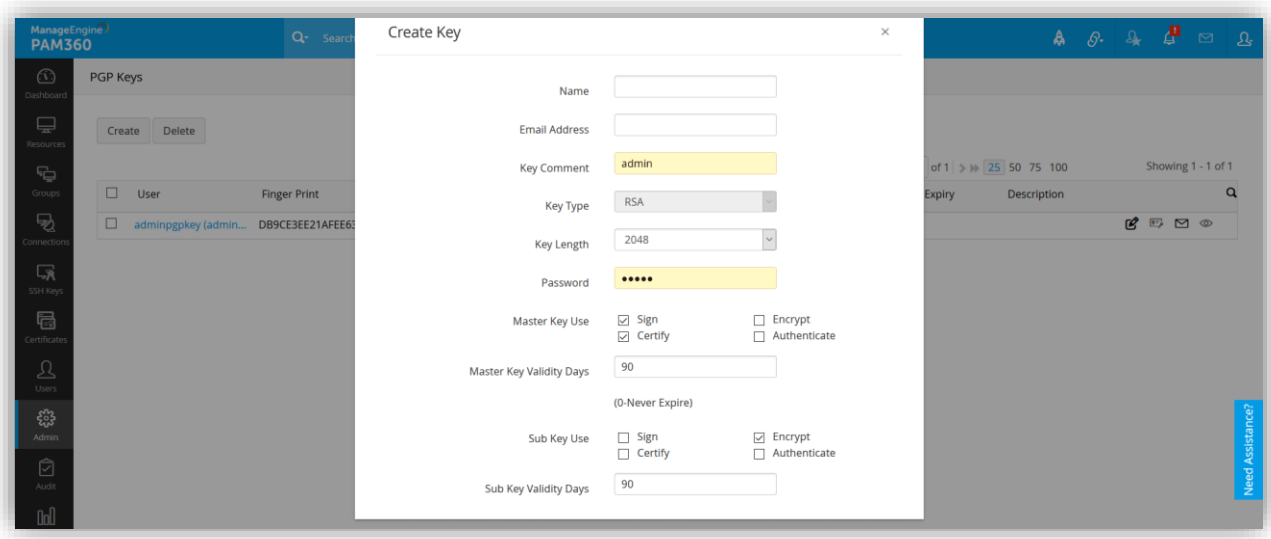
1. Create PGP Key

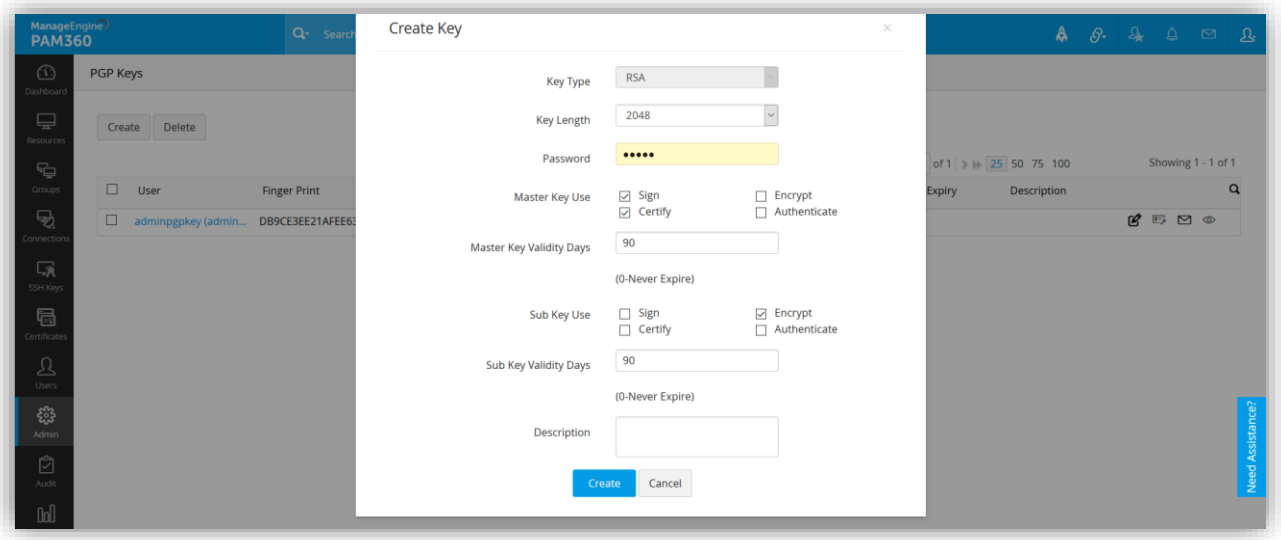
To create a key to store in the PAM360 repository:

1. Navigate to the **Admin >> SSL/SSH >> PGP Keys**.
2. Click the **Create** button.
3. Enter the following attributes:

i. **Name -** Enter the key name
ii. **Email Address** - Enter the email address of the creator.
iii. **Key Comment** - Enter a comment regarding the key explaining what it is going to be used for. Eg: Email encryption.
iv. **Key Type** - The key type is RSA by default.
v. **Key Length** - Choose the key length from the drop-down (2048 or 4096)
vi. **SSH Key Passphrase** - Enter a valid key passphrase.
vii. **Master Key Use** - Select the required check boxes to choose what the Master Key will be used for. The available options are **Sign, Certify, Encrypt, Authenticate.**
viii. **Master Key Validity Days** - Specify the expiry period for the Master Key —the default value is 90 days. Enter '0' for the key to be valid forever.
ix. **Sub Key Use** - Select the required check boxes to choose what the Sub Key will be used for. The available options are **Sign, Certify, Encrypt, Authenticate.**
x. **Sub Key Validity Days** - Specify the expiry period for the Sub Key —the default value is 90 days. Enter '0' for the key to be valid forever. Please note, the validity period of the Sub Key cannot exceed that of the Master Key.
xi. **Description** - Enter a description for the key.

4. Click the **Create** button.





Now, the key is enumerated in the **PGP Keys** tab. To view the key details of both Master Key and Sub Key, click the name of the key. The contents of the Master Key and the Sub Key will be listed separately.

> **Note:** The Master Key and the Sub Key both combine to create a single key and will be treated as such under PAM360 license too.

2. Import PGP Key

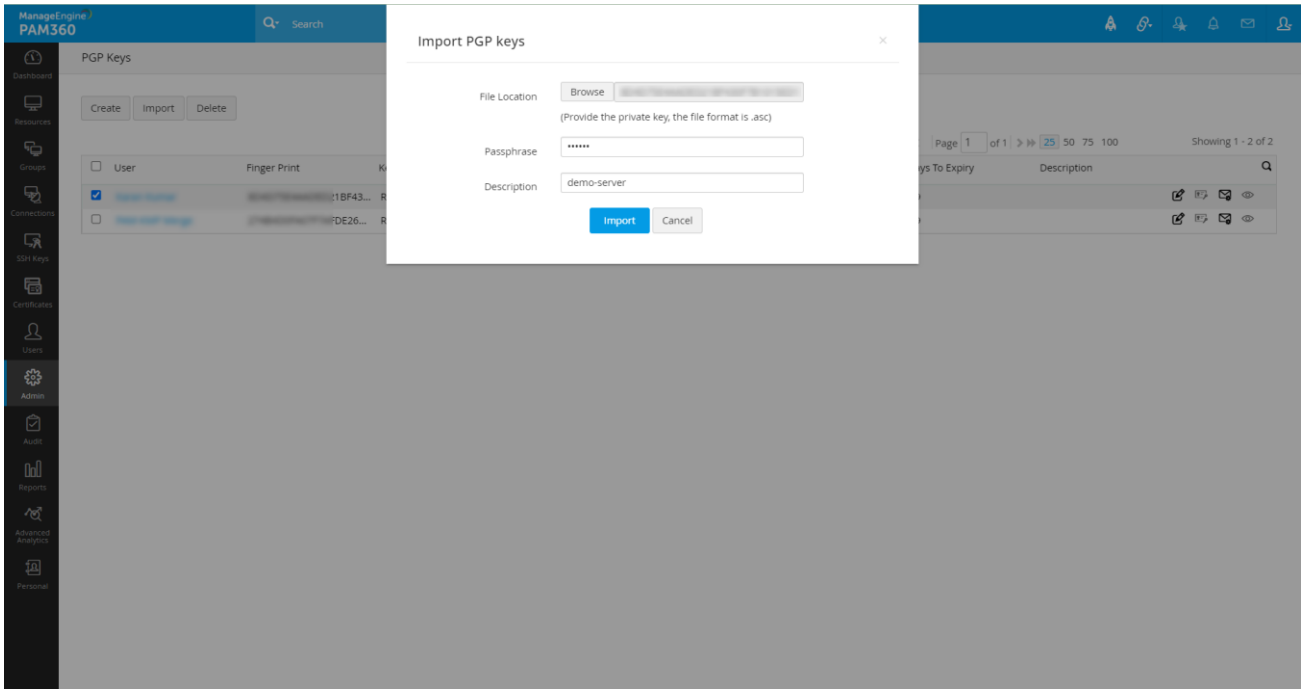
To import PGP key to the PAM360 repository:

1. Navigate to '**Admin >> SSL/SSH Config >> PGP Keys**'.
2. Click the **Import** button.
3. In the pop-up that appears:

i. **Browse** and select the **File Location.**

ii. Mention the **Passphrase** and **Description**, and click **Import.**

4. Now, you have successfully imported the PGP key(s) to the PAM360 repository.



3. Edit Key

To edit a key:

1. Click the **Edit** icon next to the required key.
2. In the **Edit** window that appears, enter a description and click **Update**.

4. Export Key

To export a key:

1. Click the Export icon next to the required key.
2. Choose **Export Public Key** or **Export Private Key** from the drop-down to download the public key or the private key separately. The keys will be downloaded as ASC (Action Script Communication) files.

> **Note:** The passphrases used to protect the keys are applicable even for exported keys. Thus, you need to provide the corresponding passphrase to use the exported keys elsewhere.

5. Email Key

To send a key to an email address:

1. Click the **Mail** icon next to the required key.
2. In the **Mail PGP Key** window, select the respective check boxes to send either the private key or the public key.
3. In the **Mail Id** field, enter an email address and click send. You can enter multiple email addresses by separating them with commas.

6. Show Passphrase

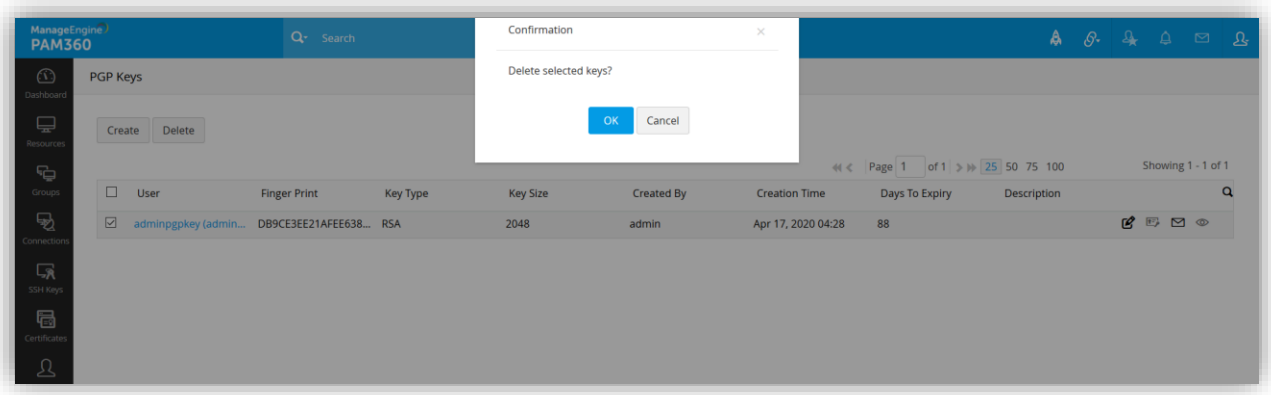
To view the passphrase of a key:

1. Click the **Show Passphrase** icon next to the required key.
2. The passphrase of the key will be displayed in a drop-down.

7. Delete Key(s)

To delete keys:

1. Select the check boxes beside the required keys.
2. Click the **Delete** button in the menu bar at the top and click **Ok** in the confirmation dialog box that appears. The key deletion action will be recorded in the Audit logs along with the date, time and the user who deleted it.



Additional Fields for SSH Keys and SSL Certificates

Use **Additional Fields** in PAM360 to attach any extra information about keys and certificates stored in the repository.

There are four types of fields to create: **Character, Numeric, Date and Email.** Once an additional field is created, the default value assigned to it will be applied to all entries in **SSH Keys** and **Certificates** tabs and will be visible to all users. Therefore, it is ideal to use additional fields for assigning common attributes such as organization name, or email address. Also, the **Column Chooser** icon helps you organize columns and additional fields in **SSH Keys** and **Certificates** tab views, and in **Reports** and **Dashboard** tab views.

Below are the operations you can perform on additional fields and the column chooser:

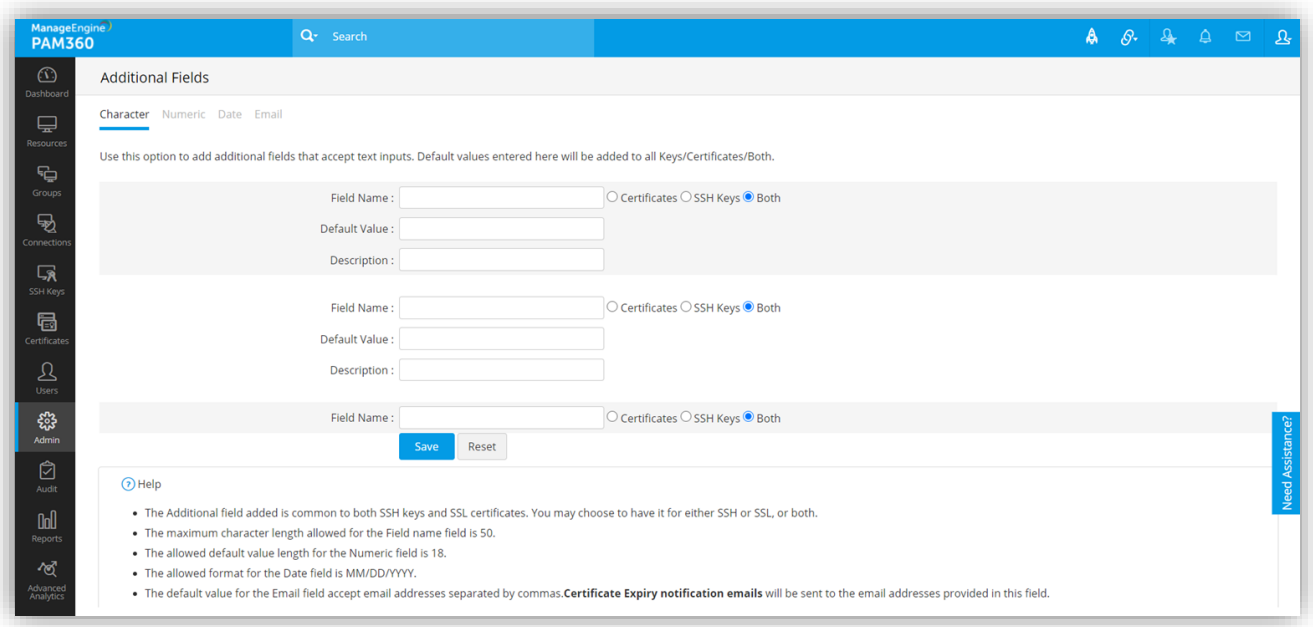
1. **Creating an Additional Field**
2. **Displaying an Additional Field**
3. **Editing an Additional Field**
4. **Resetting an Additional Field**
5. **How to Show/Hide Fields Using the Column Chooser?**

1. Creating an Additional Field

Follow the below steps to create additional fields that will apply to both keys and certificates tabs.

1. Navigate to **Admin >> SSH/SSL Config >> Additional Fields.**
2. Create a new additional field for any of the below mentioned field types:
    i. **Character:** To store text inputs
    ii. **Numeric:** To store numerical inputs
    iii. **Date:** To store date and time inputs
    iv. **Email:** To store relevant email addresses

3. Add the **Field Name, Default Value, Description**. Select **SSH Keys** or **Certificates** tab to add the additional field to either of the tabs. To add the field to both tabs, select **Both** and click **Save**.
4. To view the newly created additional field under the **SSH Keys** or the **Certificates** tab, click the column chooser icon ( ) from the top bar.



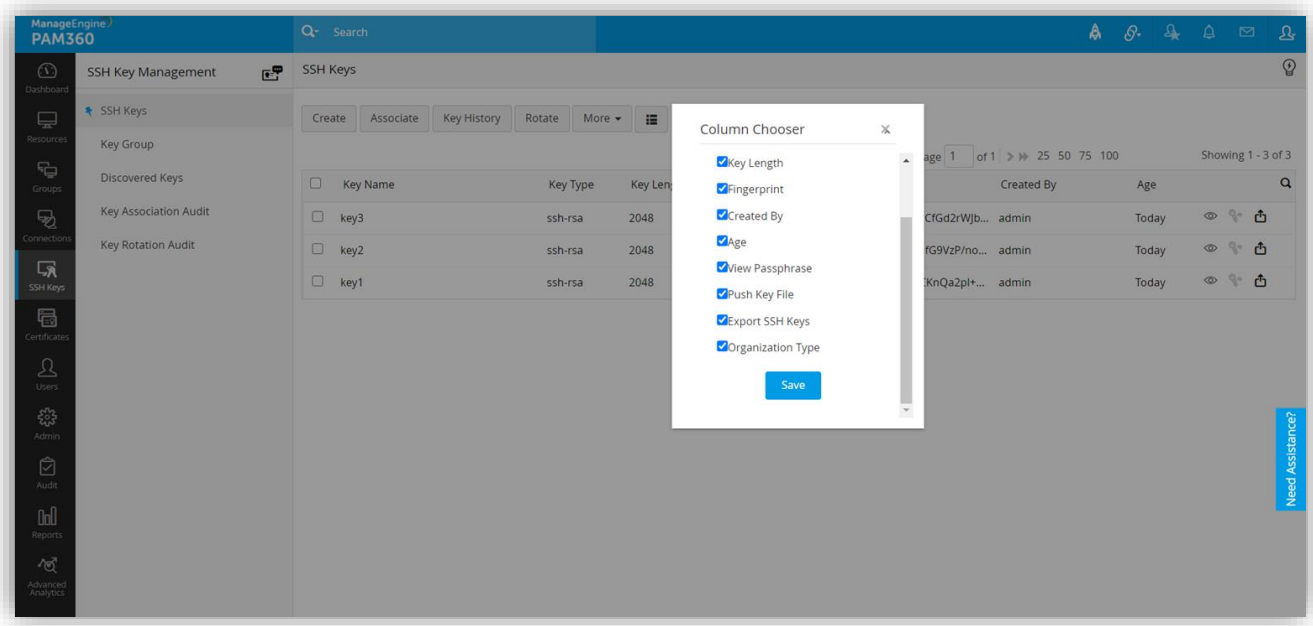
Note: Certificate Expiry Notification emails are sent to the email addresses specified in additional fields of the type **Email**. These notification emails will be customized according to the format configured for notifications under **Admin >> SSH/SSL Config >> Notification Settings** and **Admin >> SSH/SSL Config >> Schedules.**

2. Displaying an Additional Field

When you create an additional field of the type **Character/Numeric/Date/Email**, the field is added to both **SSH keys** and **Certificates** tabs immediately. Follow the below steps to display an additional field:

1. Navigate to **SSH Keys** or **Certificates** tab.
2. Click the column chooser icon ( ) from the top bar.
3. In the column chooser pop-up, select the checkbox beside the additional field you

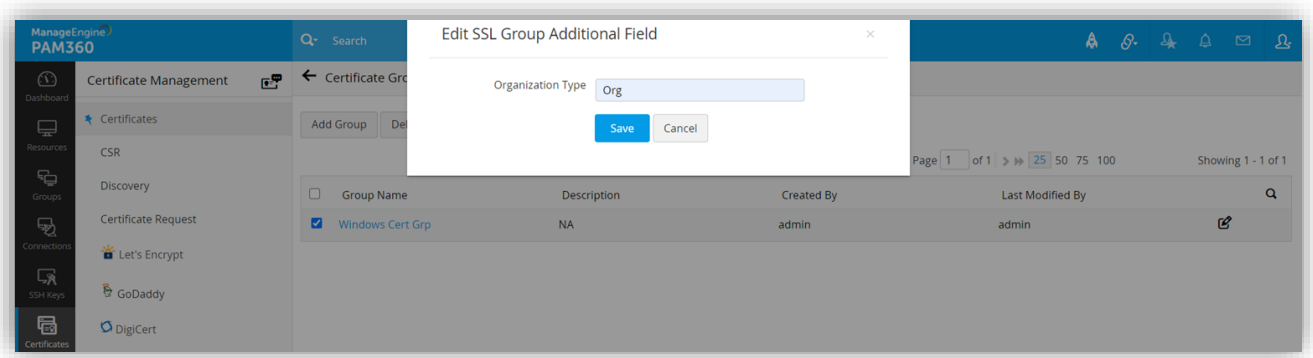
added and click **Save**. Now, the additional field and the default value added during its creation will be displayed among the other fields. The same field value will be applied to all entries in the Keys and Certificate repository but the value can be edited and customized using the **Edit** option.

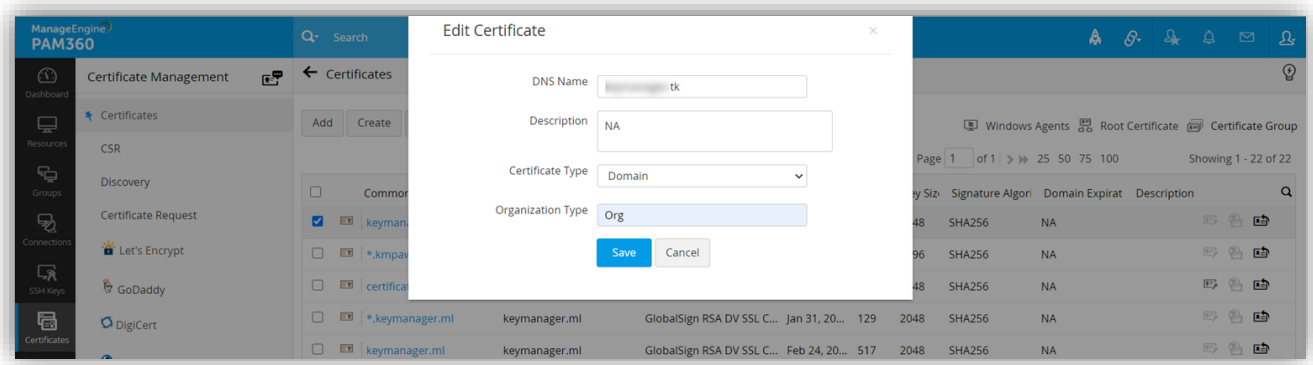


3. Editing an Additional Field

Once a default value for the additional field is added, the same value will be applied to all the certificate and key entries in the **Certificates** and **SSH Keys** tabs respectively. To change the field value for a particular certificate, follow the below steps:

1. Navigate to **SSH Keys** or **Certificates** tab.
2. Select a particular certificate and click **Edit** from the **More** drop-down in the top bar.
3. In the **Edit Certificate** window, edit the value and click **Save**. This value will be updated for the selected certificate alone.
4. To edit additional fields in bulk for a number of keys/certificates at a time, select all required keys or certificates and click **More >> Edit**. In the Edit window, add new values for the additional fields. The same values will be added for all the selected keys/certificates.
5. To edit additional fields for certificate groups, go to **Certificates >> Certificate Group**. Select the required groups and click **Edit Additional Field.**

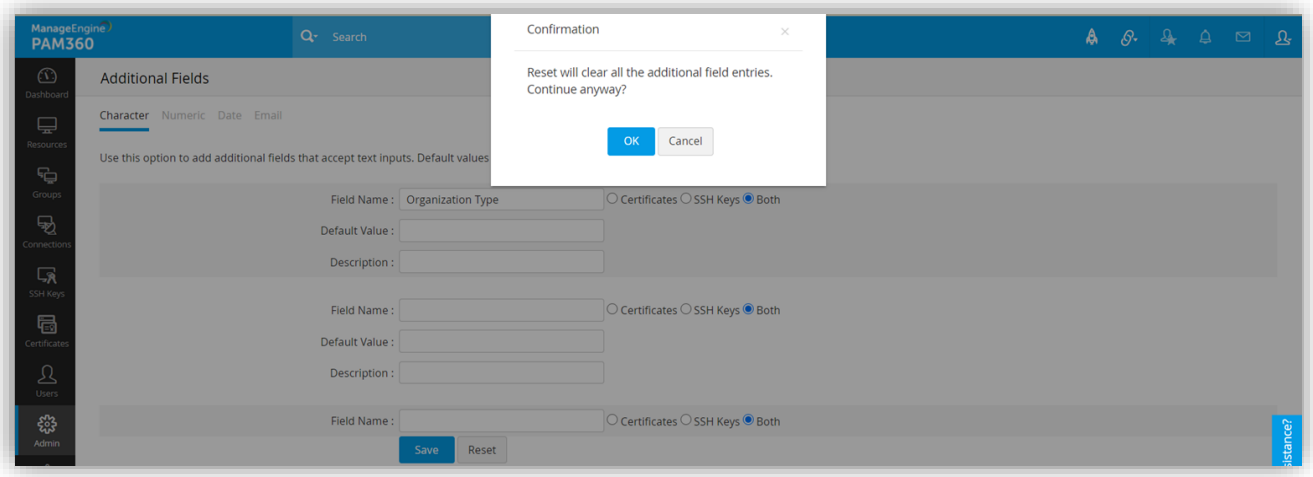




4. Resetting an Additional Field

Follow the below steps to reset the additional fields and remove any previously added ones:

1. Navigate to **Admin >> SSH/SSL Config >> Additional Fields.**
2. Click the **Reset** option available at the bottom of the page. In the pop-up that opens, confirm the reset by clicking **OK**. This process will delete the additional fields from both the SSH Keys and SSL Certificates tab.
3. To delete only selected additional fields, remove the field name, default value and description manually and click **Save**.



5. How to Show/Hide Fields using the Column Chooser?

Using the **Column Chooser** icon ( ), organize the columns and choose to show or hide both the default and additional fields as per your requirement. The **Column Chooser** icon helps declutter the columns in the following tabs: **SSH Keys**, **Certificates**, **Reports** and **Dashboard**.

In the **Reports** tab, the **Column Chooser** is available for selected reports, namely the following:

1. SSL Certificates Report
2. SHA1 Certificate Report
3. Let's Encrypt Certificates Report
4. SSL Vulnerability Report
5. PrivateKey Report
6. Certificate Renewal

In the **Dashboard** tab, the **Column Chooser** is available for the following views in the **Keys Dashboard**: SSH Keys and SSL Certificates.

> **Note:** Column chooser customization is unique to an individual user, therefore the changes in arrangement or visibility of columns made by one user will not be applied to another user.

Follow the below steps to show or hide any column from the tab view:

1. Click the **Column Chooser** icon to display all the available column names.

2. Unselect the checkboxes beside the column names that you want to hide from the tab view. You can choose to hide even the default columns in this way.
3. Apart from the show/hide option, you can change the sort order of the columns. To do so, simply click the column and drag and drop where required.
4. All the additional fields created for SSH Keys and SSL Certificates will also be listed under **Admin >> Settings >> Privacy Settings**, along with the default column values. Select the checkboxes beside the column/field names to hide or mask the corresponding data from the exported reports.

SSL Agent

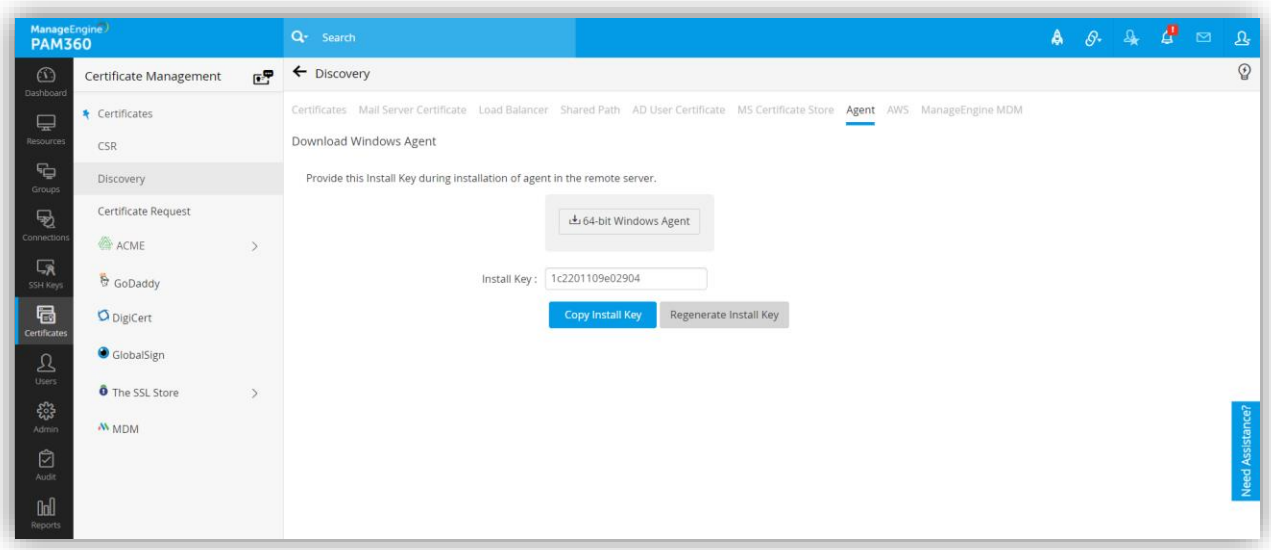
PAM360 allows you to discover the SSL Certificates deployed across their network through agents. The agent used to perform certificate management operations on remote machines is dynamically created by PAM360.

1. Downloading the SSL Agent
2. Installing the SSL Agent
3. Managing the SSL Agents
4. Discovering SSL Certificates using Agent
5. Signing Certificate(s) using Agent
6. Deploying Certificate(s) using Agent
7. Deploying Certificate(s) in Multiple Servers using Agent
8. Deleting Agent(s)

1. Downloading the SSL Agent

The agent used to perform certificate management operations on remote machines is dynamically created by the PAM360 server and is available for download from within the interface. To download the SSL Windows agent:

1. Navigate to **Certificates >> Discovery >> Agent >> Download Windows Agent.**
2. From the pop up that opens, download the agent based on your server configuration. Also, copy and save the **Install Key** in a secure location.



2. Installing the SSL Agent

Once you have downloaded the agent, follow the instructions below to install it in the target servers. The downloaded package already contains the configurations necessary to perform the required operations. Just make sure the account in the server in which the agent is installed has sufficient privileges to perform certificate discovery.

Steps to install SSL agent as a Windows service:

1. Move the .zip file downloaded from the PAM360 server to the target server.
2. Unzip its contents and place the file in an unshared folder.
3. Open the command prompt, navigate to the agent installation directory and type the command: **AgentInstaller.exe install** < Install Key > by supplying the **Install Key** stored in the secure location.

> **Note:** The Install Key is revoked after being used for a single installation. If you want to perform another installation of the agent, you need to regenerate the Install Key from the PAM360 server and supply it in the agent server.

Steps to start the agent as a Windows service:

1. Open the command prompt and navigate to the PAM360 agent installation directory.
2. Execute the following command: **AgentInstaller.exe start**.

On successful installation, you can find the SSL agent running as a service in the target server.

Steps to stop the agent:

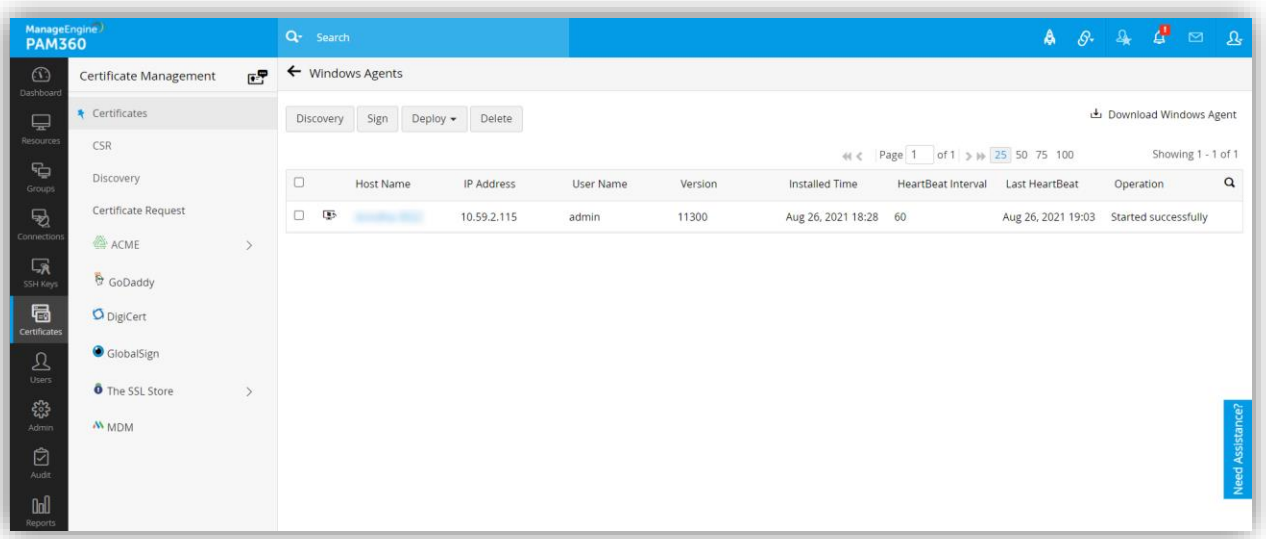
1. Open the command prompt and navigate to the SSL agent installation directory.
2. Execute the following command: **AgentInstaller.exe stop**

3. Managing the SSL Agents

PAM360 provides administrators with insights about agent activity and allows management of agents installed on various target resources.

To manage SSL agents:

1. Navigate to **Certificates >> Windows Agent.**
2. In the window that opens, you will be able to see a list of SSL agents installed on remote resources along with insights such as **Host Name, IP address, User Name, Version, Installed Time**, **HeartBeat Interval, Last HeartBeat,** and last **Operation** performed.
3. If you want to delete an agent, you can do so by choosing the agent and clicking **Delete** from the top menu.



4. Discovering SSL Certificates using Agent

1. Navigate to **Certificates >> Windows Agent** and select the agent.
2. Click **Discovery.**
3. In the pop-up that appears,

i. Choose **DMZ** to discover certificates from servers in the demilitarized zone.

ii. Choose to Discover by **Hostname / IP Address** or **IP Address Range.**

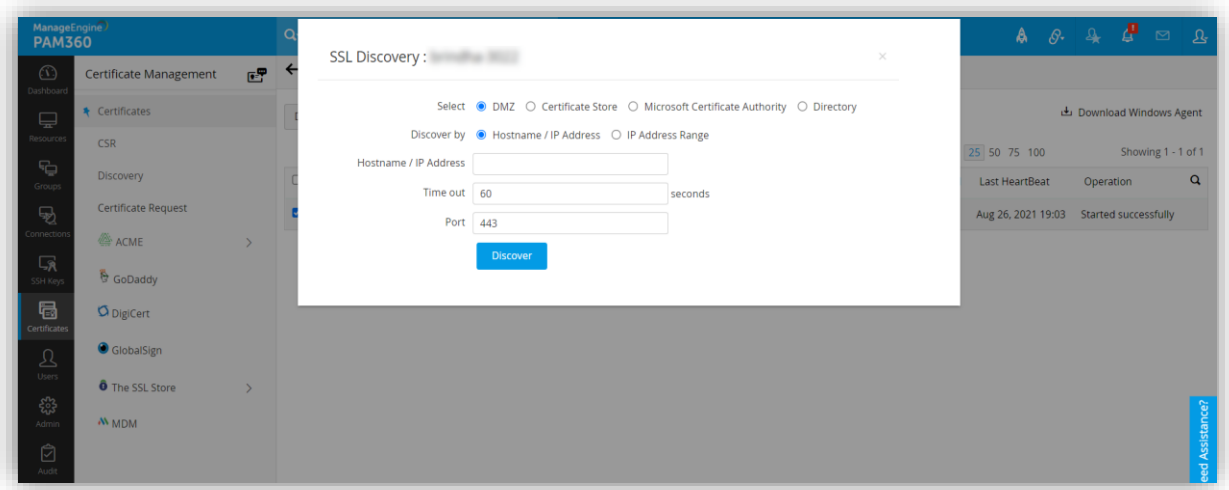
iii. If you choose to Discover by **Hostname / IP Address,** mention the **Hostname / IP Address, Time out** (in seconds), **Port** and click **Discover.**

iv. Choose **Certificate Store** or **Microsoft Certificate Authority** to perform agent-based discovery of local CA certificates.

v. If you choose **Certificate Store,** enter **Store name** and **Time out** (in seconds), **Port.**

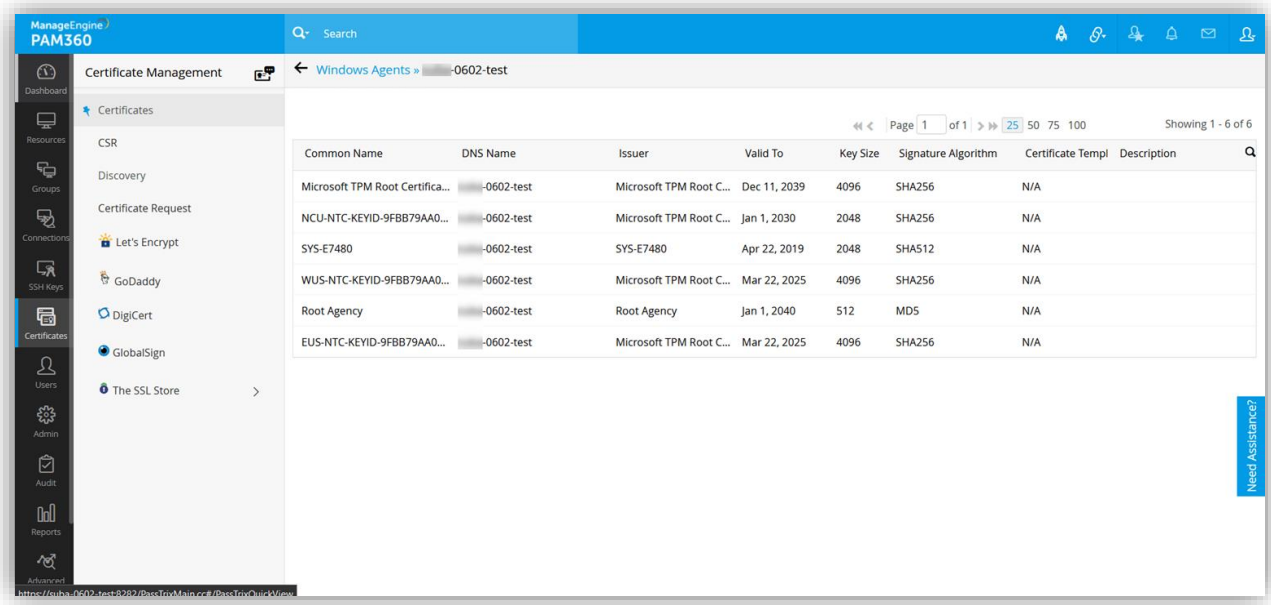
vi. To get **Store Name,** click **Get Stores** link and select from the dropdown and click **Discover.**

vii. If you choose **Microsoft Certificate Authority,** select the required checkboxes and enter the required details. If you select **Template Name / ODI,** mention the template name or click **Get Templates** to get a list of templates. You can select upto five templates from the dropdown. Mention the **Time out** (in seconds) and click **Discover.**



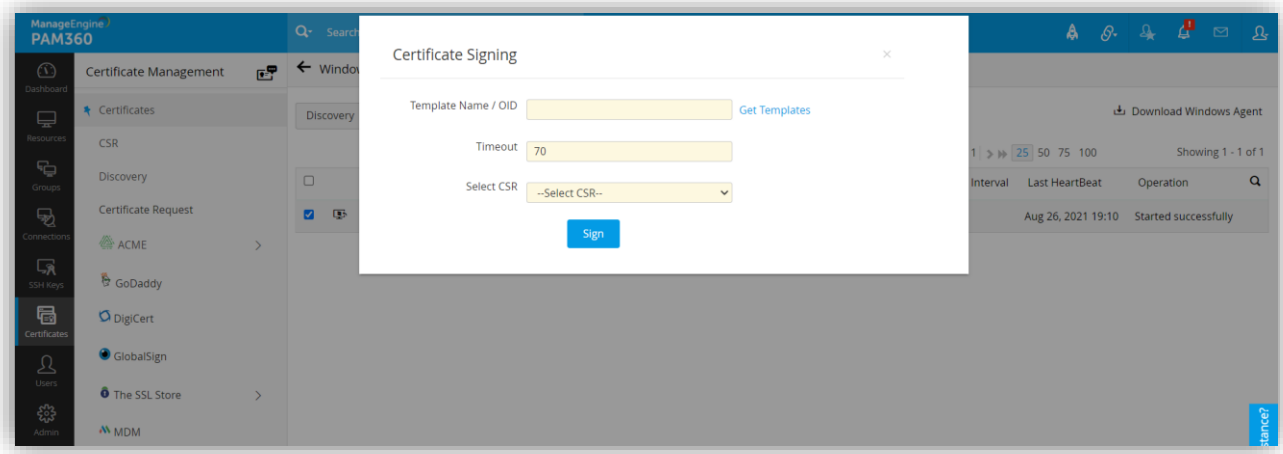
4. The certificates are successfully discovered and imported into PAM360 centralized certificate repository. You can view them from **Certificates >> Windows Agent.**

5. After certificate discovery, click the **Host Name** of an agent to view all certificates associated with that particular agent.



5. Signing Certificate(s) using Agent

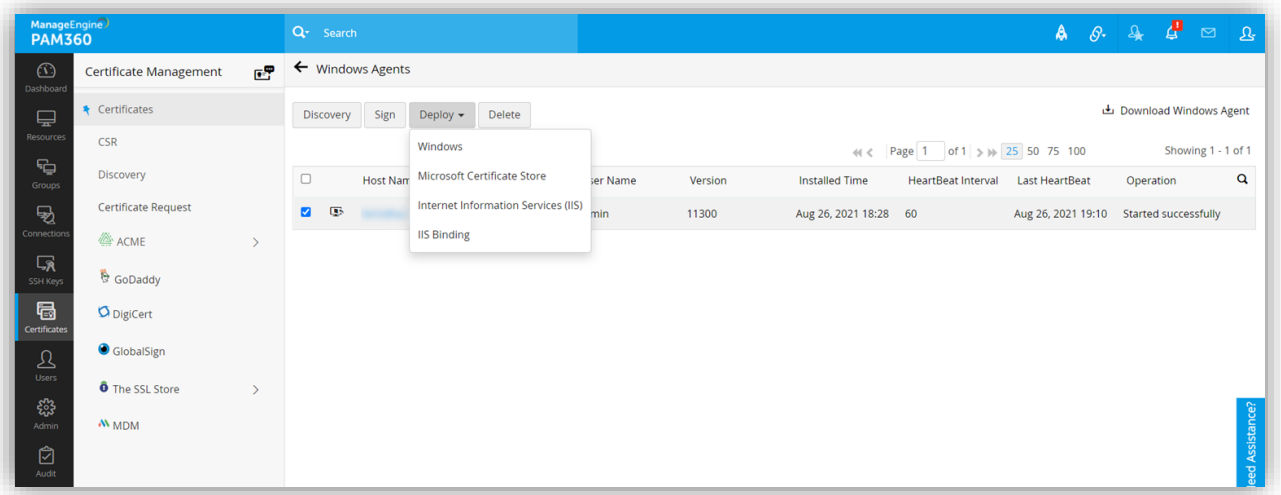
1. Navigate to **Certificates >> Windows Agent >> Discovery** and select the agent.
2. Select the **Certificate Template** or click **Get Templates** link to get new templates.
3. Mention the Agent **Time out** in seconds within which the agent should respond. If the agent doesn't respond within the timeout period, the operation will be audited as failed.
4. Select the **CSR** from the dropdown and click **Sign**.



Now the certificates are successfully signed and will be available to the repository.

6. Deploying Certificate(s) using Agent

1. Navigate to **Certificates >> Windows Agent** and select the agent.



2. Click **Deploy** and select the required server from the dropdown.
    i. If you choose **Windows** (using agent), select the **Certificate Group**, mention the **Path** and select the checkbox(es) **certificate** and/or **JKS/PKCS** based on your requirement and click **Deploy**.
    ii. If you choose **MS Store** (using agent), select the **Certificate Group** and click **Deploy.**
    iii. If you choose **IIS** (using agent), select the **Certificate Group** and click **Deploy.**
    iv. If you choose **IIS Binding** (using agent), select the **Certificate Group,** mention the **Site Name** and click **Get Bindings.**
    v. Click **Manage** link to manage the certificate group.
    vi. Click **Save** to save the changes.
3. Now, the certificates will be deployed and will be available under SSL tab.

7. Deploying Certificate(s) in Multiple Servers using Agent

1. Navigate to **Certificates >> Certificates** tab and click **multiple servers** icon corresponding to the required certificate.
2. A window opens listing the servers in which the certificate is deployed along with other information such as IP address, Port and certificate validity.
3. The DNS name should be same as the Agent's name and this agent should be running under the DNS server.
4. To modify the Server details, click **credentials** icon corresponding to the required

certificate.

i. Select the **Deployment Type** as **Agent.**

ii. Select the **Server Type** and select the required **Agent.**

iii. Mention the **Path,** and select the required checkbox(es).

iv. If you select **Certificate,** enter the **Certificate File Name.**

v. If you select **JKS / PKCS,** mention the **Store File Name.**

vi. If you choose the **Server Type** as **Microsoft Certificate Store**, select **Computer** and/or **User account** to deploy the certificate to the selected account.

vii. Now, select **Enable PrivateKey Export from MS Certificate Store after deployment** to export private key from the certificate store.

viii. Click **Save.**

5. To edit a deployed server, click **edit** icon corresponding to required certificate.

   i. In the pop-up that appears, you will be able to edit the **DNS Name, IP Address** and **Port.**

   ii. You can choose to **Deploy Certificate to all servers on Auto Renewal.**

   iii. Click **Save.**

> **Note:** You will be able to deploy certificate to all servers on auto renewal only if the user credentials are available.

6. To auto deploy certificates after renewal, select the desired certificates and click the **Edit** button.

   i. Select **Enable** and click **Save** in the pop-up that appears.

7. To check the Sync Status using the agent, select the desired certificates and click the Edit button.

   i. Select **Sync Check With Agent** and click **Save**.

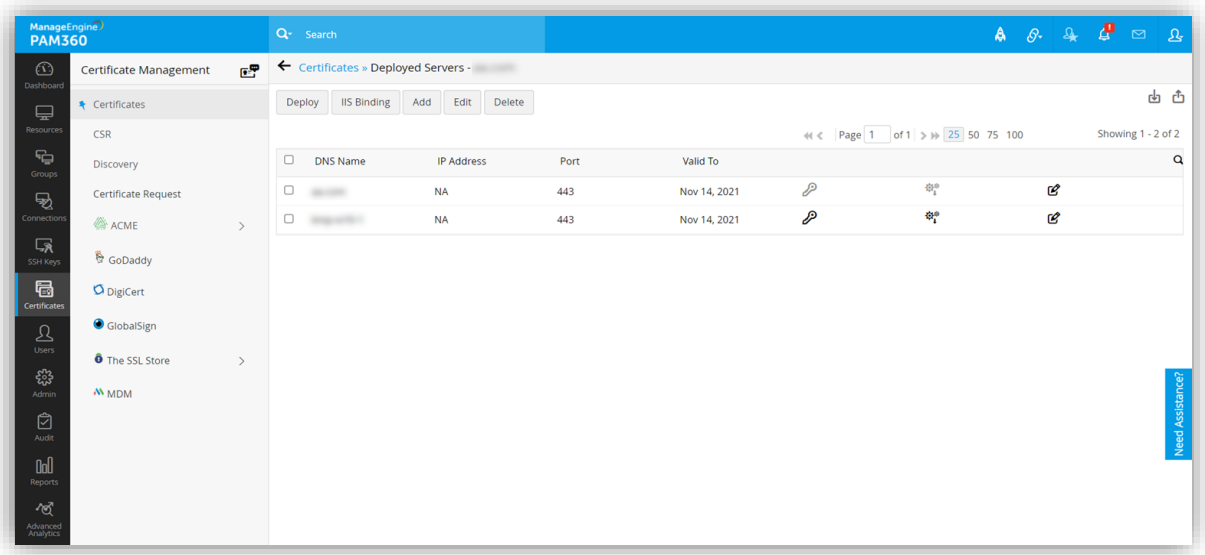
8. Click **Add** to Add Deployed Servers.

   i. In the pop-up that appears, mention the **DNS Name, IP Address** and **Port.**

ii. You can choose to **Deploy Certificate to all servers on Auto Renewal.**

iii. Click **Save.**

iv. You can also add deployed servers from **Certificates >> Certificates >> More >> Add Deployed Server.**



Now, the certificates have been successfully deployed using agent. To know more about SSL certificate deployment click here.

8. Deleting Agent(s)

1. Navigate to **Certificates >> Windows Agent** and select the required **Agent(s)** to be deleted and click **Delete**.
2. Click **Ok** in the pop-up that appears.
3. The certificate will be deleted from the list.

Working with Multiple Servers

PAM360 allows users to deploy multiple servers to certificates/add deployed servers to a certificate. By the end of this document you will have learnt the following:

1. Deploy Multiple Servers to a Certificate
2. Add Deployed Servers to a Certificate
3. Modify the Server Details
4. Edit a Deployed Server
5. Delete a Deployed Server
6. Auto Deploy a Certificate
7. Check Sync Status
8. Import Credentials
9. Export Credentials

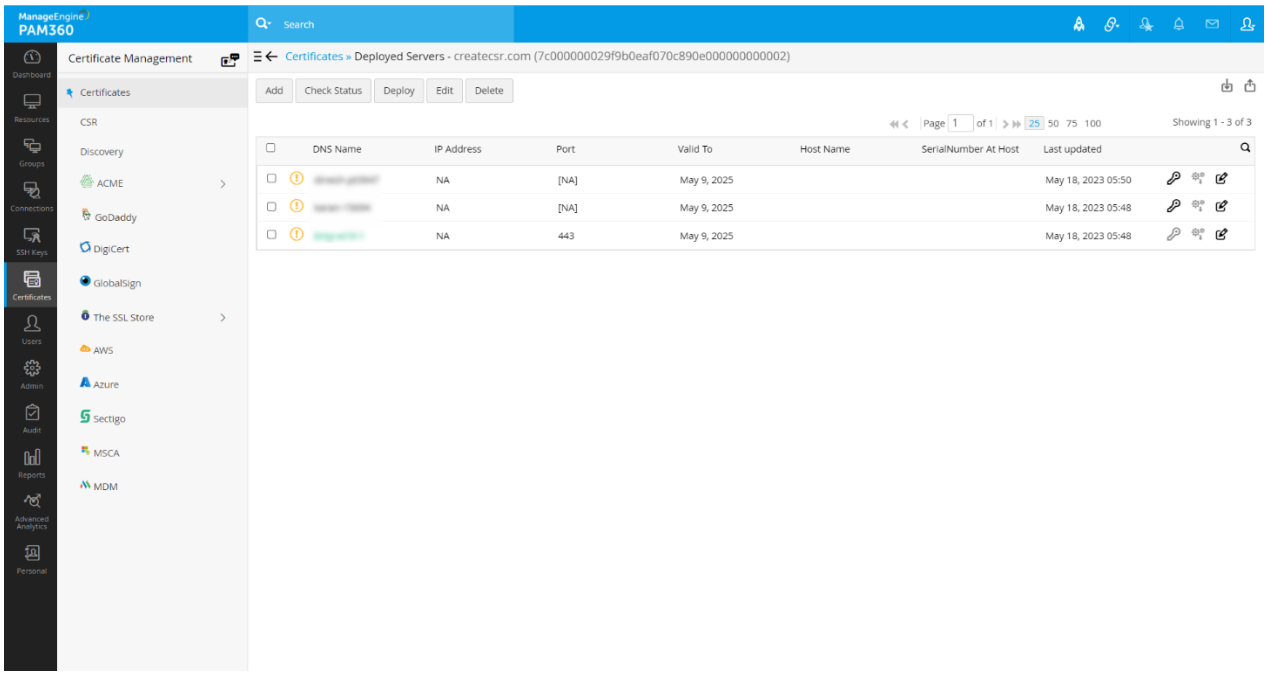
1. Deploy Multiple Servers to a Certificate

To deploy multiple servers to a certificate,

1. Navigate to Certificates >> Certificates tab.
2. Select the certificate to which you want to deploy multiple servers and click Deploy from the top pane and select to which you want to deploy the certificate.
3. Follow the steps here to know more about deploying certificates.

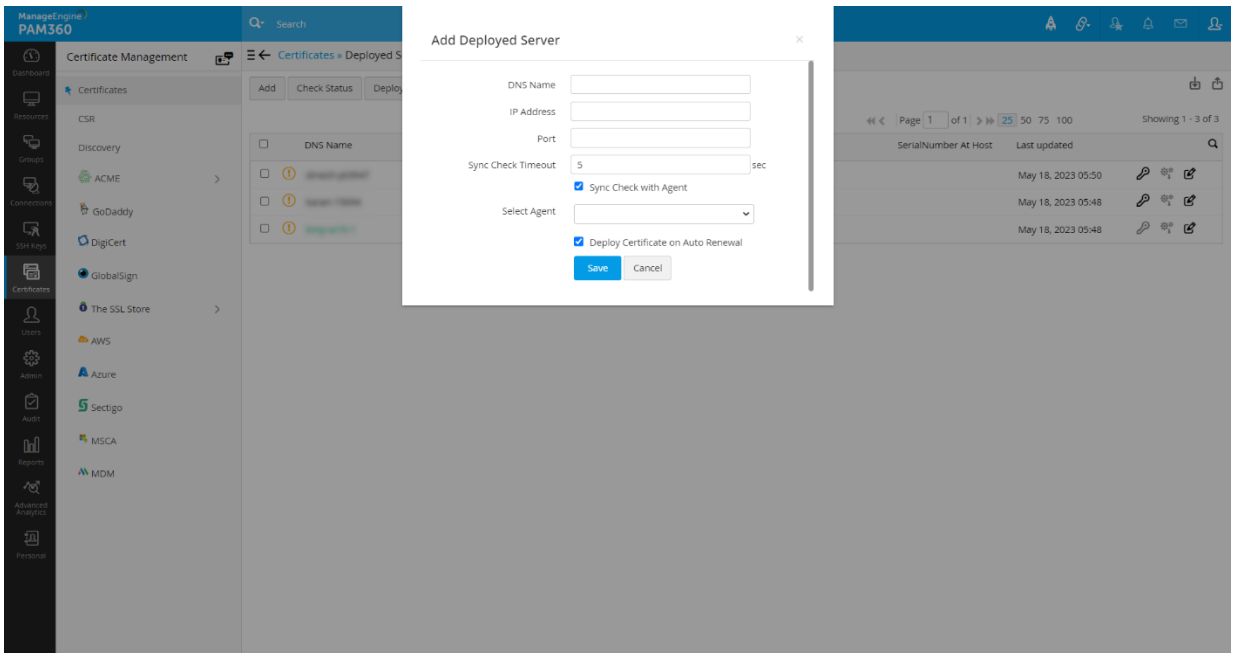
To view the multiple server page,

1. Navigate to Certificates >> Certificates tab and click multiple servers icon corresponding to the required certificate.
2. A window opens listing the servers in which the certificate is deployed along with other information such as IP address, Port and certificate validity, Host Name, Serial Number at Host and Sync Status.



2. Add Deployed Servers to a Certificate

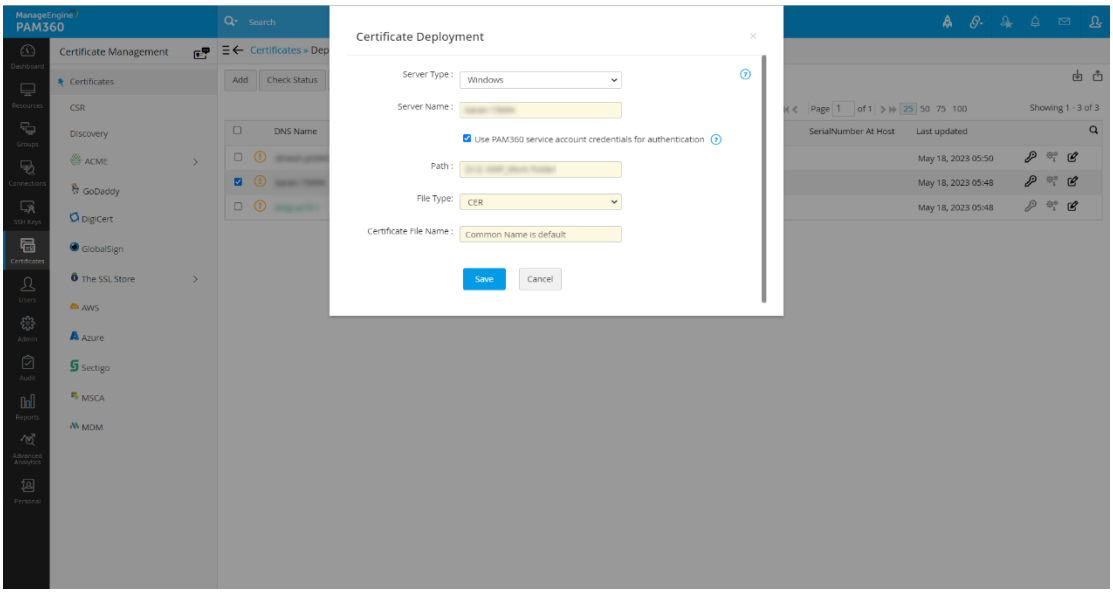
1. Navigate to **Certificates >> Certificates** tab and click multiple servers icon corresponding to the required certificate.
2. Click **Add** from the top pane to further add deployed servers to the certificate.
   i. In the pop-up that appears, mention the **DNS Name, IP Address** and **Port**.
   ii. Mention the **Sync Check Timeout** in seconds.
   iii. If you choose to **Sync Check with Agent**, select the desired **Agent**.
   iv. You can choose to **Deploy Certificate to all servers on Auto Renewal**.
   v. Click **Save**.



3. You can also add deployed servers from **Certificates >> Certificates >> More >> Add Deployed Server**.
4. Now, the certificates have been successfully deployed using agent. To know more about SSL certificate deployment, click here.

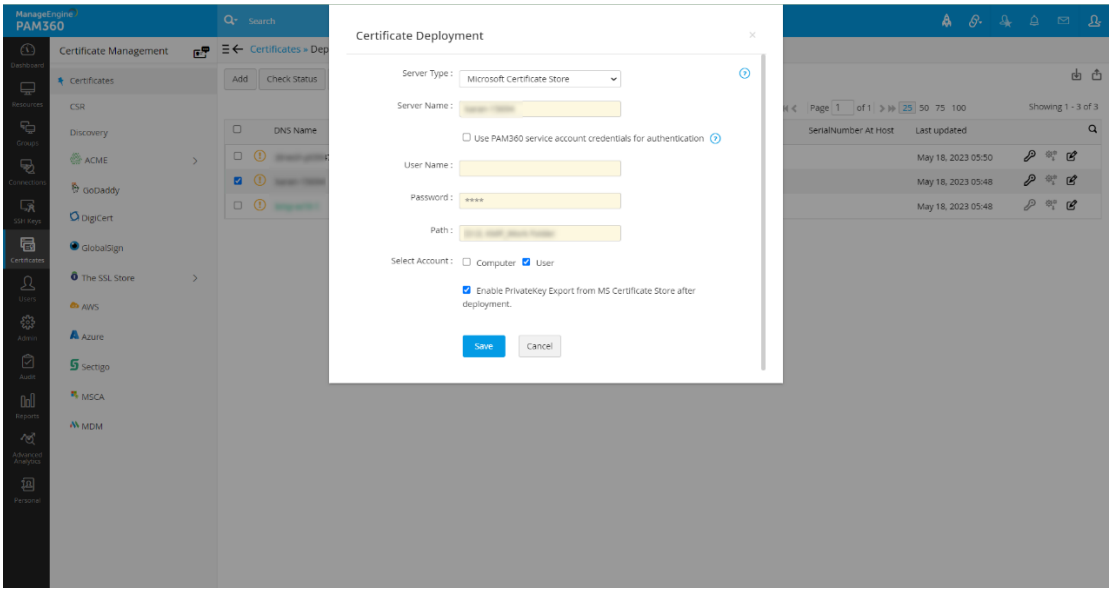
3. Modify the Server Details

1. Navigate to **Certificates >> Certificates** tab and click **multiple servers** icon corresponding to the required certificate.
2. To modify the Server details, click the **credentials** icon corresponding to the required certificate.
3. Select the **Server Type** and modify the required details.
    i. If you choose the **Server Type** as **Windows** or **Linux**,
        a. Mention the user credentials or **Use PAM360 service account credentials for authentication**, **Port** and the **Path**.



        b. If you select **Certificate**, select the **File Type** and enter the **Certificate File Name**.
        c. If you select **JKS/PKCS**, select the **Keystore Type** and mention the **Store File Name**.
    ii. If you choose the **Server Type** as **Microsoft Certificate Store**,
        a. Mention the credentials or **Use PAM360 service account credentials for authentication** and the **Path**.
        b. Select **Computer** and/or **User account** to deploy the certificate to the selected account.
        c. Now, select **Enable PrivateKey Export from MS Certificate Store after**

deployment to export private key from the certificate store.



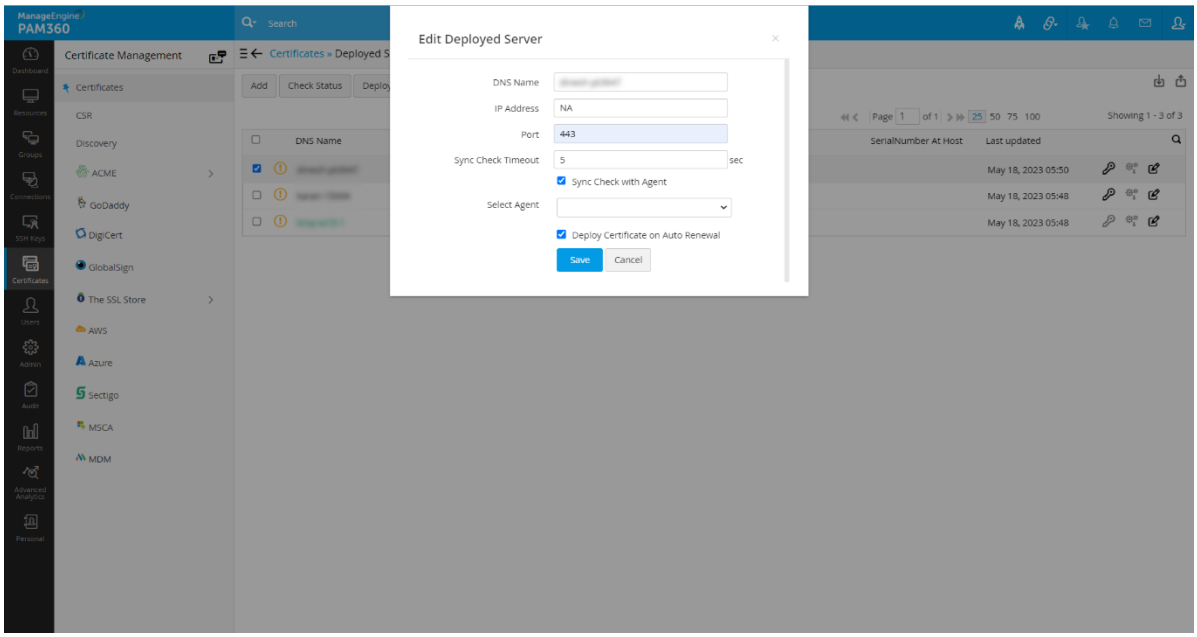
iii. If you choose the **Server Type** as **Internet Information Services (IIS)**,

a. Mention the credentials or **Use PAM360 service account credentials for authentication** and the **Path**.

4. Click **Save** to modify the server details.

4. Edit a Deployed Server

1. To edit a deployed server, click the **edit** icon corresponding to required certificate.
   i. In the pop-up that appears, you will be able to edit the **DNS Name, IP Address** and **Port**.
   ii. Mention the **Sync Check Timeout** in seconds.
   iii. If you choose to **Sync Check with Agent**, select the desired **Agent**.
   iv. You can choose to **Deploy Certificate on Auto Renewal**.
   v. Click **Save**.



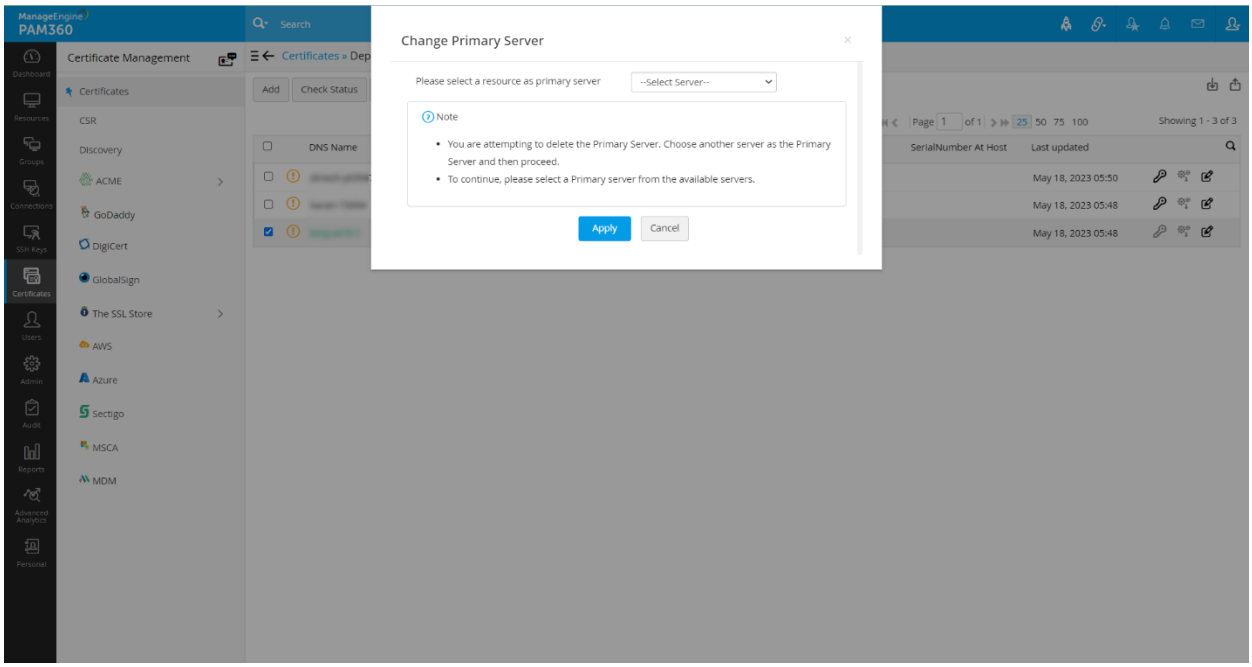
2. Now, you have successfully editted a deployed server.

> **Note**: You will be able to deploy certificate to all servers on auto renewal only if the user credentials are available.

5. Delete a Deployed Server

> **Note**: Users will not be allowed to delete the Primary server. Choose an alternate Primary Server and then proceed to delete the server.

1. To delete a deployed server, select the desired server and click **Delete** from the top pane.
2. If the server you are deleting is a Primary server, in the pop-up, select a new Primary server from the list and click **Apply**. This will assign the selected server as the Primary server.



3. Now, select the server again and click **Delete**.
4. In the pop-up that appears, click **OK**.
5. You have successfully deleted a deployed server.

6. Auto Deploy a Certificate

1. To auto deploy certificates after renewal, select the desired certificates and click the **Edit** button.
2. Select **Deploy Certificate on Auto Renewal** and click **Save** in the pop-up that appears.

7. Check Sync Status

1. To check the **Sync Status** using the agent, select the desired certificates and click the **Edit** button.
2. Select **Sync Check With Agent** and select the desired **Agent**.
3. Click **Save**.
4. To check the **Sync Status** of the server, select a server and click **Check Status** on the top pane.
5. Now, PAM360 will check the **Sync Status** and will display it on the corresponding server's column.

8. Import Credentials

1. Click the **import credentials** icon on the top-right corner.
2. In the pop-up that appers,

i. Browse and select the **File Location** from where you want to import.

ii. Select **Certificate** and/or **JKS / PKCS** and click **Import**.

3. Now you have successfully imported the credentials into PAM360.

9. Export Credentials

Select the desired resources and click the **export credentials** icon on top right corner to export the credentials to a text document.

Certificate Tools

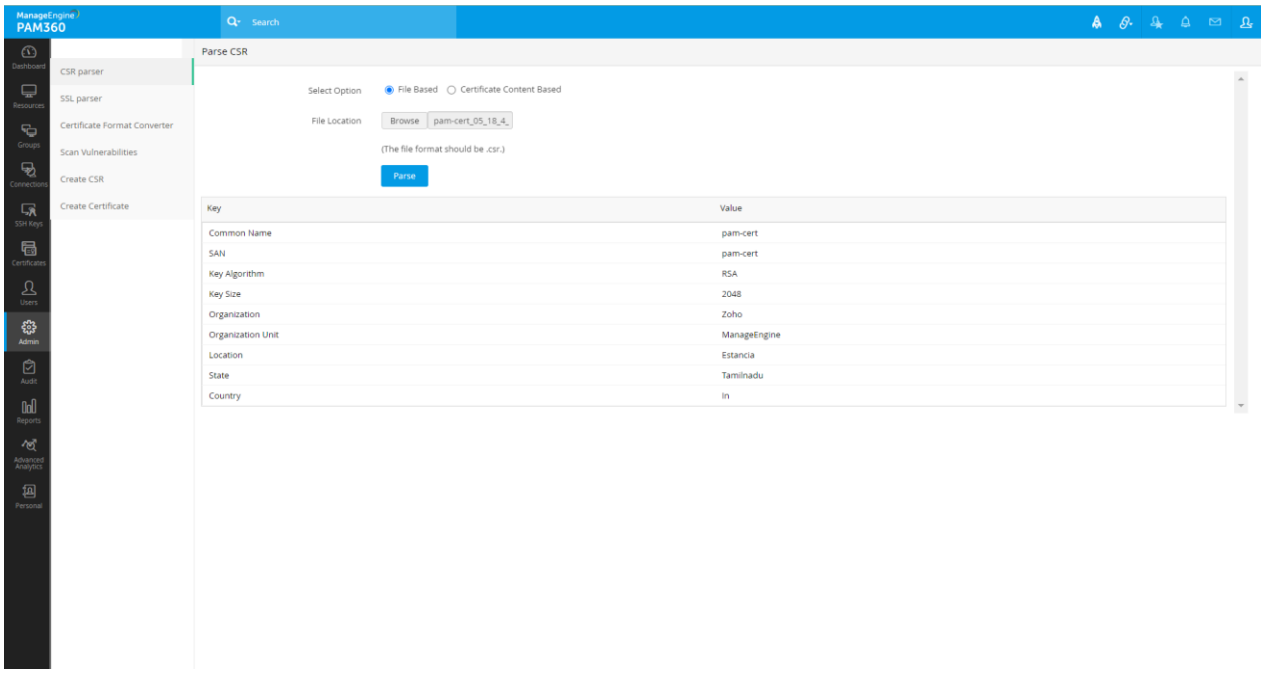
The Tools category in PAM360 comes with five options that will allow users to independently perform certificate conversion, parsing, CSR and certificate creations, and scan domains for vulnerabilities without adding them to the certificate repository. The available options in the Tools category are:

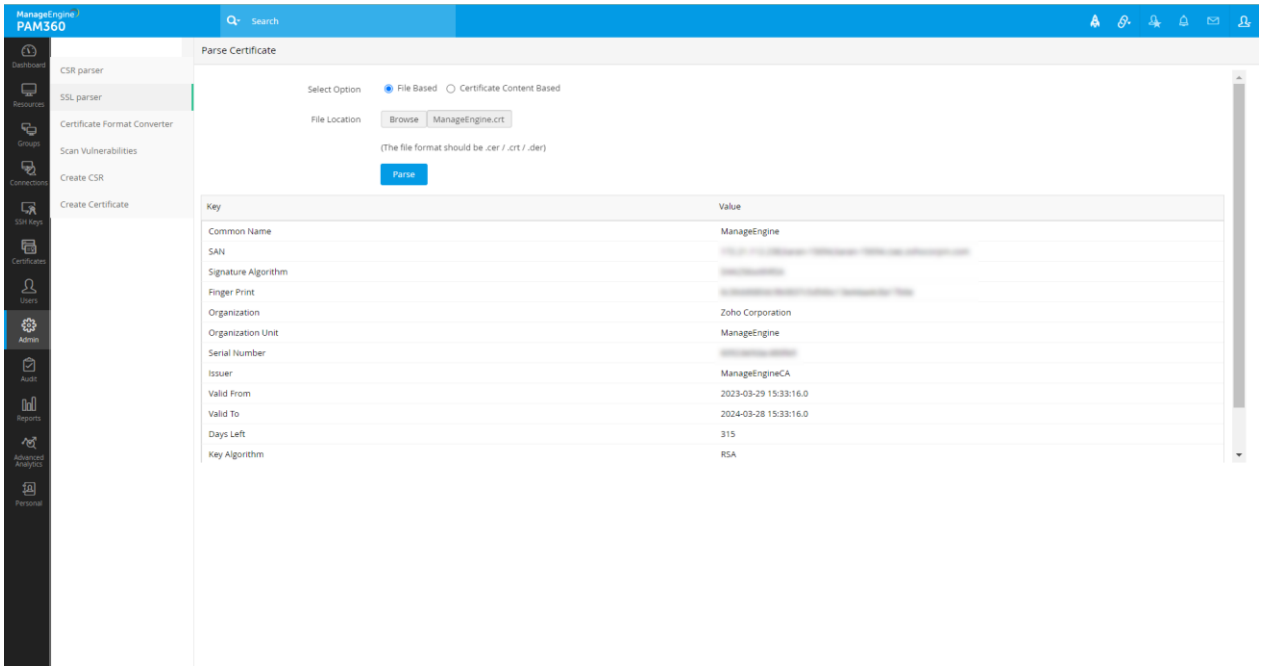
1. **Certificate signing request (CSR) and SSL parser**
2. **Certificate format converter**
3. **Scan vulnerabilities**
4. **Create CSR**
5. **Create Certificate**

1. Certificate Signing Request (CSR) and SSL Parser

The CSR and SSL parser tools allow users to upload certificates or their contents directly to the interface and sort the attributes into a readable format.

1. Navigate to **'Admin >> SSL Certificates >> Certificate Tools'** and click **CSR parser** or **SSL parser**.
2. Choose **File Based** and click **Browse** to upload a CSR or a certificate. Please note that CSR files must be in the .csr format, and the certificates must be in one of the following formats: .cer, .crt, .der. Click **Parse** and the results will be displayed below.
   [or]
   Choose **Certificate Content Based** to paste the contents of a CSR or a certificate instead of uploading the file.



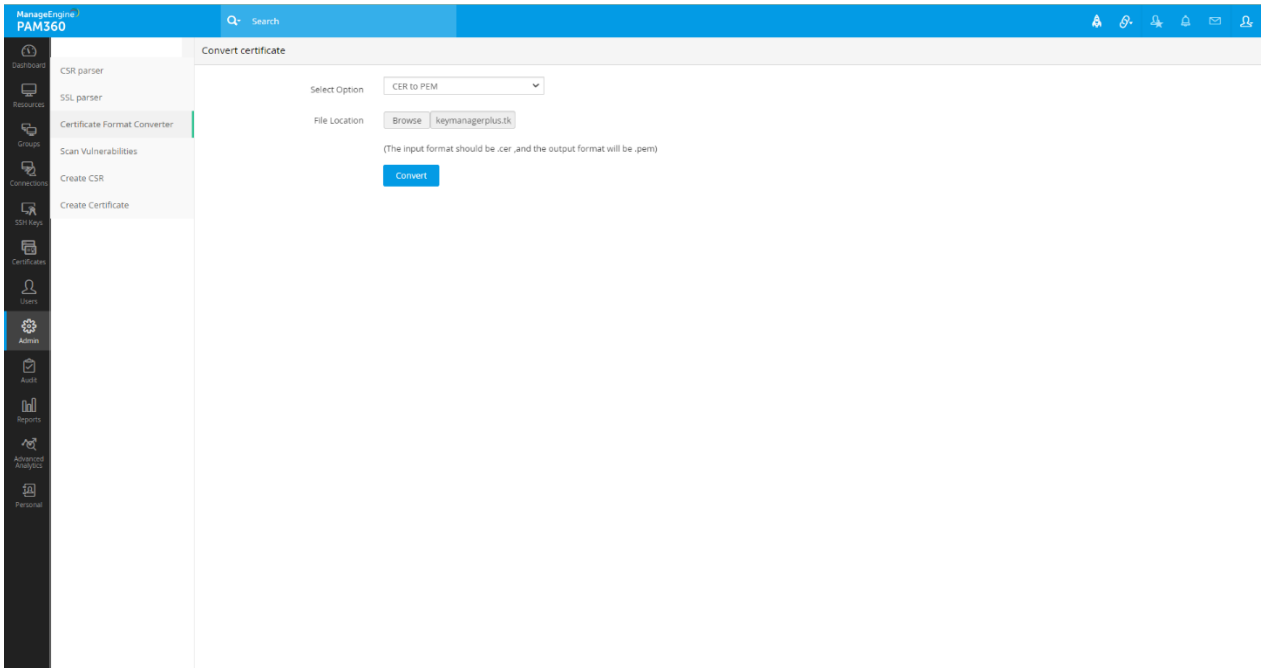


2. Certificate Format Converter

The certificate format converter tool supports one-click conversion for a wide range of certificate formats.

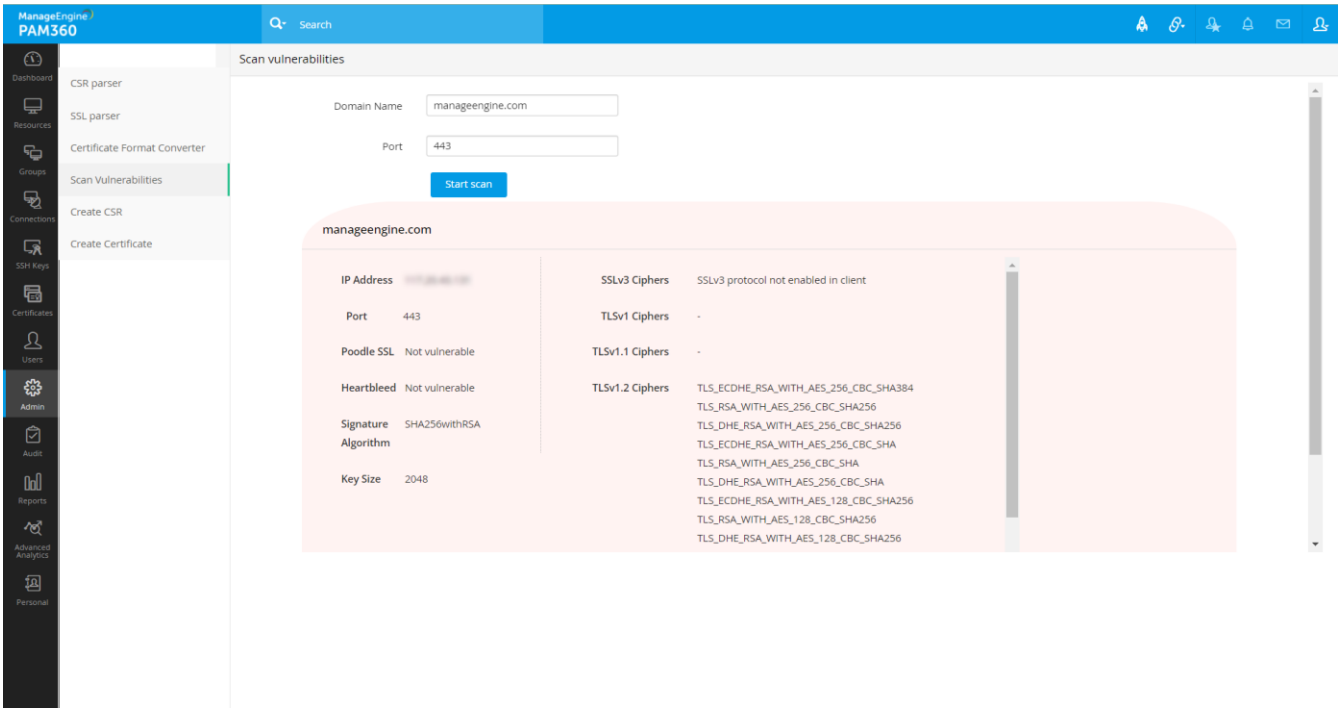
1. Navigate to **'Admin >> SSL Certificates >> Certificate Tools >> Certificate Format Converter'**.
2. Choose the required certificate format from the **Select Option** dropdown.
3. Click **Browse** to upload the certificate. Please note that while converting a certificate from and to the PKCS12 format, you must provide the import key and the keystore password. Upload your certificate, add the required attributes and click **Convert**; your

certificate will be converted to the selected destination format.



3. Scan Vulnerabilities

This scanner tool allows users to scan any domain for vulnerabilities by entering the domain name and port directly, without adding the certificate to the repository. Navigate to **'Admin >> SSL Certificates >> Certificate Tools >> Scan Vulnerabilities'** and enter the **Domain Name** and **Port** details. Once you have entered the domain details, click **Start scan**. The scan results will be displayed below.



4. Create CSR

To know about creating CSR, refer to this help section.

5. Create Certificate

To know about creating certificate, refer to this help section.

High Availability and Disaster Recovery Options

PAM360 provides a variety of high availability and disaster recovery options for various databases, allowing you to ensure operational continuity while maintaining uninterrupted access to your privileged enterprise information. Aside from high availability, PAM360 enables you to set up a failover service using MS-SQL server clusters and have a backup setup on standby in the event of a service interruption.

In the event of a catastrophic event that results in data loss, use the database backup and restore options to recover your data.

In addition to fail-safe options, PAM360 offers Application Scaling. The Application Scaling feature assists you in scaling your PAM360 setup across MS-SQL database clusters to improve accessibility and performance while ensuring continuous access to your privileged resources.

Click through the section inks listed below to learn in detail about each feature:

1. High Availability for PostgreSQL Database
2. High Availability for Microsoft SQL Server
3. How to Monitor High Availability using PAM360?
4. Read-Only Server
5. Failover Service for PAM360 using MS SQL Server Clusters
6. Database Backup using PostgreSQL
7. Database Backup using MS SQL
8. Data Restore Options
9. Application Scaling using the MS SQL Server

High Availability with PostgreSQL Database

Prerequisite

Make sure that the ports 3456 (the database port) and 8282 (the default webserver port) are open between the primary and the secondary application servers.

Setting up High Availability in the Server Running with PostgreSQL

The process of setting up High Availability in the Server running with PostgreSQL consists of four simple steps:

Step 1: Primary & Secondary Setup

You can use your current PAM360 installation as the Primary server and install another instance of PAM360 in a separate workstation as the Secondary server. During the installation of PAM360 as Secondary, you need to choose the option **Configure this server as High availability secondary server. After installation, the PAM360 Secondary server should not be started.**

Step 2: Create a Data Replication Pack for High Availability in Primary

1. Stop the Primary and Secondary Servers, if running. Ensure the postgres process of PAM360 is NOT running.
2. Open the command prompt and navigate to the **<PAM360_Primary_Installation_Folder>/bin** directory.
3. Run the script **HASetup.bat <FQDN of PAM360 Primary Server> <FQDN OF PAM360 Secondary Server > (Windows) / HASetup.sh <FQDN of PAM360 Primary Server> <FQDN OF PAM360 Secondary Server > (Linux).**

   To run this script, you need to pass the fully qualified domain names of the host where the PAM360 Primary and Secondary servers are installed as commandline arguments. For Example, if the Primary server is running at, say, **primary-server in the domain zohocorpin.com** and the Secondary server is running at, say, **secondary-server in the domain zohocorpin.com**, you need to execute the above script as follows:

   In Windows: *HASetup.bat primary-server.zohocorpin.com secondary-server.zohocorpin.com*

In Linux: sh HASetup.sh primary-server.zohocorpin.com secondary-server.zohocorpin.com

4. This will create a replication package named **HAPack.zip** under the **<PAM360_Primary_Installation_Folder>/replication** folder and contains the database package for the Secondary.
5. Copy the **HAPack.zip** and place it in the machine where the PAM360 Secondary installation is running, as detailed in Step 3 below.
6. Start the PAM360 Primary server.

Step 3: Place the HA Data Replication Pack in the Secondary

1. Place the **HAPack.zip** file, copied from the Primary Installation (as detailed in the previous step), in the <PAM360_Secondary_Installation_Folder> and unzip it.
2. Take care to extract the files under **<PAM360_Secondary_Installation_Folder>** only. It will overwrite the existing data files.

Step 4: Specify the Location of Encryption Master Key

After extracting **HAPack.zip** in the PAM360 Secondary server, navigate to the **/conf** folder, edit **manage_key.conf** and specify the location of the **pam360_key.key** (encryption master key).

> **Note**: PAM360 requires the **pam360_key.key** file to be accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

The High Availability configuration is ready now. To get it up and running, start the PAM360 Secondary server.

Important Notes:

By default, PAM360 comes with a self-signed SSL certificate. In case, you have overwritten it with a certificate signed by an internal CA (other than the prominent CAs like Verisign, Thawte, RapidSSL, etc) at the Secondary installation, you need to carry out the following additional steps to install the root certificate in the PAM360 primary server:

1. Stop Primary Server, if running.
2. Open a command prompt and navigate to the **<PAM360_Primary_Installation_Folder>/bin** directory.
3. Copy the Secondary server certificate and paste it under the **<PAM360_Primary_Installation_Folder>/bin** directory.
4. From the **<PAM360_Primary_Installation_Folder>/bin** directory, execute the following command:
   importCert.bat <name of the server certificate>
5. This adds the certificate to the PAM360 certificate store.

Now start the PAM360 Primary server.

See Also:

- Monitor High Availability Setup with PostgreSQL

High Availability for Microsoft SQL Server

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PAM360 provides the High Availability feature just to ensure this. While configuring High Availability (HA) for the setup running in Microsoft SQL (MS SQL) server, you need to carry out the replication between master and slave MS SQL databases. This can be done in two ways; from the SQL Server Management Studio and from PAM360. This document walks you through the process of configuring MS SQL server replication between the master and slave MS SQL databases using PAM360 itself.

There is another section, which discusses the same High Availability configuration for the MS SQL server, with the only difference that the replication between master and slave MS SQL databases is carried out using the Microsoft SQL Server Management Studio.

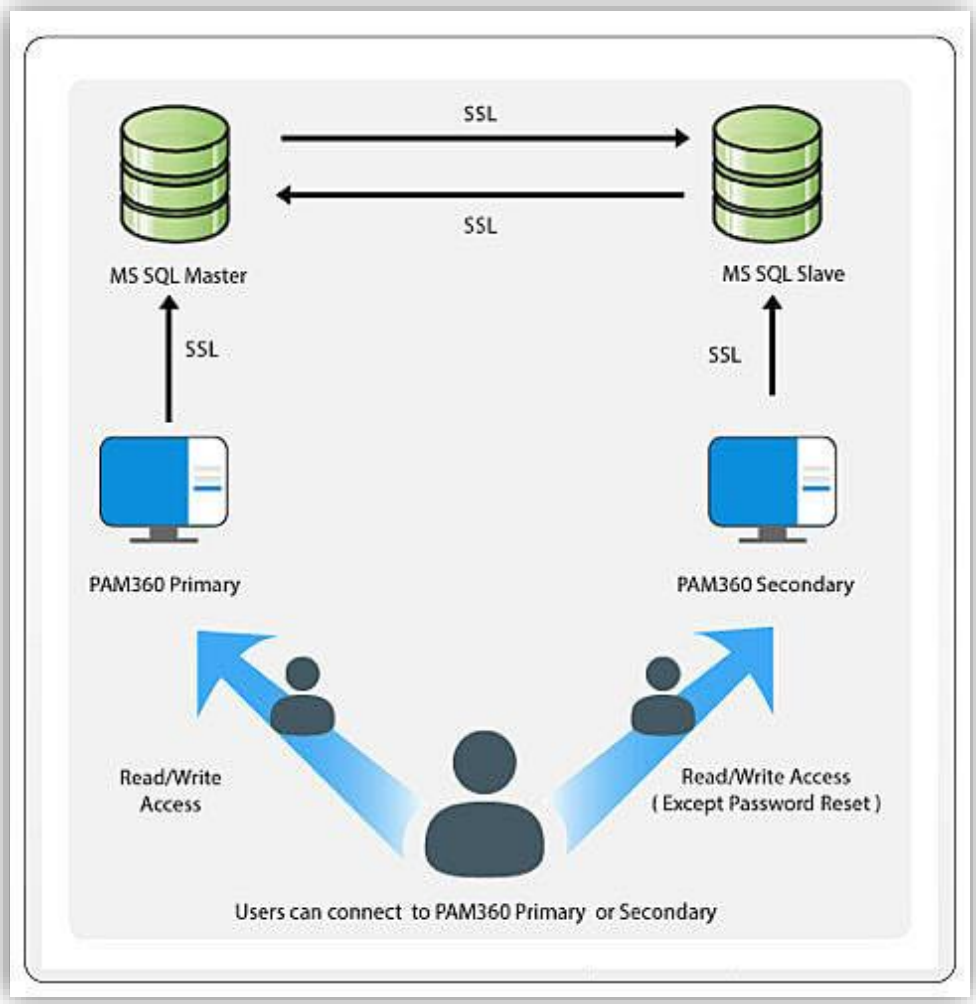
At the end of this section, you will have learnt the following topics with respect to configuring High Availability in a setup running with Microsoft SQL Server:

1. How does High Availability Work?
2. The High Availability Architecture in PAM360
3. Example Scenarios
    3.1 What happens to Audit Trails?
4. Setting up High Availability
    4.1 With Replication using PAM360
    4.2 With Replication using Microsoft SQL Server Management Studio
5. Verifying High Availability Setup

1. How does High Availability Work?

- There will be redundant PAM360 servers and database instances.
- One PAM360 instance will be the Primary, providing read/write access to the users. All users will be connected with the Primary only.
- The other instance will act as the Secondary.
- Data in both Primary and Secondary servers will always be in sync with each other.
- PAM360 leverages SQL server's data replication technique for data synchronization that happens through a secure, encrypted channel.
- When the Primary server goes down, the Secondary will offer 'Read/Write' access to the users (except password reset), until the fully-functional primary server is brought back to service. The changes made in the database in the intervening period will be automatically synchronized upon connection restoration.

2. The High Availability Architecture in PAM360



3. Example Scenarios

The HA architecture in PAM360 is designed to be compatible with two different scenarios. See the below table for a detailed explanation:

Scenario 1	
Hosting Primary & Secondary servers on the same network	The Secondary server is located on the same network, where the Primary server operates. The Secondary server is provided with the read/write access (except password reset action), in case of the Primary server failure.
Example	**Primary & Secondary within the same network & the Primary goes down:** Assume, the Primary and Secondary servers are deployed in the same geographical location, say 'A'. In the case when the Primary crashes or goes down, the users of both the Primary and Secondary servers will get

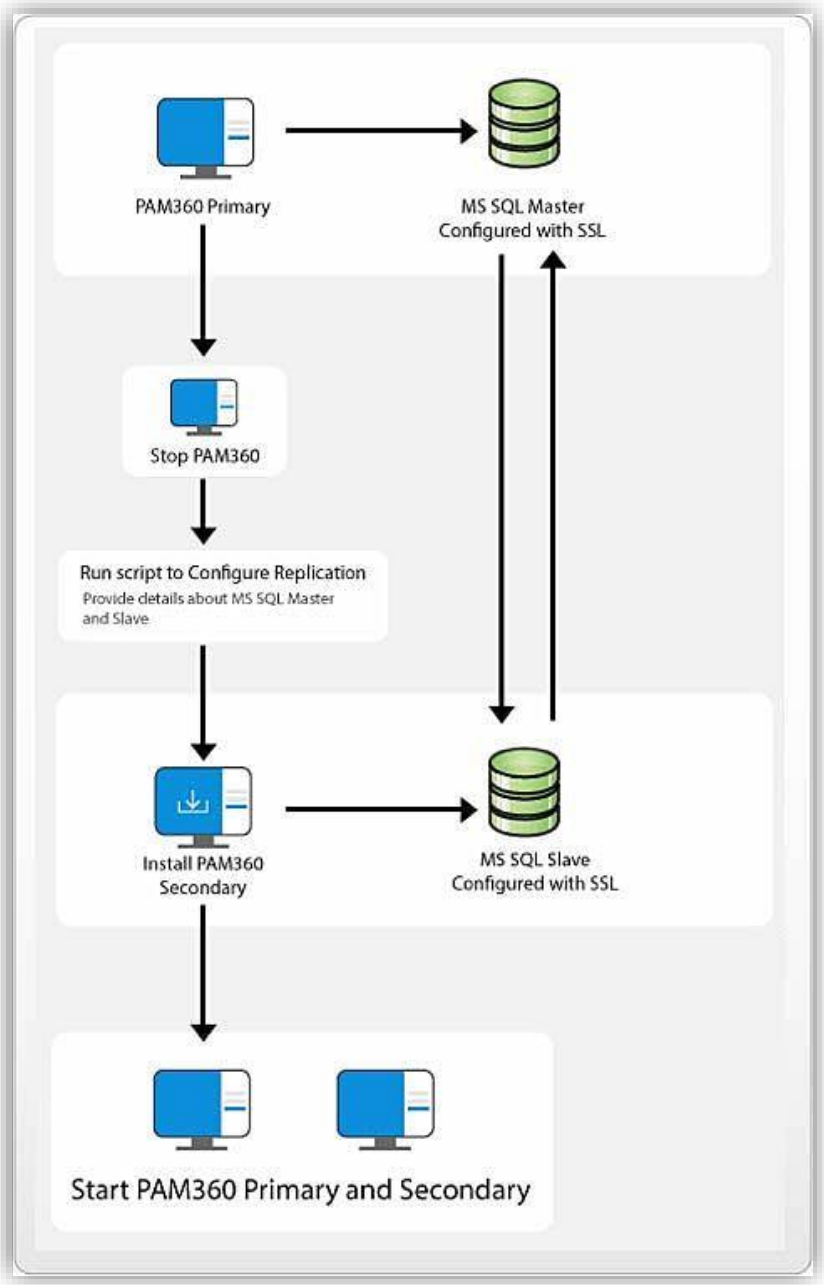
	the emergency access to the passwords from the Secondary.
Scenario 2	
Hosting Primary & Secondary servers on different networks	Primary and Secondary servers are located on different networks. The Secondary server in the remote network gets the read/write access (except password reset action), in case of a WAN link failure or Primary server failure.
Example	**Primary & Secondary in different geographical locations and WAN Link failure happens between the locations:** Assume, the Primary server is in a geographical location 'A' and the Secondary server is deployed in another location 'B'. By default, the users in both 'A' and 'B' will be connected to the Primary and will be carrying out the routine password management activities. The data in both the Primary and Secondary are in sync with each other. Now, imagine, there happens a network connectivity loss between the two locations. In such a situation, the two servers will start operating independently. Thus, the users in location 'A' will remain connected with the Primary server and will be carrying out their operations as usual. On the other hand, the users in location 'B' will get emergency access to the passwords from the Secondary server. Once the connection is re-established between 'A' and 'B', the data in both the locations will be synchronized.

3.1 What happens to Audit Trails?

In the high availability scenarios mentioned above, audit trails will be recorded as usual. In scenario 2, as long as there is network connectivity between the two locations, the audit trails will be printed by the primary. When users connect to the Secondary, it will print operations such as 'password retrieval', 'login' and 'logout'. When the two locations get back network connectivity, the audit data will be synchronized. In scenario 1, when the primary crashes, the 'password retrieval', 'login' and 'logout' done by the users in secondary will be audited. Other audit records will already be in sync at the Standby

4. Setting up High Availability - With Replication using PAM360

Pictorial Representation of How the High Availability Works:



Steps Required

Step 1:

- Stop primary server, if running

Step 2:

- The MS SQL server, which is used by the PAM360 primary server, will act as the Master database. You should now specify another instance of MSSQL as slave database. Then, you need to import the SSL certificate of MS SQL server slave database into PAM360 Primary server. **Before proceeding with this step, ensure that the MS SQL slave server is**

also configured with SSL. You can do this by carrying out Steps 1, 2, 3 in this document.

To import the SSL certificate of slave SQL server into PAM360 Primary:

- Navigate to **<PAM360 Primary Installation Folder>/bin** directory and execute the command **importCert.bat** <**slavecert**.cer >

Step 3:

- Navigate to **<PAM360 Primary Installation Folder>/conf** directory, open the file masterkey.key and copy the SQL **Master Key**. You will use this in the next step. (In case, you have moved this key to a secure location as recommended while integration SQL server, keep the key ready for use in the next step).

Step 4:

You need to configure MS SQL server replication between master and slave MS SQL databases.

- Navigate to **<PAM360 Primary Installation Folder>/bin** directory and execute the command **ConfigureReplication.bat** (in Windows) or **sh ConfigureReplication.sh** (Linux)
- Specify the details about Master and Slave databases and other details as required

Under Master Database details, provide the following details:

1. **Master Host Name:** The name or the IP address of the machine where MS SQL server is installed.
2. **Instance Name:** Helps to specify the named instance of SQL server, which has to be used for PAM360. If instance name is not specified, PAM360 will try establishing connection with the default instance on port 1433.

   Since PAM360 connects to MS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.
3. **User Name and Password:** Specify the user name and password with which PAM360 needs to connect to the database. (You need to specify the username having SQL role as sysadmin. PAM360 does not store this username and password anywhere. It is just used for carrying out some queries while configuring replication between MS SQL master and slave servers).
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as **<domain-name>\<username>**
4. **Master Database Name:** Name of the PAM360 database.
5. **Master Key:** Paste the master key copies in Step 3 above.

Under Slave Database details, provide the following details:

1. **Slave Host Name:** The name or the IP address of the machine where MS SQL server is installed.
2. **Instance Name:** Helps to specify the named instance of SQL server, which has to be used for PAM360. If instance name is not specified, PAM360 will try establishing connection with the default instance on port 1433.

   Since PAM360 connects to MS SQL only in SSL mode, it is recommended that you create a dedicated database instance running in a specific port for PAM360. If you want to specify a port number other than 1433, you can specify it in the Host Name parameter above as **<hostname>:<port>**.
3. **User Name and Password:** Specify the user name and password with which PAM360 needs to connect to the database. (You need to specify the username having SQL role as sysadmin. PAM360 does not store this username and password anywhere. It is just used for carrying out some queries while configuring replication between MS SQL master and slave servers).
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as **<domain-name>\<username>**
4. **Slave Database Name:** Name of the PAM360 database. Default is "pam360standby". (If you have chosen the option **'Custom'** for **"Encryption Key"** while configuring ChangeDB.bat for Primary server, you need to create a new database for slave, create Master Key, create Certificate and Create the Symmetric Key using AES 256 encryption. You need to mention the slave database name here.)
5. Click "Test & Configure" to complete replication. **This process will take about 30 minutes or more.**

Step 5:

Start the primary server

Step 6:

Install another instance of PAM360 as secondary server in a separate workstation. To install PAM360 as secondary, during installation process, you need to choose the option **"Configure this server as High availability secondary server (Read Only)". After installation, the PAM360 Secondary server should not be started**.

Step 7:

After installing the PAM360 secondary server, you need to change it to run with MS SQL by carrying out the following:

Execute ChangeDB.bat

Now, you need to provide the details about the SQL server to PAM360 by editing the file **<PAM360 Standby Installation Folder>/bin ChangeDB.bat** (Windows) or **<PAM360 Standby Installation Folder>/bin sh ChangeDB.sh** (Linux)

Select SQL Server and enter other values

1. **Host Name of Slave Database:** The name or the IP address of the machine where MS SQL server is installed.
2. **Port:** The port number in which PAM360 must connect with the database. Default is 1433.
3. **Database Name:** Name of the Slave database. Here, take care to specify the name of the slave database exactly as done in Step 4 above.
4. **Authentication:** The way in which you would like to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single Sign On facility provided PAM360 service is running with a service account, which has the privilege to connect to SQL server. In that case, choose the option "Windows". Otherwise, select the option "SQL". **It is recommended to choose the option 'Windows' as the username and password used for authentication are not stored anywhere.**
5. **User Name and Password:** If you have selected the option "SQL", specify the user name and password with which PAM360 needs to connect to the database. **The username and password entered here will be stored in PAM360. So, you need to take care of hardening the host.**
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, you need to enter the username as <domain-name>\<username>
6. **Encryption Key:** The key with which your data is to be encrypted and stored in the SQL server. You may either leave it "Default" making PAM360 to generate a key. If you have configured Master database with custom key, you need to choose 'Custom' here also.
7. **If you have selected the option "Custom:"** After doing the above, you need to provide certificate name and symmetric key name in the GUI as mentioned in Master database
8. Click Test and then Save.

Step 8:

To carry PAM360 license, custom icons and rebranding settings, if any, from Primary to Secondary, go to \replication directory and copy **SQLServerHAPack.zip**. Put this zip file copied from the PRIMARY Installation to the **<PAM360_Secondary_Installation_Folder>**and unzip it. **Take care to extract the files under <PAM360_Secondary_Installation_Folder> only. It will overwrite the existing files. This SHOULD NOT be unzipped under <PAM360_Secondary_Installation_Folder>/SQLServerHAPack directory.**

Step 9:

After extracting SQLServerHAPack.zip in PAM360 Secondary Server, navigate to **<PAM360_Secondary_Installation_Folder>/conf** folder, edit **manage_key.conf** and specify the location of **pam360_key.key** (encryption master key). Then, start PAM360 Secondary Server. PAM360 requires the pam360_key.key file accessible with its full path when it starts up every time. After a successful start up, it does not need the key anymore and so the device with the key file can be taken offline.

5. Verify High Availability Setup

After carrying out the above steps, you can verify if the High Availability setup is working properly by looking at the message under **Admin >> General >> High Availability** of primary or secondary server. If the setup is proper, you will see the following status message:

High Availability Status: Alive

It indicates that high availability is working fine. In case, if the status turns 'Failed', it indicates failure of the setup.

High Availability for MS SQL with Replication using SQL Server Management Studio

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PAM360 provides the High Availability feature just to ensure this. While configuring High Availability (HA) for the setup running in Microsoft SQL (MS SQL) server, you can carry out the replication between master and slave MS SQL databases using the MS SQL Server Management Studio. The above section, which discusses the same High Availability configuration for the MS SQL server, with the only difference that the replication between master and slave MS SQL databases is carried out using PAM360 itself.

Steps Required

Step 1:

Stop the primary server, if running.

Step 2:

The MS SQL server, which is used by the PAM360 primary server, will act as the Master database. You need to specify another instance of MSSQL as the slave database. Then, import the SSL certificate of MS SQL server slave database into the PAM360 primary server. **Before proceeding with this step, ensure that the MS SQL slave server is also configured with SSL**. You can do this by carrying out these steps.

To import the SSL certificate of slave SQL server into the PAM360 primary:

Navigate to **<PAM360 Primary Installation Folder>/bin** directory and execute the command **importCert.bat** <**slavecert**.cer >.

Step 3:

Navigate to **<PAM360 Primary Installation Folder>/conf** directory, open the file **masterkey.key** and copy the **SQL Master Key**. You will use this in the next step. (In case, you have moved this key to a secure location as recommended while integrating the SQL server, keep the key ready for use in the next step).

Step 4:

Configure MS SQL server replication between the master and slave MS SQL databases.

Prerequisites:

1. Ensure that MS SQL Server Management Studio is installed in your system.

2. Verify if replication is installed on the instance of the MS SQL server. Only then, the Microsoft SQL Server Management Studio will be able to access the replication components.

3. Before you configure the SQL server replication in the secondary server, create a database and execute the below mentioned queries:

i. *CREATE TABLE SeqGenState (ROWGUID UNIQUEIDENTIFIER ROWGUIDCOL UNIQUE DEFAULT NEWSEQUENTIALID(), SEQNAME VARCHAR(100) NOT NULL, CURRENTBATCHEND BIGINT NOT NULL, CONSTRAINT SeqGenState_PK PRIMARY KEY CLUSTERED (SEQNAME));*

ii. *CREATE TABLE Ptrx_ResGrpNotifyActionList (ROWGUID UNIQUEIDENTIFIER ROWGUIDCOL UNIQUE DEFAULT NEWSEQUENTIALID(), NOTIFY_ID BIGINT, ACCOUNT_ID BIGINT NOT NULL, ACTION_TYPE VARCHAR(200), SHARECHANGEUSER_ID VARCHAR(1000), OPERATED_NAME VARCHAR(300), OPERATED_TIME DATETIME, IPADDRESS VARCHAR(255), PRIMARY KEY CLUSTERED (NOTIFY_ID));*

iii. *CREATE TABLE "MSPSeqGenState" (ROWGUID UNIQUEIDENTIFIER ROWGUIDCOL UNIQUE DEFAULT NEWSEQUENTIALID(), "ORGANIZATIONID" BIGINT NOT NULL, "SEQNAME" NVARCHAR(100) NOT NULL, "CURRENTBATCHEND" BIGINT NOT NULL, CONSTRAINT "MSPSeqGenState_PK" PRIMARY KEY CLUSTERED ("ORGANIZATIONID", "SEQNAME"));*

1. Configuring SQL Server Replication

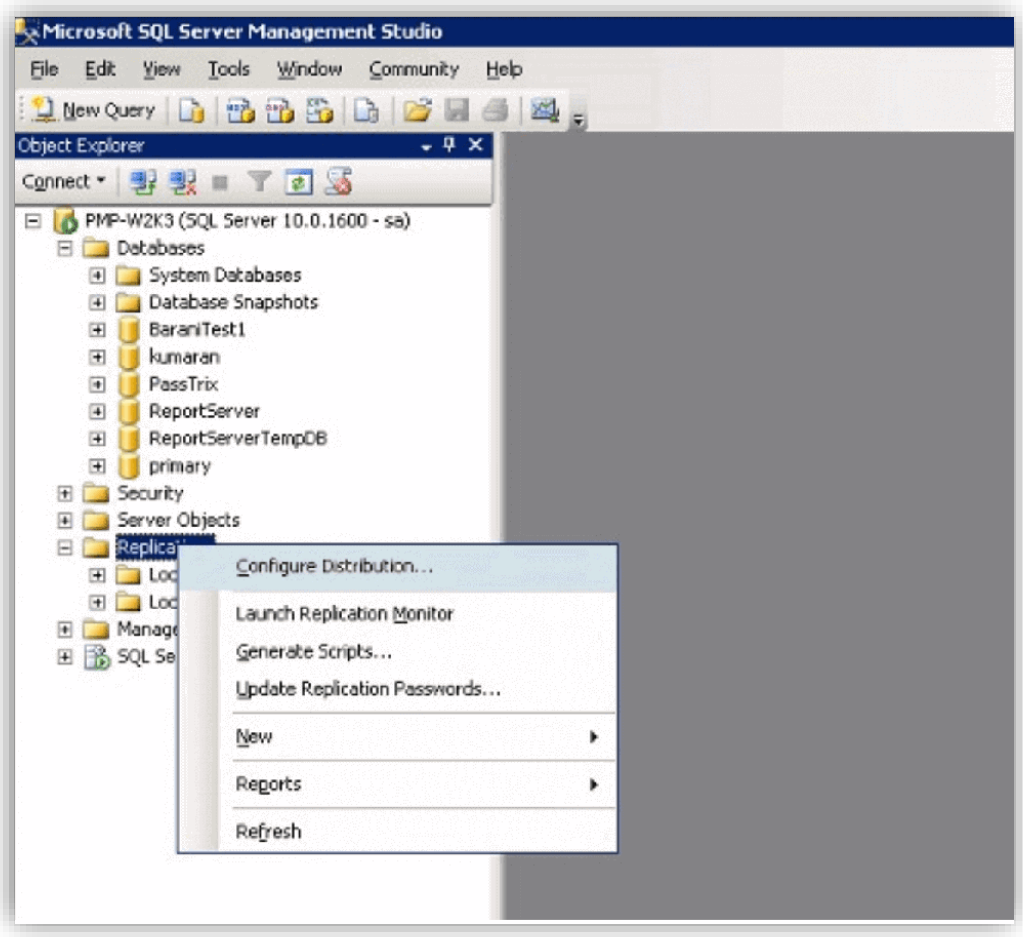
Launch the MS SQL Server Management Studio. The configuration steps are split into three parts for clear understanding.

Points to Remember:

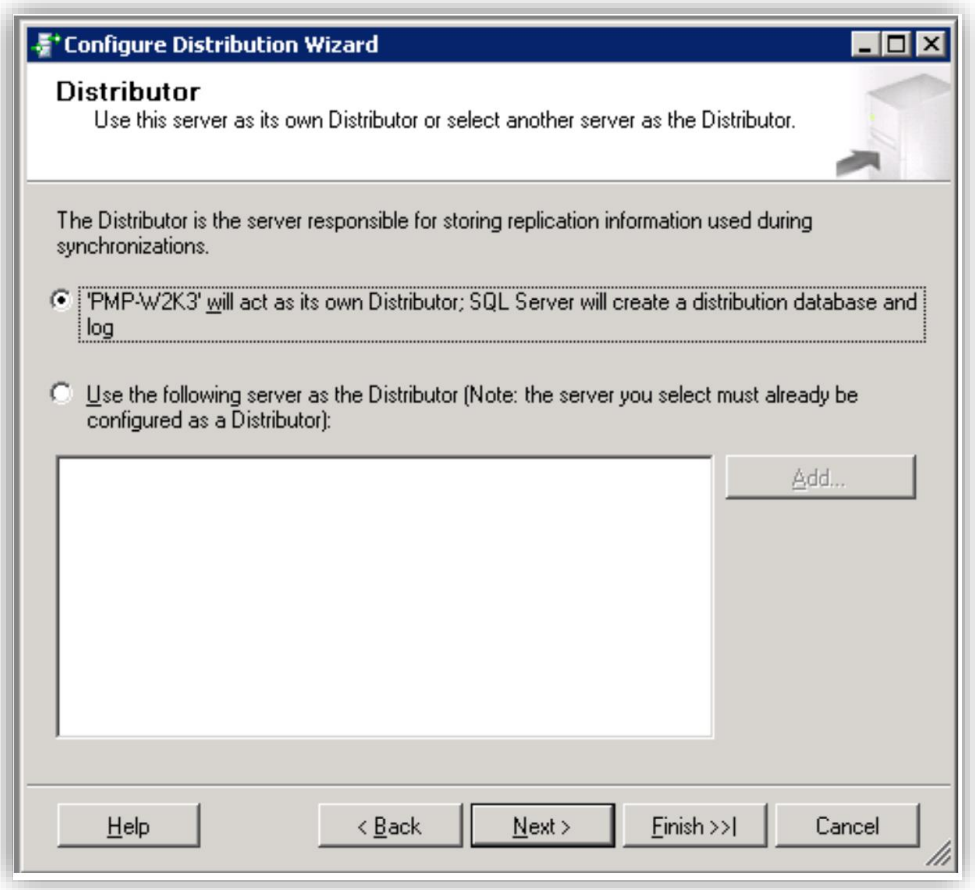
- Read the instructions carefully in each wizard before you click Next.
- Click Finish only when the complete replication process is over. Clicking Finish in the middle of the process would result in a broken or incomplete configuration.
- Click Cancel anytime to abort the configuration process.

Part I - Create Distribution:

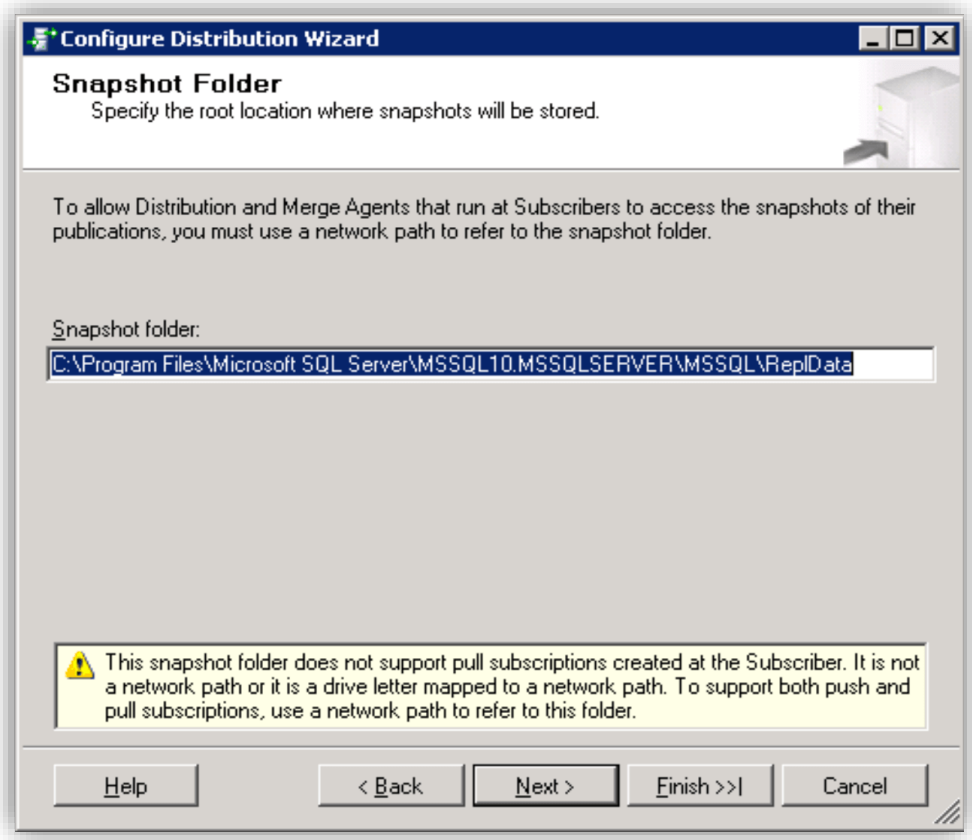
1. Under the **Object Explorer**, right-click on **Replication** and click **Configure Distribution.**



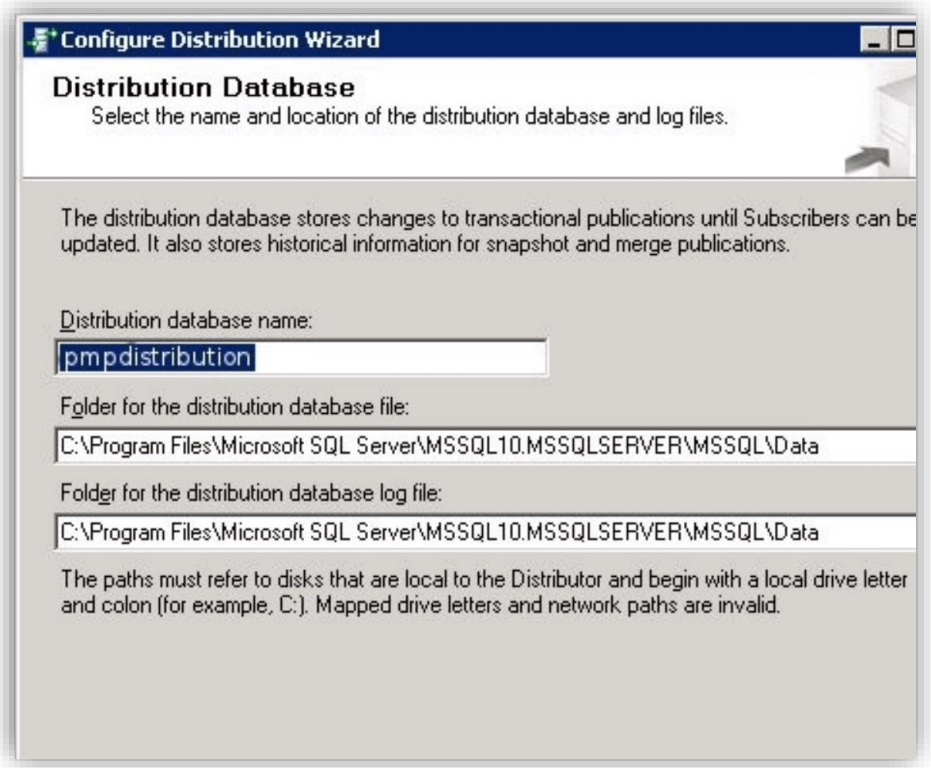
2. In the **Configure Distribution Wizard** displayed, choose the first option, i.e., choose to use this server itself as its own distributor, as shown in the below screenshot. Click **Next**.



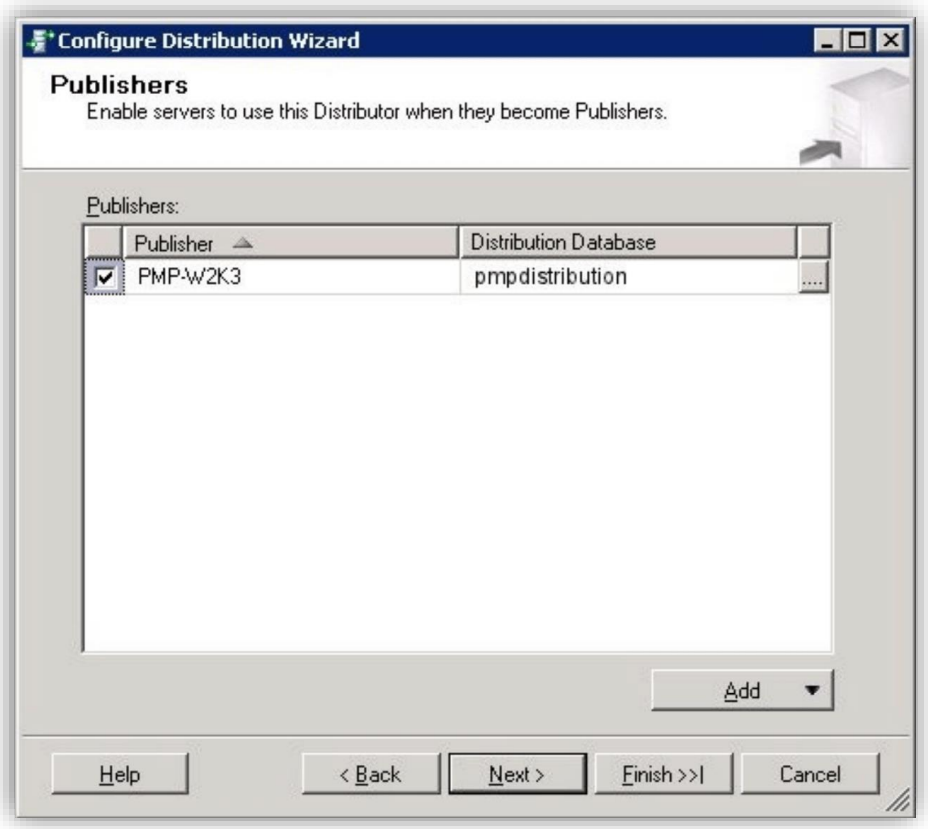
3. Specify the root folder, where you want the snapshots to be stored. Click **Next**.



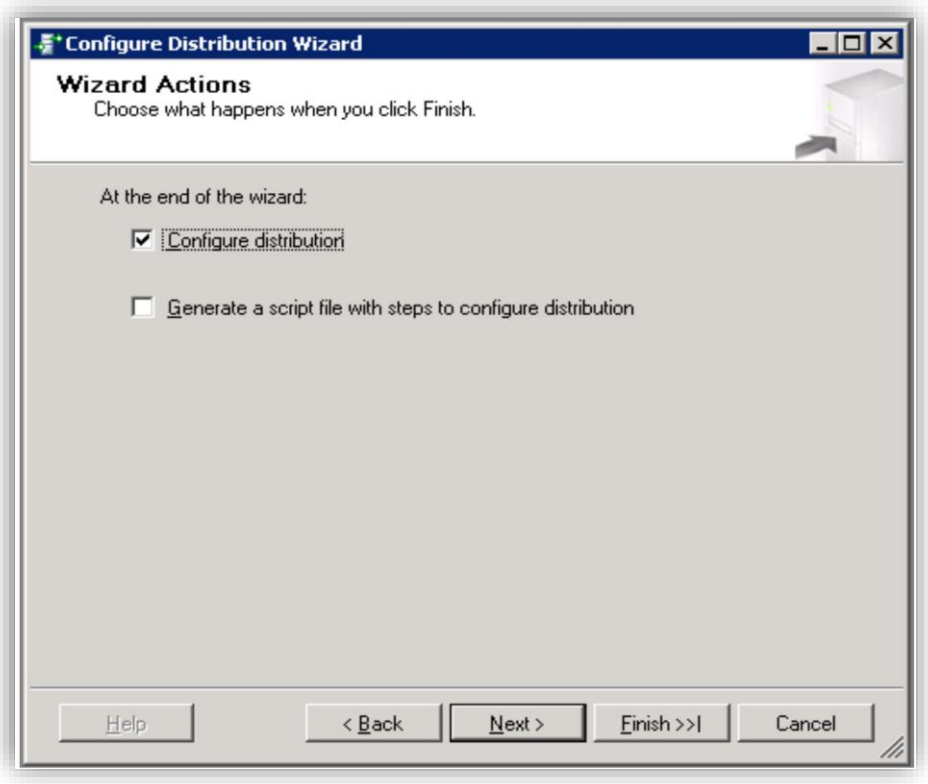
4. Specify a **name** for the distribution. Choose the **folders** where you want the distribution database file and log file, respectively. Click **Next**.



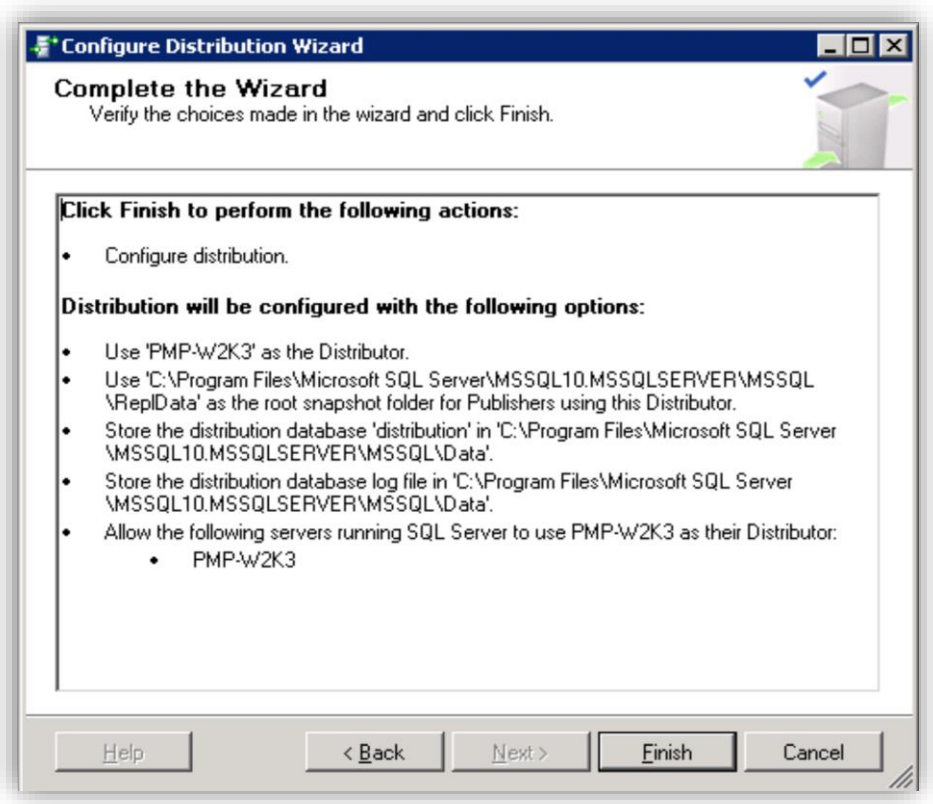
5. Select the **server(s)** which this distributor will use when they become the publishers.



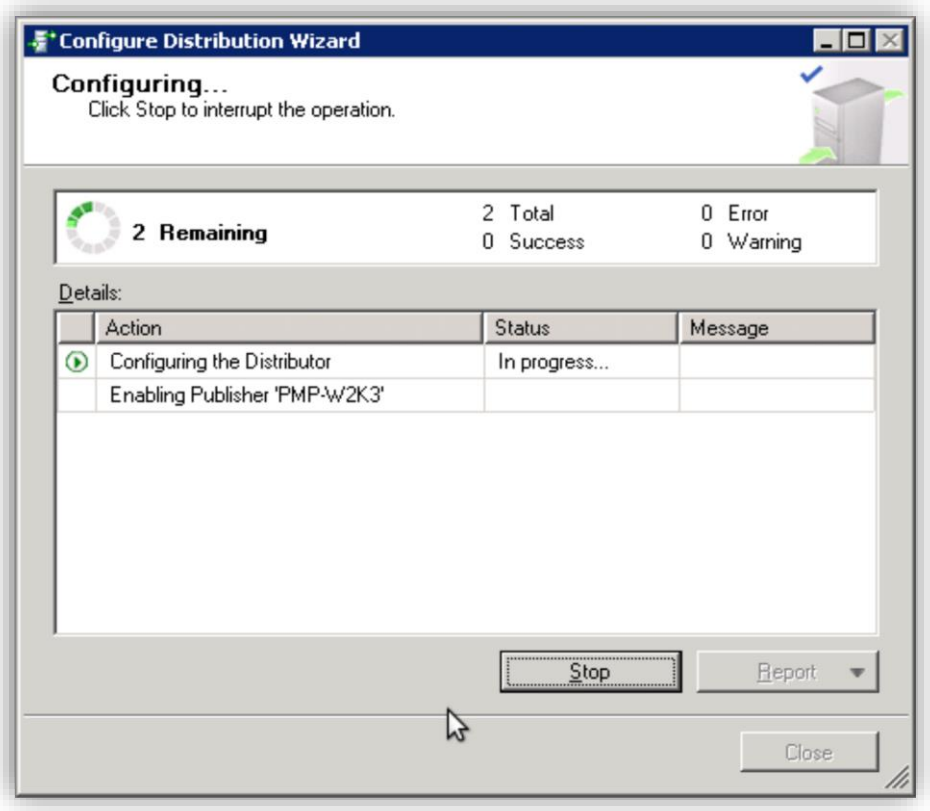
6. Select what you wish to happen when you quit this wizard. You can either choose to **Configure Distribution** or **Generate a scrip file**, or **both**. Click **Next**.



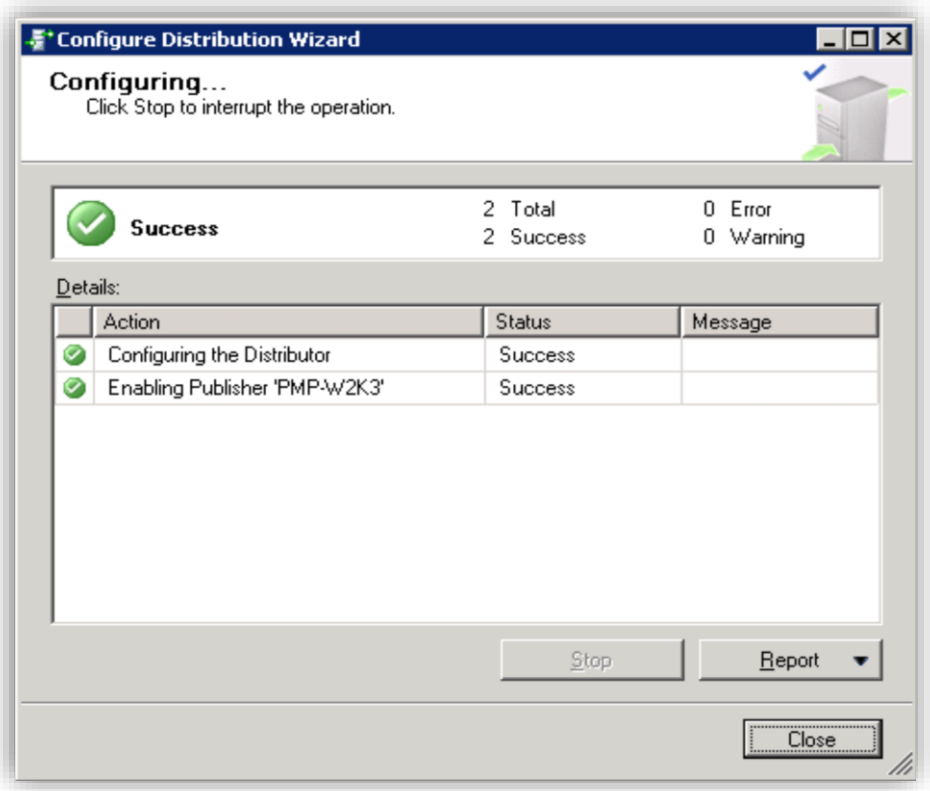
7. Click **Finish** to complete the process or click **Back** to verify the options you have chosen in the previous screens. To know in detail on what happens after you close this wizard, see the below screenshot.



8. Once you click **Finish**, you will see the configuration processing as shown in the below screenshot. Click **Stop** if you want to stop configuring the distribution.

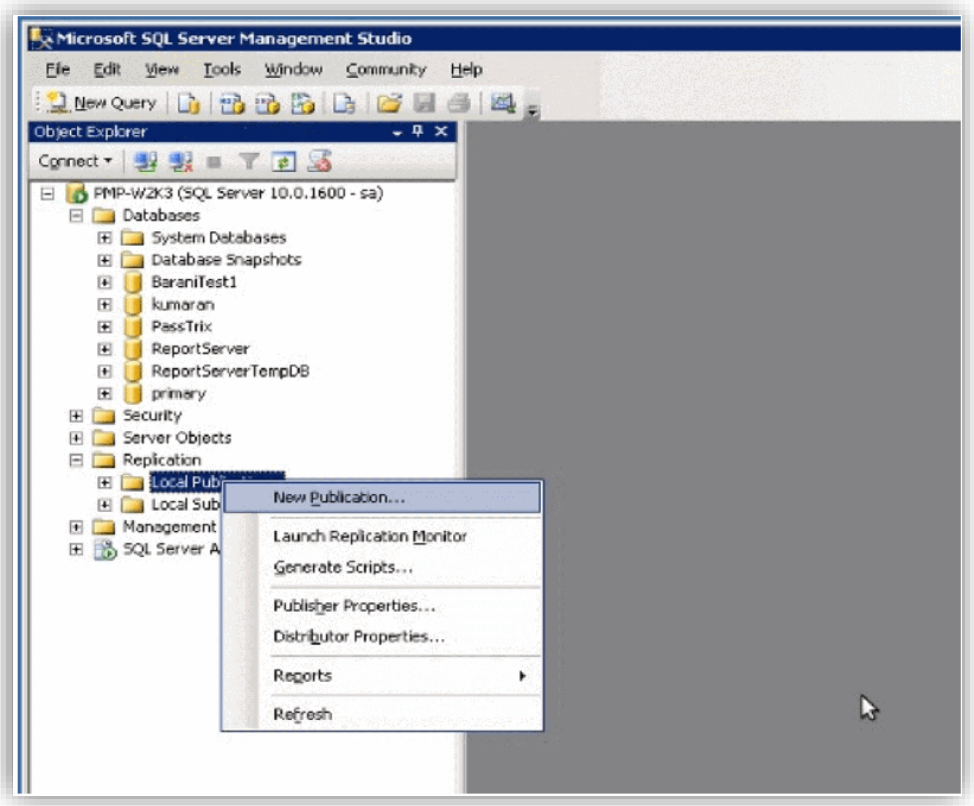


9. **Close** the window one you see the **Success** message as shown in the below screenshot.

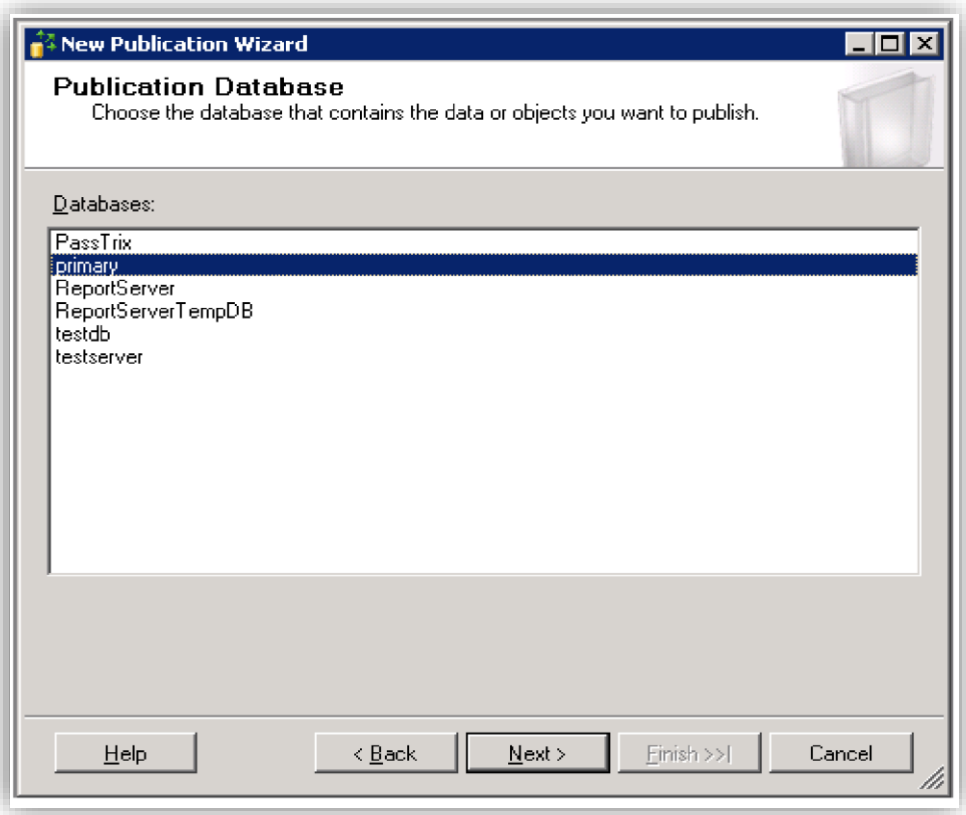


Part II - Create Publication:

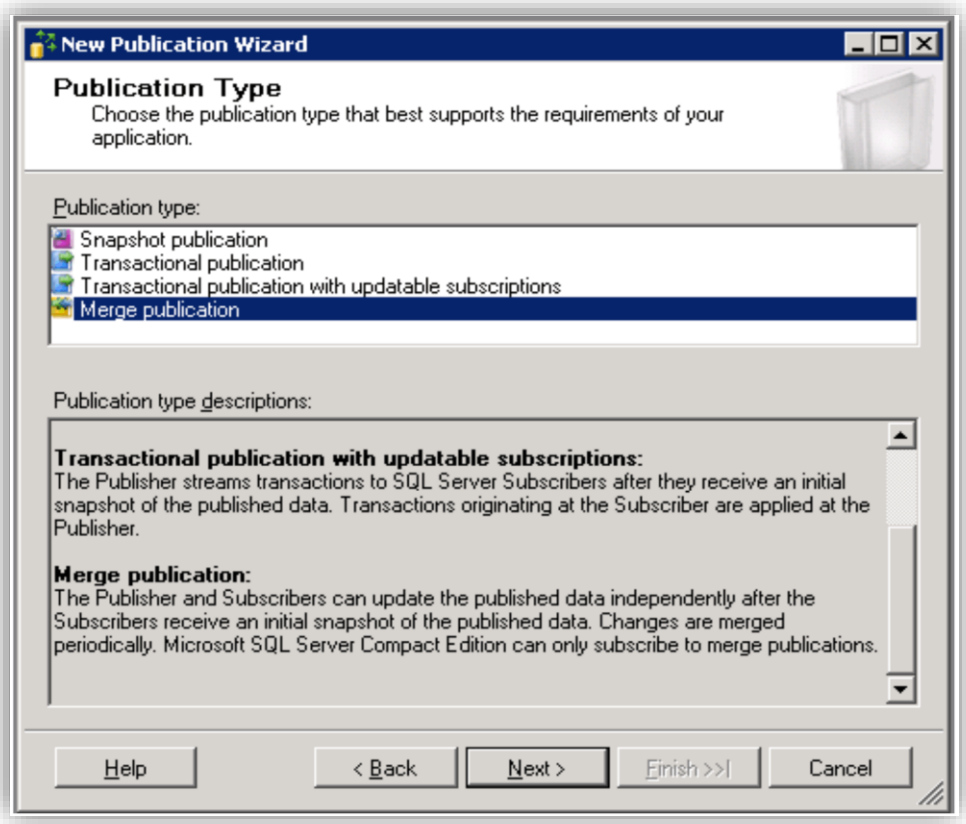
1. Under the **Object Explorer**, under **Replication**, right-click on **Local Publication** and then click **New Publication**.



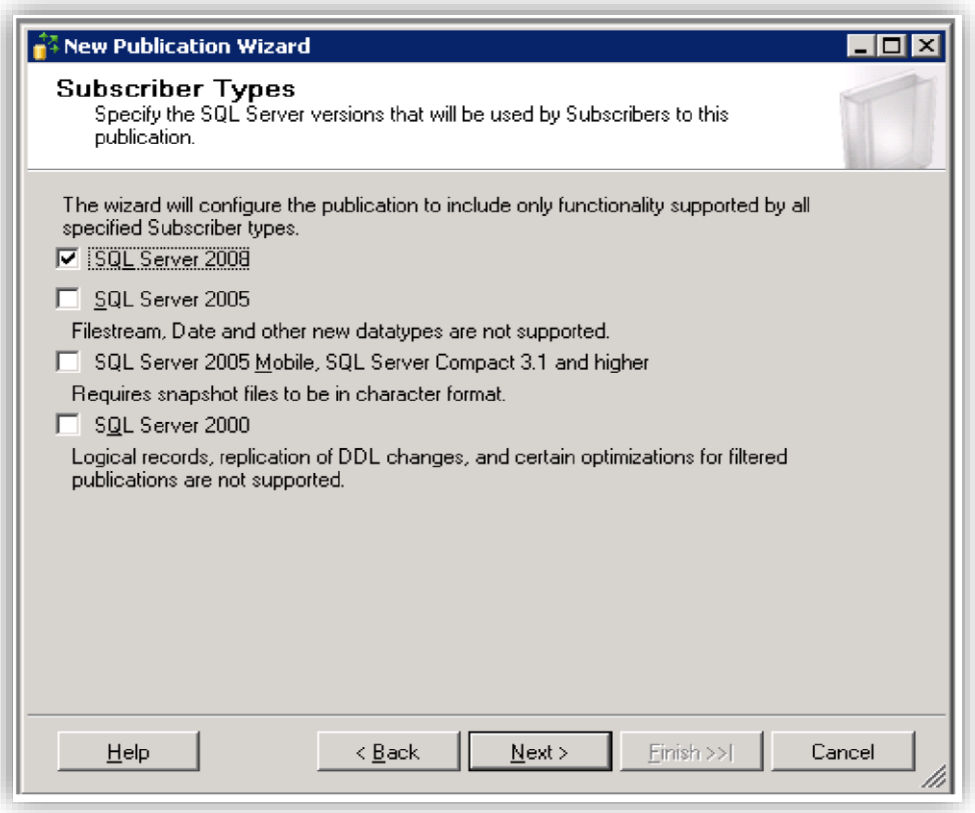
2. In the **New Publication Wizard** displayed, choose the **primary database** that contains the data and objects to be published. Click **Next**.



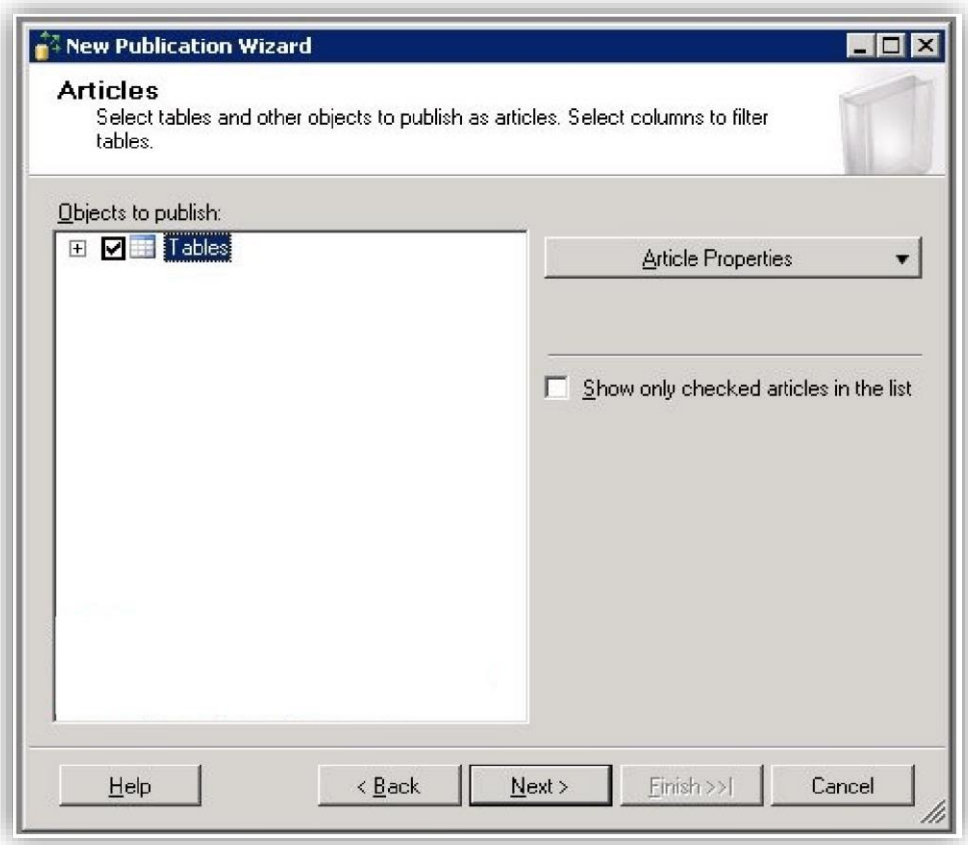
3. Choose the **Publication Type** as **Merge Publication**. Make sure, the publication type you choose is compatible with your application requirements. Click **Next**.



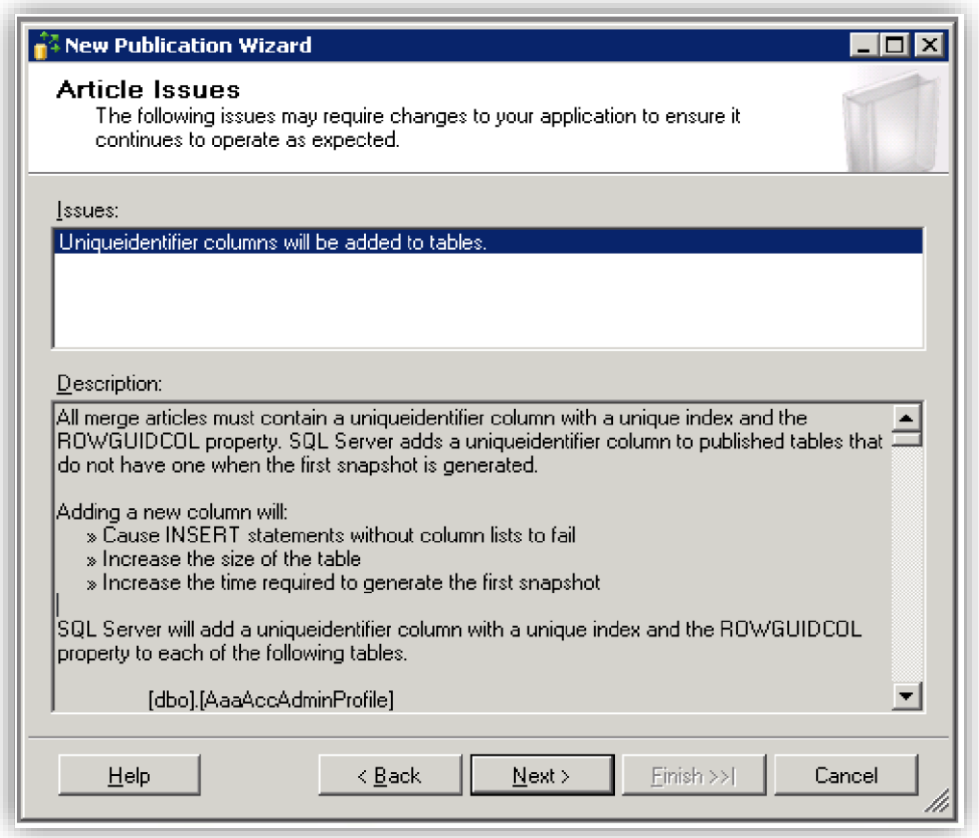
4. Select the **Subscriber Type** as **SQL Server 2008** to be used by the subscribers to this publication. Click **Next**.



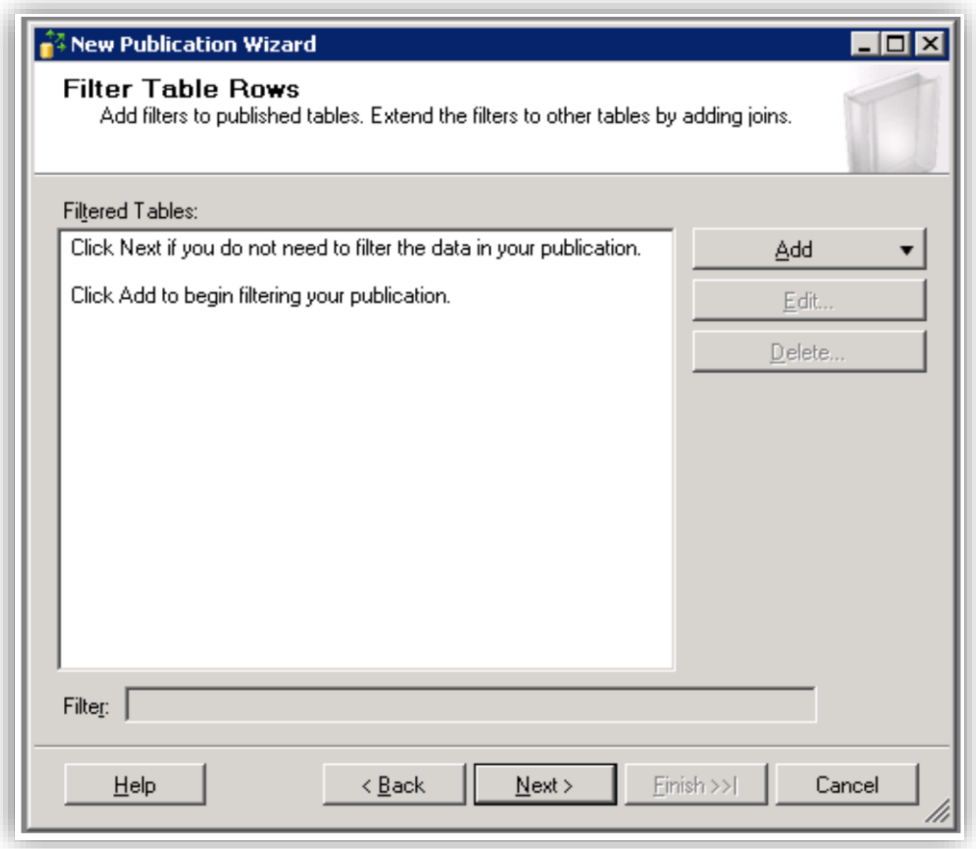
5. Next step is to select tables to be published as articles and click **Next**. Select all the tables except the below ones:
    i. **SeqGenState**
    ii. **Ptrx_ResGrpNotifyActionList**
    iii. **MSPSeqGenState**



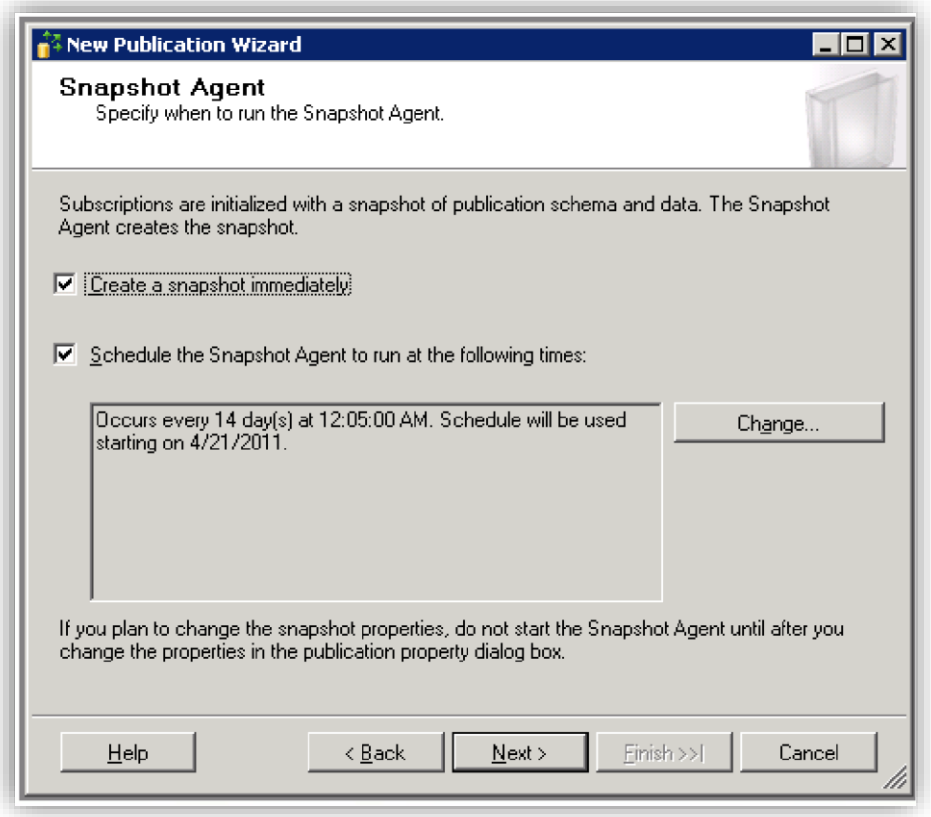
6. Select the **issue** displayed in the screen that may require changes to your application so that it continues to function as expected. Click **Next**.



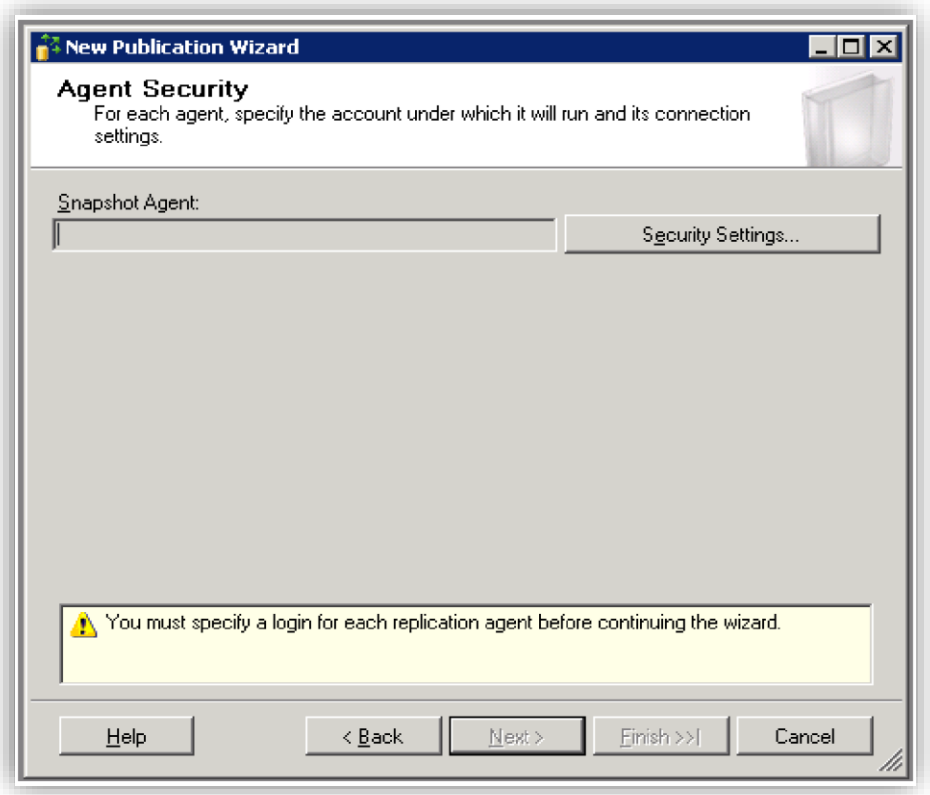
7. This step allows you to **filter table rows**. Click **Add** to start adding filters to your publication, Click **Next**, if you do not want to filter the data in your application.



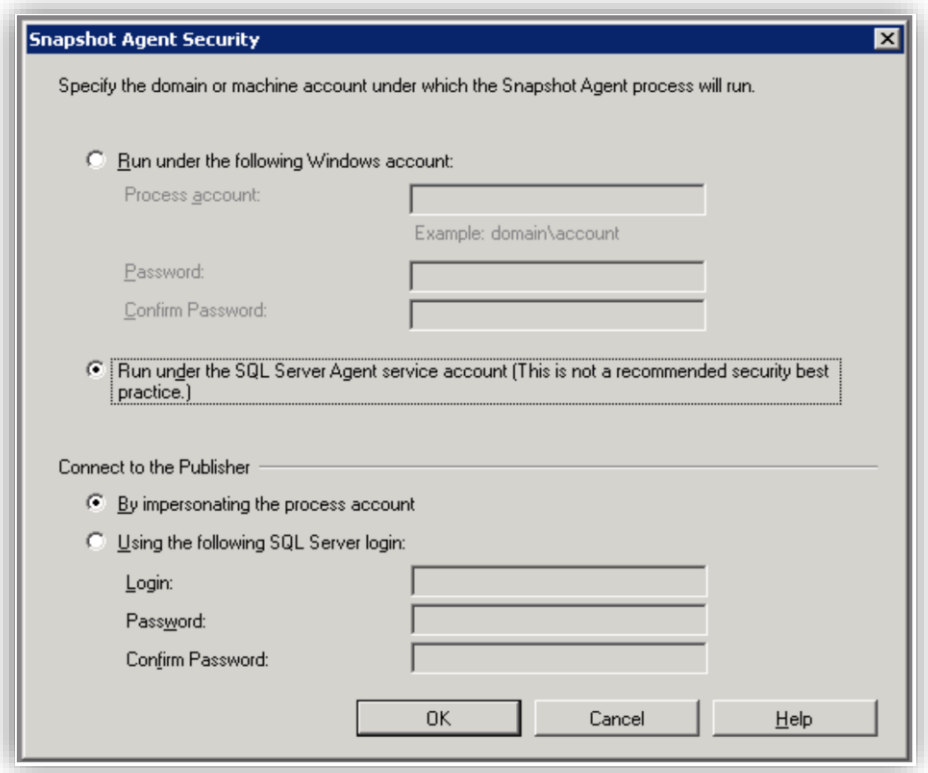
8. Select whether to run the **Snapshot Agent i**mmediately, or schedule the agent to run at the specified day/time. Click **Next**.



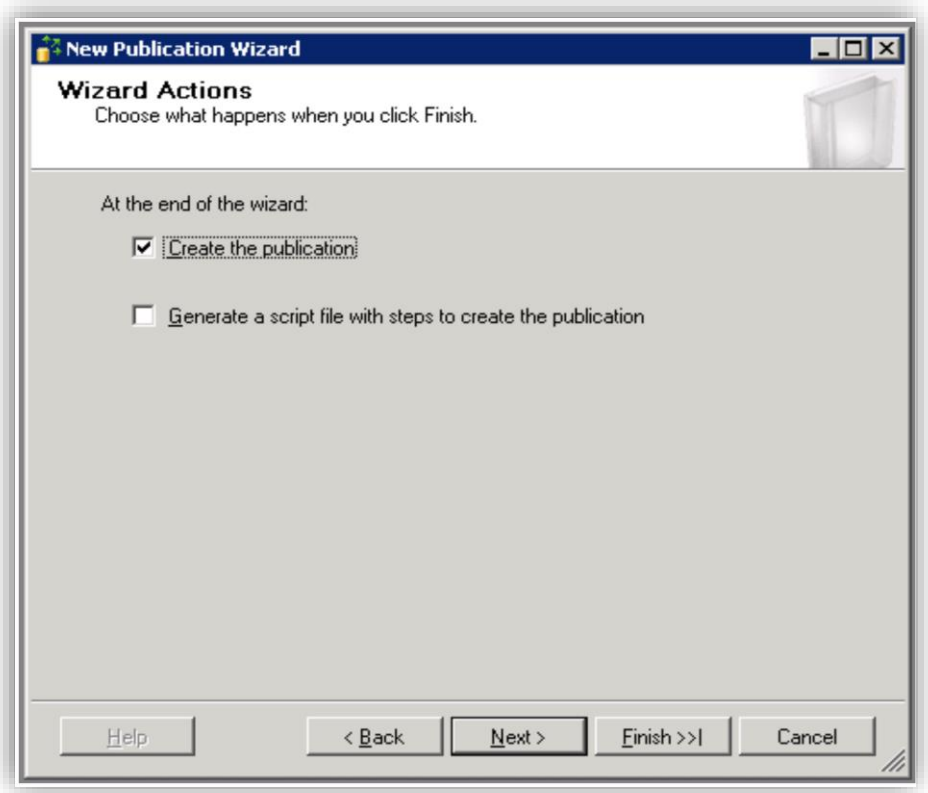
9. **[Mandatory]** Specify the **Account** name for the agent to run, and its **Connection Settings**. Click **Next**.



10. This is the step where you choose the domain or machine account, where the Snapshot Agent will run. Choose the option "**Run under the SQL Server Agent service account".** Also, choose the method "**By impersonating the process account**" to connect to the publisher. Click **OK**.

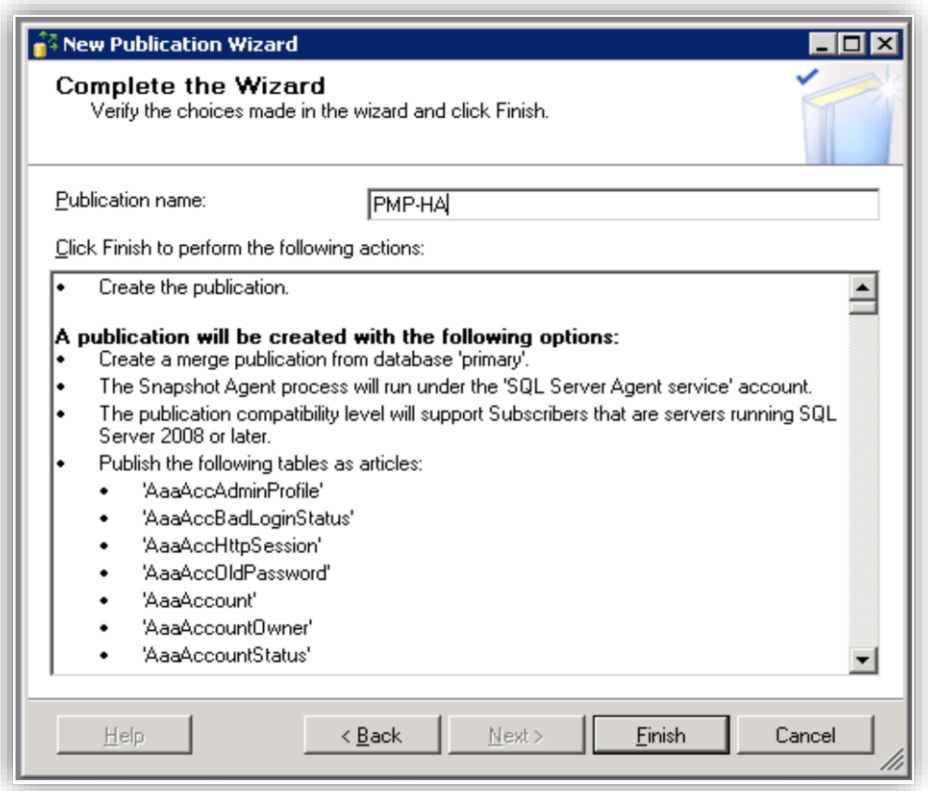


11. Select what you wish to happen when you quit this wizard. You can either choose to **Create the Publication** or **Generate a scrip file**, or **both**. Click **Next.**

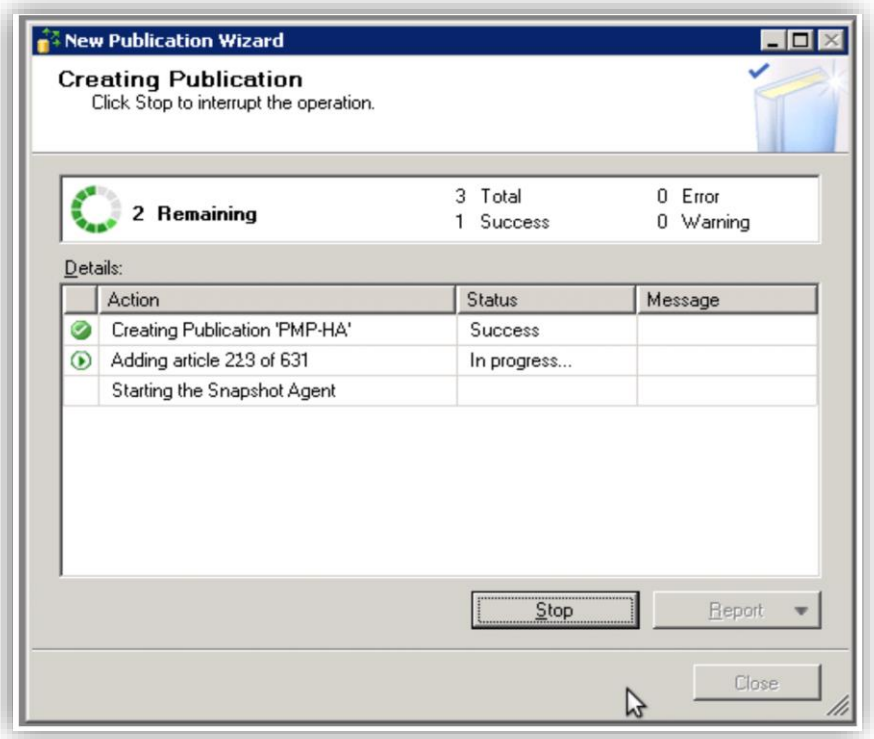


12. Specify the **Publication name**. Click **Finish** to complete the process or click **Back** to verify

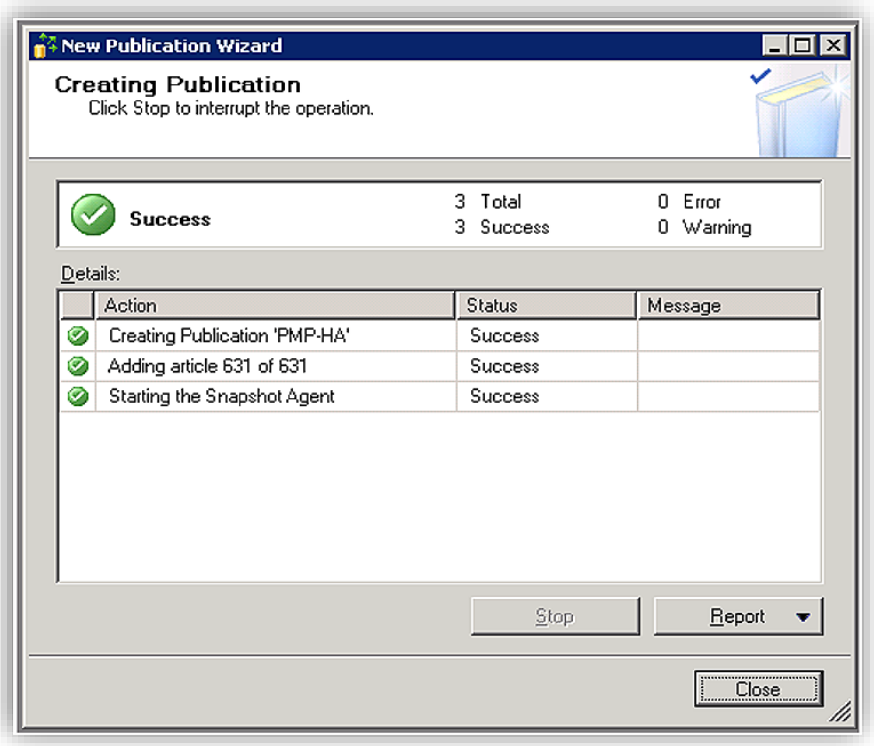
the options you have chosen in the previous screens. To know in detail on what happens after you close this wizard, see the below screenshot.



13. Once you click **Finish**, you will see the publication being created as shown in the below screenshot. Click **Stop** if you want to stop creating the publication.

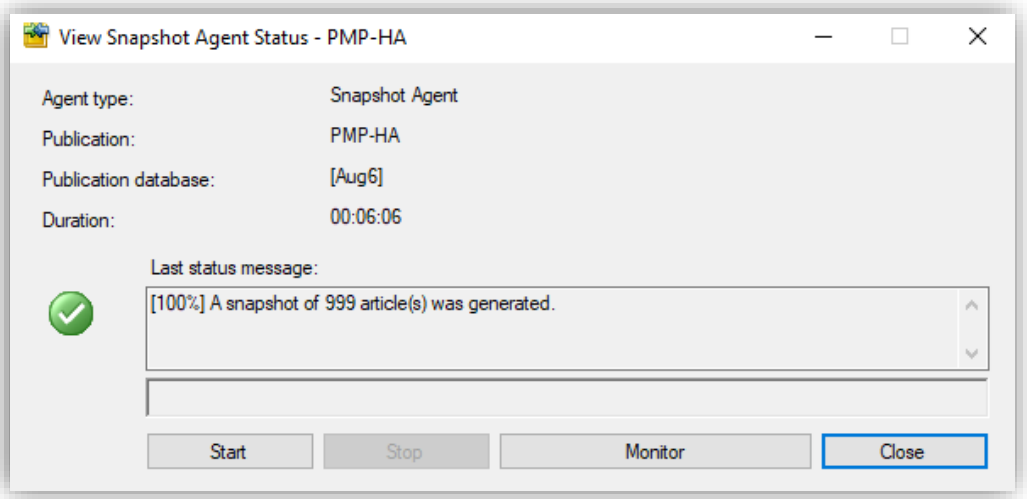


14. **Close** the window one you see the **Success** message as shown in the below screenshot.



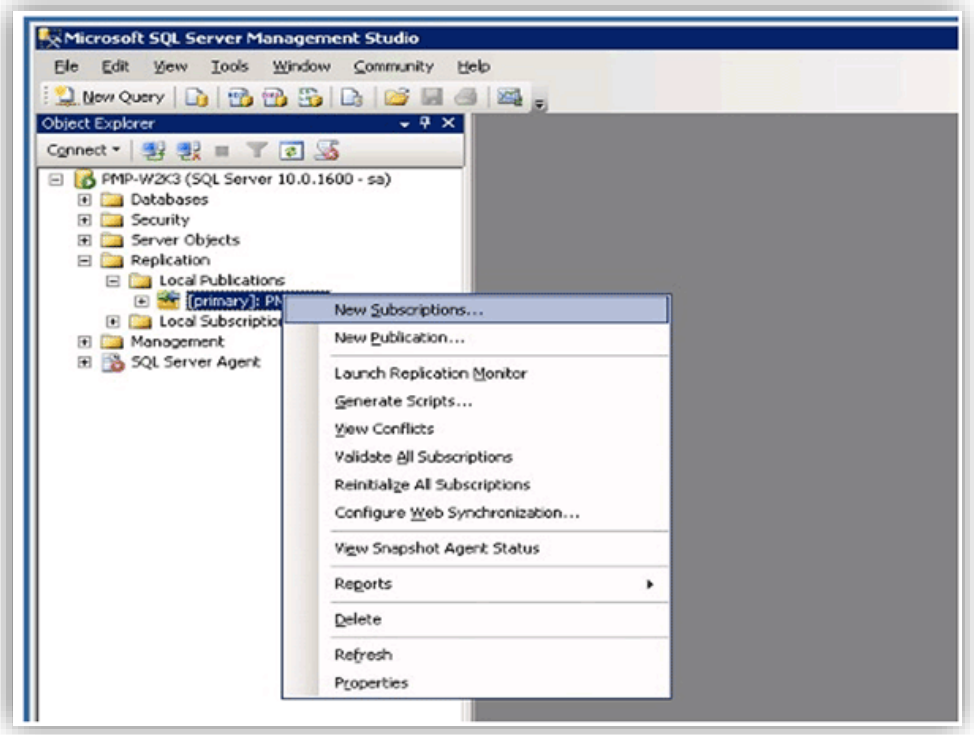
Viewing Snapshot Agent Status:

Right-click on **Publication** and click **View Snapshot Agent Status**. You will see the below window showing the progress of snapshot creation, and the process takes a few minutes. **Close** the window once the snapshot is successfully generated. You can also **Start** the agent or **Monitor** it by clicking the respective buttons.

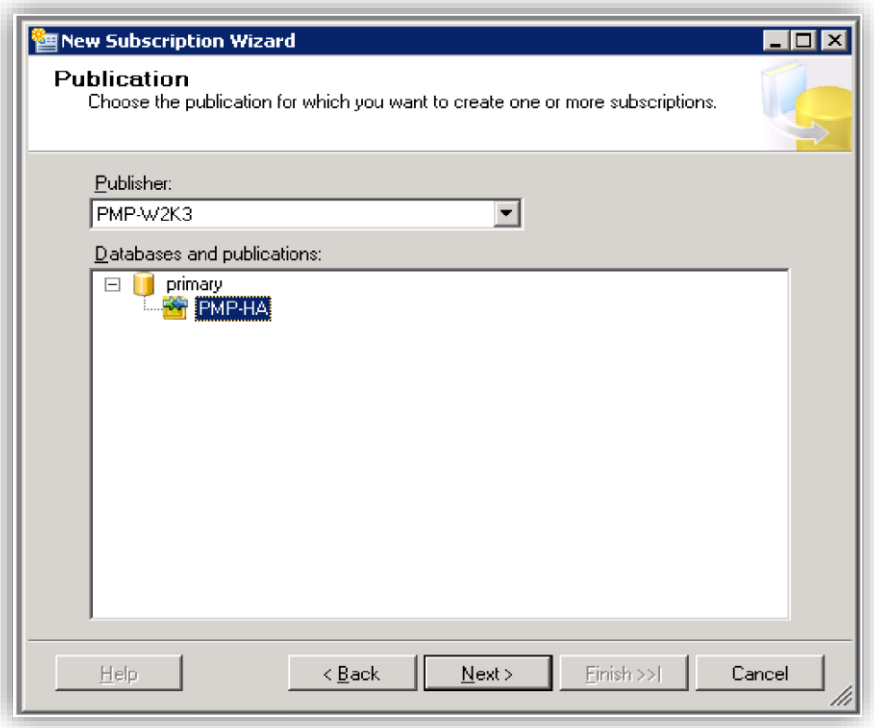


Part III - Create Subscription:

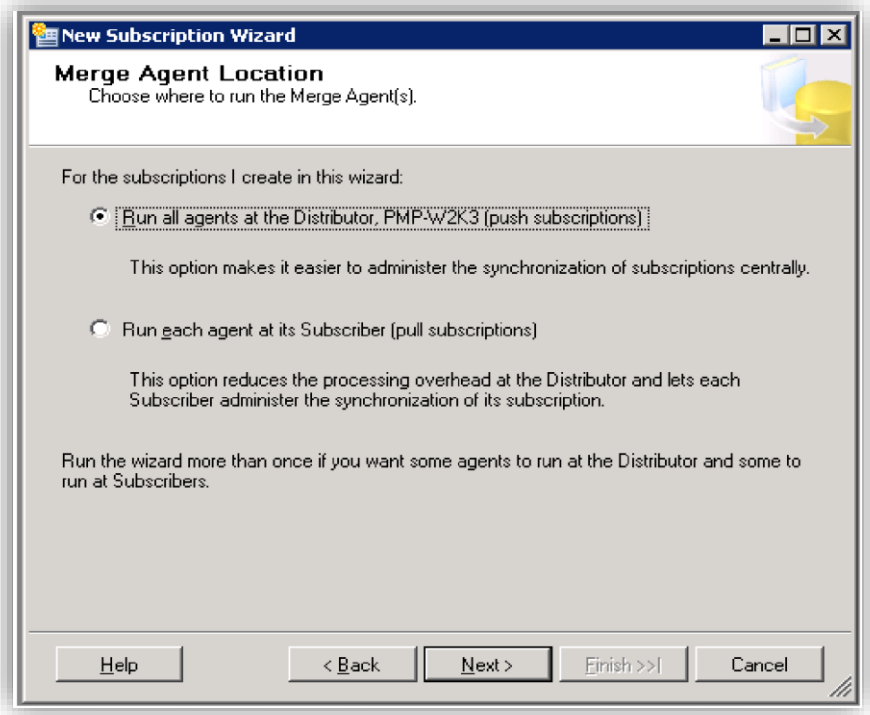
1. Under the **Object Explorer**, under **Replication >> Local Publications**, right-click on the publication created in part II (**primary**) and then click **New Subscriptions**.



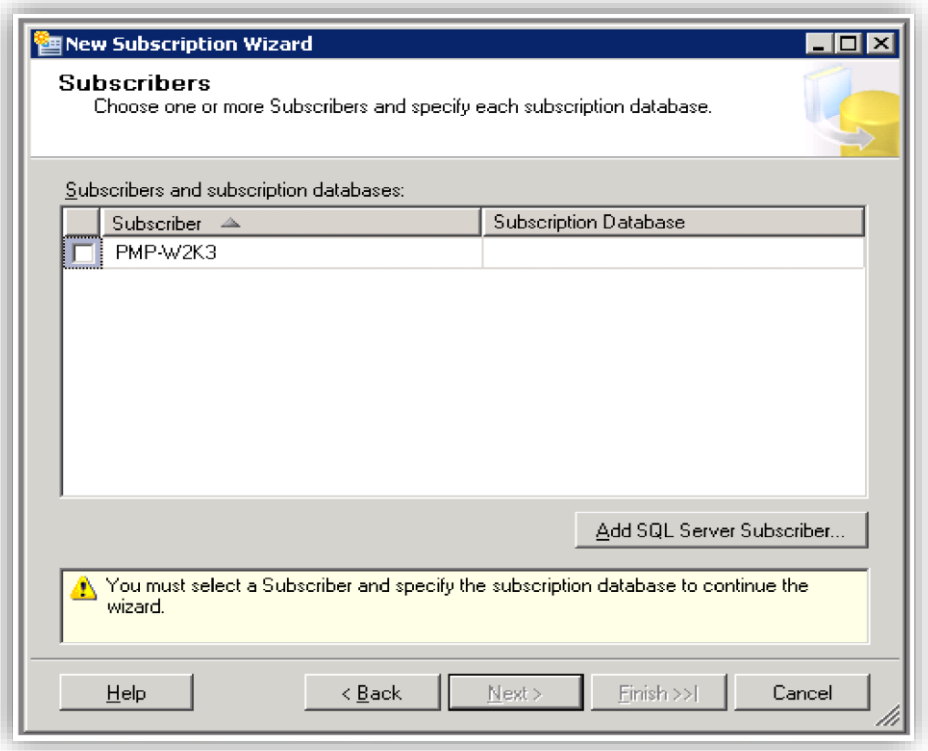
2. In the **New Subscription Wizard** displayed, select the publication created in part II (**PAM360-HA**). Click **Next**.



3. Choose the **location** to run the **Merge Agent(s)**. Choose the first option as shown in the below screenshot. Click **Next**.



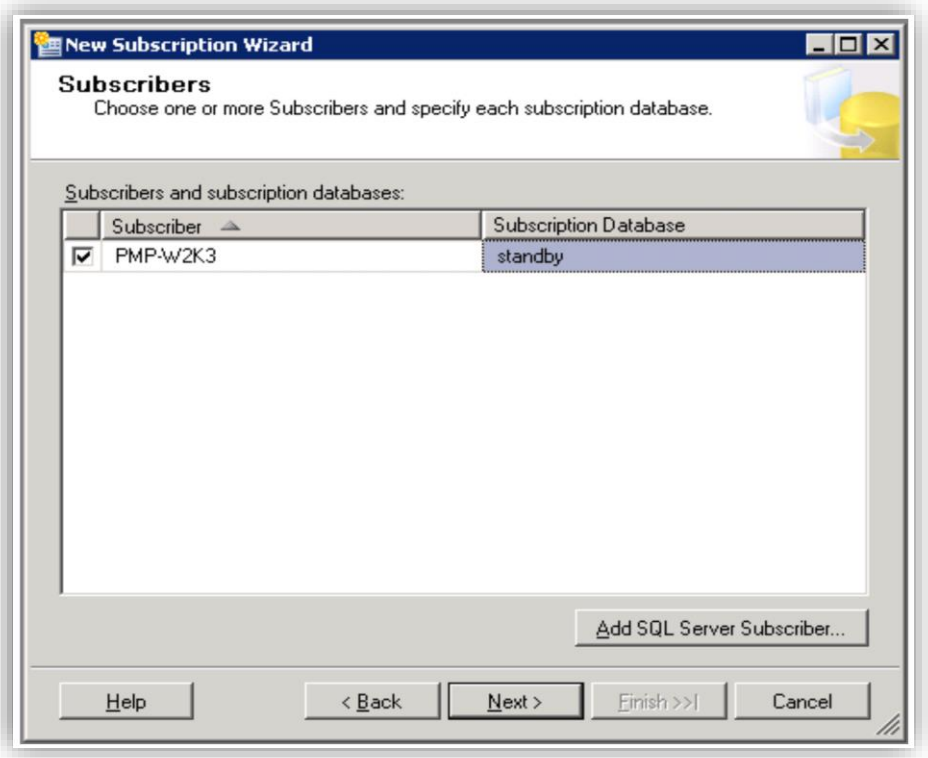
4. **[Mandatory]** Select **subscriber(s)** and also choose **database** for each subscription. Click **Next**.



5. Now, you will be allowed to **Connect to Server**. Configure the required server information as shown in the below screenshot. Click **Connect**.

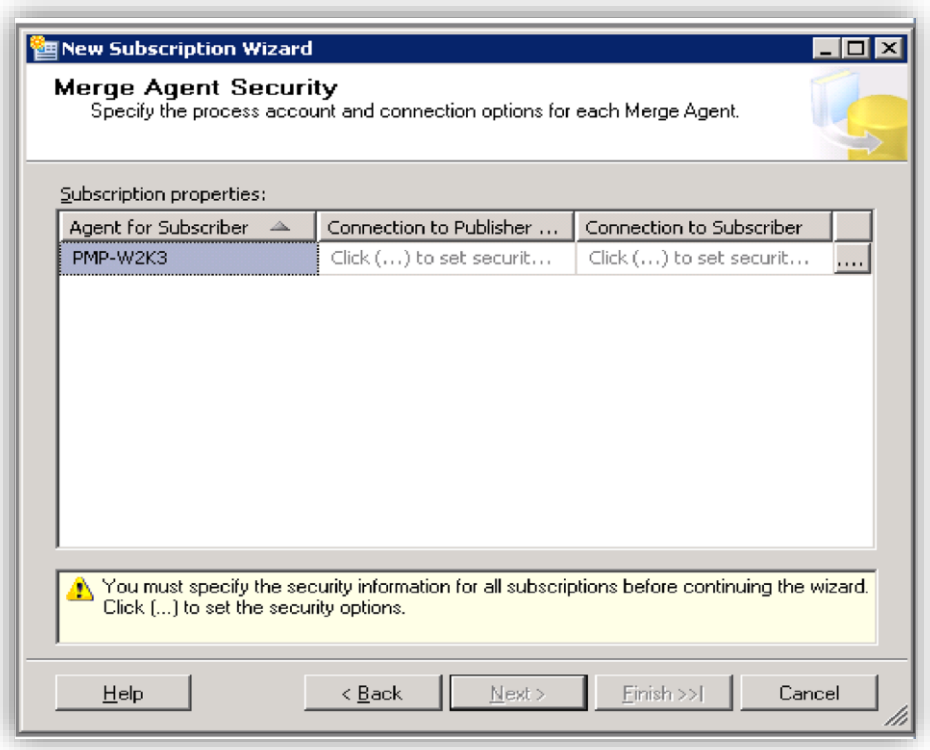


6. Once you are connected to the database server, the **New Subscription Wizard** will be shown again. Click **Next**.

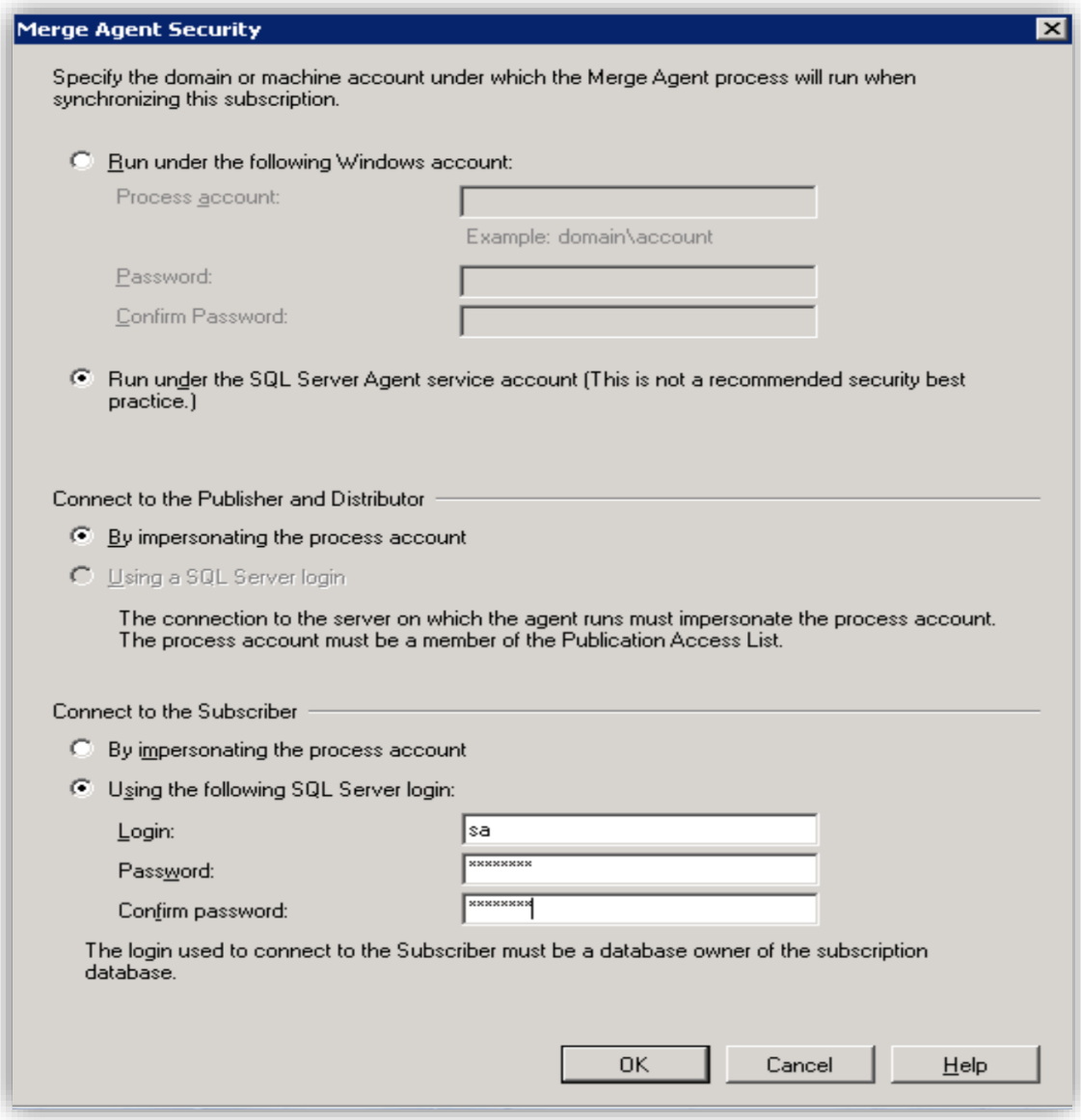


7. **[Mandatory]** Complete the security information for the subscription(s). Mention the

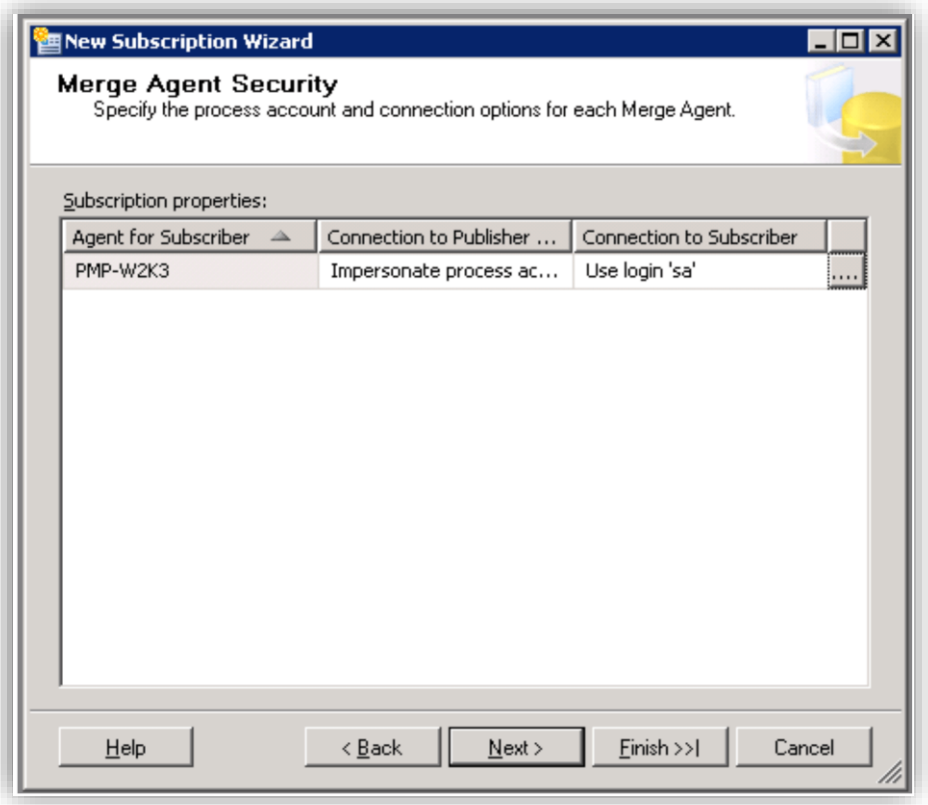
process account and **connection options** for each Merge Agent. Click **Next**.



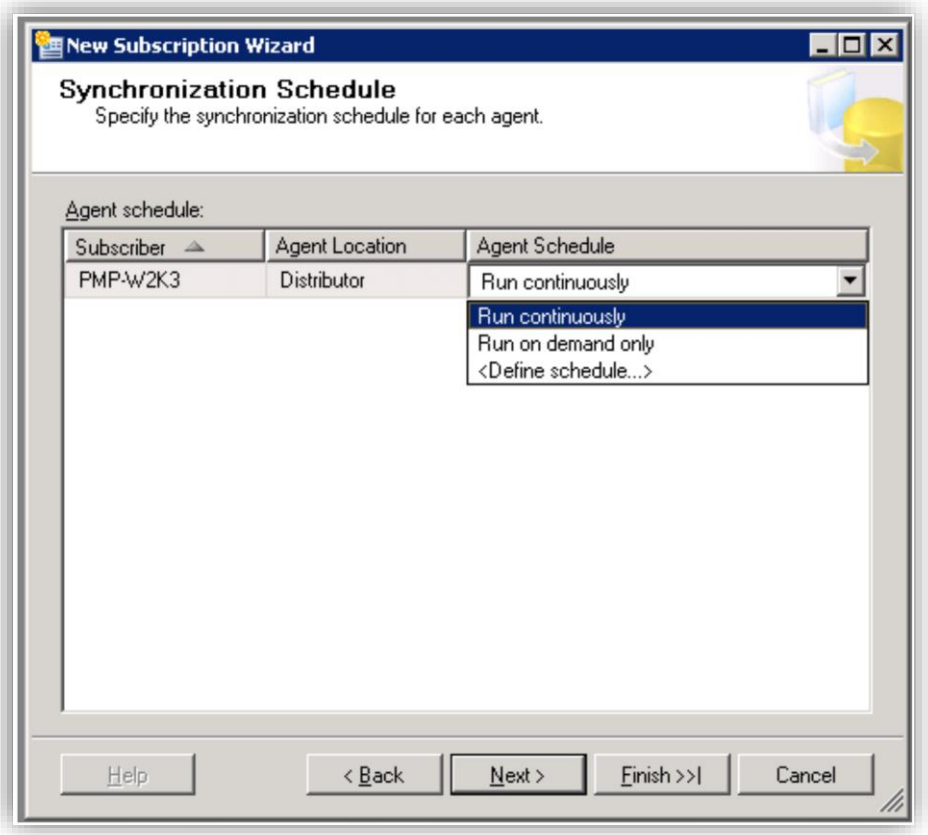
8. Specify the **domain or machine account** where the Merge Agent will run, when the subscription is synchronized. Choose the way to connect to the publisher and distributor. In addition, choose the way to connect to the subscriber. Tap **OK**.



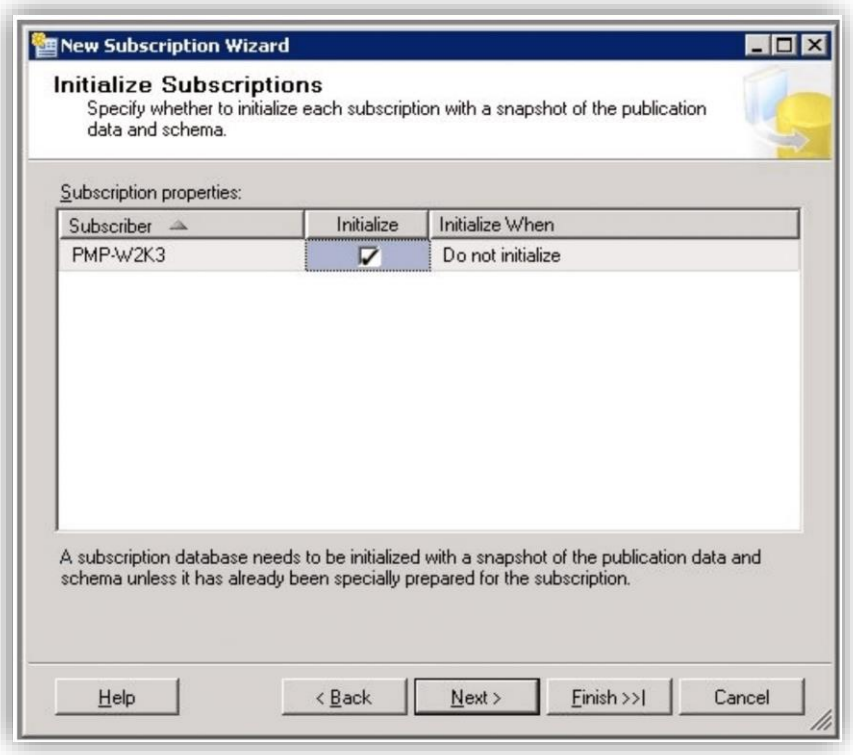
9. Specify the **process account** and **connection options** for each Merge Agent. Click **Next**.



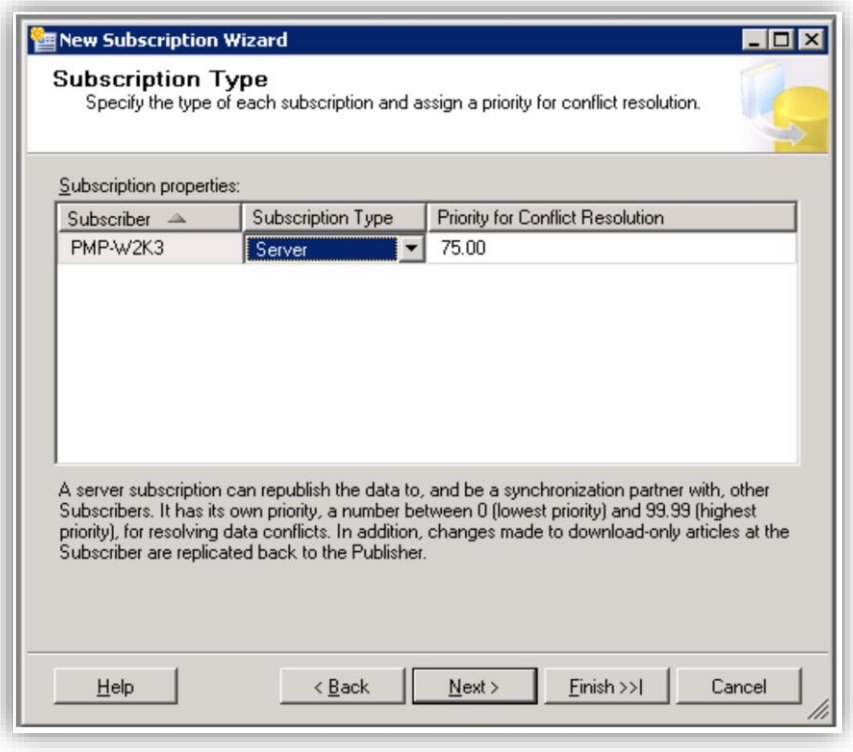
10. Choose a Synchronization Schedule for each agent from the available options under the **Agent Schedule** drop down. Click **Next**.



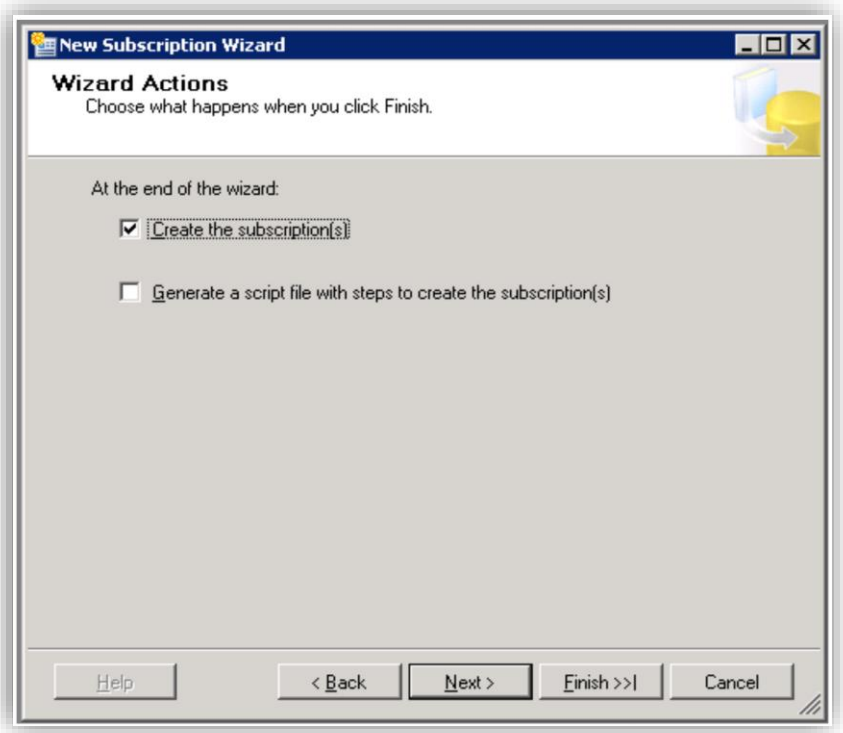
11. Choose whether to **initialize or not initialize** the subscription(s) with a snapshot of the publication data and schema. Click **Next**.



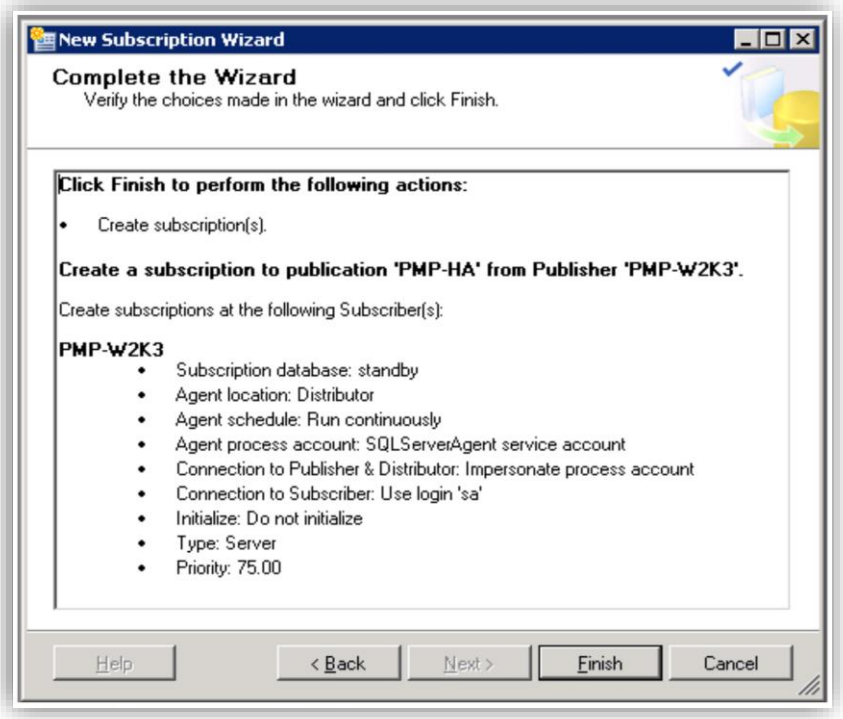
12. Choose a **Subscription Type f**or the subscription(s) from the available options. Also, choose a **Priority** for conflict resolution. Click **Next**.



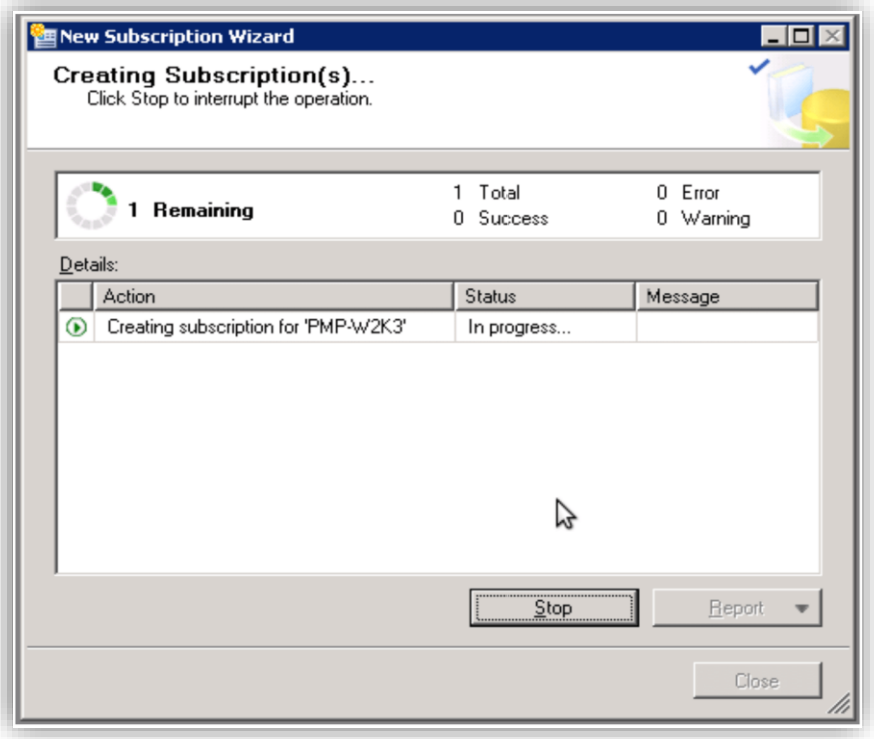
13. Select what you wish to happen when you quit this wizard. You can either choose to **Create the subscription(s)** or **Generate a scrip file**, or **both**. Click **Next.**



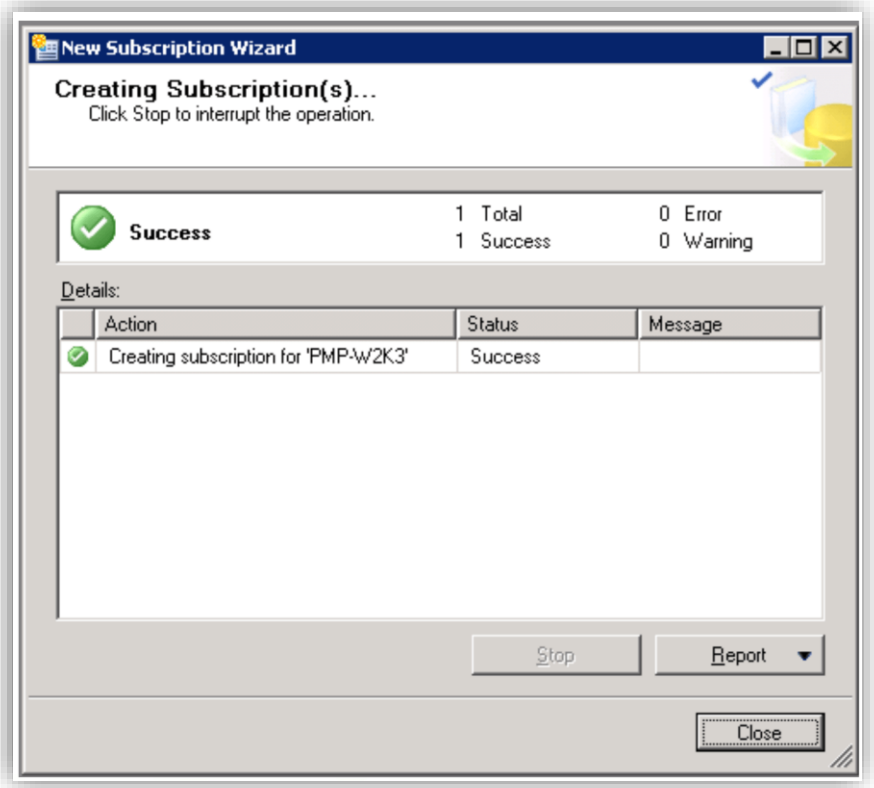
14. Click **Finish** to complete the process or click **Back** to verify the options you have chosen in the previous screens. To know in detail on what happens after you close this wizard, see the below screenshot.



15. Once you click **Finish**, you will see the subscription(s) being created as shown in the below screenshot. Click **Stop** if you want to stop creating the subscription(s).

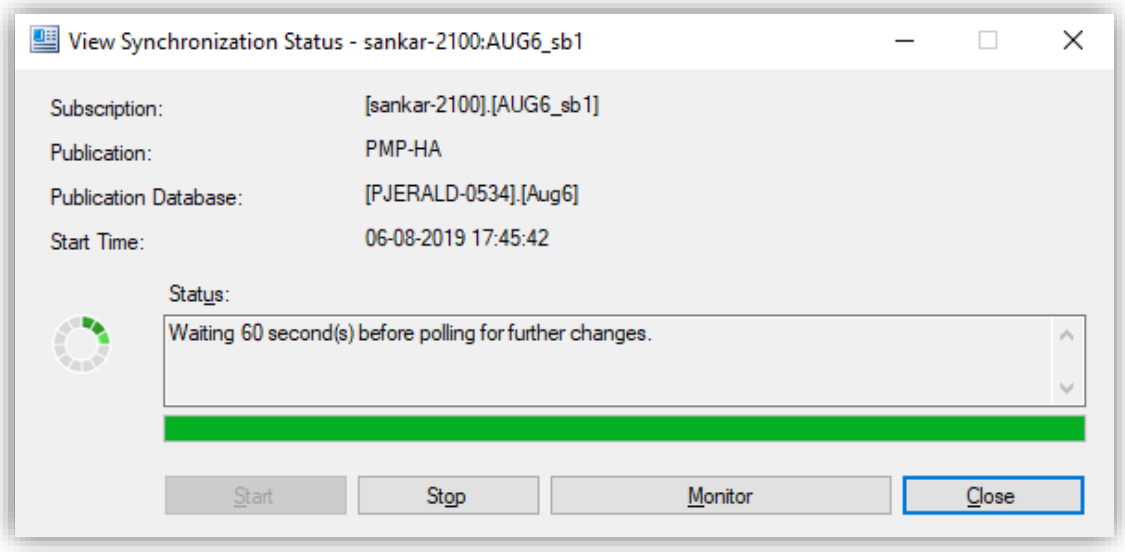


16. **Close** the window one you see the **Success** message as shown in the below screenshot.



Viewing Synchronization Status:

Right-click on **Subscription** and click **View Synchronization Status**. You will see the below window showing the progress of the synchronization, and it takes a few minutes. Close the window once the synchronization is 100% complete. You can also **Stop** the synchronization or **Monitor** it by clicking the respective buttons.



Now, the SQL server replication has been successfully completed.

Part IV - Execute Queries:

Execute the below mentioned queries in the primary server:

update Ptrx_HighAvailability set INSTANCENAME='MASTER_INSTANCE' where Ptrx_HighAvailability.ISMASTER='true';

update Ptrx_HighAvailability set INSTANCEPORT='MASTER_PORT' where Ptrx_HighAvailability.ISMASTER='true';

update Ptrx_HighAvailability set INSTANCENAME='SLAVE_INSTANCE' where Ptrx_HighAvailability.ISMASTER='false';

update Ptrx_HighAvailability set INSTANCEPORT='SLAVE_PORT' where Ptrx_HighAvailability.ISMASTER='false';

Step 5:

Start the primary server.

Step 6:

Install another instance of PAM360 as the secondary server in a separate workstation. To install PAM360 as the secondary, during installation process, choose the option **"Configure this**

server as High availability secondary server (Read Only)". After installation, the PAM360 Secondary server should not be started.

Step 7:

After installing the PAM360 secondary server, change it to run with MS SQL by carrying out the following steps:

1. Execute ChangeDB.bat.
2. Provide the details about the SQL server to PAM360 by editing the file <PAM360 Standby Installation Folder>/bin ChangeDB.bat (Windows) or <PAM360 Standby Installation Folder>/bin sh ChangeDB.sh (Linux).
3. Select SQL Server and enter the values as given below:
   i. Host Name of Slave Database: The Name or the IP address of the machine where MS SQL server is installed.
   ii. Port: The port number in which PAM360 must connect with the database. Default is 1433.
   iii. Database Name: Name of the Slave database. Here, take care to specify the name of the slave database exactly as done in Step 4 above.
   iv. Authentication: The way in which you would like to connect to the SQL server. If you are connecting to the SQL server from Windows, you have the option to make use of the Windows Single Sign On facility provided PAM360 service is running with a service account, which has the privilege to connect to SQL server. In that case, choose the option "Windows". Otherwise, select the option "SQL". It is recommended to choose the option 'Windows' as the username and password used for authentication are not stored anywhere.
   v. User Name and Password: If you have selected the option "SQL", specify the user name and password with which PAM360 needs to connect to the database. The username and password entered here will be stored in PAM360. So, take care of hardening the host.
   Here, you have the option to use even your Windows login credentials, if you are connecting to the database from Windows. In this case, enter the username as <domain-name>\<username>.
   vi. Encryption Key: The key with which your data is to be encrypted and stored in the SQL server. You may either leave it "Default" making PAM360 to generate a key. If you have configured Master database with custom key, choose "Custom' here also.

      -If you have selected the option "Custom:" After doing the above, provide the certificate name and the symmetric key name in the GUI as mentioned in the Master database:
   vii. Click Test and then Save.

Step 8:

To apply PAM360 license, custom icons and rebranding settings, if any, in secondary, copy the

respective files from primary and place them in secondary.

Step 9:

Copy the **manage_key.conf** from primary to secondary and edit the file to specify the location of the file, **pam360_key.key** (encryption master key). Then, start the secondary server. Remember, PAM360 requires the **pam360_key.key** file to be accessible with its full path, each time it starts up. Anyway, after the successful start-up, the key is not required, hence the device with the key file can go offline.

2. Verify High Availability Setup

After carrying out the above steps, you can verify if the High Availability setup is working properly by looking at the message under **Admin >> General >> High Availability** of primary or secondary server. If the setup is proper, you will see the following status message:

High Availability Status: **Alive**

It indicates that high availability is working fine. In case, if the status turns **'Failed'**, it indicates failure of the setup.

Steps to Remove High Availability (MS SQL Server as Backend Database)

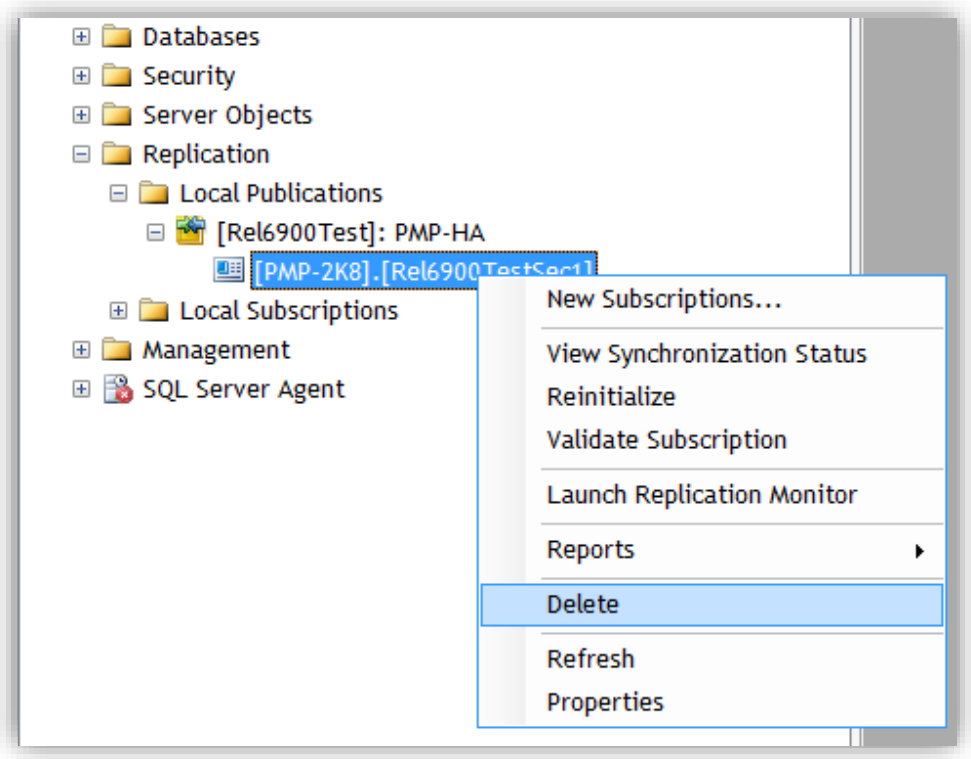
Important Note: Take a copy of the entire PAM360 installation folder before applying the upgrade pack and keep it in some other location. If something goes wrong with the PAM360 upgrade, you can rely on the copy. All your settings will remain intact. Additionally, take a backup of the PAM360 database.

Steps Required

1. In Windows, right-click the PAM360 tray icon and then click **Exit.**
2. Shutdown both PAM360 primary and secondary services, if running.
3. Login to MS SQL Server management studio and delete the following files/folders as explained below.
4. In-order to stop replication, PAM360 requires the **subscriptions** and **publications** related to PAM360 replication data be deleted AND **publishing and distribution** be disabled. To do these, carry out the steps below:

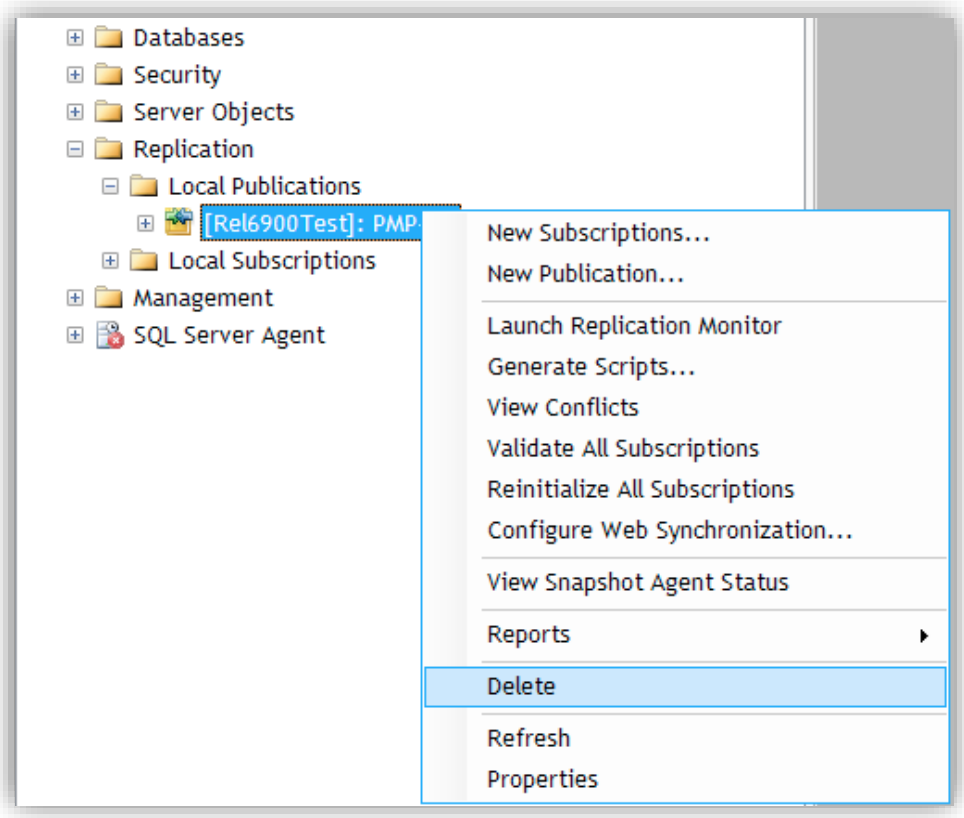
Step 1: Deleting Subscription

First, navigate to **Replication >> Local Publications >> <Name of PAM360 database:PAM360-HA>**. You will see a file with **<PAM360 server name>. <Name of PAM360 database>**. Right click the file and press **Delete** in the menu.



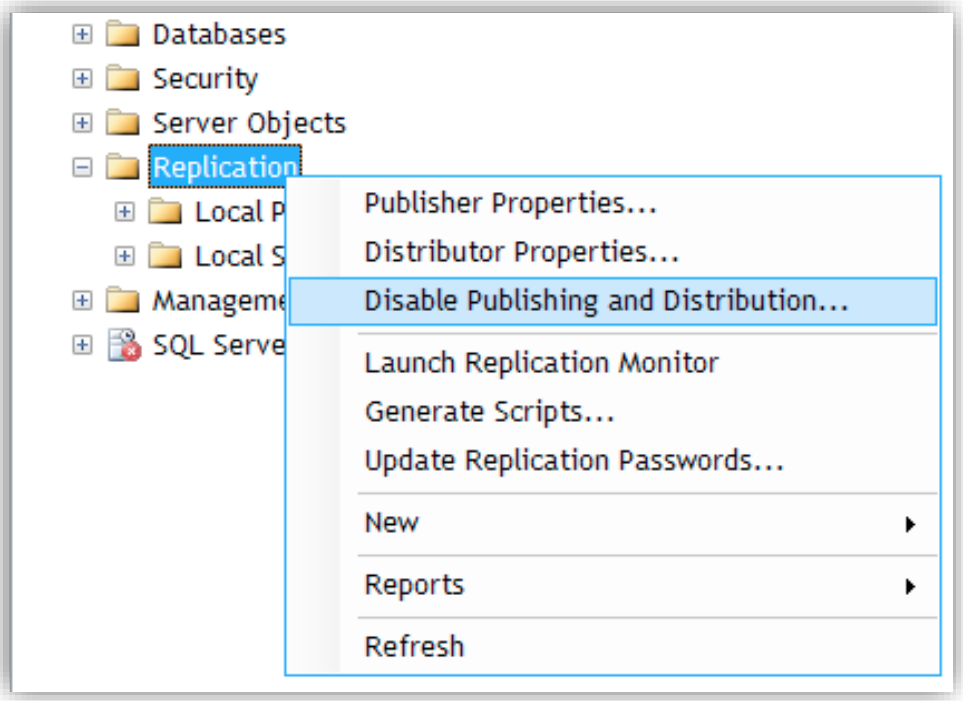
Step 2: Deleting Publication

Then, navigate to **Replication >> Local Publications >> <Name of PAM360 database:PAM360-HA>**. Right click the folder **<Name of PAM360 database:PAM360-HA>** and press **Delete** in the menu.



Step 3: Disabling Publishing & Distribution

Then, right click the **Replication** folder and click the option **Disable Publishing and Distribution.**



Monitor High Availability using PAM360

Note: Right now, PAM360 supports HA monitoring for **PostgreSQL** database only. Eventually, support will be extended for MS SQL databases as well.

In mission-critical environments, one of the crucial requirements is to provide un-interrupted access to passwords. PAM360 provides the High Availability feature just to ensure this. In general, High Availability (HA) approach is to have a Primary server and a Secondary/Standby server to take over operations, if the Primary server fails. PAM360 supports monitoring the high availability of your servers to anticipate failures, thereby avoiding costly downtimes.

This scetions walks you through the below topics:

1. Why do you need High Availability Monitoring?
2. How does High Availability work in PAM360?
3. The High Availability Architecture in PAM360
4. What happens to Audit Trails?
5. Synchronizing Primary and Secondary Servers
6. Monitoring High Availability for PostgreSQL Database Server
   - 6.1 Steps to Monitor High Availability for PostgreSQL Database Server
   - 6.2 The High Availability Console for PostgreSQL Database Server
   - 6.3 UI Elements and Definitions
   - 6.4 Impact of Server/Database Status (Active/Inactive) on High Availability
   - 6.5 Alerting Mechanism for Status Failure
   - 6.6 Modifying Server Details from the HA Console
   - 6.7 What do I do in case of a High Availability Failure?

1. Why do you need High Availability Monitoring?

Continuous monitoring of your endpoints and associated database operations ensures early detection of problems and finding solutions for the same which in turn improves the user's system experience. In addition, monitoring captures system metrics, used to analyze trends in server performance and recurring problems. In the case of the database server, a reliable monitoring system is essential as it measures availability, detects events that can put down the database server and provides immediate notifications about critical failures to the concerned parties. A perfect monitoring process is one that is highly accessible and stable, captures diagnostic data and alerts the administrator about the problems encountered.

2. How does High Availability work in PAM360?

Whenever the Primary server fails or goes down, the Secondary server takes over the functions that were being performed by the Primary. The HA setup in PAM360 provides a Secondary server, which can be used to retrieve passwords from the PAM360 repository, in case of a disaster, until the fully functional Primary server is back to service. This can be explained in detail as below:

- Redundant PAM360 servers and database instances will be present.
- One instance will be the Primary, providing read/write access to users. All the users will be connected with the Primary only.
- The other instance will act as the Secondary.
- Both the Primary and the Secondary instances will always be in sync with each other. The data replication happens through a secure, encrypted channel.
- When the Primary server goes down, the Secondary will offer emergency access to the users, until the fully-functional primary server is brought back to service. The intermediate changes (if any) made to the database will be automatically synchronized upon connection restoration.

3. The High Availability Architecture in PAM360

The HA architecture in PAM360 is designed to be compatible with two different scenarios. See the below table for a detailed explanation:

Scenario 1	
Hosting Primary & Secondary servers on the same network	The Secondary server is located on the same network, where the Primary server operates. The Secondary server is provided with the read/write access (except password reset action), in case of the Primary server failure.
Example	**Primary & Secondary within the same network & the Primary goes down:** Assume, the Primary and Secondary servers are deployed in the same geographical location, say 'A'. In the case when the Primary crashes or goes down, the users of both the Primary and Secondary servers will get the emergency access to the passwords from the Secondary.
Scenario 2	

Hosting Primary & Secondary servers on different networks	Primary and Secondary servers are located on different networks. The Secondary server in the remote network gets the read/write access (except password reset action), in case of a WAN link failure or Primary server failure.
Example	**Primary & Secondary in different geographical locations and WAN Link failure happens between the locations:** Assume, the Primary server is in a geographical location 'A' and the Secondary server is deployed in another location 'B'. By default, the users in both 'A' and 'B' will be connected to the Primary and will be carrying out the routine password management activities. The data in both the Primary and Secondary are in sync with each other. Now, imagine, there happens a network connectivity loss between the two locations. In such a situation, the two servers will start operating independently. Thus, the users in location 'A' will remain connected with the Primary server and will be carrying out their operations as usual. On the other hand, the users in location 'B' will get emergency access to the passwords from the Secondary server. Once the connection is re-established between 'A' and 'B', the data in both the locations will be synchronized.

4. What happens to Audit Trails?

In the high availability scenarios mentioned above, audit trails will be recorded as usual. In scenario 2, as long as there is network connectivity between the two locations, the audit trails will be printed by the primary. When users connect to the Secondary, it will print operations such as 'password retrieval', 'login' and 'logout'. When the two locations get back network connectivity, the audit data will be synchronized. In scenario 1, when the primary crashes, the 'password retrieval', 'login' and 'logout' done by the users in secondary will be audited. Other audit records will already be in sync at the Standby

5. Synchronizing Primary and Secondary Servers

For a Secondary server to take over the operations of a failed Primary server, it must hold accurately the same data and perform the database processing in the same way as the primary server would have done, if it had worked fine. Hence, synchronization means continuously updating the Secondary server database so that it is an exact replica of the Primary database server.

PAM360's HA functionality is thoughtfully designed to keep the data in both the servers in sync all the time. In case of a Secondary server failure or link failure, the changes made in one database are automatically synced up with the other upon service/connection restoration. Also, during such failures, the operations done in the Secondary server are audited as usual

and synced up automatically on restoration. The data replication happens over a secure, encrypted channel.

6. Monitoring High Availability for PostgreSQL Database Server

PAM360 is inbuilt with HA management and monitoring capabilities with various notification options. Follow the below steps to monitor and manage the HA for PostgreSQL Database Server using PAM360:

6.1 Steps to Monitor High Availability for PostgreSQL Database Server

1. Before you start monitoring HA, you need to first set up HA in the server running in PostgreSQL.
2. Once you have set up the HA, you can start monitoring the PostgreSQL HA setup from the PAM360 console:
   Navigate to **Admin >> Configuration >> High Availability** of Primary or Secondary server. You will see the HA console.

6.2 The High Availability Console for PostgreSQL Database Server

The HA console in PAM360 is an all-in-one, dashboard-style window for monitoring the availability of your Primary and Secondary servers and the associated databases. The console allows you to switch your view from the Primary server to the Secondary server, and vice-versa.

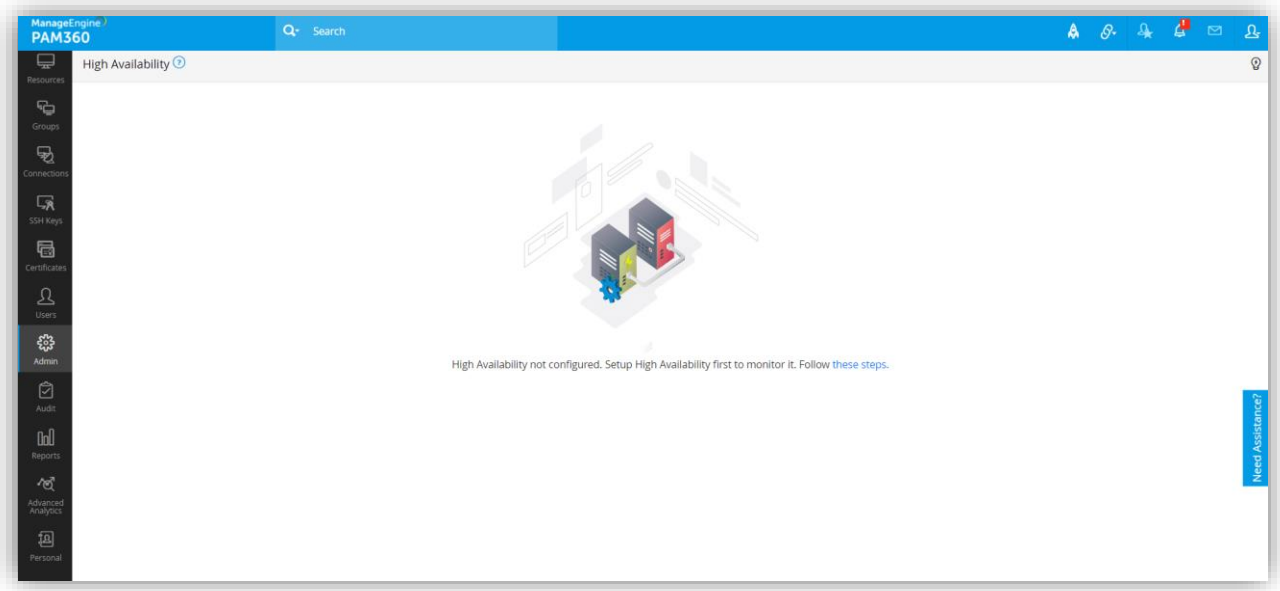
Use the HA Console to:

- View the HA summary that includes the status of the HA and its configuration.
- View the status of the servers and the associated databases.
- View the replication pending count.
- View the connection lost and connection resumed times.
- Modify the server details.

The view of the console is based on whether you have configured or not configured the HA:

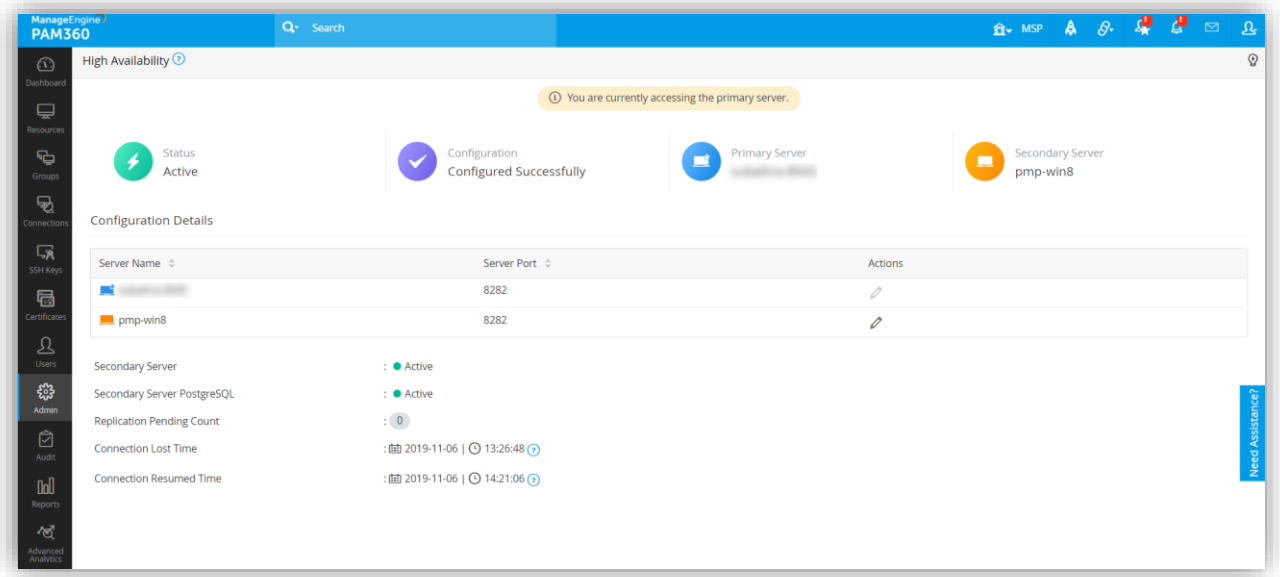
1. **If you have not configured HA:** You will see an empty console with a message displayed as shown in the below image. You need to setup the High Availability first to monitor it.

View of the console when HA is not configured with PostgreSQL



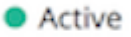
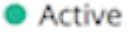
2. If you have configured the HA setup properly: You will see the console with the availability and other details of the Primary and Secondary server, as shown in the below image:

View of the console when HA is configured with PostgreSQL



6.3 UI Elements and Definitions

The PAM360 HA monitoring console includes various elements each of which corresponds to a specific detail as explained below:

Sl. No:	UI Element/Icon	Status	Definition
1		Active	This blinking icon indicates that the HA is actively running in the server (Primary/Secondary) which you are viewing right now.
2		Inactive	This blinking icon indicates that the HA is down in the server (Primary/Secondary) which you are viewing right now.
3		Success	This icon indicates that HA is configured successfully in your server. In the case of HA configuration failure, the above first screen will be shown in the console.
4		-	This icon denotes the Primary server.
5		-	This icon denotes the Secondary server.
6	Configuration Details	-	This is a table listing the following details of Primary and Secondary servers; Server Name, Server Port and Actions. You can modify the Secondary server details from here. (Please note that you cannot edit the Primary server details)
7	Primary/Secondary Server		This icon indicates that the Primary/Secondary server is up and running.
			This icon indicates that the Primary/Secondary server is down and stopped running.
8	Primary/Secondary Server PostgreSQL		This icon indicates that the PostgreSQL database of Primary/Secondary server is up and running.
			This icon indicates that the PostgreSQL database of Primary/Secondary server is down and stopped running.
9	Replication Pending Count	-	This indicates the total number of pending replications. If this value is zero, it means that there are no replications pending and the

			Primary and Secondary server are continuously in sync with each other.
10	Connection Lost Time	-	This indicates the time when the connectivity between the Primary and Secondary servers was lost.
11	Connection Resumed Time	-	This indicates the time when the connectivity between the Primary and Secondary servers was regained.

6.4 Impact of Server/Database Status (Active/Inactive) on High Availability

The basic concept underlying HA is constant replication of data between the Primary and Secondary servers, where the Primary acts as the "Master" and the Secondary as the "Slave". The "Status" corresponds to the condition of the connection/communication between the Primary and Secondary servers/databases. There are two types of HA status:

1. **Active** - Indicates perfect data replication and data synchronization between the Primary and Secondary servers.
2. **Inactive** - Indicates a breakage in connectivity between the Primary and Secondary servers. The breakage might be due to a disruption such as network problem between the servers (in turn between the databases). Due to this, there will be no communication between the databases of Primary and Secondary servers and the data replication and data synchronization between the servers will get disturbed.

Once the connection gets re-established, the synchronization will start between the databases. Anyhow, during the network disconnectivity, those who have connected to the primary and Secondary will not face any disruption in service.

6.5 Alerting Mechanism for Status Failure

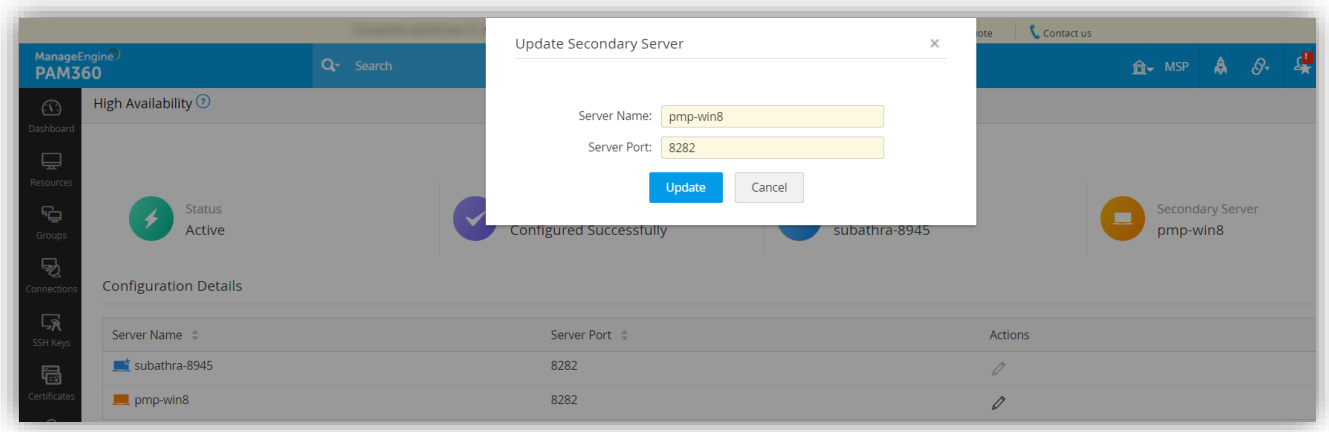
Since the above two conditions (Active/Inactive) assume importance in the HA setup, it is important to receive real-time alerts when the status turns from **Active** to **Inactive** and vice-versa. To configure alerts, navigate to **Audit >> Resource Audit >> Configure User Audit >> General Operations** and select the mode of alert (email/SNMP trap/Syslog message) for the events **High Availability Alive** and **High Availability Failed**.

Notes:

1. **Post HA Configuration**: If you change the port of the Primary PAM360 server, the high availability setup will not work. You need to re-configure the setup with suitable changes.
2. **If you have configured TFA**: Whenever you enable TFA or when you change the TFA type (PhoneFactor or RSA SecurID or One-time password) AND if you have configured HA, you need to restart the PAM360 secondary server once.

6.6 Modifying Server Details from the HA Console

Click the icon under **Actions** beside the Secondary server, whose details you wish to edit. In the window that pops up modify the details as required and click **Update**.



6.7 What do I do in case of a High Availability Failure?

Once the HA status becomes "Inactive", the PAM360 HA setup also breaks down. In case of a HA failure, contact pam360-support@manageengine.com with the below log file:

<PAM360 Installation Folder>/pgsql/data/pg_log/pgsql_Mon.log

Read-Only Server with PostgreSQL Database

A Read-Only (RO) server is a secondary application server that allows users to execute only the Read-Only operations in PAM360 and averts them from performing any modifications to the data. Depending on the needs, any number of Read-Only servers can be configured in various locations, unlike HA, which allows you to configure one Secondary server only. All these Read-Only servers are connected and in sync with the Primary server. The Read-Only server acts like a mirror server and synchronizes all the actions carried out by the Primary server. In case of a Primary server failure, any Read-Only server can be configured as the Primary server.

Notes:

- PAM360 will allow users to retrieve only the passwords through the Read-Only server.
- All the operations carried out in the Read-Only server will be returned and audited in the Primary server and then replicated to other Read-Only servers.
- In the event of Primary server failure, administrators can convert any Read-Only server into the Primary server and reconfigure all other Read-Only servers to point to the new Primary server.

Setting up Primary Server and Read-Only Server

Before configuring your Primary and the Read-Only server(s), you should install the Read-Only server(s) in your environment. Once you have successfully installed the Read-Only server(s), read further to learn how to make the required configuration changes in the Primary and the Read-Only servers. Also, find below the steps to make a Read-Only server take charge as the Primary server when the current Primary server is down.

1. Creating a Read-Only Server Configuration Pack in the Primary Server

1. Navigate to **<PAM360_Installation_Folder>/bin.**
2. Execute the following command in the Primary server to create a **ROPack.zip** file which will contain the files needed to be copied to the Read-Only server:
   - **Windows:** *ROSetup.bat <IP_of_RO_Server> <userName> <password> <slotName>*
   - **Linux:** *ROSetup.sh <IP_of_RO_Server> <userName> <password> <slotName>*

Notes:

- Every Read-Only server must have a unique **slotName** while creating **ROPack.zip.**
- Supply a **userName** and **password** of your choice when creating the replication pack for the first time to configure the Read-Only server. To generate additional replication packs in the future, you must provide the same username and password. Please note that the PAM360 database will not store the username and password. Hence, we recommend you save them in a secure location.

Where,

i. **IP_of_RO_Server -** Valid IP address of an Read-Only server.
ii. **userName -** Username used for replication.

Constraints:

- Single username and password is enough for all Read-Only servers.
- Username can only contain lower case letters, numbers, and underscores.

iii. **password -** Password for the replication user.
iv. **slotName -** Slot name of the Read-Only server for the replication.

Constraints:

- Replication slot names may only contain lower case letters, numbers, and underscores.
- Each Read-Only server should have a unique slot name.

The generated replication pack zip will be found under **<PAM360_Installation_Folder>/replication** folder.

3. Execute the following commands in the Primary server to import the certificates:

Linux:

sh importCert.sh ../conf/ServerCer.cer

sh importCert.sh ../conf/CACert.pem

sh importCert.sh ../agent/ServerCer.cer

Windows:

importCert.bat .. |conf |ServerCer.cer

importCert.bat .. |conf|CACert.pem

importCert.bat .. |agent|ServerCer.cer

> **Note:** To install custom certificates, replace the path of the certificate in the above command.

You have successfully created the Read-Only configuration pack and set up the Primary server.

2. Setting up the Read-Only Server

1. Navigate to the **<PAM360_Installation_Folder>** in Read-Only server and extract the **ROPack.zip** file. This will replace the files from the Primary server that are already available here.
2. Copy **pam360_key.key** file from Primary server to the Read-Only servers and update the Path of the **pam360_key.key** file in **<PAM360_Installation_Folder>/conf/manage_key.conf** file.

> **Note:** If the **manage_key.conf** file is not present in the Read-Only server, then create a new file named **manage_key.conf** and mention the location of the encryption key. If the encryption key is in a remote path, mention the path in a UNC format.

3. Navigate to **<PAM360_Installation_Folder>/bin** and execute the following command in the Read-Only server to import the certificates:

   Linux:

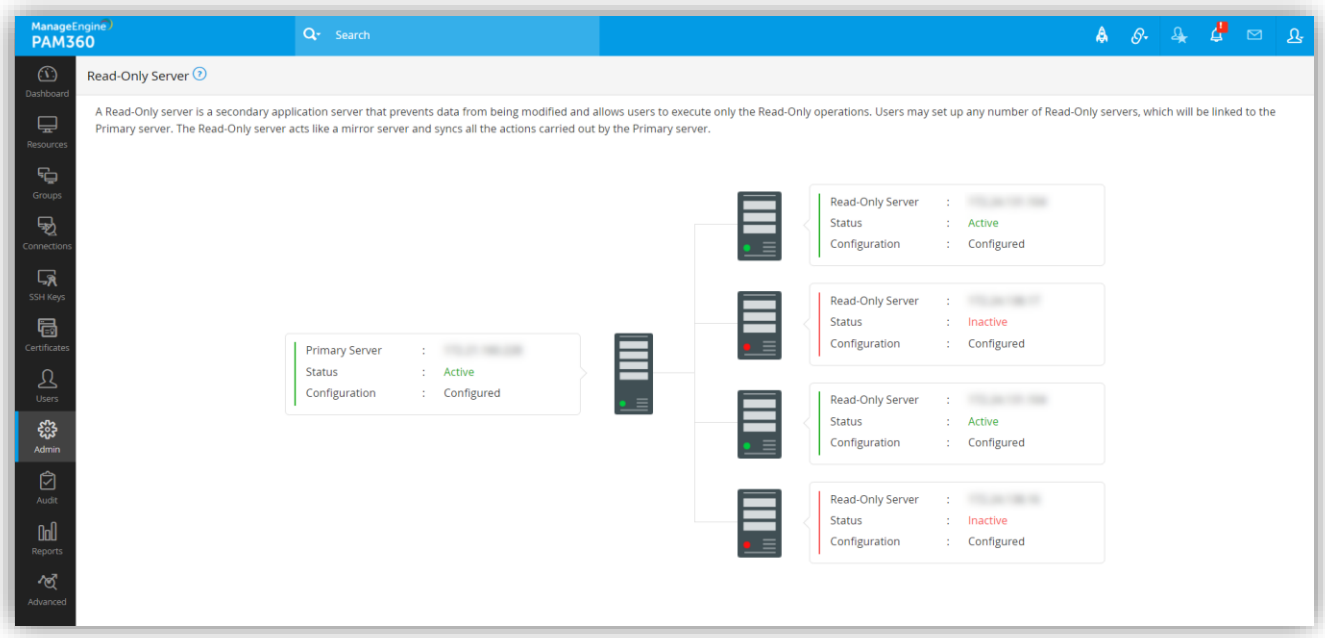
   - *sh importCert.sh ../conf/ServerCer.cer*
   - *sh importCert.sh ../conf/CACert.pem*
   - *sh importCert.sh ../agent/ServerCer.cer*

   Windows:

   - *importCert.bat .. |conf|ServerCer.cer*
   - *importCert.bat .. |conf|CACert.pem*
   - *importCert.bat .. |agent|ServerCer.cer*

Note: To install custom certificates, replace the path of the certificate in the above command.

You have successfully set up the Read-Only server. Navigate to **Admin >> Configurations >> Read-Only** server to view the configured Read-Only servers in the PAM360 interface.



3. Configuring Read-Only Server as the Primary Server

1. Stop the Read-Only server that is to be converted as the Primary server.
2. Remove **recovery.conf** file from **<PAM360_Installation_Folder>/pgsql/data** folder.
3. Delete the entry **readonly.mode=true** in the **<PAM360_Installation_Folder>/conf/configurations.properties** file.
4. Edit the **<PAM360_Installation_Folder>/conf/serverstate.conf** and change **"ro"** to **"master".**
5. Start the PAM360 server and now this Read-Only server will start as the Primary server.

   You have successfully configured the Read-Only server as the Primary server.
6. Now, execute the following commands to remove the IP address of the converted Read-Only server from the database.

   Windows:

   - *<PAM360_Installation_Folder>|bin|DeleteROServerIP.bat*

<IP_Address_of_RO_that_was_converted_to_Primary>

- *<PAM360_Installation_Folder>|bin|DeleteSlot.bat <slotName_of_RO_that_was_converted_to_Primary>*

Linux:

- *<PAM360_Installation_Folder>/bin/DeleteROServerIP.sh <IP_Address_of_RO_that_was_converted_to_Primary>*
- *<PAM360_Installation_Folder>/bin/DeleteSlot.sh <slotName_of_RO_that_was_converted_to_Primary>*

7. Now, follow **step 1** (Creating a Read-Only server Configuration Pack in the Primary Server) and **step 2** (Setting up the Read-Only server) to reconfigure the existing Read-Only servers to be in sync with this Primary server.

4. Deleting a Read-Only Server from the Cluster

Execute the following commands from the Primary Server to remove a Read-Only server from the cluster:

1. To delete an existing Read-Only server,

   Windows:

   <PAM360_Installation_Folder>|bin|DeleteROServerIP.bat <RO_IP_Address>

   Linux:

   <PAM360_Installation_Folder>/bin/DeleteROServerIP.sh <RO_IP_Address>

2. To delete an existing slot configured to the Read-Only server,

   Windows:

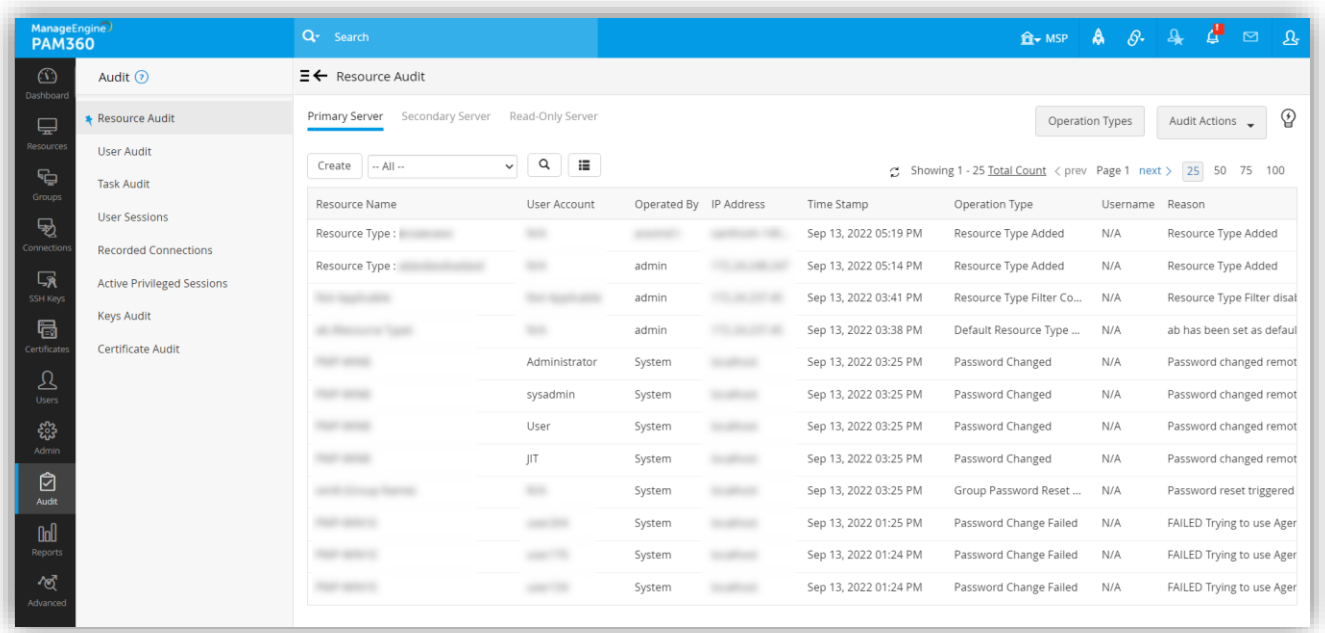
   <PAM360_Installation_Folder>|bin|DeleteSlot.bat <RO Slot Name>

   Linux:

   <PAM360_Installation_Folder>/bin/DeleteSlot.sh <RO Slot Name>

5. Read-Only Server Audit Trials

When Read-Only server is enabled, the Read-Only server audits will be displayed as separate columns with the full audit trails under Resource Audit and User Audit. Click here to learn more about audits.



Troubleshooting Tips

Navigate to **Admin >> Configurations >> Read-Only Server** and check if the status of the Read-Only server(s) is inactive. If so, follow the below steps to troubleshoot:

Primary Server:

1. Navigate to **<PAM360_installation_folder>/pgsql/data** folder.
2. Open **pg_hba.conf** file and check if the **IP Address** of the Read-Only server and the **replication user name** is correct.

Read-Only Server:

1. Navigate to **<PAM360_installation_folder>/conf.**
   i. Open **roserver.conf** file and check if the **Primary** and **Read-Only server IP address** are correct.
   ii. Now, open the **configuration.properties** file and check for the value **"readonly.mode=true".**
2. Navigate to **<PAM360_installation_folder>/pgsql/data** folder.
   i. Open **recovery.conf** file and check if the **Primary server IP, Port, replication username, password** and the **slot name** are correct.

If the problem persists, send us the log files from the directory paths **<PAM360_installation_folder>/logs** and **<PAM360_installation_folder>/pgsql/data/pg_log** to pam360-support@manageengine.com for further assistance.

Failover Service for PAM360 (MS-SQL Server Clusters)

(Procedure applicable ONLY for Windows installations of PAM360 with MS SQL cluster as the backend database)

The Failover Service in PAM360 is also aimed at ensuring uninterrupted access to passwords and other privileged resources. While the 'High Availability' feature in PAM360 requires two separate database instances to be mapped to the Primary and secondary servers of PAM360 respectively, the 'Failover Service' functions with redundant PAM360 server instances which have access to a common MS-SQL cluster, which in turn has multiple PAM360 database instances bound to it.

> **Note**: Failover Service for PAM360 allows configuration of a maximum of TWO instances of PAM360 only.

At the end of this document you will have learnt the following:

1. How does the Failover Work?
2. How to Set Up a Failover Service?
3. How to Uninstall the Failover Service?
4. Troubleshooting Tips

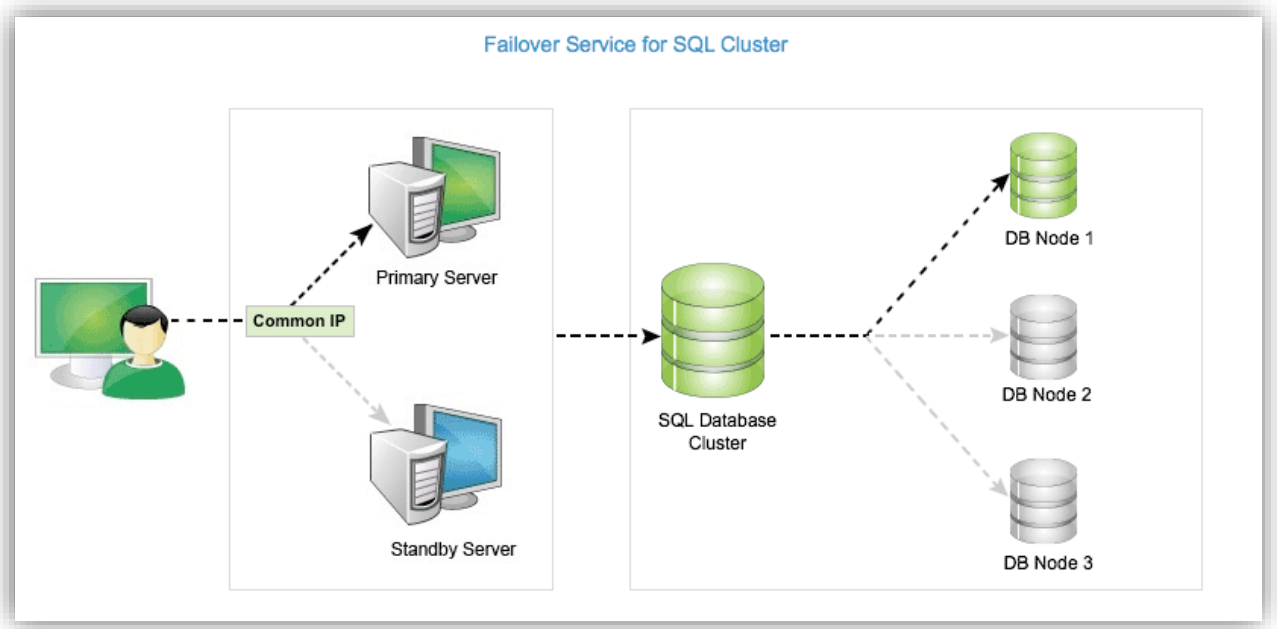
1. How does the Failover Work?

- There will be redundant PAM360 server instances which will have access to a common MS-SQL cluster, which in turn has multiple PAM360 database instances bound to it.
- Both the instances of PAM360 server will be primary installations providing read/write access to the users. While one instance acts as the primary, the other will act as the Standby. (Primary, standby and SQL cluster database will be installed on three separate machines)
- In this setup, PAM360 installed in the primary will normally be up and running. The standby machine will keep monitoring the primary. The PAM360 application in the standby is configured to start up and take-over, in case the primary crashes or goes down.
- When the primary server is brought back to service, it will automatically act as the 'standby'. The server, which was originally configured to act as standby will become the

primary.

- Both the primary and standby servers are bound by a common public IP and the PAM360 web-interface will always be connected to this specific IP. Irrespective of whether PAM360 is running on the Primary or Standby server, end-users can anytime connect to PAM360 using the same public IP.

> **Note:** All three machines should be in the same subnet. In case the primary crashes and goes into an unrecoverable state, you can configure a yet another alternate server from the standby server itself, which, by then, will be up & running and also serve as the primary thereafter.



2. How to Set Up a Failover Service?

Step 1: Install Primary and Standby Servers

Install PAM360 in two different machines. One will act as the primary server and the other one as standby. (You can specify which machine should run as primary and which one as Standby through a configuration later)

Important Notes:

- Failover service can be set up only if the processor compatibility of both PAM360 installations are the same, i.e., both 64-bit or both 32-bit.
- The same version of PAM360 should be installed in both the machines.
- If you want to remove High Availability and migrate to Failover Service, follow the steps in this document.

Step 2: Database Setup

Failover service can be configured only with MS-SQL cluster setups as backend database. Follow the steps in this document to use MS-SQL cluster as backend database.

Note: While mapping the clustered instance of the MS-SQL database with PAM360, ensure that you enter only the fully qualified DNS name of the failover clustered instance.

Step 3: Failover Service configuration in Primary and Standby installations

A) Configuration to be done in Primary Installation:

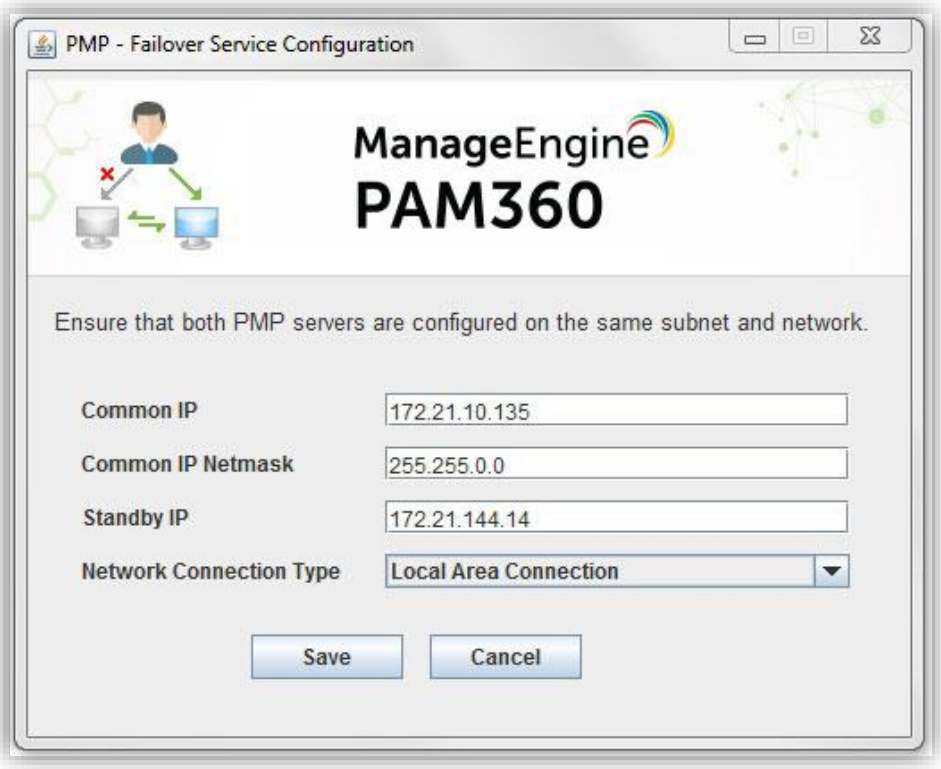
Open the **command prompt** with **administrator privileges** and navigate to **<PAM360_Primary_Installation_Folder>/bin** directory. Run the script **FOSSetup.bat**
In the pop-up that appears, enter the details as specified below for each field:

Common IP: Assign a common IP address for both the Primary and Standby PAM360 servers, so that the PAM360 web interface could always be connected to this specific IP. The PAM360 server will be bound by this single public IP and irrespective of whether PAM360 is running as Primary or Standby, end-users can connect to the same public IP. **The common IP that you enter here should be static and not be assigned to any other machine.**

Common IP Netmask: Specify the subnet mask value of the Common IP.

Standby IP: Enter the IP address of the Standby server. This step ensures that the Primary knows where the standby is running and vice-versa.

Network Connection Type: Ensure that both Primary and secondary servers rest on the chosen network.



Note: Before saving the details, make sure that PAM360 is not running during the configuration process.

Once you enter the details and click 'Save', the configuration settings will be created as a .zip file in primary. This configuration pack will be named as "**FOSPack.zip**" and placed under the directory: **PAM360-Primary-Installation-Folder>/FailoverService**. This step completes the Failover service configuration in Primary. To configure FOS in the standby, the first step is to copy this .zip file and place the same in the PAM360 standby installation home directory.

B) Configuration to be done in Standby Installation

Open the **command prompt** with **administrator privileges** and navigate to **<PAM360_Standby_Installation_Folder>/bin** directory. Run the script **ConfigureStandbyFOS.bat** <file-path>, passing the location of FOS configuration settings pack .zip file as the command line argument. Once unzipped, FOS instance will get installed in the Standby installation as well.

Once the FOS settings pack has been unzipped and installed in the Standby, ensure that the **pam360_key.key** file, which contains the encryption key, is present in the configuration file named **manage_key.conf** under **<PAM360_HOME>/conf** folder in both the primary and standby installations.

Note: PAM360 License - Normally, when the FOS Settings file is unzipped in the standby, the PAM360 license will also get automatically reflected respectively. Therefore, standby does NOT require a separate license file. You can use the same license you purchased for primary. On the other hand, if you are changing your PAM360 license in the future, the same will not get reflected in the standby. In that case, you need to apply the license file in the standby as a separate step.

Step 4: Start Failover Service(FOS) in Primary and Standby

Navigate to Windows Services Panel. Upon configuration of Failover Service, the panel will begin showing two PAM360 services - "PAM360" and "PAM360 Modules". For the Failover service to function, only the "**PAM360**" service should be started in both Primary and Standby. While PAM360 application in the primary will be up and running, PAM360 application in the standby will just be monitoring the primary in FOS mode. It will get started when the primary goes down.

Note: By default, the standby monitors the primary's status once in every 40 seconds. In case, it finds that the primary is down and not running, it tries twice to ensure that the primary is down before starting up PAM360 application.

3. How to Uninstall the Failover Service?

You can deactivate Failover service either from the primary or secondary server. To uninstall, execute **UninstallFOS.bat** in **{Prod-home}/bin** folder, from any of the servers. With the completion of this step, failover service will get deactivated. Next, you can uninstall PAM360 itself completely from the other server.

4. Troubleshooting Tips

1. After configuring Failover Service, you should run PAM360 service and PAM360 Modules service with a domain account that has sysadmin privileges in the MS SQL server.
2. Ensure all the machines are accessible from both master and standby instances of PAM360.

Database Backup (PostgreSQL)

Data stored in PAM360 is of critical importance. In any production environment, there would be constant requirements for backing up the data, either for reference purposes or disaster recovery. To achieve this, PAM360 provides the Database Backup feature.

The rest of the document allows you to understand two types of Database Backup in detail.

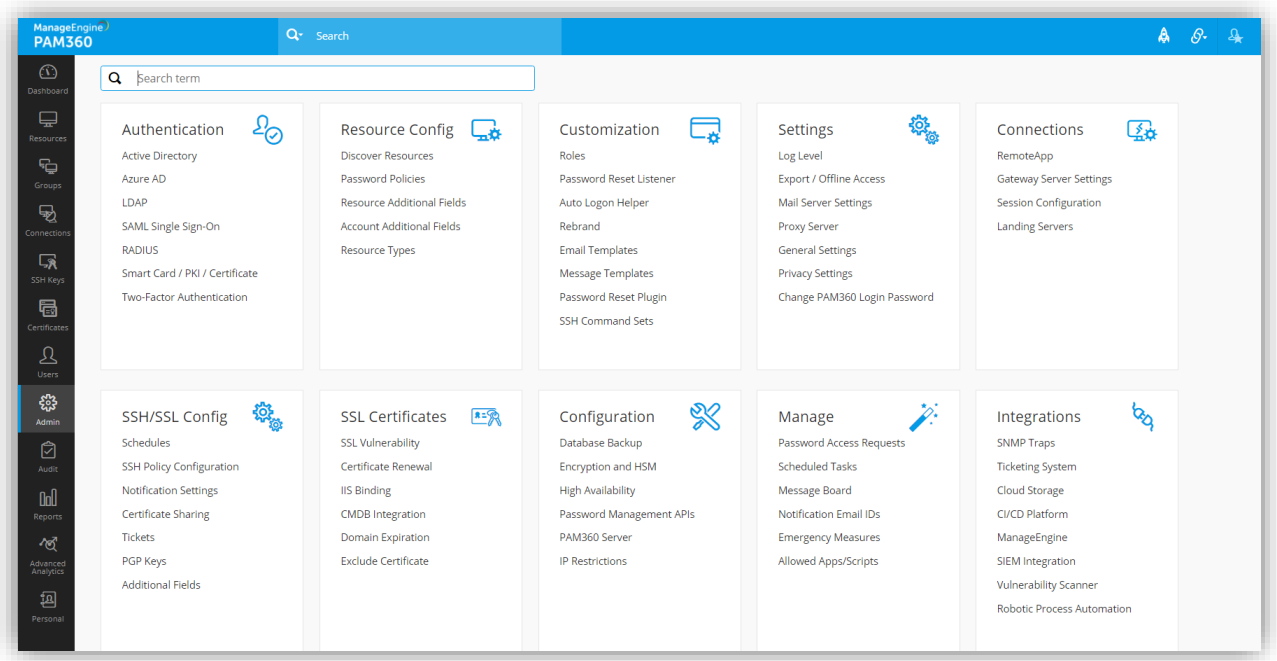
1. **Scheduled Backup**
2. **Instant Backup**

1. Scheduled Backup

This type of backup allows you to schedule the database backup to be executed at any specific point of time.

Steps to Schedule a Database Backup:

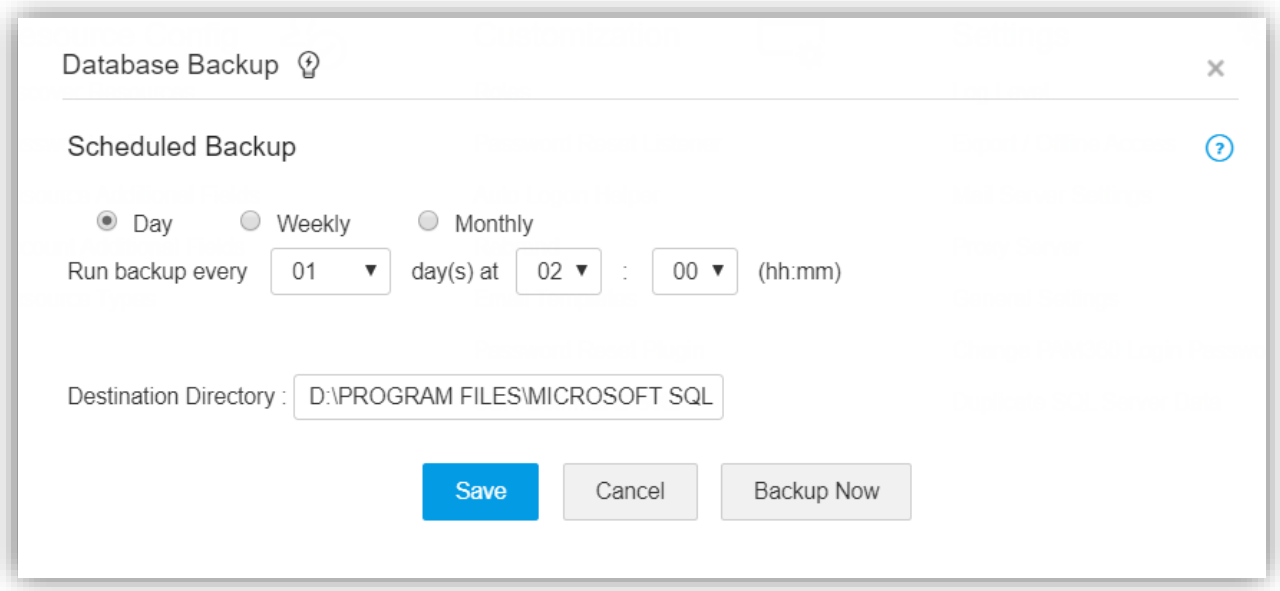
1. Navigate to **Admin >> Configuration >> Database Backup**.



2. In the pop-up window that appears, select the schedule option - **day, weekly** or **monthly**.
3. Select the time frequency **(dd:hh:mm)** at which the backup has to occur.
4. The **Destination Directory** field shows the default directory path: **<PAM360_Home>/backUp**. You can change the path, if required.
5. Every time backup is executed according to schedule, one backup file will be created. Specify the maximum number of latest backup files to be stored in the directory. For

example, if you choose "**10**" from the drop-down **Maintain latest**, only the latest 10 backup files will be stored in the directory.

6. Click **Save**. The required backup schedule is created.



2. Instant Backup

This type of backup allows you to execute a Database Backup instantly.

1. Navigate to **Admin >> Configuration >> Database Backup.**
2. Click **Backup Now.**

Now, your database has been backed up successfully.

Database Backup (MS SQL Server)

Data stored in PAM360 database is of critical importance. In any production environment, there would be constant requirements for backing up the data, for either reference purpose or disaster recovery. You can schedule tasks to back up the database contents periodically. The backup will be stored as a **.bak** file by default in the host, where the SQL server is running. All the sensitive data will remain encrypted in that file.

The rest of the document allows you to understand two types of Database Backup in detail:

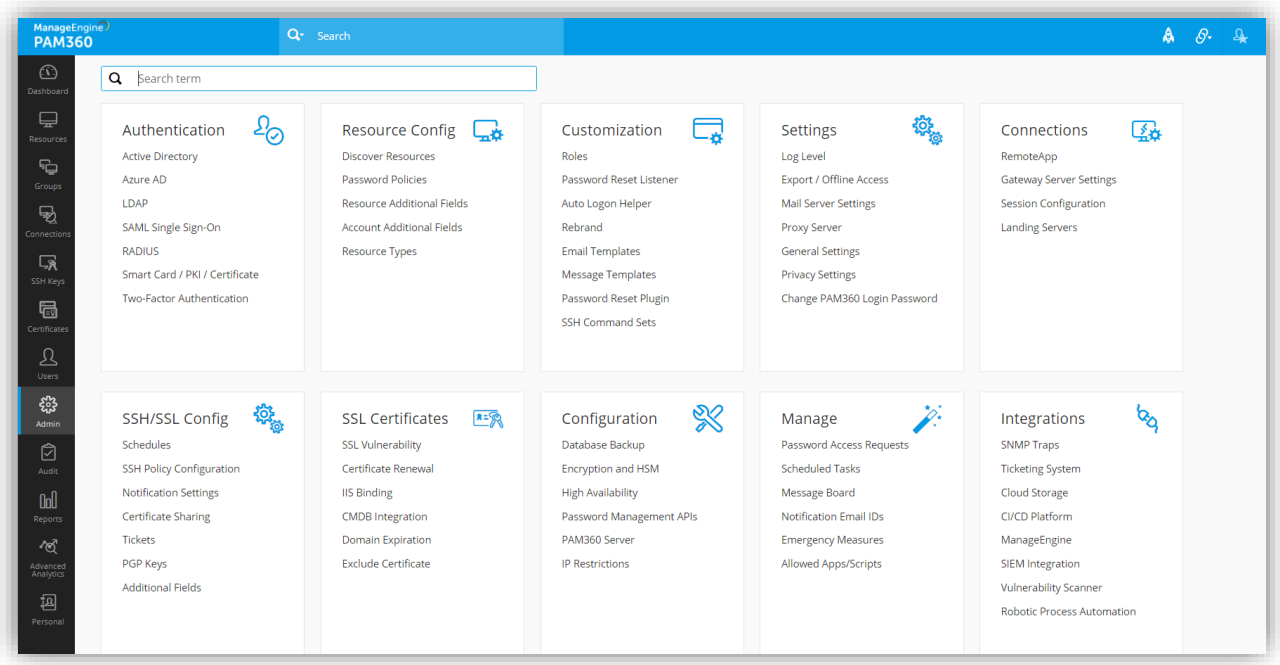
1. **Scheduled Backup**
2. **Instant Backup**
3. **Offline Backup**

1. Scheduled Backup

This type of backup allows you to schedule the database backup to be executed at any specific point of time.

Steps to Schedule a Database Backup:

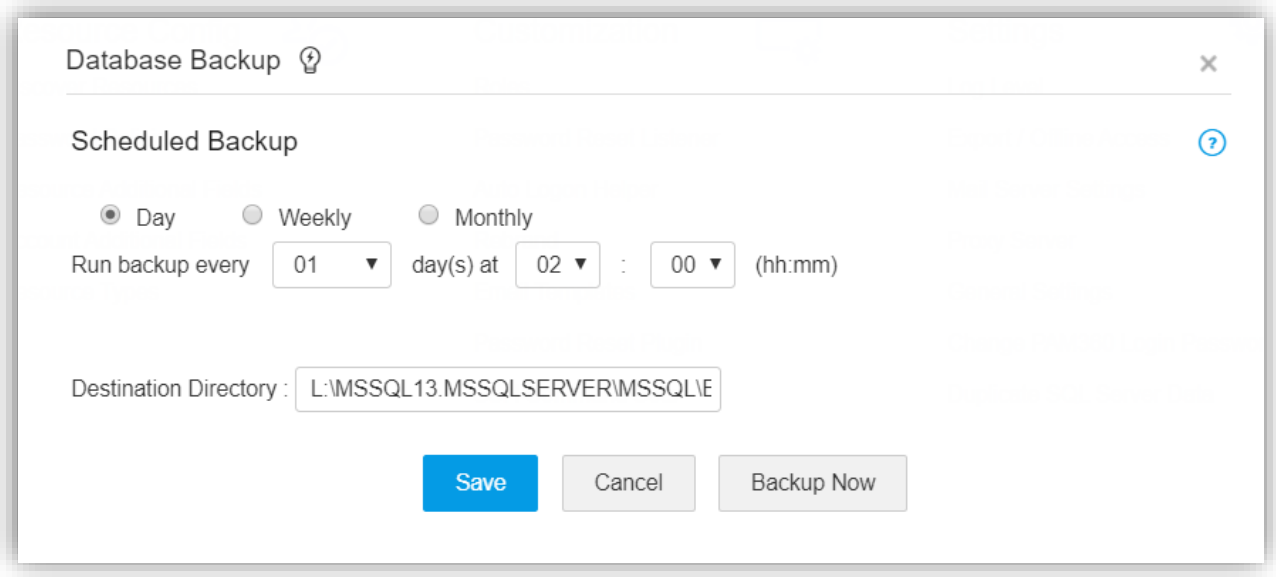
1. Navigate to **Admin >> Configuration >> Database Backup**.



2. In the window that pops up, select a schedule option - **day, weekly** or **monthly**.
3. Select the time frequency **(dd:hh:mm)** at which the backup has to occur.
4. The **Destination Directory** field shows the directory path **(<MSSQL_installation_folder>\Backup)** in the **host where the SQL server is running**. The

backup will be stored as a **.bak** file which holds all the encrypted sensitive data. It is recommended that you backup this file to a secure, secondary storage. The backup file will have the file name structure as **pam360backup_pam360version_YYMMDD-time.bak**.

5. Click **Save**. The required backup schedule is created.



2. Instant Backup

You can take a one-time, on-demand backup anytime, by clicking the button **Backup Now** available in the web interface shown above.

3. Offline Backup

Follow the steps below to take an offline backup of your PAM360 data:

1. Stop the PAM360 service.
2. Open the command prompt and navigate to the **<PAM360_Installation_Folder>/bin** directory.
3. Execute the command **BackupDB.bat**.

A **.bak** file is created with the following file name structure: **OfflineBackup_backupdate-time**.

Data Restore

In the event of a disaster or data loss, you can restore the backed up data to the PAM360 database. To restore the data, PAM360 provides scripts.

In the following sections, you will learn in detail, the steps for data restoration for the below databases:

1. PAM360 with PostgreSQL

   1.1 Windows

   1.2 Linux

2. PAM360 with MS SQL Server

1. Steps Required for PAM360 with PostgreSQL

The following steps are applicable for the default installation of PAM360 with PostgreSQL as the backend database.

Important Notes:

1. Stop PAM360 server before trying to restore data. If restoration is done while the server is running, it may lead to data corruption.
2. Data backed up from PAM360 running on Windows can be restored only in Windows.
3. While restoring the back up, ensure that you re-install the same PAM360 build that was present earlier. For example: If you had PAM360 build 4500 previously, then install the same again.
4. Make sure you start and stop the service once each time before using the restoreDB command.

1.1 For Windows

1. Navigate to the **<PAM360_Installation_Directory>/bin** folder.
2. Execute the script '**restoreDB.bat <backup file name> -p <Key path>'.** Enter your backup file name in .ezip format. Note that the backup file and the pam360_key.key file should be located in the same folder under the same path inside the PAM360 server.
3. Open the **<PAM360_Installation_Folder>/conf** folder, edit the **manage_key.conf** file, and specify the location of **pam360_key.key** (AES 256 encryption master key). PAM360

requires the pam360_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

4. The backed up contents would be restored to the PAM360 DB. Now, execute the command **updateserverconf.bat**. In the pop-up that appears, enter the default certificate name as **Server.keystore** and password as **passtrix**. This action will apply the default SSL certificate that comes with the product to your PAM360 server.
5. To add your trusted SSL certificate to your PAM360 server, follow these steps:
    i. Login to the PAM360 web interface using an administrator account and go to **Admin >> Configuration >> PAM360 Server.**
    ii. Here, browse for your trusted certificate, enter the necessary certificate details, and save the changes. Now, your PAM360 server will be encrypted using the trusted SSL certificate you provided.

1.2 For Linux

1. Navigate to the **<PAM360_Installation_Directory>/bin** folder.
2. Execute the script **'sh restoreDB.sh <backup file name> -p <Key path>'.** Enter your backup file name in .ezip format. Note that the backup file and the pam360_key.key file should be located in the same folder under the same path inside the PAM360 server.
3. Open the **<PAM360_Installation_Folder>/conf** folder, edit **the manage_key.conf** file, and specify the location of **pam360_key.key** (AES 256 encryption master key). PAM360 requires the pam360_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.
4. The backed up contents would be restored to the PAM360 DB. Now, execute the command **updateserverconf.sh**. In the pop-up that appears, enter the default certificate name as **Server.keystore** and password as **passtrix**. This action will apply the default SSL certificate that comes with the product to your PAM360 server.

> **Note:** Before executing the **updateserverconf.sh** command, ensure that x11 is enabled on your PAM360 server.

5. To add your trusted SSL certificate to your PAM360 server, follow these steps:
    i. Login to the PAM360 web interface using an administrator account and go to **Admin >> Configuration >> PAM360 Server.**
    ii. Here, browse for your trusted certificate, enter the necessary certificate details, and save the changes. Now, your PAM360 server will be encrypted using the trusted SSL certificate you provided.

2. Steps Required for PAM360 with MS SQL Server

2.1 Prerequisite

PAM360 uses SQL server's encryption mechanism to encrypt the data. The encryption master key will be stored under **<PAM360 Installation Folder>/conf** directory with the name **masterkey.key**. For security reasons, during installation of MS SQL, we recommend moving the encryption key from the default location to a secure location and use it while performing disaster recovery.

2.2 Procedure

Step 1

Install another instance of PAM360 with MS SQL server as the backend. You are now specifying a new instance of MS SQL server where the backup has to be restored. Ensure that the new instance of MS SQL server is configured with SSL. For details, refer steps 10.1.1 to 10.1.3 under MS SQL Configuration.

Step 2

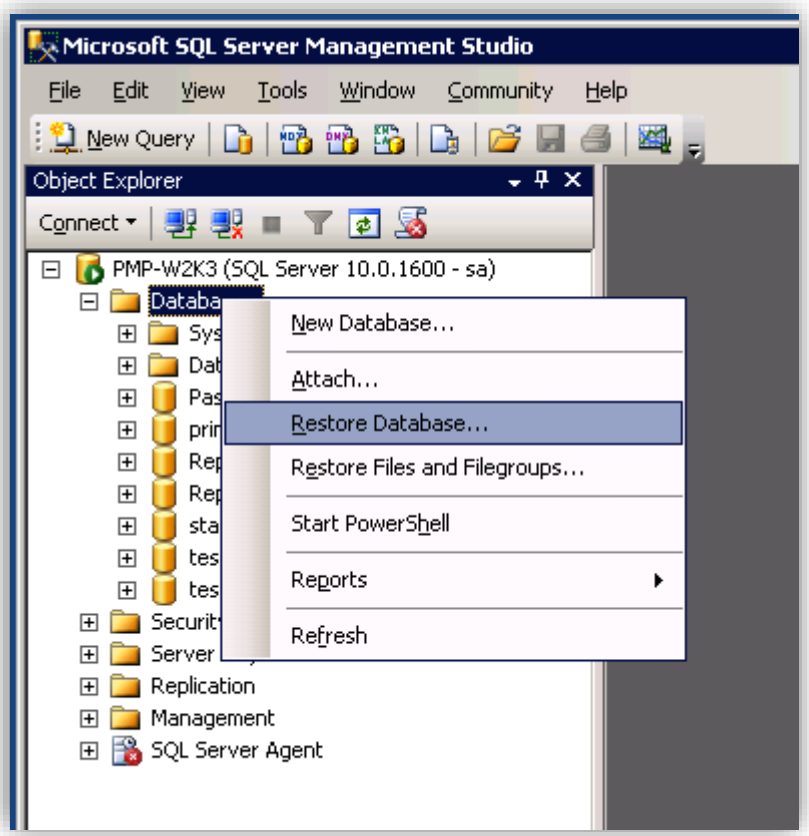
Copy the PAM360 backup file from the SQL server. By default, it will be present under the **<MSSQL_installation_folder>/Backup** folder with a file name in the following format: **pam360backup_pam360version_backupdate-time.bak** (For example, pam360backup_4500_110721-1159.bak). Click here to learn more about taking backups of your PAM360 data. The backups taken from the MS SQL database will be stored as a **.bak** file in the host, where the SQL server is running.

Step 3

Launch "Microsoft SQL Server Management Studio" (in the machine where the backed up data are to be restored - that is, another instance of SQL server) and connect to the Database Engine.

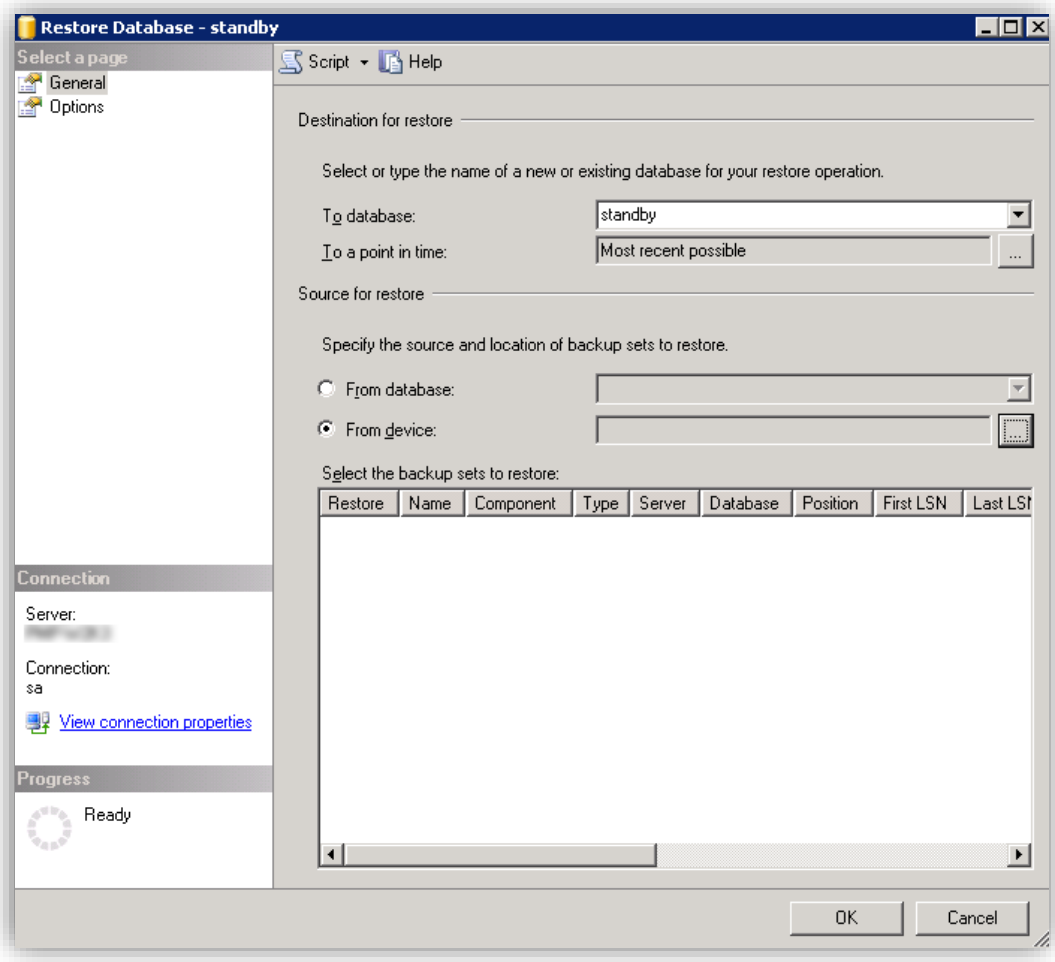
Step 4

Right-click on **Databases** and the click **Restore Database** from the displayed menu.



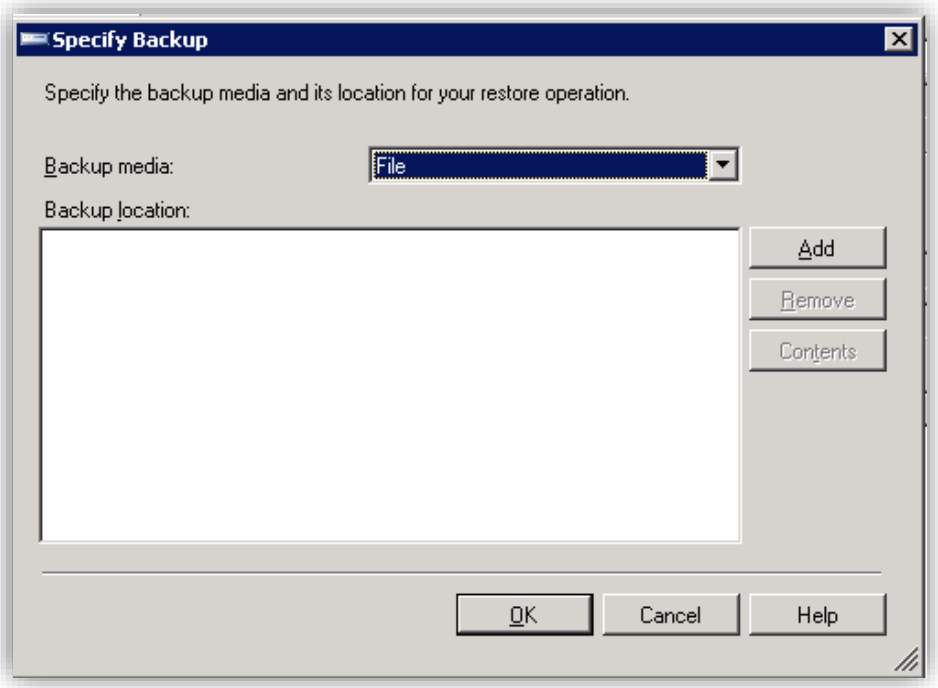
Step 5

In the **Restore Database** window, choose the option **From device** and click the [...] button to browse the PAM360 backup file.



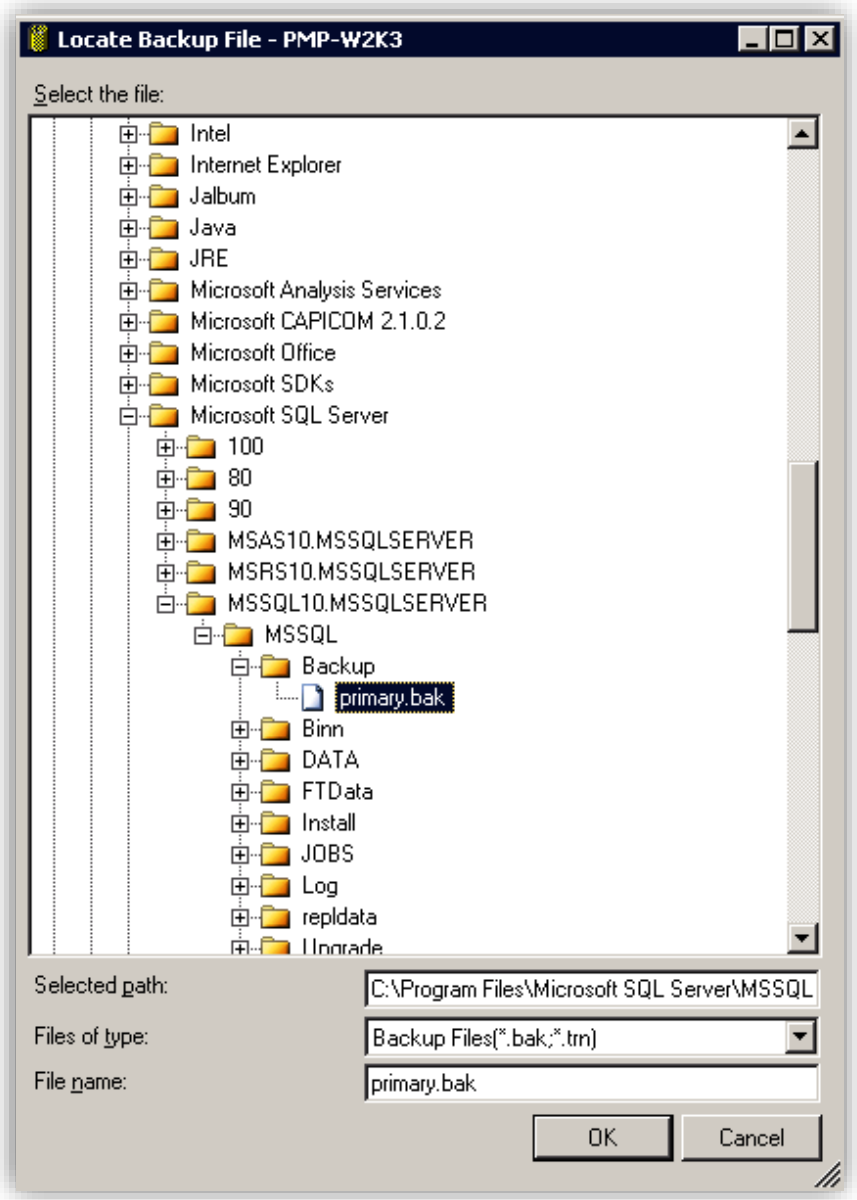
Step 6

In the **Specify Backup** window that opens up, choose the option **File** as the Backup media and click **Add**.



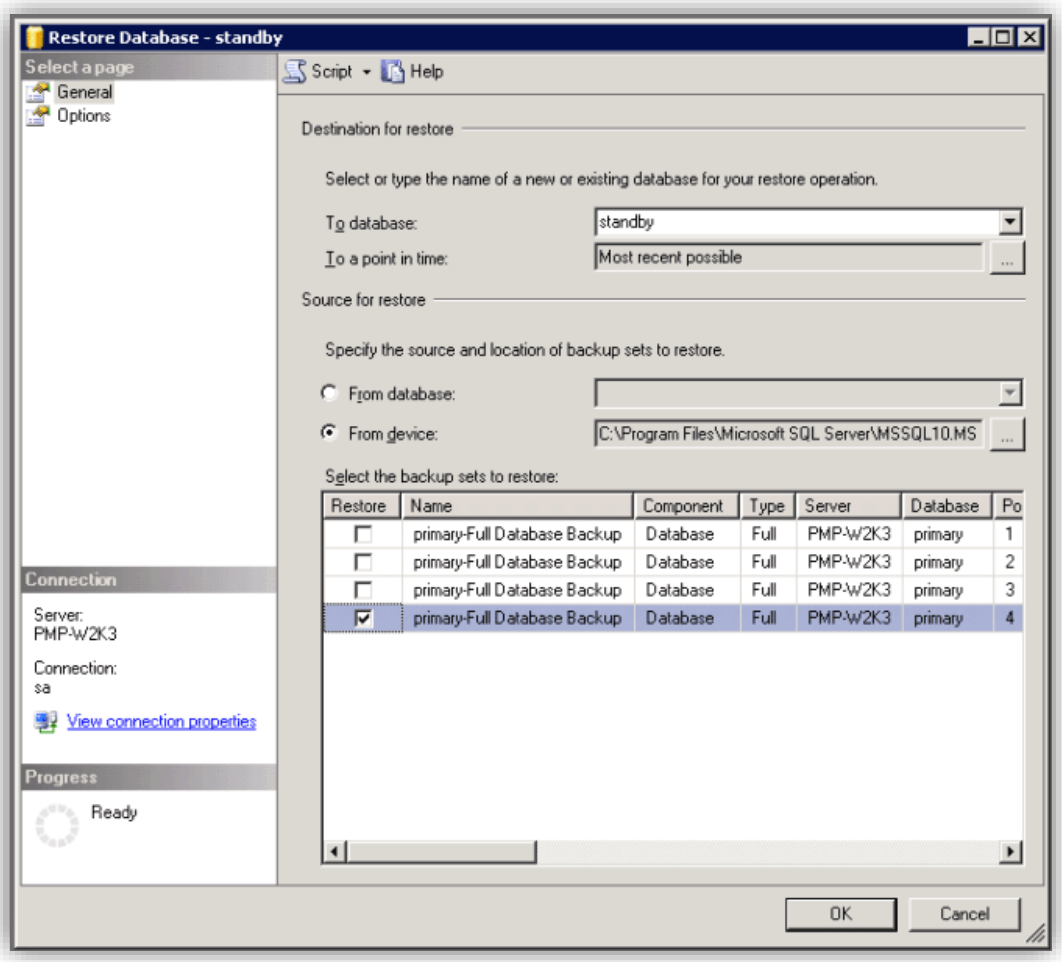
Step 7

In the **Locate Backup File** window, select the PAM360 backup file and click **OK**.



Step 8

1. Now, in the **Restore Database** window, select the database where the backup is to be restored and specify it in the **To database** field.
2. Under **Select the backup sets to restore**, select the required **Restore column**.
3. Click **OK** to start the restoring the database.
4. Upon completion of the restoration, a status window pops-up.



Step 9

Now, you need to restore the Master Key. As mentioned in the prerequisite section above, by default, the encryption master key will be stored under **<PAM360 Installation Folder>/conf** directory in the file named **masterkey.key**. For security reasons, if you have moved the file to some other secure location, identify that. Open the **masterkey.key** file and copy the password.

Step 10

1. Connect to the SQL server in which you have restored the PAM360 backup file.
2. Open Microsoft SQL Server Management Studio and connect the database engine.
3. Execute the following queries:

```
use write_the_name_of the restored_database;
OPEN MASTER KEY DECRYPTION BY PASSWORD = 'type_the_master_key_password';
alter master key regenerate with encryption by password =
'type_the_master_key_password';
```

Example:

```
use passtrix;
OPEN MASTER KEY DECRYPTION BY PASSWORD = 'secret';
```

alter master key regenerate with encryption by password = 'secret';

Execution of the above queries will help decrypt the data.

Step 11

Navigate to **<PAM360_Installation_Folder>/conf** folder, edit **manage_key.conf** and specify the location of **pam360_key.key** (encryption master key). PAM360 requires the pam360_key.key file accessible with its full path when it starts up every time. After a successful start-up, it does not need the key anymore and so the device with the key file can be taken offline.

Important Notes:

1. Perform database restore of the .bak file and execute the above queries to set the master key using the same account with which PAM360 connects to the database.
2. However, if you are using a different account to restore the database in SQL studio and to execute the Alter master key queries, then execute the additional queries given below to provide required permissions for the PAM360 account to read the master key.

   GRANT VIEW DEFINITION ON CERTIFICATE::PMP_CERT TO [user]
   GRANT VIEW DEFINITION ON SYMMETRIC KEY::PMP_SYM_KEY TO [user]
   GRANT CONTROL ON CERTIFICATE::PMP_CERT TO [user]

3. The [user] in the above queries refers to the actual login name of the account used by PAM360 to connect to the SQL database. You can find this account's name in the JDBC URL present in the **<PAM360_Installation_Folder>/conf/database_params.conf** file, unless the account uses Windows authentication.
4. Execute the queries given below to verify the correct names of the CERTIFICATE and SYMMETRIC KEY:

   select * from sys.certificates
   select * from sys.symmetric_keys

Application Scaling in PAM360 using Microsoft SQL Server

In general, Scaling is the process of making an application bigger and better, and scalability is the inherent capacity of an application to handle growth without any hindrance. For a privileged access security solution like PAM360, it is essential to make it highly available and scalable so that even with increased complexity, the application can render the maximum overall performance, without having any significant effect on the average service level per node.

The Application Scaling model in PAM360, designed using Microsoft SQL server, is aimed at providing enhanced scalability and performance while ensuring uninterrupted access to the privileged resources and passwords stored in PAM360. The model works with one main PAM360 node and several sub-nodes, all of them connected to a single MS-SQL database cluster.

> **Note:** The application scaling model in PAM360 currently works only with the MS-SQL database cluster.

1. How does it Work?

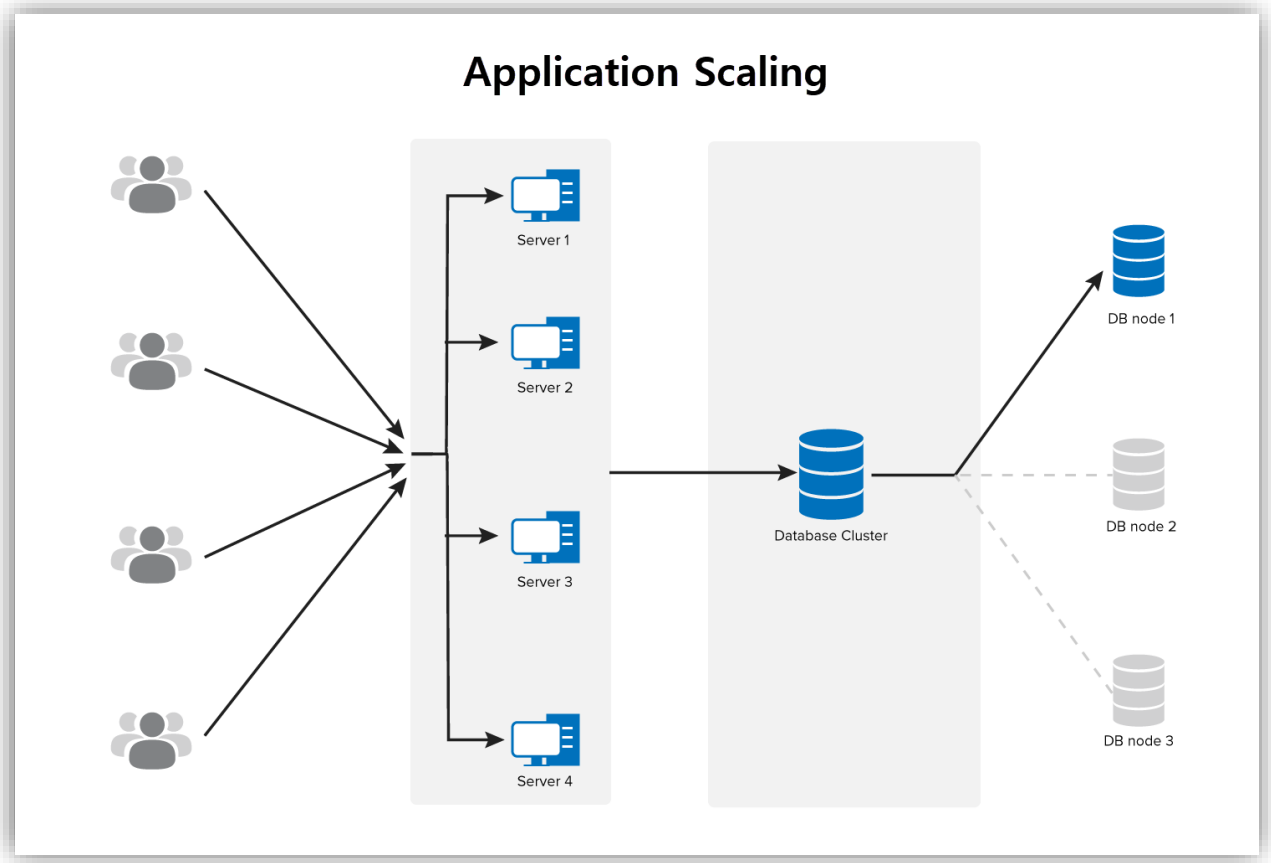
The main node for PAM360 and all its sub-nodes must point to the same MS-SQL cluster, though they do not have to be connected individually. However, the main node, i.e., the machine that will carry out the scheduled operations, requires to fulfill either of the following conditions:

1. The main node and the target end-points, having the agentless password management capabilities enabled from PAM360, should reside in the same subnet.

   (OR)

2. If the main node and the target end-points reside in different networks, they should be able to communicate with each other, i.e., they should not be blocked by a firewall or reside outside the range of connectivity such as demilitarized zones.

The Schematic Architecture Diagram Depicting Application Scalability in PAM360



Notes:

1. You can assign any of the secondary nodes as the main node, provided it has proper connectivity to other machines to carry out the scheduled operations without any interference.
2. The current model allows you to assign up to three machines as sub-nodes.

2. Steps to Configure the Main Node and Sub-Nodes

To configure sub-nodes pointing to the same cluster, follow the below steps:

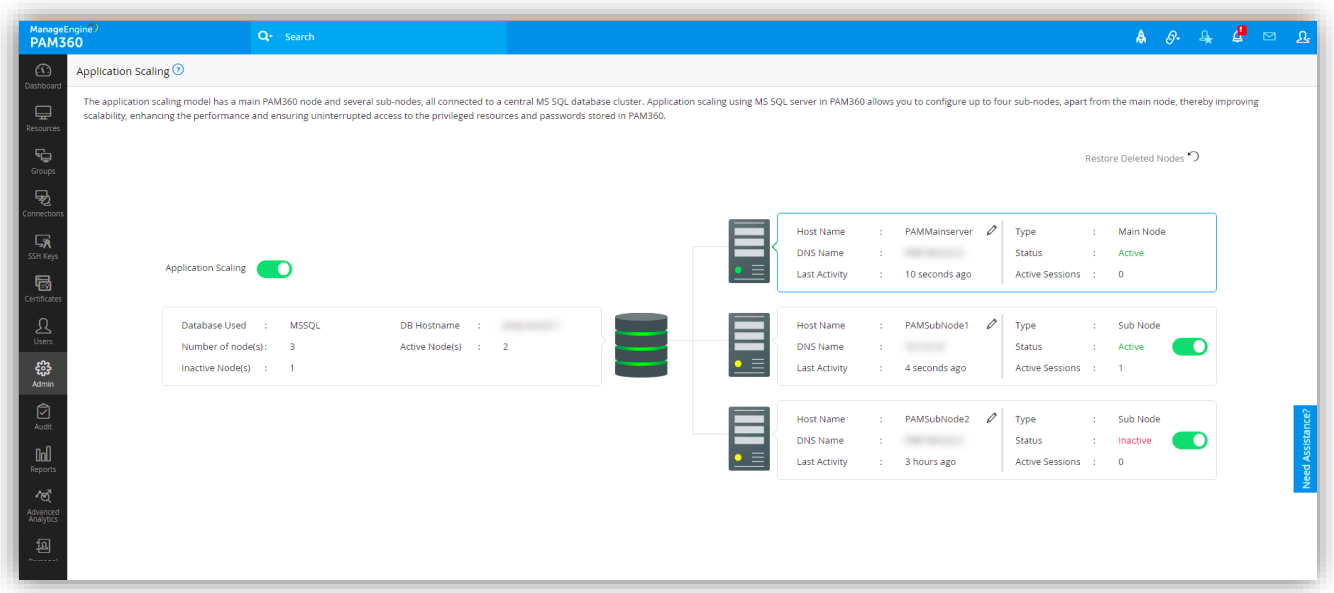
1. Install PAM360 in the machine which you want as the main node.
2. Configure an SSL certificate in your MS SQL cluster, import the certificate into PAM360, and point the application to a SQL listener IP/Host. Now, the PAM360 application operating as the main node will work using the MS SQL Cluster.
3. Install PAM360 in the secondary application servers, which you want as sub-nodes. During the installation process, choose the Primary Server in the installation wizard. Once the installation is complete, PAM360 will start with the default PostgreSQL

database. Stop the PAM360 service after the initial startup.

4. Copy and paste the MS SQL cluster certificate into the **<PAM360 Installation Folder>\bin** directory in all the sub-nodes. Open a command prompt and execute the command **importCert.bat Your_cluster_cert.cer**. This command will import the MS SQL cluster certificate into all the sub-nodes.
5. Copy the **pam360_key.key** file from the main node and paste it into any directory in the sub-nodes. Now, update the full path of the **pam360_key.key** file in the **<PAM360-Home>\conf\manage_key.conf** file in all the sub-nodes. If the key is stored in a remote directory, then supply the full path of the remote location in the **manage_key.conf** file.
6. Open the services console (services.msc) in all the sub-nodes and update the service account of the PAM360 service. Ensure that this service account has all the necessary permissions to connect to the MS SQL cluster and to read the pam360_key.key file.
7. Open command prompt as administrator in all the sub-nodes and navigate to the **<PAM360 Installation Folder>\bin** directory and execute the command **ChangeDB.bat**. In the **DB Change Configuration** wizard, select SQL server as the backend, supply the MS SQL Cluster hostname in the format SERVER:port. For example, CLUSTER01:5432. If port number is specified in this format, the Instance name field can be left empty. If Cluster is using dynamic ports, then supply the correct hostname and the instance name separately. Provide the correct SQL database name using which the main node is working and select **Windows** as the authentication option. For this option to work, note that command prompt should be running with an account that has access to the SQL database. Click **Test** and once it is successful, click **Save** to save the changes.
8. Edit the file named **system_properties.conf** present in the path **<PAM360_installation_directory>\conf** in the sub-nodes using Wordpad with administrator rights. Add the line **ignore.scheduler=true** at the end of the file and save it.
9. Now, start the PAM360 service in all the sub-nodes. As a result of all the previous steps, all the sub-nodes will start using the same MS SQL Cluster as the backend database.
10. The default URL of the sub-nodes will look like **https://subnode_servername:8282**. To apply your license file in all the sub-nodes, open the URL of all the sub-nodes in a web browser and login. Click the profile icon in the top right corner and click the **License** option. Here, add your license XML file and apply.
11. Navigate to **Admin >> Configuration >> PAM360 Server** and update your SSL certificate keystore with the correct password. If required, change the port from 8282 to 443 and save the settings.
12. Restart the PAM360 service in all the sub-nodes. Now all the sub-nodes will start with the correct SSL certificate and use the same MS SQL Cluster backend.

2.1 Steps to View the Configured Nodes in PAM360

Once the main node and sub-nodes are configured, navigate to **Admin >> Configuration >> Application Scaling** to view them from the PAM360 interface. Here, you can enable or disable Application Scaling using the toggle button.



3. Steps to Change a Sub-Node into a Main Node

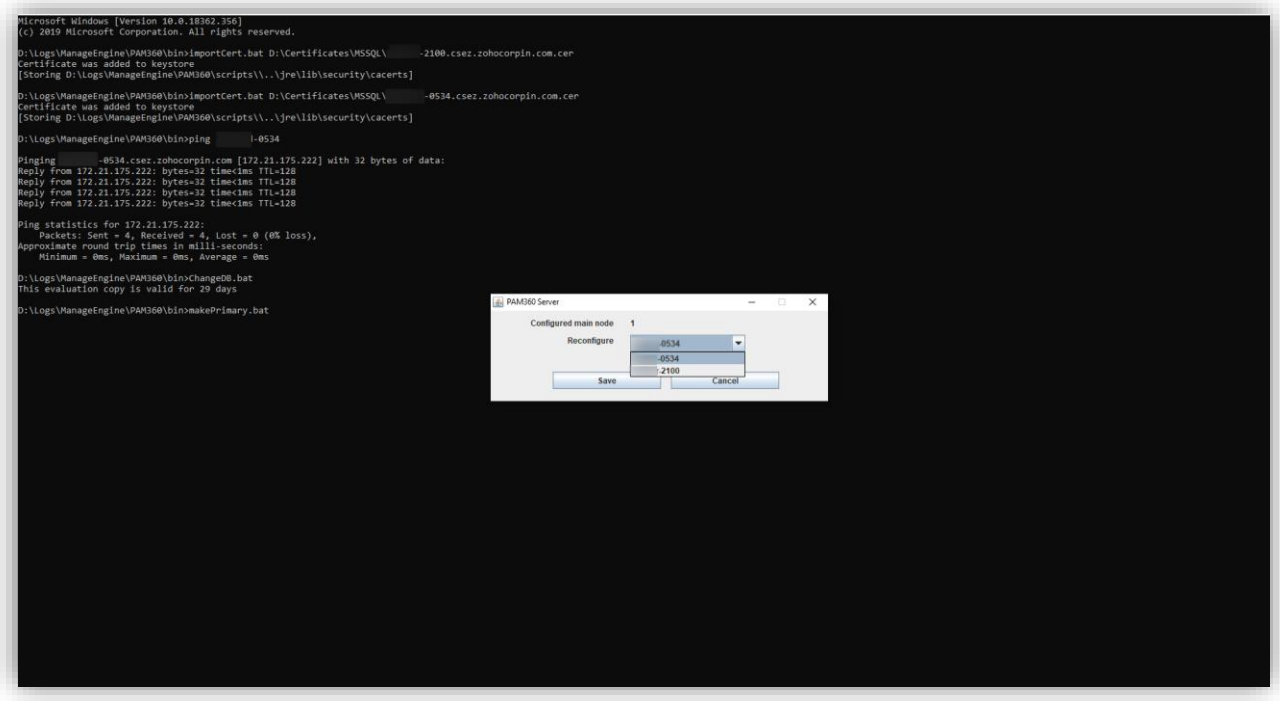
Follow the below steps to change any secondary node into the main node. This change can be done at any point of time from any sub-nodes.

1. Keep the MS-SQL database running.
2. Stop all application servers including the main node.
3. Open a command prompt and execute the following commands:

   For Windows:
   <PAM360_installation_directory>\bin\makePrimary.bat

   For Linux:
   <PAM360_installation_directory>/bin/sh makePrimary.sh

4. Current main node and the list of available servers will be displayed. Choose any server from the drop-down and click **Save**.



5. Restart all application servers that were stopped earlier.
6. The selected server will be assigned as the main node now.

Click here for more information on how to set up a Microsoft SQL cluster.

4. Steps to Rename a Node

1. Navigate to **Admin >> Configuration >> Application Scaling.**
2. From the Application Scaling dashboard, click the **edit** icon beside the desired node.
3. In the pop-up that appears, enter a name and click **Confirm.**
4. You have successfully renamed the node.

> **Note:** Only the Administrators and users with custom roles having the 'Application Scaling' permission can enable/disable, delete, and restore the sub-node(s), that too, from the Main node only.

5. Steps to Enable/Disable a Sub-Node

1. Navigate to **Admin >> Configuration >> Application Scaling.**
2. From the Application Scaling dashboard, enable/disable the toggle beside the respective Sub-node to enable or disable the sub-node.

6. Steps to Delete and Restore a Sub-Node

Navigate to **Admin >> Configuration >> Application Scaling.**

To Delete a Sub-node,

1. First, disable the Sub-node using the toggle.
2. Click the **Delete** icon on the top right corner of the Sub-node. In the pop-up that appears, click **Confirm.**
3. You have successfully deleted the Sub-node.

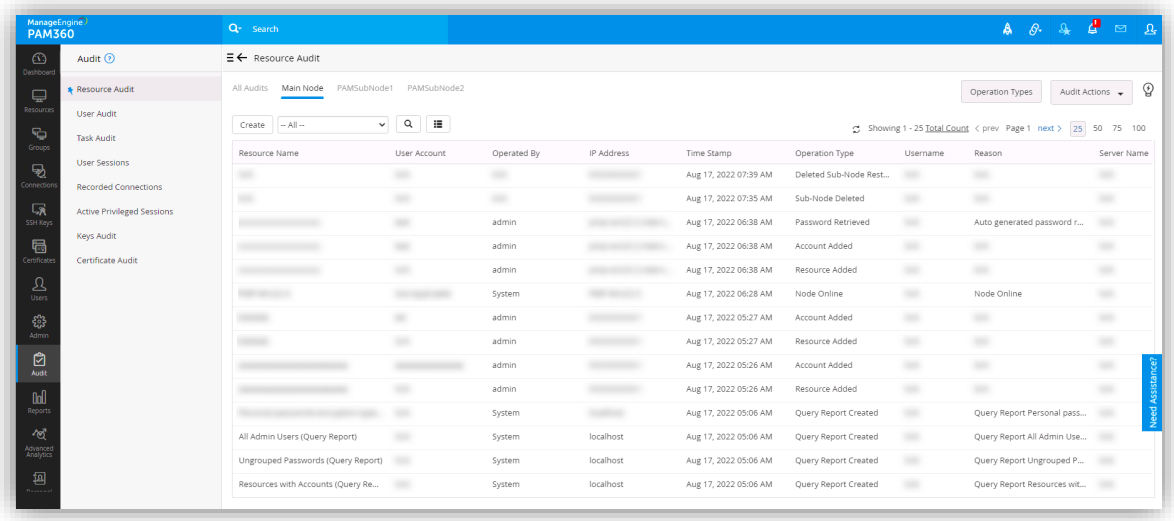
> **Note:** To install custom certificates, replace the path of the certificate in the above command.

To Restore a Sub-node,

1. Click **Restore Deleted Nodes** from the UI.
2. Now, select the desired Sub-node(s) and click **Restore.**
3. You have successfully restored the selected Sub-node(s).

7. Node Audit Trails

PAM360, by default, provides separate sections for Resource, User, and Task-based audits. Additionally, the product shows node-based audits for the main node and each sub-node as separate columns with the complete audit trails under Resource Audit and User Audit when Application Scaling is enabled. To know more about Audits, click here.



Application Scaling in PAM360 using PostgreSQL Server

Considering the continually growing user base, an organization should have continuous and uninterrupted access to the database to provide sustainable service. In general, application scaling is the process of improving an application's ability to handle huge loads and operations without disrupting its performance and user experience.

In PAM360, implementing Application Scaling via the external PostgreSQL database cluster aims at providing uninterrupted access to the resources and accounts, thereby enhancing the application scalability and overall performance. The model operates with one main node and several subnodes connected by a single PostgreSQL database cluster.

At the end of this document, you will have learned the following topics related to Application Scaling:

1. Prerequisites
2. Configuring the Application Nodes (Main-Node and Subnode)
3. Changing a Subnode into a Main-Node
4. Node-Based Operations Performed from PAM360 Web Interface
5. Node-Based Audit Trails

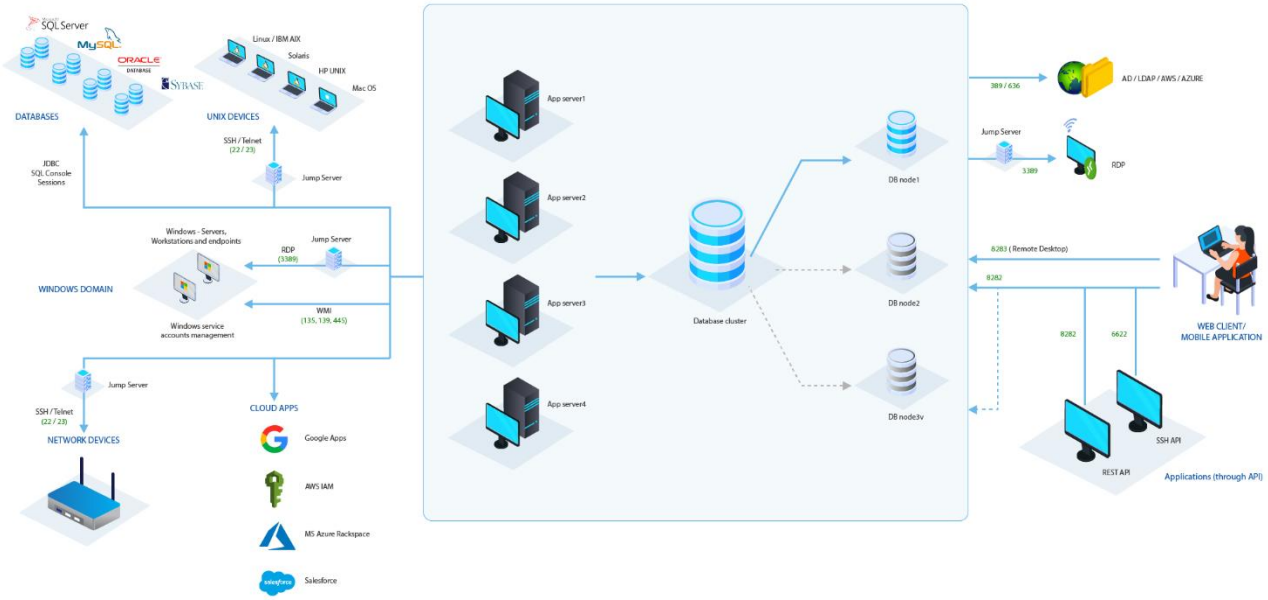
1. Prerequisites

The PAM360 main node and all its sub-nodes should point to the same PostgreSQL database cluster, although they do not need to be connected individually. However, the main node, i.e., the machine that will perform the operations, is required to satisfy any of any of the following conditions:

i. If PAM360's agentless password management capability is enabled, the main-node and the target endpoints should reside in the same subnet.
(or)
ii. The main-node and the target end-points must be capable of communicating with one another when residing in different networks, i.e., they should not be blocked by a firewall or situated outside the range of connectivity, such as demilitarized zone.

The Architecture Diagram Depicting Application Scalability in PAM360

PAM360 Application scaling architecture diagram



Notes:

1. You can change any configured subnode into a main-node until it has adequate connectivity to other machines and can carry out the scheduled operations without interruption.
2. You can create up to four subnodes in this application scaling model.

2. Configuring the Application Nodes (Main-Node and Subnode)

To configure the main-node pointing to the database cluster, do the steps that follow:

1. Install the PAM360 application in the server that you want as the main-node.

Notes:

1. During the installation process, select the configuration server as the **'High Availability Primary Server'**.
2. Post the installation, do not start the PAM360 service.

2. Configure the PostgreSQL database cluster (refer to the configuration section) as the backend database. Now, the PAM360 application installed in the main-node will work using the standalone PostgreSQL database cluster.
3. Restart the PAM360 application post the external database configuration.

To configure a subnode pointing to the same database cluster, do the steps that follow:

1. Install the PAM360 application in the server that you want as the subnode.
2. Download the root CA certificate of the PostgreSQL database cluster. If you are unaware of creating an SSL for the PostgreSQL database, refer to this section to generate the required SSL certificates and validate the SSL connection.
3. Import the root CA certificate of the PostgreSQL database cluster into the PAM360 application installed in the subnode.
4. Open the command prompt and navigate to the **<PAM360_Primary_Installation_Folder>/bin** directory in the main node.
5. Execute the AppScalingSetup file that follow based on your Operating System:
   i. For Windows, execute the command **AppScalingSetup.bat**
   ii. For Linux - execute the command **AppScalingSetup.sh**
6. Navigate to **<PAM360 installation directory>\ApplicationScaling** and copy the file named **ApplicationScalingPack.zip**.
7. Now, navigate to the required subnode and paste the file into the **conf** folder present in the PAM360 installation directory.
8. Unzip the **ApplicationScalingPack.zip** in the conf folder of the subnode.
9. Copy the **pam360_key.key** file from the main-node and paste it into any directory of the subnodes. Now, update the full path of the **pam360_key.key** file in the **<PAM360-Home>\conf\manage_key.conf** file in the subnode. If the key is stored in a remote directory, supply the full path of the remote location in the **manage_key.conf** file.
10. Edit the file named **system_properties.conf** present in the path **<PAM360 installation directory>\conf** in the subnodes using Wordpad with administrator rights. Add the line **ignore.scheduler=true** at the end of the file and save it.
11. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** and open the file **pg_hba.conf**:
    i. Add an entry at the end with the IP address of the configured subnode. E.g., **host all <user name> <ip address>/32 md5**
12. Navigate to **<PostgreSQL_Installation_folder>pgsql_installation\data** and open the file **postgresql.conf**:

i. Search for **listen_addresses** and provide the IP address of the configured subnode in a comma- separated manner.

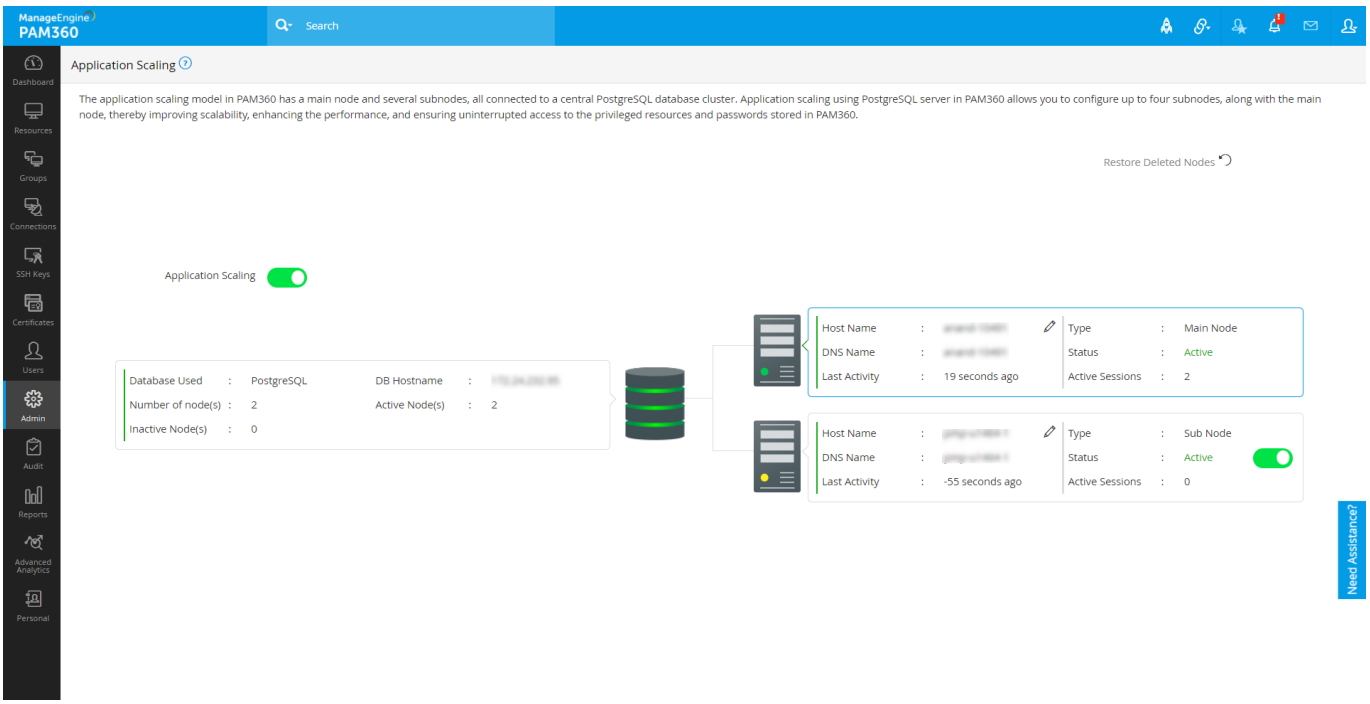
13. Restart the PostgreSQL server.

> **Note:** Repeat the procedure for all the required subnodes.

14. Now, start the PAM360 service in all the subnodes. As a result of the previous steps, all the subnodes will start using the same PostgreSQL cluster as the backend database.
15. The default URL of the subnodes will look like **https://subnode_servername:8282**. To apply your license file in all the subnodes, open the URL of all the subnodes in a web browser and log in. Click the profile icon in the top right corner and click the License option. Here, add your license XML file and upgrade.
16. Navigate to **Admin >> Configuration >> PAM360 Server** to update your SSL certificate in all your subnodes.
17. Restart the PAM360 service in all the subnodes.

Now all the subnodes will start with the relevant SSL certificate and use the same PostgreSQL cluster as the backend database.

Once the main-node and subnodes are configured, navigate to **Admin >> Configuration >> Application Scaling** to view and manage them from the PAM360 GUI.



3. Changing a Subnode into a Main-Node

Follow the below steps to change any of the configured subnode in the PostgreSQL database cluster into a main- node. This change can be done at any point in time from any of the available PAM360 application servers.

8. Keep the PostgreSQL database cluster running.
9. Stop all the PAM360 applications in the servers, including the main-node.
10. Open a command prompt and execute the following commands from any of the PAM360 application servers:

    For Windows:
    <PAM360_installation_directory>\bin\makePrimary.bat
    For Linux:
    <PAM360_installation_directory>/bin/sh makePrimary.sh

11. Executing the above commands will show the main-node and the list of available subnode servers. Choose any PAM360 application server from the drop-down and click Save.
12. Restart all the application servers that stopped earlier.
13. Now, the selected subnode server will start performing as the main-node.

4. Node-Based Operations Performed from PAM360 Web Interface

Note: Only the administrators and users with custom roles having the **'Application Scaling'** permission can enable, disable, rename, delete, and restore the subnode(s), from the server that act as a main-node.

a. Enable/Disable a Subnode

1. Navigate to **'Admin >> Configuration >> Application Scaling'**.
2. From the Application Scaling dashboard, click the **toggle** button beside the desired subnode to enable or disable it.

b. Rename a Node

1. Navigate to **'Admin >> Configuration >> Application Scaling'**.
2. From the Application Scaling dashboard, click the edit icon beside the **Host Name** of the desired node.
3. In the pop-up that opens, update the server name and click **Confirm**.
4. Now, you have successfully renamed the node.

c. Delete and Restore a Subnode

Navigate to '**Admin >> Configuration >> Application Scaling**'.

To Delete a Subnode:

1. First, disable the subnode using the **toggle** button.
2. Click the **Delete** icon on the top right corner of the subnode. In the pop-up that opens, click **Confirm**.
3. You have successfully deleted the subnode.

> **Note:** Deleting the subnode will only hide the node from the Application Scaling dashboard and will not remove the entry from the database cluster. Delete the physical server and any server-specific configurations to remove the server from PAM360 entirely.

To Restore a Subnode:

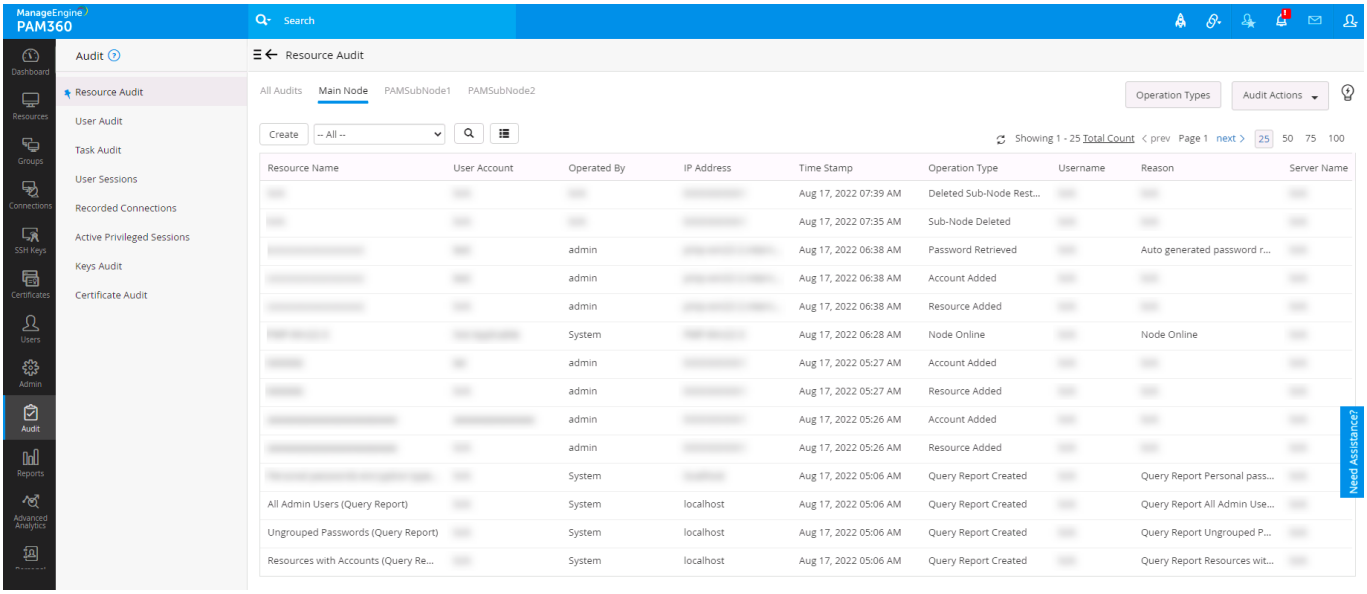
1. Click the **Restore Deleted Nodes** icon in the Application Scaling dashboard.
2. Now, select the desired subnode(s) and click **Restore**.
3. You have successfully restored the selected subnode(s).

> **Note:** The subnode(s) cannot be restored if the node(s) is(are) removed from the database cluster and the application server(s).

5. Node-Based Audit Trails

By default, PAM360 comprises Resource, User, and Task-based audit categories. Once configured and Application Scaling is enabled, the product additionally shows node-based

audits in each category with the main-node and available subnode(s) in separate columns. This assists you with the complete audit trails under Resource Audit and User Audit.

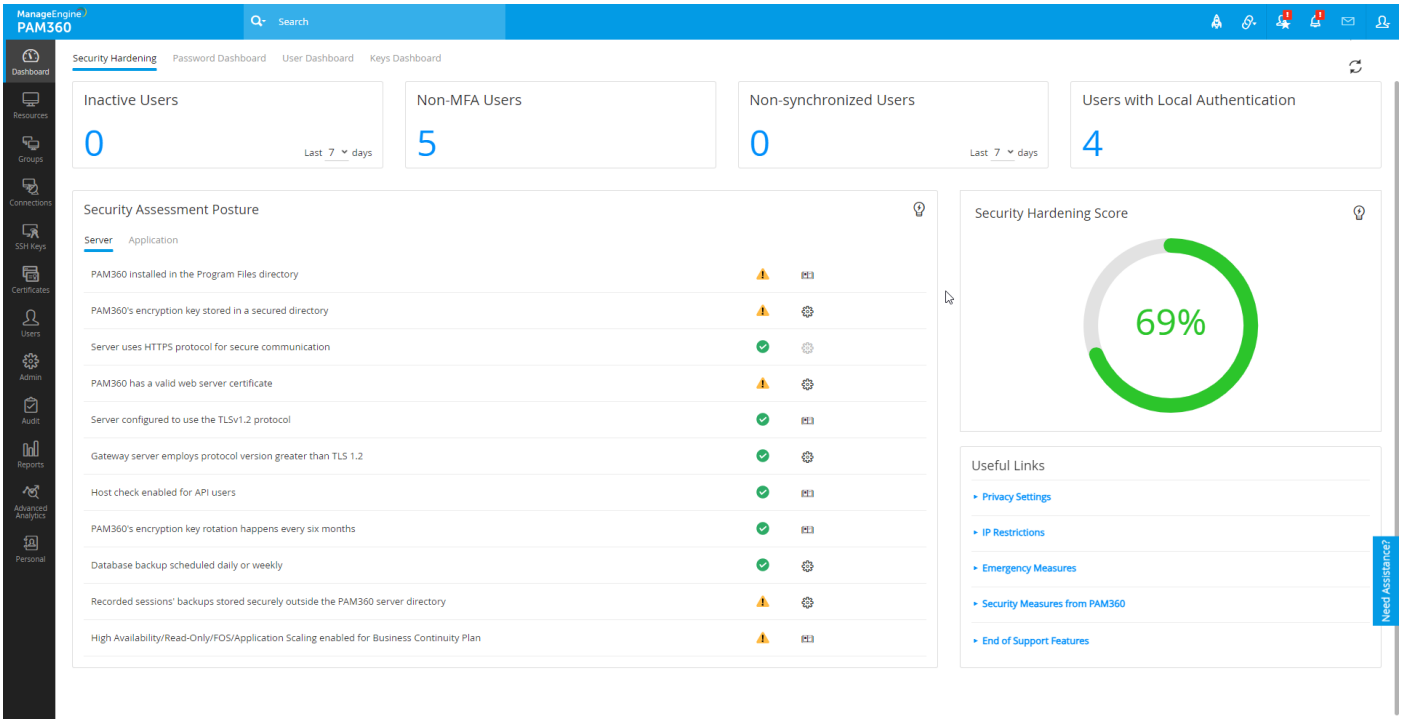


Security Hardening Dashboard

The security hardening dashboard is an advanced PAM360 dashboard designed to assess and enhance the security posture of both the PAM360 application and server, supported by a dynamic security score. This centralized dashboard serves as a powerful tool for administrators, facilitating the quick implementation of best practices for PAM360. Going beyond application and server postures, the dashboard includes user status reports and security hardening scores, providing a holistic approach to security management. This all-in-one toolkit is a valuable resource for administrators looking to maximize the security potential of PAM360 efficiently.

Salient Highlights of Security Hardening Dashboard:

- Introduces a dynamic security score that serves as a real-time indicator of your PAM360 environment's security health.
- Spotlights PAM360's best practices, thus allowing for proactive security management.
- Gain deep insights into the security postures of both the PAM360 application and server through a centralized and user-friendly interface.
- Offers assessment procedures that streamline the identification and resolution for security improvements.



1. User Status Reports

The comprehensive overview of user status reports within the security hardening dashboard offers valuable insights into user activities and authentication methods, aiding in a more secure and well-managed PAM360 environment.
You will discover user statuses via four following diverse sections:

1.a. Inactive Users

The **Inactive Users** section shows the total number of users who have not logged into PAM360 in the selected number of days from the current date. Click on the Inactive Users section to get the list of inactive users with the relevant details, including the user role and the last login time.

1.b. Non-MFA Users

The Non-MFA Users section shows the number of PAM360 user accounts without Multi-Factor Authentication (MFA). Click on the **Non-MFA Users** section to get the list of user accounts with MFA in detail. In the dialog box that opens, you will get a list of user accounts from where you can also enable the MFA for the PAM360 user login.

1.c. Non-synchronized Users

The Non-synchronized Users section shows the total number of user accounts that are not synchronized between Active Directory/Microsoft Entra ID/LDAP and PAM360 in the selected number of days from the current date. Click on the **Non-synchronized Users** section to get the list of non-synchronized user accounts with the relevant details, including the sync detail with the last synced time.

1.d. Users with Local Authentication

This section shows the total number of users with local authentication without Active Directory/Microsoft Entra ID/LDAP authentication.

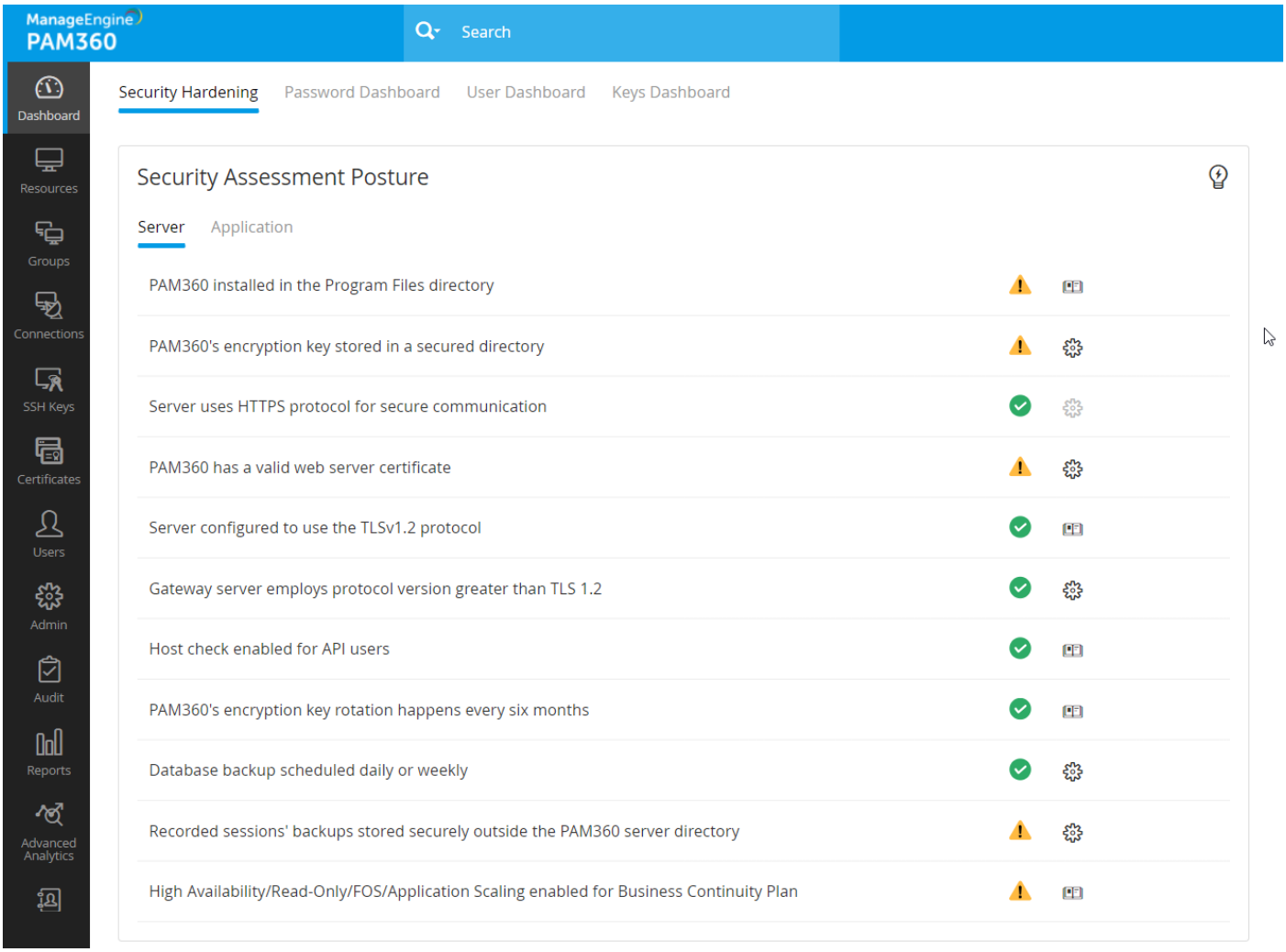
> **Note:** User accounts with Super Administrator privilege are excluded from this list.

2. Security Assessment Posture

The security assessment posture is a comprehensive list of both PAM360 server and application postures responsible for the PAM360 security hardening. It encompasses a range of lists that include server-side protocols, SSL, licenses, user accounts, and application-specific elements to ensure the robust hardening of the PAM360 environment. The security assessment postures are broadly classified into two categories: Server and Application.

Info: A green check mark beside the respective posture indicates that the posture meets the recommended configuration/setting that is required for the hardening of PAM360. On the other hand, the alert icon indicates that an action is required to meet the recommended status.

2.a. Server



i. **PAM360 installed in the Program Files directory** - The posture ensures that the PAM360 application is installed in the Program Files directory of the server.

ii. **PAM360's encryption key stored in a secured directory** - Verifies that the encryption key of PAM360 is stored outside the PAM360 installation directory.

iii. **Server uses HTTPS protocol for secure communication** - Ensures that the server employs the HTTPS protocol for a secure data transfer.

> **Note:** Only super administrators can modify the recommended setting in this posture.

iv. **PAM360 has a valid web server certificate** - Verifies the authenticity of the PAM360 server through a valid web server certificate, establishing trustworthy connections.

v. **Server configured to use the TLSv1.2 protocol** - Ensures that the server is configured to use the TLSv1.2 protocol, enhancing the security of data transmissions.

vi. **Gateway server employs protocol version greater than TLS 1.2** - Verifies that the gateway server utilizes an SSL protocol version higher than TLS 1.2 for secure communication.

vii. **Host check enabled for API users** - Check whether the host check is enabled for API users for an added layer of verification during the server interactions.

viii. **PAM360's encryption key rotation happens every six months** - Ensures that the PAM360's encryption key rotation happens every six months to enhance the overall security.

ix. **Database backup scheduled daily or weekly** - Verifies that the database backup schedule is enabled daily or weekly to minimize data loss in unforeseen circumstances.

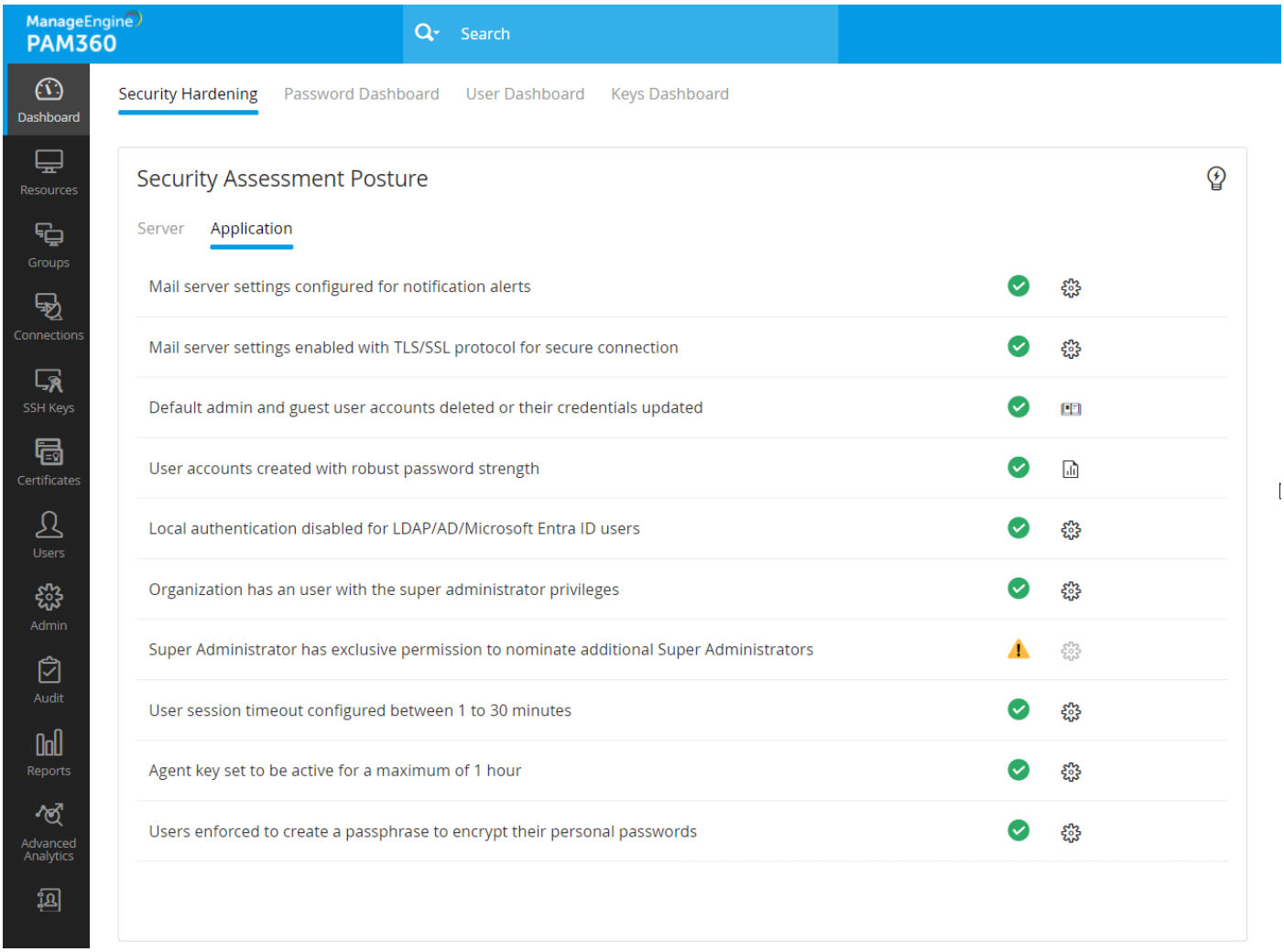
x. **Recorded sessions' backups stored securely outside the PAM360 server directory** - Verifies that the recorded session backups are stored securely outside the PAM360 server directory.

xi. **High Availability/Read-Only/FOS/Application Scaling enabled for Business Continuity Plan** - Ensures that the High Availability/Read-Only/Failover Service/Application Scaling recovery is activated for uninterrupted business continuity.

xii. **PAM360 has a valid license** - Ensures that the PAM360 license is valid and not expired.

xiii. **Notification enabled for license expiry** - Verifies that the notification is enabled for the PAM360 license expiry.

2.b. Application



i. **Mail server settings configured for notification alerts** - Verifies that the mail server setting is configured to send email alerts to the users within the application.

ii. **Mail server settings enabled with TLS/SSL protocol for secure connection** - This posture ensures that the TLS/SSL protocol is enabled in the mail server settings for a secured connection.

iii. **Default 'admin' and 'guest' user accounts deleted or their credentials updated** - Verifies that the default admin and guest user accounts are deleted or their corresponding credentials are updated.

iv. **User accounts created with robust password strength** - Ensures that all the user accounts in PAM360 have robust password strength.

v. **Local authentication disabled for Active Directory/Microsoft Entra ID/LDAP users** - Ensures that the local authentication is disabled for the Active Directory/Microsoft Entra ID/LDAP user accounts.

vi. **Organization has an user with the super administrator privileges** - Ensures that the PAM360 has at least one user with super administrator privileges.

vii. **Super Administrator has exclusive permission to nominate additional Super Administrators** - Verifies that the super administrator has the only access to create further super administrators.

> **Note:** Only super administrators can modify the recommended setting in this posture.

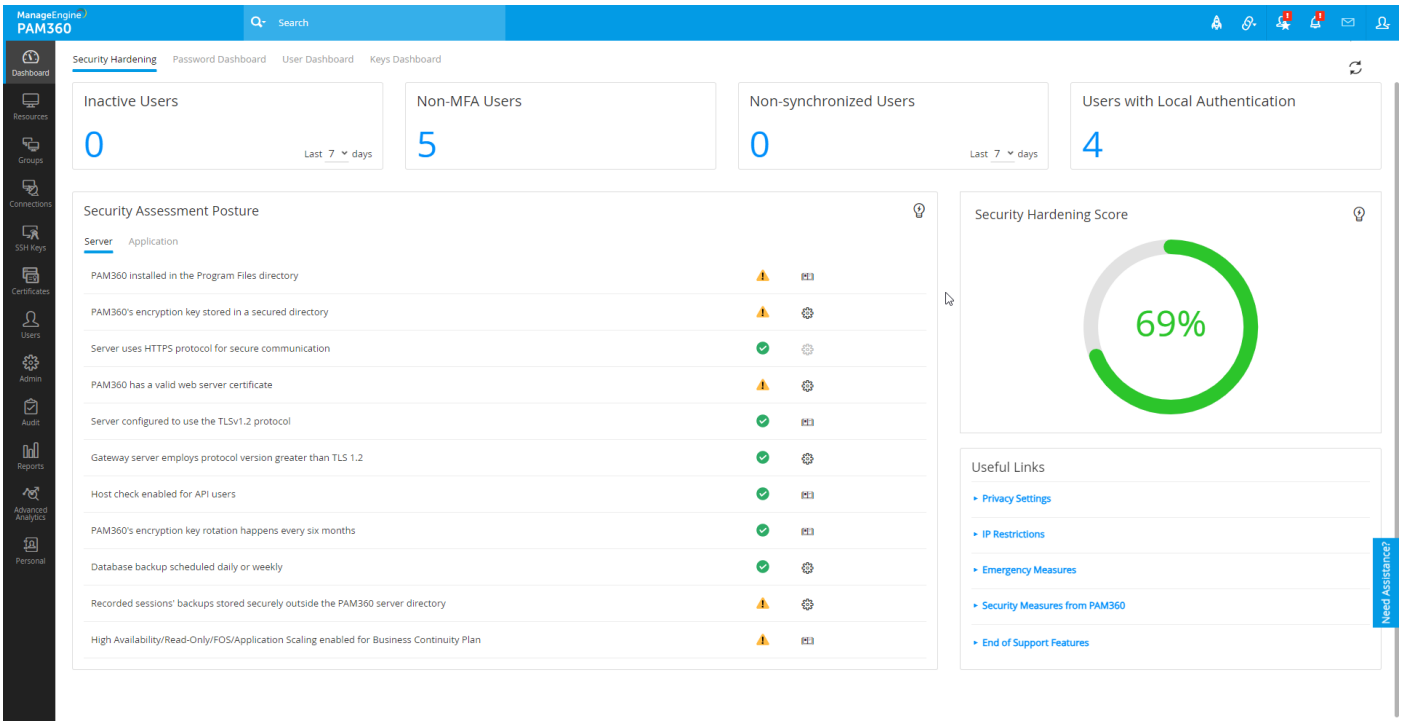
viii. **User session timeout configured between 1 to 30 minutes** - Ensures that the user session auto logout setting is configured between 1 to 30 minutes.

ix. **Agent key set to be active for a maximum of 1 hour** - Verifies that the Windows Domain/Windows/Linux agent installation key is set to be active for a maximum of one hour.

x. **Users enforced to create a passphrase to encrypt their personal passwords** - Ensures that the users are forced to create their own passphrase for encrypting their personal passwords.

3. Security Hardening Score

The security hardening dashboard provides a comprehensive assessment of PAM360's overall security readiness, presenting a score percentage based on predefined posture requirements and user statuses. This concise metric serves as a measure of PAM360 environment's security level, reflecting the configurations implemented.



A perfect 100% hardening score is achieved when all Security Assessment Posture parameters are marked with a green check mark, and there are no inactive, non-MFA, non-synchronized, or local authentication users. A lower score indicates areas that require attention and action to bolster PAM360 environment's security.

It is important to note that the score is dynamic and adjusts based on the selected time frame for user status evaluation. For instance, if there are no inactive users in the last 15 days, the score improves. However, a broader timeframe, such as the past 90 days, may reveal inactive users that impact the score. In such cases, proactive measures, such as locking or deleting users from PAM360, are recommended to enhance the security hardening score.

Refer to the following section for insights to increase the security hardening score of your PAM360 environment.

4. Increasing the Security Hardening Score

You can increase your security hardening score by performing the required actions from the Security Assessment Posture section. The following icons will help you in accomplishing the recommended actions for a better security score.

i. **Alert icon** - The alert icon on the Server and Application postures indicates that the posture does not meet the recommended PAM360 practices. Click the gear or help manual icon beside the alert icon and perform the required actions to increase the security score and harden your PAM360 environment.
ii. **Gear icon** - Clicking the gear icon redirects you to the settings page inside the PAM360 console. For a few cases, you can directly configure the setting from the Security Assessment Posture using the dialog box that opens.
iii. **Help Manual icon** - Clicking the help card icon beside the respective posture gives you the information on configuring the necessary action as required. Read the instructions and apply the steps to complete the recommended configuration to increase your security hardening score.

Report icon - Access comprehensive reports linked to each posture within the Security Assessment section by clicking the report icon. Based on the report, perform the necessary actions to make the posture ticked with a green check mark.

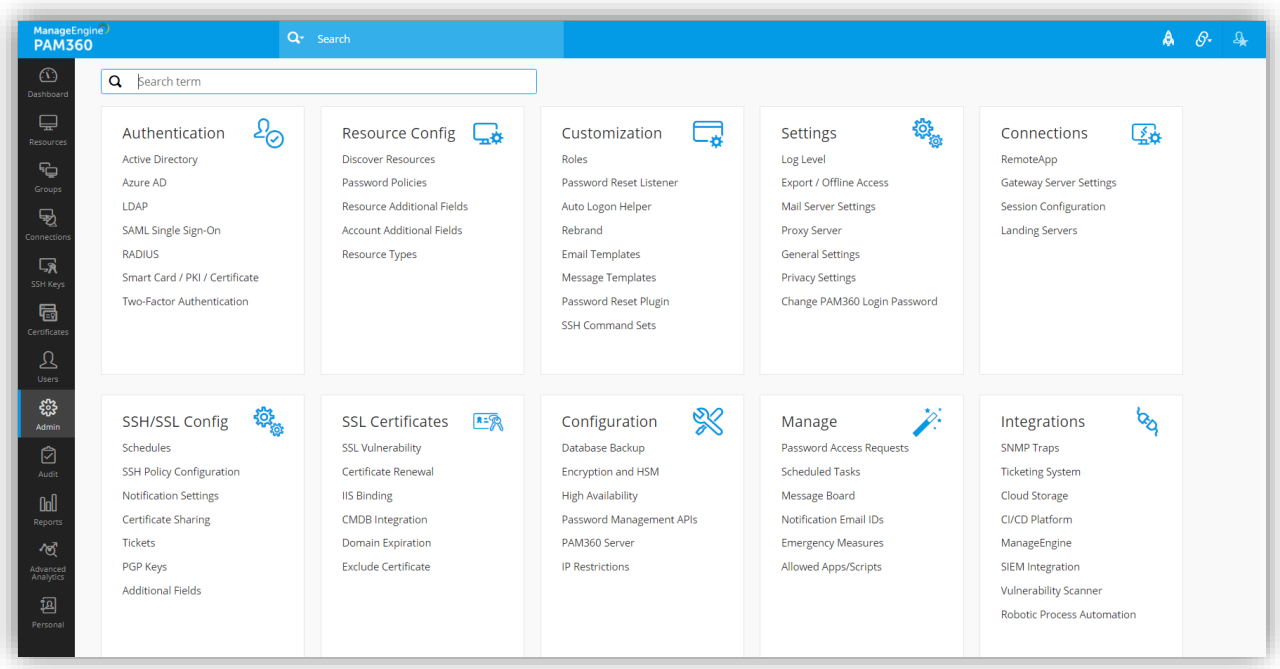
Rebranding PAM360

If you want to replace PAM360 logo appearing on the login screen and on the web interface with that of yours, you can do so from the web interface itself. It is preferable to have your logo of the size 210*50 pixels. PAM360 provides an option to add policies and/or conditions in its login page. If you want your users to accept the legal and/or privacy policies before logging into PAM360, you may configure and enable this option. At any point, this configuration can be disabled.

Steps Required

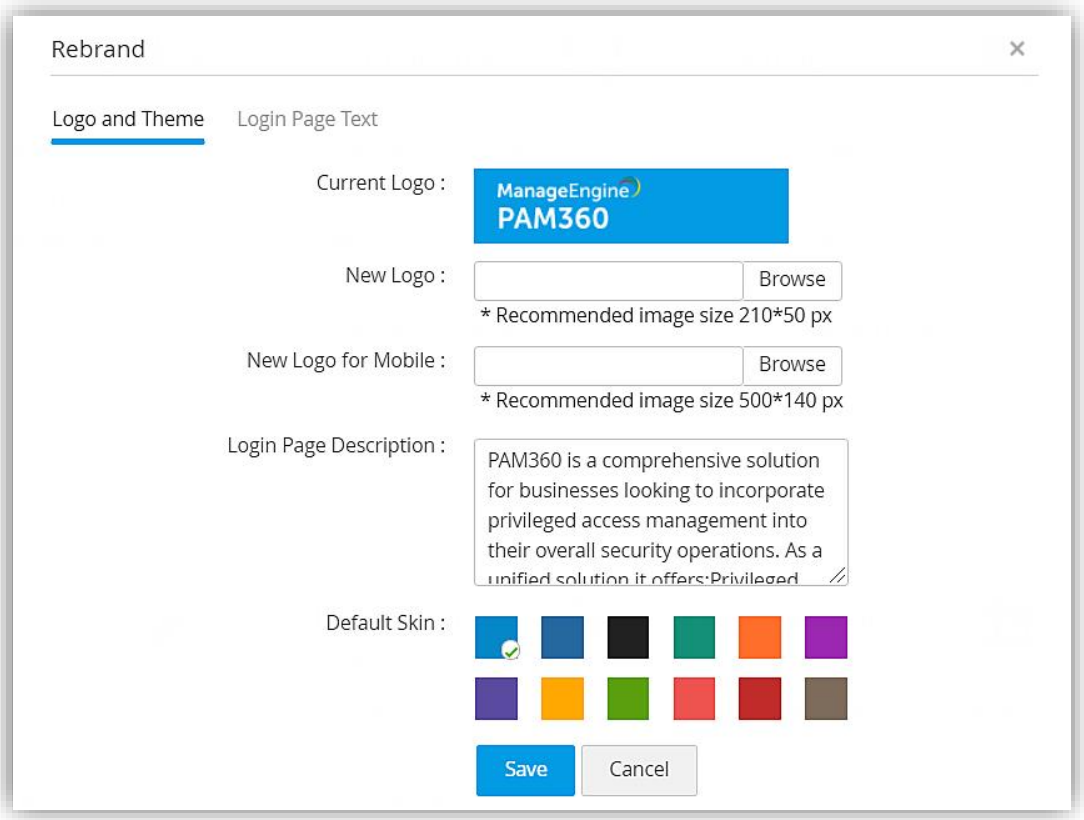
To customize PAM360,

1. Navigate to **Admin >> Customization >> Rebrand.**



2. A pop-up window appears with two possible customizations:
   a. Logo and Theme
      i. Click **Browse** from the **New Logo** field to choose a new logo. The recommended size is **210*50 px.**
      ii. You can also select a logo for mobile devices by selecting **Browse** from the **New Logo for Mobile** field. The recommended size is **500*10 px.**
      iii. Enter a new description that will be displayed in the login page through **Login Page Description** field.
      iv. Pick a new skin color from the **Default Skin** tab.

v. Click **Save** to apply the changes.



b. <u>Login Page Text</u>

i. Click **Login Page Text** to edit and display the legal and privacy policy banner.

ii. Select **Display Legal Banner** to edit and display the legal banner.

iii. Enter the label that you want to display for the content in the **Display Label for Legal Banner** field.

iv. Enter the detailed legal content to be displayed in the **Legal Content field.**

v. Select **Display Privacy Policy Banner** to edit and display the privacy policy banner.

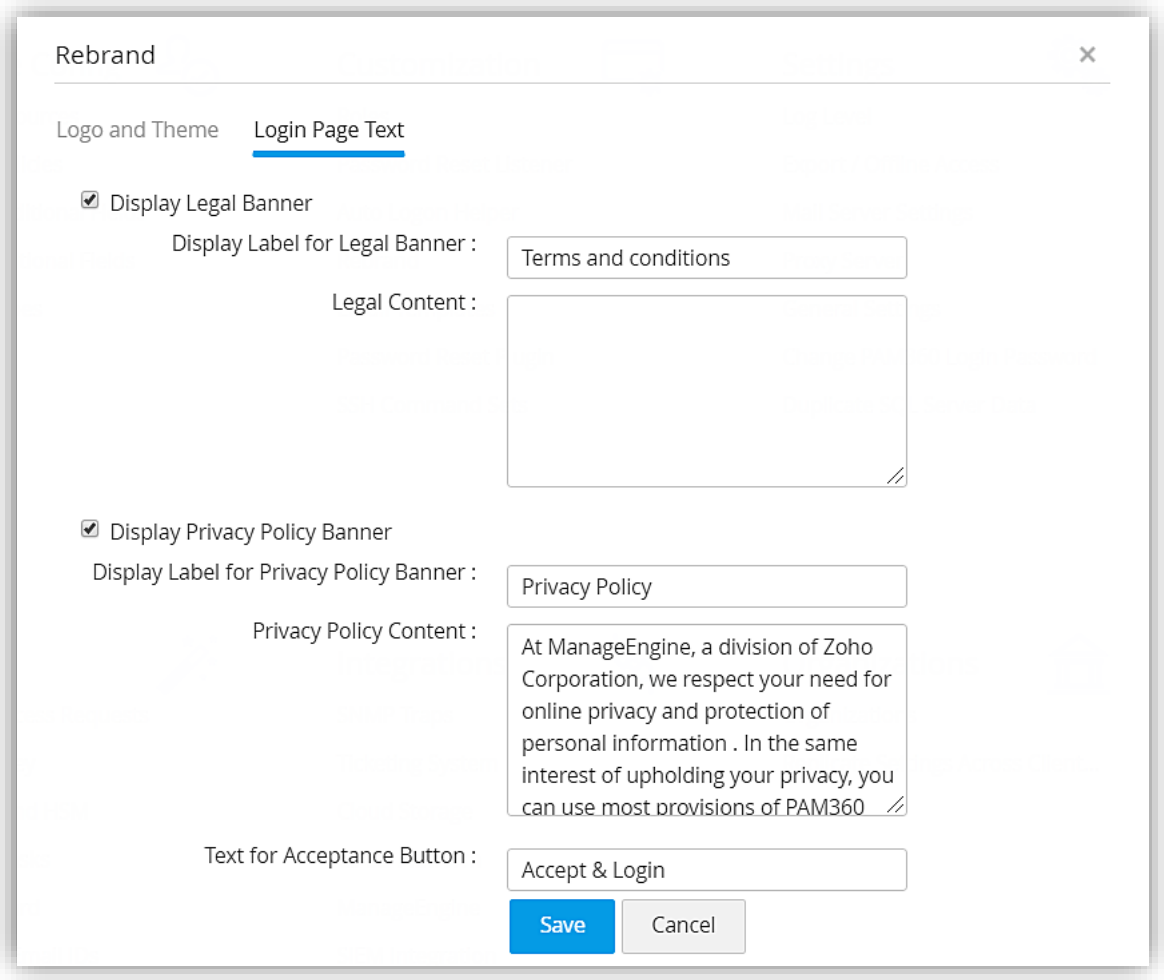
vi. Enter the label that you want to display for the content in the **Display Label for Privacy Policy Banner** field.

vii. Enter the detailed privacy policy content to be displayed in the **Privacy Policy Content** field.

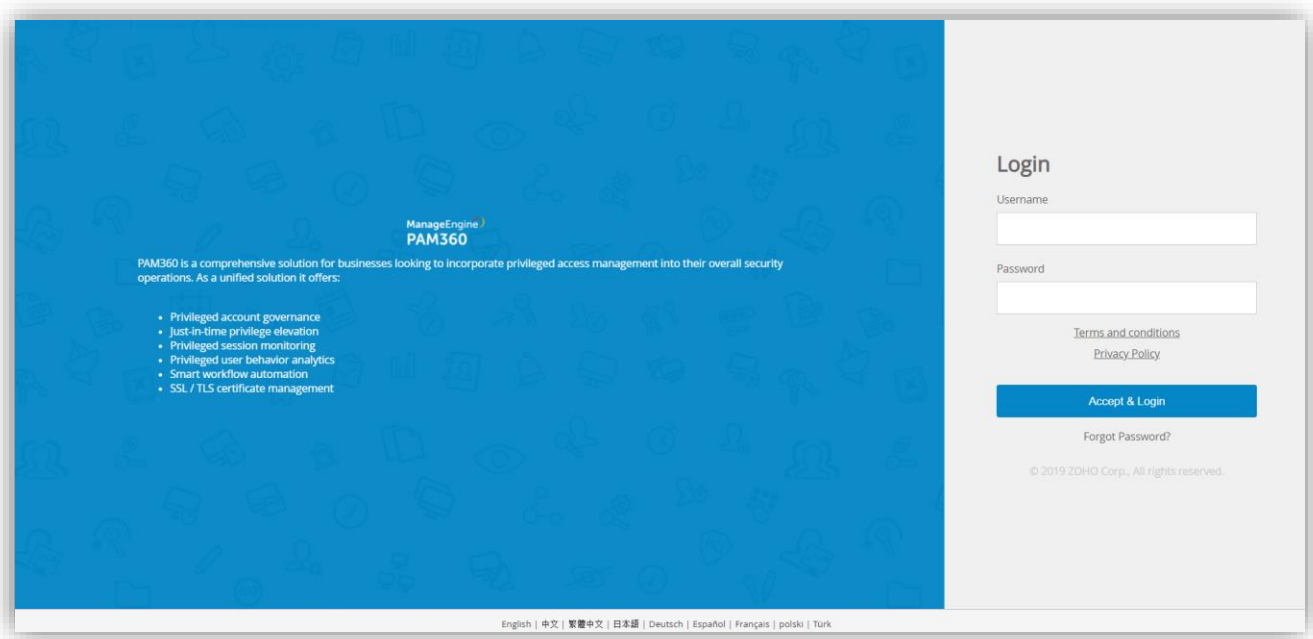
viii. Specify the label for the **Text for Acceptance Button.**

ix. Click **Save** to apply the changes.

Note: The legal and privacy policy banners will be shown in the login page only if their respective content fields are filled. If these fields are empty, the settings cannot be saved.



Now, from the next login onwards, these configurations will be displayed in the login page, as shown below:


ManageEngine
PAM360
PAM360 is a comprehensive solution for businesses looking to incorporate privileged access management into their overall security operations. As a unified solution it offers:
Privileged account governance
Just-in-time privilege elevation
Privileged session monitoring
Privileged user behavior analytics
Smart workflow automation
SSL / TLS certificate management
Login
Username
Password
Terms and conditions
Privacy Policy
Accept & Login
Forgot Password?
© 2019 ZOHO Corp., All rights reserved.
English | 中文 | 繁體中文 | 日本語 | Deutsch | Español | Français | polski | Türk

Displaying Messages to PAM360 Users

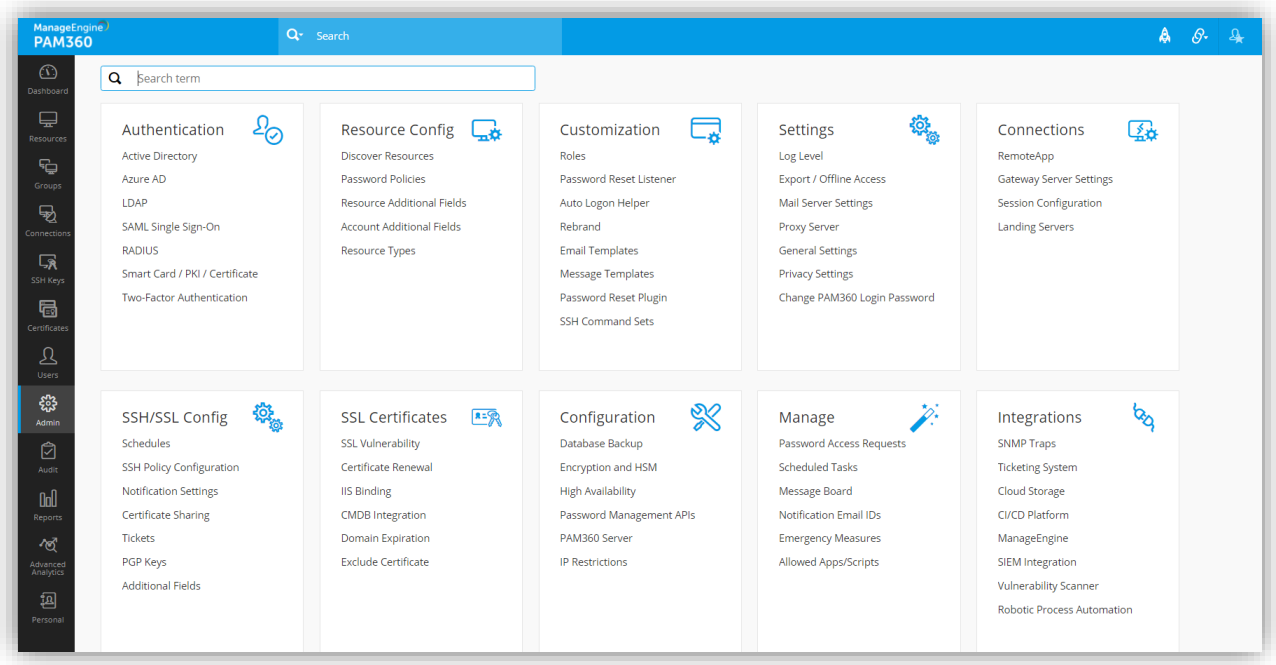
If you want to display a common message to all PAM360 administrators or users, you can do so from PAM360. The 'Message Board' feature helps to achieve this. For example, whenever PAM360 server is down for a few hours due to maintenance you can intimate this information to all the administrators/users using this feature. The common message entered by you will be displayed to all the users/administrators as you decide.

This feature enables you to display the message as a banner on PAM360 GUI. In addition, you can also choose to send the same message as an email notification.

Steps Required

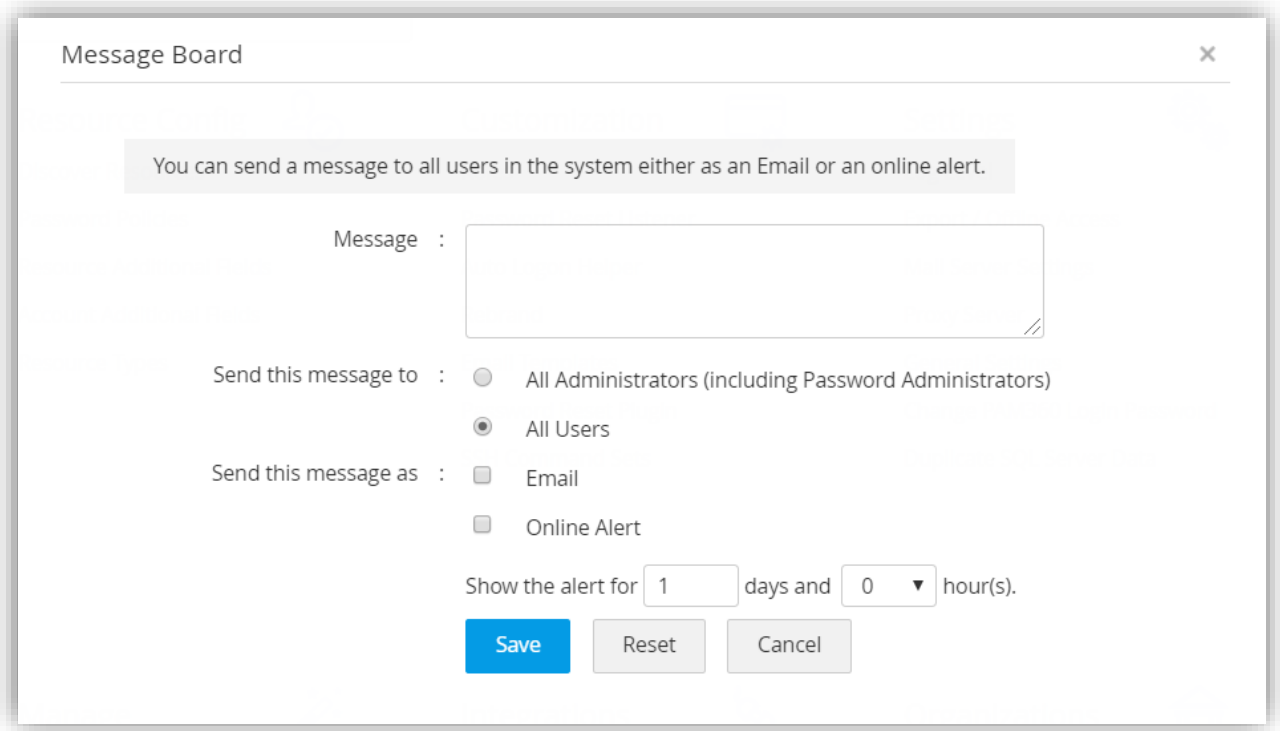
To display the message,

1. Go to the **Admin >> Manage >> Message Board**.



2. In the text field, enter the common **message** which you wish to display.
3. Specify to whom you wish to display the message.
4. Select the type of display - **Online Alert** or **Email** notification or both.
5. If you choose **Online Alert**, the message will be indicated in the PAM360 GUI. When users click that, the message will be displayed as a banner
6. When you choose the option **Email** notification, PAM360 will take the respective email ids from the user database and send out mails

7. You also have the option to specify the time period up to which the message should remain in force. By default, the time period is 1 day.
8. Click **Save.**



Managing General Settings

Using the **General Settings** section of PAM360, you can carry out important setting changes such as enforcing **Password Policies**, enabling the **Forgot Password** option to reset user passwords, configuring to send **Email Notifications** on user creation or role modification, provision for managing **Personal Passwords**, exporting resources, remote password reset and so on.

Configuring General Settings

To configure the general settings in PAM360, navigate to:

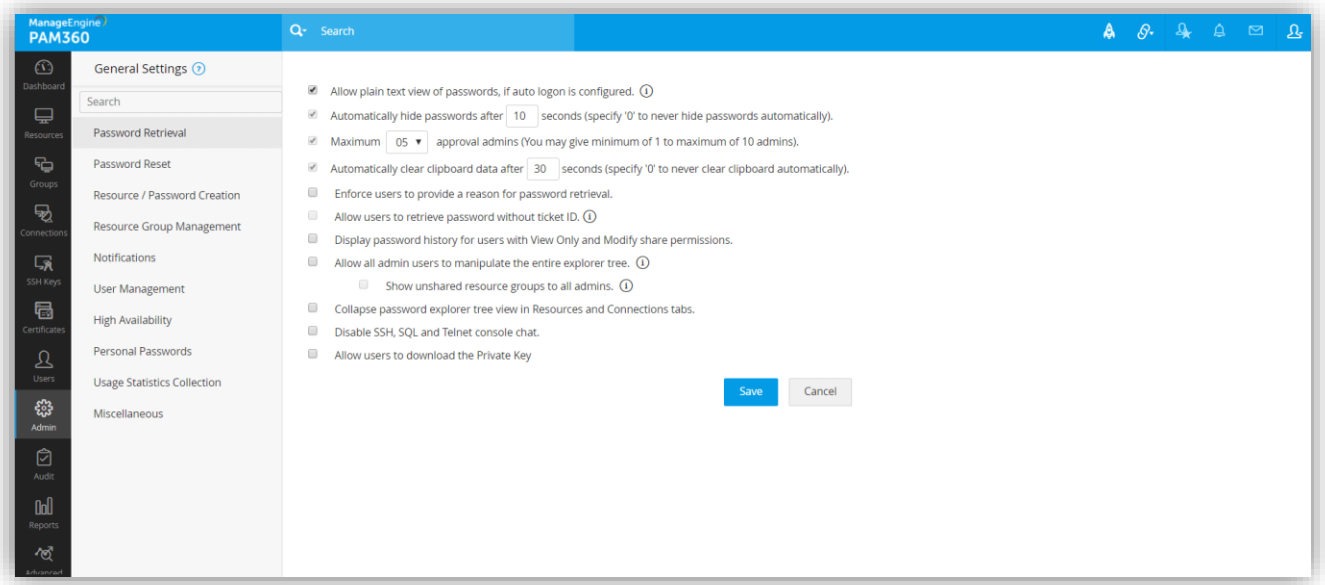
Admin >> Settings >> General Settings.

You will see different settings categorized under the following sections.

1. **Password Retrieval**
2. **Password Reset**
3. **Resource / Password Creation**
4. **Resource Group Management**
5. **Notifications**
6. **User Management**
7. **High Availability**
8. **Personal Passwords**
9. **Usage Statistics Collection**
10. **Miscellaneous**

1. Password Retrieval

To view and manage all global settings related to password retrieval, click **Password Retrieval** from the left pane.



1.1 Allow plain text view of passwords, if auto logon is configured

Enable this option to allow the users to view the passwords of shared resources in plain text when auto logon is configured. If this option is disabled, users cannot retrieve the password, however they can still launch remote sessions through auto logon. This restriction applies only to Password Users, Password Auditors and custom user type roles with the same privileges as Password Users and Auditors.

1.2 Automatically hide passwords after 5 seconds (specify '0' to never hide passwords automatically)

By default, passwords are hidden behind a string of hash symbols. On clicking the string, the passwords appear in plain text. By default, the passwords are shown for 10 seconds only, after which they will be automatically hidden. Specify the desired value in seconds in the **Automatically hide passwords after X seconds** option. If you specify 0, passwords will continue to remain in plain text until you click the password to hide.

1.3 Maximum X approval admins (You may give minimum of 1 to maximum of 10 admins)

Select a maximum number of admins (upto 10 admins) needed to approve a password request for resources which have the password access control workflow set up. The number of admins selected here will reflect in the Password Access Control workflow configuration, under the option "Enforce approval by at least __ administrators".

1.4 Automatically clear clipboard data after 30 seconds (specify '0' to never clear clipboard automatically)

PAM360 uses the clipboard utility of browsers to copy passwords when you copy them from PAM360. By default, the copied passwords will be available for 30 seconds. In this option, specify the time in seconds after which the clipboard will be cleared and the copied password will no longer be available. If you specify 0, clipboard will not be cleared automatically.

1.5 Enforce users to provide reason for password retrieval

Enable this option to enforce users to provide a reason for requesting access to the password. This reason for retrieval will be recorded in the audit logs.

1.6 Allow users to retrieve password without ticket ID

If ticketing system integration is done in your environment, then by default, users will be prompted to provide a ticket ID while requesting for a password. Enable this option to allow users to retrieve passwords without providing a ticket ID.

1.7 Display password history for users with View Only and Modify share permissions

Password History (available under Account Actions) shows the previously used passwords for a particular account as well as the details on who modified it. Enable the option **Display password history for users with View Only and Modify share permissions** to display the password history details for users with View Only and Modify share permissions.

1.8 Allow all admin users to manipulate the entire explorer tree

Once this option is enabled, PAM360 creates an organization-wide, global explorer tree structure containing the names of resource groups under a root node and the following things will apply:

- Any administrator in PAM360 can create/edit the explorer tree structure of resource groups.
- Admins and Password Admins can add their resource groups into the global tree and the whole structure will be available for view to all the end users.
- Types of users who will be able to access this tree structure: Administrators, Privileged Administrators, Password Administrators and Password Users.
- If this option is disabled, users can modify only their portion of the tree with the resources that are shared to them.

  Show unshared resource groups to all admins: If this option is enabled, resource groups of all the admins will be available visible to other admins but they will be disabled as the resource groups are not shared. If this option is disabled, then only the shared resource groups will be available for the admins.

1.9 Collapse password explorer tree view in Resources and Connections tab

By default, the nodes of the password explorer tree are shown in expanded form. Enable this option to collapse the explorer tree view.

1.10 Disable SSH, SQL and Telnet console chat

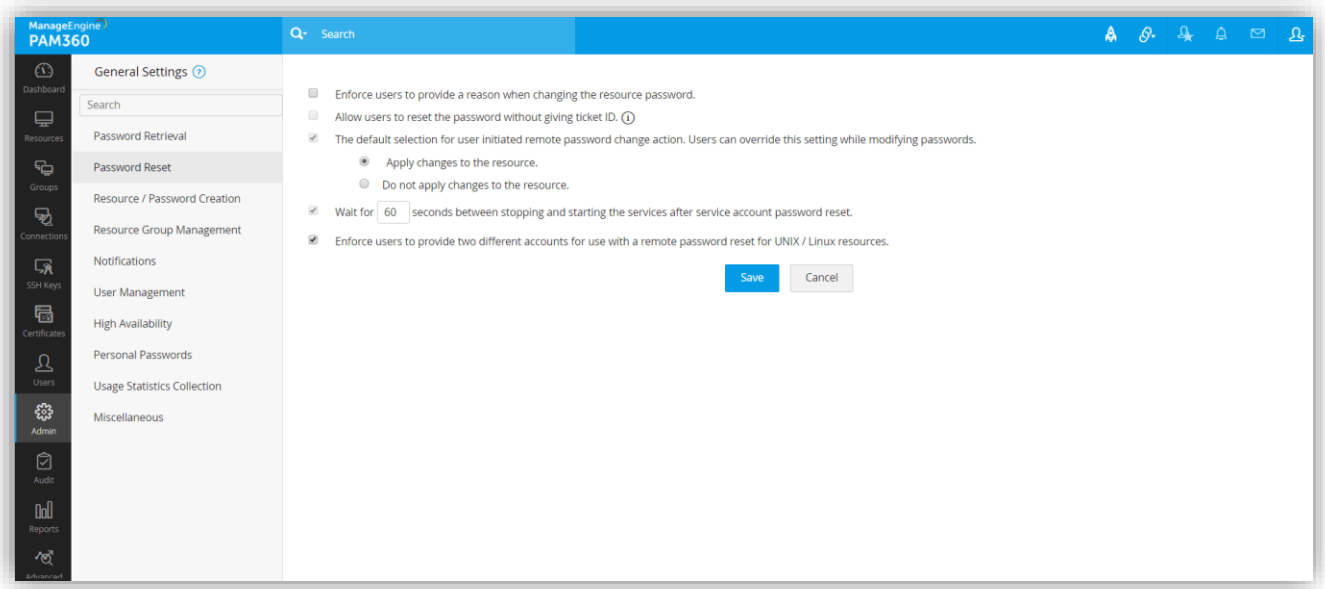
By default, SSH, SQL and Telnet console chat will be enabled. Select this option to disable the console chat for remote sessions.

1.11 Allow users to download the private key

If this option is enabled, the user will be able to download the private key that is added to an account shared with them.

2. Password Reset

To view and manage all global settings related to password reset in PAM360, click **Password Reset** from the left pane.



2.1 Enforce users to provide a reason when changing the resource password

Enable this option to prompt users to enter a reason while attempting to change the password of a resource. This reason will be recorded in the audit logs.

2.2 Allow users to reset password without giving a ticket ID

If ticketing system integration is done in your environment, then by default, users will be prompted to provide a ticket ID when they try to reset the password of a resource. Enable this option to allow users to reset passwords without providing a ticket ID.

2.3 Default selection for user-initiated remote password change action. Users can override this setting while modifying passwords

When changing the password of a resource in the PAM360 console, by default the password changes are applied in the remote resource instantaneously. (Resource types supported for remote synchronization are: Windows, Windows Domain, and Linux). Select the option **Do not apply changes to the resource** to not change the password in the remote resource automatically.

2.4 Wait for X seconds between stopping and starting the services after service account password reset

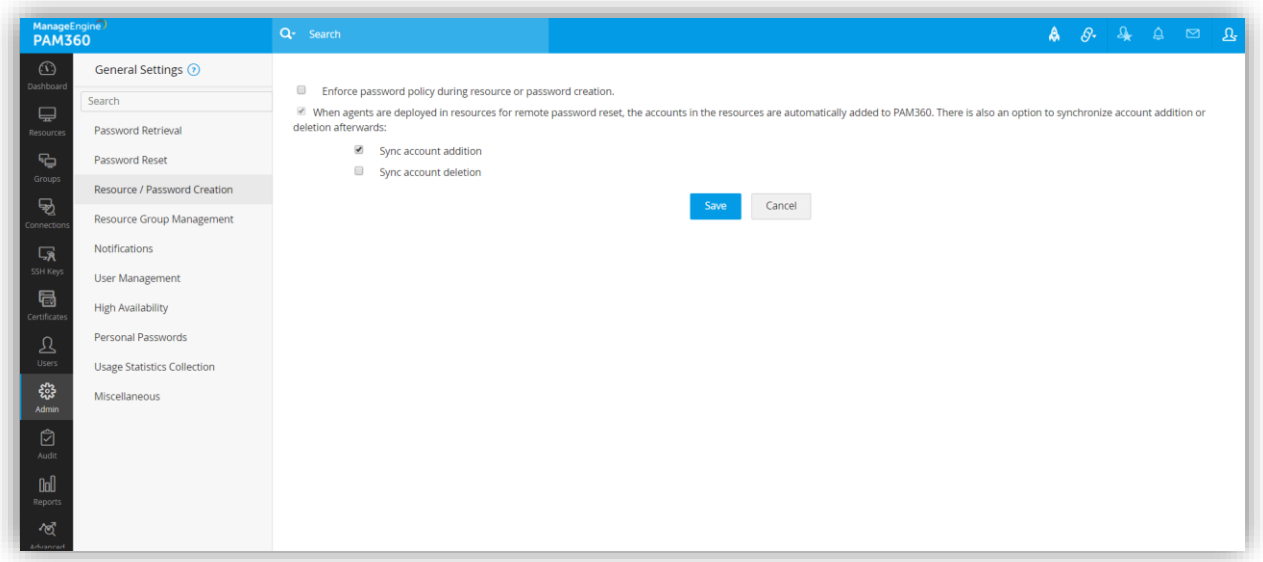
You can configure PAM360 to wait for a specified time (in seconds) before stopping and restarting the services after automatically resetting the service account password. This is useful in cases where service account password reset is enabled for a Windows Domain account and the corresponding domain password is changed.

2.5 Enforce users to provide two different accounts for use with remote password reset for UNIX / Linux resources

Enable this option to enforce users to provide provide two different accounts for password reset for Unix/Linux resources. If this option is disabled, then users will be allowed to enable remote synchronization with just one account. To know more about remote password reset, click here.

3. Resource/Password Creation

To view and manage all global settings related to resource/password creation in PAM360, click **Resource / Password creation** from the left pane.



3.1 Enforce password policy during resource or password creation

By default, password policies are enforced for passwords in PAM360 only at the time of password change.

Enable this option to check policy compliance at the time of resource/account addition itself. Once you enable this, you will be permitted to add your resource / account only if the password is in accordance with the password policy defined in PAM360.

When agents are deployed in resources for remote password reset, the accounts in the resource are automatically added to PAM360. There is also option to synchronize account addition or deletion afterwards.

- **Sync account addition:**

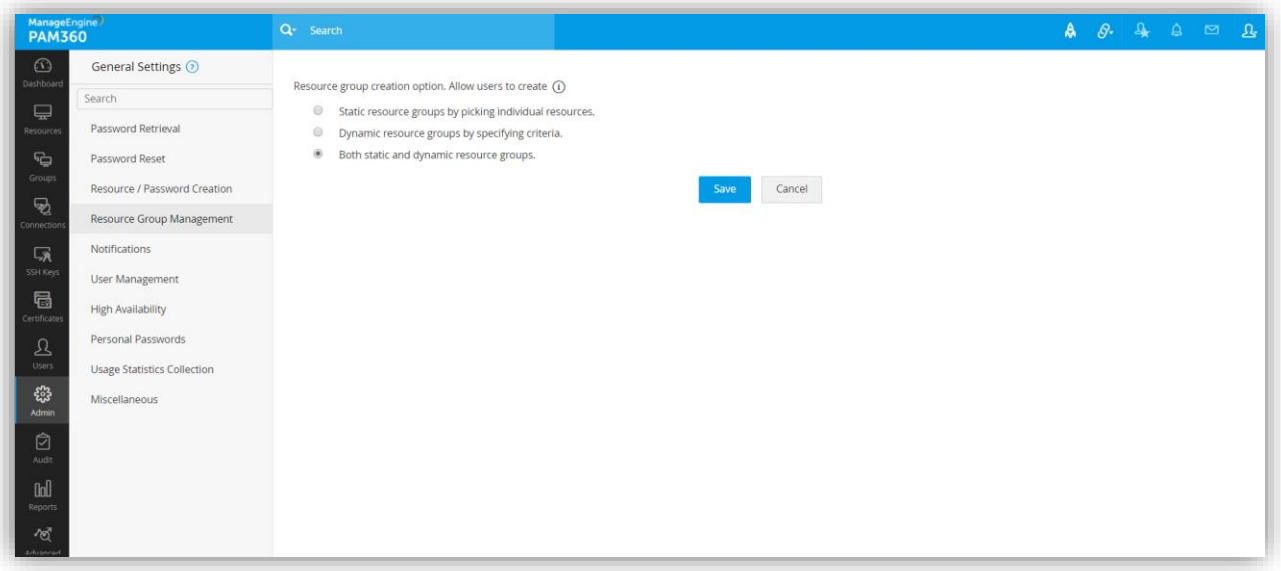
  Enable this option to add new accounts into PAM360 whenever they are added in the remote resource.

- **Sync account deletion:**

  Enable this option to delete an account in PAM360 whenever the account is deleted in the remote resource.

4. Resource Group Management

To view and manage all global settings related to resource group management in PAM360, click **Resource Group Management** from the left pane.



4.1 Resource group creation options

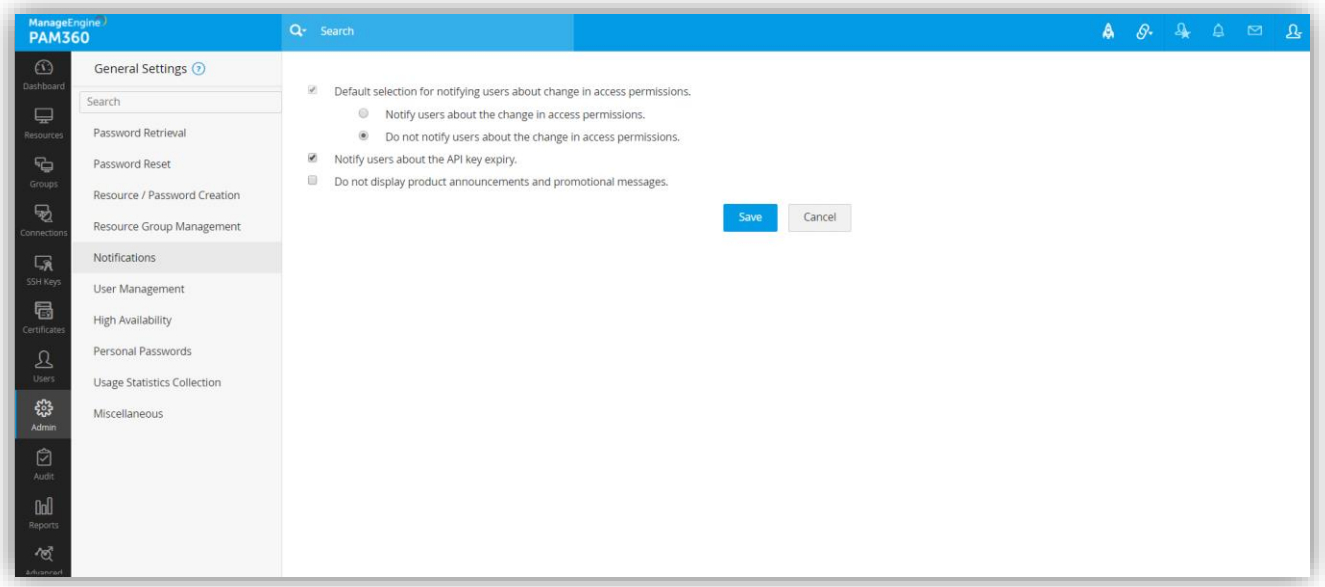
You can allow users to create:

- Static resource groups by picking individual resources.
- Dynamic resource groups by specifying criteria.
- Both static and dynamic resource groups.

Select the required option and click **Save**.

5. Notifications

To view and manage all global settings related to notifications in PAM360, click **Notifications** from the left pane.



5.1 Default selection for notifying users about change in access permissions

i. **Notify users about the change in access permissions**: Select this option to notify the respective users whenever their access permission is changed.

ii. **Do not notify users about the change in access permissions:** Select this option if you do not wish to notify users regarding the change in their access permissions.

> **Note:** Admins can override this setting while modifying the access permission.

5.2 Notify users about the API key expiry

When an API user is created, an auth token (API key) will be generated. You can specify a date on which the API key will expire. Enable this option to notify the users about the expiry of the API key. Three notifications will be sent as follows:

1. A notification 7 days before expiry.
2. A notification on the day of expiry.
3. A notification every day after the day of expiry.

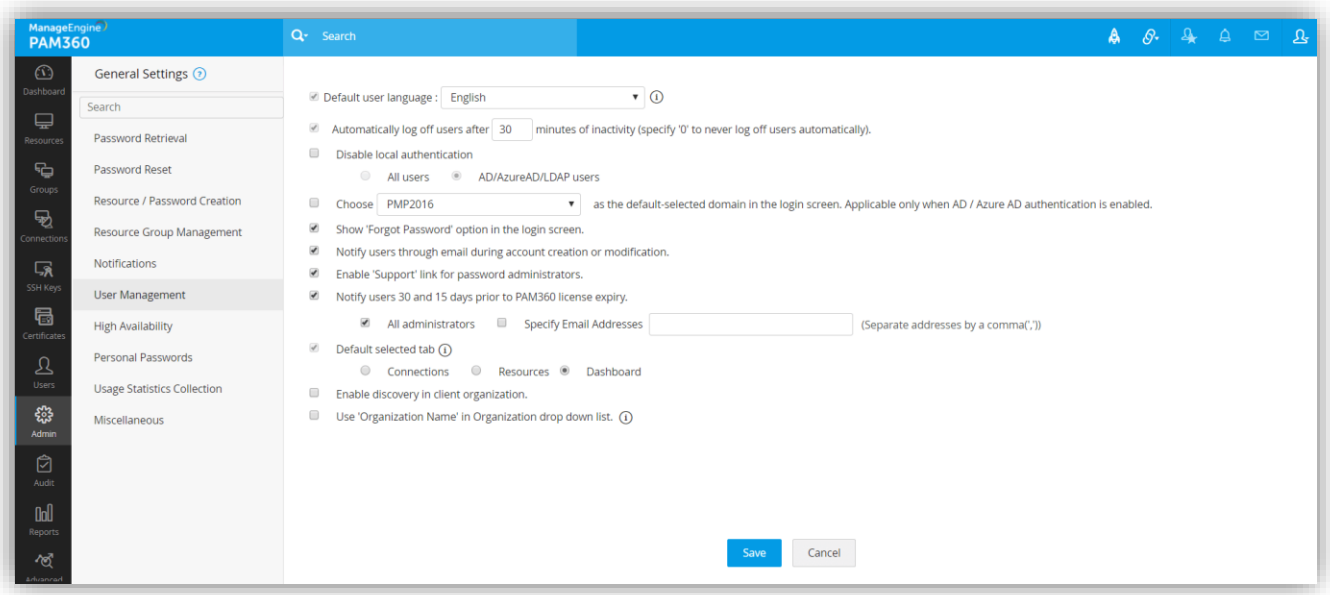
Click here for more about adding API users in PAM360.

5.3 Do not display product announcements and promotional messages

Enable this option if you do not wish users to see any promotional in-product banners or messages in PAM360.

6. User Management

To view and manage all global settings related to user management in PAM360, click **User Management** from the left pane.



6.1 Default user language

You can choose a default user language for the web interface from the given drop down.

6.2 Automatically log off users after X minutes of inactivity (specify '0' to never log off users automatically).

Specify a specific time in minutes after which an inactive user session will timeout and log off automatically; by default, the time will be set as 30 minutes. You can specify '0' minutes to never log off inactive users automatically. To impose the same restriction on users logged in through the browser extensions, select the option: **Enforce this as a maximum time limit also for users logged in through browser extension.**

6.3 Disable local authentication

PAM360 provides three types of authentication:

- LDAP authentication
- AD authentication/Azure AD authentication
- PAM360's local authentication.

By default, PAM360 allows local authentication along with LDAP or AD authentication. If you want to restrict either the LDAP or AD/Azure AD authentication alone, then select the

respective options: **All users** or **AD/AzureAD/LDAP users.** Once the local authentication is disabled, the PAM360 users will be able to login to PAM360 using their workstation password alone.

6.4 Choose default-selected domain in the login screen. (Applicable only when AD/Azure AD authentication is enabled).

If you have users from various domains, the PAM360 login screen will list down all the domains in the drop-down. You can choose the frequently used domain here for ease of use for the users. Once you do so, that domain will be shown as selected by default in the login screen.

6.5 Show 'Forgot Password' option in the login screen

By default, the 'Forgot Password' option is enabled for all users who use PAM360's local authentication. By clicking on 'Forgot Password', users can get a new login password sent to their email. Disable this option if you do not wish to display the 'Forgot Password' option in the login screen for all users.

6.6 Notify users through email during account creation or modification

By default, users are notified via email whenever their account is added in PAM360 or an existing account is modified. Disable this option if you do not wish to send email notifications to users regarding account creation or modification.

6.7 Enable 'Support' link for password administrators

By default, Password Administrators in PAM360 cannot view the 'Support' option in their profile. Enable this option to make the 'Support' option accessible for password administrators also.

6.8 Notify users through email 30 and 15 days prior to PAM360 license expiry

You can notify all administrators or any users regarding the expiry of PAM360 license.

Two notifications will be sent:

- 15 days prior to the expiry.
- 30 days prior to the expiry.

To send notifications you can either select all administrators as recipients or specify email addresses separated by a comma (',').

6.9 Default selected tab

Select a default tab which will open for users right after logging in:

- Connections
- Resources
- Dashboard

6.10 Allow password caching for offline access via mobile

Enable this option to allow saving password cache in the PAM360 mobile application so that users can access the passwords offline.

6.11 Enable logins to mobile apps with fingerprint authentication

Enable this option to allow users to login to their PAM360 mobile applications using their device's fingerprint authentication.

6.12 Allow website auto-fill actions using browser extensions

Website forms can be auto-filled using PAM360 browser extensions, allowing users to log on to websites with just a click. Enable this option to allow auto filling of login credentials for saved website accounts through the PAM360 browser extensions.

6.13 Allow website auto-logon actions using browser extensions

PAM360 enables automatic login to websites and allows users to launch connections to applications directly through native browser extensions. Enable this option to allow users to connect to a remote resource through the auto logon feature using the PAM360 browser extensions.

6.14 Disable accounts addition via browser extensions

Disable this option to prevent users from adding accounts to resources through the PAM360 browser extensions. The option to add accounts through browser extension is available only for the Chrome browser. To know more about PAM360 browser extensions, click here.

6.15 Enable discovery in client organization

Enable this option to allow every client organization to discover accounts and resources using the Discovery option in PAM360.

6.16 Use 'Organization Name' in Organization drop down list

Enable this option to display the Organization Name in the Organization drop down list; the Organization display name will be shown on mouseover.

7. High Availability

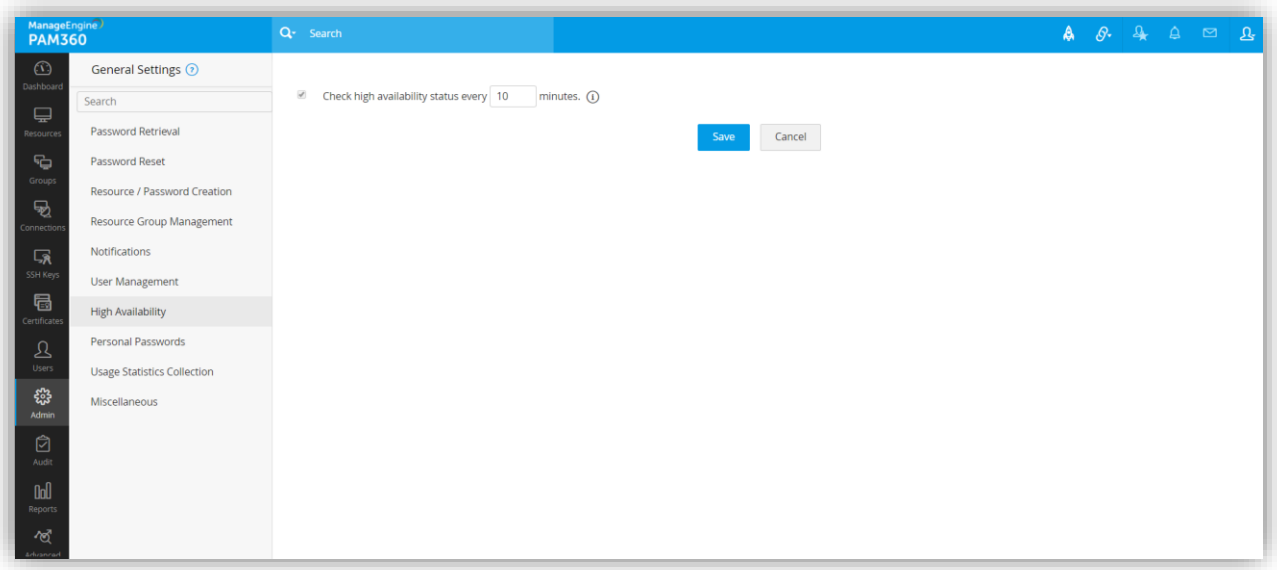
In a High Availability (HA) set up, constant replication of data takes place between Primary and Standby servers. High Availability status 'Alive' indicates perfect data replication and data synchronization between both servers. In case of any disruption like network problems between Primary and Standby (in turn between the databases), the status will change to 'Failed'. This may happen when there is no communication/connection between the database of primary server and that of the standby server.

When the connection gets re-established, data synchronization will happen and both databases will be in sync with each other. During the intervening period, those who have connected to the primary and standby will not face any disruption in service. This status is only an indication of the connection/communication between databases and does not warrant any troubleshooting.

To configure periodic status, check for high availability in PAM360:

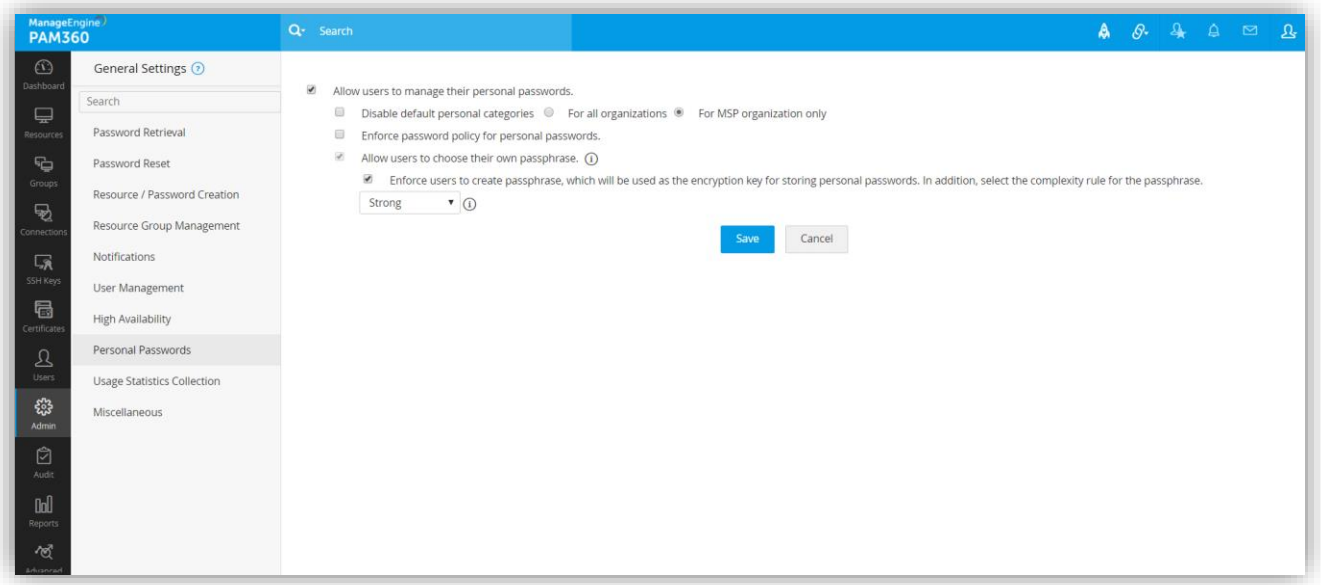
1. Click **High Availability** from the left pane.
2. Specify the number of minutes to check the status in the option **Check High Availability Status Every --- Minutes.**

To know more about High Availability, click here.



8. Personal Passwords

Individual users can manage their personal passwords such as credit card PIN numbers, bank accounts credentials etc in PAM360 through the personal password management feature. This personal password management section will be visible exclusively to the individual users and not even the Super Admin users will have access to it. To access this section, click **Personal Passwords** from the left pane.



8.1 Allow users to manage their personal passwords

Select this option to enable the **Personal** tab in which users can save their personal passwords. To disable the **Personal** tab, uncheck this option.

> **Note:** In MSP editions of PAM360, only the MSP administrator can enable or disable this option.

8.2 Disable default personal categories

In the **Personal** tab, you will find a few default categories for various personal passwords such as bank credentials. You can disable the default categories and allow users to create their own custom categories for saving personal passwords. You can disable categories either **for all organizations** or **for MSP organization only.**

8.3 Enforce password policy for personal passwords

Enabling this option will apply the password policy selected for accounts in PAM360 to the personal passwords of users too. You can disable this option to allow users to set personal passwords without any complexity restrictions.

8.4 Allow users to choose their own passphrase

By default, when you allow users to manage their personal passwords, PAM360 will prompt them to choose a passphrase. Once set, there is no way to change or reset this passphrase.

i. **Enforce users to create passphrase, which will be used as the encryption key for storing personal passwords. In addition, select the complexity rule for the passphrase**

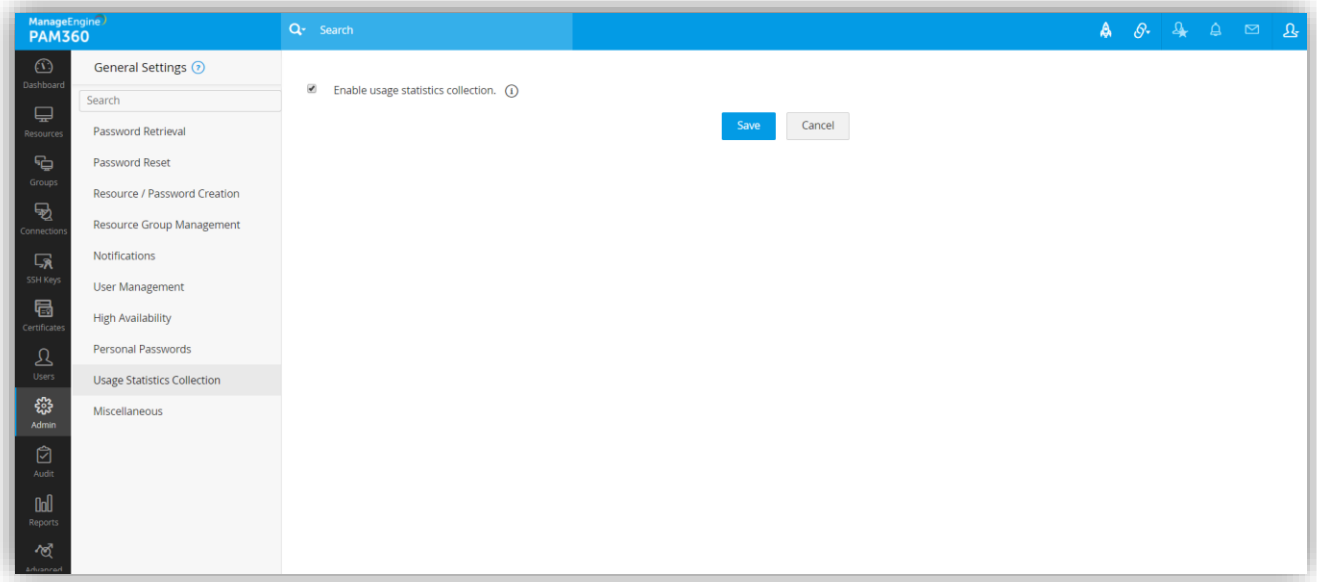
Select this option to enforce a password policy for the passphrase. By default, there are four options: low, medium, strong and an offline password file option. To create a custom password policy for personal passwords, navigate to **Admin >> Customization >> Password Policies**. If the chosen enterprise policy is deleted, the default password policy will be automatically chosen for passphrase complexity.

1. If you do not want to enforce passphrase complexity, select [-None-] in complexity option.
2. If you do not want to enforce users with own encryption passphrase complexity, uncheck this option.

9. Usage Statistics Collection

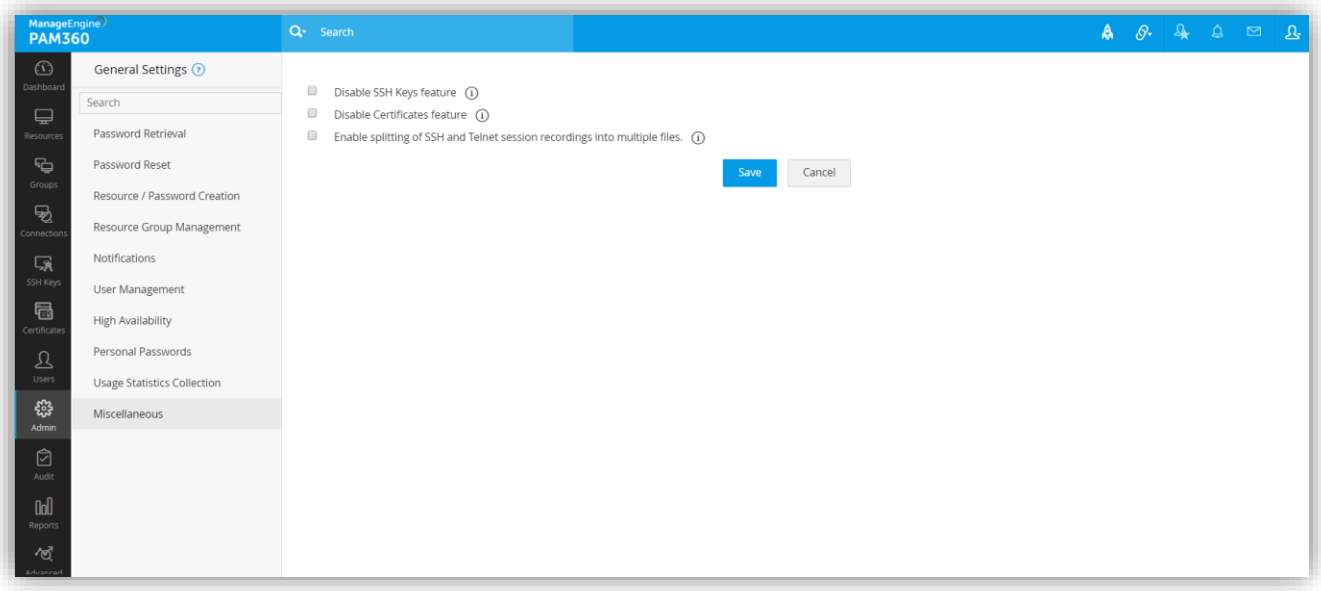
By selecting this option, you can choose to send information to ManageEngine about how the product is used. As per the product End-user License Agreement (EULA), the data collected will pertain to the license details, configuration of the system in which PAM360 is installed, usage statistics on the frequency of use of various features. This is a feedback mechanism to improve the product. You can uncheck the option if you don't wish to allow usage data collection.

Click **Usage Statistics Collection** from the left pane and enable or disable the option **Enable Usage Statistics Collection**.



10. Miscellaneous

Click **Miscellaneous** from the left pane; this section consists of optional customizations you can apply to PAM360 based on your requirement.



10.1 Disable SSH Keys feature

Selecting this option will disable the **SSH Keys** tab from your installation. However, the feature will not be removed completely; you can enable the **SSH Keys** tab again by deselecting this option.

10.2 Disable Certificates feature

Selecting this option will disable the **Certificates** tab from your installation. However, the feature will not be removed completely; you can enable the **Certificates** tab again by deselecting this option.

10.3 Enable Splitting of SSH and Telnet Session Recordings into Multiple Files

If you enable this option, PAM360 will split large session recording files from Legacy SSH and Telnet remote sessions into several small files and save them individually in your local storage. Refer to the help section **Privileged Session Recording** to learn about session splitting in detail.

After making changes in the settings, click **Save** to save the changes.

Mail Server Settings

PAM360 sends email notifications to newly added users to inform them the details about their PAM360 access credentials. Therefore, it is necessary to configure mail server settings prior to adding new users into the product. You can either configure the SMTP mail server used in your environment or use the Microsoft Exchange Online mailbox. PAM360 supports OAuth 2.0 authentication for SMTP-based email communications when using Microsoft Exchange Online. Choosing Microsoft Exchange Online as the mail server will activate OAuth 2.0 authentication for all emails sent from the product. Read further to learn how to configure mail server settings.

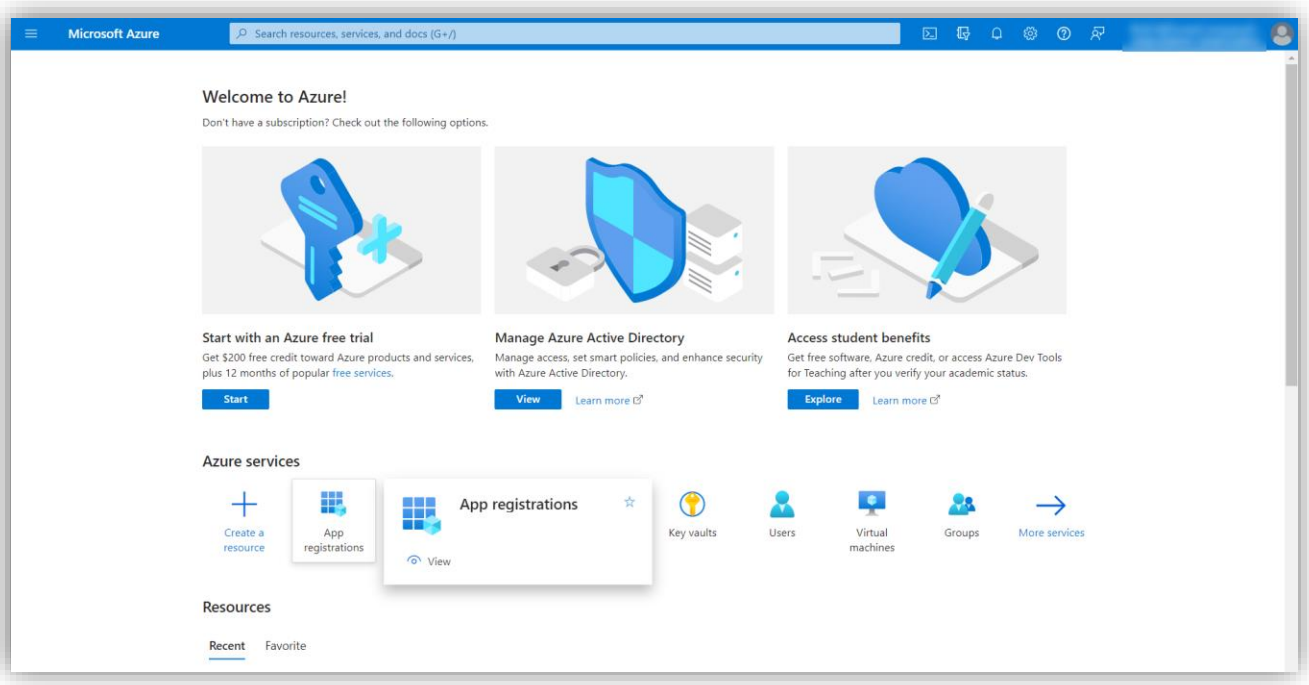
1. **Configure Microsoft Exchange Online as the mail server**
2. **Configure other mail servers**

1. Configure Microsoft Exchange Online as the Mail Server

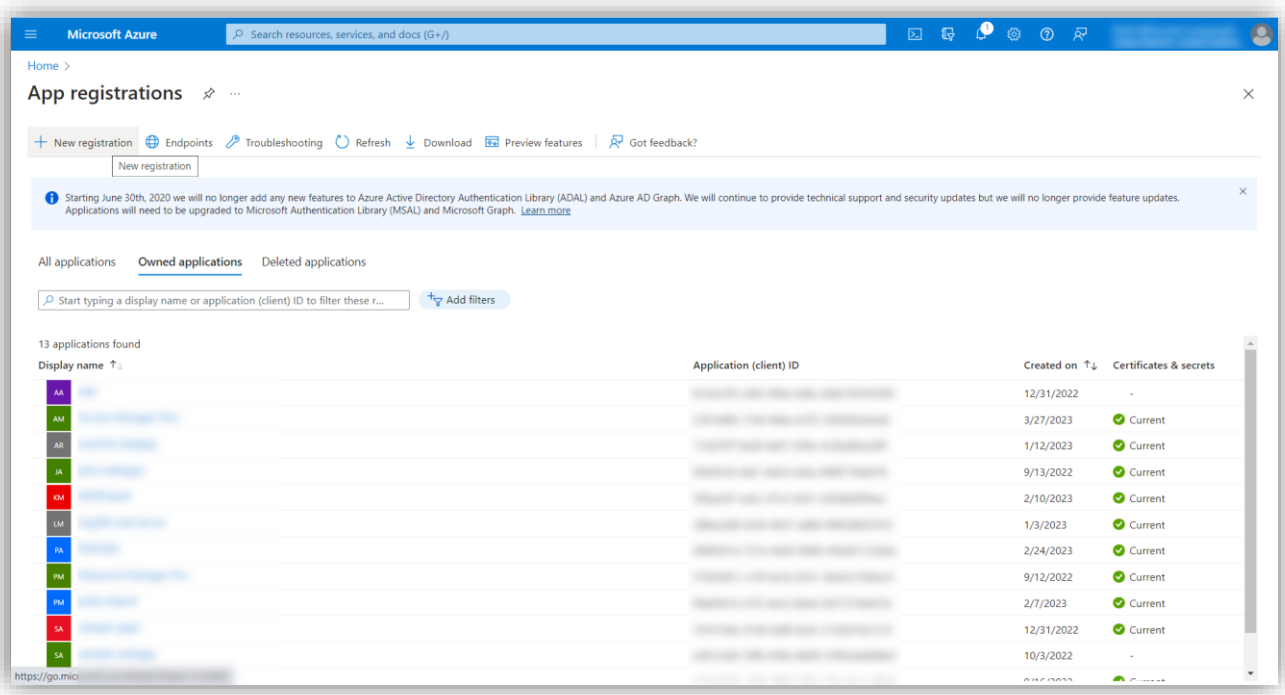
To configure Microsoft Exchange Online as the mail server in PAM360, you must create an application in the Azure portal and generate the Application ID, Client ID, and Client Secret value. Follow the below steps:

1.1 Steps to Configure an Azure Application for Microsoft Exchange Online Server

1. Log in to the Microsoft Azure portal.
2. Click **App registrations** from the Microsoft Azure homepage.



3. Click **+ New registration** from the top pane of the **App registrations** page.

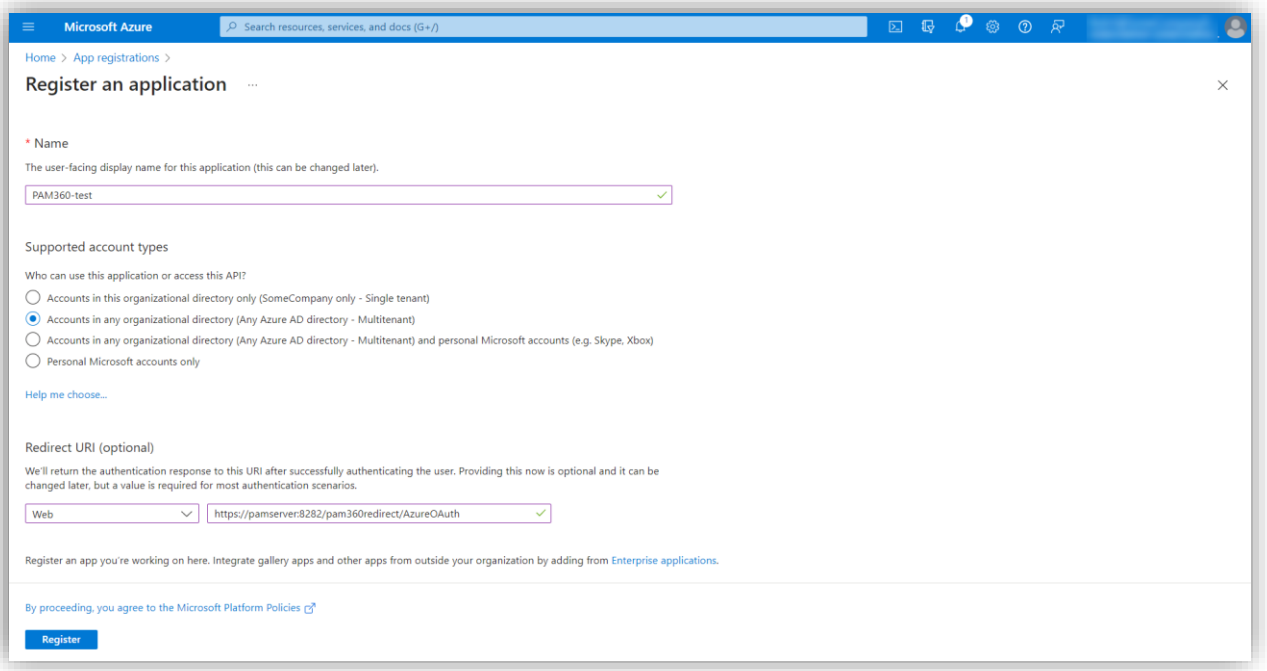


4. In the **Register an application** page, enter the following attributes:

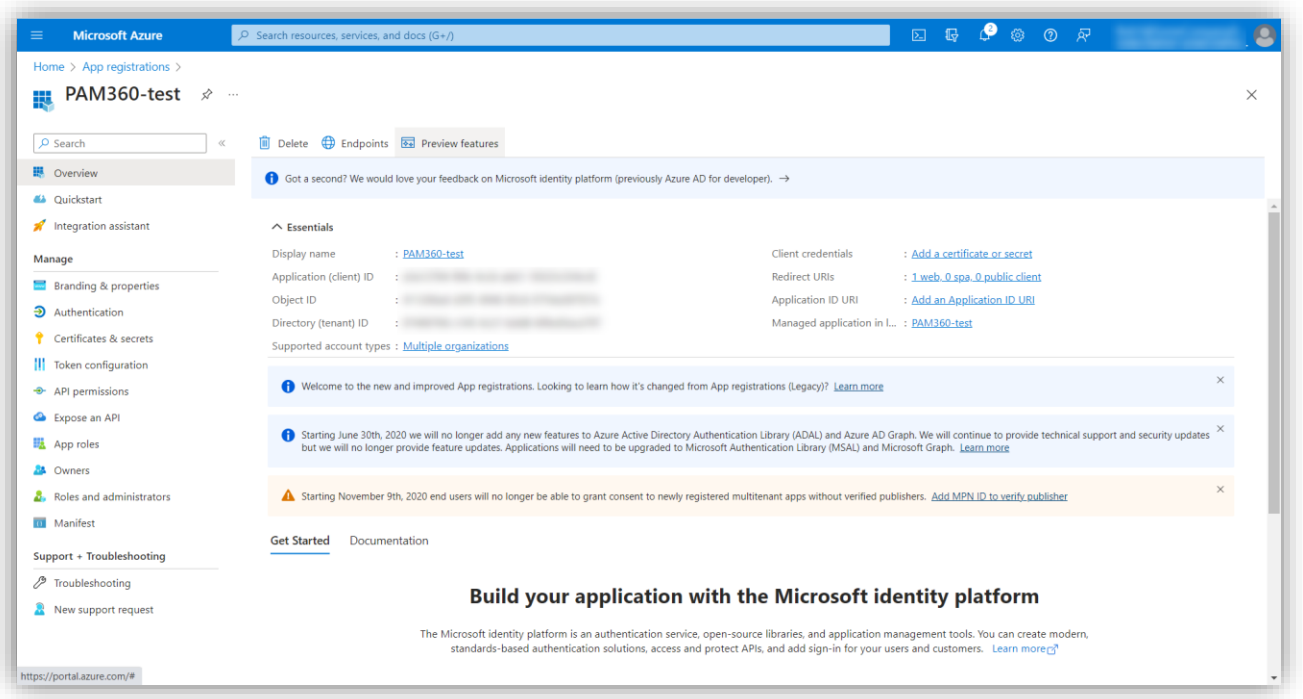
   i. Enter a name of your choice.

   ii. Choose **Supported account types** - Accounts in any organizational directory (Any Azure AD directory - Multitenant)

iii. For the **Redirect URI**, choose **Web** from the drop-down and enter the URI of PAM360 application in the following format: https://Hostname:port/pam360redirect/AzureOAuth. Please ensure that the PAM360 application URI provided here is the same as the one users can use to access the PAM360 application from other machines. Provide the same link in the Access URL section in step 1.2.



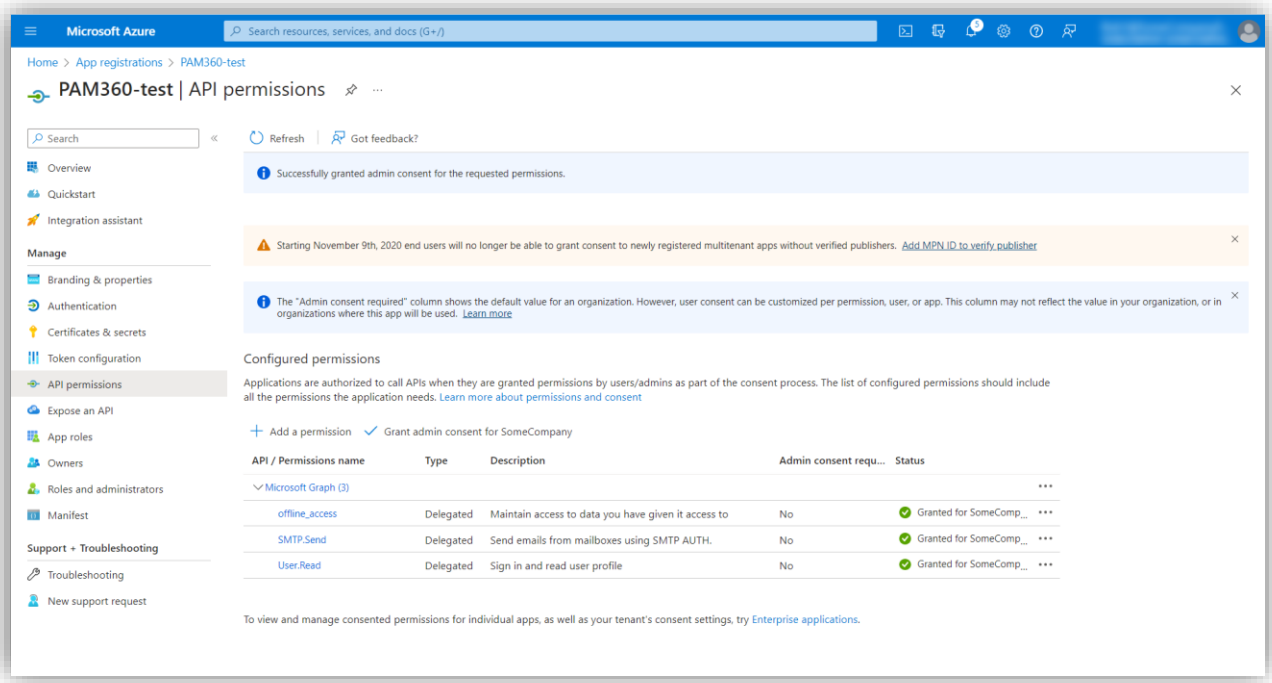
5. Click **Register**. PAM360 will be added as an application in the Azure AD portal.
6. You will be taken to the page with the details of the newly registered application.



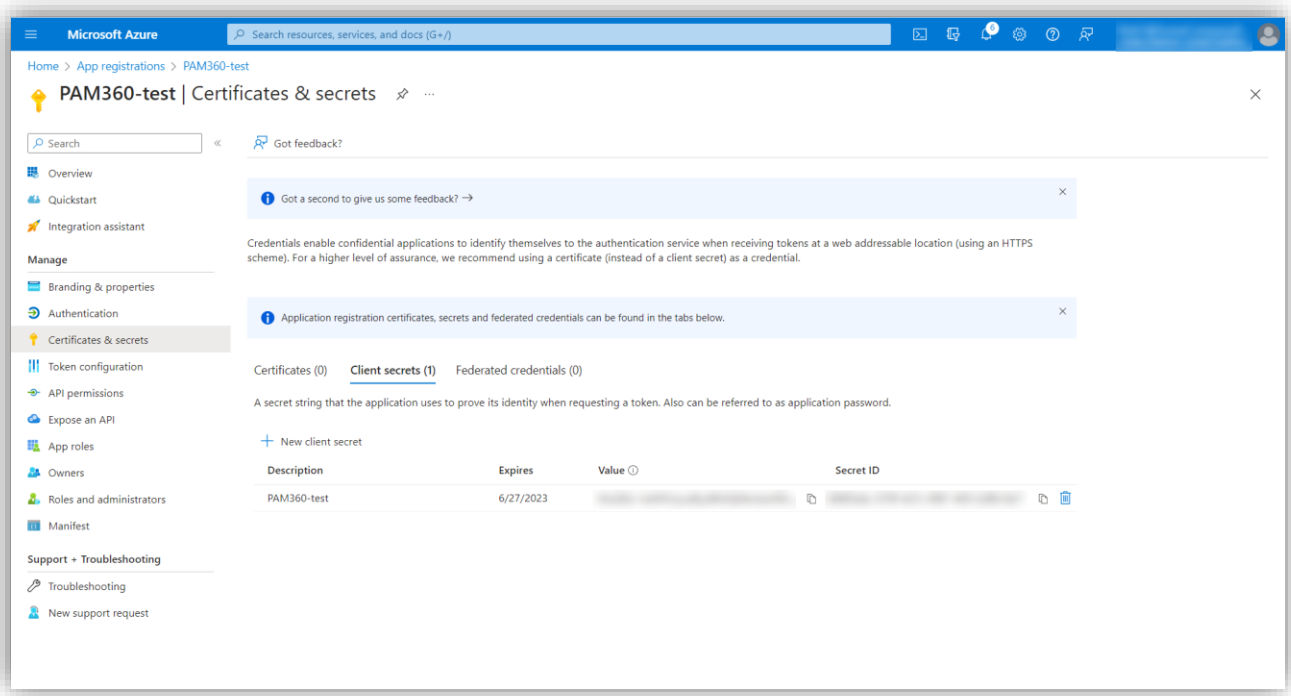
7. Click **API permissions** under **Manage** in the left pane. In the **API Permissions** page, click **+Add a permission**.

    i. In the **Request API Permissions** page, choose **Microsoft Graph.**
    ii. Search for "**SMTP.Send**" in the **Select Permissions** search bar to populate relevant permissions. Select the option **SMTP.Send** and click **Add Permissions.**
    iii. Search for "**offline_access**" in the **Select Permissions** search bar to populate relevant permissions. Select the option **offline_access** and click **Add Permissions.**

8. Now, click the **Grant admin consent** button beside the + Add a permission button.
9. In the pop up that opens, click **Yes** to grant consent for the requested permissions.



10. Click the **Certificates & secrets** option on the left pane.
11. Navigate to the Client secrets tab and click **+ New client secret**.
12. Enter a description and choose an expiry period. Click **Add**.
13. Immediately after creation, the client secret value is displayed under the **Value** column in the table, copy the value and save it in a secure location. This client secret value will be displayed only once and will not be accessible once you move away from this page.

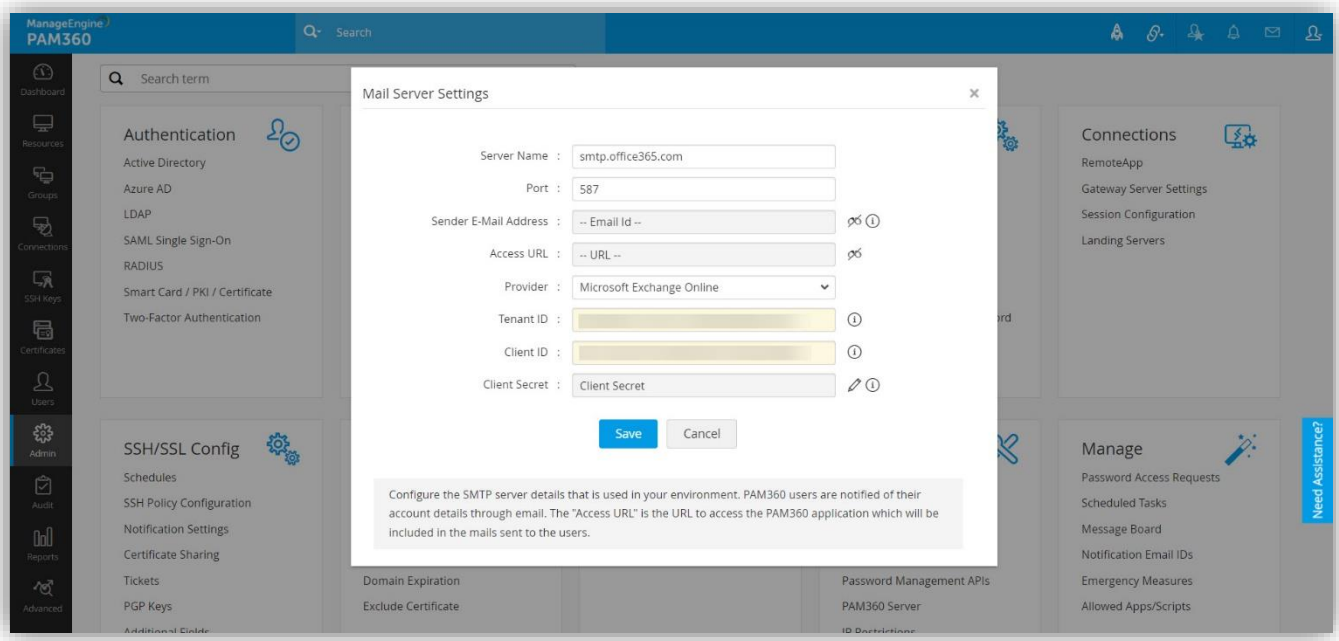


14. Once you have registered the application with the appropriate permissions, go to PAM360's web interface and configure mail server settings.

1.2 Steps to Configure Microsoft Exchange Online in PAM360

1. Navigate to **Admin >> Settings >> Mail Server Settings**
2. In the pop-up form that opens, enter the following:
    i. Server name - The actual SMTP server's name. For e.g. smtp.office365.com.
    ii. Port - The default port for TLS is 587 and for SSL is 465. Enter the port that you are using.
    iii. Sender E-mail Address - Please ensure that the sender e-mail address you are providing is the same as the Microsoft Azure credentials used to authenticate the mail server in point 3.
    iv. Access URL - The URL that is to be displayed on the mail intimation sent to users to access PAM360. Please ensure that the Access URL is the same as the Redirect URI mentioned in step 1.1. For example, if the mentioned Redirect URI is https://win10-prod-qa:8282/pam360redirect/AzureOAuth, then the Access URL given here must be https://win10-prod-qa:8282.
    v. **Mail Server** - Choose **Microsoft Exchange Online** from the drop-down.
    vi. **Tenant ID** - The directory ID of the Azure application.
    vii. **Client ID** - The application ID of the Azure application.
    viii. **Client Secret** - The client secret value created for the Azure application.
    Click **Save** to save the settings.

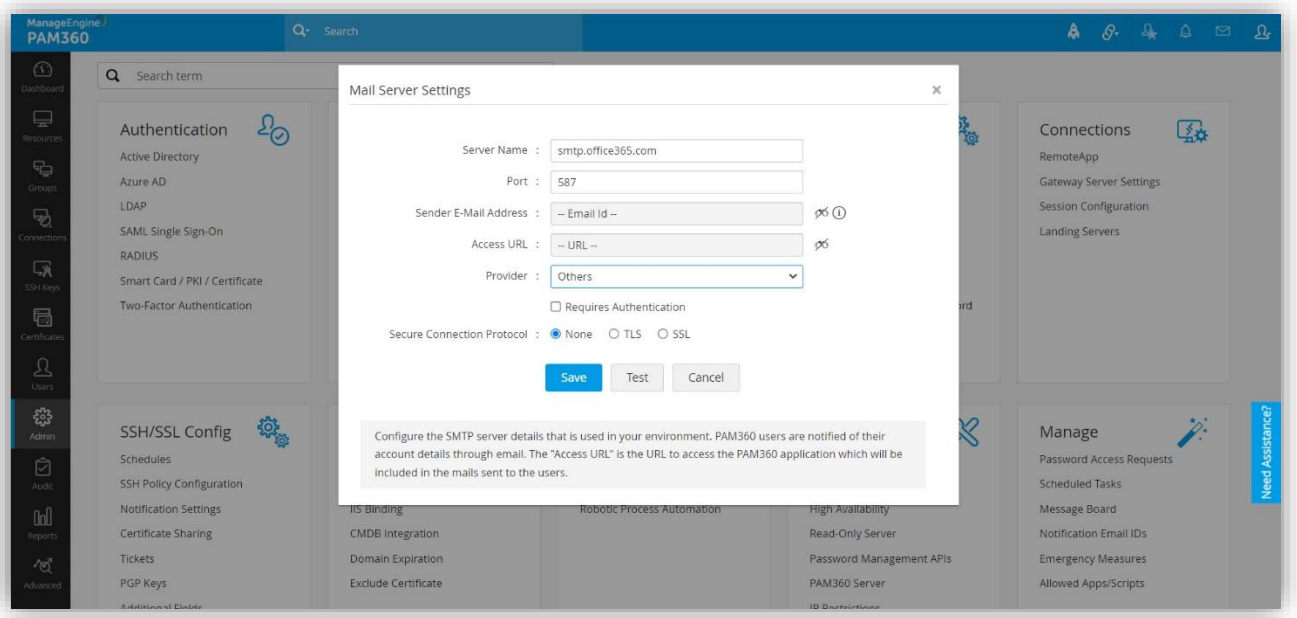
You have configured Microsoft Exchange Online as the mail server. When you save the settings, it will redirect you to the Microsoft Azure portal for authentication. This is a one-time operation.



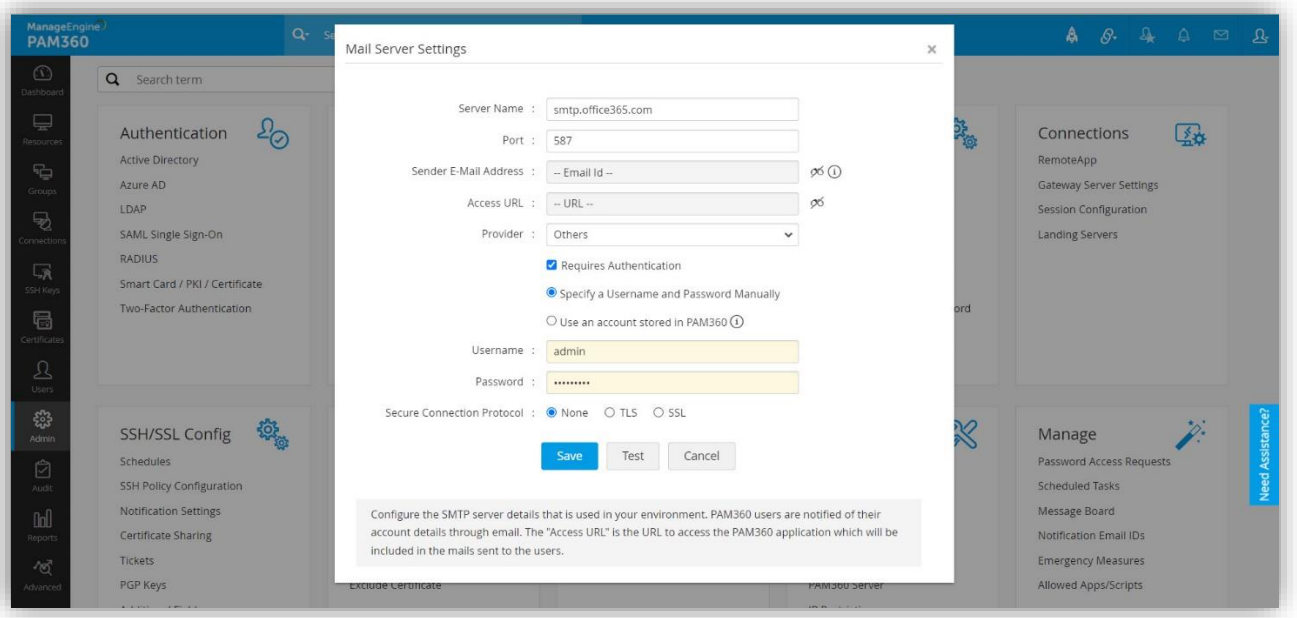
2. Configure Other Mail Servers

1. Navigate to **Admin >> Settings >> Mail Server Settings**
2. In the pop-up form that opens, enter the following:

    i. **Server name** - The actual SMTP server's name. For e.g. smtp.zoho.com.
    ii. **Port** - Most SMTP servers work with port 25. However, the default port for TLS is 587 and for SSL is 465.
    iii. **Sender E-mail Address**
    iv. **Access URL** - The URL that is to be displayed on the mail intimation sent to users to access PAM360.
    v. **Mail Server** - Choose **Others** from the drop-down.

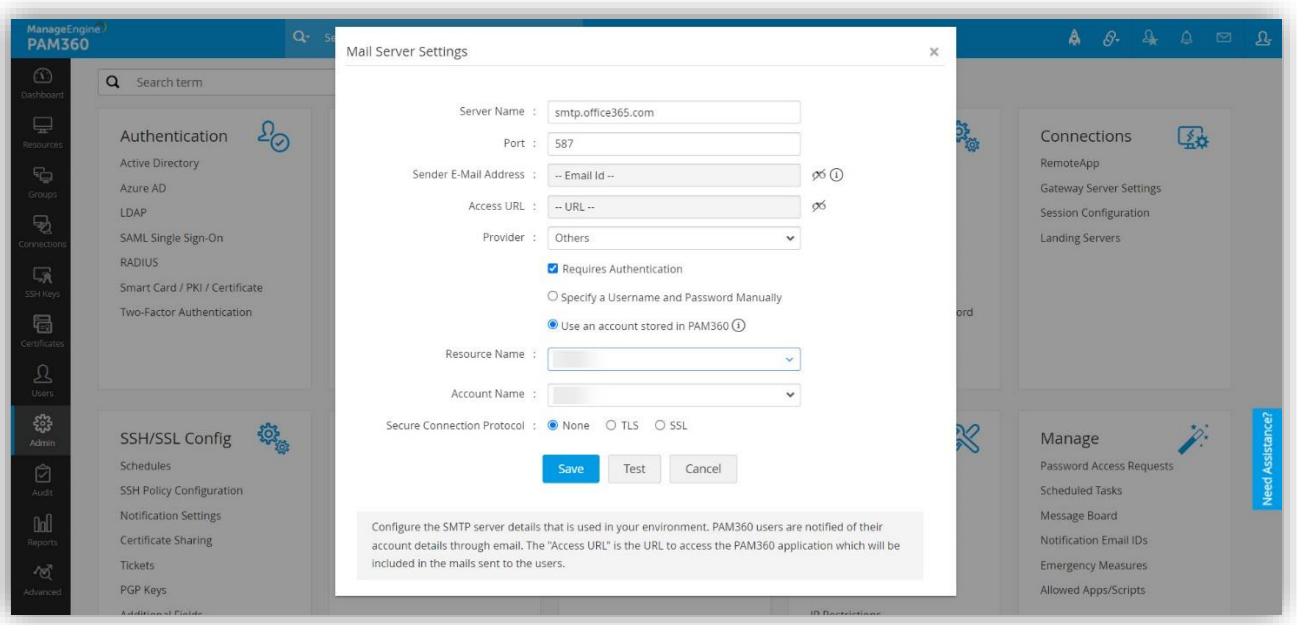


3. Upon clicking the **Requires Authentication** checkbox, the pop-up form lists two options:
4. Specify a Username and Password Manually or use an account used in PAM360.
5. If you choose the first option **Specify a Username and Password Manually**, enter the authentication details and click **Save**.



6. If you choose the second option **Use an account used in PAM360**, the resources and accounts that appear in your resources tab will be listed in a drop-down. You can choose the required details and click **Save**. The chosen Account will be used for authentication. Earlier, in case of a password change, the user has to manually update

the new password in the mail server settings. But now, the new password will be automatically updated for authentication.



7. You also have the option to choose the Secure Connection Protocol - None/SSL/TLS.
    i. **SSL** - Secure Sockets Layer (SSL) is a cryptographic protocol that enables secure connection over the internet.
    ii. **TLS** - Transport Layer Security (TLS) is a new version of SSL that enables secure connection over the internet.

Once you have provided the authentication details and the secure connection mode, click **Save**.

Notes:

1. It is recommended to use SSL/TLS options for secure communication over the internet /intranet.
2. If the mail server is using a self-signed certificate, then we need to import it in PAM360.
    - Copy the server certificate and paste it under **<PAM360 Installation Folder>/bin** directory.
    - From **<PAM360 Installation Folder>/bin** directory, execute the following command:

        importCert.bat ***<name of the server certificate>***

    - This adds the certificate to the PAM360 certificate store.

3. After providing the authentication details and the secure connection mode, you also have the option to test mail server before clicking save.

Privacy Settings

> **Note:** Privacy Settings can be viewed and modified only by privileged administrators.

PAM360 provides enhanced security options to its users while generating canned reports and exporting files from PAM360 in the below two ways:

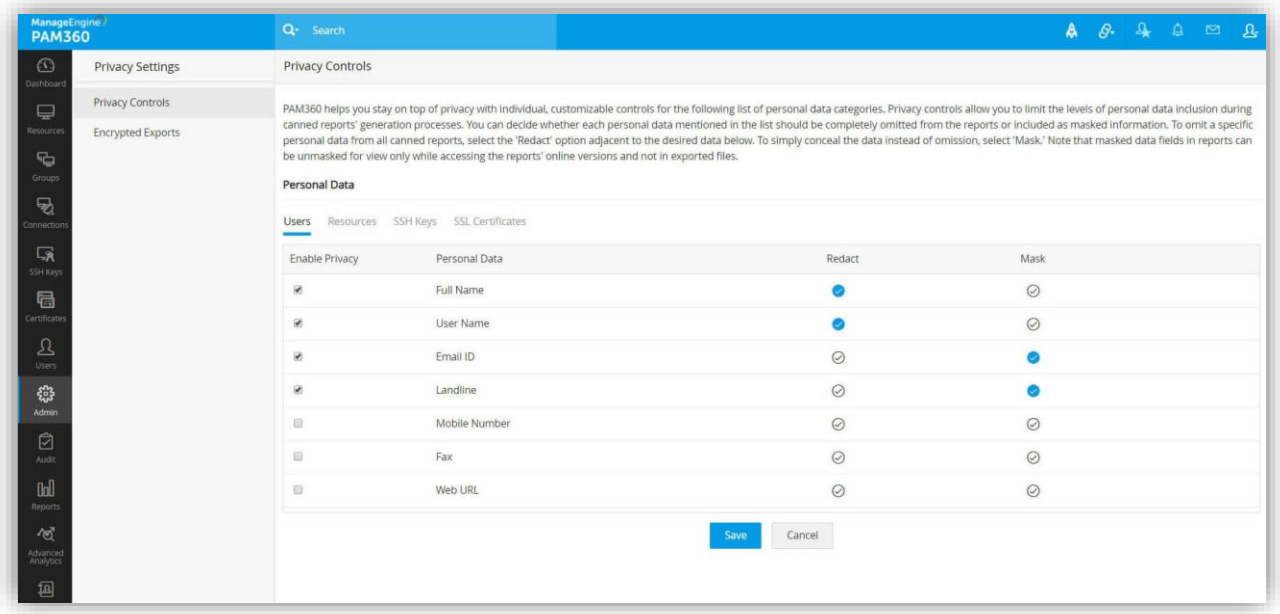
1. **Privacy Controls**
2. **Encrypted Exports**

1. Privacy Controls

To enhance privacy within the product, PAM360 helps you customize and control the inclusion of personal data in canned reports' generation processes. Canned reports are pre formatted reports generated by PAM360 that are available to users for visual analysis. You can decide whether each personal data input in PAM360 should go as masked entries in the reports or be completely removed from them.

To format the inclusion of personal data in the reports, follow the below steps.

1. Navigate to **Admin >> Settings >> Privacy Settings >> Privacy Controls.**
2. You'll find four categories with all their respective data listed under **Personal Data** column.
3. Select the checkbox(es) under **Enable Privacy** column for all the data you want to be masked or redacted from the reports.
4. If you select **Redact** adjacent to the selected data, PAM360 will omit the data completely from all canned reports. You can choose this option for the data you don't want to be generated in the reports.
5. If you select **Mask** adjacent to the selected data, PAM360 will simply mask the data in the reports. The data will be denoted by asterisks in the reports generated. Note that masked data in the reports can be unmasked for view by clicking them while accessing the reports' online versions.
6. Once you have made the necessary choices, click **Save.**



7. You can generate a canned report and test the visibility of the selected personal data in it by navigating to **Reports** and generating a canned report of your choice.
8. You'll notice that the data you chose to be redacted has not been generated in the report, and the data you chose to be masked has been denoted by asterisks. You can click on the masked data in order to view them. However, they'll remain masked when you export the report as a PDF or an XLS file.

> **Note:** This feature is available only for generating canned reports and not for custom or query reports.

2. Encrypted Exports

In order to protect all the exported files across PAM360 with a password, you can either set a single password which will be uniformly used for all export operations or allow the users to set their own passwords for the files they export. In order to do so, please follow the steps below:

1. Navigate to **Admin >> Settings >> Privacy Settings >> Encrypted Exports.**
2. Select the checkbox for "Enable automatic encryption of all exports from Resources, Groups, Audit, and Reports." This will enable you to set a common password for all the exported files in two ways.
   i. **Manually specify a passphrase:** You can choose this option to manually enter a passphrase for encrypting your files.
   ii. **Use the password of an account stored in PAM360:** You can choose this field to select the password of any account added in PAM360, by choosing the respective

resource and the corresponding account from the drop-down menu. Using the password of a stored account will enable you to define password policies, effect regular resets, and also maintain password history for export operations.

3. In addition, you can also allow the users to set their own passphrase for encrypting an exported file by choosing the checkbox for **Allow users to supply their own passphrase.**
4. Click **Save.**

Important note:

- Enabling encryption for exports will apply only to the following export operations:
  - ➤ Resources and resource groups export to XLS file
  - ➤ Audit export to PDF and CSV files
  - ➤ Reports export to PDF and XLS files
- The option to export resources and resources groups as an encrypted HTML file is excluded here since HTML file encryption is a default setting in PAM360, unlike the aforementioned export operations which are not password protected by default
- Encrypted exports setting applies only for users' enterprise resources and not their personal data stored under the **Personal** tab. Files exported from the personal section in PAM360 will instead be protected with the passphrase that the user supplied earlier to be used as their exclusive encryption key.

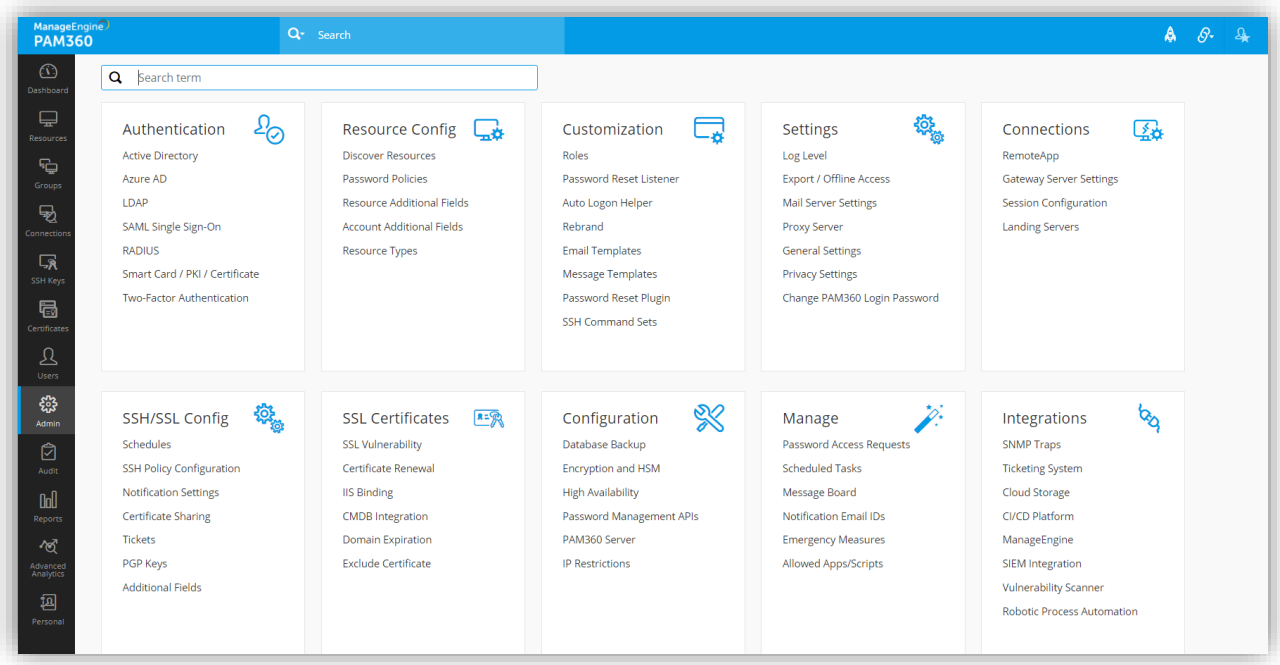
SNMP Traps

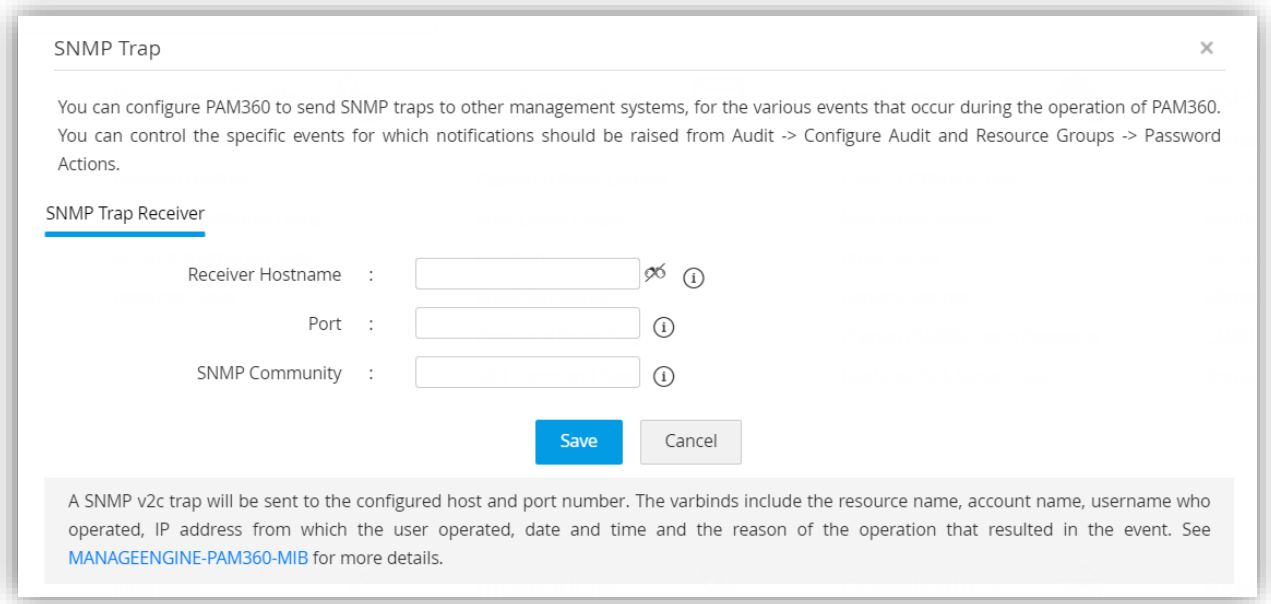
PAM360 facilitates raising SNMP Traps to your management systems on the occurrence of various password actions and audit events.

Configuring the SNMP

PAM360 has built-in support to send a SNMP v2c trap to the desired host and port. The varbinds include the resource name, account name, name of the user who operated, IP address from which the user operated, date and time and the reason of the operation that resulted in the event.

1. Navigate to **Admin >> Integration >> SNMP Traps**





2. In the dialog box that opens,
   i. Switch to **SNMP Trap Receiver** tab
   ii. Enter the **Receiver Host Name** of the receiver to whom you wish to send the traps.
   iii. Specify its **Port** and the **SNMP Community**.
   iv. Click **Save.**

Remote Host

Imagine a hierarchical organization with a massive number of users and resources with the following organization setup:

i. Proxy servers - configured between the target resources and the user machines
ii. Load balancers - deployed between the target resources and the user machines to maintain the request traffic

With the above organization setup, the audits and reports reflect the IP address of the load balancer/proxy server through which the user request(s) is forwarded instead of the actual user machines' IP addresses. When multiple requests occur consecutively, the same IP address (of the load balancer/proxy server) is captured for all the user requests under audits and reports. Because of this, none knows who accessed what and the exact user access information is also lost. Here comes the need for the Remote Host Header - it identifies the IP addresses of user machines accessing target endpoints through the load balancer or proxy server. As a result, the product audits and reports provide good visibility into user access.

Prerequisite

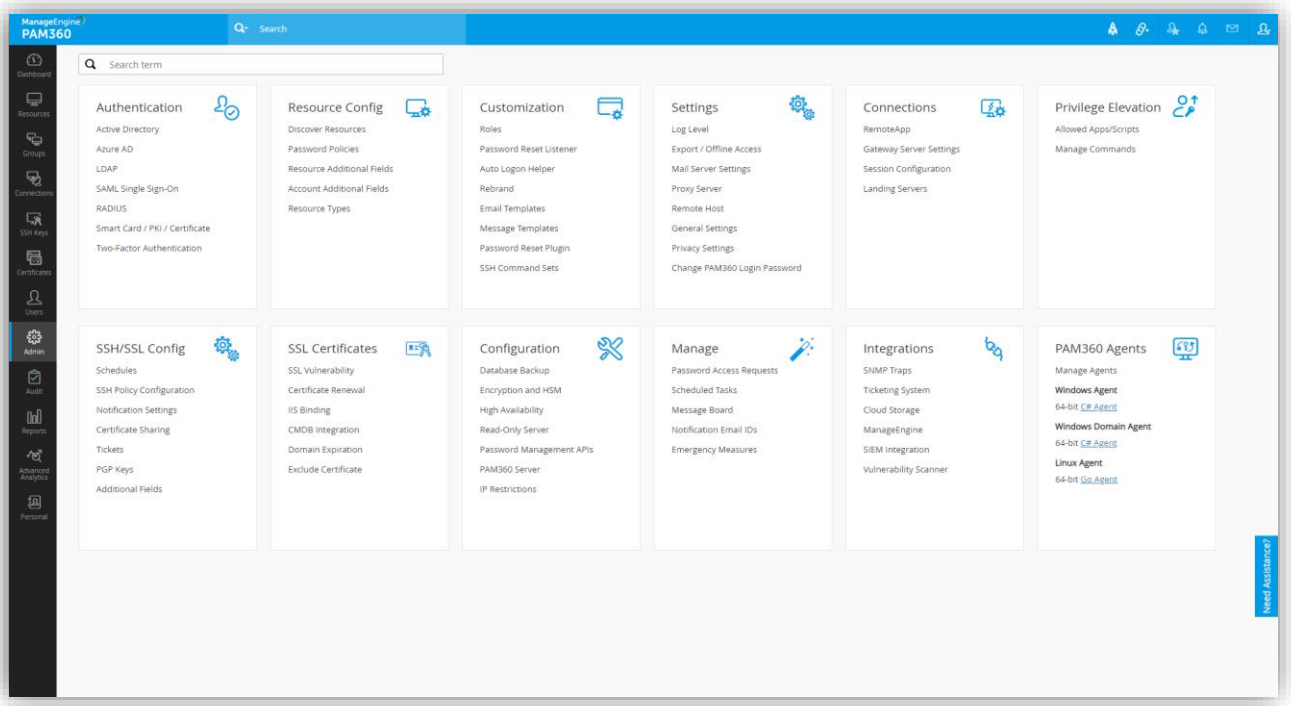
Before configuring Remote Host, find the request header information (e.g., X-Real-IP, X-Forward-For, etc.) in the 'conf' file of your load balancer/proxy server.

Notes:

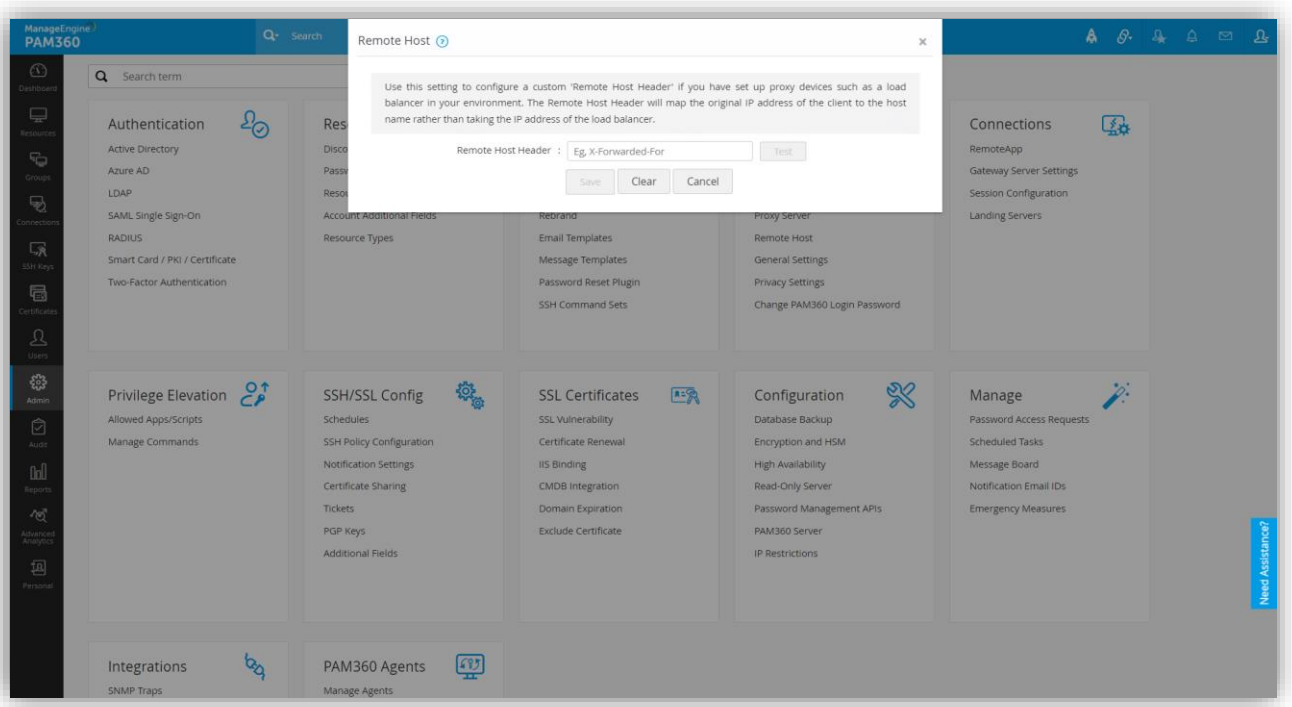
1. If an organization has multiple load balancers/proxy servers, ensure you configure the request header of all those with the same header information.
2. We recommend you configure the load balancers/proxy servers in such a way that they forward only the IP address of the client. For example, replacing the header variable '$proxy_add_x_forwarded_for' with

Steps Required

1. Navigate to '**Admin >> Settings >> Remote Host**'.



2. Enter the header information obtained from the 'conf' file of the load balancer/proxy server in the **Remote Host Header**.



3. Click **Test** to validate the provided header information with your load balancer/proxy server.

4. Upon successful test validation, click **Save** to complete the remote host configuration.
5. Click **Clear** to revoke the Remote Host configuration.

IP Restrictions

Note: This feature is available for privileged administrators only.

PAM360 allows the privileged administrators to limit inbound connections to PAM360 server by enforcing IP-based restrictions to minimize unwanted traffic. It provides an added layer of security by letting the administrator to choose exactly which systems should be allowed to or blocked from accessing and sending requests to the PAM360 server. Allowing or restricting access can be done for an individual IP as well as a range of IP address(es).

PAM360 offers three types of IP restrictions:

1. **Web Access**
2. **API Access**
3. **Agent Access**

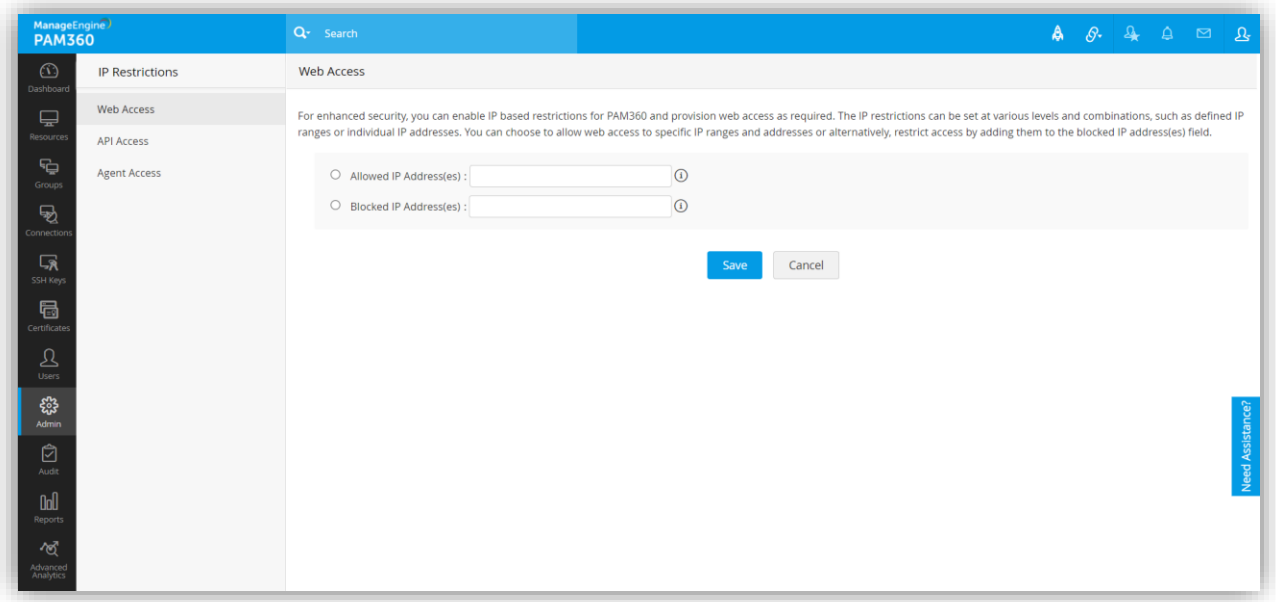
1. Web Access

You can enable IP based restrictions for access to PAM360 web server. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses.

To configure IP based restrictions, follow the below steps:

1. Navigate to **Admin >> Configuration** and select **IP Restrictions.**
2. Under **Web Access,** you have two options to choose from:
   - **Allowed IP Address(es):** If this option is selected, only the IP addresses specified in this field will be allowed access and the rest of the IP addresses will be blocked from accessing the PAM360 web server.
   - **Blocked IP Address(es):** This option can be used to block a specific IP address or an IP range and allow access to all other IP addresses.

Note: The IP addresses must be entered in the text field as comma-separated values. **Eg: 10.0.2.1 - 10.0.2.15, 10.0.3.176, 10.0.3.222.** There is no limit to the number of IP addresses that can be defined in both the fields.



2. API Access

PAM360 allows you to enable IP based restrictions for API calls as well as communication from native mobile apps and browser extensions to PAM360 server. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses.

To configure IP based restrictions, follow the below steps:

1. Navigate to **Admin >> Configuration** and select **IP Restrictions.**
2. Under **API Access,** you have two options to choose from:
   - **Allowed IP Address(es):** If this option is selected, only the IP addresses specified in this field will be allowed API access and the rest of the IP addresses will be blocked from sending and/or receiving API calls.
   - **Blocked IP Address(es):** This option can be used to block a specific IP address or an IP range and allow access to all other IP addresses.

Note: The IP addresses must be entered in the text field as comma-separated values. **Eg: 10.0.2.1 - 10.0.2.15, 10.0.3.176, 10.0.3.222.** There is no limit to the number of IP addresses that can be defined in both the fields.

3. Agent Access

PAM360 allows you to regulate agent communication from target machines to PAM360 server with IP based restrictions. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses.

To configure IP based restrictions, follow the below steps:

1. Navigate to **Admin >> Configuration** and select **IP Restrictions.**
2. Under **Agent Access,** you have two options to choose from:
    - **Allowed IP Address(es):** If this option is selected, only the IP addresses specified in this field will be allowed access and the rest of the IP addresses will be blocked from accessing the PAM360 web server.
    - **Blocked IP Address(es):** This option can be used to block a specific IP address or an IP range and allow access to all other IP addresses.

> **Note:** The IP addresses must be entered in the text field as comma-separated values. **Eg: 10.0.2.1 - 10.0.2.15, 10.0.3.176, 10.0.3.222.** There is no limit to the number of IP addresses that can be defined in both the fields.

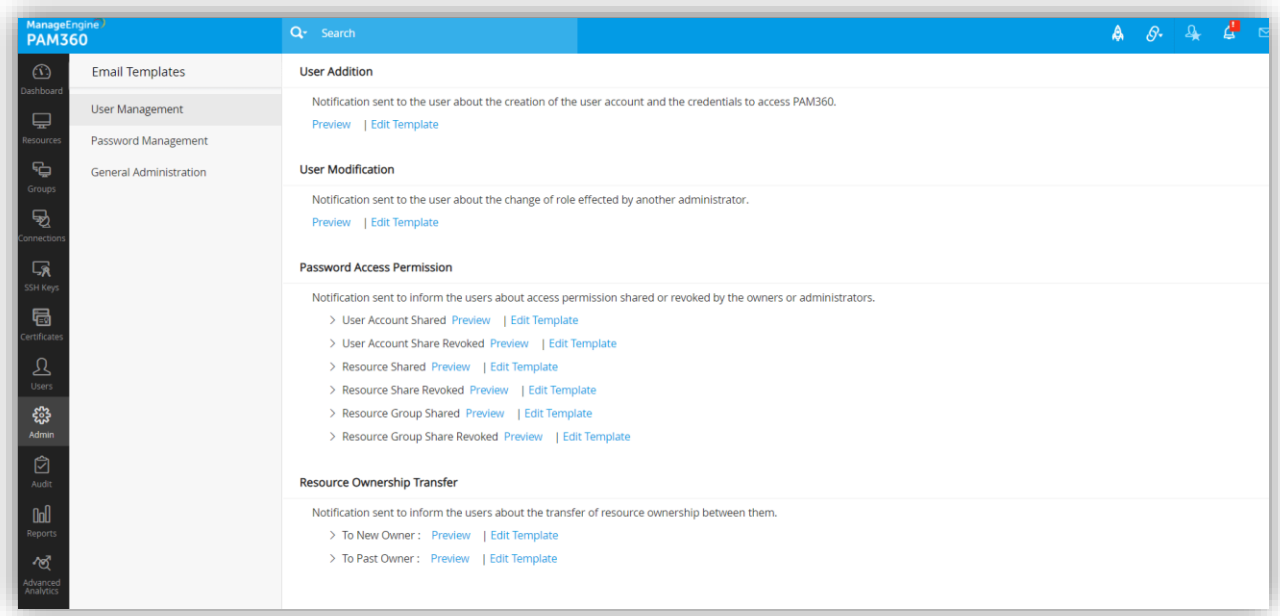
Email Templates

PAM360 facilitates sending email notifications on the occurrence of various password actions. By default, PAM360 has a specific content for the email notification. If you want, you can customize the content and have your own content.

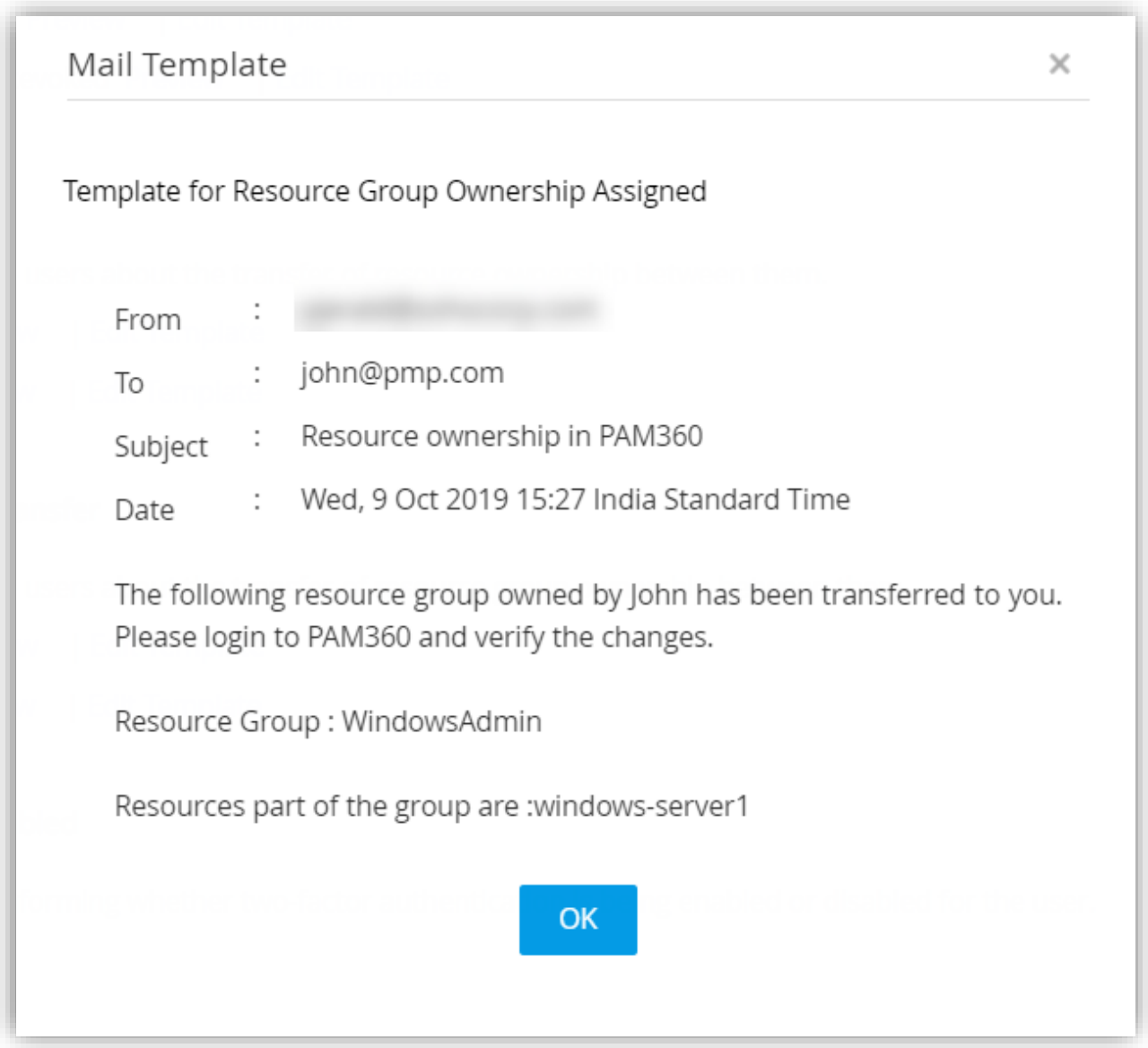
Steps Required

To customize the email content,

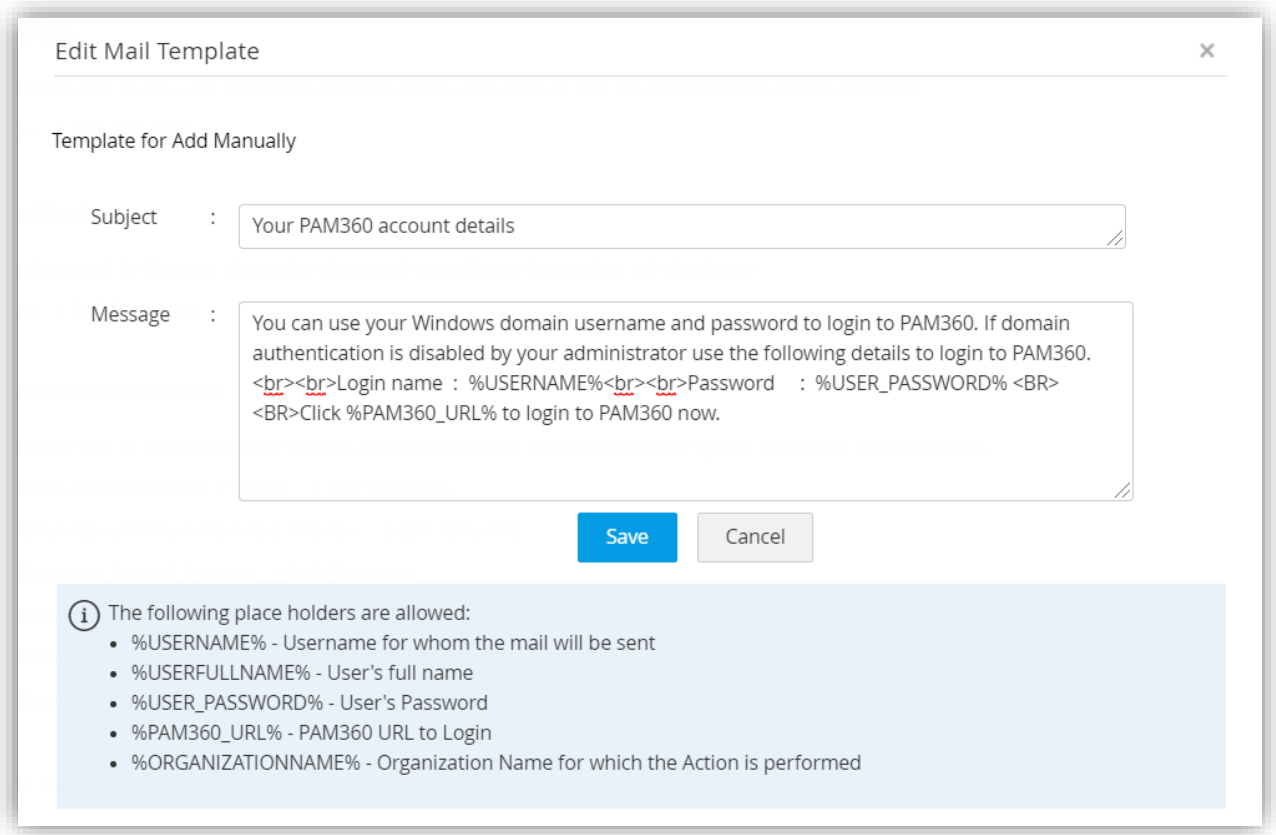
1. Navigate to **Admin >> Customization >> Email Templates.**



2. In the UI that opens, select the required category - **User Management, Password Management & General Administration,** shown on the right hand side of the UI. For each category, you will find a number of sub-categories with a dedicated email template for each action such as user addition, user modification, user account shared etc.
3. You can **preview** the existing email content for each notification by clicking the respective **Preview** link.



4. If you want to edit the content, click **Edit Template** against the desired template.
5. In the **Edit Template** window, you can specify a customized message in the **Subject** line.
6. You can also modify the body content in the **Message** field.
7. While entering the content of the body, you can specify placeholders for certain values like user name. The exact user name will be replaced with the placeholders at runtime. The allowed placeholders for each template can be found at the bottom of its respective Edit Template window.
8. Click **Save**. The email notifications of the respective categories will now have the new content.



Notes:

- PAM360 facilitates customizing most of the email content in PAM360. However, email notifications on reports and alerts are not customizable.
- You can use html tags in your customized message with the restriction that only single quotes be used inside the html tags instead of double quote. For example: **instead of** , **you need to use** >span style='padding-left:10px'<

Additional Fields

PAM360 allows you to add custom fields to the **Add Resource/Add Account** windows, thereby enabling you to attach any additional information about the resources and accounts such as EOL dates, serial numbers etc. Additional fields are also useful while creating dynamic groups in PAM360, since you can use the custom values stored to provide criteria expressions for the groups. You can create around 20 custom fields individually for both resources and accounts.

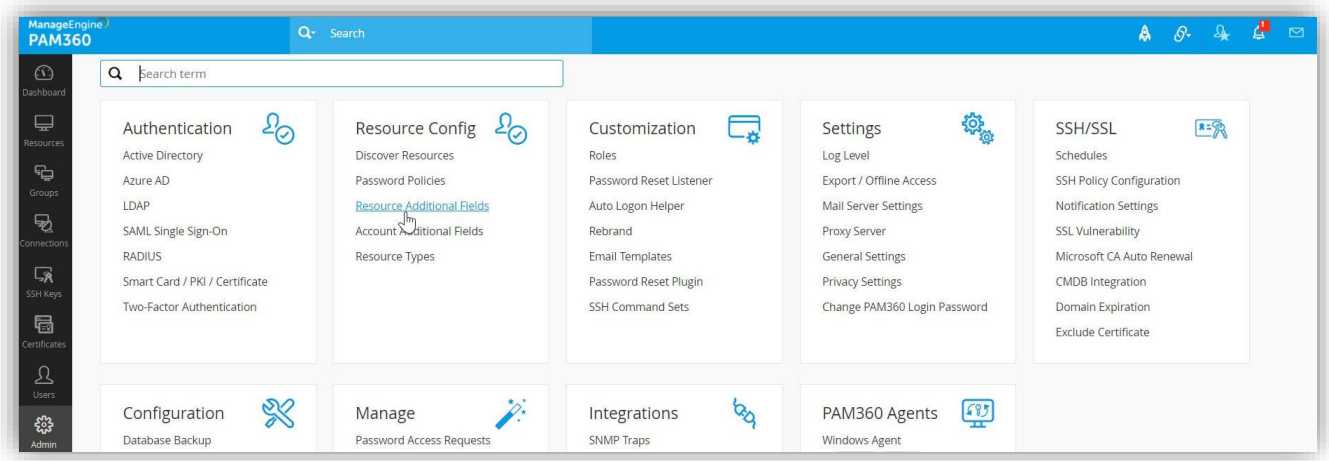
This document walks you through the following topics:

1. **Creating Additional Fields**
2. **Enabling Additional Fields**
3. **Additional Fields - Use Cases**

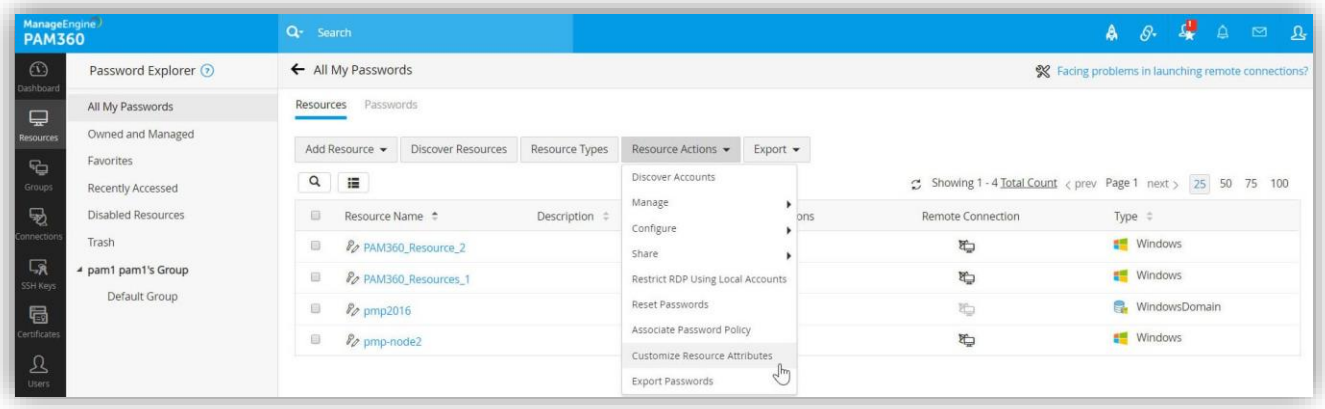
1. Creating Additional Fields

These fields can be globally created from **Admin >> Resource Config >> Resource / Account Additional Fields** (or) **Resources >> Resource Actions >> Customize Resource Attributes** (applicable only for resource additional fields).

<u>Through the Admin tab</u>:



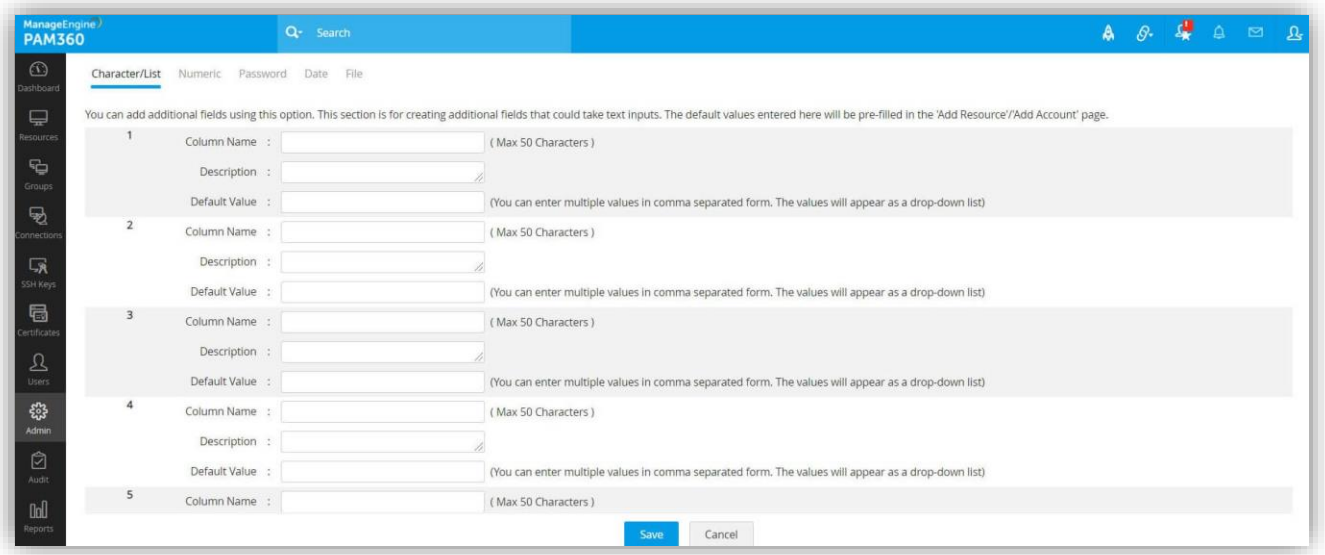
<u>Through the Resource tab</u>:

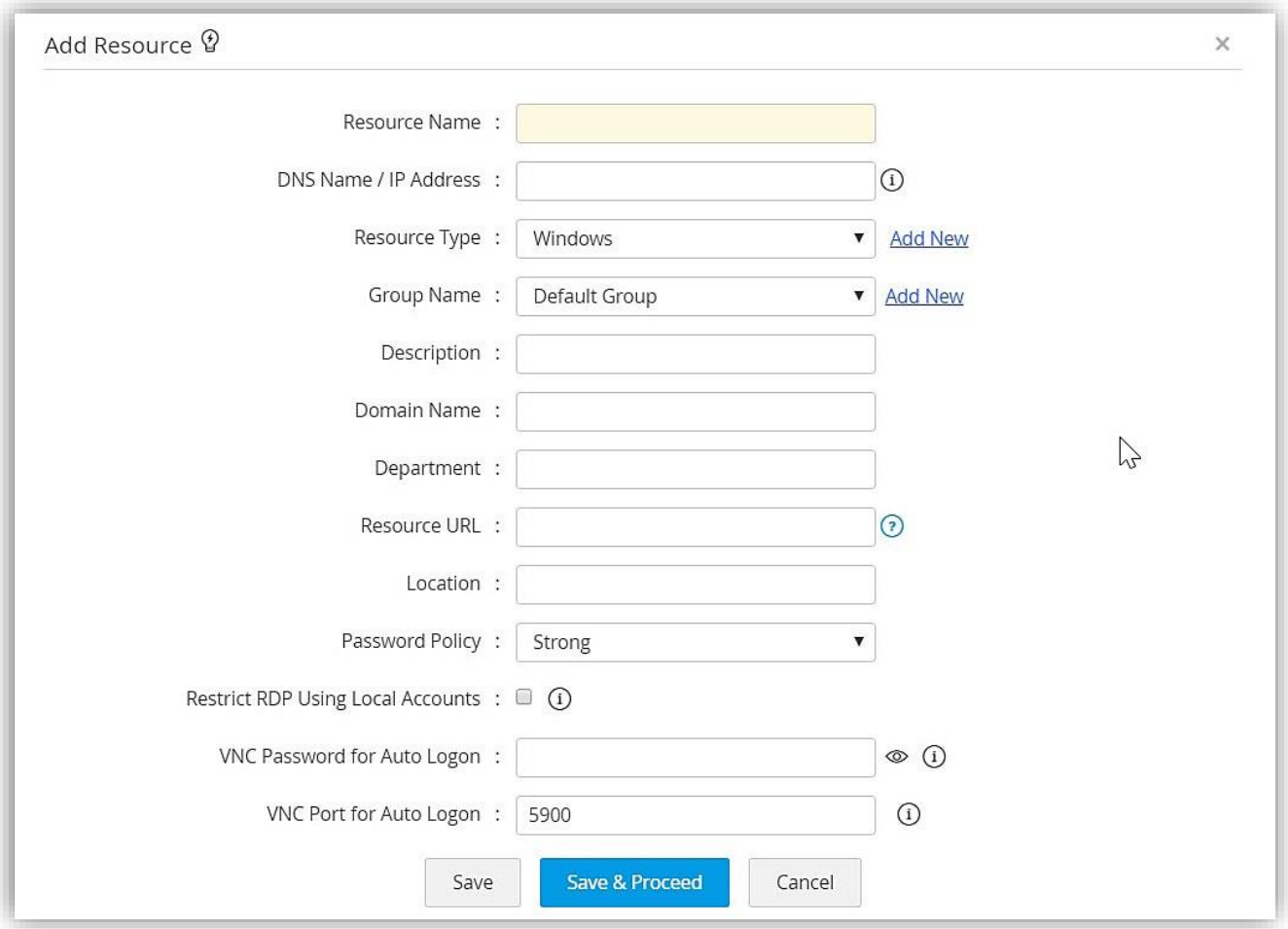


The different types of additional fields available are,

1. **Character/List** - For text inputs.
2. **Numeric** - To store numerical inputs.
3. **Password** - To store password inputs. The values entered here will be treated the same as the predefined password field and will not be shown in plain text in the GUI. Additionally, you can also specify separate password policies for this field; a password generator icon will also be present beside the field to help generate values according to the defined policy.
4. **Date** - To store date and time inputs.
5. **File** - To store file-based inputs.

Once you have added the desired details for the new column field, click **Save**. You can find the newly added column in the **Add Resource** window.





2. Enabling Additional Fields (for Specific Resource Types)

When you create an additional field of the type **Character/Numeric/Password/Date**, the fields are typically created globally for all resource types and take effect immediately. However, you can also choose to display those fields in the **Add Resource** (or) **Add Account** window only for specific resource types. To enable this setting, you have to disable the fields for the other resource types.

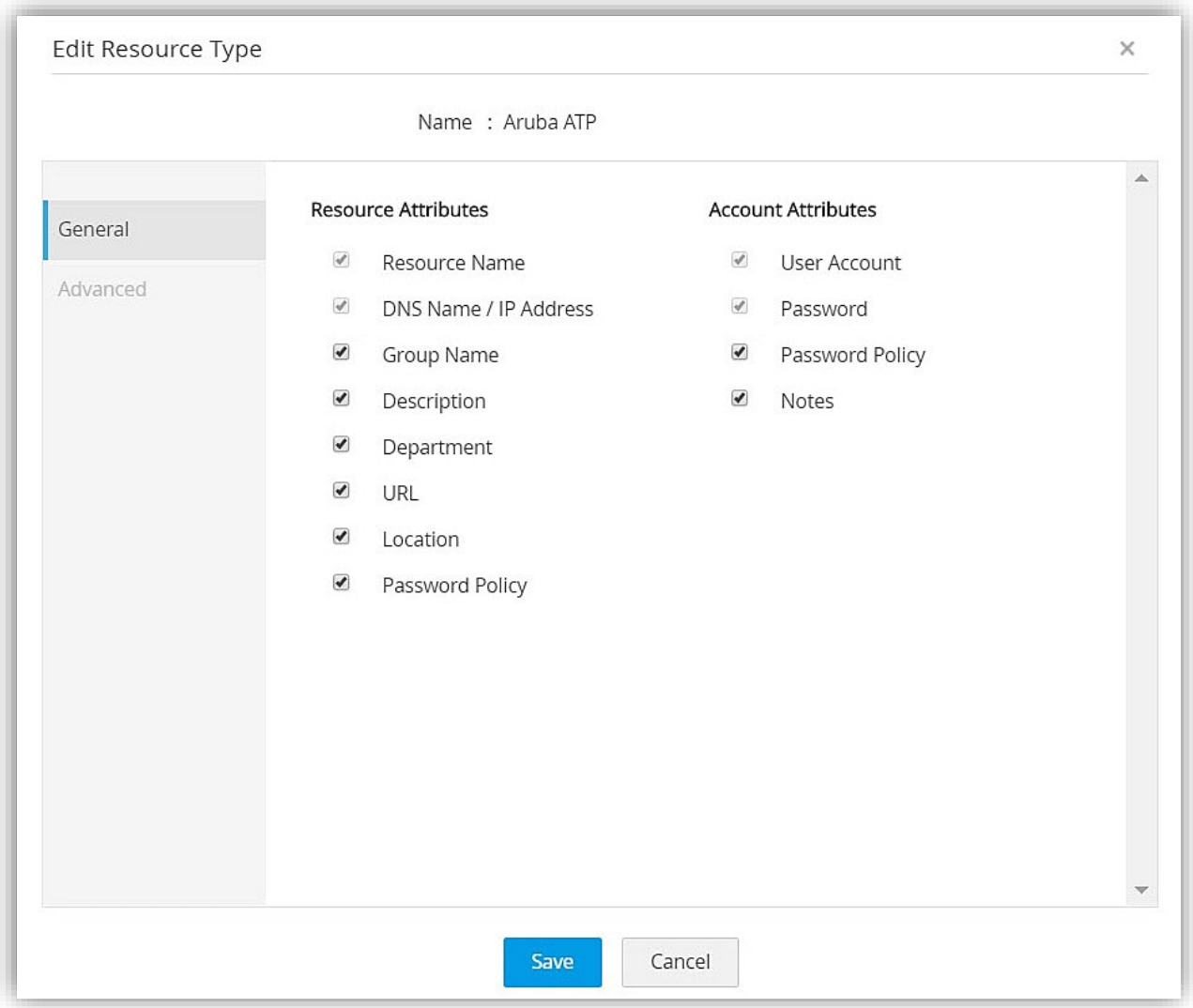
To do this,

1. Navigate to **Admin >> Resource Config >> Resource Types.**
2. Then click the **Edit** icon against the required resource type for which the additional field should be disabled.
3. In the dialog box that opens, uncheck the checkbox against the additional field.
4. Click **Save.**

Alternatively, when you create a custom field of the type **File**, it does not take effect automatically for both resources and accounts. You need to specify for which resource types you would like to have this additional field.

To do this,

1. Navigate to **Admin >> Resource Config >> Resource Types.**
2. Then click **Edit** icon against the required resource type.
3. In the pop-up form that opens, select the checkbox against the field **File.**
4. Click **Save.**



Show/Hide Columns - Customize **Resources** tab view when there are various additional fields, users can customize their Resources tab by choosing to display only preferred columns. This can be carried out using the **Column Chooser.**

Apart from **Show/Hide** option, users can also change the sort order of the columns by simply dragging and dropping the required columns.

3. Additional Fields - Use Cases

Case 1: Adding BIOS Password fields for Windows and Linux resources**:**

Securely storing the BIOS password of Windows and Linux systems is a mandatory requirement for many enterprises. To tag this password to the resource, you can create an additional **Password** field and enable the field only for Windows and Linux resources.

Case 2: Adding EOL and EOS dates for Network Devices:

Network devices such as switches, routers, and firewalls usually come with End of Life (EOL) and End of Sale (EOS) dates. To keep track of these dates, you can create an additional **Date** field and enable the field for desired network devices and other resource types.

Case 3: Securing critical accounts with a Severity Rating:

To mark privileged accounts that are highly critical in nature such as firewall administrative accounts and important database accounts, you can create an additional **Character** field at account-level as mentioned below:

1. Navigate to **Admin >> Resource Config >> Account Additional Fields.**
2. Under **Character/List** tab, create a new field with the name **Severity Rating**. Beside **Default Values**, enter the following: **High, Medium, Low.**
3. Click **Save.**

Now, when you add multiple accounts under a resource, you can mark accounts of highly critical nature with a severity rating of **High.**

Managing Schedules

PAM360 provides the option to quickly view and edit the schedules created by users and system at one place, thus helping IT admins to easily manage all the schedules. Users can also enable, disable or delete a schedule.

> **Note:** If a schedule is disrupted by a modification in its associated configuration, it will be deactivated in **Scheduled Tasks**. To reactivate a schedule upon re-enabling the export options, click on **Schedule Actions** beside the schedule and select the **Enable Schedule** option.

To manage schedules,

Navigate to **Admin >> Manage >> Scheduled Tasks.**

The following topics explains the possible ways to manage schedules:

1. Schedule Actions
   1.1 View Schedules
   1.2 Edit Schedule
   1.3 Enable or Disable a Schedule
   1.4 Delete Schedule
2. Filter
3. Search

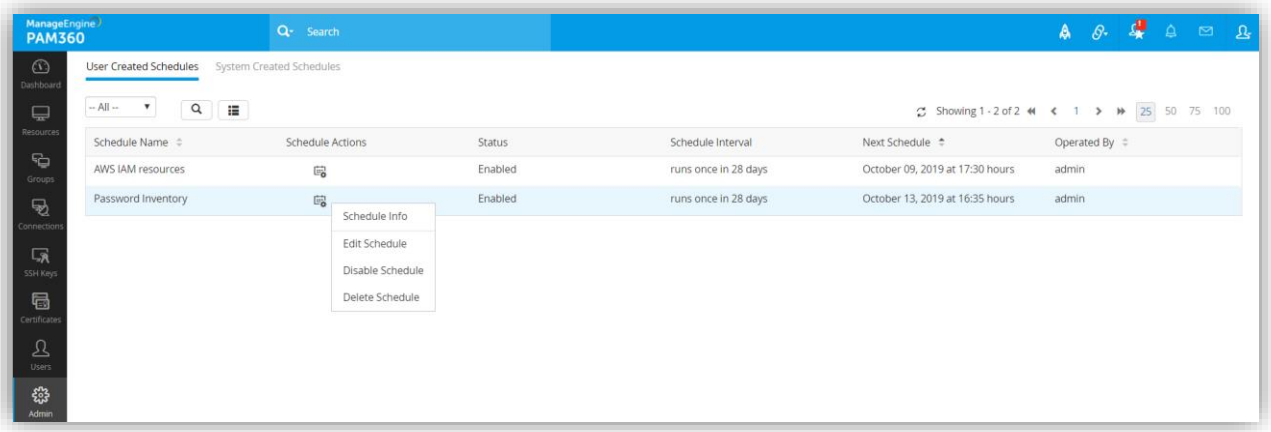
1. Schedule Actions

PAM360 provides schedule actions option, that helps you perform the following tasks:

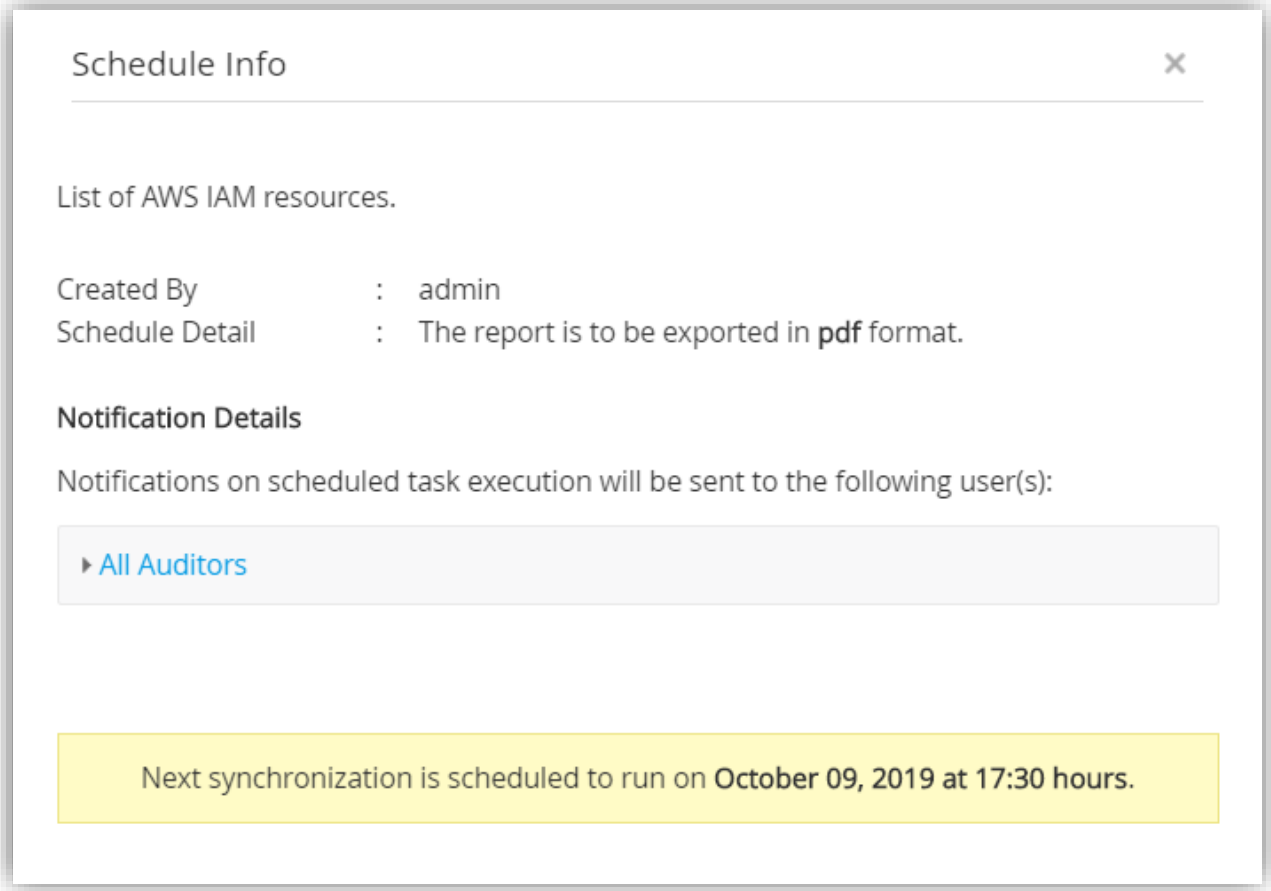
- View schedule info for system created schedule.
- Edit any user created schedule.
- Enable or disable any user created schedule.
- Delete any user created schedule.

Schedule Info:

1. Click the **Schedule Actions** icon against the schedule whose schedule details you want to view and select **Schedule Info** from the drop down list.



2. You can now view schedule details such as schedule description, schedule type, user name, schedule owner, notification details and the next scheduled time.



Schedule Info is available only for system created schedules.

1.1 View schedules

From **Scheduled Tasks** page, you can view both user created schedules and system created schedules. The list includes details such as:

- Schedule name
- Schedule actions
- Schedule status
- Schedule interval
- Next schedule
- Operated by

1.2 Edit schedule

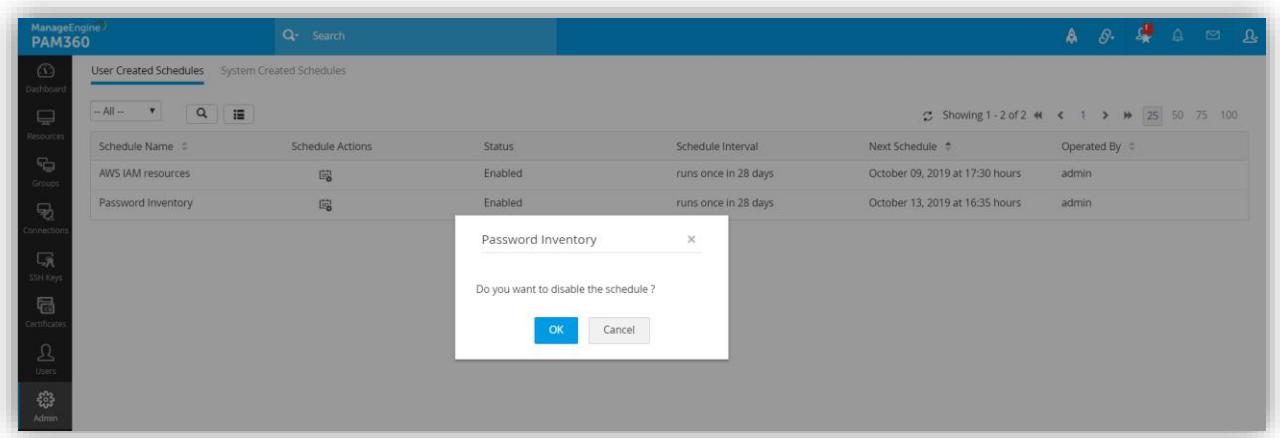
You can view the current status of every schedule at the top of edit schedule window. Using this option, you can edit the schedule interval, date and schedule start time of any user created schedule. You can also edit the list of recipients for notification after the execution of each schedule. The edit schedule option is not available for system created schedules.

1. Click the **Schedule Actions** icon against the resource whose schedule you want to edit and select **"Edit Schedule"** from the drop down list.
    i. Schedule Interval
    ii. Date
    iii. Schedule Start Time
2. You can also configure the users to be notified after the execution of each schedule.

1.3 Enable or Disable a schedule

Using this option, you can enable or disable any user created schedules. This option is not available for the system created schedules. However, you can disable system created password synchronization schedule.

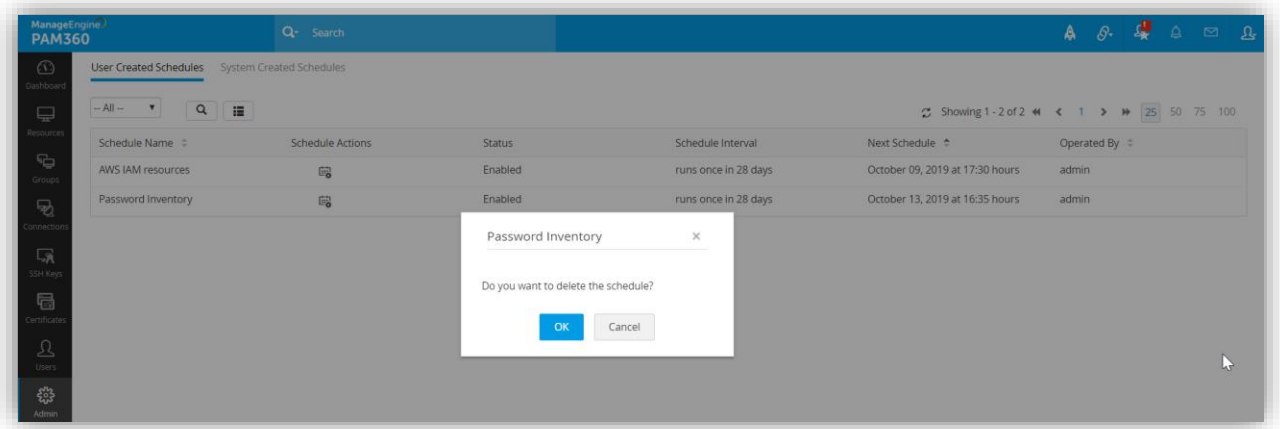
1. Click the **Schedule Actions** icon against the schedule whose schedule is to be enabled / disabled and select the required option from the drop-down.
2. You can now enable or disable any user created schedules.



1.4 Delete schedule

This option helps you delete any user created schedule.

1. Click the **Schedule Actions** icon against the schedule whose schedule you want to delete and select **Delete Schedule** from the drop down list.
2. In the pop-up that appears, click **Ok** to delete the schedule.



2. Filter

Using this option, you can filter and view the list of schedules.

To use filter option, click the **filter** icon present in the top left corner and filter the schedules by choosing the scheduled task's execution time interval.

3. Search

The search option helps you to find any schedule just by specifying the schedule name or schedule operator name.

To search schedule, click the **search** icon present in the top left corner and search any

schedule by specifying the schedule name or operator name.

Storing Personal Passwords in PAM360

In addition to enterprise passwords, PAM360 allows you to store personal passwords in the PAM360 repository. It is also possible to save personal details such as your personal email account information, credit card numbers, and other banking data, contact addresses, phone numbers. To store such sensitive personal data, PAM360 offers a private repository that only you can access, in the form of a **Personal** tab for each user role. The information stored in the **Personal** tab is encrypted independently and hidden from all other users, including the administrator; this is to ensure complete privacy and security of your data.

To activate your **Personal** tab, supply an encryption passphrase for data encryption. In case your organization has enforced password complexity rules in your environment, PAM360 will also ask you to enter a passphrase that matches the complexity requirements. Once you set up your passphrase, PAM360 encrypts all your personal passwords using this passphrase. By default, PAM360 does not store the encryption key anywhere in the PAM360 database. You must provide this passphrase to access your personal passwords every time. If you forget the passphrase, you cannot reset or recover it, leading to a loss of access to your personal

At the end of this document, you will have learned the following:

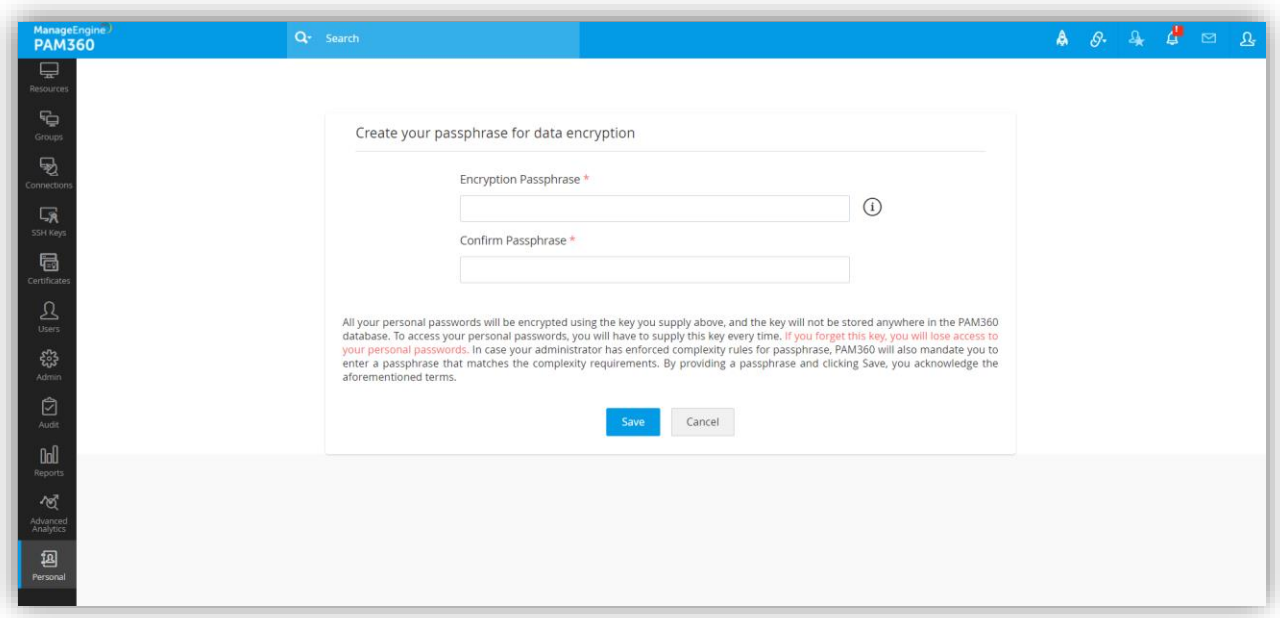
1. Encrypting Personal Passwords
2. Storing Personal Accounts
   - 2.1 Web Accounts
   - 2.2 Banking Accounts
   - 2.3 Credit Card Accounts
   - 2.4 Personal Contacts
   - 2.5 Deleting Accounts
3. Adding Custom Fields
   - 3.1 Creating Custom Categories
   - 3.2 Managing Custom Categories
4. Managing Passwords in Bulk
   - 4.1 Importing Passwords
   - 4.2 Exporting Passwords
5. Reset Personal Passphrase

1. Encrypting Personal Passwords

To gain access to the **Personal** tab, you must provide an encryption passphrase. While using the **Personal** tab in PAM360 is optional, administrators can enforce creation of an encryption passphrase for all users from the **General Settings**. To set a strong password policy, go to the **General Settings** page or navigate to **Admin >> Customization >> Password Policies** and customize password polices as per your requirement.

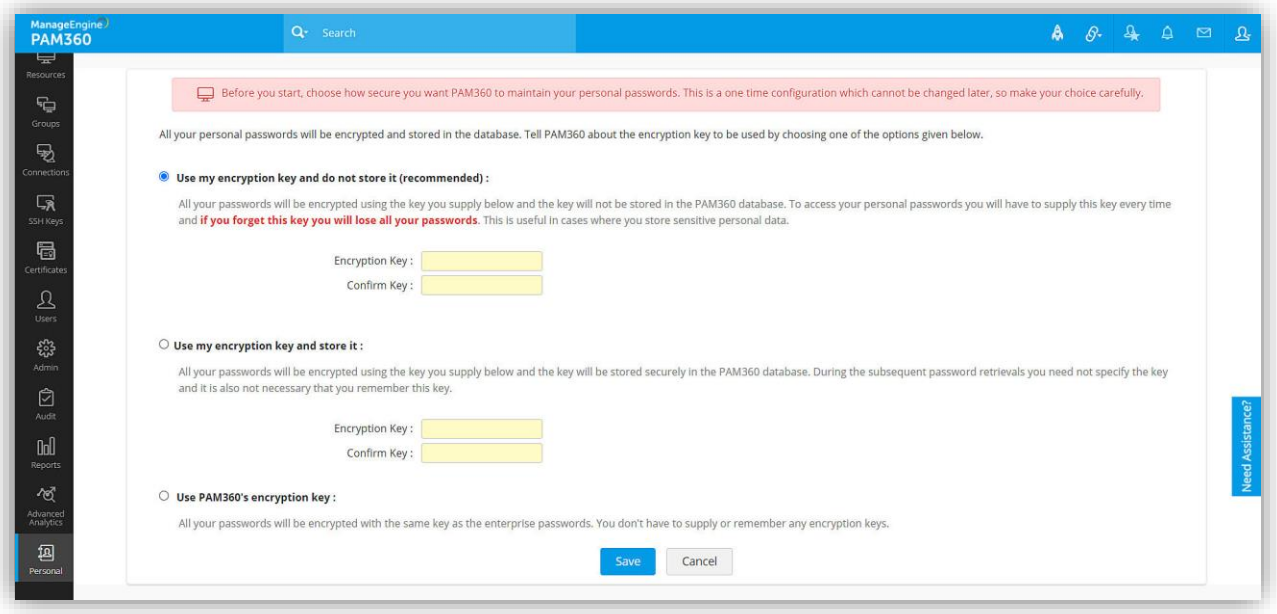
Follow the below steps to set an encryption passphrase for your **Personal** tab:

1. Navigate to the **Personal** tab.
2. Enter a complex passphrase. Click the tool-tip icon for the passphrase complexity rules.
3. Enter your passphrase again to confirm it and click **Save**.



PAM360 will use this passphrase to encrypt your data. Ensure that the passphrase you create is long and obeys the complexity rules for enhanced security. Whenever you need to access personal passwords in the **Personal** tab, you need to supply this passphrase. Remember, if you forget your passphrase, there is no way to retrieve your personal data.

If the administrator disables the option that allows user to choose their own passphrase for the personal passwords section, PAM360 provides options to choose an encryption method for securing the data stored in the **Personal** tab. Please note that all your personal passwords will be encrypted and stored in the database. PAM360 will encrypt your personal data based on the encryption key you choose to use based on the options given below:



Option 1: Use my encryption key and do not store it: If you choose this option, all your passwords will be encrypted using the encryption key you set up below. Note that this key will not be stored in the PAM360 database. To access your personal passwords you will have to supply this key every time and if you forget this key you will lose all your passwords. This is the recommended option for achieving a high level of security for your sensitive personal data. In choosing not to store the encryption key, the risk of it getting exposed and compromising your passwords is significantly low.

Option 2: Use my encryption key and store it: If you choose this option, all your passwords will be encrypted using the key you supply below and the key will be stored securely in the PAM360 database. During the subsequent password retrievals you need not specify the key and it is also not necessary that you remember this key.

Option 3: Use PAM360's encryption key: All your passwords will be encrypted with the same key as the enterprise passwords. You don't have to supply or remember any encryption keys.

Choose the required encryption method, enter your encryption passphrase and click **Save** to save the changes.

2. Storing Personal Accounts

Once you have set your passphrase, proceed with adding your personal accounts in the **Personal** tab in the default categories provided by PAM360. The default categories cannot be

deleted. However, there is also provision to add your own custom categories, which is discussed in the next section of the document.

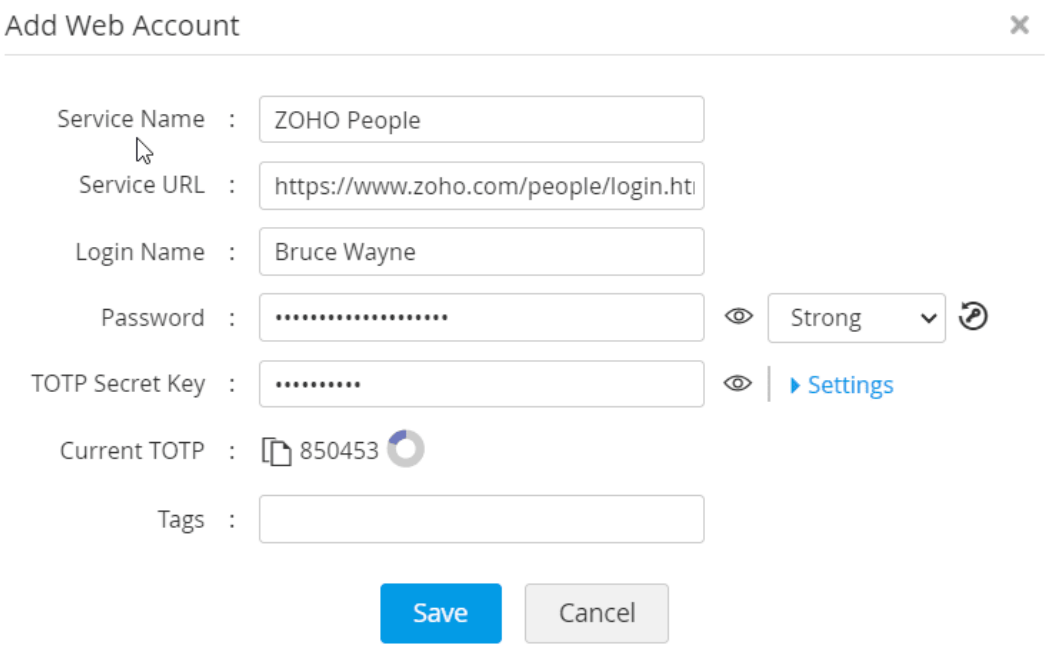
The four default categories of accounts are:

1. Web accounts
2. Bank accounts
3. Credit card accounts
4. Personal contacts list

2.1 Web Accounts

To add a new web account, follow the below steps:

1. Navigate to the **Personal** tab.
2. Click the **Web Accounts** option from the left pane.
3. In the **Web Accounts** page, click the **Add Accounts.**
4. In the **Add Web Account** pop-up that appears, enter the following attributes:
    i. **Service Name**: Enter the name of the web service.
    ii. **Service URL**: Enter the URL.

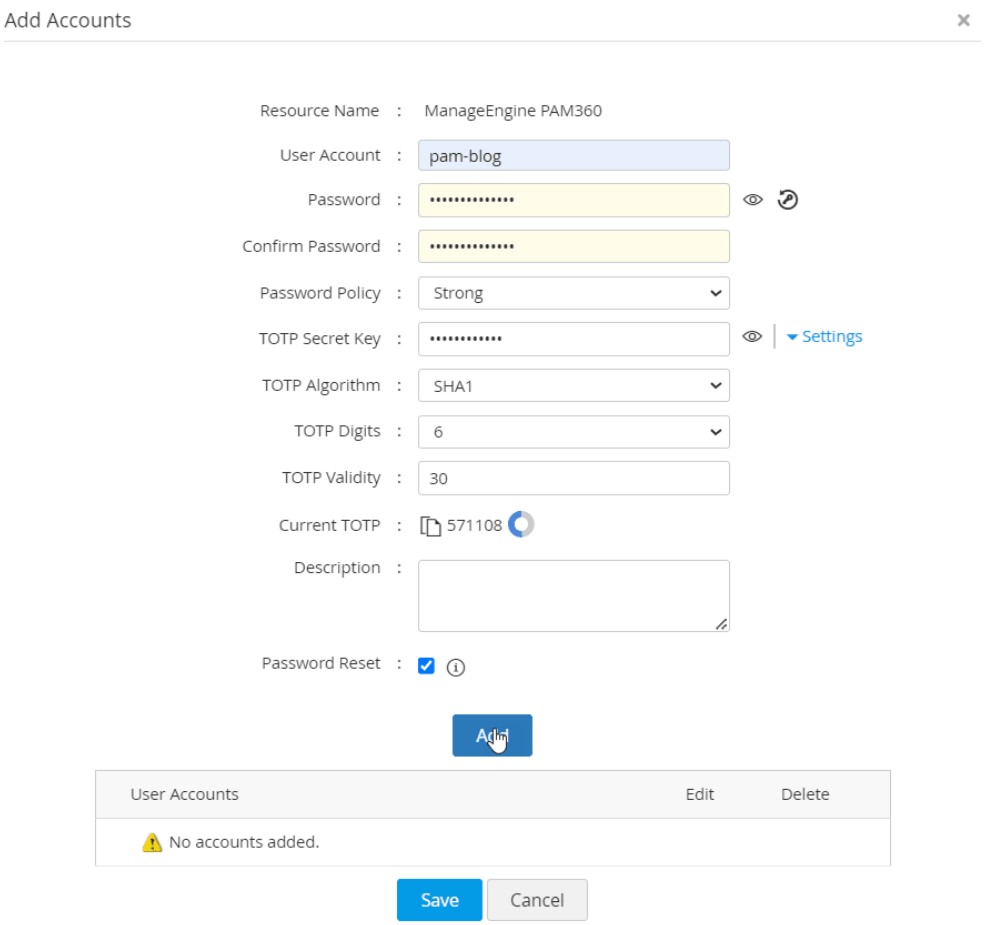


    iii. **Login Name**: Enter the login name of the web account.
    iv. **Password:** Enter the password of the account. Also, choose a complexity from the

dropdown.

v. **TOTP Secret Key:** If your web account is enabled with TOTP as the Two-Factor Authentication (2FA), input the **TOTP Secret Key**. This allows you further to directly access the account through the PAM360 interface, streamlining the generation of TOTP one-time codes alongside the added passwords.

- By default, the website accounts configured with TOTP as the 2FA supports the SHA1 Algorithm, 6-digit TOTP codes, and a validity of 30 seconds. If your account supports a different set of parameters for TOTP codes, please select the appropriate **TOTP Algorithm** and **TOTP Digits** and enter the **TOTP Validity** in seconds by clicking upon the **Settings** dropdown beside the **TOTP Secret Key** field.



> Note that if the TOTP Algorithm, TOTP Digits, and TOTP validity differ between the account and the values entered here, the authentication mechanism will not work as expected due to generation of incorrect one-time codes. Also, once configured, the TOTP secret key cannot be retrieved again for the account. Therefore, exercise caution to ensure that the values entered or selected here match those values supported by the account.

vi. **Tags:** Enter keywords that can be used to search for the account in the **Web Accounts** page.

5. Click **Save**.

2.2 Banking Accounts

To add a new banking account, follow the below steps:

1. Navigate to the **Personal** tab.
2. Click the **Banking** option from the left pane.
3. In the **Banking** page, click the **Add Accounts.**
4. In the **Add Bank Account** pop-up that appears, enter the attributes such as Bank name, Account number, Branch name, etc. Leave the unwanted fields blank.
5. Click **Save**.

2.3 Credit Card Accounts

To add a new credit card account, follow the below steps:

1. Navigate to the **Personal** tab.
2. Click the **Credit Cards** option from the left pane.
3. In the **Credit Cards** page, click the **Add Accounts.**
4. In the **Add Credit Card Account** pop-up that appears, enter the attributes such as Card name, Card Number, PIN, Phone number, etc. Leave the unwanted fields blank.

5. Click **Save**.

2.4 Personal Contacts

To add a new contact, follow the below steps:

1. Navigate to the **Personal** tab.
2. Click the **Contacts** option from the left pane.
3. In the **Contacts** page, click the **Add Contact.**
4. In the **Add Contact** pop-up, enter the attributes such as Contact name, Email Address, etc.
5. Click **Save**.

2.5 Deleting Accounts

To delete any of the accounts, go to the respective accounts page,

1. Navigate to the **Personal** tab.
2. Click a category of accounts from the left pane.
3. Select the required accounts using the check-boxes and click the **Delete Accounts** option at the top.
4. Click **OK** in the confirmation dialog box to complete the delete operation.

> **Note:** Once you delete accounts, they will be deleted from the database once and for all and cannot be recovered.

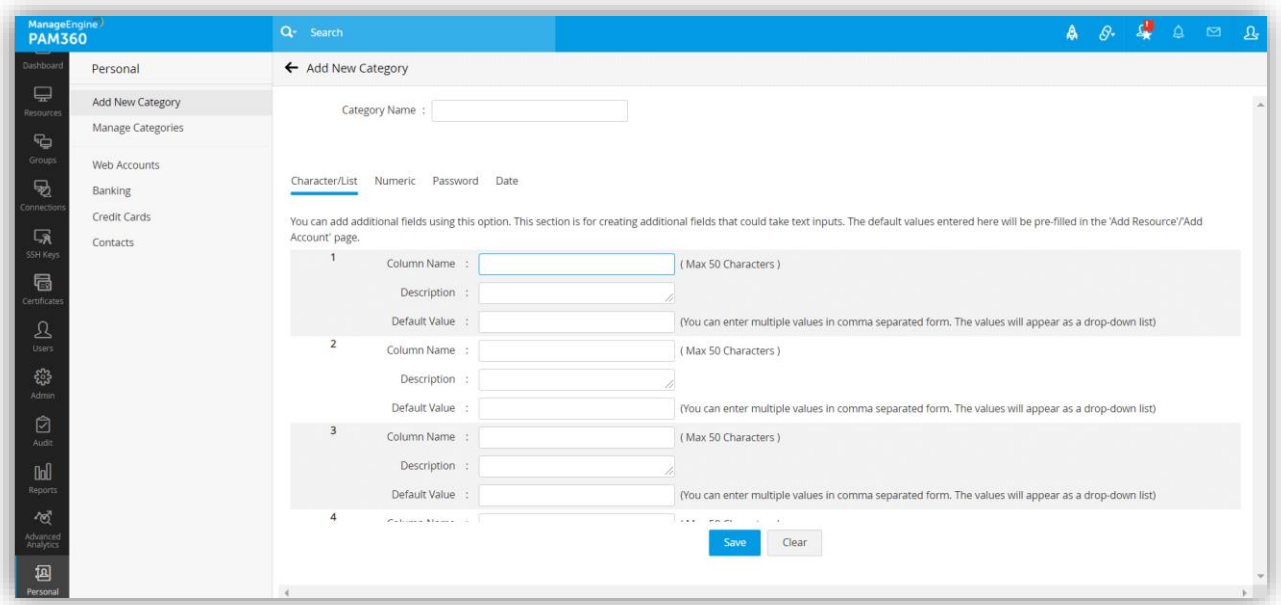
3. Adding Custom Fields

In addition to the default categories, add any number of additional custom fields to your **Personal** tab to store other information. For instance, if you wish to store details about the properties owned by you, add a custom category named **Properties**.

3.1 Creating Custom Categories

Follow the steps below to add a custom field:

1. Click **Add New Category** from the left pane.
2. Enter a category name in the text field. Your custom fields can be in any of the following four formats - **Character/List**, **Numeric**, **Password**, **Date**. Add attributes such as column name, description, and default value.
3. You can add a maximum of nine **Character/List** fields, four **Numeric** fields, three **Password** fields, and four **Date** fields. Click **Save** to add the custom field as a new category next to the default ones. Remember, once added, custom fields cannot be deleted.

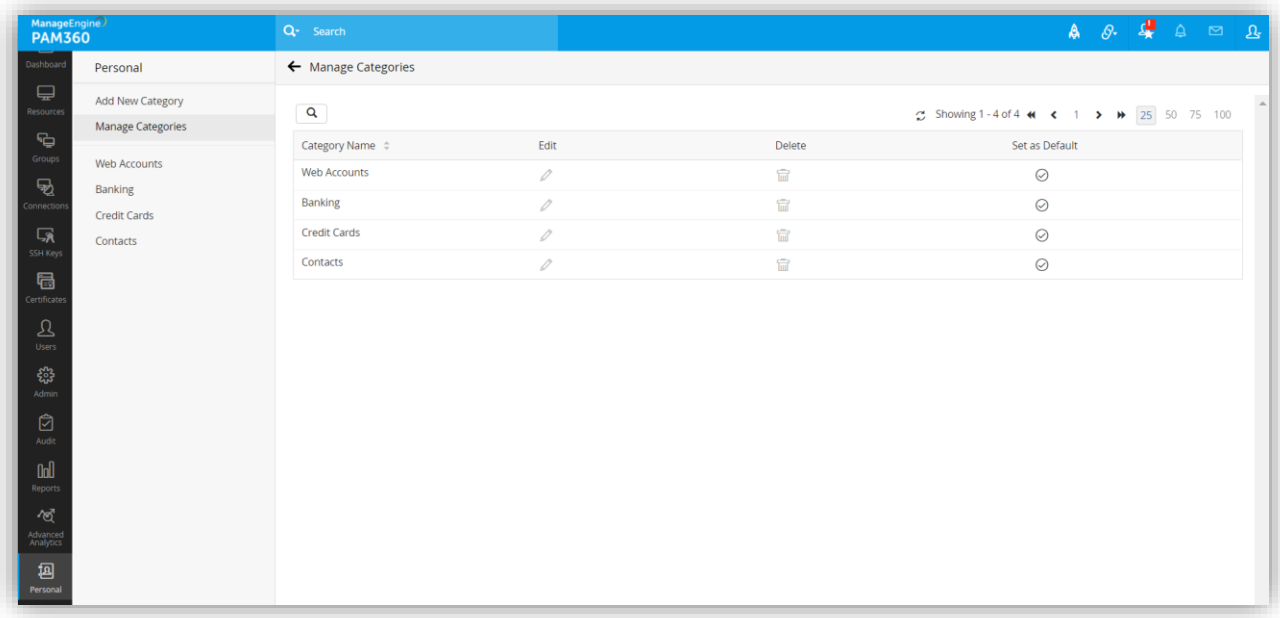


3.2 Managing Custom Categories

If any of the custom categories are no longer required, delete them in the **Manage Categories** page. Once you delete the categories, they will be deleted from the database once and for all. So, exercise care before deleting. You can also edit the custom categories.

To manage a custom category,

1. Go to **Personal** Tab
2. Click the link **Manage Categories** present in the left side of the web-interface.
3. If you want to edit a custom category, click the **Edit** icon present against the required custom category.
4. If you want to delete a custom category, click the **Delete** icon present against the required custom category.



4. Managing Passwords in Bulk

Import and export passwords added to the **Personal** tab in bulk. Click here to view file samples and learn more about file formats supported for importing. The data from the imported file will autofill the fields matching the column names. You can also choose which field in the imported file should map to the attributes of the corresponding personal category.

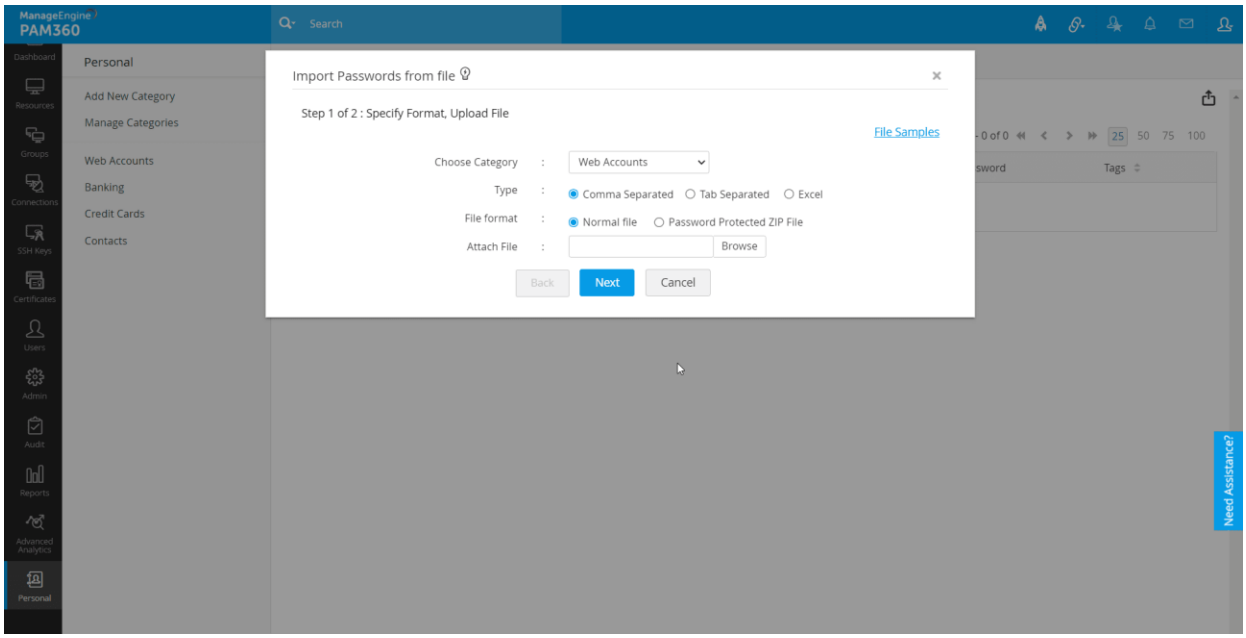
Note: Earlier, it was possible to import a .txt file containing comma-separated data, and in step 2, the data would be listed as expected. However, from build 6400 onwards, if the entries are comma-separated, the file format must be .csv. Files with tab-separated values should be saved as .txt or .tsv for importing.

4.1 Importing Passwords

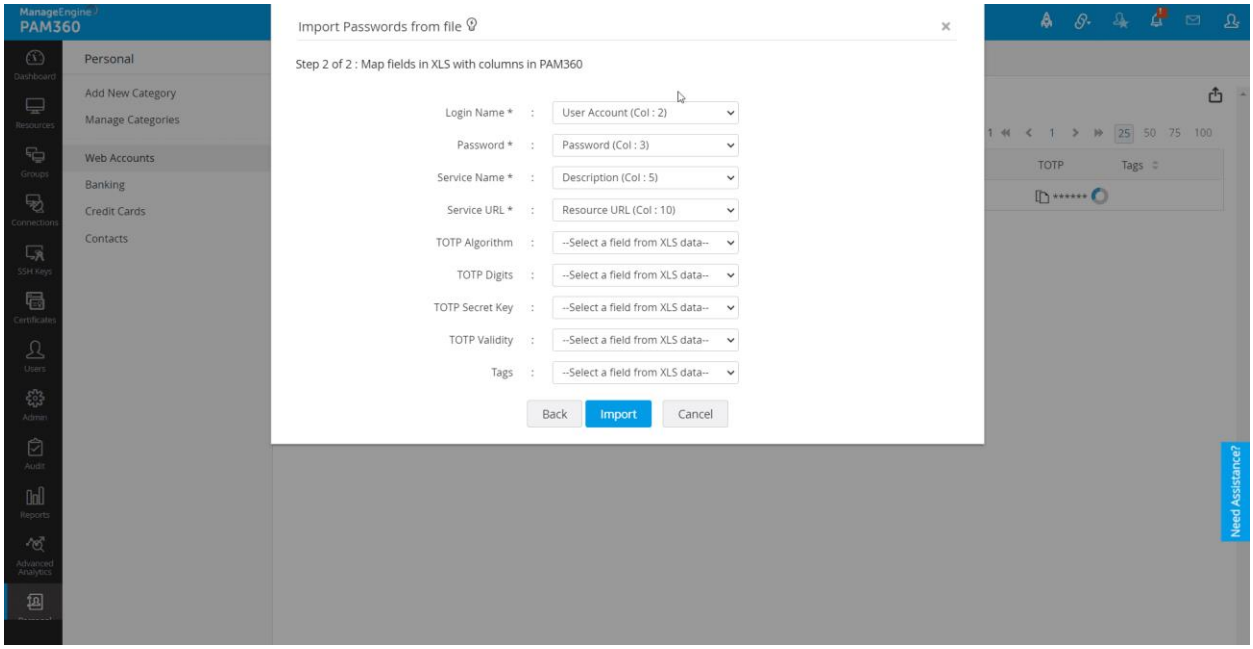
Follow the below steps to import passwords:

1. Navigate to **Personal** tab.
2. Click the **Import Passwords** option.

3. In the pop-up form that appears, choose the category.
4. Select the file type and file format.
5. Click **Browse** and select the file to import passwords.



6. Click **Next** and map the fields accordingly with the data available in the attached file.
7. Click **Import** to complete the import process.

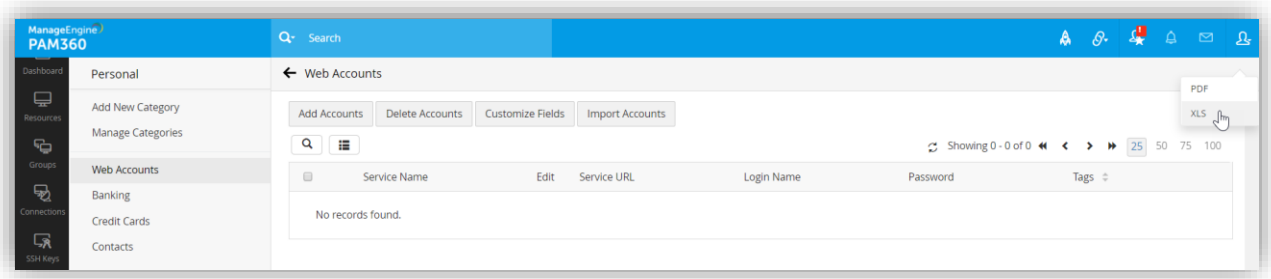


4.2 Exporting Passwords

Export personal passwords in PDF or XLS format using the Export option.

1. Navigate to **Personal** tab.

2. Click the Export icon ( ) present in the top right corner.
3. Select **PDF or XLS** format based on your preference. The passwords are exported in a PDF or XLS file based on your selection and saved to your local machine.



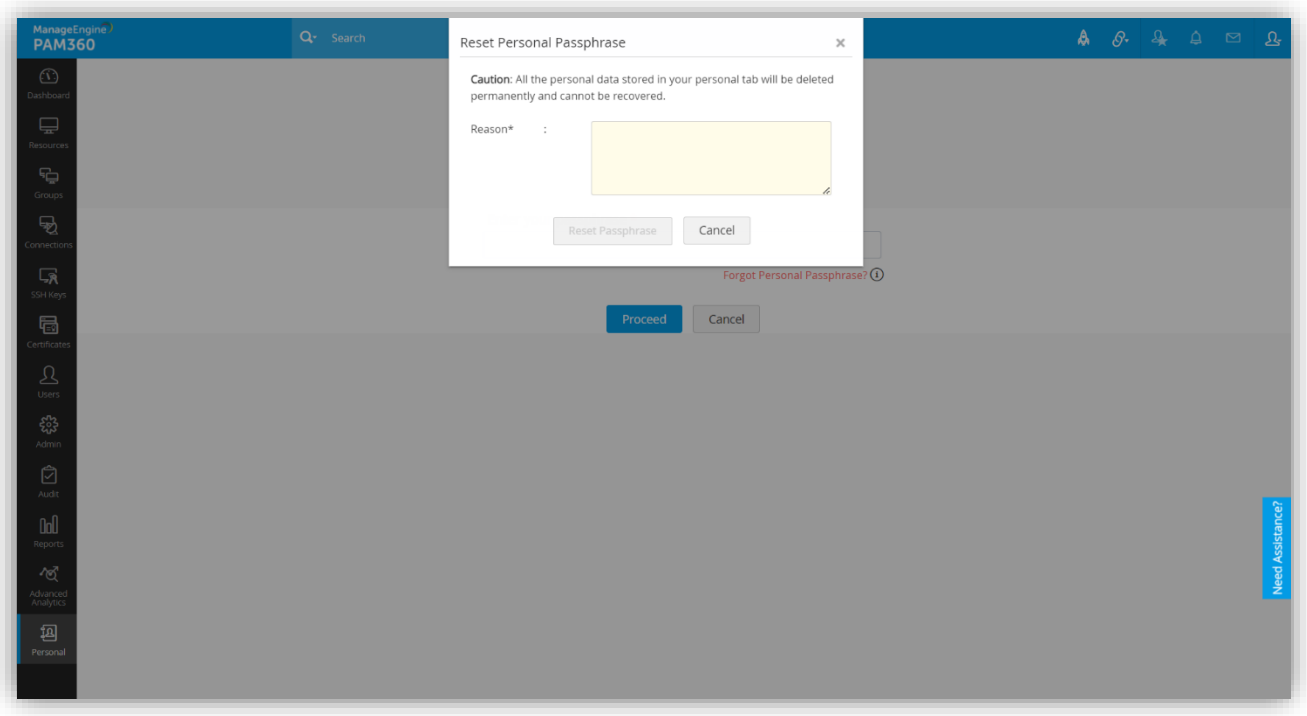
5. Reset Personal Passphrase

(Reset personal passphrase feature is applicable from build 6000)

PAM360 allows you to reset the personal passphrase of the Personal tab. Do the steps that follow for the reset procedure:

> **Note:** Resetting personal passphrase will delete all the data stored in the Personal tab permanently.

1. Navigate to the **Personal** tab and click **Forgot Personal Passphrase?**
2. In the pop-up that appears, enter a **Reason** for the passphrase reset and click **Reset Passphrase**.



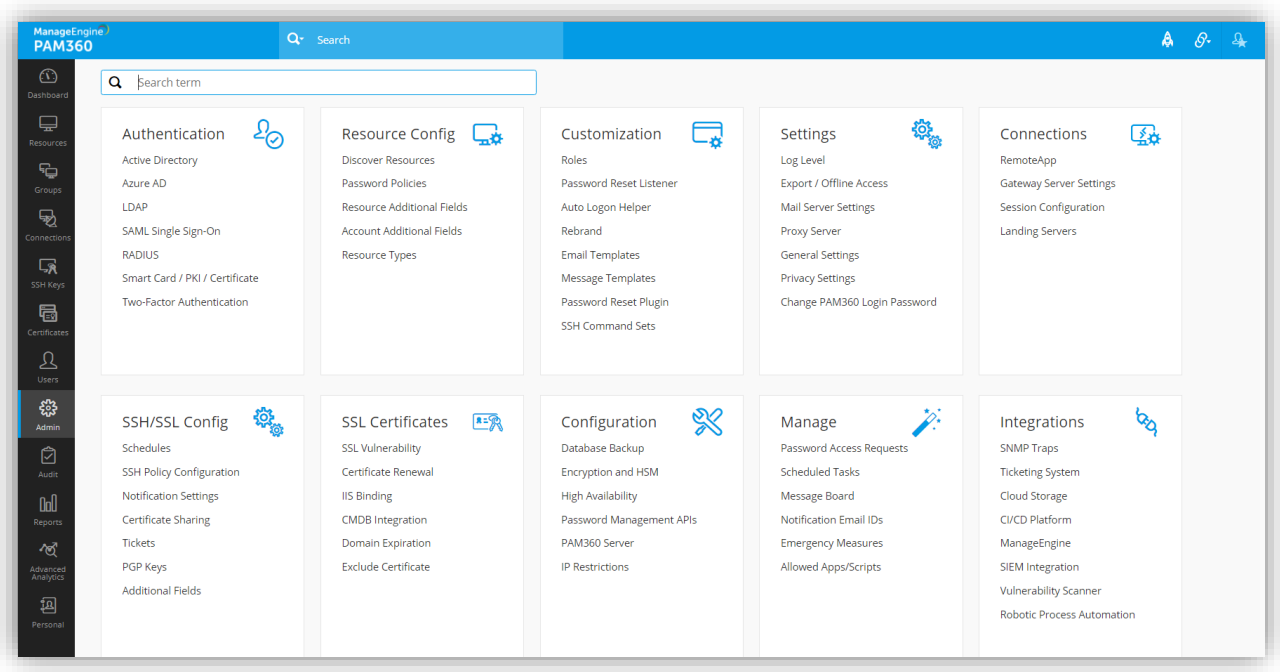
3. Now, you have successfully reset the personal passphrase of the **Personal** tab.

Changing PAM360 Login Password

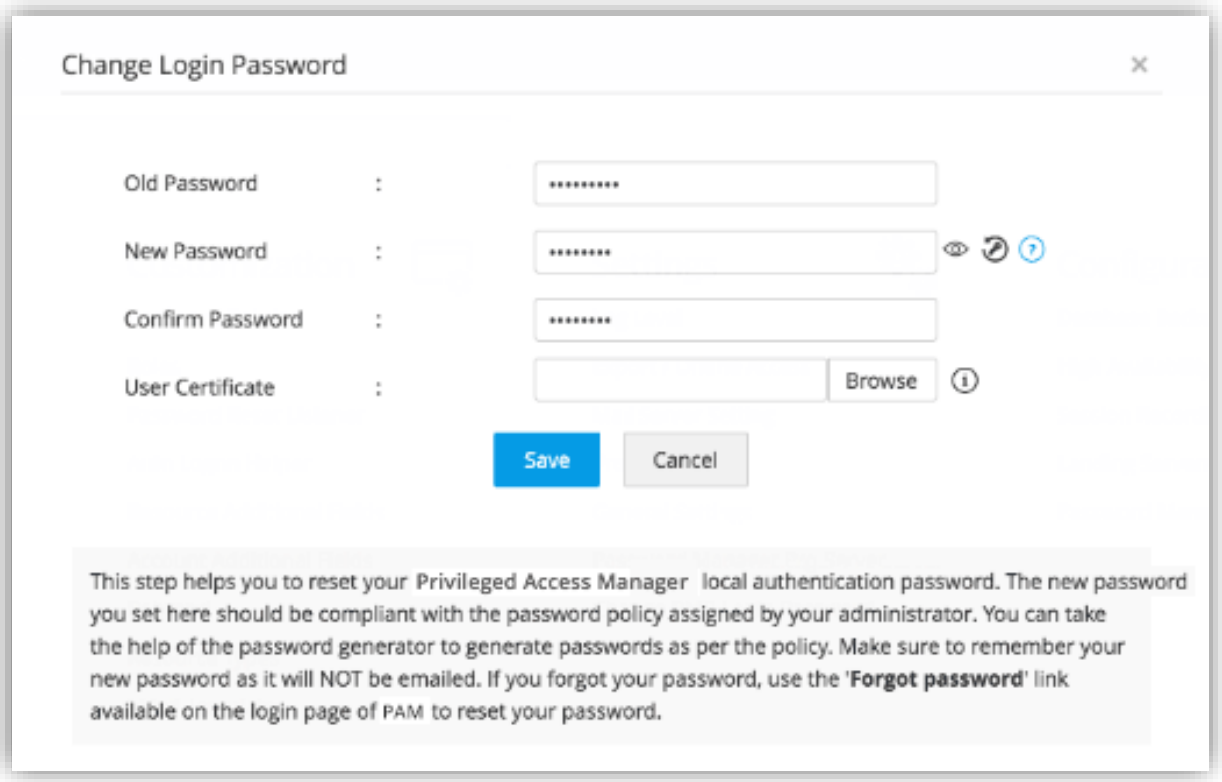
Users having an account with the PAM360, can change their own password.

Steps Required

1. Navigate to **Admin >> Settings >> Change Login Password**.



2. In the dialog box that opens,
   i. Enter the **Old Password.**
   ii. Enter the **New Password.** The new password you provide will have to be compliant to the password policy assigned to your account by your administrator. Alternatively, you can also use the built-in password generator to generate passwords according to the assigned policy.
   iii. Confirm your new password.
   iv. **Browse** and select the **User Certificate** for smartcard/PKI/Certificate authentication.
   v. Click **Save**.



3. Now you have successfully reset your Password.

Advanced Analytics

PAM360 offers robust, native integrations with state-of-the-art data analytics tools to help you manage and automatically analyze account activity from your privileged resources. This document provides detailed information on which data analytics applications you can integrate with PAM360 and how you can view and interpret the data from the **Advanced Analytics** module.

At the end of this document, you will have learned the following:

1. Benefits of the Advanced Analytics Module
2. How does the Integration Work?
3. How to Activate Advanced Analytics in PAM360?
4. Data Analytics Tools Integrated with PAM360
5. Viewing Advanced Analytics in PAM360
   5.1 ManageEngine Analytics Plus
   5.2 ManageEngine Log360 UEBA

1. Benefits of the Advanced Analytics Module

Use the Advanced Analytics tab to:

- Spot unusual user behavior and gain insights to identify security threats.
- Intelligently monitor historical audit logs for malicious account activities.
- Use Zia, the analytics assistant powered by machine learning, to help identify sources of anomalies.
- Blend data from several sources and PAM360 modules to get unified insights for better visibility.
- Get notified of suspicious activity when pre-configured thresholds are breached.
- Email, export, publish, and share key findings through secure sharing options.

The scope and benefits of integration differ based on the product integrated and its functionalities. Still, the basic idea behind the integration is to manage shared sensitive information from PAM360. Read further to learn how the integration works for each product.

2. How does the Integration Work?

When you integrate PAM360 with a data analytics tool, PAM360 consolidates all of the resource and user audit logs recorded here and sends them to the analytics tool of your choice. The audit data is interpreted and visualized in the form of Dashboards and displayed in the **Advanced Analytics** tab.

3. How to Activate Advanced Analytics in PAM360?

To activate Advanced Analytics for your PAM360 instance, you need a working license for any one of the data analytics applications listed below. If you already have a license, click the name of the application to learn how to set up the dashboard. For further queries, please write to us at pam360-support@manageengine.com.

4. Data Analytics Tools Integrated with PAM360

PAM360 integrates with the below products:

1. **ManageEngine Analytics Plus**
2. **ManageEngine Log360 UEBA**

Refer to the respective help section to learn how to integrate the product with PAM360.

5. Viewing Advanced Analytics in PAM360

Once the integration is complete, follow the below steps to view your data dashboards in Advanced Analytics:

1. Login to PAM360 and click the **Advanced Analytics** tab.
2. In this page, you will see dashboards from both ManageEngine Analytics Plus and ManageEngine Log360 UEBA, if you have integrated both the products with PAM360. The data will be segregated here the same way it appears in the Analytics Plus and Log360 UEBA servers respectively.

5.1 ManageEngine Analytics Plus

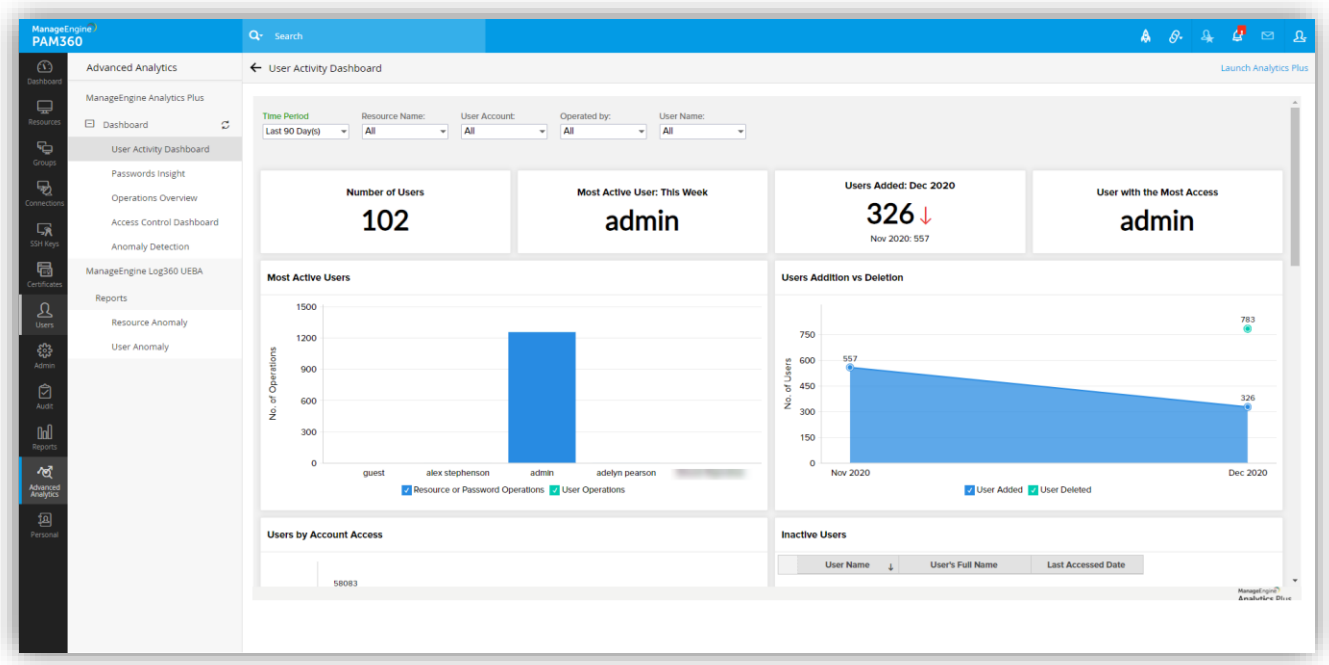
1. The **Dashboard** menu in the left pane displays different types of dashboards based on the data already imported to Analytics Plus from PAM360. Click each dashboard type to view the corresponding data in the display area on the right.
2. The data displayed here depends on the following:
   i. The modules you had already imported to Analytics Plus from PAM360.
   ii. The time period you had chosen to import data from PAM360.
   iii. The data import schedule you had chosen in Analytics Plus during the integration.

Click the **Launch Analytics Plus** link if you wish to switch over to the Analytics Plus portal.

Advanced Analytics View in PAM360

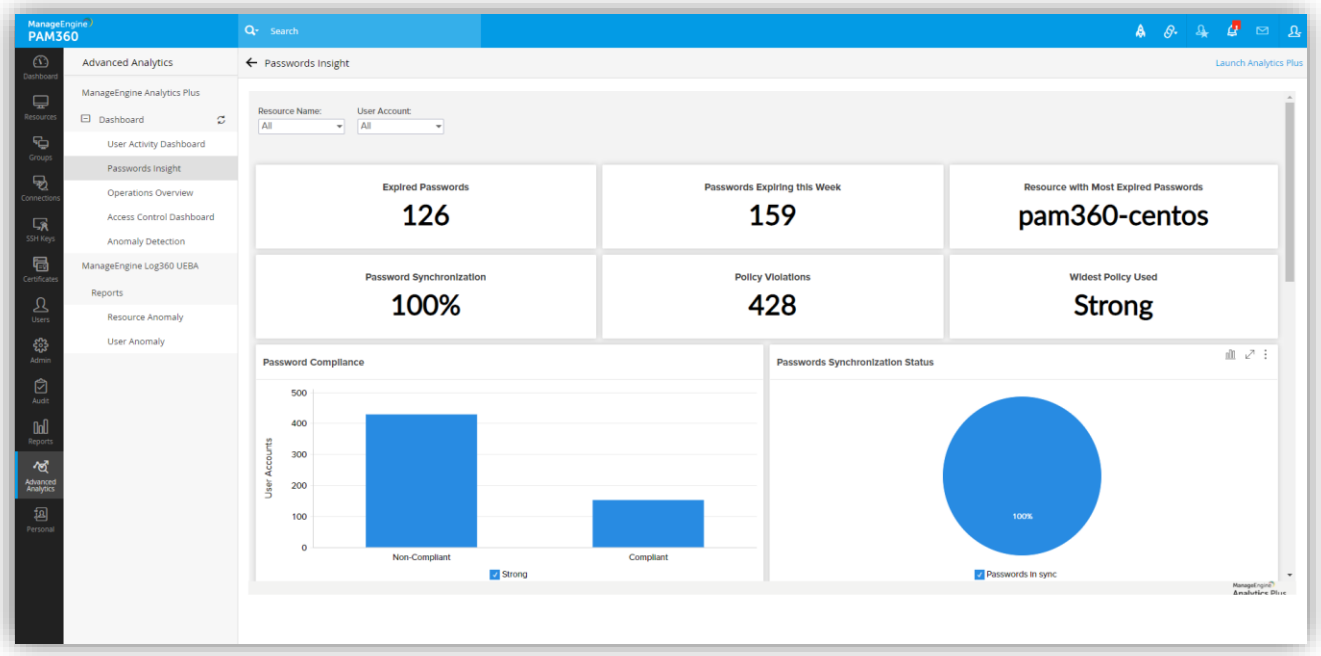
5.1.1 User Activity Dashboard

The User Activity Dashboard gives you all possible data related to user activity in your PAM360 environment. Use the **User Account, Resource Name**, and **Time Period** filters to refine the dashboard view. At a glance, you can view details such as the number of users who have accessed a particular resource/account in a particular time period, most active user, number of users added within the selected time period, and the user who has the highest level access. Analytics Plus segregates user activity into various divisions and renders them as graphs for easy interpretation. Scroll down to view all the available graphs.



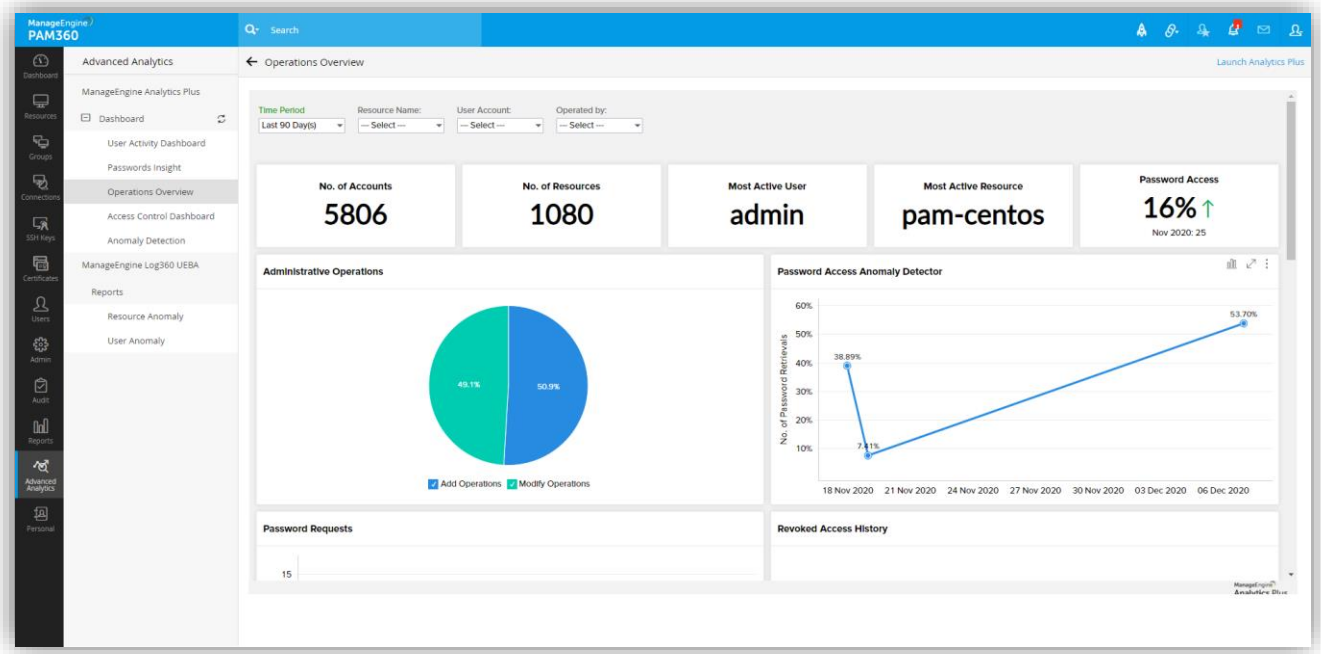
5.1.2 Passwords Insight

The Passwords Insight dashboard gives all data related to the passwords saved in PAM360 that are owned and managed by you. Use the **Resource Name** and **Account Name** filters to refine the dashboard view. At a glance, you can view the number of expired passwords, the number of passwords expiring this week, and the name of the resource with the most expired passwords. Along with the above, the dashboard also displays the synchronization percentage of the passwords, the widely used password policy, and the number of policy violations. Similar to other dashboards, Analytics Plus segregates password insights into various sections and renders them as graphs for easy interpretation. Scroll down to view all the available graphs.



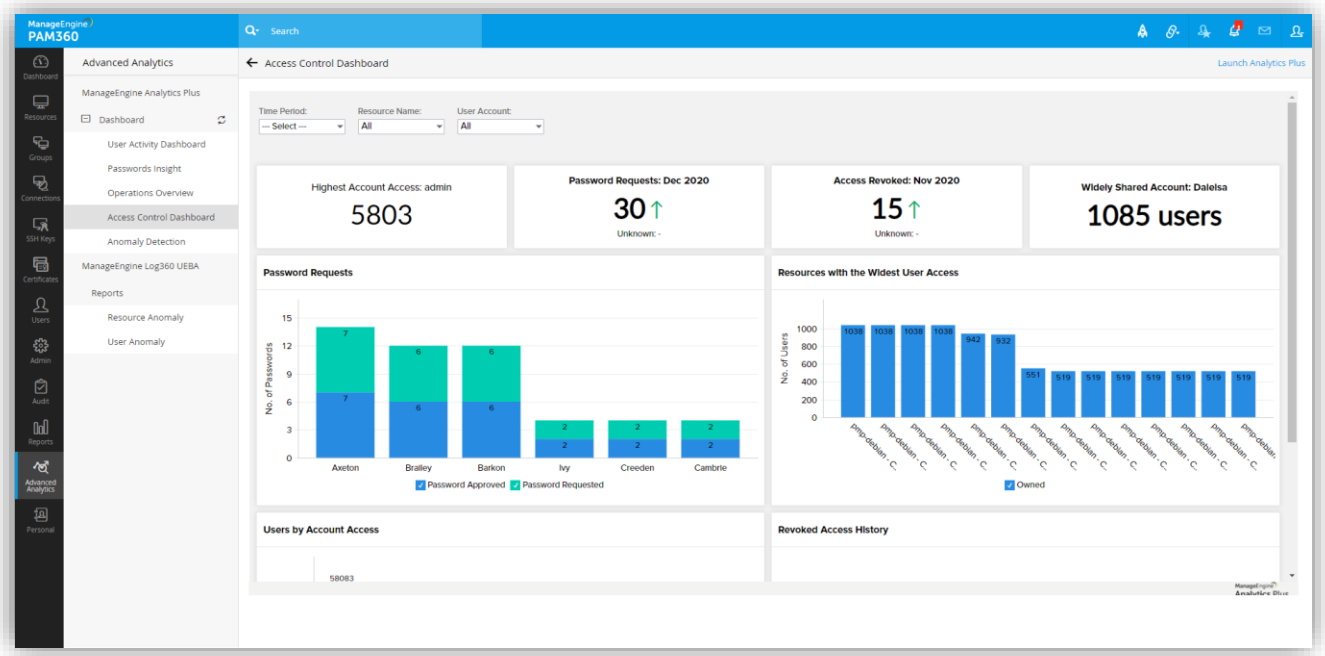
5.1.3 Operations Overview

The Operations Overview dashboard provides a detailed overview of the resource and password related operations that were performed within the selected time period. Use the **Resource Name, Account Name,** and **Time Period** filters to refine the dashboard view. At a glance, it gives you details such as the number of resources and accounts present, the most active user, the most active resource, and the password access percentage. Similar to other dashboards, Analytics Plus segregates operation details into various sections and renders them as graphs for easy interpretation. Scroll down to view all the available graphs.



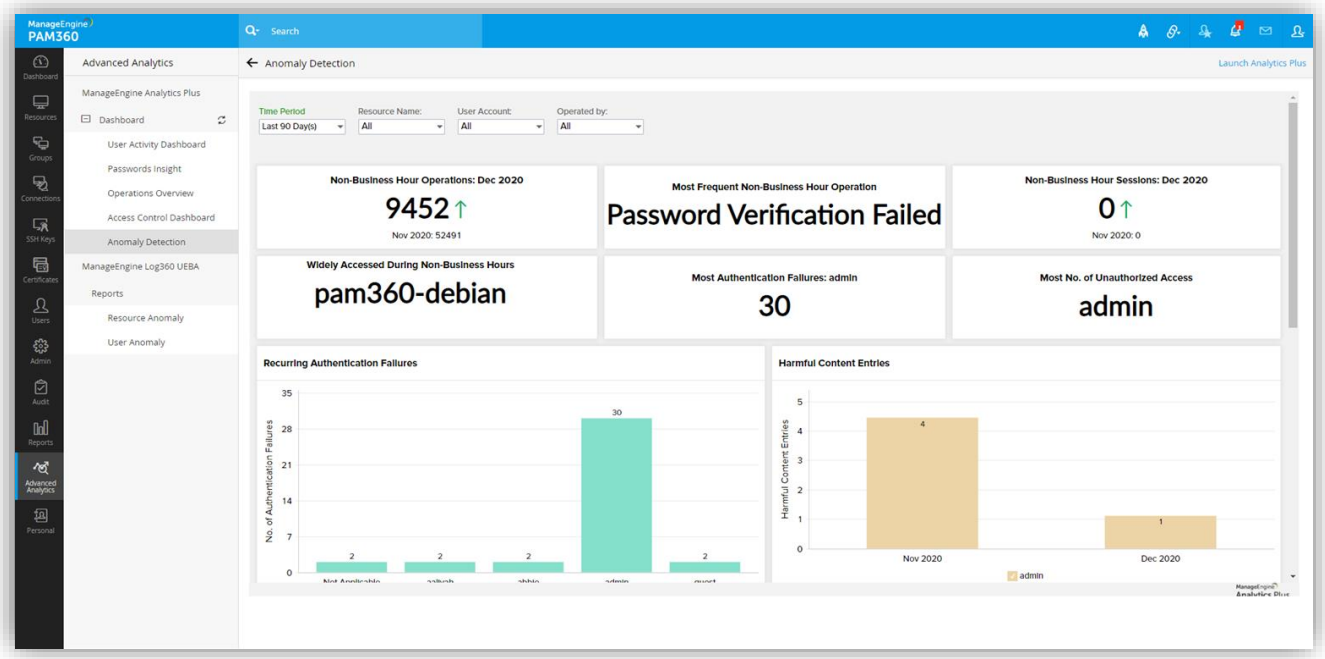
5.1.4 Access Control Dashboard

The Access Control Dashboard provides you details about the resource and password related operations that were performed within the selected time period. Use the **Resource Name, Account Name,** and **Time Period** filters to refine the dashboard view. At a glance, it gives you details such as the user who has access to the most number of accounts, the name of the account which is widely shared, and the total number of password requests, and the number of requests revoked for the selected time period. Similar to other dashboards, Analytics Plus segregates access control details into various sections and renders them as graphs for easy interpretation. Scroll down to view all the available graphs.



5.1.5 Anomaly Detection

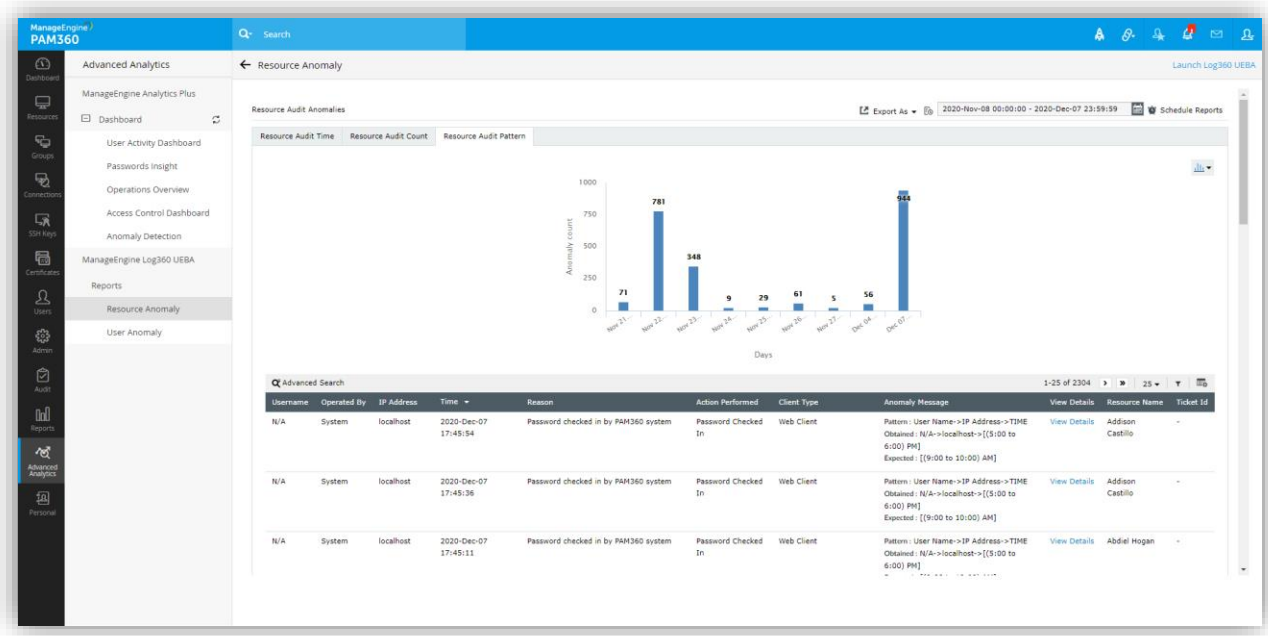
The Anomaly Detection dashboard provides you details about any anomalous activities that may have taken place within the selected time period. Use the **Resource Name, Account Name,** and **Time Period** filters to refine the dashboard view. At a glance, it gives you details such as the number of operations performed in non-business hours, the most frequent non-business hour operation, the number of user sessions carried out during non-business hours, the name of the account that was widely accessed during non-business hours, the user who had the most number of authentication failures, and the user who performed the most number of unauthorized access. Similar to other dashboards, Analytics Plus segregates access control details into various sections and renders them as graphs for easy interpretation. Scroll down to view all the available graphs.

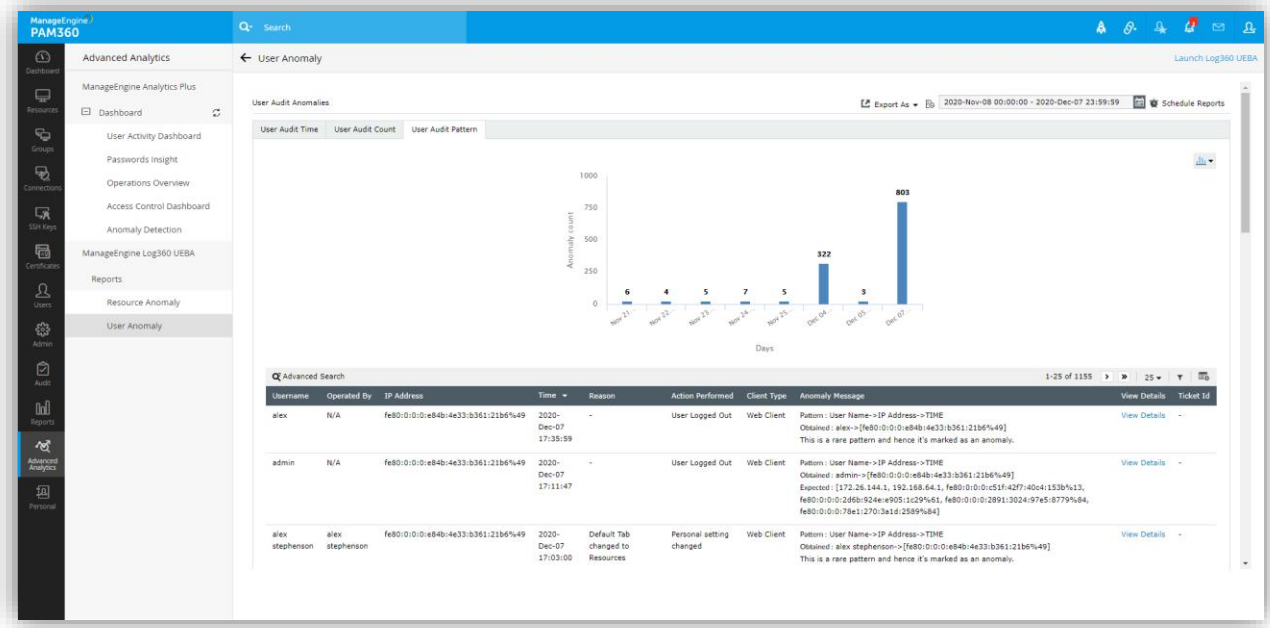


5.2 ManageEngine Log360 UEBA

To view analytics data consolidated by ManageEngine Log360 UEBA, choose one of the reports: **Resource Anomaly** or **User Anomaly**. As per your choice, the analysis of resource and user audit reports will be displayed in the dashboard area on the right.

1. Log360 UEBA segregates resource and user audit trails from PAM360 and renders the data in three ways:
    i. **Audit Time** - The time at which user activity is detected.
    ii. **Audit Count** - The number of times a user activity is detected.
    iii. **Audit Pattern** - Based on the Audit Time and Audit Count, Log360 UEBA generates patterns for user behavior.
2. Through a score-based risk assessment, Log360 UEBA marks any activity that strays from the normal pattern as an anomaly in the **Anomaly Reports**. Log360 UEBA provides an option to visualize the **Anomaly Reports** in the form of bar graphs and pie charts.
3. Click the **Export As** option in the top right corner to export the report that is currently displayed. You can export reports in four formats namely: **CSV, PDF, XLS,** and **HTML**.
4. To schedule the generation of reports, click the **Schedule Reports** option. Please note that the report schedules set in the Log360 UEBA dashboard and the **Reports** tab of PAM360 are independent of each other.


ManageEngine PAM360
Search
Advanced Analytics
Resource Anomaly
Launch Log360 UEBA
ManageEngine Analytics Plus
Dashboard
User Activity Dashboard
Passwords Insight
Operations Overview
Access Control Dashboard
Anomaly Detection
ManageEngine Log360 UEBA
Reports
Resource Anomaly
User Anomaly
Resource Audit Anomalies
Export As
2020-Nov-08 00:00:00 - 2020-Dec-07 23:59:59
Schedule Reports
Resource Audit Time
Resource Audit Count
Resource Audit Pattern
Anomaly count
Days
71
781
348
9
29
61
5
56
944
Advanced Search
1-25 of 2304
Username
Operated By
IP Address
Time
Reason
Action Performed
Client Type
Anomaly Message
View Details
Resource Name
Ticket Id
N/A
System
localhost
2020-Dec-07 17:45:54
Password checked in by PAM360 system
Password Checked In
Web Client
Pattern : User Name->IP Address->TIME Obtained : N/A->localhost->[(5:00 to 6:00) PM] Expected : [(9:00 to 10:00) AM]
View Details
Addison Castillo
2020-Dec-07 17:45:36
Password checked in by PAM360 system
Password Checked In
Web Client
Pattern : User Name->IP Address->TIME Obtained : N/A->localhost->[(5:00 to 6:00) PM] Expected : [(9:00 to 10:00) AM]
View Details
Addison Castillo
2020-Dec-07 17:45:11
Password checked in by PAM360 system
Password Checked In
Web Client
Pattern : User Name->IP Address->TIME Obtained : N/A->localhost->[(5:00 to 6:00) PM]
View Details
Abdiel Hogan


ManageEngine PAM360
Search
Advanced Analytics
User Anomaly
Launch Log360 UEBA
ManageEngine Analytics Plus
Dashboard
User Activity Dashboard
Passwords Insight
Operations Overview
Access Control Dashboard
Anomaly Detection
ManageEngine Log360 UEBA
Reports
Resource Anomaly
User Anomaly
User Audit Anomalies
Export As
2020-Nov-08 00:00:00 - 2020-Dec-07 23:59:59
Schedule Reports
User Audit Time
User Audit Count
User Audit Pattern
Anomaly count
Days
6
4
5
7
5
322
3
803
Advanced Search
1-25 of 1155
Username
Operated By
IP Address
Time
Reason
Action Performed
Client Type
Anomaly Message
View Details
Ticket Id
alex
N/A
fe80:0:0:0:e84b:4e33:b361:21b6%49
2020-Dec-07 17:35:59
User Logged Out
Web Client
Pattern : User Name->IP Address->TIME Obtained : alex->[fe80:0:0:0:e84b:4e33:b361:21b6%49] This is a rare pattern and hence it's marked as an anomaly.
View Details
admin
N/A
fe80:0:0:0:e84b:4e33:b361:21b6%49
2020-Dec-07 17:11:47
User Logged Out
Web Client
Pattern : User Name->IP Address->TIME Obtained : admin->[fe80:0:0:0:e84b:4e33:b361:21b6%49] Expected : [172.26.144.1, 192.168.64.1, fe80:0:0:0:cc51f:42f7:40c4:153b%13, fe80:0:0:0:2d6b:924e:e905:1c29%61, fe80:0:0:0:2891:3024:97e5:8779%84, fe80:0:0:0:78e1:270:3e1d:2589%84]
View Details
alex stephenson
alex stephenson
fe80:0:0:0:e84b:4e33:b361:21b6%49
2020-Dec-07 17:03:00
Default Tab changed to Resources
Personal setting changed
Web Client
Pattern : User Name->IP Address->TIME Obtained : alex stephenson->[fe80:0:0:0:e84b:4e33:b361:21b6%49] This is a rare pattern and hence it's marked as an anomaly.
View Details

Integrating PAM360 with Enterprise Ticketing Systems

PAM360 comes with the facility to integrate with a wide range of ticketing systems, to automatically validate service requests related to privileged access. The integration ensures only users with a valid ticket ID can access the authorized privileged passwords. This integration also extends to the PAM360 workflow, which helps in granting approvals to password access requests upon automatic validation of corresponding service requests in the ticketing system.

In this section you will learn the following with respect to integrating PAM360 with ticketing systems:

1. How does this Integration work?
2. Ticketing Systems
3. Steps to integrate your Ticketing System with PAM360
4. Ticketing system validation enforcement and exceptions
5. Disabling ticketing system integration
6. Integrating other Ticketing Systems
7. Code Snippet For ServiceNow Custom Implementation
8. Interface Description

1. How does this Integration work?

Once you integrate PAM360 with an Enterprise Ticketing System, users will be required to enter a valid ticket ID for password retrieval or reset and PAM360 will do the following before granting access:

- Validate that the ticket ID entered by the user exists in the ticketing system.
- Verify that the incident connected with the ticket is NOT in the 'Closed' state.
- Verify whether the user is authorized to view that password and thereby access the IT resource.
- Verify for appropriate permissions in the case of password reset attempts.

In addition to verifying the above by default, PAM360 also lets you define custom criteria and validate them with the ticketing system before granting access to the passwords. The entire process is completely audited - which means, privileged actions can be traced using ticket IDs

and password access can be traced using ticket numbers in the ticketing system. In addition, you can generate custom reports on privileged access scenario through the ticket IDs.

2. Ticketing Systems

Integrating PAM360 with your ticketing system is so simple. PAM360 readily integrates with the following:

- ManageEngine ServiceDesk Plus On-Demand (Cloud)
- ServiceDesk Plus MSP
- ServiceDesk Plus
- ServiceNow
- JIRA
- BMC Helix Remedyforce

Apart from the above, you can integrate PAM360 with any other Enterprise Ticketing System.

3. Steps to Integrate your Ticketing System with PAM360

Remember: If your ticketing system is ServiceDesk Plus or ServiceDesk Plus MSP and it is running in the HTTPs mode, the identity of the system needs to be verified through a valid SSL certificate, which has to be imported into the PAM360 certificate store. To do this, follow the below steps:

1. Stop the service.
2. Navigate to the **<PAM360_Installation_Folder>/bin** directory.
3. Execute any of the following:

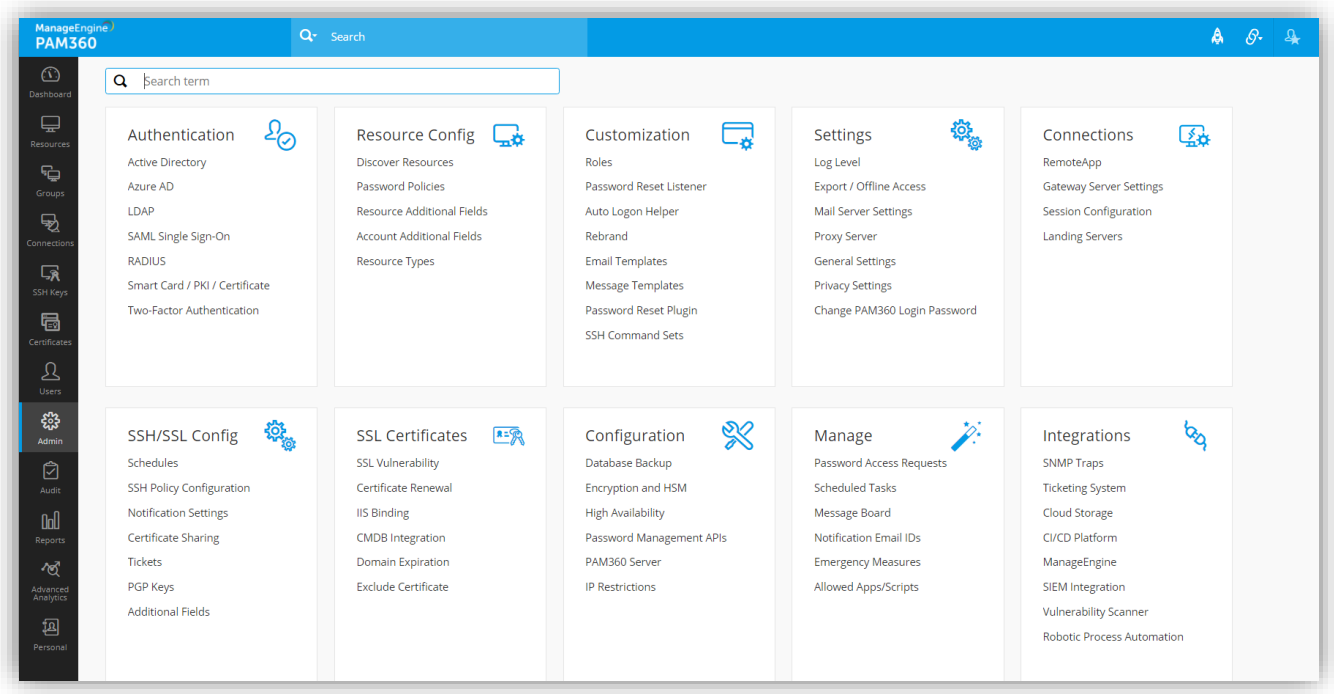
   Windows:

   importCert.bat *<Path of the certificate used by ServiceDesk Plus or ServiceDesk Plus MSP>*

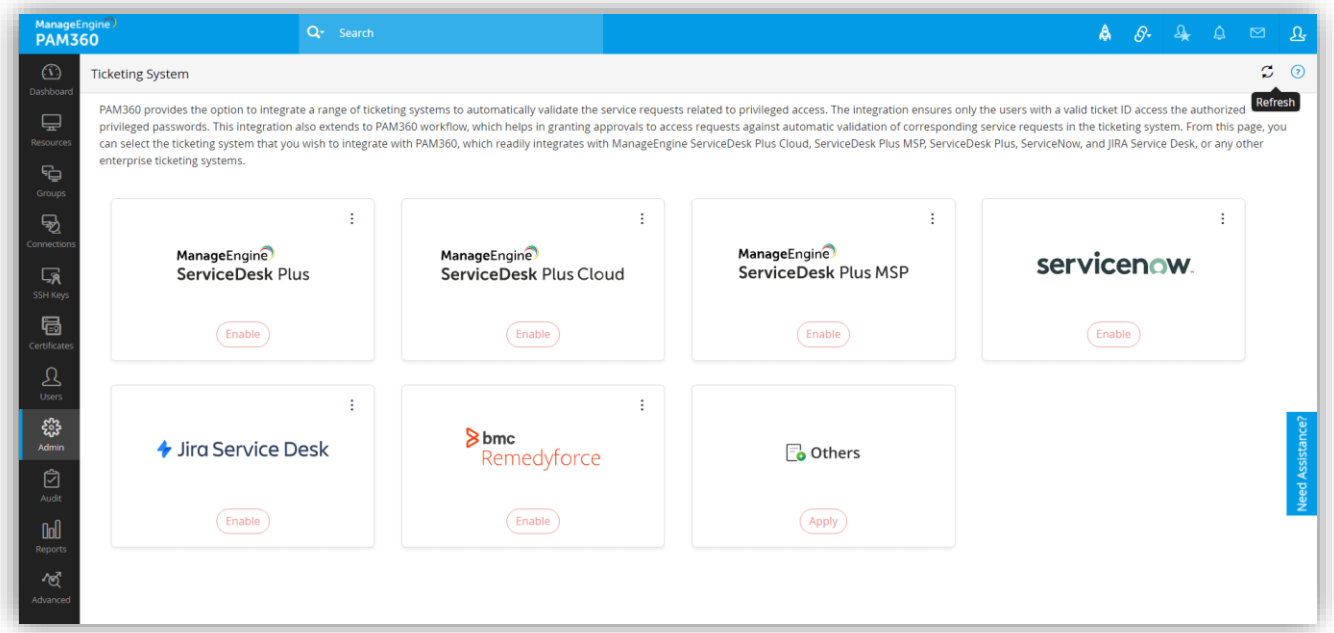
   Linux:

   importCert.sh *<Path of the certificate used by ServiceDesk Plus or ServiceDesk Plus MSP>*
4. Restart the service.

1. Navigate to **Admin >> Integration** >> **Ticketing System Integration**.



2. In the page displayed, select the ticketing system you wish to integrate, from the list of supported ticketing systems. If the ticketing system that you use is not found in the list, select **Others**.

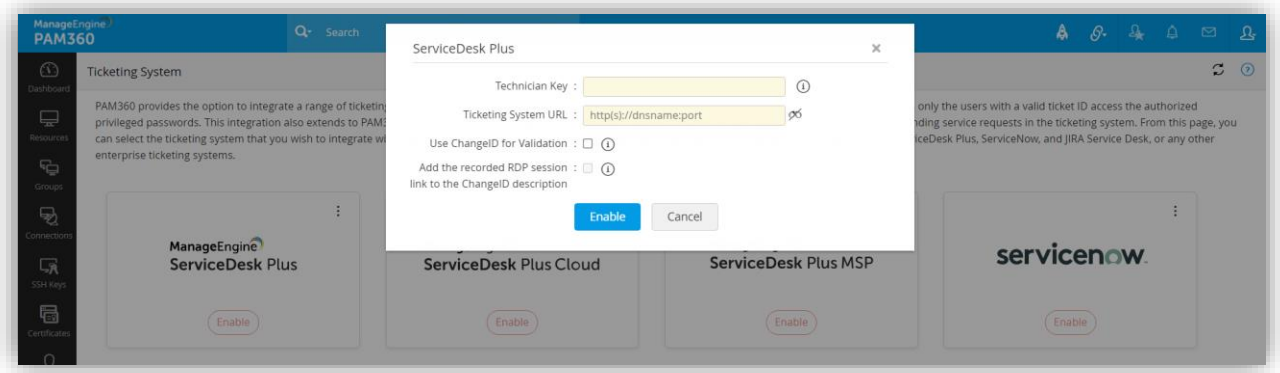


3. Click **Save**.

3.1 Detailed steps to integrate with the Ticketing Systems that are readily supported

Integration with the ticketing systems that are readily supported is very straightforward. You just need to provide the details necessary to establish connection with the ticketing system.

> **Note: Ticketing System URL** should not be entered with a '**/**' at the end (Eg: https://localhost:8080/).



3.2 Settings to Establish Connection with different Ticketing Systems

Basically, the integration is achieved leveraging the REST APIs provided by the respective ticketing system. So, all that you need to do is to specify/generate the Authentication Token and Ticketing System's application URL.

Generating Auth Token:

You can generate and obtain the the Auth Token for each of the ticketing systems as below:

1. ManageEngine ServiceDesk Plus:

i. Log in to ManageEngine ServiceDesk Plus.

ii. Click **API Key Generation** under the Username at the top right corner of the page.

2. ManageEngine ServiceDesk Plus MSP:

i. Log in to ManageEngine ServiceDesk Plus MSP.

ii. Click **API Key Generation** under the Username at the top right corner of the page.

3. ManageEngine ServiceDesk Plus Cloud:

i. Go to Zoho Developer Console.

ii. Choose the **Client Type** as **Server-based Application.**

iii. Enter the following details:

a. **Client Name:**
The name of your application you want to register with ManageEngine ServiceDesk Plus Cloud (PAM360 is advisable).

b. **Home page URL:**
Mention the PAM360 access URL.
Example: *https://<server>:port/* ***(or)*** *https://<domain_name>.com*

c. **Authorized Redirect URIs:**
<homepageurl>/PassTrixMain.cc#/SDPODAuthentication/code/

iv. Click **Create** to generate the following credentials:

a. **Client ID:** The consumer key generated from the connected app.

b. **Client Secret:** The consumer secret generated from the connected app.

4. **ServiceNow:**

i. Log in to PAM360 and navigate to **Admin >> Integration >> Ticketing System.**

ii. Click **ServiceNow.**

iii. Click **Generate** beside the **AUTH Token** field.

iv. Mention the **Username, Password** and click **Proceed.**

5. **JIRA Service Desk:**

i. Go to Atlassian Developer Console.

ii. Click **Create** and select **OAuth 2.0 integration.**

iii. Provide the app **Name** ("**PAM360**" recommended) and click **Create.**

iv. In the UI that appears, click **Permissions** from the left pane.

a. Click **Add** against **Jira API**.

b. Now, click **Configure** against **Jira API.**

c. In the page that appears, under **Jira Service Management API,** click **Edit Scope.**

d. Select **View Jira Service Management request data** and click **Save.**

v. Click **Authorization** from the left pane.

a. Click **Add.**

b. In the UI that appears, mention the **Callback URL** in the below given format and click **Save changes.**

c. **https://<HOSTNAME>:<PORT>/jiraAuth/saveJiraAccessToken**

vi. Click **Settings** from the left pane.

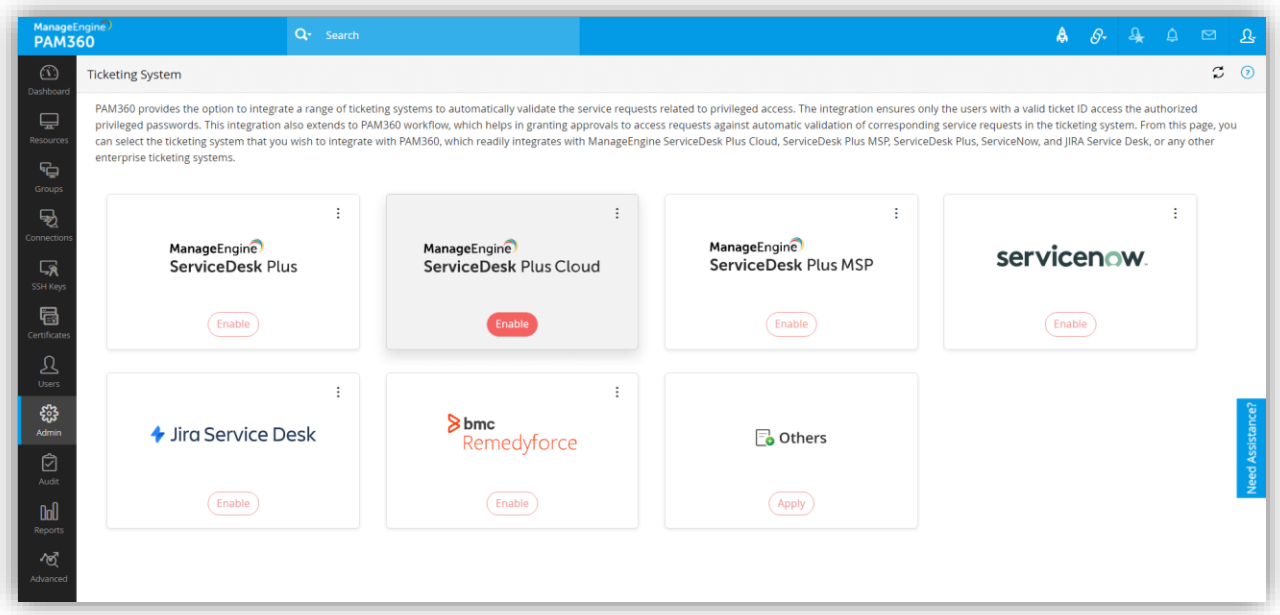
a. Here, you will find the **Client ID** and **Secret.**

3.2.1 ServiceDesk Plus Cloud

PAM360 integrates with ManageEngine ServiceDesk Plus Cloud to automatically validate access request with a valid ticket ID to grant privileged access. This can be done by generating AUTH token and entering the valid ticket ID in the ticketing system. You can also check the value of the change ID status associated with the ticket ID by selecting that option and entering the changeID status.

Configuring ServiceDesk Plus Cloud in PAM360:

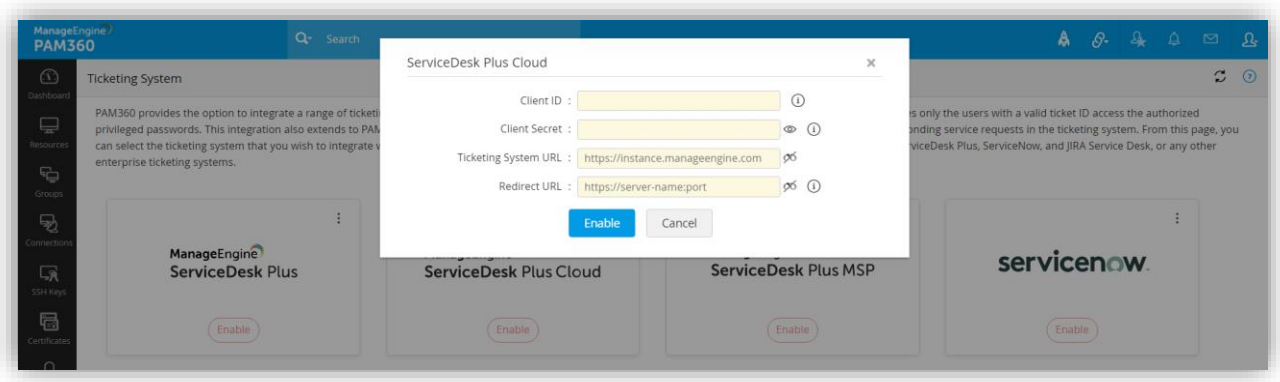
1. Navigate to **Admin >> Integrations >> Ticketing System.**
2. Click **Enable** under **ManageEngine ServiceDesk Plus Cloud.**



3. Now, enter the **Client ID, Client Secret** generated from the previous Auth Token generation step.
4. Mention the **Ticketing System URL** and **Redirect URL.**

> **Note:** Mention the **Home page URL** from the previous step as the **Redirect URL.**

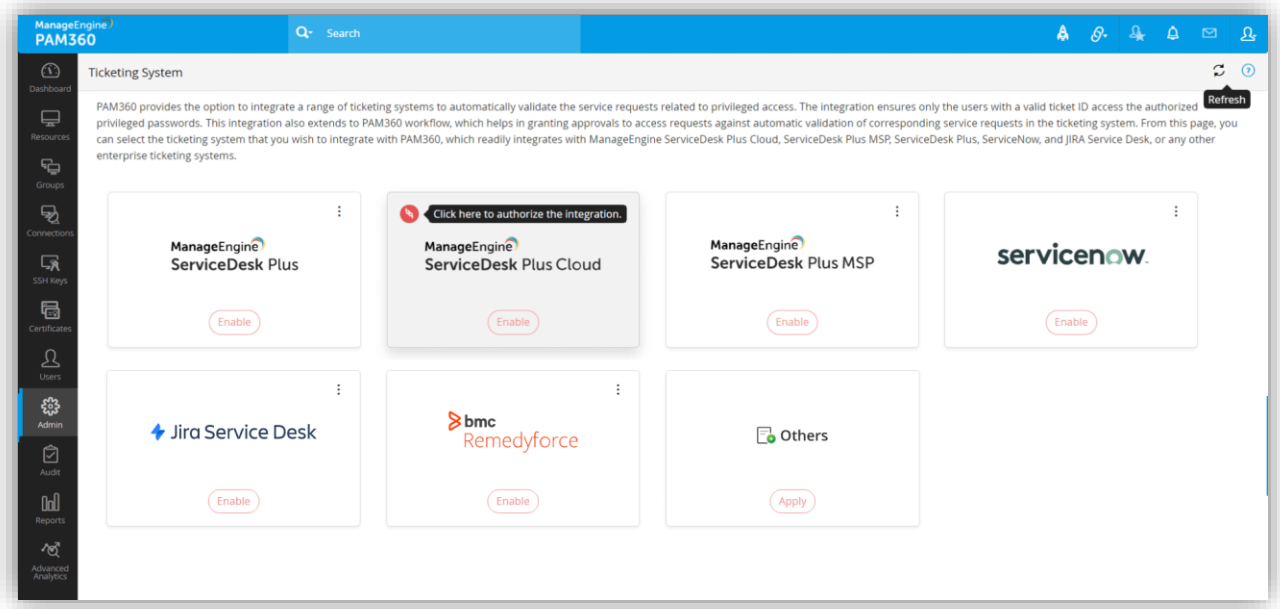
5. Click **Enable.**



The ServiceDesk Plus Cloud configurations have been saved successfully.

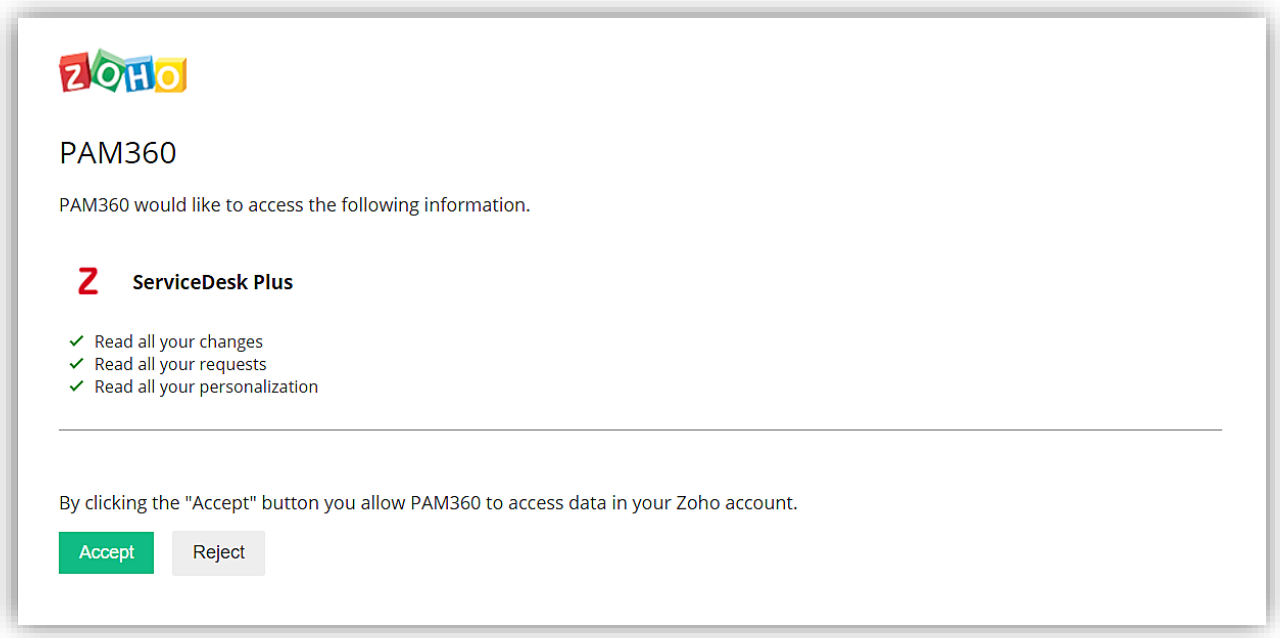
Authorizing ServiceDesk Plus Cloud:

1. To authorize ServiceDesk Plus Cloud, click the **refresh icon** on top right corner of PAM360 to find the **red icon** on top left corner of **ManageEngine ServiceDesk Plus Cloud.**
2. Click the **red icon** to authorize and enable the integration.

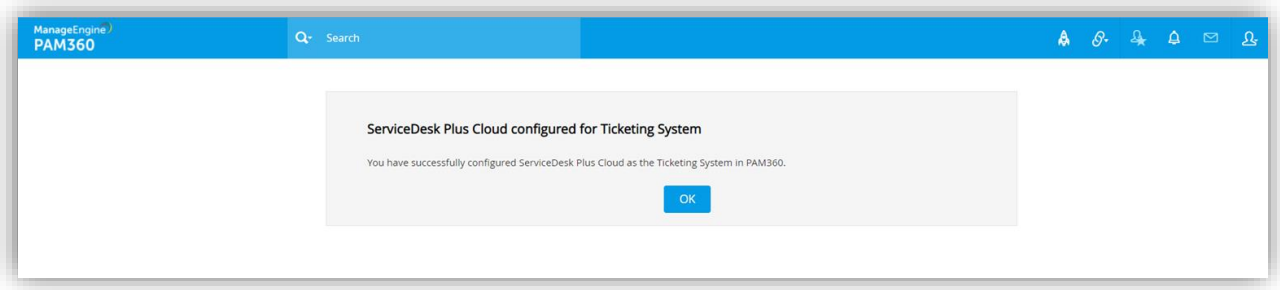


3. In the UI that appears, read the conditions and click **Accept** to allow PAM360 to access data.

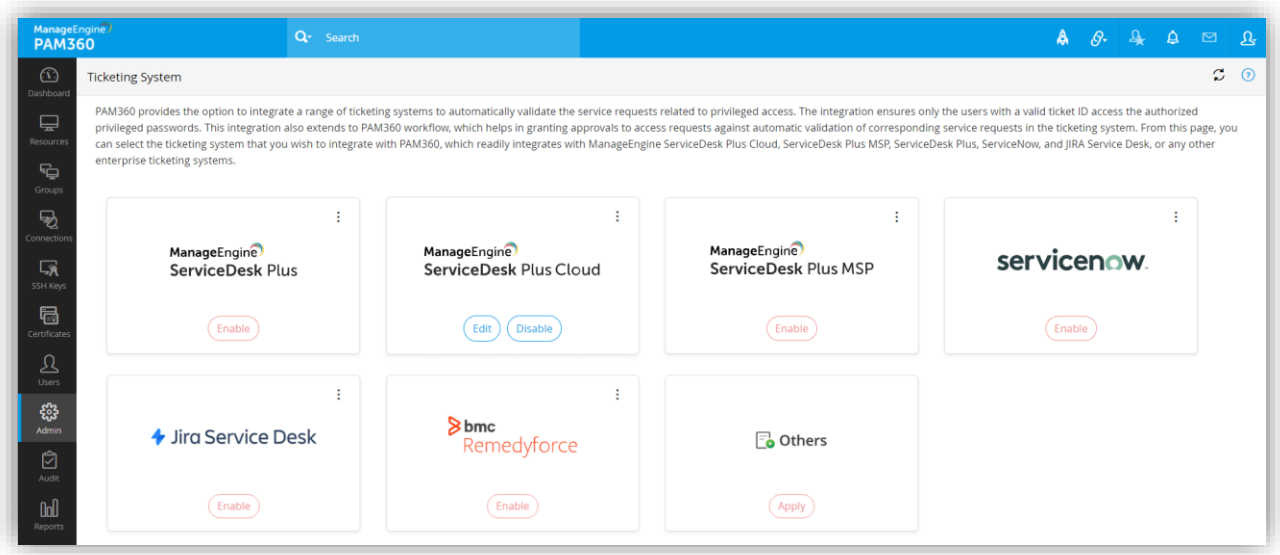
> **Note:** Remember, only users with a **technician role** in the **Ticketing System** should **'Accept'** the above request to view and validate the tickets.



4. ServiceDesk Plus Cloud has been configured successfully as ticketing system in PAM360.



5. Now, click **Ok** to exit the GUI and click the **refresh icon** on top right corner of PAM360 for the changes to appear.



3.2.2 ServiceDesk Plus MSP

PAM360 integrates with ManageEngine ServiceDesk MSP to automatically validate access request to privilege access only with a valid ticket ID. This can be done by generating Technician key and entering the valid ticket ID in the ticketing system.

3.2.3 ServiceDesk Plus

- PAM360 now integrates with ManageEngine ServiceDesk Plus by validating change request in addition to the ticket ID entered by the user in the ticketing system. And validation occurs only when the change ID provided is approved in Manage Engine Service Desk Plus.
- Enabling this option will require your users to provide valid Change IDs for validation of password access requests and other similar operations. On the other hand, if you leave this option unchecked, users will have to submit valid Request IDs for validation.

3.2.4 ServiceNow

PAM360 now integrates with ServiceNow. By integrating with ServiceNow, you can get data from the following simply by entering the **Ticketing system URL** in the respective field **<instance>. <ticketingsystem>.com** and by entering the number.

- ServiceNow Incident – INC (7 digit number) eg) INC0010007
- ServiceNow Change – CHG (7 digit number) eg) CNG0000003
- ServiceNow Change Task – CTASK (7 digit number) eg) CTASK0000009
- ServiceNow Request - REQ (7 digit number) eg) REQ0010004
- ServiceNow Request Item - RITM (7 digit number) eg) RITM0010007
- ServiceNow Problem – PRB (7 digit number) eg) PRB0000007
- ServiceNow Project - PRJ (7 digit number) eg) PRJ0000009
- ServiceNow Project Task – PRJTASK (7DIGIT NUMBER) eg) PRJTASK0010001

- ServiceNow Task – TASK (7 digit number) eg) TASK0010001

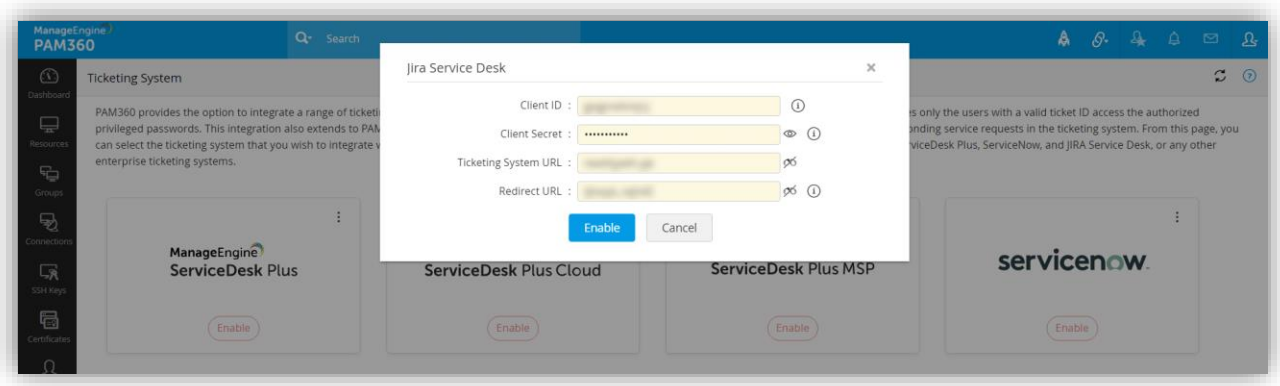
Enabling this option will require your users to enter any of the above valid numbers in PAM360 for validation of password access requests.

3.2.5 JIRA Service Desk

PAM360 now readily integrates with JIRA Service Desk integration to automatically validate service requests related to privileged access.

Configuring JIRA Service Desk in PAM360:

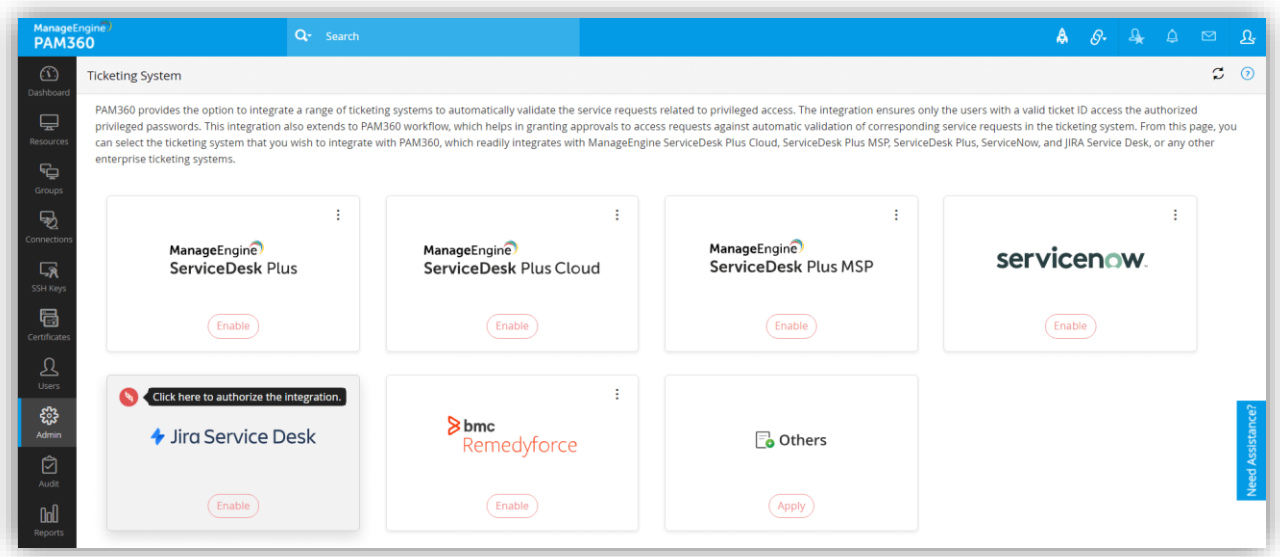
1. Navigate to **Admin >> Integrations >> Ticketing System.**
2. Click **Enable** under **Jira ServiceDesk.**
3. Now, enter the **Client ID** and **Client Secret** generated from the previous Auth Token generation step.
4. Mention your **Jira Service Management URL** as the **Ticketing system URL** and the **Access URL** you use to access the PAM360 server as the **Redirect URL.**
5. Click **Enable.**



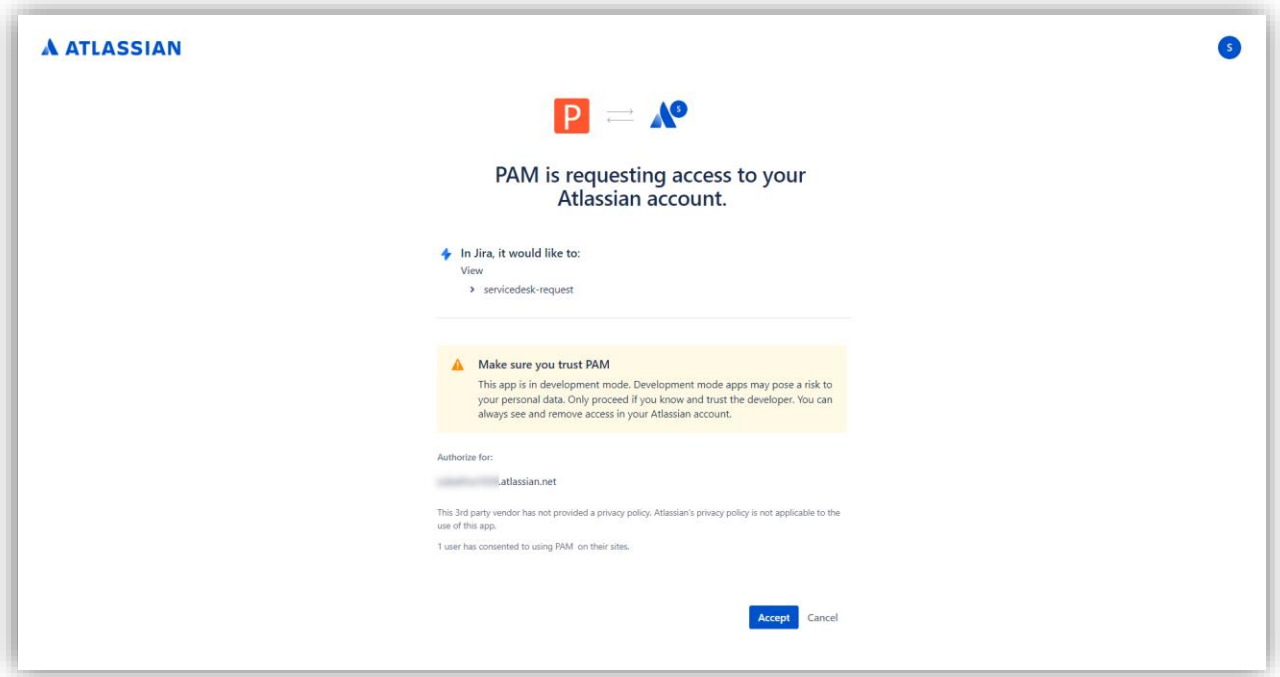
The Jira Service Desk configurations have been saved successfully.

Authorizing Jira Service Desk:

1. Click the **red icon** on top left corner of **Jira Service Desk** to authorize and enable the integration.



2. In the UI that appears, read the conditions and click **Accept** to allow PAM360 to access data.



3. You will now be redirected to PAM360 UI with a success message.

Jira Service Desk has been configured successfully as a ticketing system in PAM360.

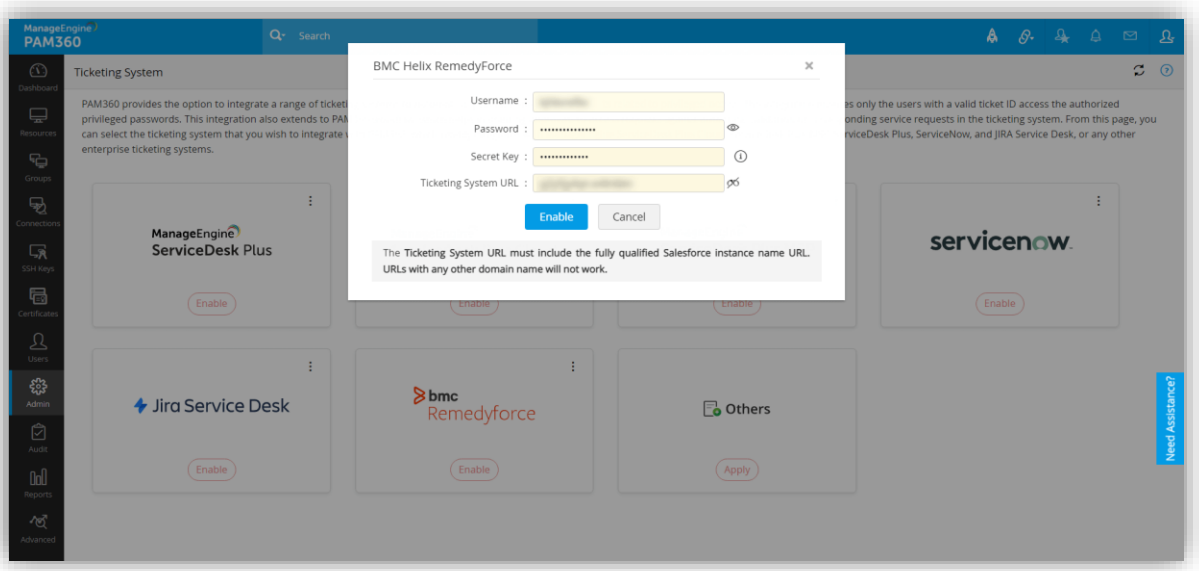
3.2.6 BMC Helix Remedyforce

BMC Helix Remedyforce is a complete IT service management tool that includes Incident/Problem Management, Client Management, Service Management, Reports/Analysis,

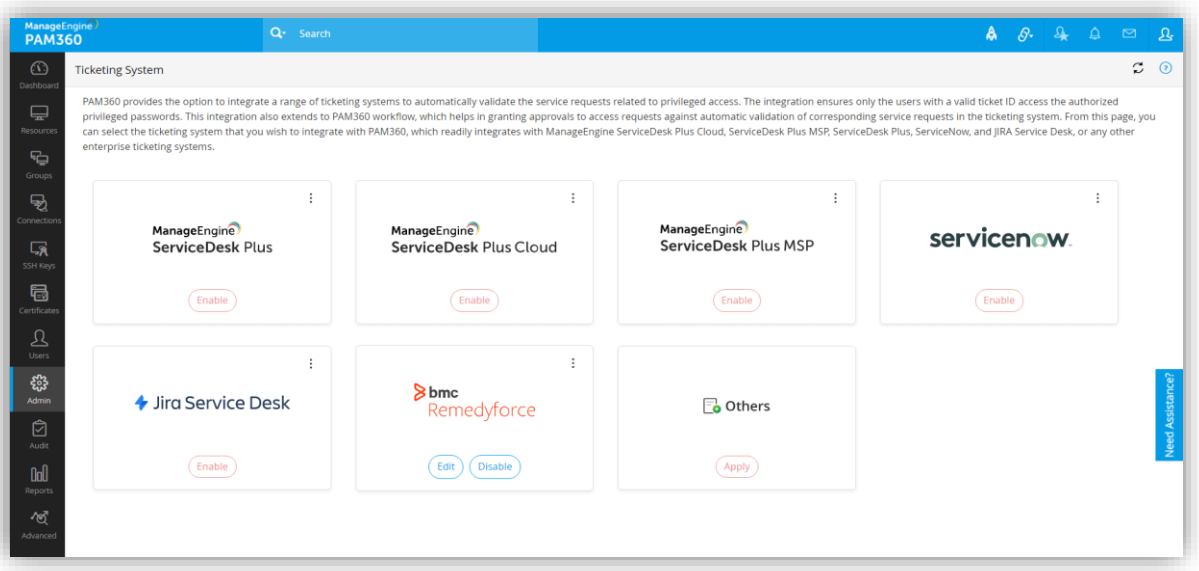
etc., that can be tailored to meet the requirements of enterprises. PAM360 now integrates with BMC Helix Remedyforce to provide automatic validation of service requests pertaining to privileged access. Users will have to submit valid ticket ID's to administrators to gain access to privileged passwords. Through automatic validation of the relevant service requests in the ticketing system, the integration assists in approving access requests.

Configuring BMC Helix Remedyforce in PAM360:

1. Navigate to **Admin >> Integrations >> Ticketing System.**
2. Click **Enable** under **BMC Helix Remedyforce.**
3. In the pop-up that appears,
    i. Mention the Salesforce **Username** and **Password.**
    ii. Mention the **Security Token.** To know more about **Security Token,** click here.
    iii. Mention the Salesforce Instance Name URL as the **Ticketing System URL.**
    iv. Click **Enable.**



BMC Helix Remedyforce has been configured successfully as ticketing system in PAM360.



3.2.7 Others

If you are using any other ticketing system, you can integrate it with PAM360 by having your own custom implementation.

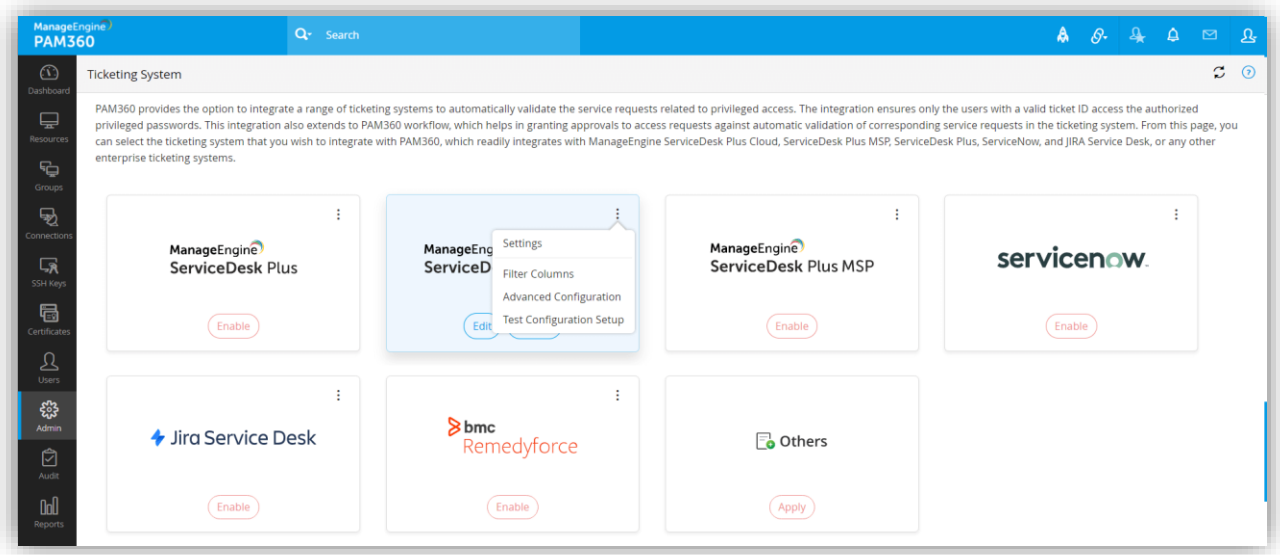
By default, PAM360 validates if the ticket ID entered by the user exists in the ticketing system and also verifies if the incident connected with the ticket is NOT in 'Closed' state. If your requirement is satisfied with these, ticketing system integration is complete.

3.3 Optional Advanced Configurations

In case, you want to validate some other criteria (in addition to ticket number and ticket status), you have the option to configure advanced settings. For example, you can choose to check if the PAM360 user who is raising the password access request matches with the 'REQUESTER' column in the ticketing system. Similarly, you can check for certain specific conditions related to the ticket - for instance, 'PRIORITY' of the ticket as 'HIGH'. PAM360 offers the total flexibility to check for any parameter in the ticketing system, including additional fields.

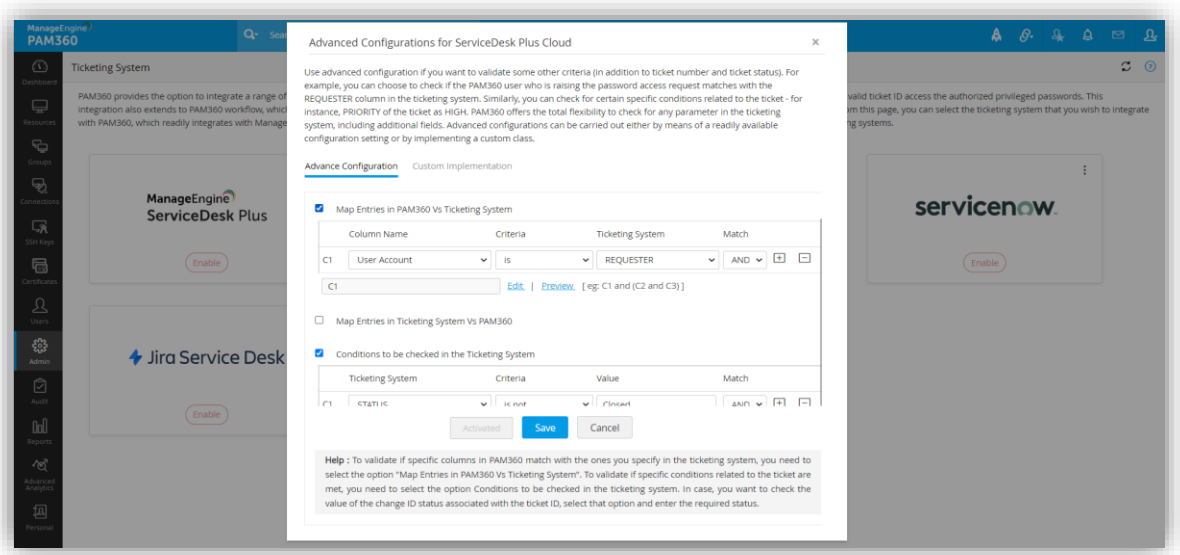
To carry out advanced configurations,

1. Click the three dots on top right corner and select **Advanced Configuration.**
2. In the GUI that opens, Advanced configurations can be carried out either by means of a readily available configuration setting or by implementing a custom class.



Options in Advanced Configurations:

1. Validating if specific columns in PAM360 match with the ones you specify in the ticketing system
    i. Select Map Entries in PAM360 Vs Ticketing System to validate if specific columns in PAM360 match with the ones you specify in the ticketing system.
    ii. The **Column Name** drop-down lists the column names as available in PAM360 - **Resource Name, Resource Type, Account Name, PAM360 User Name, DNS Name,** etc. (including custom fields).
    iii. Select a **Criteria** to validate based on conditions such as **is, is not, contains, does not contain, starts with or ends with.**
    iv. The **Ticketing System** column lists the fields (including custom fields) available in the ticketing system. Choose the field, that has to be mapped with the corresponding field in PAM360.
    For example, you can choose to map **RESOURCE NAME** in PAM360 with **ASSET** in the ticketing system. Once you specify such a mapping, before granting access to the password, PAM360 will check if the RESOURCE NAME as specified in PAM360 matches with the ASSET name in the ticketing system. Only if the validation succeeds, access will be granted.

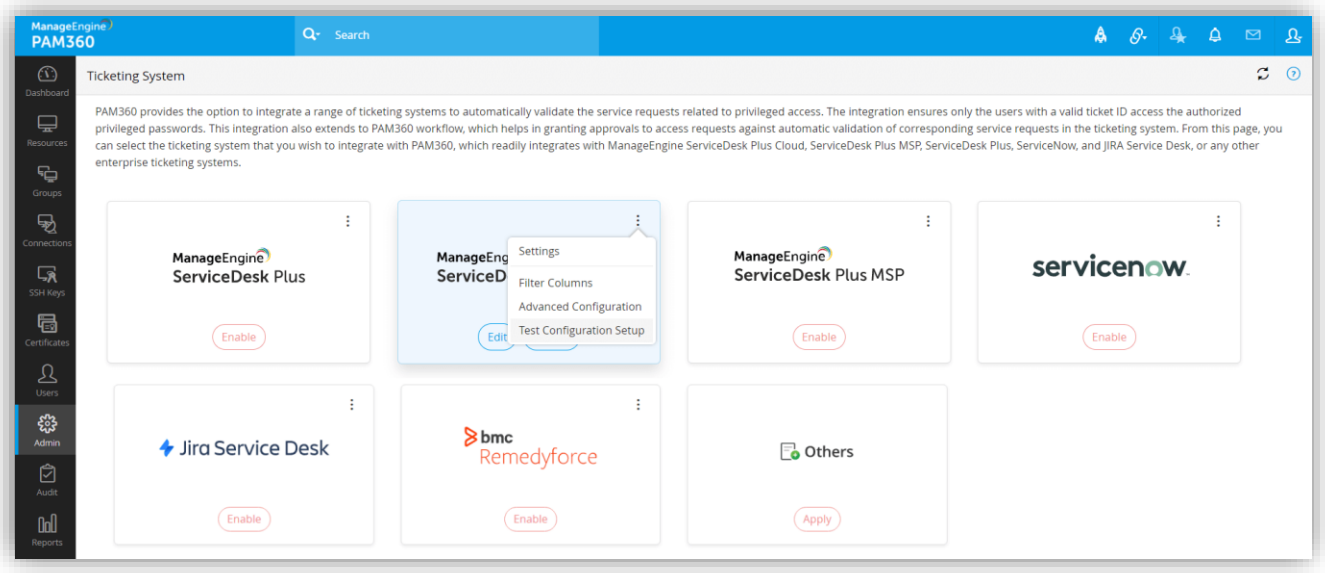


2. Validating if specific columns in the Ticketing System match with the ones you specify in PAM360.
    i. Select **Map Entries in Ticketing System Vs PAM360** to validate if specific columns in the ticketing system match with the ones you specify in PAM360.
    ii. The **Ticketing System** column lists the fields (including custom fields) available in the ticketing system. Choose the field that has to be to be mapped with the corresponding field in PAM360.
    iii. Select a **Criteria** to validate based on conditions such as is, is not, contains, does not contain, starts with or ends with.
    iv. The **Column Name** drop-down lists the column names available in PAM360 such as: **Resource Name, Resource Type, Account Name, PAM360 User Name, DNS Name,** etc. (including custom fields).
3. Validating specific conditions related to the ticket in the ticketing system.
    i. To validate if specific conditions related to the ticket are met, you need to select the option '**Conditions to be checked in the ticketing system**'. By default, PAM360 checks if the ticket STATUS is not in CLOSED state.
    ii. You can select any number of additional conditions and PAM360 will validate all of them with the ticketing system. By default, PAM360 lists down all the fields available in the ticketing system, including the custom fields. You can specify the value, which PAM360 has to validate.
4. Select to **Check the value of change ID status associated with the ticket ID** and mention the **Change ID Status.**
5. Click **Save** to save changes to the ticketing system configurations.

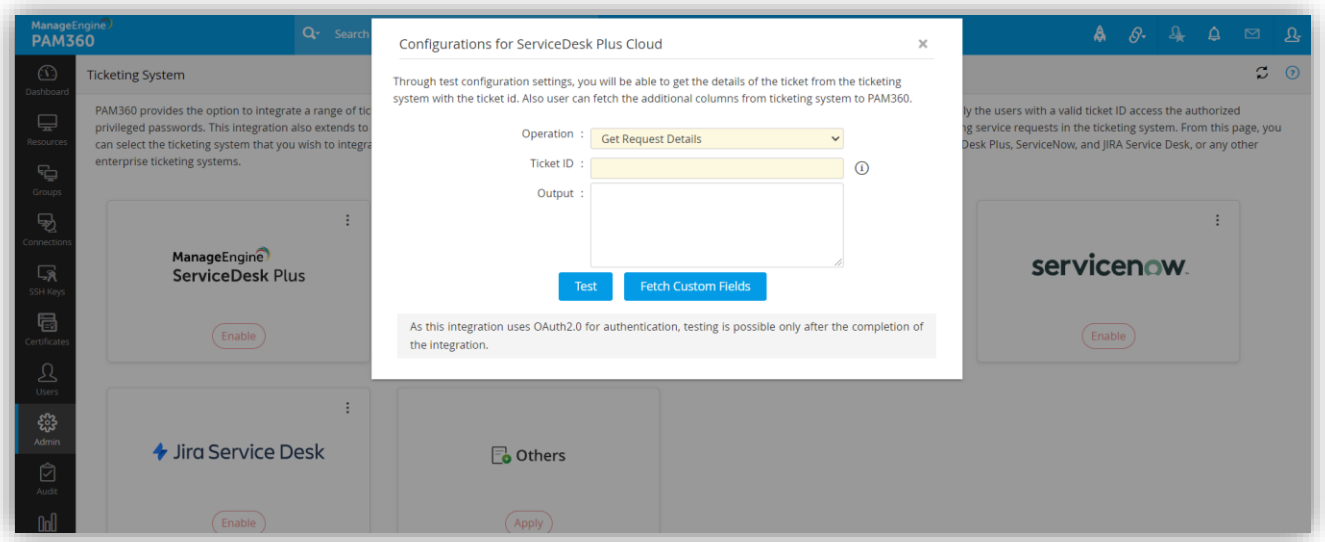
3.4 Test Ticketing System Configuration Setup

After completing the integration, you can do a testing to ensure if PAM360 is able to establish communication with the ticketing system properly. Click the three dots on top right corner

and select **Test Configuration Setup.**

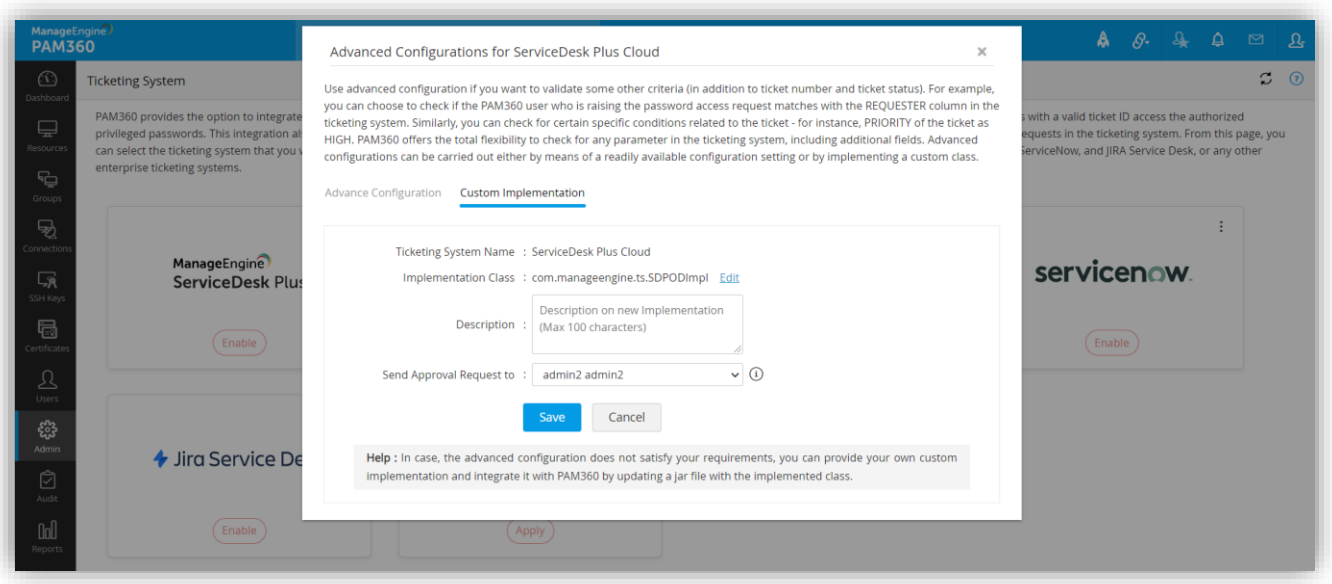


As part of this testing, you can also fetch the custom fields available in PAM360 to the advanced configuration setup.



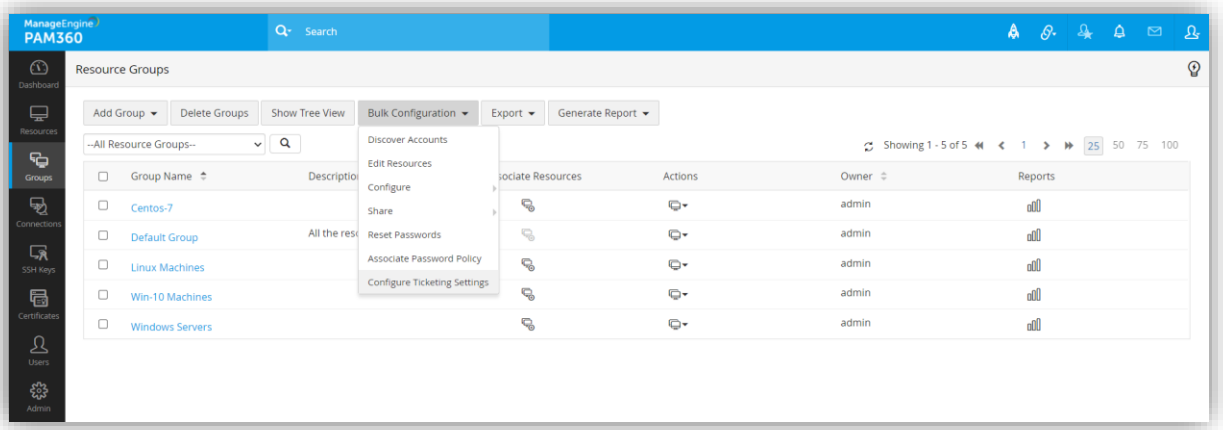
3.5 Custom Implementation

In case, the advanced configuration does not satisfy your requirements, you can provide your own class implementation and integrate it with PAM360 by updating a jar file with the implemented class. For more details, refer to '' Integrating Other Ticketing Systems section below. The steps outlined there hold good here too.



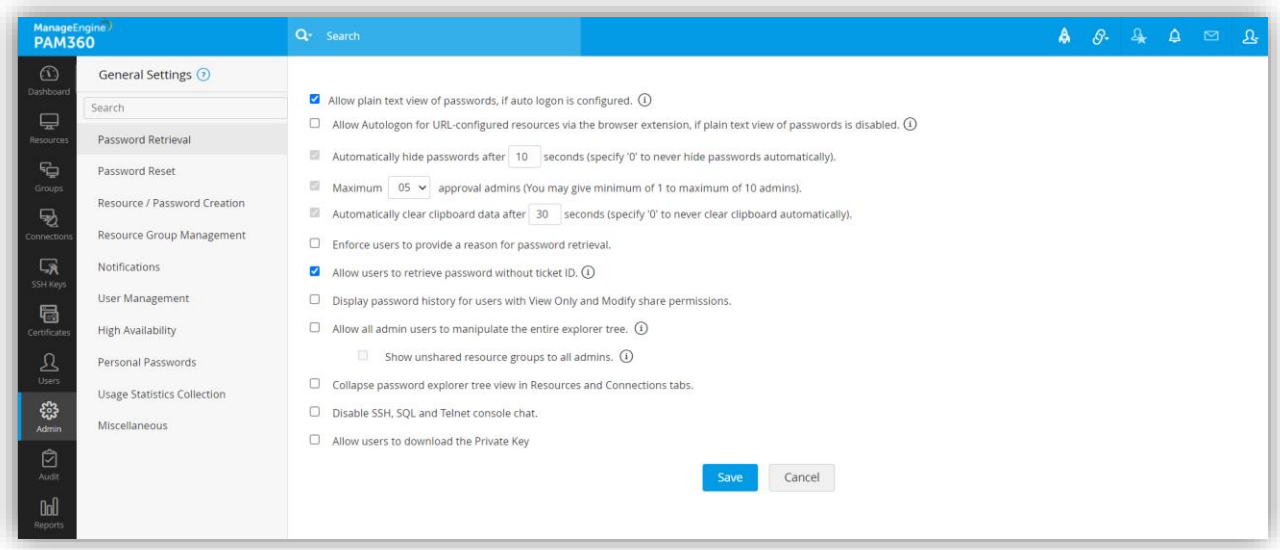
4. Ticketing System Validation Enforcement and Exceptions

1. Once you complete ticketing system integration, it takes immediate effect globally and users will have to produce valid ticket IDs to access passwords. By design, super administrators are exempted from ticket ID enforcement. In addition, as part of access control workflow too, users could be enforced to produce ticket IDs and access can be automatically granted after validating the IDs.
2. You also have the option to selectively enable/disable ticketing enforcement for select resource groups.
    i. This can be done from **Groups.**
    ii. Select the required resource group(s).
    iii. Click on **Bulk Configuration** button at the top of the groups list and select **Configure Ticketing Settings** from the dropdown.

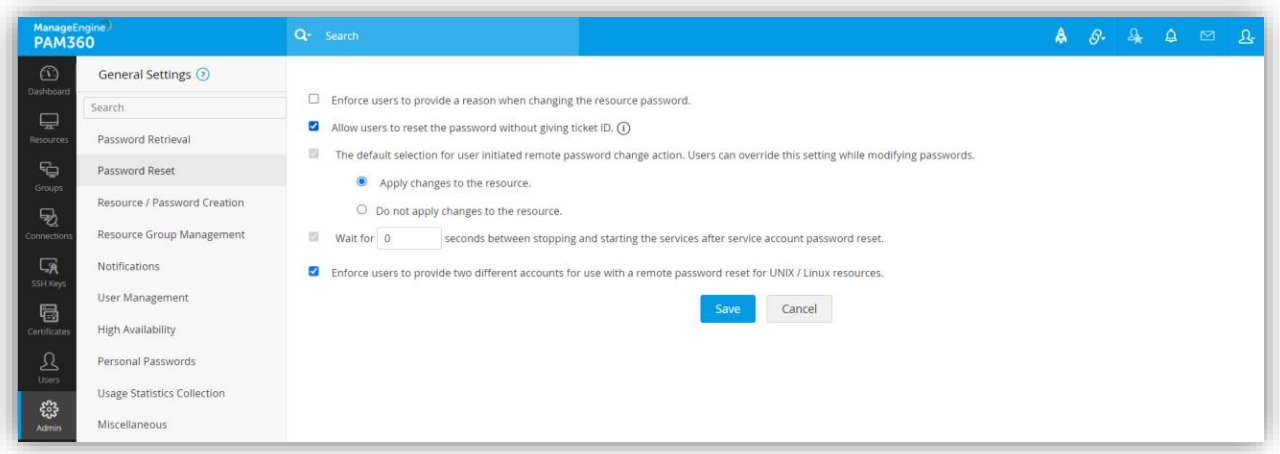


3. From **General Settings,** you can selectively allow/restrict users for ticketing validation

through the options **Allow users to retrieve password without ticket ID** under **Password retrieval** section.



4. And, **Allow users to reset passwords without ticket ID** from **Password Reset** section.



5. In addition, you can have user group-specific settings too, which can be done from the **User Groups** tab.

5. Disabling Ticketing System Integration

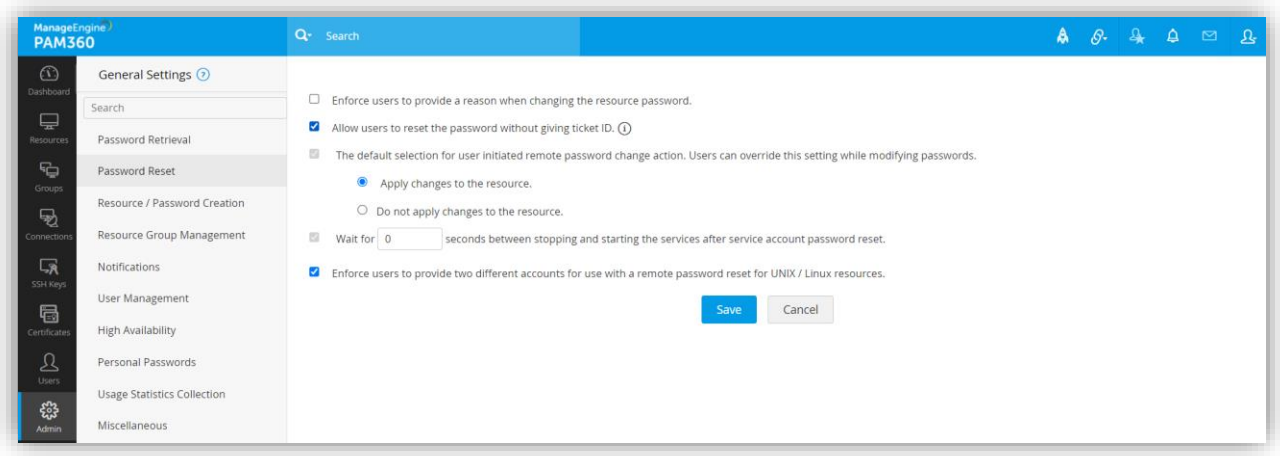
You can disable the integration with the ticketing system anytime. To disable/remove the integration from PAM360,

1. Click the **Disable** icon to disable the integration.

Note: The integration details will not be removed from PAM360 when the integration is **disabled.** You will be able to enable the integration at any given time.

2. Click **Remove** to completely remove all the integration details from PAM360.

Note: To enable ServiceDesk Plus Cloud integration again, you have to generate a new set of **Client ID, Client Secret** as instructed above in section 3.2, and configure ServiceDesk Plus Cloud to PAM360.



6. Integrating Other Ticketing Systems

If you are using any other ticketing system, you can integrate it with PAM360 by having your own custom implementation. To guide you through the process, we have taken integrating Zendesk as an example to explain the steps involved.

Step 1: Create your implementation class

Refer to the sample implementation class created for integrating Zendesk. The important aspects of the implementation class have been explained below:

Generate Authentication Token

The first step is to generate authentication token of the ticketing system to enable PAM360 establish connection. When generating the AUTH TOKEN, ensure that you provide the credentials of an administrator who has full access to the ticketing system. You can do this

either by providing the credentials directly in the implementation class or by generating the token and putting the token.

The snippet below shows how to generate Base64 Authstring belonging to a privileged account of the ticketing system. This will come in handy when the REST API is based on Base64 Authorization header. Some ticketing systems offer AUTH-Token with inbuilt GUI. In such cases, you can directly use the authentication parameters. In addition, instead of hard coding username and password in the implementation class, you can very well skip this part and make REST API call with direct Base64 token that are generated through Java or through any online editors.

Refer to the code snippet below:

```
// Constructing Authstring from Zendesk login credentials

String username = "username@example.com"; //Zendesk username
String password = "zendeskpassword"; //Zendesk password
Base64 encoder = new Base64();
byte[] encodedPassword = (username + ":" + password).getBytes();
byte[] encodedString = encoder.encodeBase64(encodedPassword);
String authStr = new String(encodedString);
```

Step 2: Check connection with ticketing system

Using REST APIs, PAM360 can be made to get the information about tickets from the ticketing system. Each ticketing system follows its own procedure to disseminate ticket details. Refer to the respective documentation to identify the procedure. After obtaining the ticket details, you need to validate the details.

Refer to the code snippet below:

```
String sUrl = "https://<zendesk-instance>.zendesk.com/api/v2/tickets/"; //REST
API call Zendesk
sUrl = sUrl + ticketId +".json"; //This is the ticket ID that will be validated against
the one supplied by the user in PAM360
URL url = new URL(sUrl);
HttpsURLConnection connection = (HttpsURLConnection)
url.openConnection();
connection.setRequestProperty("Authorization","Basic "+authStr); //Setting
Authstring in the header
```

Step 3: Validating if specific columns in PAM360 match with the ones you specify in the ticketing system (optional configuraion)

Refer to the code snippet below to validate if specific columns in PAM360 match with the ones you specify in the ticketing system (For example, you can choose to map RESOURCE NAME in PAM360 with the SUBJECT in the ticketing system. Once you specify such a mapping, before granting access to the password, PAM360 will check if the RESOURCE NAME as specified in PAM360 matches with the SUBJECT name (if the subject contains the resource name) in the ticketing system. Only if the validation succeeds, access will be granted):

```
String assetName = (String)pam360Columns.get("Resource Name");//PAM360 Asset Name for which password related operation done
String subject = (String)ticket.get("subject");//Getting the ticket subject
boolean descriptionCheck = subject.toLowerCase().contains(assetName.toLowerCase());
//Checking the description of the ticket contains the resource name of user account
```

Step 4: Validating specific conditions related to the ticket in the ticketing system (optional configuraion)

You can validate if specific conditions related to the ticket are met - by default, PAM360 checks if the ticket STATUS is not in CLOSED state. You can select any number of additional conditions and PAM360 will validate all of them with the ticketing system. By default, PAM360 lists down all the fields available in the ticketing system, including the custom fields. You can specify the value, which PAM360 has to validate.

```
JSONObject ticket = (JSONObject)ticketingOuput.get("ticket");
String status = (String)ticket.get("status");
boolean statusCheck = "open".equalsIgnoreCase(status); //Checking whether the status of the ticket is in open state
```

Step 5: Compilation

While compiling, keep the following jars in the classpath (the jars are available under <PAM360_HOME>\lib folder)

- *AdventNetPassTrix.jar;*
- *json_simple-1.1.jar;*

- *commons-codec-1.7.jar*

For Example,

javac -d . -cp AdventNetPassTrix.jar;json_simple-1.1.jar;commons-codec-1.7.jar ZendeskImpl.java - (For Windows)

javac -d . -cp AdventNetPassTrix.jar:json_simple-1.1.jar:commons-codec-1.7.jar ZendeskImpl.java - (For Linux)

Step 6: Configurations in PAM360 installation

1. Compile the implemented class files as a single jar and place that jar in **PAM360_HOME\lib** folder.
2. Restart the PAM360 Service so that PAM360 will make use of the implemented class.
3. Navigate to **Admin >> Integration >> Ticketing System Integration.**
4. In the GUI that opens, select the option 'Other' (to integrate any ticketing system) OR the 'Class Implementation' 'Advanced Configuration' of the already integrated ticketing system (if you want to extend the functionality).
5. Specify the name of your implementation class.
6. Your implementation has to be approved by another administrator. All other administrators (other than those who made the request) will receive an alert regarding the request for approval.
7. Once an admin approves the implementation, it will be made available for use.
8. After enabling, ticketing system workflow will be made mandatory for password retrieval and password reset.

For further information, refer to the sample implementation class created for integrating Zendesk.

Implementation tips:

For steps 3 and 4 above, you might require additional information for implementation. Refer to the tips below for details:

Columns in PAM360

List of data related to the user account for which ticketing request is raised through pam360Columns parameters from PAM360 side:

PAM360 User Name - Logged in user name
Resource Name - Name of the resource
DNS Name - IP Address of the resource
User Account - Account name

Resource Type - Type of the resource being accessed (Windows/ WindowsDomain/ Linux etc.)
Resource Description - Description about the resource
Department - Department to which the resource belongs
Location - Resource location
Domain Name - Domain name of the resource
Request Type - Request Type for which ticketing system call is made. It can be

> RETRIEVAL - Password access
> REQUEST - Password access request raised through Access-Control workflow
> RESET - Password reset
> AUTOLOGON - 'Open Connection' request

User Organization Name - Organization name of the user who made the request
User Current Organization Name - Name of the organization where the requested account is present
Other than this, all additional columns will be sent as shown below:
Resource additional field - **Resource@<field_name>**
Account additional field - **Account@<field_name>**

Credentials to Access Ticketing System

> **AUTHTOKEN -** Authentication token value given in the integration GUI
> **TICKETINGSYSTEMURL -** URL given in the integration GUI

Advanced Configuration Details:

ISPAM360TICKETCRITERIA - To check if PAM360 vs Ticketing system is configured or not

> (Boolean - true or false)

PAM360TICKETCRITERIACOLUMNS - Mapping details between PAM360 and ticketing system. Each element in the array represents a criteria. For example, the column 'User Account' in PAM360 has to be validated against Ticketing system column 'REQUESTER' with match parameter 'EQUAL' in criteria 'C1'

JSONArray - [["C1","User Account","REQUESTER","EQUAL"],
["C2","PAM360 User Name","TECHNICIAN","EQUAL"]]

PAM360TICKETCRITERIA - Specifies the relationship between different criteria. Each element of 'PAM360TICKETCRITERIACOLUMNS' contains the first parameter as criteria name. It gives the relationship between criteria

(String - Example: C1 or C2)

ISTICKETVALUECRITERIA - To check if the validation for ticketing system values is configured or not

(Boolean - true or false)

TICKETVALUECRITERIACOLUMNS - Mapping details that ticket should satisfy. Each element in the array represents an criteria. For example, ticket column 'STATUS' has to be validated against value other than 'Closed' in criteria 'C1'

JSONArray - [["C1","STATUS","Closed","NOT_EQUAL"],
["C2","URGENCY","high","EQUAL"],
["C3","IMPACT","high","EQUAL"]]

TICKETVALUECRITERIA - Specifies the relationship between different criteria. Each element of 'TICKETVALUECRITERIACOLUMNS' contains the first parameter as criteria name. It gives the relationship between criteria

(String - Example: C1 or (C2 and C3)

ISTICKETCHANGEIDSTATUS - To check if the validation for system change status check is configured or not (true or false)

TICKETCHANGEIDSTATUS - Associated 'change ID status' of the ticket ID value

Match Parameters:

EQUAL - Values of two parameters should be same
NOT_EQUAL - Values of two parameters should not be same
CONTAINS - First parameter value should contain the value of second parameter
NOT_CONTAINS - First parameter value should not contain the value of second parameter,
STARTS_WITH - First parameter must start with value of second parameter,
ENDS_WITH - First parameter must end with value of second parameter,
(Date based comparison parameters)
LESS_THAN - First parameter date value should be less than the second one,
GREATER_THAN - First parameter date value should be greater than the second one,
LESS_THAN_EQUAL - First parameter date value should be less than or equal to the second one,
GREATER_THAN_EQUAL - First parameter date value should be greater than or equal to the second one
Depending on the match parameters, the criteria should get validated.

7. Code Snippet For ServiceNow Custom Implementation

If the advanced configuration does not satisfy your requirements, you can have a custom implementation. You can extend the default implementation provided by PAM360 and have the additional functionalities. The following example shows how the default implementation created for ServiceNow, can be extended to serve as the custom implementation.

```
package com.manageengine.ts;
import java.util.Properties;
import org.json.simple.JSONObject;
import com.adventnet.passtrix.helpdesk.ServiceNowImpl;
//ServiceNow custom implementation
public class ServiceNowCustomImpl extends ServiceNowImpl
{
public boolean checkViewHelpDeskRequest(String ticketId, Properties
pam360Columns, Properties credentialDetails, JSONObject criteriaDetails)
throws Exception
{
boolean result = super.checkViewHelpDeskRequest(ticketId, pam360Columns,
credentialDetails, criteriaDetails);
//Your own implementation
return result;
}}
```

The table below lists down default functionality processing classes for the ticketing systems that readily integrate with PAM360:

ServiceDesk Plus On-Demand	com.adventnet.passtrix.helpdesk.ServiceDeskPlusOnDemandImpl
ServiceDesk Plus MSP	com.adventnet.passtrix.helpdesk.ServiceDeskPlusMSPImpl
ServiceDesk Plus	com.adventnet.passtrix.helpdesk.ServiceDeskPlusOnPremiseImpl
ServiceNow	com.adventnet.passtrix.helpdesk.ServiceNowImpl
JIRA	com.adventnet.passtrix.helpdesk.JiraServiceDeskImpl

8. Interface Description

The interface for ticketing system integration:

```
package com.manageengine.ts;
import java.util.Properties;
import org.json.simple.JSONObject;
// This class provides the methods to implement ticketing system integration. You
need to implement this interface
public interface TicketingSystemInterface
{
/**
* Used to display the error message while doing the ticketing system related
operations. The output gets reflected in audit trails.
* @return Error message, if the ticketing system accessible, return null. Otherwise,
return a proper error message.
*/
public String getErrorMsg();
/**
* Used to return the properties related to the ticketing system operation
* @return Comments and needed message
*/
public Properties getRequestProperties();
/**
* Used for testing configuration setup. While testing, administrator will be able to get
ticket details from the ticketing system.
* @param tsName Ticketing system Name
* @param tsUrl Ticketing system Web URL
* @param authToken Authentication Token assigned to a technician of ticketing
system (Base64 authorization string constructed
using login credentials in the case of ServiceNow ticketing system)
* @param ticketId Ticket ID given as the input ((Ticket ID/Sys ID in the case of
ServiceNow ticketing system)
```

```
* @param Ticketing System operation type
* {@value 0} Ticketing Operation
* {@value 1} Change Related Operation
* @return the output from ticketing side
* @throws Exception
*/
public JSONObject helpdeskCheck(String tsName, String tsUrl, String authToken,
String ticketId, String operation) throws Exception;
/**
* Actual function that will be called upon whenever a ticketing system related
operation is done from PAM360 GUI
* @param ticketId Ticket ID (Ticket ID/Sys ID in the case of ServiceNow ticketing
system)
* @param pam360Columns Details of the PAM360 account for which ticketing
system query is raised
* @param credentialDetails Key details of ticketing system (Authentication token or
Base64 authorization string
and web URL of ticketing system)
* @param criteriaDetails Criteria mapping done as part of advanced configuration
* @return Final output that will be sent to PAM360 server
* {@value true} Success case - Allows the operation to proceed
* {@value false} Failure case - Denies the operation to proceed
* @throws Exception
*/ public boolean checkViewHelpDeskRequest(String ticketId, Properties
pam360Columns, Properties credentialDetails, JSONObject criteriaDetails)
throws Exception; }
```

Secure Cloud Storage Options for Anytime, Anywhere Access to Passwords

In addition to the options to export passwords to a spreadsheet in plain-text or to an encrypted HTML file, PAM360 provides cloud storage provisions to enable anytime, anywhere access to passwords in a secure way. This can be done by enabling auto-synchronization of the encrypted HTML file to the authorized users' mobile devices via **Dropbox, Amazon S3, and Box** accounts. Typical use case scenarios for this option include:

- A managed service provider (MSP) using PAM360 to store shared passwords of their clients and technicians; has no access to the application inside the client's network while visiting them.
- Technicians working in DMZs with no access to the application's web UI.

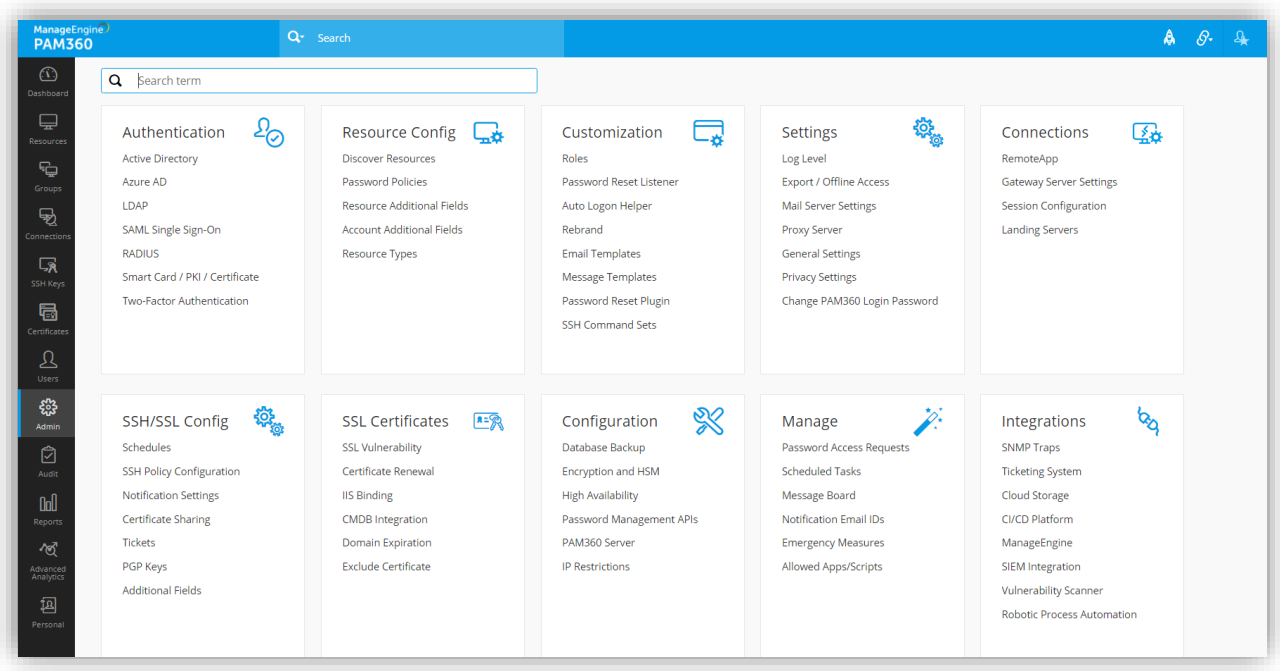
To enable cloud storage option for users and set up synchronization for each option, refer to their respective sections given below:

1. **Steps to Configure Dropbox Synchronization**
2. **Steps to Configure Amazon S3 Synchronization**
3. **Steps to Configure Box Synchronization**

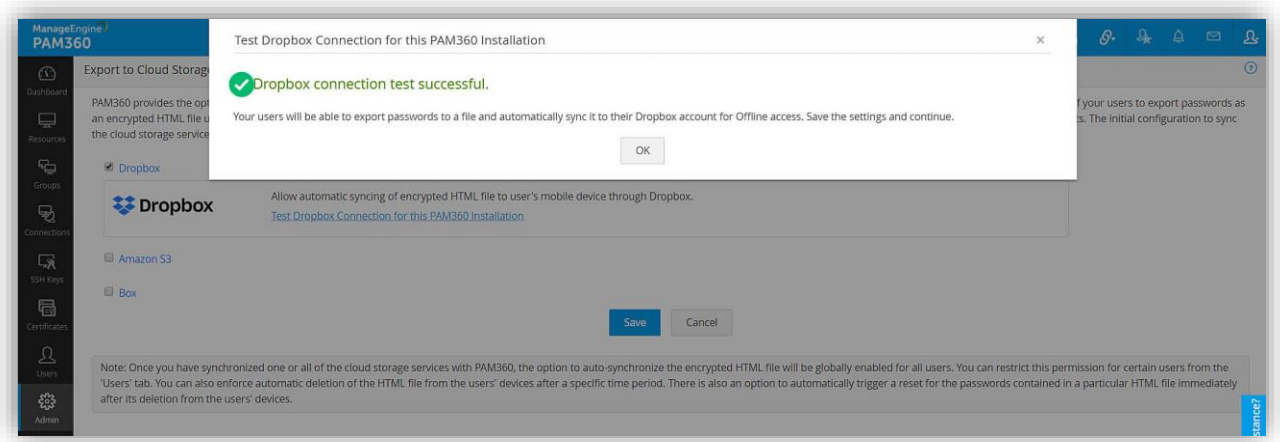
1. Steps to Configure Dropbox Synchronization

To enable Dropbox sync for your users, follow the below steps:

1. Go to **Admin >> Integration >> Cloud Storage.**



2. In the page that loads, select **Dropbox.** Then, click the link - **Test Dropbox Connection for this PAM360 Installation.** This basically checks the proxy settings (if applicable in your environment) and does the necessary background processes to try and connect to the Dropbox app named "ManageEngine PAM360" created by PAM360 for this purpose. A successful connection will enable users to upload the encrypted HTML file to their Dropbox account.

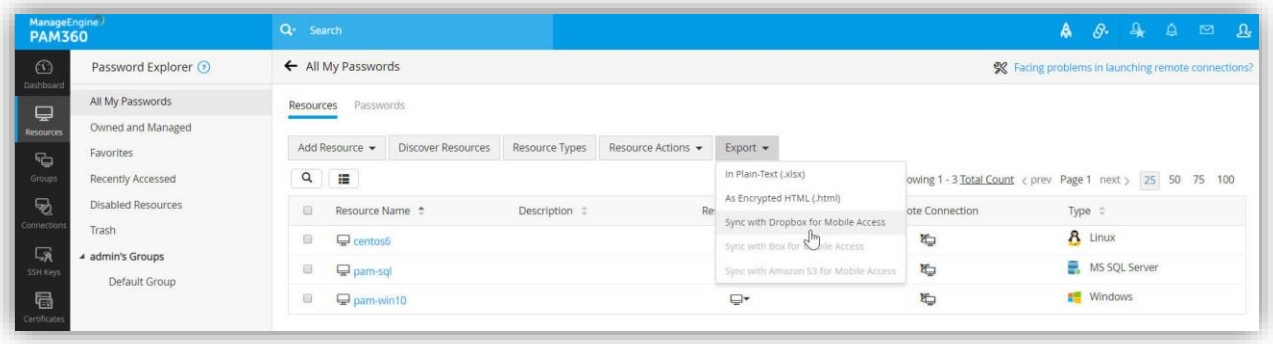


3. Then, click **Save.** Dropbox synchronization will be enabled for users in your organization.

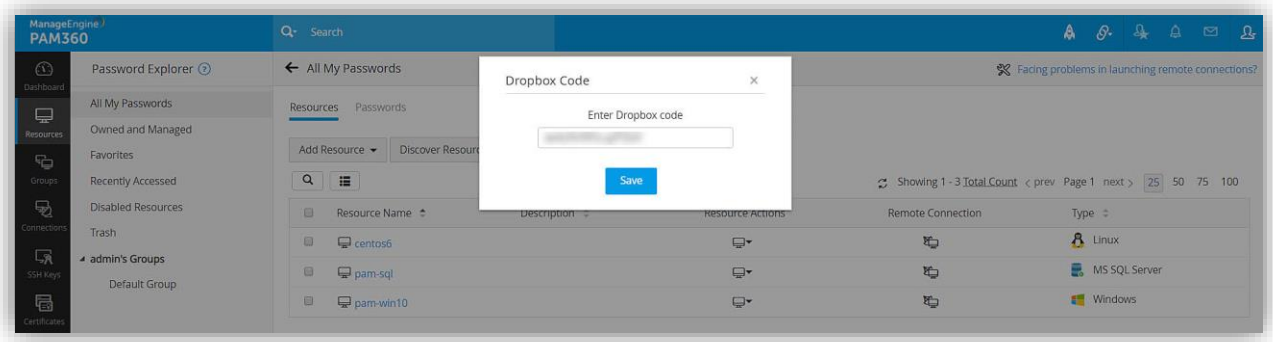
1.1 Steps to Export and Synchronize the Encrypted HTML file to Dropbox

If you are a user who wants to export and synchronize the encrypted HTML file to your Dropbox account (provided that you already have a Dropbox account. If not, create one to proceed with the following steps),

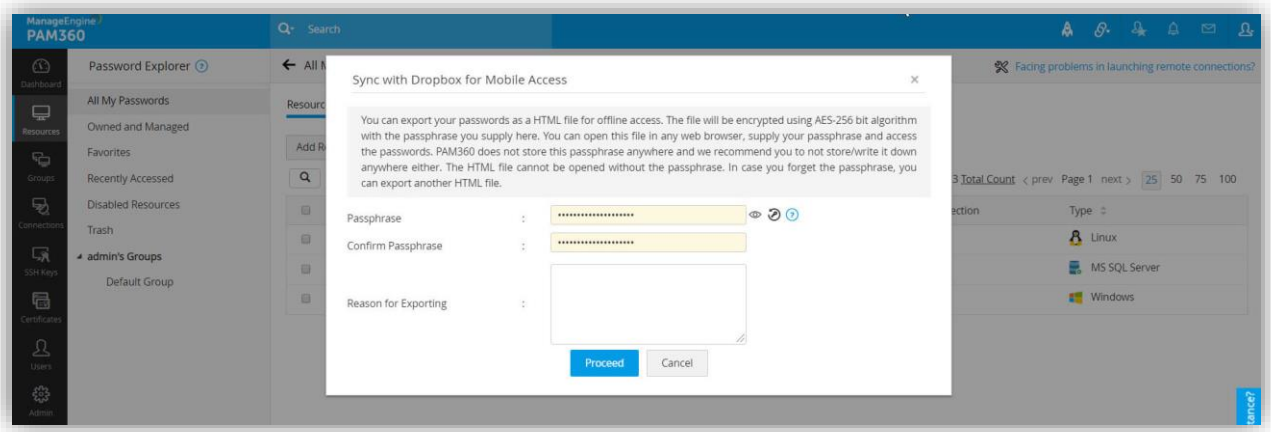
1. Go to **Resources >> Export >> Sync with Dropbox for Mobile Access.**



2. In the dialog box that opens, click **Authorize.** A new window will open, asking you to log into Dropbox account. Once you log in, the page will display a request from PAM360 to access its folder **ManageEngine PAM360** inside your Dropbox account. Click **Allow** to approve the request.
3. A Dropbox code will be displayed as shown in the image below. Copy the code and navigate back to the PAM360 active session in the other browser tab. Paste the Dropbox code in the displayed text field and click **Save.**



4. Now, click on **Export** again and select **Sync with Dropbox for Mobile Access.**
5. In the dialog box that opens, set a passphrase for that HTML file that you are about to export. The file will be encrypted using AES-256 bit algorithm with the passphrase you supply here. Then, enter your reason for export if mandated by your PAM360 administrator.

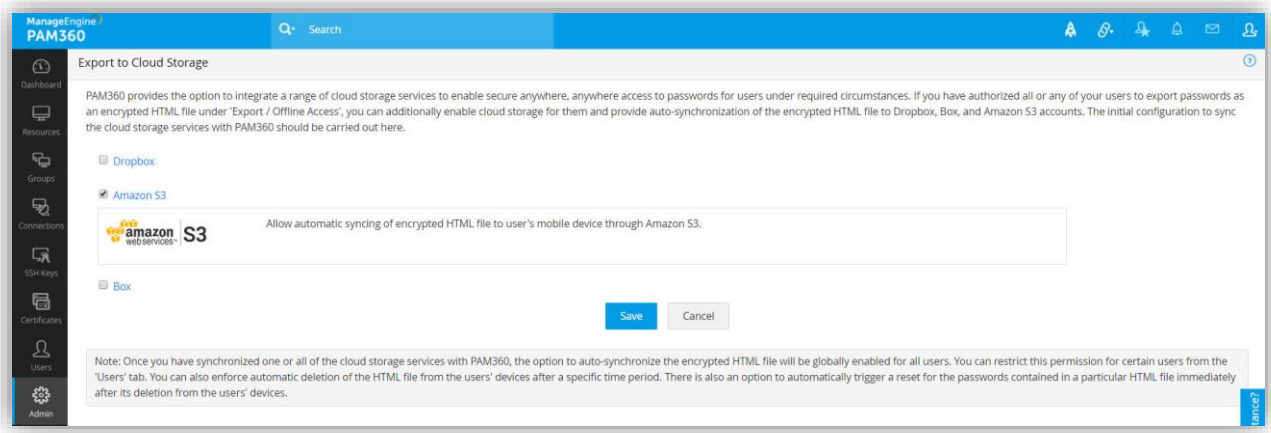


6. Click **Proceed.** Once the HTML file has been successfully synchronized, PAM360 will shortly display a message at the bottom left corner of the UI. You can click on the message or directly access your Dropbox account to check if the file has been synchronized. In your Dropbox account, the encrypted HTML file will appear under a new folder created in the name of ManageEngine PAM360.

2. Steps to Configure Amazon S3 Synchronization

To enable Amazon S3 sync for your users, follow the below steps:

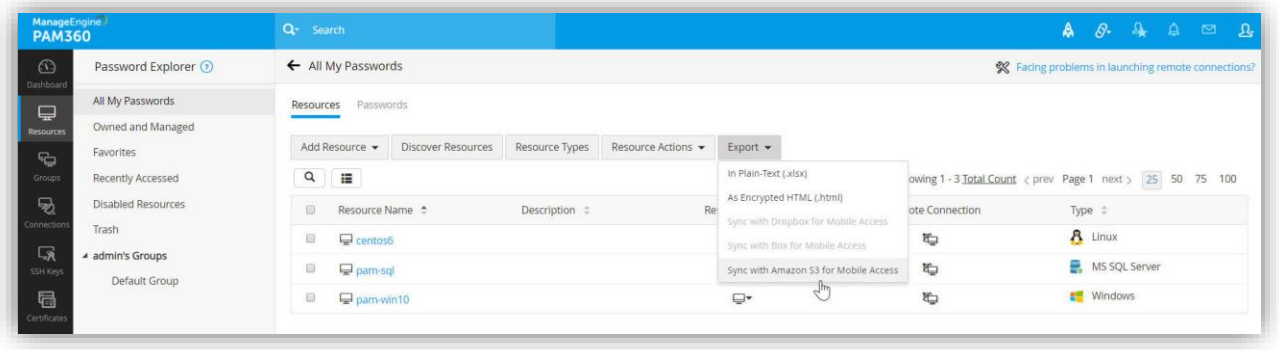
1. Go to **Admin >> Integration >> Cloud Storage.**
2. In the page that loads, select **Amazon S3** and click **'Save'.** Amazon S3 synchronization will be enabled for users in your organization.



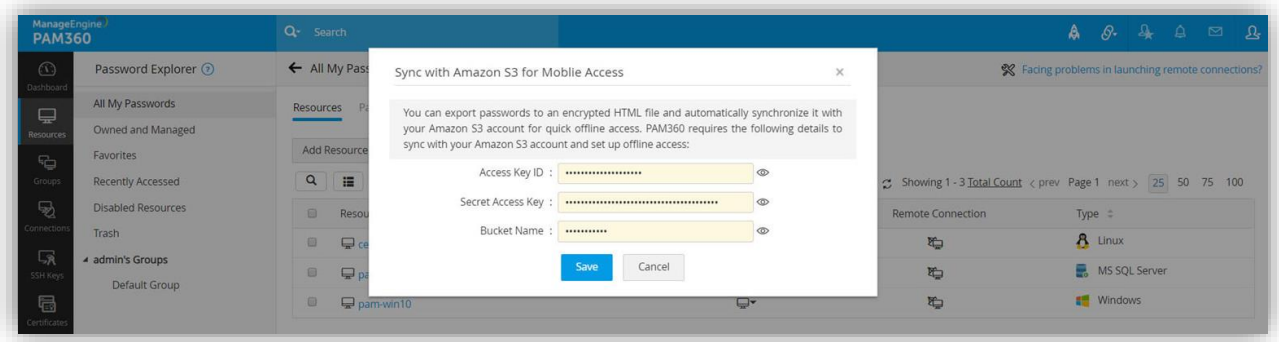
2.1 Steps to Export and Synchronize the Encrypted HTML file to Amazon S3

If you are a user who wants to export and synchronize the encrypted HTML file to your Amazon S3 account (provided that you already have an Amazon S3 account. If not, create one to proceed with the following steps),

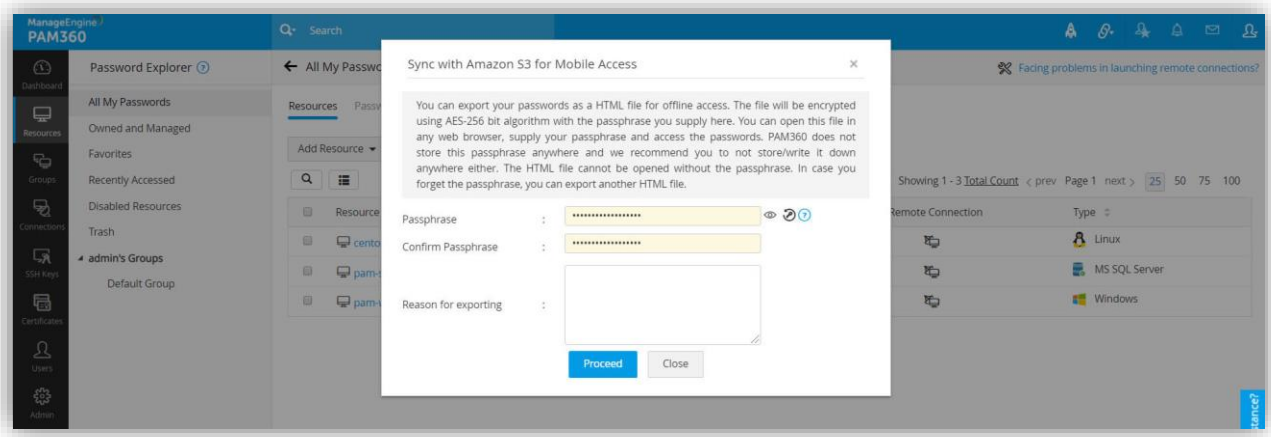
1. Go to **Resources >> Export >> Sync with Amazon S3 for Mobile Access.**



2. In the dialog box that opens, you have to provide the following details: Access key ID, Secret access key, and Bucket Name.



3. Access key ID and Secret access key are user security credentials that are automatically assigned to you when your AWS administrator creates your user profile in your organization's AWS account. The credentials are usually sent via an email to your inbox. In case you do not have access to your Access key ID and Secret access key, contact your AWS administrator.
4. Bucket Name: Bucket Names are the names of the folder that you create in your Amazon S3 account. Here, provide the Bucket Name of an existing folder. This is where the encrypted HTML file will be stored upon synchronization.
5. After providing the required details, click **Save.**
6. Now, click on **Export** again and select **Sync with Amazon S3 for Mobile Access.**
7. In the dialog box that opens, set a passphrase for that HTML file that you are about to export. The file will be encrypted using AES-256 bit algorithm with the passphrase you supply here. Then, enter your reason for export if mandated by your PAM360 administrator.

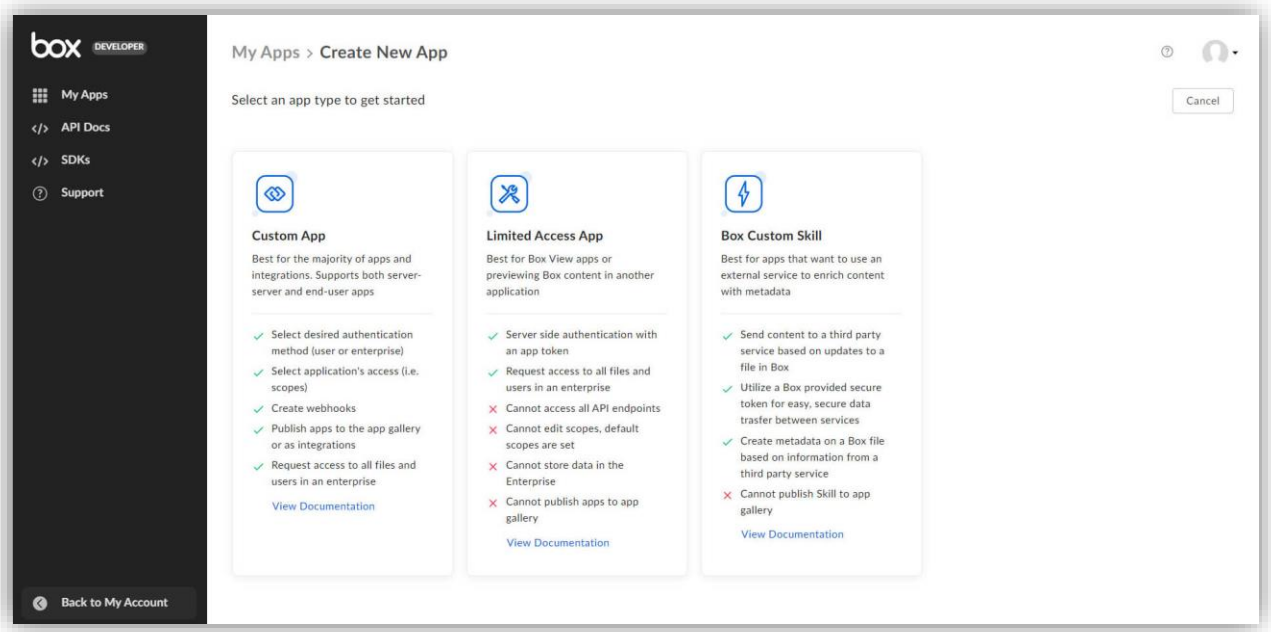


8. Click **Proceed.** Once the HTML file has been successfully synchronized, PAM360 will shortly display a message at the bottom left corner of the UI. You can click on the message or directly access your Amazon S3 account to check if the file has been synchronized. In your Amazon S3 account, the encrypted HTML file will appear under the bucket that you have specified earlier.

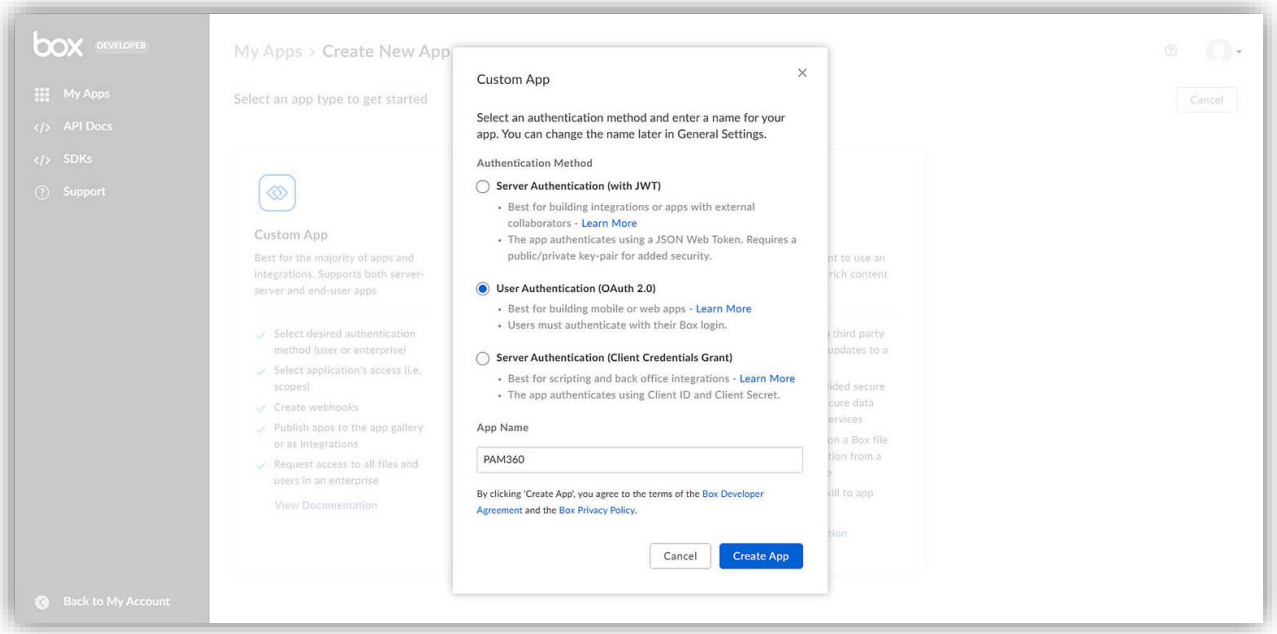
3. Steps to Configure Box Synchronization

Synchronizing Box with PAM360 first requires a Box account. If you do not own a Box account, go to the Box website and create one. Upon creating your account, follow the below steps:

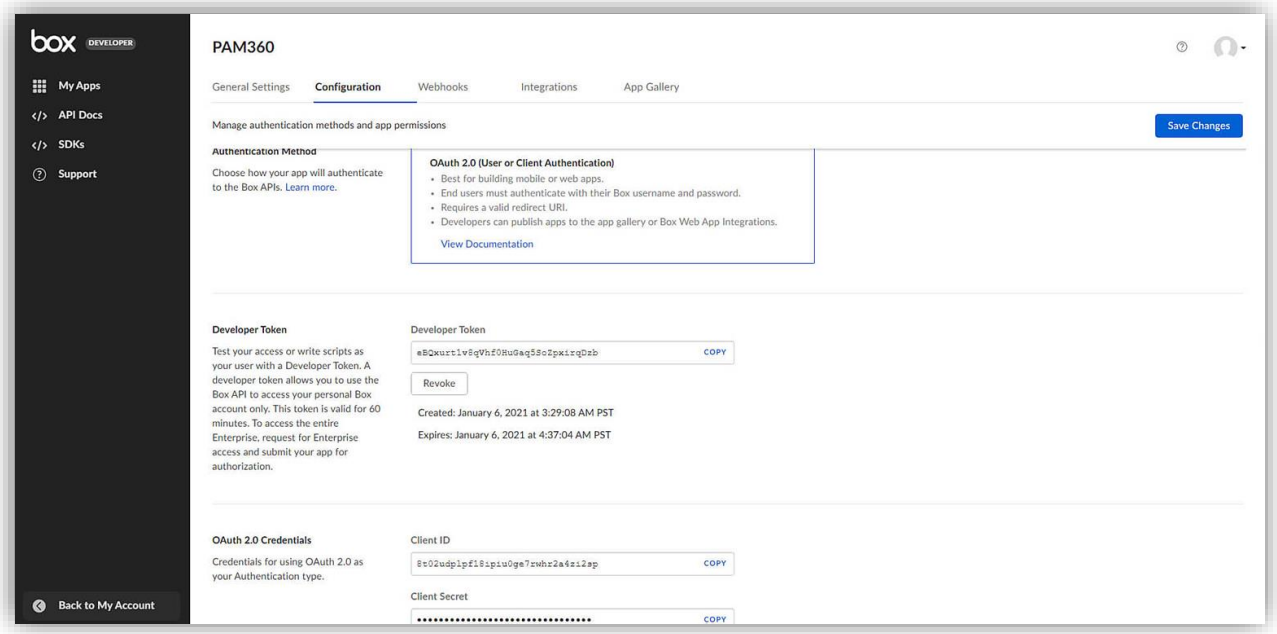
1. Go to the Box Developers console and log in with your Box credentials. Once you log in, click **Create New App,** and select **Custom App**.



2. In the **Custom App** window, choose **User Authentication (OAuth 2.0)** as the Authentication Method. Enter a name for the app and click **Create App**.



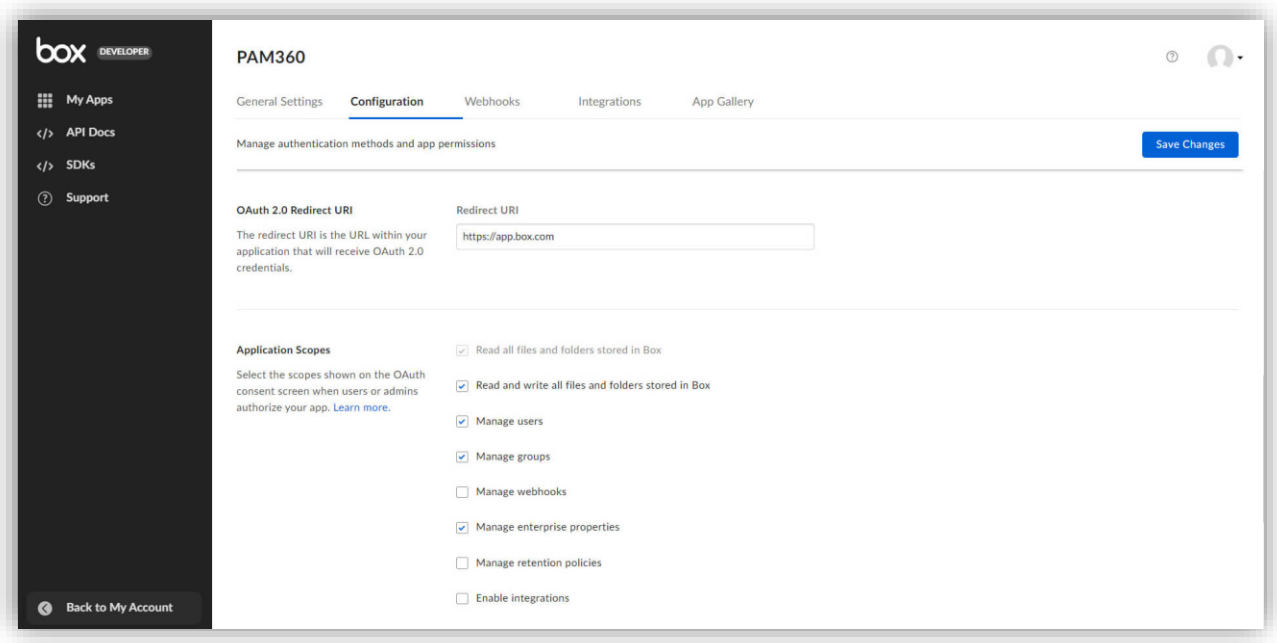
3. In the **Configuration** page, ensure that the selected **Authentication Method** is **OAuth 2.0 (User or Client Authentication).**
4. Next, copy the **Client ID** and **Client Secret** provided under the **OAuth 2.0 Credentials** section and save them elsewhere. You will need to provide these credentials later in the PAM360 server to complete the integration.



5. Next, under **OAuth 2.0 Redirect URI** section, enter your PAM360 server URL.
The format of the redirect URI should be as follows: **https://<Host-Name-of-PAM360-Server OR IP address>:<port>/PassTrixMain.cc#/ExternalApp/code/**

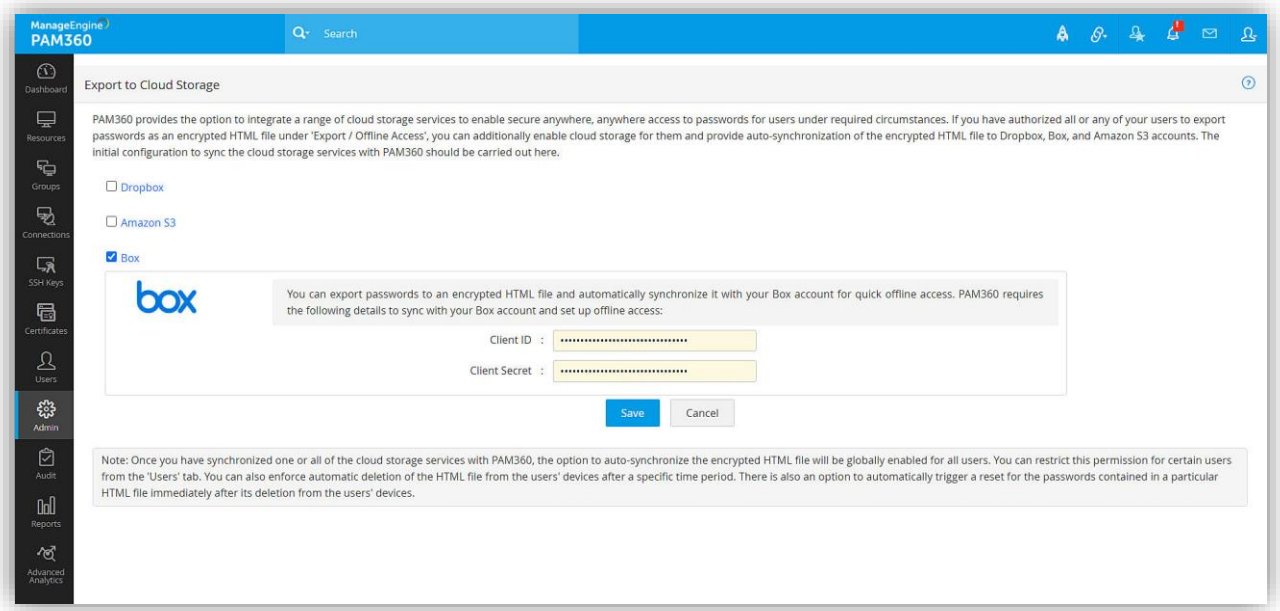
Note: If you have high availability configured in your PAM360 installation, and if the primary server is down and the secondary server is running, you have to modify the redirect URL in your Box configuration settings as required for the synchronization to work.

6. Finally, under **Application Scopes**, ensure that permission to **Read and write all files and folders stored in Box** is checked.
7. Click **Save Changes.**



Once you have carried out all the aforementioned steps in the **Box Developers** console, follow the below steps to complete the configuration in **PAM360**:

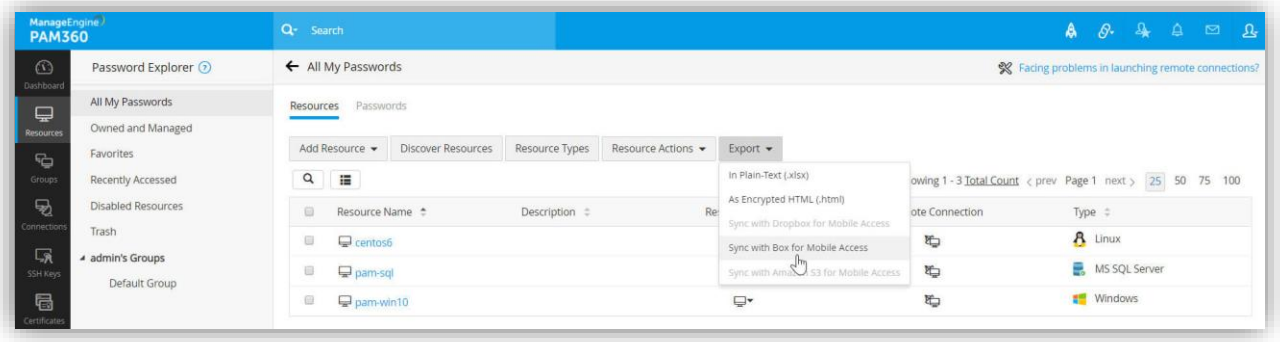
1. Navigate back to **PAM360 >> Admin >> Integration >> Cloud Storage.**
2. Select **Box** and enter the **Client ID** and **Client Secret** copied from the Box console. Click **Save**. Box synchronization will be enabled for users in your organization.



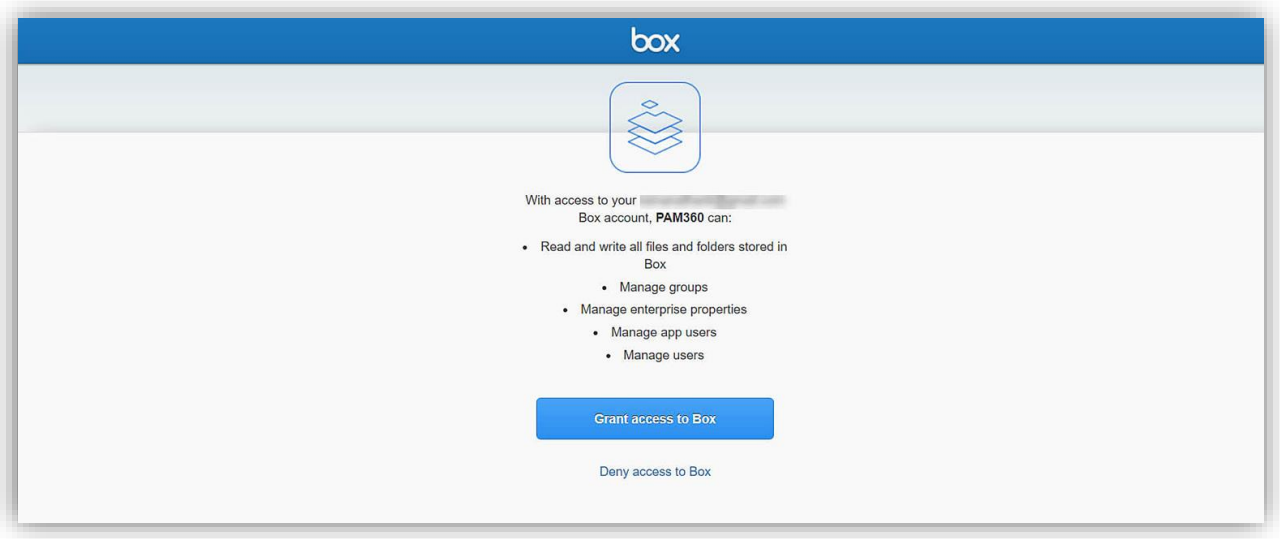
3.1 Steps to Export and Synchronize the Encrypted HTML file to Box

If you are a user who wants to export and synchronize the encrypted HTML file to your Box account:

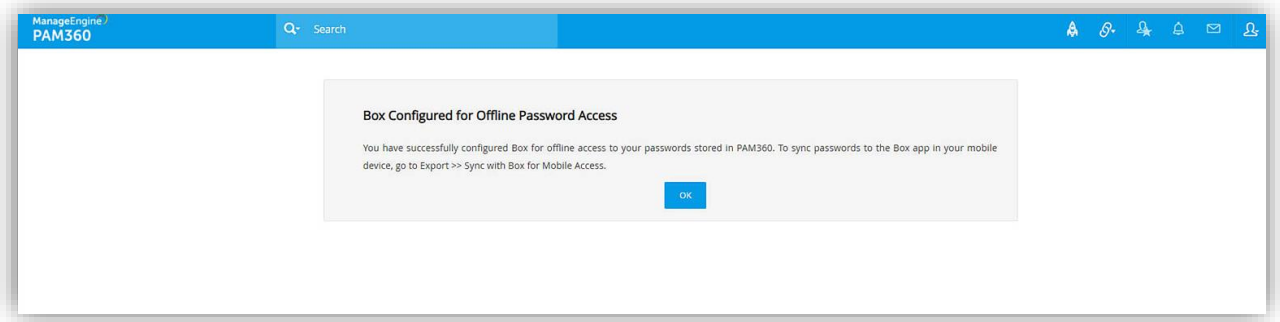
1. Go to **Resources >> Export >> Sync with Box for Mobile Access.**



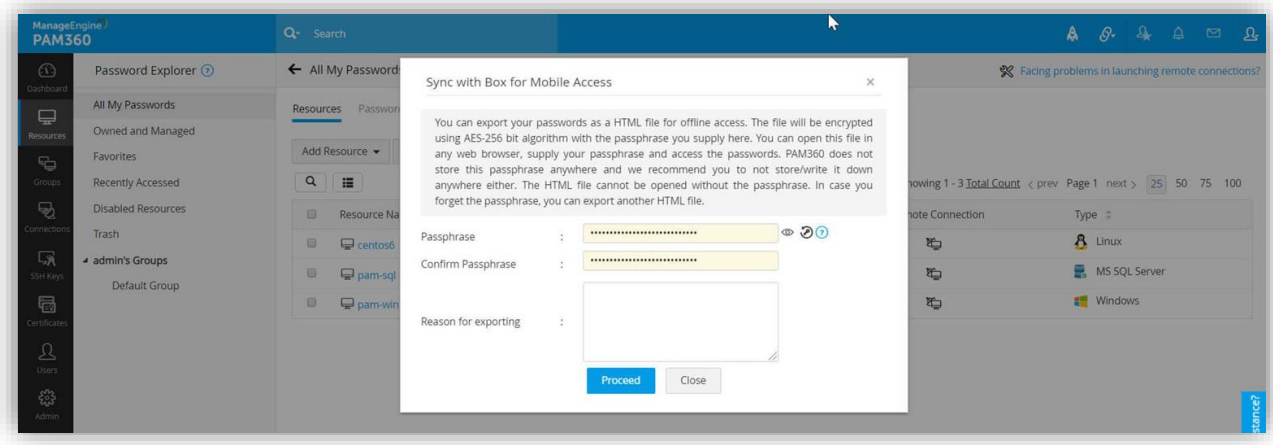
2. In the dialog box that opens, click **Authorize.** Box's login page will open in a new window. Log in with your Box credentials and in the page that loads, click **Grant access to Box.** A message saying the authorization is successful will be displayed. Click **OK**. You will then be automatically redirected back to the PAM360 interface.



3. A message saying the authorization is successful will be displayed. Click **'OK'.** You will then be automatically redirected back to the PAM360 interface.



4. Now, navigate again to **Resources >> Export** and click on **Sync with Box for Mobile Access.**
5. In the dialog box that opens, set a passphrase for that HTML file that you are about to export. The file will be encrypted using AES-256 bit algorithm with the passphrase you supply here. Then, enter your reason for export if mandated by your PAM360 administrator.



6. Click **Proceed.** Once the HTML file has been successfully synchronized, PAM360 will shortly display a message at the bottom left corner of the UI. You can click on the message or directly access your Box account to check if the file has been synchronized. In your Box account, the encrypted HTML file will appear under a new folder created in the name of PAM360.

PAM360 Plugins for CI/CD Platforms

Continuous integration and continuous delivery (CI/CD) platforms are automation tools that help organizations automate their configuration management through pipelines to run routine tasks without human supervision. Execution of these tasks often require sensitive information like privileged passwords, API keys, and access tokens to interface with other systems, applications, and services in the environment. In most DevOps environments, such credentials are stored in plaintext within script files to enable smooth task execution but that can lead to many security issues.

To mitigate such risks, PAM360 helps eliminate embedded credentials in the DevOps pipeline by providing integration capabilities with various CI/CD tools. The integration ensures that the required credentials are retrieved securely from PAM360's vault every time a task is executed, instead of being stored in plaintext within the script files.

PAM360 plugins are available for the following CI/CD platforms:

1. **Jenkins**
2. **Ansible**
3. **Chef and Puppet**

Check the respective help section to know more about setting up the plugin for the required platform.

PAM360 Plugins for Jenkins

Jenkins is a leading Java-based open source automation tool that is widely used in DevOps environments to build and test software projects continuously. SDLC tasks related to building, testing, and delivering or deploying software can be created as automation schedules in Jenkins, named as 'jobs.' Execution of these 'jobs' more often than not requires user credentials and similar sensitive information like privileged passwords, API keys, and access tokens to interface with other systems and services. In most DevOps environments, such credentials are stored within plain text files in the Jenkins server, which can lead to a horde of security and management issues.

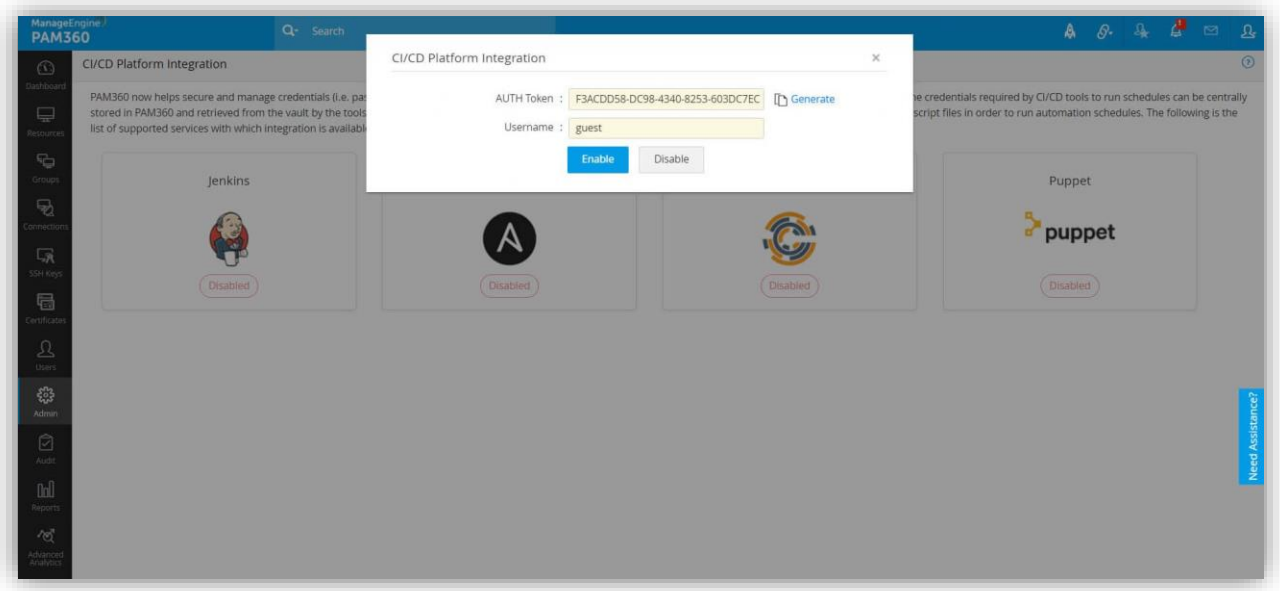
The PAM360 plugin developed for secrets management in Jenkins helps improve security in organizations' DevOps pipeline. The plugin once enabled in Jenkins, ensures that required credentials are retrieved from PAM360's vault every time when a job is run, instead of being embedded in plain text within script files. Upon secure retrieval, the credentials can then be used in environment variables, such as connecting to a remote server for build activation. The plugin also saves the user from the arduous job of having to manually update the password in the script file every time there's an update. Often, there are instances when a user is unable to run a job since they're locked out of the target application or server owing to an outdated password in the script file. Now with the credentials stored in PAM360, they're regularly rotated and also updated on the respective remote device, which ensures that only the latest passwords are retrieved from the vault while running jobs. Currently, the plugin can be used for secrets management at a job level, i.e. for freestyle project jobs.

Read further to learn in detail on how to use the PAM360 plugin for secrets management in Jenkins.

1. Enabling Jenkins Integration in PAM360
2. Installing and Enabling the PAM360 Plugin in Jenkins
3. Retrieving Passwords from PAM360 for Jenkins' Freestyle Project Jobs
4. List of Available PAM360 Attributes

1. Enabling Jenkins Integration in PAM360

1. Log in to PAM360 and navigate to **Admin >> Integration >> CI/CD Platform Integration >> Jenkins.**
2. **AUTH Token**: Click on '**Generate**' to populate an AUTH Token automatically. This will be required later while configuring the plugin in Jenkins' console. Once set up, all incoming connections from Jenkins will be validated by PAM360 using this AUTH token.



3. **Username**: Here, enter the username of an active PAM360 user whose account will be used automatically by Jenkins to securely retrieve the required passwords from PAM360's vault.

> **Note**: Ensure that the user account you provide has the minimum required permissions for this workflow i.e. privilege to view/retrieve the passwords of resources to which Jenkins has to connect.

4. Click **Enable**.

> **Note:** Since Jenkins may have multiple instances, **Host Name** check will be disabled for the Jenkins requests.

2. Installing and Enabling the PAM360 Plugin in Jenkins

The following actions to be carried in Jenkins' console require a user role with the privilege to manage plugins in the tool.

2.1 Installing the Plugin

1. First, download the plugin here.
2. Open Jenkins' console and navigate to **Manage Jenkins >> Manage Plugins >> Advanced**.
3. Under **Upload Plugin** section, upload the plugin file.

4. Additionally, Jenkins also requires the SSL certificate of your PAM360 installation while establishing a connection. So the SSL certificate has to be added to Jenkins' keystore. Add the SSL certificate using the below command:

```
keytool -import -trustcacerts -keystore <<PATH_TO_JENKINS_JAVA_KEYSTORE>> -alias <<ALIAS_NAME>> -import <<PATH_TO_PAM360_SSL_CERTIFICATE>>
```

5. Upon installation, restart the Jenkins server to apply the changes.

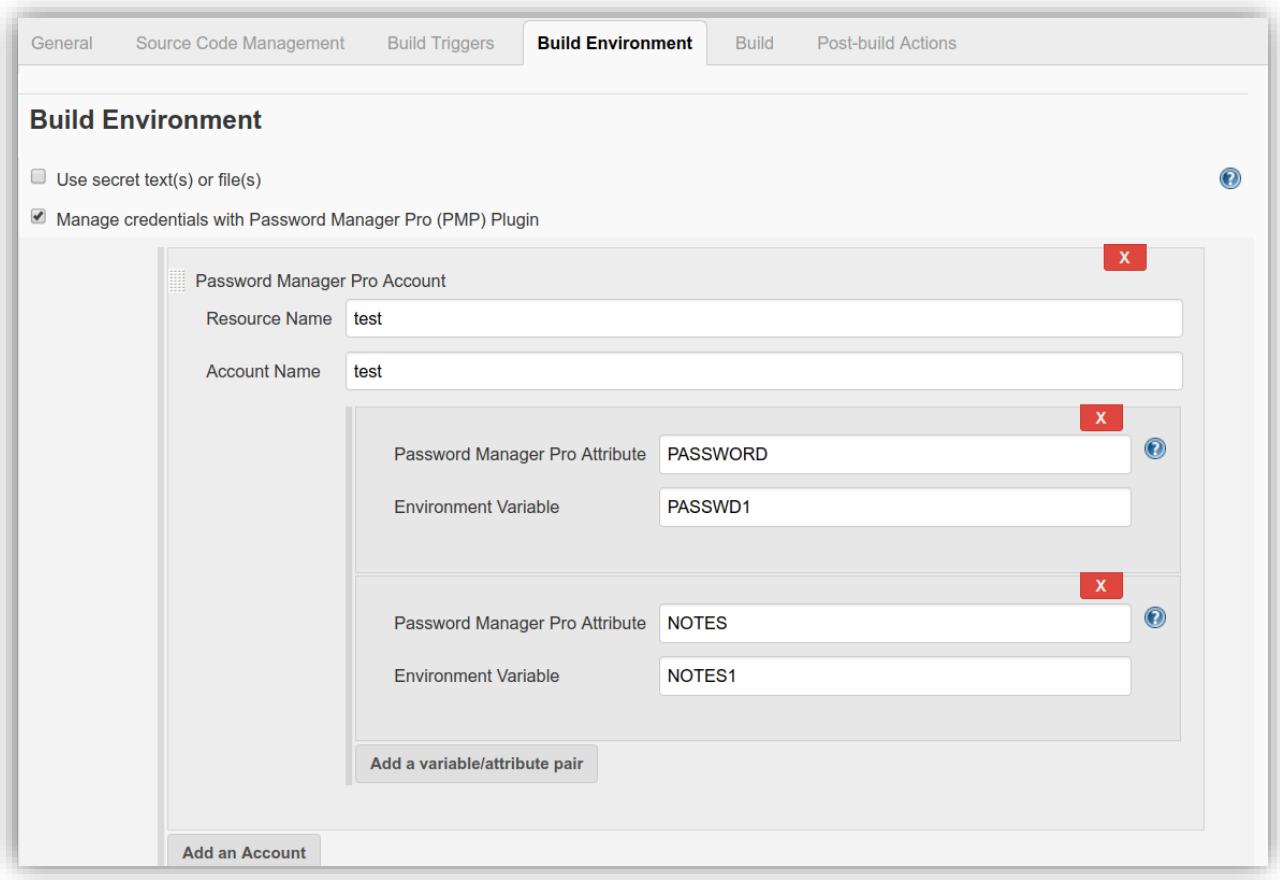
2.2 Enabling the Plugin

1. Navigate to **Manage Jenkins >> Configure System**.
2. In the UI that loads, scroll down to locate the PAM360 plugin section.
    i. **PAM360 URL:** Enter the URL to your PAM360 instance, in the format **https://<hostname>:<portnumber>**
    ii. **PAM360 AUTH Token:** Here, copy and paste the AUTH Token generated earlier in PAM360's interface. Please note that the AUTH Token entries in both PAM360 and Jenkins should always match for successfully plugin configuration and password retrieval.
    iii. **Save** the changes to enable and start using the PAM360 plugin in Jenkins.

3. Retrieving Passwords from PAM360 for Jenkins' Freestyle Project Jobs

At present, the plugin can be used to retrieve required credentials from PAM360 for Jenkins' freestyle project jobs. This requires adding various PAM360 attributes such as resource name, account name, and password while configuring the job. Upon this attribute configuration at job level, the value of these PAM360 attributes will be available as 'Environmental Variables' during job execution. When Jenkins connects to PAM360 to retrieve a specific password, the environmental variables will be how the former identifies the required values in the latter. Below is a step-wise explanation of the actions involved:

1. Once you create a specific freestyle project job, you can find an option to use the PAM360 plugin for that job under its 'Build Environment' section.
2. Enable the check box beside **Manage credentials with PAM360 Plugin** and click **Add an Account.**
3. In the **Resource Name** and **Account Name** fields, specify the respective names of the resource and its account that you want Jenkins to fetch from PAM360.



4. The next step is creating variable-attribute pairs, using which Jenkins will retrieve the required values from PAM360. To create a pair, first refer to the list of available PAM360 attributes given below and specify the required attribute in the **PAM360 Attribute** field. Then add a desired name for the **Environment Variable**, for which the value of the corresponding PAM360 attribute will be automatically assigned.
5. Click **Add a variable/attribute pair** to include all the required PAM360 attributes in a similar fashion and then save the configuration. The plugin is now ready for use in Jenkins.

4. List of Available PAM360 Attributes

- RESOURCE_NAME
- RESOURCE_DESCRIPTION
- OPERATINGSYSTEM
- DNSNAME
- DEPARTMENT
- LOCATION
- RESOURCE_URL
- ACCOUNTNAME
- NOTES

- PASSWORD
- Resource-level and account-level additional fields, excluding file-based additional fields.

PAM360 Plugin for Ansible

Ansible is a popular open source orchestration tool provided by Red Hat, which helps organizations automate their configuration management and similar repetitive processes. Ansible users can create instructions for a routine task in the form of a 'playbook' that is basically an automation schedule. Execution of these playbooks more often than not require user credentials and similar sensitive information like privileged passwords, API keys, and access tokens to interface with other systems, applications, and services in the environment. In most DevOps environments, such credentials are stored in plaintext within the playbooks to enable smooth task execution without service delays, which can lead to many security and management issues.

The PAM360 lookup plugin developed for secrets management in Ansible helps improve security in organizations' DevOps pipeline. The plugin once enabled in Ansible, ensures that required credentials are retrieved from PAM360's vault every time when a play is executed, instead of being embedded in plain text within the written template. Upon secure retrieval, the credentials can then be used for actions such as connecting to a remote server. The plugin also saves the user from the arduous job of having to manually update the password/SSH key in the playbooks every time there's an update. Often, there are instances when a play fails owing to an outdated credential in the template. Now with the credentials stored in PAM360, they're regularly rotated in the vault and also updated in the respective remote device, which ensures that only the latest passwords or keys are retrieved from the vault while running plays.

1. Steps to Configure PAM360 Plugin for Ansible

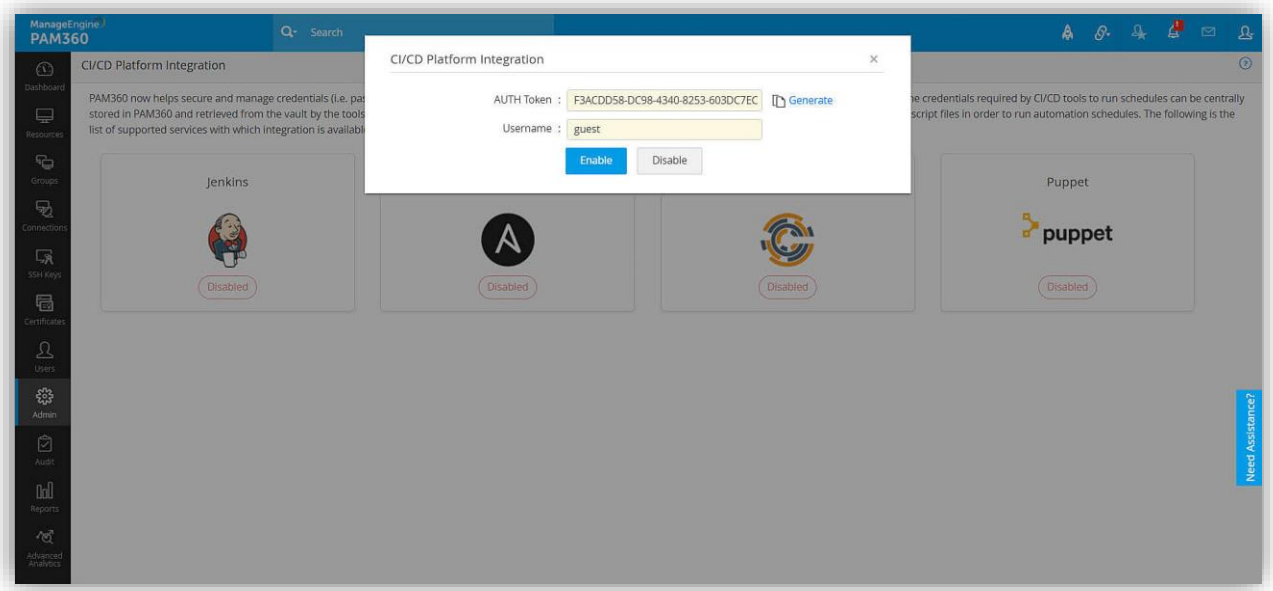
The following are the major two steps involved in getting set up and starting to manage secrets in Ansible with PAM360.

Step 1: Enabling Ansible integration in PAM360

Step 2: Activating the plugin in Ansible playbooks

1.1 Enabling Ansible Integration in PAM360

1. Log in to PAM360 and navigate to **Admin >> Integration >> CI/CD Platform Integration.**
2. Click on the **Ansible** option.
3. **AUTH Token:** Click on '**Generate**' to populate an AUTH Token automatically. This will be required later while configuring the plugin in Ansible playbooks. Once set up, all incoming connections from Ansible will be validated by PAM360 using this AUTH token.



4. **Username**: Here, enter the username of an active PAM360 user whose account will be used automatically by Ansible to securely retrieve the required passwords from PAM360's vault.

> **Important Note**: Ensure that the PAM360 user account you provide has the minimum required permissions for this workflow i.e. privilege to view/retrieve the passwords of resources to which Ansible has to connect. The passwords of resources owned by and shared to this user are the only credentials that Ansible will have access to in PAM360.

5. Click **Enable.**

1.2 Activating the Plugin in Ansible Playbooks

Basically, the PAM360 plugin is called a 'lookup plugin' in Ansible's terms. As an Ansible user, you'll be able to activate this custom lookup plugin by adding it to the lookup folder within the Ansible's installation directory. Once added, you can configure your playbooks to trigger the plugin whenever the play execution requires a set of credentials and the plugin will in turn connect to PAM360 to retrieve the required password or key.

> **Note:** PAM360's Ansible Lookup plugin works with **Ansible python version 3 and above** only.

Given below are detailed steps to achieve credential management workflow in Ansible using

PAM360's lookup plugin.

1. First, download the lookup plugin here. Extract the plugin Python script(.py) from the zip **(SHA256: 3164196bf9feba013367740ae225ffb233ba3977212718db8e5208bf39ea0a32)**.
2. Now go to Ansible's installation directory and trace the following path: **ansible/lib/ansible/plugins/lookup.**
3. In the lookup folder, drop the plugin file.
4. Restart the Ansible service.
5. Once the service is up again, open a playbook that has embedded credentials and remove the plain text credentials. In their place, add a command to invoke the PAM360 lookup plugin to connect to PAM360 and retrieve those credentials securely from the vault.
6. The command should also specify the names of the resource and account that the plugin should check out from PAM360.
7. The command to invoke the plugin should be configured in the playbook in the following format:

   {{ lookup('pam360', 'RESOURCENAME', 'ACCOUNTNAME')}}

8. Repeat the above step for every playbook that requires privileged credentials. During this process, ensure that every resource and account names that you specify are added to PAM360's vault beforehand.
9. After you've made necessary changes in the required playbooks, configure PAM360's URL and the AUTH Token generated earlier as environmental variables in Ansible.
   - **PAM360_URL**
   - **PAM360_AUTHTOKEN**
10. You're now all set up now and ready to begin credential management in Ansible using PAM360.

PAM360 Plugins for Chef and Puppet

Chef

1. Introduction to Chef

Chef is a ruby-based configuration management tool that provides a way to define infrastructure as code (IAC) wherein managing infrastructure is made simple through writing code rather than using manual processes. Chef operates using a Client-Server architecture.

The PAM360 lookup plugin developed for Chef helps improve security and ease of Password Management in an organization's DevOps pipeline. Once imported into Chef, the PAM360 plugin can fetch credentials and account information directly from the PAM360 vault during Chef cookbook runtime, thus eliminating the need to use hard-coded credentials. Upon secure retrieval, the credentials can then be used for actions such as connecting to a remote host. The credentials stored in PAM360 are regularly rotated in the vault and also updated in the respective remote device; this ensures that only the latest passwords or keys are retrieved from the vault when the Chef plugin is invoked.

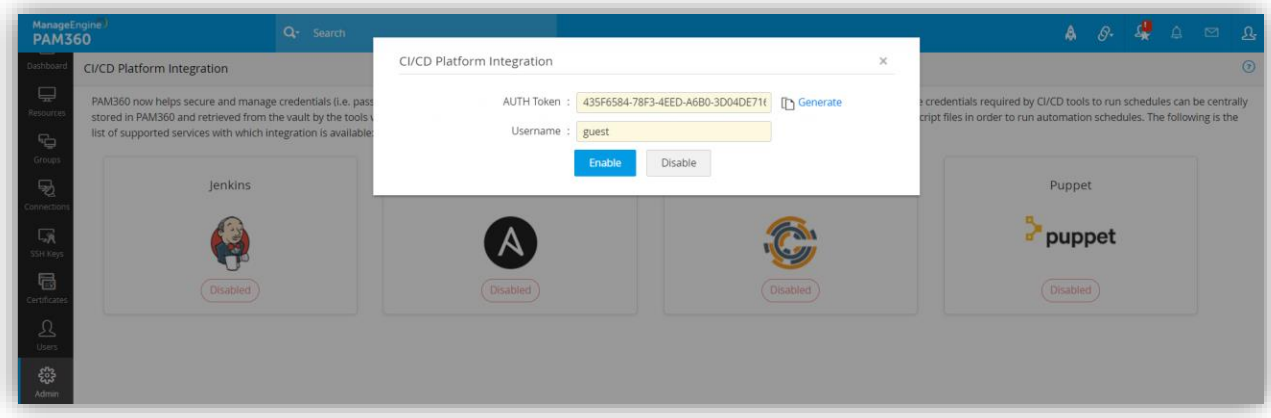
2. Steps to Set Up the PAM360 Plugin for Chef

The following are the steps to set up and manage sensitive credentials in Chef with PAM360.

1. Enabling Chef integration in PAM360.
2. Invoking the PAM360 plugin in the Chef cookbooks.

2.1 Enabling Chef Integration in PAM360

1. Log in to PAM360 and navigate to **Admin >> Integration >> CI/CD Platform Integration.**
2. Click the **Chef** option.
3. In the CI/CD Platform Integration window, click **Generate** to populate an AUTH Token automatically. This will be required later while invoking the plugin in the Chef cookbooks. Once set up, all incoming connections from Chef will be validated by PAM360 using this AUTH token.



4. Enter the username of an active PAM360 user. PAM360 will map the auth token to this user account and it will be used to retrieve required passwords from PAM360's vault. Once PAM360 maps the auth token to this user, the resources owned/shared to this user can also be accessed using this auth token.
5. Click **Enable**.

> **Note:** Ensure that the PAM360 user account you provide has the minimum required permissions for this workflow i.e. privilege to view/retrieve the passwords of resources which Chef has to connect to. The passwords of resources owned by and shared to this user are the only credentials that Chef will have access to in PAM360.

2.2 Invoking the PAM360 Plugin in Chef

Import PAM360's ruby gem into your Chef cookbooks by executing the following:

2.2.1 Initialize the PAM360 Class Object with Credentials

syntax:gemData = PAM360Gem.new("Hostname","Auth token",Path,port number)

Wherein,

- Host name = The PAM360 hostname of the account whose username was provided in Step 2.1.
- Auth Token = The respective auth token generated in Step 2.1.
- Path = Path to SSL certificate of the PAM360 server.
- Port number = The port number used for your PAM360 server. You need to specify this only if the port used is not the default PAM360 port 8282.

2.2.2 Methods To Be Applied to the Chef Cookbook to Invoke the PAM360 Plugin

gemData.getAccountPassword("resource name","account name")

This method fetches the account password as a string.

gemData.getAccountDetails("resource name","account name")

This method returns the resource and account details in the array of JSON format.

Puppet

1. Introduction to Puppet

Puppet is a ruby-based configuration management tool similar to Chef. Puppet also operates using a Client-Server architecture in which the Master and Slave communicate through a secure encrypted channel with the help of SSL. Puppet is mainly used for deploying, configuring and managing servers. Similar to Chef, the PAM360 lookup plugin can retrieve passwords from PAM360's vault when invoked.

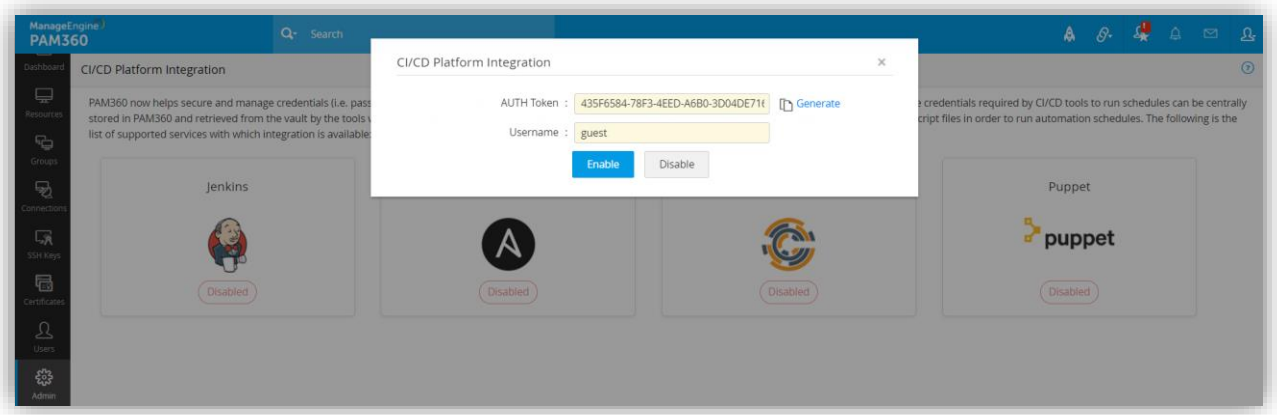
2. Steps to Set Up the PAM360 Plugin for Puppet

The following are the steps to set up and manage sensitive credentials in Puppet with PAM360.

1. Enabling Puppet integration in PAM360.
2. Invoking the PAM360 plugin in Puppet.

2.1 Enabling Puppet Integration in PAM360

1. Log in to PAM360 and navigate to **Admin >> Integration >> CI/CD Platform Integration.**
2. Click the **Puppet** option.
3. In the CI/CD Platform Integration window, click **Generate** to populate an AUTH Token automatically. This will be required later while invoking the plugin in Puppet. Once set up, all incoming connections from Puppet will be validated by PAM360 using this AUTH token.



4. Enter the username of an active PAM360 user. PAM360 will map the auth token to this user account and it will be used to retrieve required passwords from PAM360's vault. Once PAM360 maps the auth token to this user, the resources owned/shared to this user can also be accessed using this auth token.
5. Click **Enable**.

> **Note:** Ensure that the PAM360 user account you provide has the minimum required permissions for this workflow i.e. privilege to view/retrieve the passwords of resources which Puppet has to connect to. The passwords of resources owned by and shared to this user are the only credentials that Puppet will have access to in PAM360.

2.2 Invoking the PAM360 Plugin in Puppet

Import PAM360's ruby gem into Puppet by executing the following:

2.2.1 Initialize the PAM360 Class Object with Credentials

syntax:gemData = PAM360Gem.new("Hostname","Auth token",Path,port number)

Wherein,

- Host name = The PAM360 hostname of the account whose username was provided in Step 2.1.
- Auth Token = The respective auth token generated in Step 2.1.
- Path = Path to SSL certificate of the PAM360 server.
- Port number = The port number used for your PAM360 server. You need to specify this only if the port used is not the default PAM360 port 8282.

2.2.2 Methods To Be Applied to Puppet to Invoke the PAM360 Plugin

getAccountPassword(resourceName,AccountName)

This method fetches the account password as a string.

getAccountDetails(resourceName,AccountName)

This method returns the resource and account details in the array of JSON format.

Sample Codes

1. Sample Code to Fetch Resource and Account Details using the PAM360 Plugin

The following are the sample input and output codes and the corresponding sample responses to fetch the account details using the PAM360 plugin. The sample codes remain the same for both Chef and Puppet.

Sample Input

```
gem 'PAM360_Gem'

require 'PAM360_Gem' gemData = PAM360Gem.new("localhost","060CCDB8-71A0-4B8B-AC57-XXXXX","/home/local/user/servercertificate")

# resourcename = Windows accountname = useraccount1

puts("resourcedetails\n")

result = gemData.getAccountDetails("Windows ","useraccount1"))

puts(result[0])

puts("accountdetails\n")

puts(result[1])
```

Sample Output

```
resource details
{"RESOURCE_ID":1,"RESOURCE_NAME":"Windows","RESOURCE_DESCRIPTION":"","OPERATINGSYSTEM":"Windows","DNSNAME":"","DEPARTMENT":"","LOCATION":"","RESOURCE_URL":""} account details
{"ACCOUNTNAME":"useraccount1","PASSWORD":"Test@123"}
```

2. Sample Code to Fetch the Password using the PAM360 Plugin

The following are the sample input and output codes and the corresponding sample responses to fetch the password using the PAM360 plugin. The sample codes remain the same for both Chef and Puppet.

Sample Input

```
gem 'PAM360_Gem'

require 'PAM360_Gem'

gemData = PAM360Gem.new("localhost","060CCDB8-71A0-4B8B-AC57-XXXXX","/home/local/user/servercertificate")

# resourcename = Windows accountname = useraccount1

puts("accountpassword\n")

puts(gemData.getAccountPassword("Windows ","useraccount1"
```

Sample Output

```
accountpassword
Test@123
```

For more information on Chef and Puppet, refer to the following links:

Chef: https://www.chef.io

Puppet: https://puppet.com/

Integrating PAM360 with other ManageEngine Products

Integrating different IT functionalities enables determining, accessing and sharing the best available features among the available key IT management solutions. Though it's not essential to integrate each IT function with one another, doing it contextually eliminates duplicate actions and redundancies, thereby improving efficiency.

PAM360 offers robust, native integrations with industry-leading apps from ManageEngine to manage the shared sensitive information such as account credentials, passwords, etc. PAM360 integration dismisses the need for your password users to spend much time bungling with login screens and allows them to concentrate on what matters. It eliminates the need to manually update & maintain the credentials individually in each ManageEngine product, as PAM360 exclusively takes care of performing the periodic password rotation of all such credentials and updating the same in the native products.

The scope and benefits of integration differ based on the product integrated and its functionalities. Still, the basic idea behind the integration is to manage shared sensitive information such as account credentials, passwords, etc. Read further to know about how the integration works for each product.

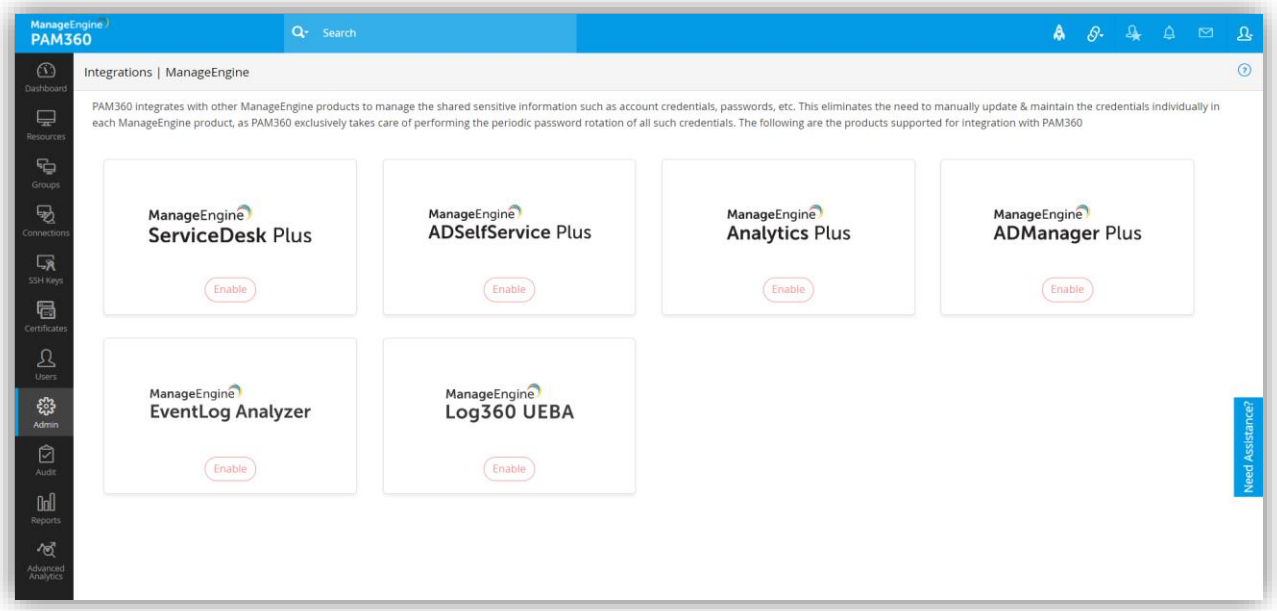
ManageEngine Products Integrated with PAM360

PAM360 integrates with the below products:

1. **ManageEngine Servicedesk Plus (SDP)**
2. **ManageEngine ADSelfService Plus (ADSSP)**
3. **ManageEngine Analytics Plus**
4. **ManageEngine ADManager Plus**
5. **ManageEngine EventLog Analyzer**
6. **ManageEngine Log360 UEBA**

Navigate to **Admin >> Integration >> ManageEngine.** You will see a consolidated view of all ManageEngine products integrated with PAM360:

> Only the users with the "**ManageEngine Integration"** role will see the **ManageEngine** option under **Integration**.


ManageEngine
PAM360
Search
Integrations | ManageEngine
Dashboard
Resources
Groups
Connections
SSH Keys
Certificates
Users
Admin
Audit
Reports
Advanced Analytics
PAM360 integrates with other ManageEngine products to manage the shared sensitive information such as account credentials, passwords, etc. This eliminates the need to manually update & maintain the credentials individually in each ManageEngine product, as PAM360 exclusively takes care of performing the periodic password rotation of all such credentials. The following are the products supported for integration with PAM360
ManageEngine ServiceDesk Plus
Enable
ManageEngine ADSelfService Plus
Enable
ManageEngine Analytics Plus
Enable
ManageEngine ADManager Plus
Enable
ManageEngine EventLog Analyzer
Enable
ManageEngine Log360 UEBA
Enable
Need Assistance?

Integrating PAM360 with ManageEngine ServiceDesk Plus

The following topics are discussed in this document:

1. Key Benefits
2. Prerequisites
3. Configuration Steps
4. Viewing Configuration Details
5. How Do Technicians Benefit from the Integration?

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine ServiceDesk Plus (SDP), a web-based Help Desk and Asset Management software. Organizations use helpdesk software such as the SDP to deliver customer service and manage their internal IT perfectly.

Technicians using SDP often need to access target machines (or resources) manually to resolve issues, which involves security-related challenges, such as sharing sensitive passwords for authentication, etc., especially while using the privileged accounts. They also had the pain of jumping between machines to perform different tasks. With this integration, accessing the remote systems from the ServiceDesk Plus portal is just a click away for the Technicians. Administrators can now provide the advantage of secure remote access to the target machines (or resources) only to the authorized Technicians, without sharing the credentials. The Technicians can remotely access the target endpoints (or resources) from the ServiceDesk Plus portal without having to log in to PAM360 each time to fetch the credentials.

2. Prerequisites for Performing the Integration

Before commencing the integration, verify if all of the below prerequisites are satisfied:

1. All the configurations related to the PAM360-SDP integration can be done from the **SDP portal**. Hence, make sure you have access to an active SDP portal.
2. The SDP Technician should also be a PAM360 user, with the same **User Name** in both the applications. Using Active directory integration will ensure that the same username is

present in both the products.

3. PAM360 should be accessible from the server on which SDP is running. To verify this, try launching your PAM360 web-client from the SDP server.
4. The Authentication token (**Auth Token**) generated during the integration process is specific to your ServiceDesk Plus instance, and will be displayed only once. Hence, make sure you copy the Auth Token as you need to paste it in the required field in the PAM360 portal.

3. Configuration Steps

All the configurations related to the PAM360 - ServiceDesk Plus integration can be performed from the ServiceDesk Plus console only.

> From ServiceDesk Plus build 13000 onwards, it is required to deploy the PAM360's SSL certificate in the SDP installation directory to complete the integration process. Follow these steps to complete the SSL certificate deployment process.

From the PAM360 console, you can view the configuration details and regenerate the AuthToken.

Once you have finished configuring the integration, you will be able to remotely access the accounts in target endpoints (or resources), without having to enter the credentials.

Note:

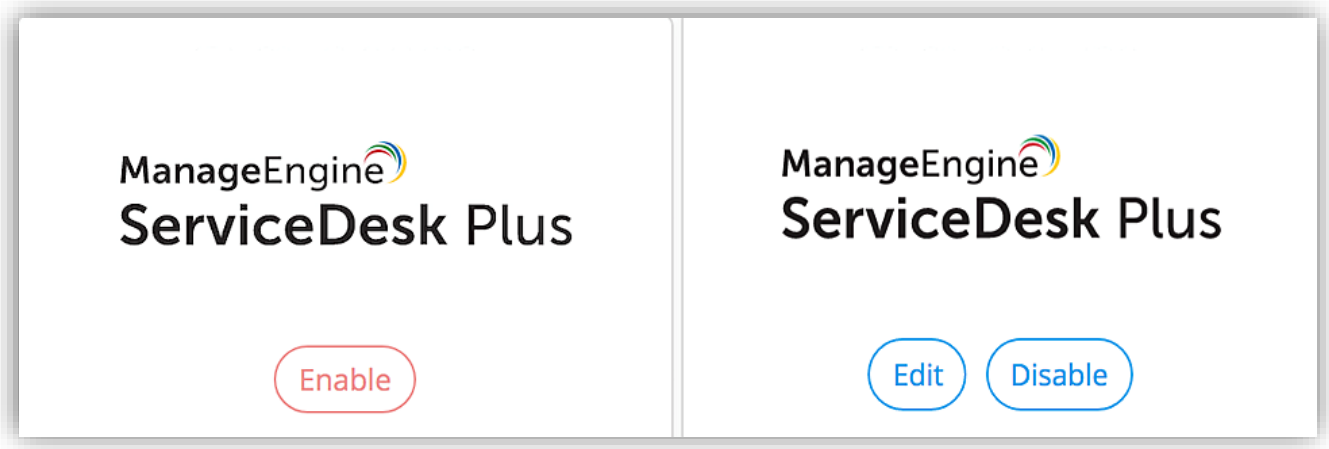
1. If the integration is not successful, first verify if the server is reachable. Then, follow the below steps:
   i. Navigate to the **<PAM360_Installation_Folder>/logs** directory and open the **pam0** file.
   ii. Search for **remoteHost in api filter** and try pinging the value/IP address corresponding to it.
   iii. If the server is not reachable using the IP address, then determine the correct IP/DNS, using which you can ping the server from the PAM360 installation machine.
   iv. If the problem persists, please contact PAM360 support.
2. ServiceDesk Plus does not support launching remote sessions to resources for which Remote App-only access is enabled in PAM360.

4. Viewing the Configuration Details

Once you are done with configuring the integration, you can view the configuration details from the PAM360 console. Navigate to **Admin >> Integration >> ManageEngine**. You will see the **Integrations | ManageEngine** page.

Note: Only the users with the **"ManageEngine Integration"** role will see the **ManageEngine** option under **Integration**.

In the **Integrations | ManageEngine** page, you will see the **ServiceDesk Plus** block that looks like any of the below images based on whether integration is enabled or disabled:



Buttons and Definitions:

Sl. No:	Button	Definition
1	**Enable**	You will see this option if the integration is disabled. Click this button and you will be notified with a message to set up the integration from the SDP portal.
2	**Edit**	Click this button, and the ServiceDesk Plus Integration window pops up.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

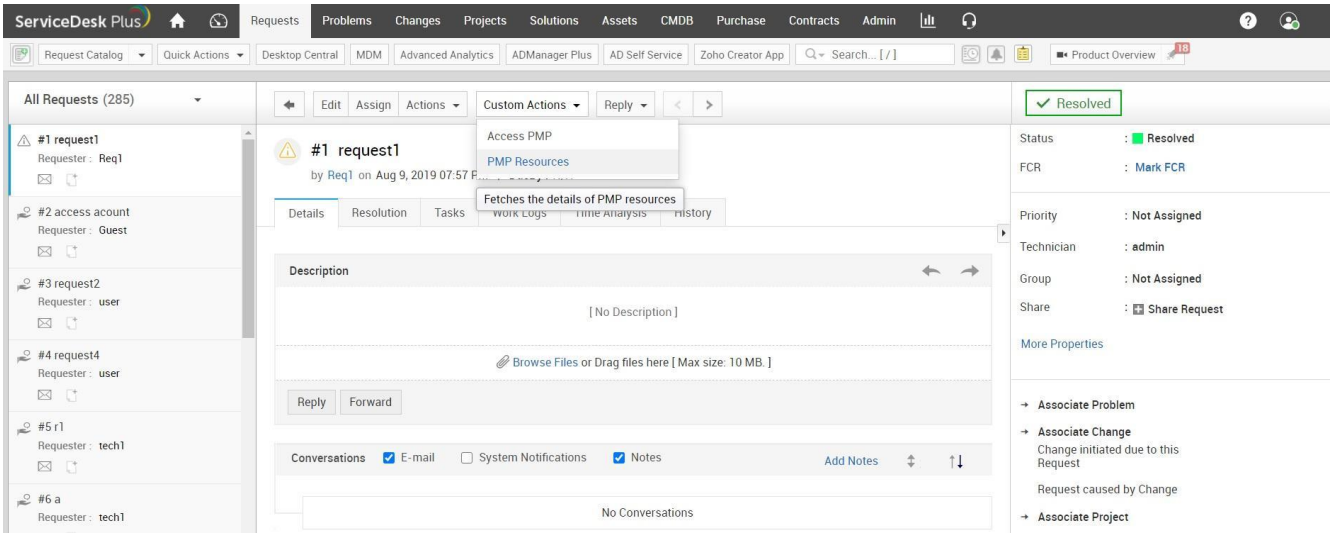
From the **ServiceDesk Plus Integration** window, you will be able to do the following:

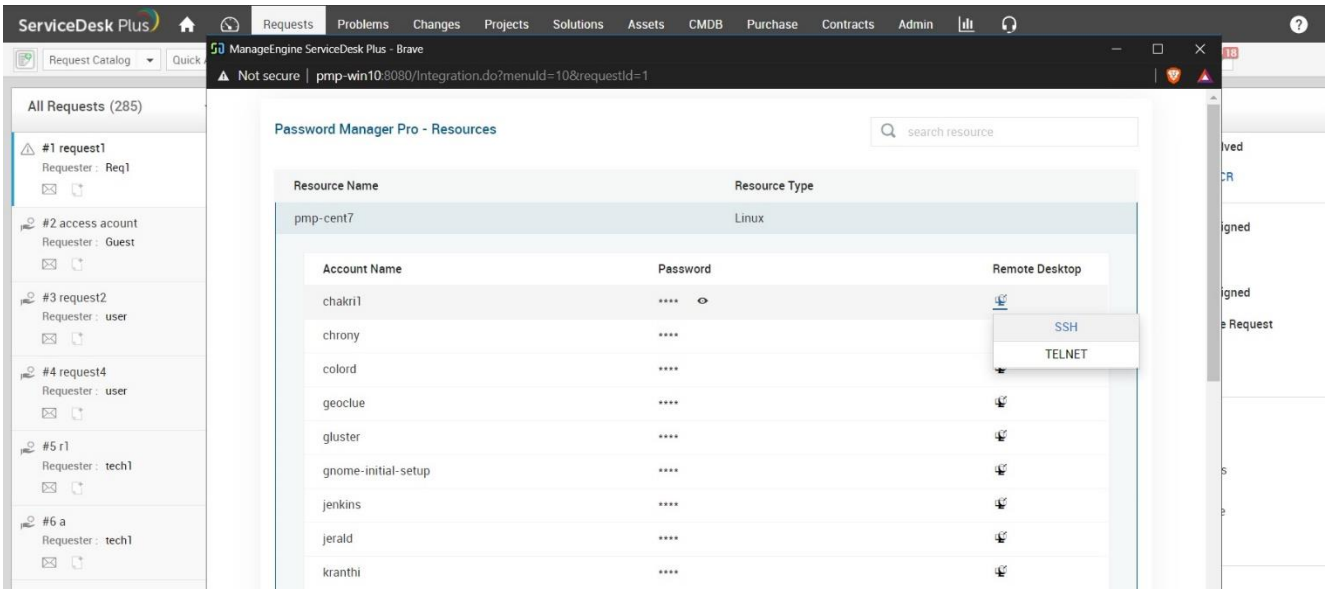
1. **View** the configuration details that include:
   - **Auth Token:** The available Auth Token will be hidden and you will see only a "Auth Token Available" message in this field.
   - **Host Name**: The DNS name of the machine, where ServiceDesk Plus is hosted.
   - **Port Number**: The port number on which ServiceDesk Plus is listening.
2. Click the **Regenerate button** to generate a new Auth Token.
3. Click **Update** to save the changes.

You can generate any number of Auth tokens from here. This option comes handy if you have lost the Auth Token that was generated during the initial configuration process. Whenever you generate a new Auth token, click **Update** for the change to take effect.

5. How Do Technicians Benefit from the Integration?

After the successful completion of the integration and configuring the required actions from the ServiceDesk portal, you can access the PAM360 portal and view the resources using the Custom Actions menu on the Request Details page, as shown below:





Using these options, the Technicians can remotely access the Windows server via RDP, and Linux and Mac machines over Telnet or SSH.

Integrating PAM360 with ManageEngine ServiceDesk Plus Cloud

By integrating PAM360 with ManageEngine ServiceDesk Plus (SDP) Cloud, technicians can access target endpoints for privileged sessions to resolve the issues easily. This integration ensures data security by eliminating the need to share sensitive passwords and allowing technicians to access remote systems directly from the ServiceDesk Plus Cloud portal with a single click. Administrators can ensure that only authorized technicians with the request have access to privileged accounts without sharing credentials. This integration also eliminates the need for technicians to switch between platforms constantly, enhancing efficiency and security in IT management workflows.

Required Roles in PAM360

Any of the below roles is required to perform the integration process:

i. Privilege Administrator
ii. Administrator
iii. Password Administrator
iv. Any custom role with 'ManageEngine Integration' privilege enabled

At the end of this document you will learn about following process involved in integrating PAM360 with ServiceDesk Plus cloud

1. Prerequisites
2. Installing the Probe to Establish Communication between PAM360 and SDPOD
3. Installing a PAM360 Extension to Integrate PAM360 with the ServiceDesk Plus Cloud
4. How Do Technicians Benefit from the Integration?

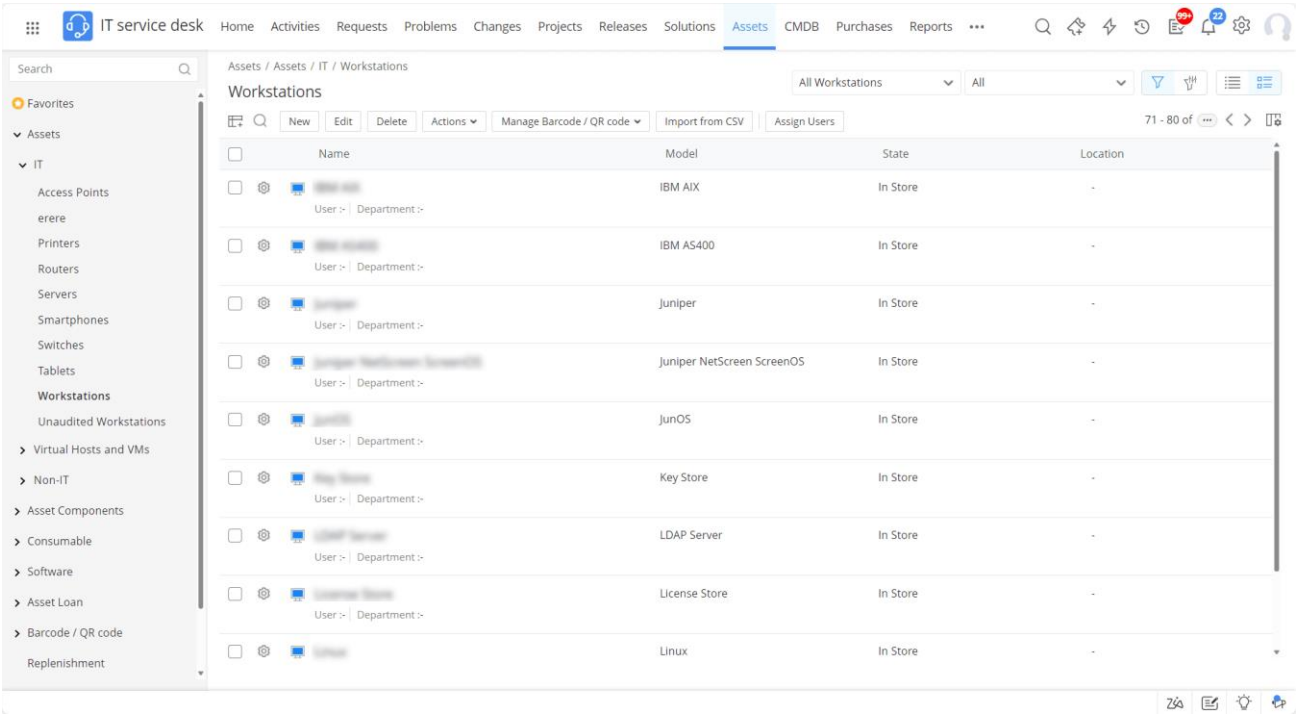
1. Prerequisites

Before commencing the integration, verify if all of the below prerequisites are satisfied.

i. Access to an active SDP Cloud portal for configuration.
ii. Technicians using SDP Cloud must also be PAM360 users with identical email ID on both platforms.

iii. Privileged resources present in the PAM360 application should be added as workstations under **Assets >> IT >> Workstations** in the ServiceDesk Plus Cloud.

- The resource name of PAM360 and the workstation name of SDP cloud should be the identical (including case-sensitive) to make a privileged remote session from ServiceDesk Plus Cloud.
- You can add the required resources from PAM360 to the SDP cloud, individually or in bulk, using the Import from CSV feature.



iv. SDP Cloud and PAM360 on-premise applications only communicates using probe, so a probe installation is required to establish the communication.

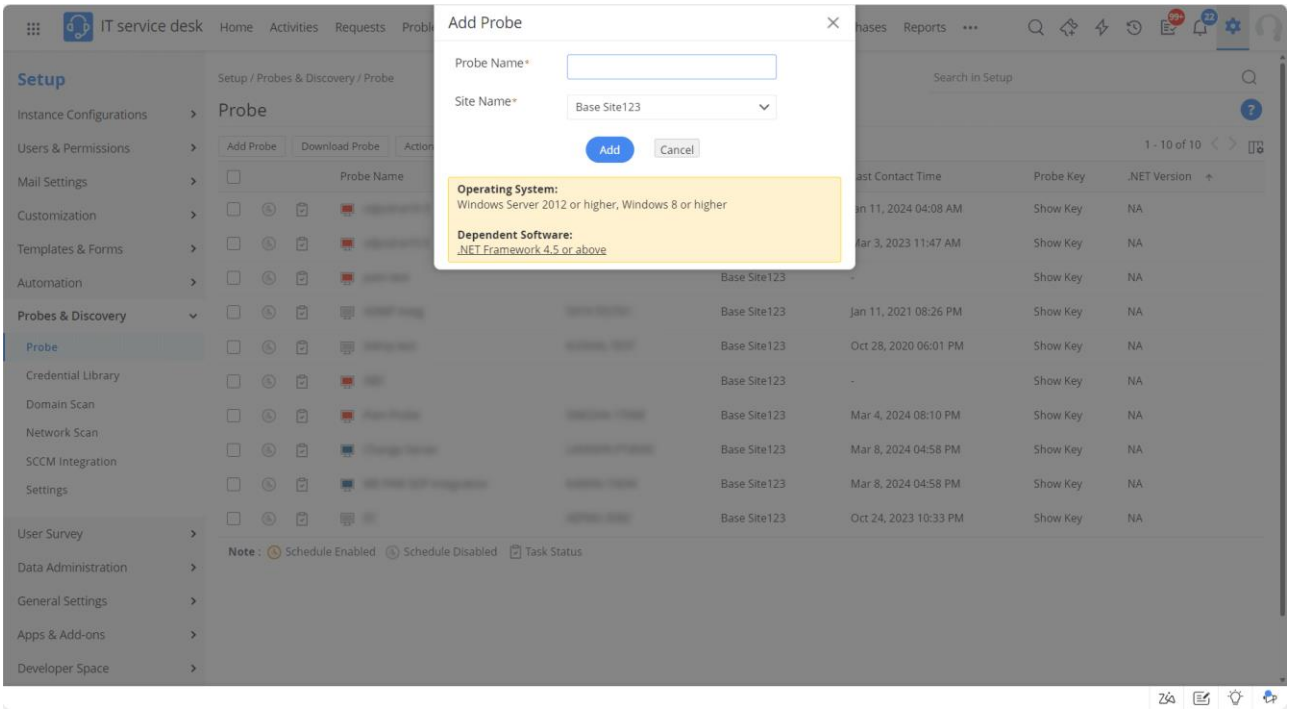
v. Remember to copy the Authentication Token (Auth Token) generated during integration as it's specific to your ServiceDesk Plus Cloud instance.

2. Installing the Probe to Establish Communication between PAM360 and SDPOD

Since PAM360 is an on-premise application, a remote probe application must be installed on a server that resides in the LAN of the PAM360 server to connect with the cloud version of ServiceDesk Plus. To install a remote probe application in the PAM360 server, follow these steps:

1. Log in to the ServiceDesk Plus Cloud application and navigate to **Setup >> Probes & Discovery >> Probe**.

2. Click **Add Probe** to add a new probe for PAM360 integration.
3. Provide the **Probe Name** as **Pam Probe** and click **Add**.



4. Upon adding the probe, click **Show Key** and copy the probe key for further installation process.
5. Now, download the probe using the **Download Probe** button from the top pane and execute the downloaded .msi file in the PAM360 server to install the probe.
6. After successful installation, provide the probe key copied previously to register. If you are using a proxy server, then provide proxy server details such as proxy host and proxy port, proxy username, and password.
7. Upon registering, the probe created in the ServiceDesk Plus cloud will become active for successful communication with the PAM360 server.

For more details on managing the Probe, refer to this ServiceDesk Plus cloud help document.

3. Installing a PAM360 Extension to Integrate PAM360 with the ServiceDesk Plus Cloud

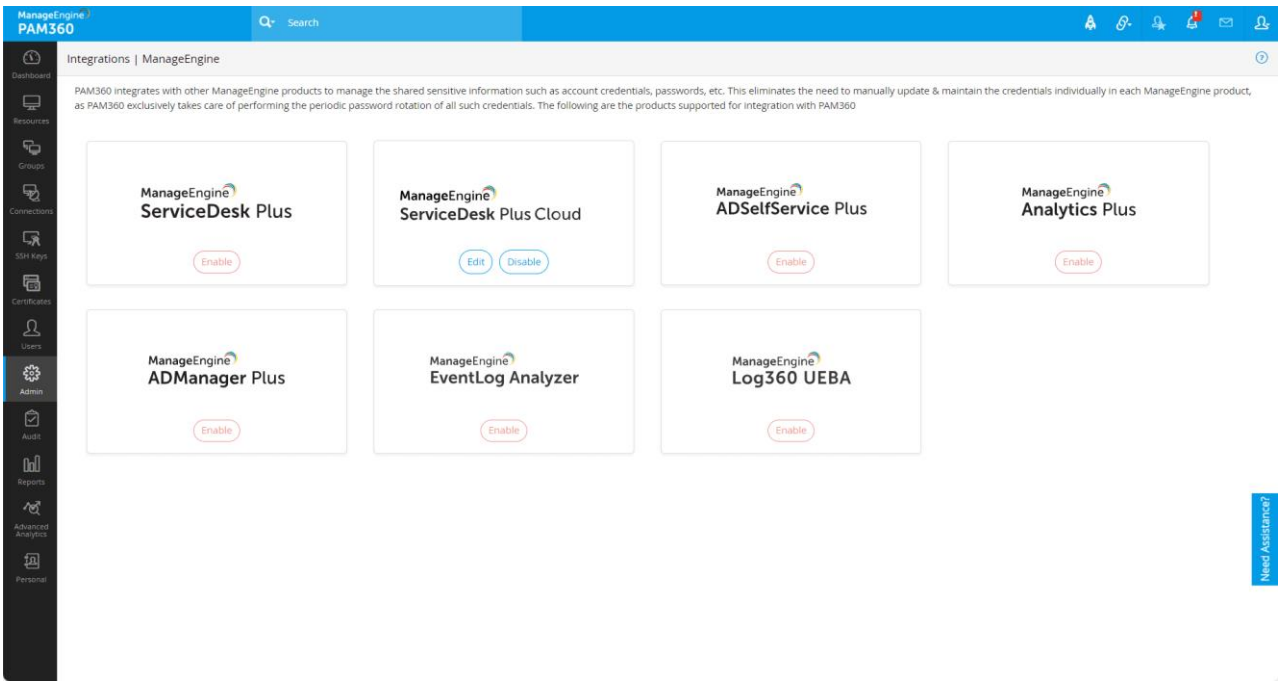
Upon completing the probe installation, a further PAM360 extension installation in the SDP cloud is required to complete the integration process. To do so, perform the following steps:

1. Log in to the PAM360 application and navigate to **Admin >> Integrations >> ManageEngine**.

2. In the page that appears, you will see the ServiceDesk Plus Cloud block with an integration enabled or disabled.

Sl. No:	Button	Definition
1	Enable	You will see this option if the integration is disabled. Click this button and you will be notified with a pop-up to set up the integration from the SDP Cloud portal.
2	Edit	Click this button, and the ServiceDesk Plus Cloud Integration window pops up for AUTH Token regeneration.
3	Disable	You will see this option if the integration is enabled. Click this button to disable the integration.

3. Click **Enable** to proceed with the integration process.

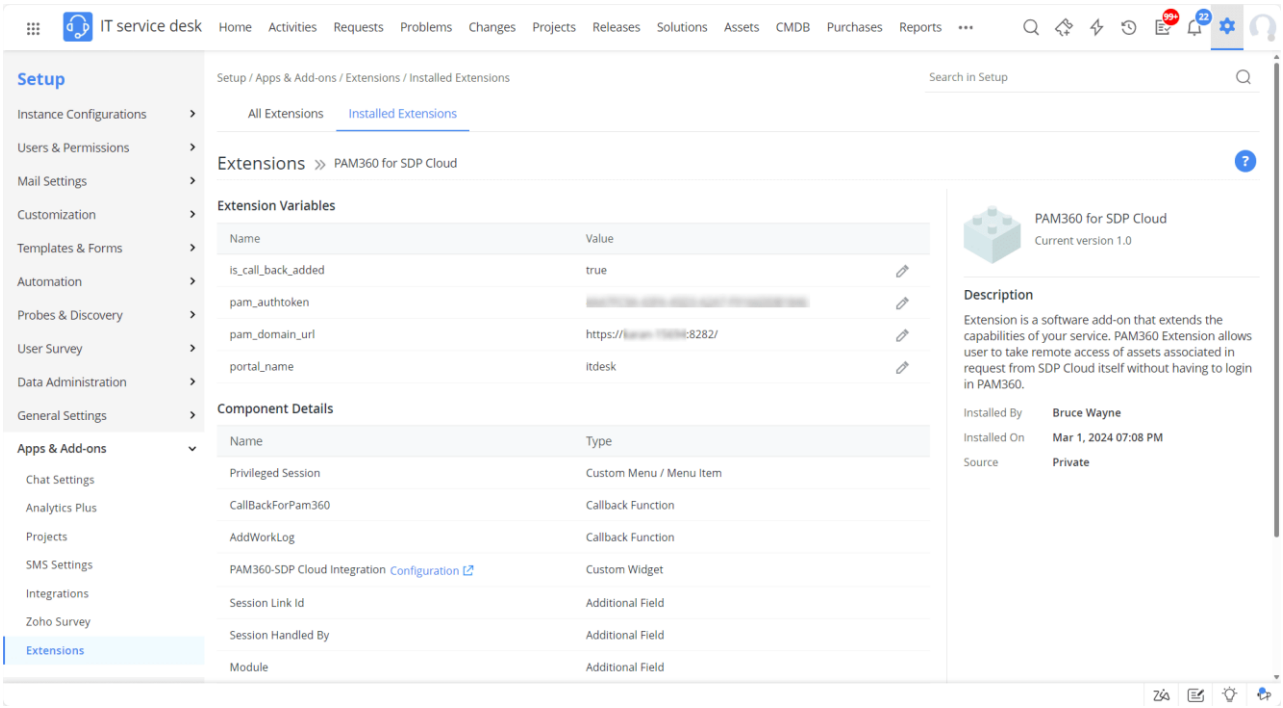


4. In the dialogue box that opens, click **Generate** to generate the AUTH Token for the PAM360-ServiceDesk Plus integration.
5. Copy the generated AUTH Token and click **Save**.
6. Now, log in to the ServiceDesk Plus Cloud application and navigate to **Setup >> Apps & Add-ons >> Extensions >> Installed Extensions**.
7. Click **Install Extension** to add PAM360 as the ready-to-use plugins and configurations.
8. In the dialogue box that opens, paste the below PAM360 extension URL and click Install.
   https://sdpondemand.manageengine.com/InstallPlugin.do?

uid=7a758699785469b2aa1579a71323942fab697ccd850a9c27c400356cb467c8bd559af8d63ebabb7f82dce7b94b1b941b&dc=US

You can also refer to this section on installing an extension in ServiceDesk Plus Cloud.

9. Upon successful installation, go to the Installed Extension and click on the PAM360 extension to update the **Extension Variables** with the PAM360 information.
10. In the window that appears, enter the **AUTH Token** copied from the PAM360 interface in the **pam_authtoken field**.
11. Enter the PAM360 service URL in the **pam_domain_url**.



Now, you have successfully integrated PAM360 with the SDP cloud application.

4. How this Integration Benefits?

Vision - To streamline the remote session process and to ensure that the technician has immediate access to the relevant asset/endpoint required to address the user's request directly from the SDP cloud interface.

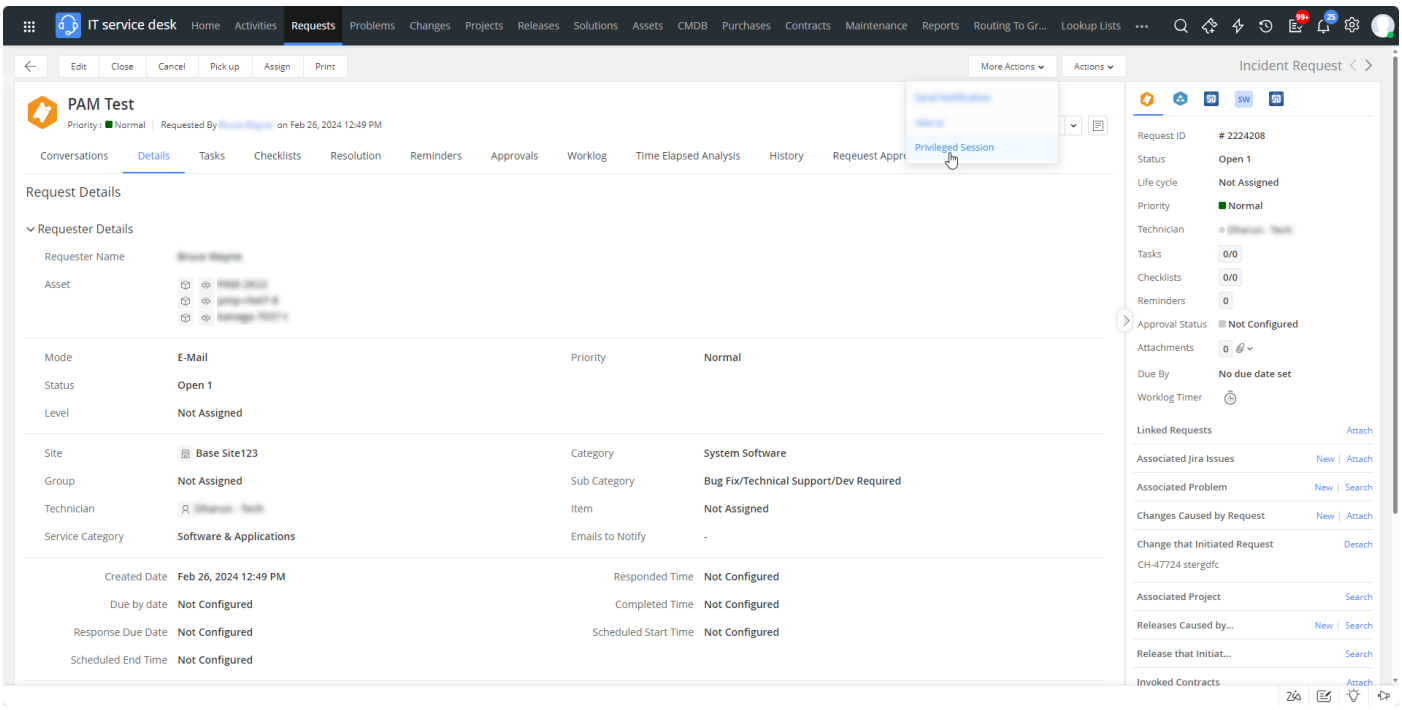
Scenario - A user in an organization creates a request in the IT service desk of the SDP cloud. While creating the request, the user mapped an asset (i.e., a privileged endpoint/machine) on which the request was to be handled.

Action After Request Creation - The request will automatically link the asset mapped by the user as a privileged resource for a remote session if it exists as a workstation in the SDP Cloud's asset section and as a resource in PAM360.

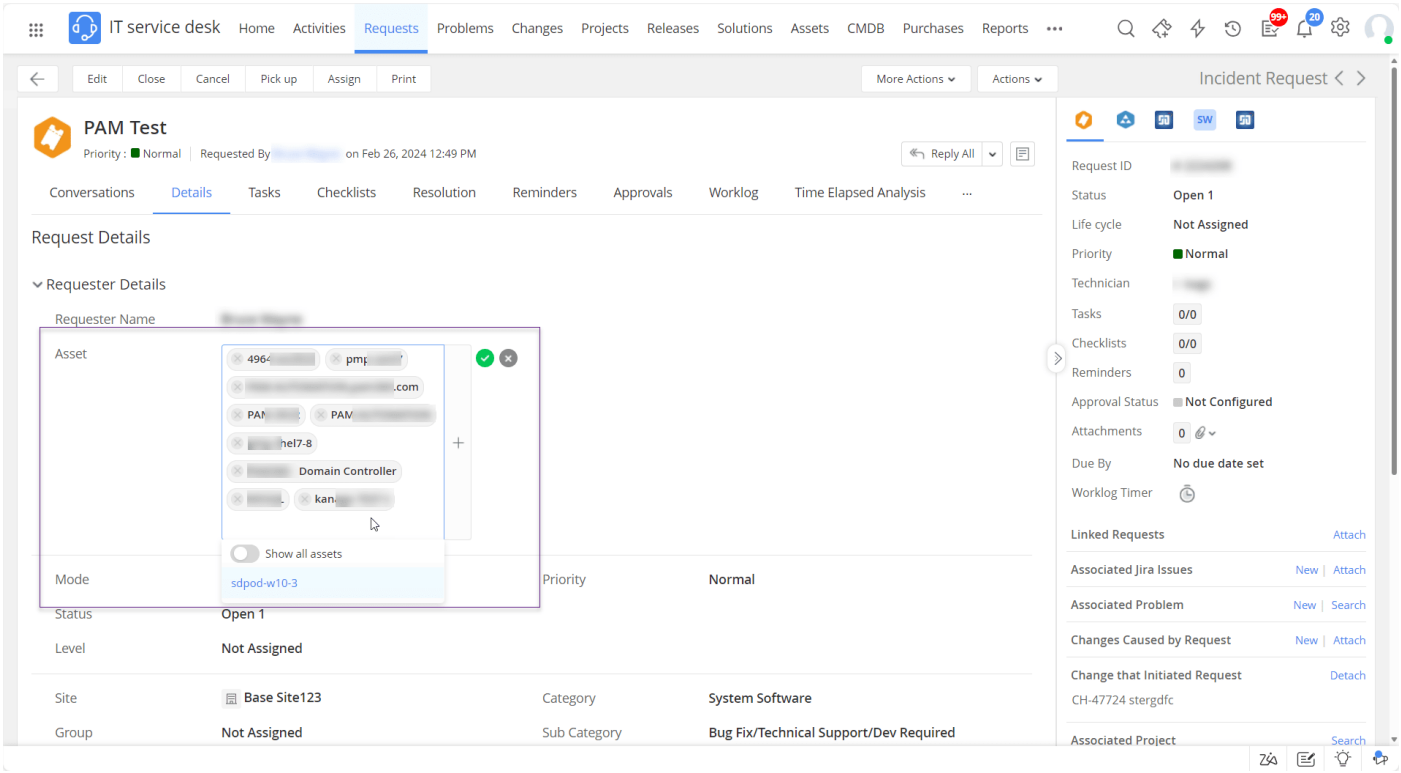
How this integration eases the technician for the above scenario?

To facilitate the necessary actions, such as troubleshooting/installation/maintenance, the technician requires privileged access to the target resource. With the active integration between PAM360 and SDP Cloud and the above-satisfied prerequisites, this is seamlessly achieved.

By navigating to the respective assigned request and selecting **More Actions** followed by **Privileged Session**, the technician can initiate a privileged remote session to the machine directly from the SDP cloud request interface. This integration not only enhances efficiency but also ensures secure and controlled access to critical resources, thereby empowering technicians to fulfill user requests effectively.



Note: If a user submits a request to install several applications on a group of machines belonging to a privileged group but provides only the name of the group instead of specifying individual assets in the request, the administrator or technician must manually associate the required group of machines as the assets with the request to facilitate the necessary privileged remote sessions.


IT service desk
Home
Activities
Requests
Problems
Changes
Projects
Releases
Solutions
Assets
CMDB
Purchases
Reports
Edit
Close
Cancel
Pick up
Assign
Print
More Actions
Actions
Incident Request
PAM Test
Priority : Normal
Requested By
on Feb 26, 2024 12:49 PM
Reply All
Conversations
Details
Tasks
Checklists
Resolution
Reminders
Approvals
Worklog
Time Elapsed Analysis
Request Details
Requester Details
Requester Name
Asset
Domain Controller
Show all assets
sdpod-w10-3
Mode
Priority
Normal
Status
Open 1
Level
Not Assigned
Site
Base Site123
Category
System Software
Group
Not Assigned
Sub Category
Bug Fix/Technical Support/Dev Required
Request ID
Status
Open 1
Life cycle
Not Assigned
Priority
Normal
Technician
Tasks
0/0
Checklists
0/0
Reminders
0
Approval Status
Not Configured
Attachments
0
Due By
No due date set
Worklog Timer
Linked Requests
Attach
Associated Jira Issues
New | Attach
Associated Problem
New | Search
Changes Caused by Request
New | Attach
Change that Initiated Request
Detach
CH-47724 stergdfc
Associated Project
Search

Integrating PAM360 with ManageEngine ADSelfService Plus (ADSSP)

This document walks you through the procedure for integrating PAM360 with ManageEngine ADSelfService Plus (ADSSP).

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine ADSSP, an integrated web-based self-service password management and Single-Sign-On solution. ADSSP assists domain users in performing activities such as self-service password reset, self-service account unlock, etc. ADSSP utilizes PAM360 to manage its domain controller passwords, especially the privileged accounts.

Earlier, when remote password reset of the ADSSP privileged domain account was performed in PAM360, the new password had to be manually updated in ADSSP. If not, ADSSP still retains the old password and therefore restricts the AD users from performing tasks such as password reset, account unlock, etc. This may lead to more help desk calls. With PAM360-ADSSP integration, the privileged domain account details of ADSSP will be mapped with the domain account in PAM360. So, whenever the password of the ADSelfService Plus's privileged domain account mapped in PAM360 is updated, PAM360 automatically updates the password of the privileged domain account in ADSelfService Plus as well.

2. Prerequisites for Performing the Integration

Before commencing the integration, verify if all of the below prerequisites are satisfied:

1. PAM360 should be accessible from the server on which ADSSP is running. To verify this, try launching your PAM360 web-client from the ADSSP server.
2. For this integration to work, ADSSP should be running in secured **HTTPs** mode only.
3. As ADSSP is running in the **HTTPs** mode, the identity of the system needs to be verified through a valid SSL certificate, which has to be imported into the PAM360 certificate store. Follow the steps listed below:
    i. Stop the PAM360 service.
    ii. Open the command prompt and go to the "**<PAM360_Installation_Folder>/bin**" directory.
    iii. Execute the following command:

    importCert.bat *<Path of the certificate used by ADSSP>*

iv. Restart the PAM360 service.

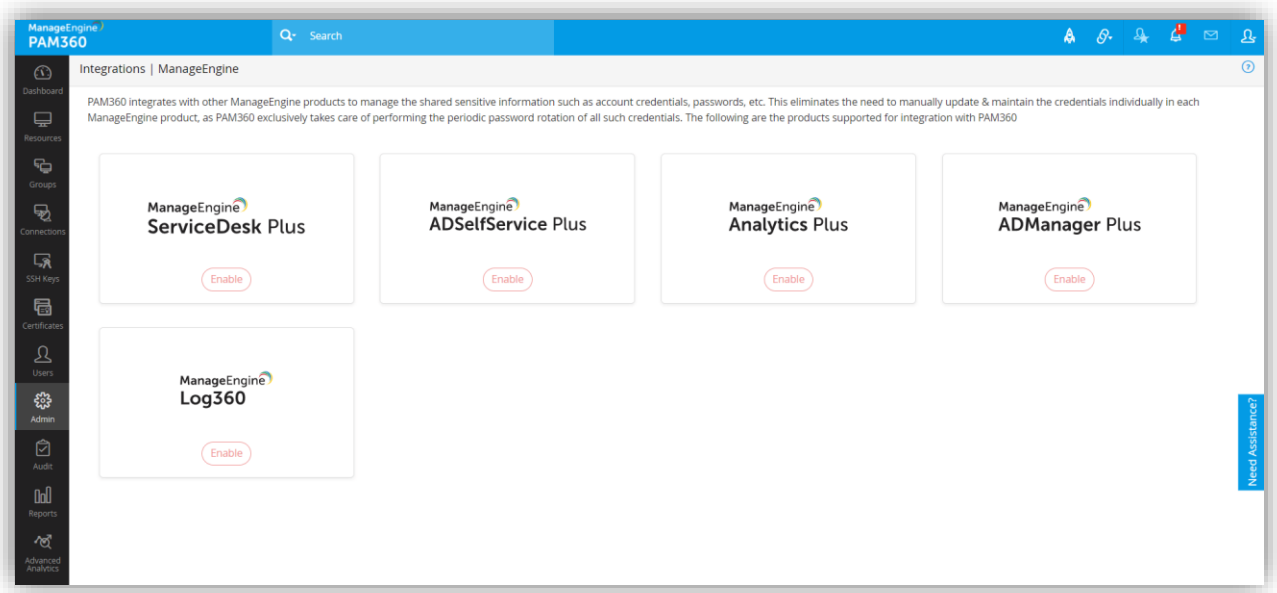
3. Steps to Configure the Integration

You can perform all the configurations related to the PAM360-ADSSP integration from the PAM360 portal itself. To configure the integration, you need to provide the details of the machine, where ADSSP is installed. The details include Host Name, Port Number, etc. Once you have entered all the required details and saved the configuration, PAM360 will try to set a connection with ADSSP. After the successful connection, the domain details will be retrieved from ADSSP and saved in the PAM360 database, and the integration will be established.

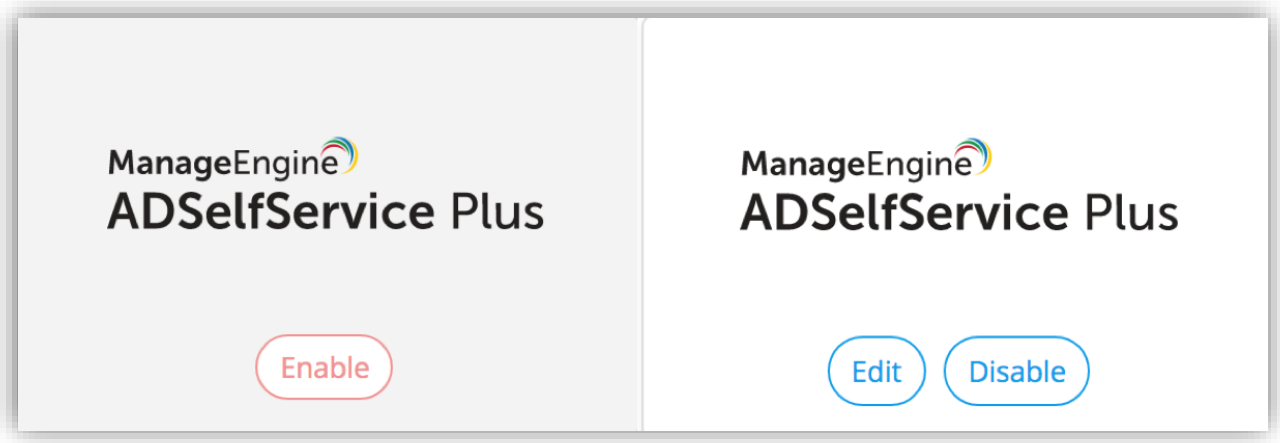
Here are the steps:

1. Navigate to **Admin >> Integration >> ManageEngine.**

> **Note:** Only the users with the **"ManageEngine Integration"** role will see the **ManageEngine** option under **Integration**.



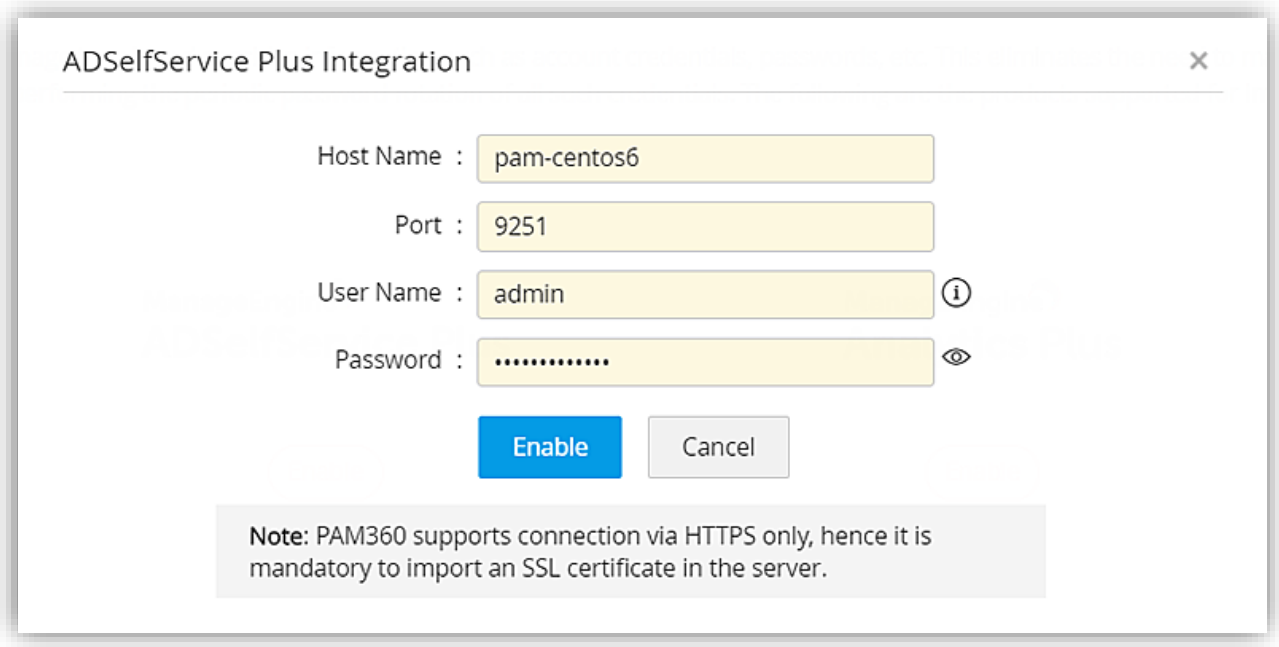
2. In the page displayed, you will see the **ADSelfService Plus** block with either of the below options based on whether you have disabled or enabled the integration, respectively:



Buttons and Definitions:

Sl. No:	Button	Definition
1	**Enable**	You will see this option if the integration is disabled. Click this button, and the **ADSelfService Plus Integration** window pops up.
2	**Edit**	Click this button, and the **ADSelfService Plus** Integration window pops up. Modify the configuration details, if required.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

3. Click the **Edit** button and you will see the below window:



4. Configure the following details:
    i. Enter the ADSelfService Plus **HostName**.
    ii. Specify the **Port** at which ADSelfService Plus is listening.
    iii. Enter the **UserName** and **Password** of an ADSSP user with Admin privileges only.
    iv. Click **Enable**.

Now, the integration will be enabled, and the domain details fetched from ADSSP will be saved in the PAM360 database. Proceed with mapping the domain account details of ADSSP with PAM360.

4. Steps to Map Domain Account Details

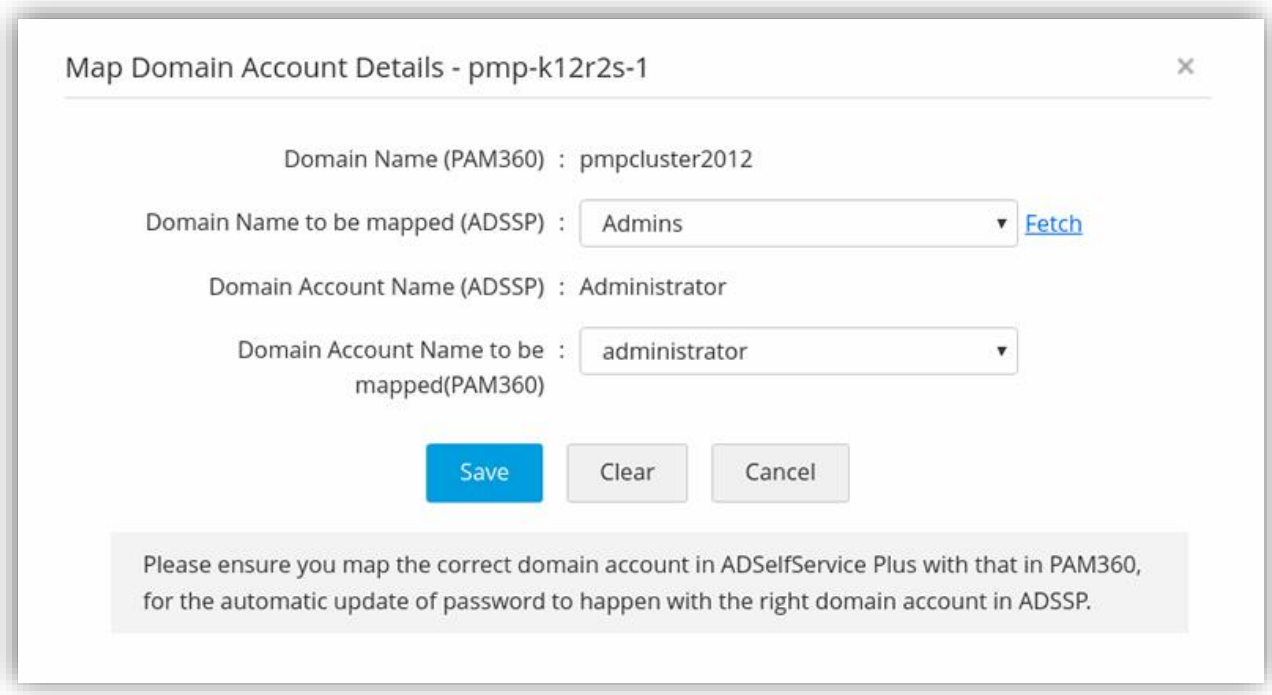
Ensure, the correct domain account in ADSSP is mapped with the domain account in PAM360. Only then, the automatic update of the password will happen with the right domain account in ADSSP.

1. Navigate to **Resources >> Resource Actions**. Click the option **Configure ADSelfService Plus Domain Details.**

    This option will be available only:

    - For the **Windows Domain** resources.
    - If ADSSP integration is configured.

2. A window pops-up with the selected **Resource Name** appended with the title. The **Domain Name in PAM360** is shown by default.



i. Choose the **Domain Name in ADSSP** to be mapped with the Domain Name in PAM360. If you do not find any domain name, click the **Fetch** link to import the domain from ADSSP.

ii. The **Domain Account Name in ADSSP** and the **Domain Account Name in PAM360** fields will be automatically populated based on the Domain Name in ADSSP selected in step i. You can also select a different account for PAM360.

> You will be prompted with an alert message when a mismatch in the ADSSP-PAM360 domain account details in suspected. Verify if you have mapped the correct domain account details of ADSSP in PAM360. Only then the automatic password update will happen with the right domain account in ADSSP.

3. Click **Save**.

Once the mapping of domain account details of PAM360 and ADSSP is successfully done, PAM360 will automatically update the password of the domain account in ADSSP, whenever the password reset for the account is done in PAM360.

5. Troubleshooting Tips

1. Check if the certificates are properly imported.
2. Check the connectivity between the two machines; connectivity should be bi-directional.

3. Click fetch under **Windows DC >> Resource Actions >> Configuring ADSelf service plus domain details** to get the domain details. If it fails, check the **pam0** file available under **<PAM360_Installation_Folder>/logs** directory for any error.

Integrating PAM360 with ManageEngine Analytics Plus

This document discusses the process of integrating PAM360 with ManageEngine Analytics Plus.

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine Analytics Plus, an on-premises reporting and business intelligence service. The PAM360-Analytics Plus integration brings about out-of-the-box analytics using data from the following modules:

- **Resources:** Detailed record of resources and their usage.
- **User Accounts:** List of users, their access levels and permissions.
- **Audits:** Elaborate history of the operations performed by users.

Through advanced analytics on these modules, you will gain a comprehensive analysis of all your privileged account activities through a unified outlook, with the ability to drill down into specifics and gain actionable insights.

2. How does the Integration Work?

Analytics Plus sources data from PAM360 via its API using your login credentials. The reports are generated automatically with up-to-date data, and you can gain a complete overview of the reports from the PAM360-specific dashboard of Analytics Plus. You can also set timeline filters. Once the integration is complete, you will be able to access the workspace created with all the relevant reports and live dashboards built using data from PAM360.

3. Prerequisites

> **Note:** ManageEngine PAM360 integration is applicable from Analytics Plus build **4310** only.

Before commencing the integration, verify if all of the below prerequisites are satisfied:

1. All the configurations related to the PAM360-Analytics Plus integration can be done from the **Analytics Plus portal** only. Hence, make sure you have access to an active

Analytics Plus portal.

2. PAM360 should be accessible from the server on which Analytics Plus is running. To verify this, try launching your PAM360 web-client from the Analytics Plus server.
3. To login PAM360, the Analytics Plus user should have their user login mapped in PAM360.
4. The Auth token generated during the integration process is specific to your Analytics Plus instance, and will be displayed only once. Hence, make sure you copy the Auth Token as you need to paste it in the required field in the Analytics Plus portal.
5. PAM360 and Analytics Plus servers should be running in the same time zone.

4. Steps to Configure the Integration

All the configurations related to the PAM360 - Analytics Plus integration can be performed from the Analytics Plus console only. From the PAM360 console, you can view the configuration details and regenerate the AuthToken. Click the below link for the configuration steps:

Configuration steps to integrate PAM360 with Analytics Plus

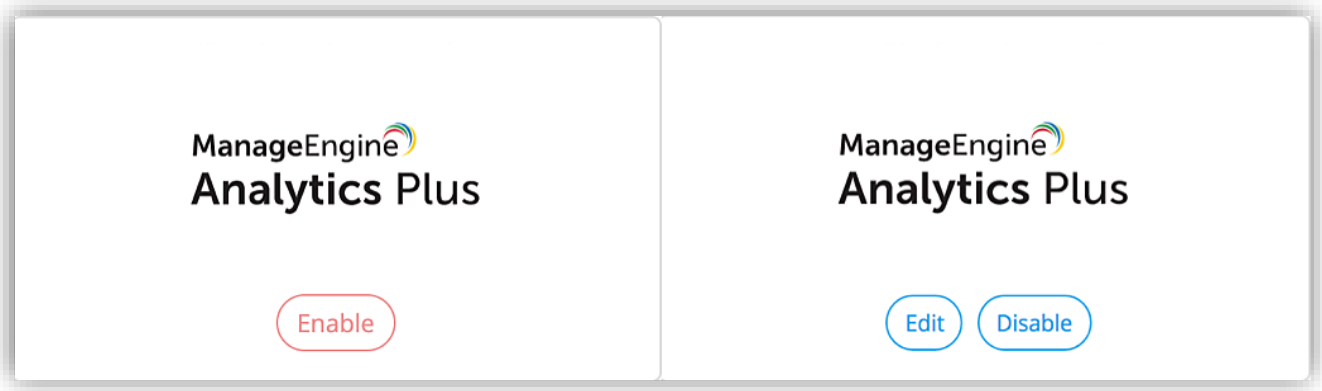
Once you have finished configuring the integration as instructed in the above link, you will be able to automatically generate reports with up-to-date data and gain a complete overview of the reports from the PAM360-specific dashboard in Analytics Plus.

5. Steps to View the Configuration Details from PAM360

Once you are done with configuring the integration from the Analytics Plus portal, you can view the configuration details from the PAM360 console. Navigate to **Admin >> Integration >> ManageEngine**. You will see the **Integrations | ManageEngine** page.

> Only the users with the **ManageEngine Integration** role will see the **ManageEngine** option under **Integration**.

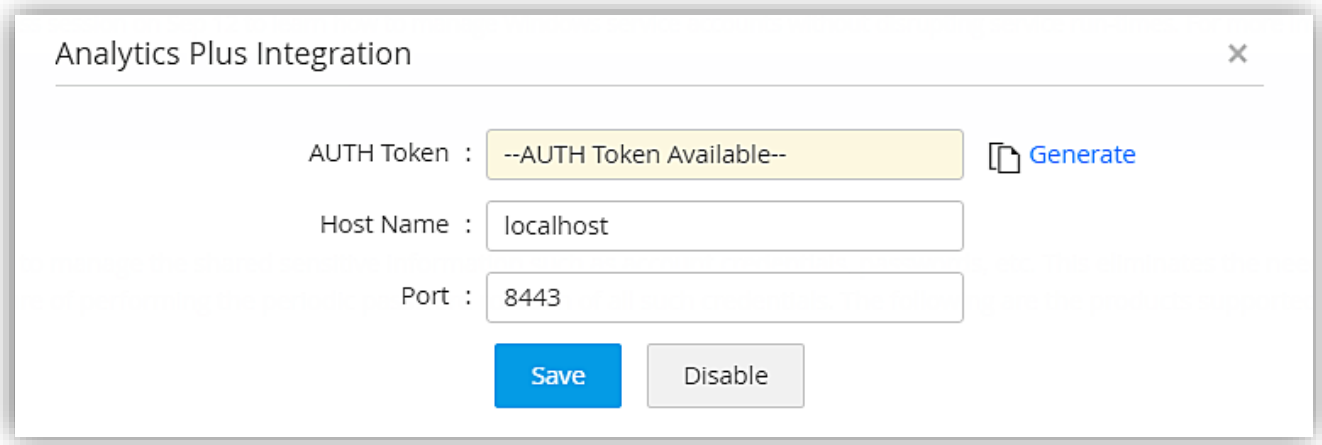
In the **Integrations | ManageEngine** page, you will see the **Analytics Plus** block that looks like any of the below images based on whether you have disabled or enabled the integration, respectively:



Buttons and Definitions:

Sl. No:	Button	Definition
1	**Enable**	You will see this option if the integration is disabled. Click this button and you will be notified with a message to set up the integration from the Analytics Plus portal.
2	**Edit**	Click this button, and the Analytics Plus Integration window pops up.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

Click the **Edit** button and you will see the below window:



From the Analytics Plus Integration window, you will be able to do the following:

1. **View** the configuration details that include:

- **AUTH Token:** You will see the "Auth Token Available" message in this field. Each time you click the **Generate** button, the new Auth Token will be shown here.
- **Host Name**: The DNS name of the machine, where Analytics Plus is hosted.
- **Port Number**: The port number on which Analytics Plus is listening.

2. Click the **Generate button** to generate a new Auth Token.
3. Click **Save** to save the changes.

> You can generate any number of Auth tokens from here. This option comes handy if you have lost the Auth Token that was generated during the initial configuration process. Whenever you generate a new Auth token, click **Save** for the change to take effect.

6. How to View Analytics Plus Dashboards in PAM360?

The Advanced_Analytics module of PAM360, offered via ManageEngine Analytics Plus, automatically analyzes privileged account activity data to help you identify anomalies in password and user account activities. Once the integration is complete, follow the below steps to view Analytics Plus dashboards in PAM360:

Navigate to the Advanced Analytics tab.

Click **ManageEngine Analytics Plus** from the left pane. Under this, click the required dashboard from the list of dashboards available. You can see the relevant audit data displayed in the dashboard area on the right. Refer to the dashboard section in Advanced_Analytics section to learn about the dashboards offered by Analytics Plus in detail.

7. Troubleshooting Tips

1. While re-authenticating Analytics Plus, if the **Advanced Analytics** tab in PAM360 shows no integration details and displays the **download Analytics Plus** option, then remove the integration, create a new workspace in Analytics Plus, and reconfigure.
2. If the Advanced Analytics tab does not show data (charts) and instead displays the report tabs, do the following:
   i. Check if the Analytics Plus server and ports are reachable from the accessed machine.
   ii. Click '**Launch Analytics Plus**' to check if the integrated Analytics Plus is reachable and has a valid certificate.
3. If the Advanced Analytics tab does not show data (charts), instead displays the report tabs and an error message **(blocked by an extension/refused to connect):**

i. Navigate to the **<PAM360_Installation_Folder>/logs** directory and open the **"pam0"** file.
ii. Search for **"remoteHost in api filter"** and try pinging the value/IP address corresponding to it. If the server is not reachable using the IP address, then determine the correct IP/DNS, using which you can ping the server from the PAM360 installation machine.
iii. If the problem persists, please contact PAM360 support.

Integrating PAM360 with ManageEngine ADManager Plus

This document discusses the process of integrating PAM360 with ManageEngine ADManager Plus.

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine ADManager Plus, a management and reporting solution that allows IT Administrators and Technicians to manage Active Directory objects and groups and generate reports.

The PAM360-ADManager Plus integration allows you to perform timely elevation and delegation of domain users in the Active Directory (AD) security groups through the ADManager Plus server. By leveraging the ADManager Plus integration, enforce access control for PAM360 users on domain accounts and provide just-in-time privilege elevation for the domain accounts. You can also add and remove accounts from the AD security groups right from the PAM360 interface. Once the integration is complete, all the security groups from the active directory server will be available in PAM360.

Read more about AD groups management in ADManager Plus here.

2. How does the Integration Work?

PAM360 sources data from ADManager Plus via its API and using the server details of ADManager Plus. The AD security groups listed in ADManager Plus will be consolidated and listed in PAM360. The AD domain users imported into PAM360 can be given controlled access to the security groups populated from ADManager Plus.

3. Prerequisites for Performing the Integration

Before commencing the integration, verify if all of the below prerequisites are satisfied:

1. PAM360 supports connection via HTTPS only, hence it is mandatory to import a valid SSL certificate in the server. Follow the steps to import a certificate in the server:
    i. Stop the PAM360 service.
    ii. Open the command prompt and go to the **"<PAM360_Installation_Folder>/bin"** directory.
    iii. Execute the following command:

    importCert.bat <Path of the certificate used by ADSSP>

iv. Restart the PAM360 service.

2. The common name of the certificate must match the host name of the active ADMP server.
3. At least one authorized admin in PAM360 must be a valid technician in ADMP.

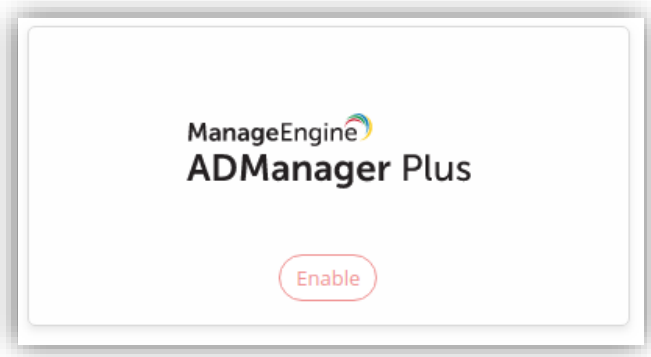
4. Steps to Configure the Integration

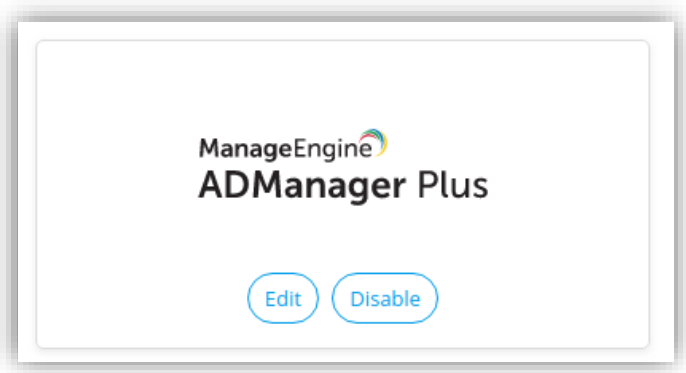
You can perform all the configurations related to the PAM360-ADManager Plus integration from the PAM360 portal. To configure the integration, provide the host name and port details of the machine where ADManager Plus is installed. Once you have entered all the required details and saved the configuration, PAM360 will try to set up a connection with ADManager Plus. After the successful connection, the domain details will be retrieved from ADManager Plus and saved in the PAM360 database, and the integration will be established.

1. Navigate to **Admin >> Integration >> ManageEngine**. You will see a consolidated view of all ManageEngine products integrated with PAM360.

> Only the users with the **ManageEngine Integration** role will see the **ManageEngine** option under **Integration**.

2. In the page displayed, you will see the **ADManager Plus** block with any of the below options based on whether you have disabled or enabled the integration, respectively:

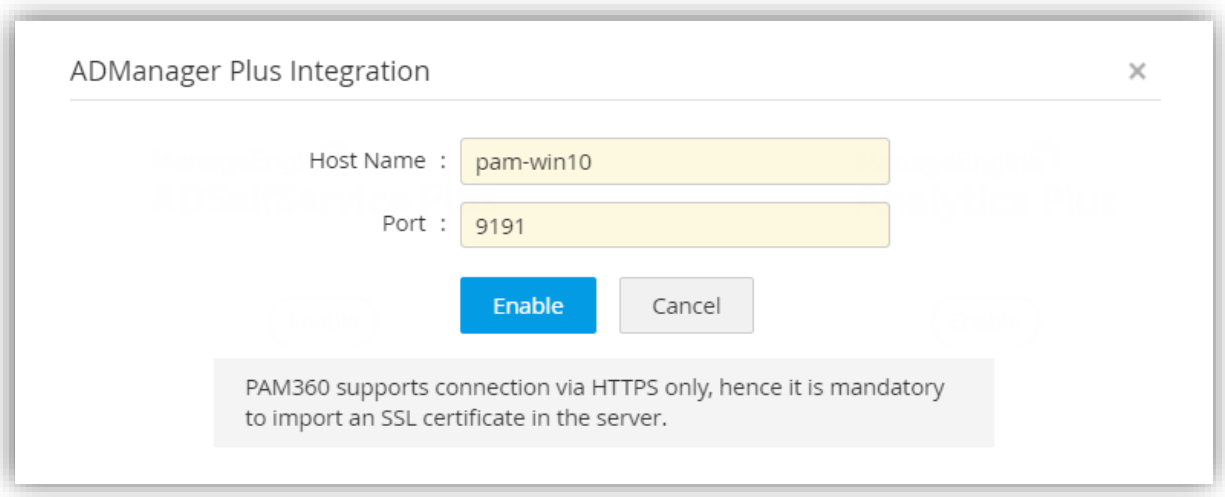




Buttons and Definitions:

Sl. No:	Button	Definition
1	**Enable**	You will see this option if the integration is disabled. Click this button to enter required details of the ADManager Plus server and enable integration.
2	**Edit**	You will see this option if the integration is enabled. Click this button to update the ADManager Plus host name and port details.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

1. Click **Enable** and configure the following details:
   i. Enter the ADManager Plus host name.
   ii. Enter the port of the ADManager Plus server.



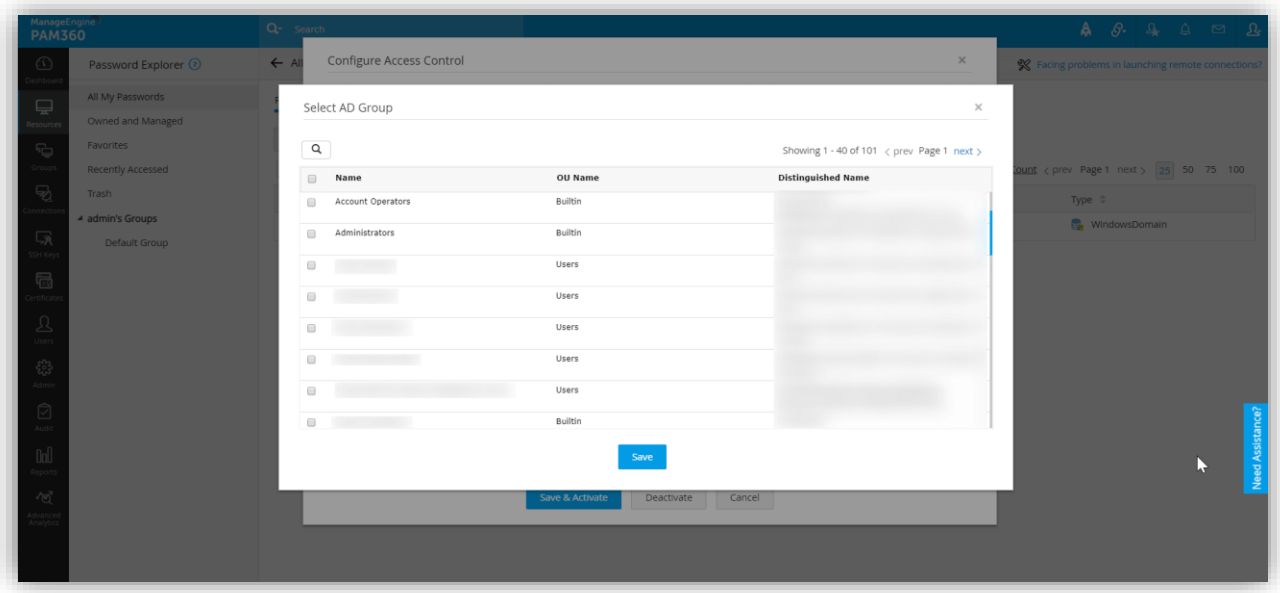
2. Click **Enable** to save the settings.
3. Now, access the ADManager Plus web console, navigate to **Admin -> Integrations -> PAM360,** enable the checkbox **Enable tight integration with PAM360** and save the settings.

The PAM360 - ADManager Plus integration is enabled now. Proceed with mapping of domain accounts to the AD security groups.

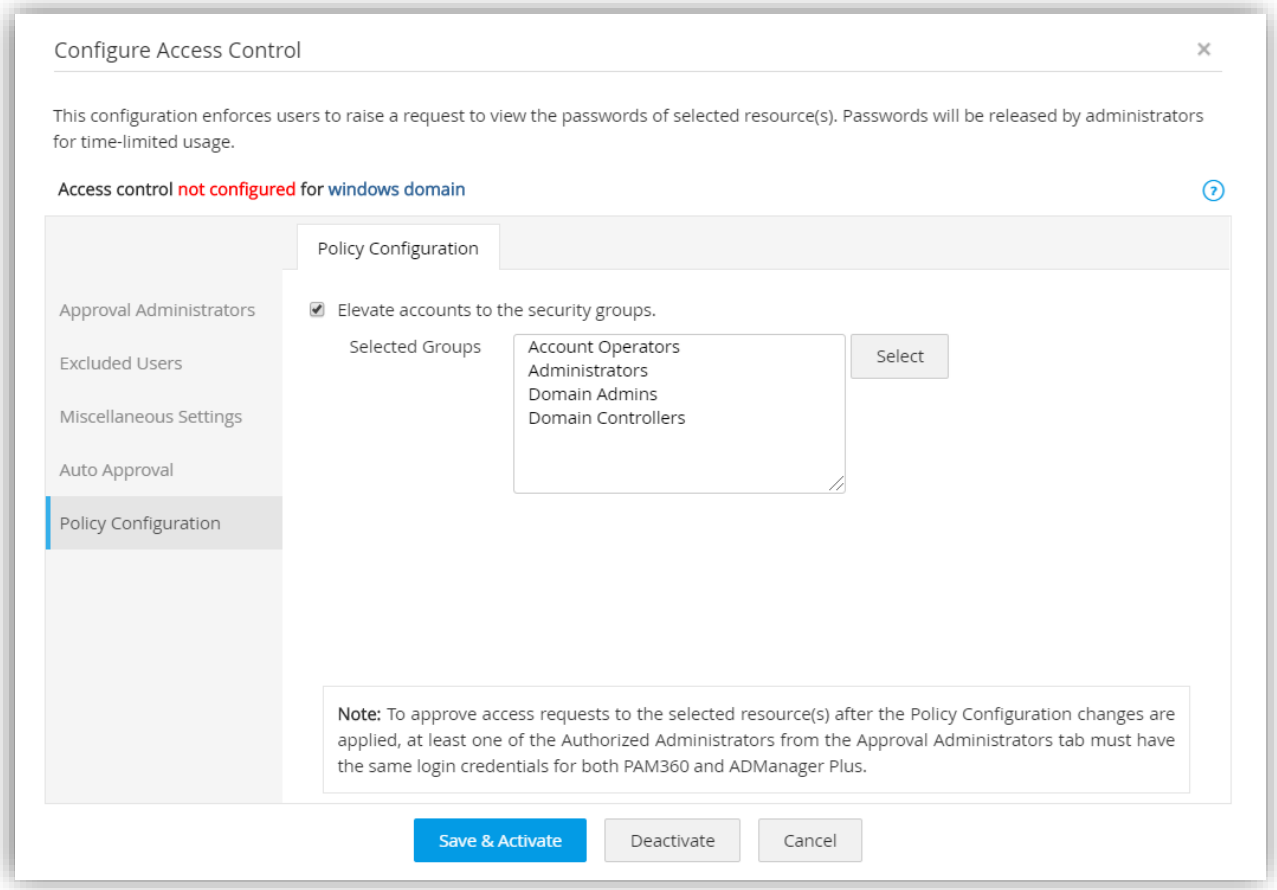
5. Steps to Map Accounts to ADManager Plus Security Groups

Once the PAM360-ADManager Plus integration is complete, follow the below steps to perform policy configuration. The **Policy Configuration** option lets you elevate domain accounts to security groups just in time (AD security groups already exist in the Domain Controller and by extension, in the ADManager Plus also.)

1. Navigate to **Resources >> Add Resource** to add the AD Domain Controller as a resource in PAM360.
2. Click **Resource Actions** beside the required resource and click **Configure Access Control**.
3. In the **Approval Administrators** tab, ensure that at least one of the **Authorized Administrators** listed here is a valid technician in ADManager Plus also. This is to facilitate approval of access requests to the selected resource(s) once the policy configuration changes are applied.
4. In the **Policy Configuration** tab, click **Select** to list all the AD groups available in ADManager Plus.
5. Choose the groups to which you want to add the resource to and click **Save**. You can view the chosen groups under the **Selected Groups** box.



6. Select the **Elevate accounts to the security groups** option and click **Save and Activate**.



Now when the resource is shared to a user with Password User/Password Auditor capabilities, they can request for password access or elevation. This request can be approved/rejected by any admin in the Authorized Administrator list as long as their user role satisfies the following criteria:

- The user designated to perform privilege elevation must have an **Administrator** role in PAM360 (i.e., any one of the following user roles: Privileged Administrator, Administrator, and Password Administrator), and in ADManager Plus, they must have a user role with any of the following permissions: **modify users** and **modify groups.** However, the users who receive privilege elevation in PAM360 need not have any special permissions in ADManager Plus.

Important Notes:

1. Direct changes made to the group configuration in ADManager Plus will override the changes made in PAM360.

   Example:

   i. A domain account is elevated to the **System Admin** security group through PAM360 policy configuration.

   ii. A user connects to a shared server using the domain account.

   iii. Through the defined access control and policy configuration in PAM360, the normal domain account is automatically elevated just-in-time to the security group **System Admin** and gets assigned with the required privilege.

   iv. However, during this time, if the domain account elevation is removed from the security group in ADManager Plus, then the privilege will be removed in PAM360 immediately.

2. To perform the **Group Membership Automation** operations in this integration, you must be using the **Professional** edition of **ADManager Plus,** as the Group Automation functionality is supported only in that edition.

6. Troubleshooting Tips

1. Check if the certificates are properly imported.
2. Check the connectivity between the two machines; connectivity should be bi-directional.
3. If the groups are not displayed under **Access Control >> Policy Configuration,** check for the domain name field in PAM360 Windows Domain Controller resource.

Integrating PAM360 with ManageEngine EventLog Analyzer

This document discusses the process of integrating PAM360 with ManageEngine EventLog Analyzer.

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine EventLog Analyzer, an end-to-end log management solution that facilitates log collection, custom log parsing, and complete log analysis with reports.

The PAM360-EventLog Analyzer integration allows you to consolidate and visualize the log data for remote sessions initiated from the PAM360 interface. To check these logs within PAM360, go to **Audit >> Recorded Connections** and view the **Activity Log** column beside any resource name.

> **Note:** Currently, log data collection through the PAM360-EventLog Analyzer integration is available only for **Windows** RDP sessions.

2. How does the Integration Work?

EventLog Analyzer sources data from PAM360 via its API using your server details and login credentials. The log data sent to EventLog Analyzer from PAM360 is updated periodically and visualized for better comprehension. Once the integration is complete, you will be able to view the list of active and closed remote sessions, a complete overview of the events carried out during the remote sessions, and the machine log details, right from the PAM360 interface.

3. Prerequisites for Performing the Integration

3.1 Allow Windows Resources to Accept Remote Sessions from PAM360

Execute the following commands in the Windows device for which a remote session will be initiated from PAM360. These commands have to be executed in every device for which a remote session will be launched from PAM360 for the first time. After the first time, you don't need to execute the commands again for future remote sessions. This can also be executed through a bulk GPO update on all the target end-points. These commands allow the log data to be sent from the particular Windows machine to EventLog Analyzer.

Open a command prompt from an Administrator account and execute the following:

1. **auditpol /set /category:"Account Logon" /success:enable /failure:enable**
2. **gpupdate /force**

3.2 Import SSL Certificate in the Server

PAM360 lets you enable HTTPS to secure the remote connections. To enable HTTPS during the integration, it is mandatory to import a valid SSL certificate in the server. Follow the steps below to import a certificate in the server:

1. Stop the PAM360 service.
2. Open the command prompt and go to the "**<PAM360_Installation_Folder>/bin**" directory.
3. Execute the following command:
   importCert.bat *<Path of the certificate used by EventLog Analyzer>*
4. Restart the PAM360 service.

4. Steps to Configure the Integration in EventLog Analyzer

Before you enable the EventLog Analyzer integration in PAM360, follow the below configuration steps in the EventLog Analyzer console to optimize EventLog Analyzer to receive the log data from PAM360.

4.1 Add PAM360 and Resource as Devices in EventLog Analyzer

1. Navigate to **Log360 >> EventLog Analyzer.**
2. Add the following devices to the EventLog Analyzer console:
   i. Add the PAM360 server.
   ii. Add all the resources for which a remote session will be launched from PAM360 and for which the corresponding logs to be collected from EventLog Analyzer.
   iii. Please note that the resources/devices can be manually added using the discovery function in EventLog Analyzer.

4.2 Add PAM360 as an Application in EventLog Analyzer

1. In **Log360 >> EventLog Analyzer**, navigate to **Settings >> Manage Application Sources >> Other Application Sources >> ManageEngine Apps >> PAM360.**
2. Here, choose the machine in which PAM360 is running and click **Add**.

4.3 Enable Activity Rules for PAM360 Sessions

1. In **Log360 >> EventLog Analyzer**, navigate to **Correlation >> Manage Rules >> Activity Rules.**
2. Click the red icon beside **PMP Sessions** to enable activity logs for remote sessions taken via PAM360.

Once you have completed the steps as instructed above, you can proceed to the next step and enable the EventLog Analyzer integration in PAM360.

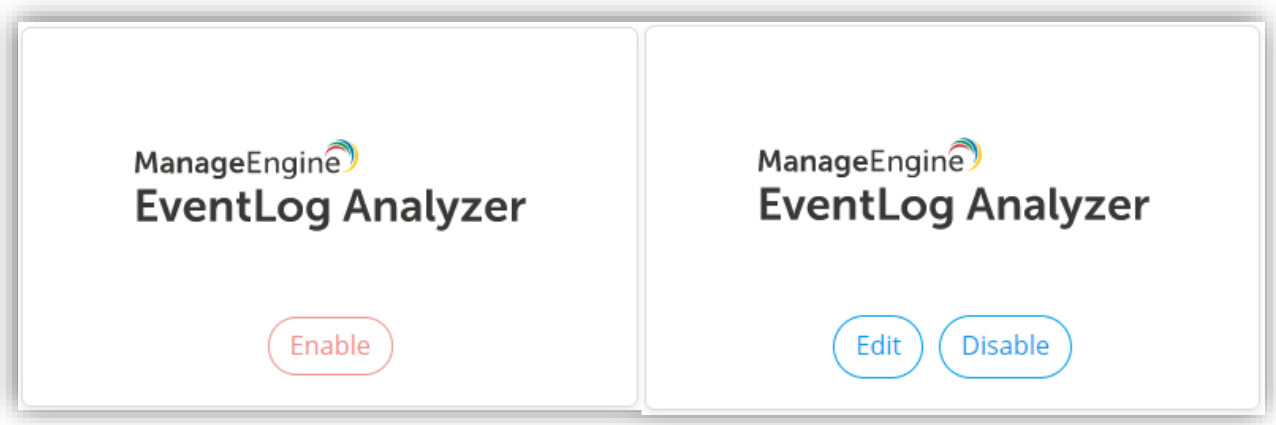
5. Steps to Enable EventLog Analyzer Integration in PAM360

In the PAM360 console, follow the below steps to enable the integration:

1. Navigate to **Admin >> Integration >> ManageEngine**. You will see a consolidated view of all ManageEngine products integrated with PAM360.

   > Only the users with the **ManageEngine Integration** role will see the **ManageEngine** option under **Integration**.

2. In the page displayed, you will see the EventLog Analyzer block with any of the below options based on whether you have disabled or enabled the integration, respectively:

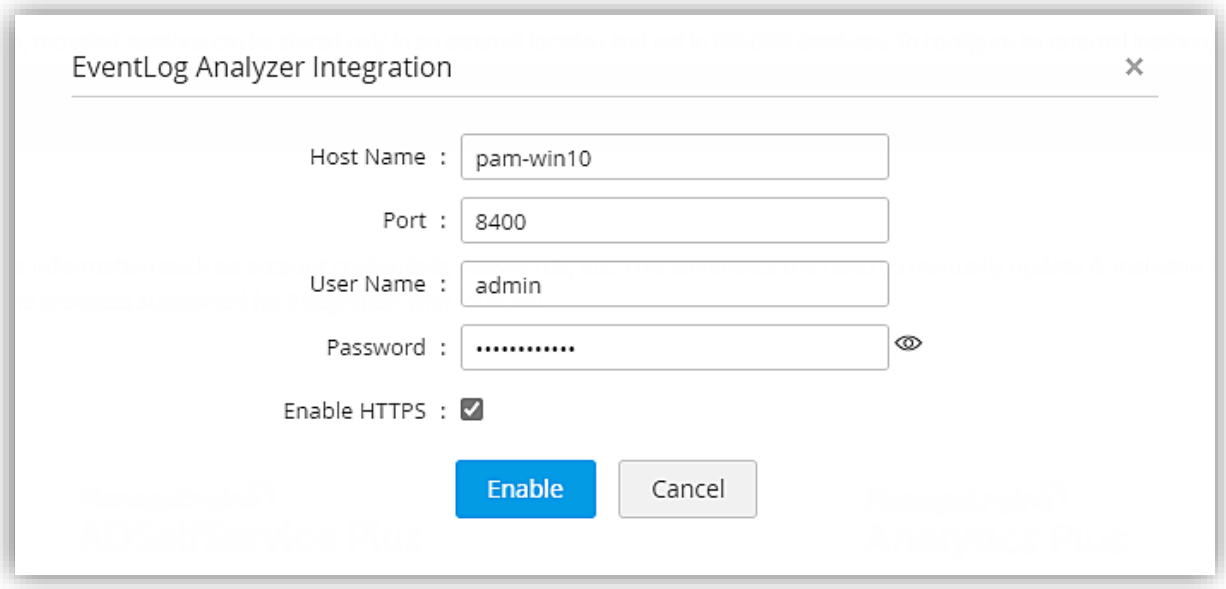


Buttons and Definitions:

Sl. No:	Button	Definition
1	Enable	You will see this option if the integration is disabled.

		Click this button to enter required details of the EventLog Analyzer server and enable integration.
2	**Edit**	You will see this option if the integration is enabled. Click this button to update the EventLog Analyzer host name and port details.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

1. Click **Enable** and enter the following details:
   i. **Host Name** - The host machine in which EventLog Analyzer is running
   ii. **Port**
   iii. **User Name**
   iv. **Password**
   v. **Enable HTTPS** - Select this checkbox to enable connection via HTTPS. If HTTPs is enabled, it is mandatory to import a valid SSL certificate in the server. Refer to the section 3.2 for the steps to import an SSL certificate.



2. Click **Enable**. PAM360-EventLog Analyzer integration is complete. Now, when a remote session is initiated via PAM360, all the events will be recorded in **Audit >> Recorded Connections** under the **Activity Logs** column.

Notes:

- Once EventLog Analyzer integration is enabled under **Admin >> Integrations >> ManageEngine**, the SIEM integration for EventLog Analyzer will also be enabled automatically under **Admin >> Integrations >> SIEM Integration**. This is to ensure that all the log details from PAM360 are sent to EventLog Analyzer in the form of syslogs.
- To ensure that the EventLog Analyzer integration works smoothly, it is recommended that the SIEM integration with EventLog Analyzer is always enabled.
- Click here for more information on SIEM integration.

5.1 How to Set Up Alert Notifications in EventLog Analyzer?

Receive alerts for activities related to PAM360 in the form of **email** or **SMS** whenever your PAM360 server encounters unauthorized logins. Start configuring the alerts once the PAM360-EventLog Analyzer integration is complete. Remember, the alerts can be configured from the EventLog Analyzer console only. Create a new alert profile and specify your preferences. Here are the steps in detail:

1. Navigate to **Log360 >> EventLog Analyzer** and switch to the **Alerts** tab.
2. To add a new profile, click **+ Add** in the top right corner and click **Configuration >> Alerts**.
3. Here, enter a name, choose a severity, and select the required device.
4. Under the **Select Alert** option, click the **Custom Alerts** tab.
5. Using the available drop-downs, specify the following criteria:

Source Device not equals pam360-server (choose the name of your PAM360 server)

+

Logon Type equals **10**

+

Event ID equals **4624** (this ID signifies unauthorized login)

The specified criteria will look like: **Rule Criteria = (SOURCEHOST:pam360-server) AND (LOGONTYPE:10) AND (EVENTID:4624)**

6. Click **Save** to save the criteria.
7. Under **Alert Notification**, choose your preferred notification settings. Based on these settings, you will receive an alert through **Email** or **SMS** whenever an unauthorized login is detected in your PAM360 server. To invoke a workflow for the alert, click the **Workflow** tab, choose a pre-defined workflow from the drop-down and assign it to an admin or an operator. Click **Save Profile** to save all alert settings.

The alert profile creation is complete. Now, all alerts related to the selected criteria will be listed under the Alerts tab.

To know more in detail about creating alert profiles, click here. To know more about creating new workflows in EventLog Analyzer, click here.

6. Troubleshooting Tips

1. If the activity log is not captured, check for the time difference between the PAM360 server and the remote machines. The time of the remote machine should be the same or behind PAM360 server time.
2. If all the integrations are proper but the correlation is not collecting data, check the Syslog values to confirm if **Session Started** and **Session Ended** logs are captured from PAM360.
3. If the PAM360 sessions in ELA are not displaying data, check for the remote server name displayed in ELA. The remote server name has to be the same as the DNS name of the resource in PAM360.

Integrating PAM360 with ManageEngine Log360 UEBA

This document discusses the process of integrating PAM360 with ManageEngine Log360 UEBA (User and Entity Behavior Analytics).

1. Key Benefits of Integration

ManageEngine PAM360 integrates with ManageEngine Log360 UEBA, a machine learning-based add-on that analyzes audit logs and detects abnormal behavior using risk scores, anomaly trends, and audit reports. The PAM360-Log360 UEBA integration allows you to consolidate and visualize the resource and user audit trails within the Advanced Analytics tab in PAM360.

2. How does the Integration Work?

Log360 UEBA sources data from PAM360 via its API using your server details and login credentials. The audit trails from PAM360 are sent to Log360 UEBA at regular intervals and visualized as graphs for better understanding. Once the integration is complete, you will be able to view the resource and user audit data segregated as audit and anomaly reports interpreted using patterns and user behavior, right from the PAM360 user interface.

> **Note:** PAM360 - Log360 UEBA integration works with **Log360 UEBA build 4023 and above** only.

3. Prerequisites for Performing the Integration

Before commencing the integration, follow the steps detailed below to satisfy the prerequisites.

3.1 Enable HTTPS Connection in Log360 UEBA

Change the connection type to **HTTPS** in the Log360 UEBA server. The integration works only with HTTPS connections as PAM360 uses HTTPS to secure remote connections. Click here to learn how to change the connection type in the Log360 UEBA server. Once you change the connection type, follow the steps given in this document to generate and apply an SSL certificate in the Log360 server.

3.2 Import SSL Certificate in the PAM360 Server

Once HTTPS is enabled, import a valid SSL certificate into PAM360. Follow the steps below:

1. Stop the PAM360 service.
2. Open the command prompt and go to the "**<PAM360_Installation_Folder>/bin**" directory.
3. Execute the following command:
   importCert.bat *<Path of the certificate used by Log360 UEBA server>*
4. Restart the PAM360 service.

3.3 Enable Log360 UEBA Analytics under User Roles

Only the users with Log360 UEBA Analytics role will see the Log360 UEBA option under ManageEngine Integrations. By default, this role is enabled for all admin users. If you have a custom user role that requires access to the Log360 UEBA dashboard, follow the below steps to provide access:

1. Navigate to **Admin >> Customization >> Roles.**
2. Click **Add Role** to create a custom role.
3. In the **Add Role** dialog box, click the **Analytics** tab and select the check box **ManageEngine Log360 UEBA**. Once this option is enabled, **ManageEngine Integration** option will also be enabled automatically. Now, once you assign this custom role to a user, they can access Log360 UEBA under **Admin >> Integrations >> ManageEngine**.

4. Steps to Configure the Integration in PAM360

In the PAM360 console, follow the below steps to enable the integration:

1. Navigate to **Admin >> Integration >> ManageEngine**. You will see a consolidated view of all ManageEngine products integrated with PAM360.

> Only the users with the **"ManageEngine Integration"** role will see the **ManageEngine** option under **Integration**.

Buttons and Definitions:

Sl. No:	Button	Definition
1	Enable	You will see this option if the integration is

		disabled. Click this button to enter required details of the Log360 UEBA server and enable integration.
2	**Edit**	You will see this option if the integration is enabled. Click this button to update the Log360 UEBA host name and port details.
3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

2. Under **ManageEngine Log360 UEBA**, click **Enable**. In the Log360 UEBA Integration dialog box that opens up, the following details are required:
    i. **Host Name** - The host machine in which Log360 UEBA is running.
    ii. **Port** - The port number in which Log360 UEBA is listening.

Before providing the authentication password, consider the below two cases:

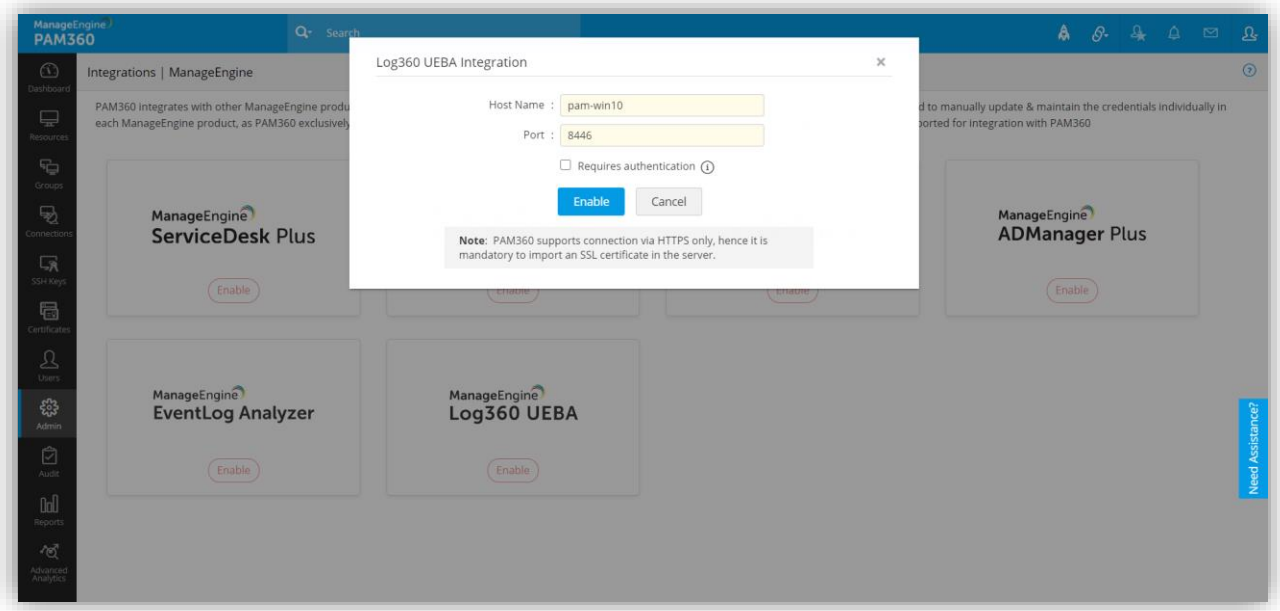
Case 1: Both PAM360 and Log360 UEBA servers reside in the same machine

Case 2: PAM360 and Log360 UEBA servers reside in different machines

Case 1: Both PAM360 and Log360 UEBA Servers Reside in the Same Machine

If both PAM360 and Log360 UEBA servers reside in the same machine, then the authentication password is not necessary. In this case, do as follows:

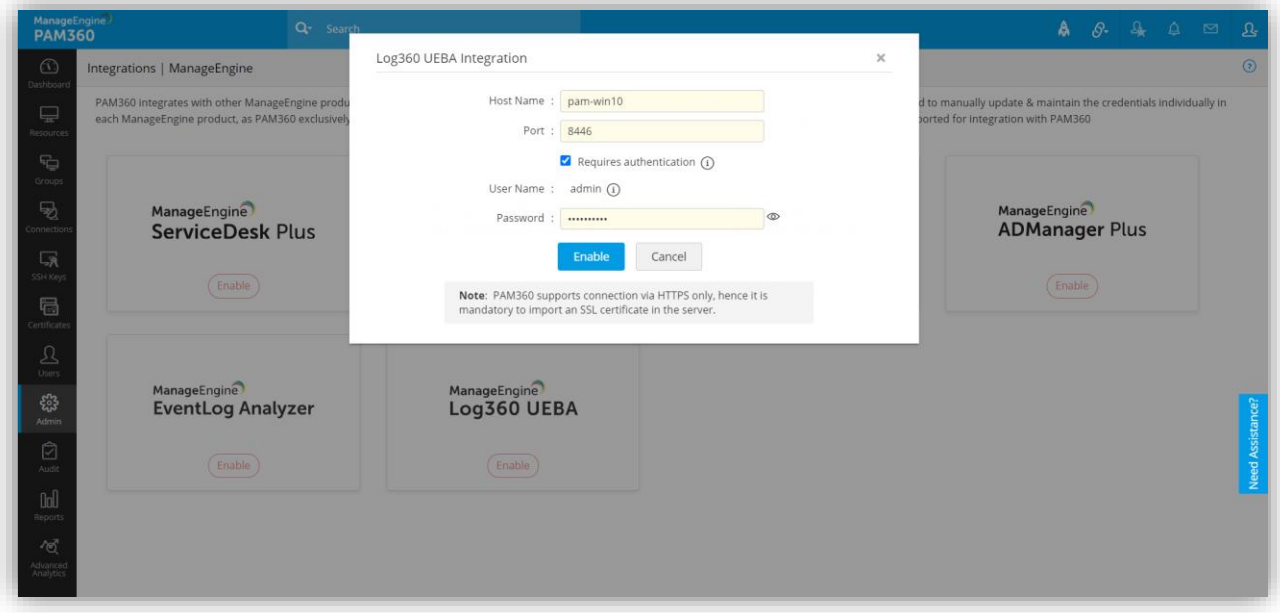
1. Enter the **Host Name** and **Port**.
2. Leave the **Requires Authentication** option unchecked and click **Enable**.



Case 2: PAM360 and Log360 UEBA Servers Reside in Different Machines

If PAM360 server and Log360 UEBA servers reside in different machines, then the authentication password is mandatory. In this case, do as follows:

1. Enter the **Host Name** and **Port**.
2. Select the **Requires Authentication** checkbox and enter the **Password**. This password must be the login password of the server in which Log360 UEBA is running.
3. Click **Enable**.



> **Note:** This integration will work only with the username "**admin**" which is the default username of the Log360 UEBA Super Admin account. As of now, Log360 UEBA does not support PAM360 integration with Active Directory users and custom users in Log360 UEBA.

The integration is complete. Now, all existing the audit trail from PAM360 will be sent to Log360 UEBA right away. This is a one-time operation, after which the audit data will be sent from PAM360 once every one hour. As of now, this integration supports only two types of audit data from PAM360: **Resource audit** and **User audit.**

If **Case 2** applies to you, Log360 UEBA reports Dashboard may not work as expected in Google Chrome and Microsoft Edge browsers. If you are using either of those browsers, follow any one of the workaround steps given below:

Workaround 1:

Enter the Fully Qualified Domain Name (FQDN) as the **Host Name** above.

Example of an FQDN: **[hostname].[domain].[top level domain]**

Workaround 2:

Follow the below steps in Google Chrome or the Microsoft Edge browser:

1. Open a new tab and go to **chrome://settings/**. Here, click **Cookies and other site data** and choose the **Allow all cookies** option.
2. Open a new tab and go to **chrome://flags/**. In the search bar, enter the keyword "**samesite**". Disable the **SameSite by default cookies** option by choosing **Disabled** from the drop-down beside it.
3. Relaunch the browser.

5. How to View Log360 UEBA Reports in PAM360?

Once the integration is complete, follow the below steps to view Log360 UEBA reports in PAM360:

1. Navigate to the Advanced_Analytics tab.
2. Click **ManageEngine Log360 UEBA** from the left pane. Under this, choose **Resource Anomaly** or **User Anomaly**. As per your choice, the analysis of resource and user audit reports will be displayed in the dashboard area on the right. Refer to the section 5.2 in Advanced_Analytics to learn about the dashboards in detail.
3. Log360 UEBA dashboard works well in the following browsers: IE 11 and above, Mozilla Firefox 4 and above, Microsoft Edge, and Google Chrome.

If you have applied steps for Case 2, then Log360 UEBA reports dashboard may not work as

expected in Google Chrome and Microsoft Edge browsers. Refer to the section 4 above to learn about the workaround steps.

6. Important Points to Consider

- You can integrate only one PAM360 server with a Log360 UEBA server because, as of now, Log360 UEBA does not have the provision to segregate data from different PAM360 servers as separate reports. Therefore, attempting to integrate multiple PAM360 servers with a single Log360 UEBA server might lead to data loss.
- All audit trails sent to Log360 UEBA are stored in the Log360 UEBA server and will remain there forever. Purging audit records in PAM360 will not delete the data stored in Log360 UEBA.
- Once the integration is enabled, all existing audit data from PAM360 are imported to Log360 UEBA immediately. After the initial import, the audit data is sent from PAM360 once every one hour.
- If your Log360 UEBA server license expires and you move to the free edition, Log360 UEBA will stop fetching audit trails from PAM360. As a result of this, the Log360 UEBA dashboard in PAM360 will not display new reports. However, the anomaly reports generated before the license expiry will remain in PAM360 unless the integration is manually disabled.
- To configure how audit trails are recorded in PAM360, go to the **Audit** tab and click **Audit Actions >> Configure Resource Audit** or **Configure User Audit**. Any configuration setting applied to the Resource and User audit types will apply to the audit data sent to Log360 UEBA. However, it is not possible to control the type of audit logs sent to Log360 UEBA without affecting the way PAM360 records the audit trails.

Click here to learn more about audits in PAM360.

Integrating PAM360 with Robotic Process Automation Tools

PAM360 offers robust integrations with industry-leading Robotic Process Automation (RPA) tools to effectively automate the management of shared sensitive information such as account credentials, passwords, etc. The integration with RPA tools eliminates the need for administrators to manually intervene with password-related tasks that are performed on an everyday basis.

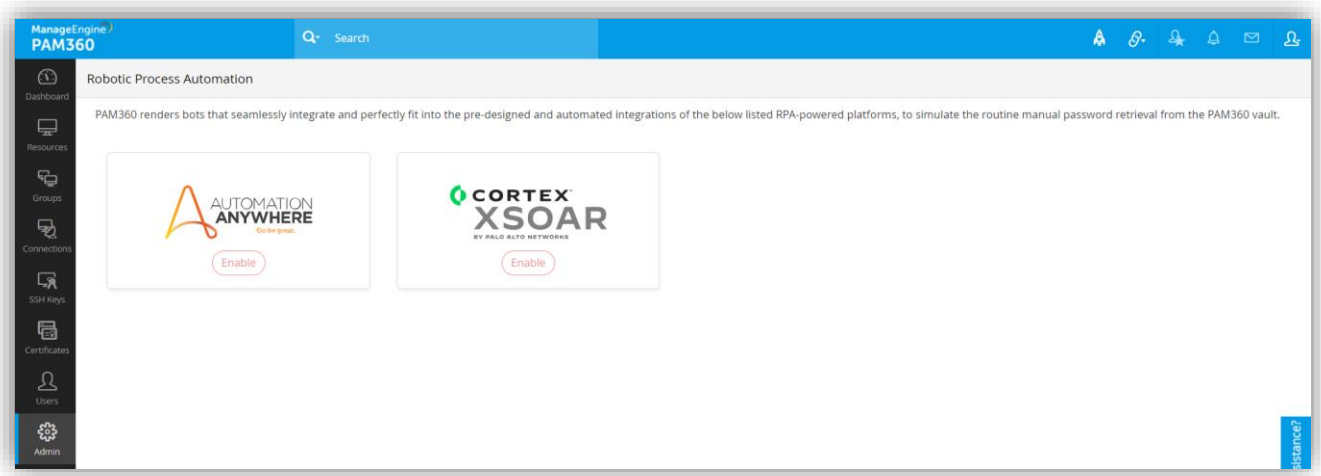
The scope and benefits of each integration differ based on the product integrated and its individual functionalities. However, the objective behind the integration is to help users manage sensitive enterprise data in a secure and efficient manner. Read further to learn how the integration works for each product in detail.

Robotic Process Automation Tools Integrated with PAM360

PAM360 integrates with the following products:

1. **Automation Anywhere**
2. **Cortex XSOAR**

To begin the process of integration, navigate to **Admin >> Integration >> ManageEngine.** You will see a consolidated view of all the available products integrated with PAM360:



Note: The **Robotic Process Automation** option will be visible only to users with RPA privilege - Administrators, Privileged Administrators and users for whom RPA custom role is enabled.

Integrating PAM360 Automation Anywhere

This document discusses the procedure to integrate PAM360 with Robotic Process Automation (RPA) tools. PAM360 integrates with Automation Anywhere, an RPA tool that mimics different software processes using bots. At the end of this ection, you will have learned the following:

1. Key benefits of integration
2. How does the integration work?
3. Setting up the Automation Anywhere portal
   3.1 Retrieving password using resource name and account name
   3.2 Retrieving password using the Read from File option
4. Configuring RPA integration in PAM360
   4.1 Adding Entries
   4.2 Editing Entries
   4.3 Approval workflow for RPA entries
   4.4 Deleting Entries
5. Downloading account details in PAM360

1. Key Benefits of Integration

The PAM360 bot automatically fetches passwords using resource and account details from PAM360's vault, thereby eliminating the need to retrieve passwords manually to perform different tasks. The PAM360 bot can be combined with other bots in Automation Anywhere to create a complete endpoint management workflow. Let's assume your company needs a secure remote login setup automated using bots. You can combine PAM360's bot with another bot that initiates the remote connection. The password fetching mechanism of PAM360's bot will ensure that the password is fetched securely from PAM360's vault and used to log in to the remote device.

2. How does the Integration Work?

Through the integration, the PAM360 bot can automate the process of fetching passwords from PAM360's password repository. The securely fetched password can then be used to connect to a machine, application, or a database.

PAM360's Taskbots can fetch the password from PAM360 vault in two ways: Through resource & account name and through resource & account ID. The Taskbots can take input values from the user manually and also read the data from a text file. The input value includes a unique App Token, generated from PAM360's web interface. Once the required input details are provided, run the Taskbot in the Automation Anywhere portal; the password of the requested resource and account will be fetched and displayed in Automation Anywhere.

3. Setting up the Automation Anywhere Portal

First-time users, click here to download Automation Anywhere and get started.

Follow the below steps to set up the Automation Anywhere portal and add the PAM360 bot in there:

1. Download the PAM360 bot from the Bot Store.
2. Double click the **.msi** file and follow the installation instructions. Copy the license code from the Downloads page of Automation Anywhere. The Installer creates the following folder structure with respective contents under the <Automation Anywhere Directory>

< Automation Anywhere Installation Directory >
- My Tasks
  - Bot Store
    - Retrieve Credentials from PAM360-ManageEngine
      - Error Folder
        - Logs
        - Snapshot
      - Input Folder
      - My Tasks
        - MasterBot.atmx
        - MasterBot-ReadInputFromFile.atmx
- My Metabots
  - ManageEngine-PAM360.mbot

The PAM360 bot package contains two Taskbots that can perform the following functions:

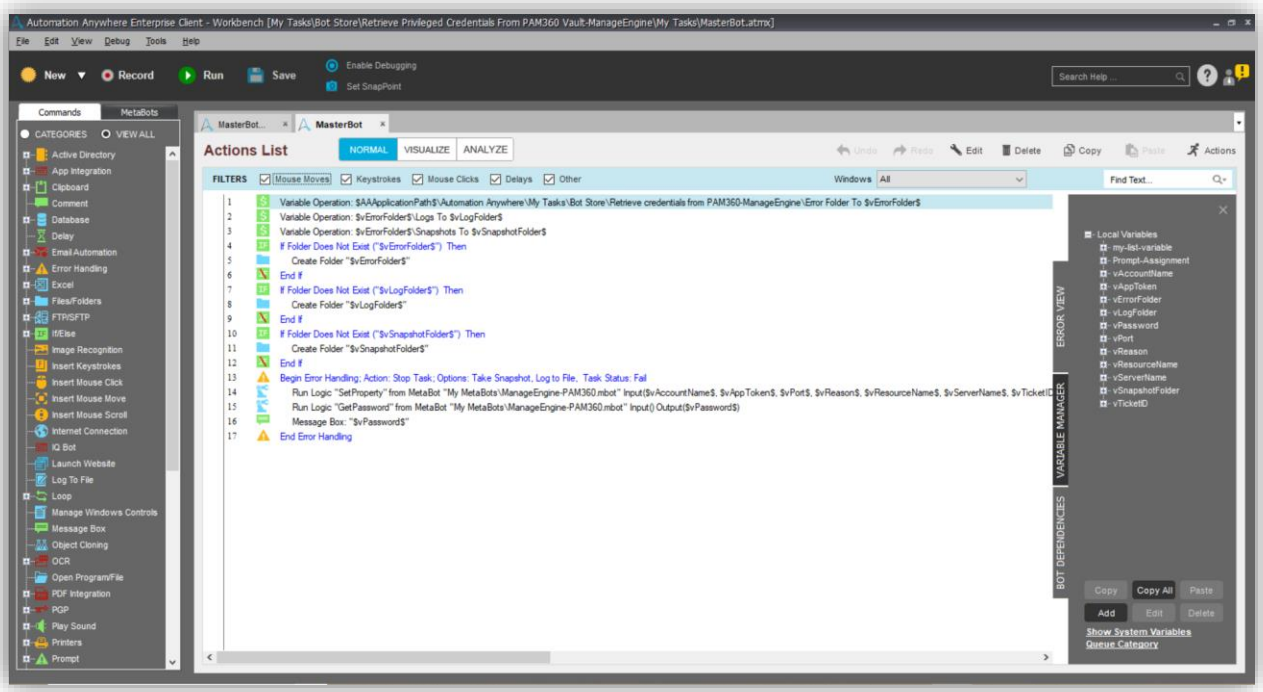
- **MasterBot.atmx** - Password retrieval by providing resource name and account name manually
- **MasterBot-ReadInputFromFile.atmx** - Password retrieval by reading resource ID and account ID from a text file which can be downloaded from PAM360's web interface. Refer to the section 5 to learn how to download the account details from PAM360.

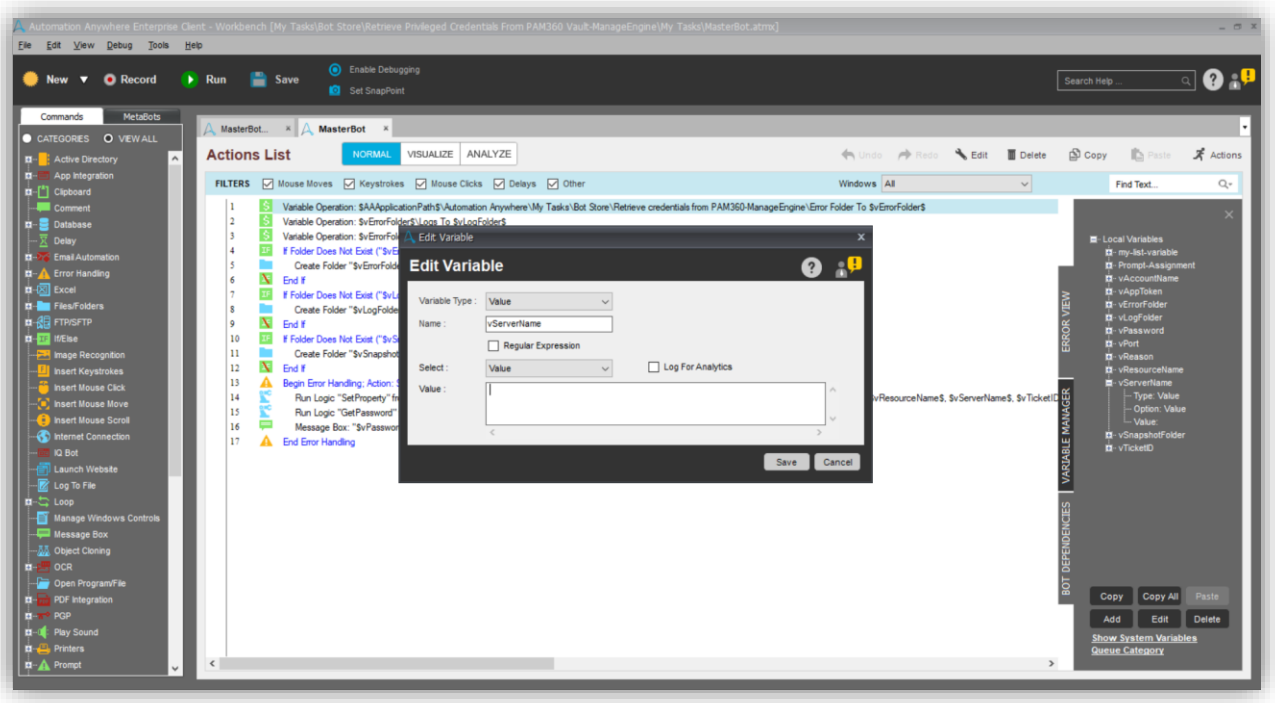
3. Now, open the Automation Anywhere portal and proceed with the further steps below.

3.1 Retrieving Password using Resource Name and Account Name

To fetch password using the Taskbot **MasterBot.atmx,** follow the below steps:

1. In the left pane, under **Tasks >> Bot Store >> Retrieve Credentials from PAM360-ManageEngine**, you will find **MasterBot.atmx** in **My Tasks**. Right click **MasterBot.atmx** and click **Edit**.
2. In the **Variable Manager** on the right pane, the following variables will be listed: **vServerName, vPort, vAccountName, vResourceName, vReason, vAppToken, vTicketID.** Double click on the required variable, the **Edit Variable** window will pop up. Here, enter a value for the selected variable. You need to supply input parameters such as **vAppToken** generated from PAM360, **vPort**, **vServerName, vResourceName, vAccountName**, along with **vReason** and **vTicketID** for password retrieval if applicable.





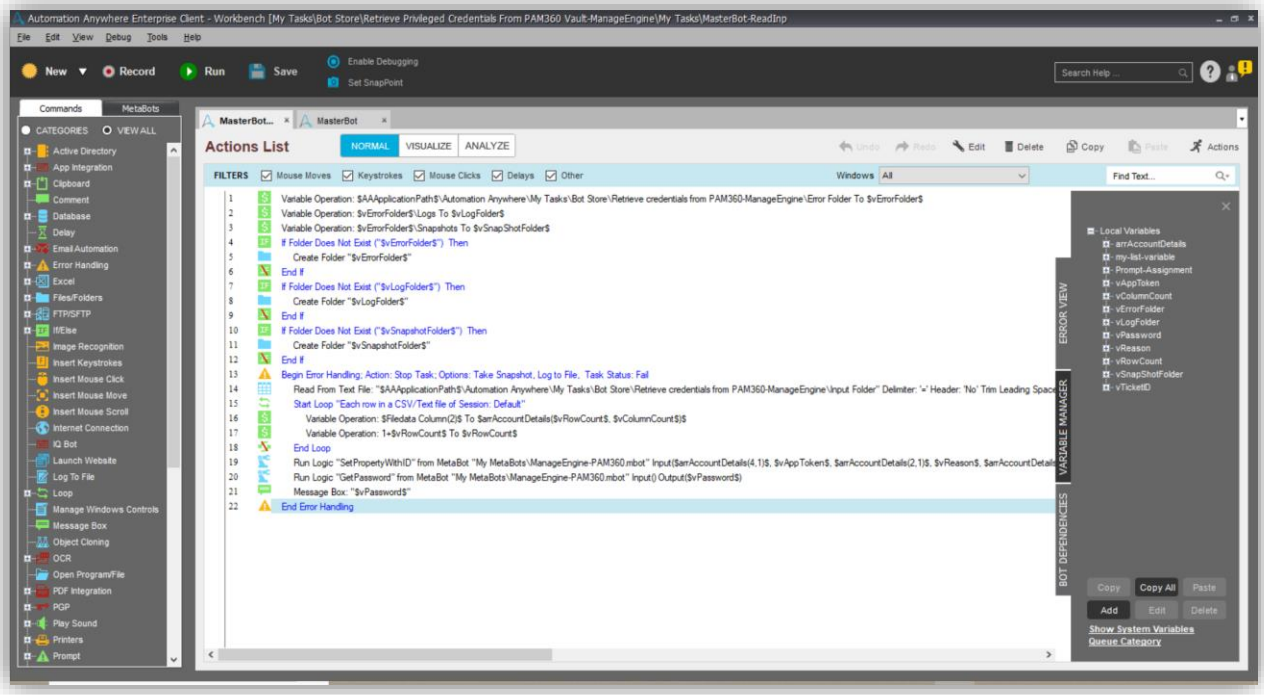
3. Click **Save** from the menu bar at the top and click **Run** to execute the bot. If all the input parameters are given correctly, the bot will fetch the required password from PAM360 and display it in a message box.

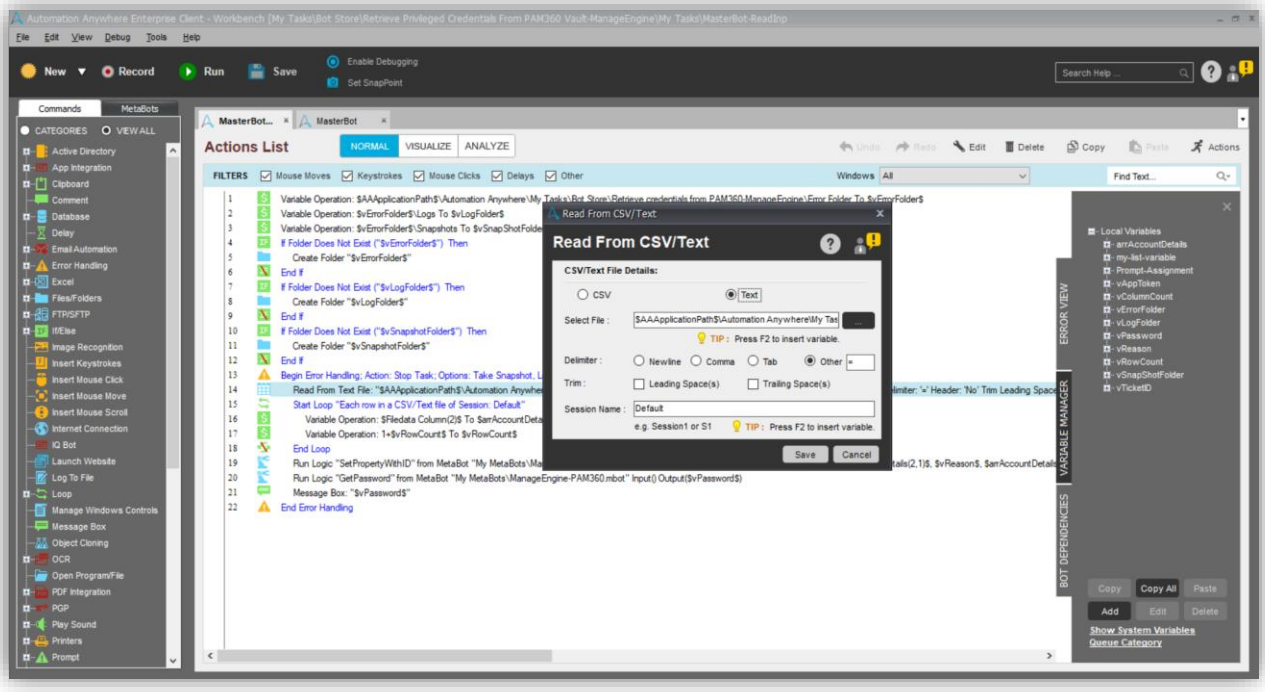
3.2 Retrieving Password using the Read From File Option

To fetch the password using the Read From File option, you need to download the text file containing the resource and account details for a particular account, from PAM360. Refer to section 5 to learn how to download the text file from PAM360.

Once you have the text file saved in your local disk, continue with the below steps:

1. In the left pane, under **Tasks >> Bot Store >> Retrieve Credentials from PAM360-ManageEngine**, you will find **MasterBot-ReadInputFromFile.atmx** in **My Tasks**. Right click **MasterBot-ReadInputFromFile.atmx** and click **Edit**.
2. In the **Actions List**, double click **Read From Text File** (line 14 in the image below). The **Read from CSV/Text** window will pop up. Here, click the browse option to select and add the text file stored in your local disk. By default, the text file downloaded from PAM360 has '=' as the delimiter. Click **Save** to save the changes.





3. The input parameters such as v**Port, vResourceID, vAccountID, vServerName** will be populated directly from the text file. However, it is mandatory to enter the **vAppToken** generated from PAM360. Furthermore, add values for **vReason** and **vTicketID** parameters if applicable.
4. Click **Save** from the menu bar at the top and click **Run** to execute the bot. If all the input parameters are given correctly, the bot will fetch the required password from PAM360 and display it in a message box.

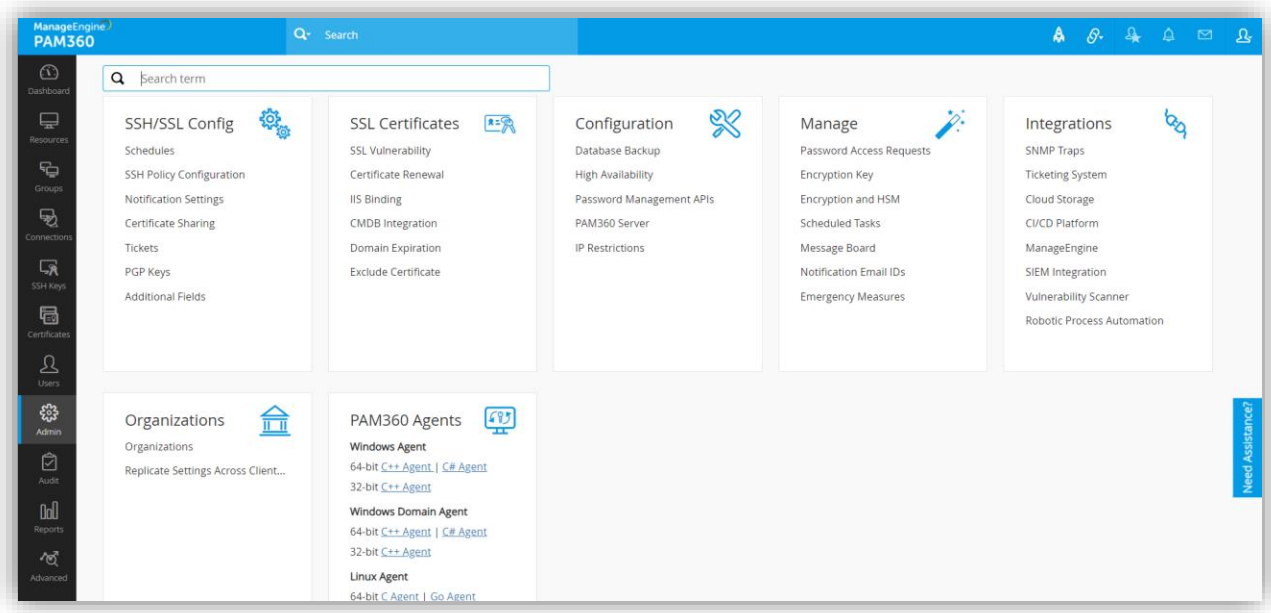
Automation Anywhere set up is complete.

Now that you have completed setting up PAM360's Metabots in the Automation Anywhere portal, follow the below steps to learn how to configure and complete the integration in PAM360.

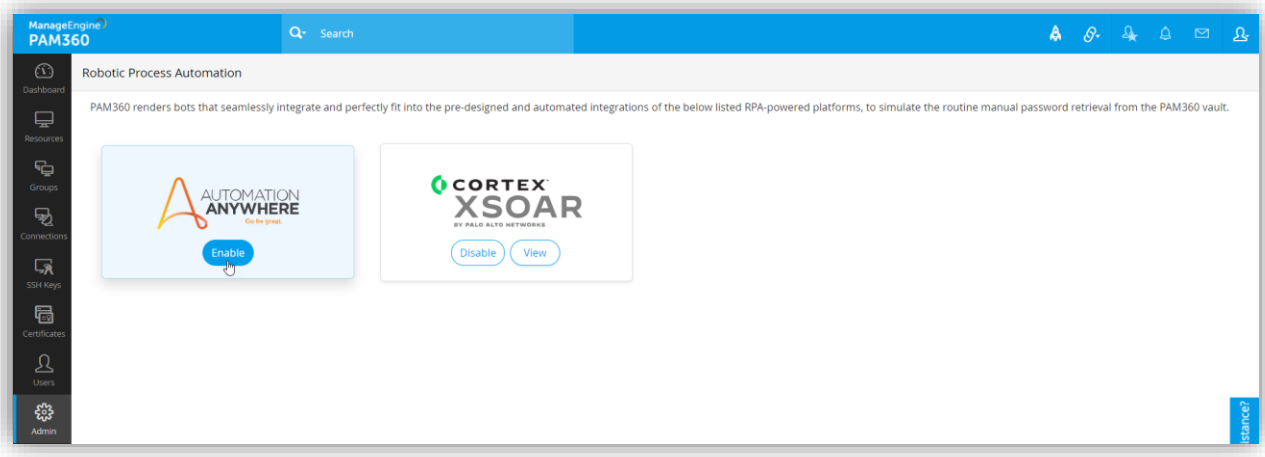
4. Configuring RPA Integration in PAM360

> **Note:** The **Robotic Process Automation** option will be visible only to users with RPA privilege - Administrators, Privileged Administrators and users for whom RPA custom role is enabled.

1. Login to PAM360's web interface and navigate to **Admin >> Integrations >> Robotic Process Automation**.



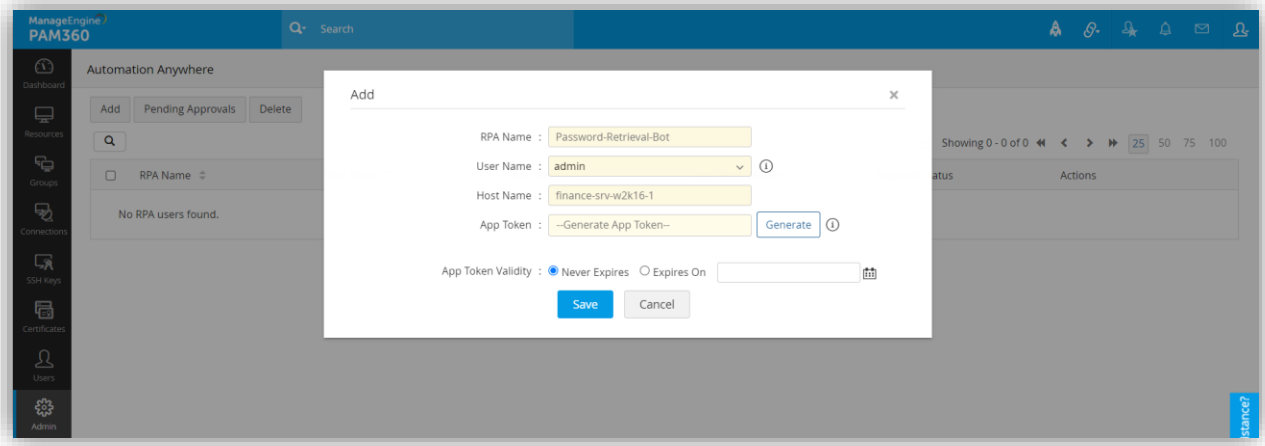
2. Click **Enable** under **Automation Anywhere**.



3. In the new window, there are three options: **Add, Pending Requests**, **Delete**.

4.1 Adding Entries

1. Click **Add** and enter the following attributes to add a new RPA entry for a user:



i. **RPA Name:** Enter a unique name for your reference, e.g. username-hostname

ii. **User Name:** Users that are visible to you in PAM360 will be listed in the drop-down. The user selected here will be the one who can use the App Token in Automation Anywhere from the Host Name specified in the next step. Before the App Token can be used, the request will go through an approval mechanism. Refer to the section 4.3 **Approval Workflow section** below to know how the approval works for different types of users.

iii. **Host Name:** Enter a **Host Name** from which the selected user can use the PAM360 bot after the generated App Token is approved. There can only be one RPA entry for a unique User Name - Host Name combo.

iv. **App Token:** Click **Generate** to generate an App Token. This App Token will become active only after RPA entry request is approved by the selected user. By default, the

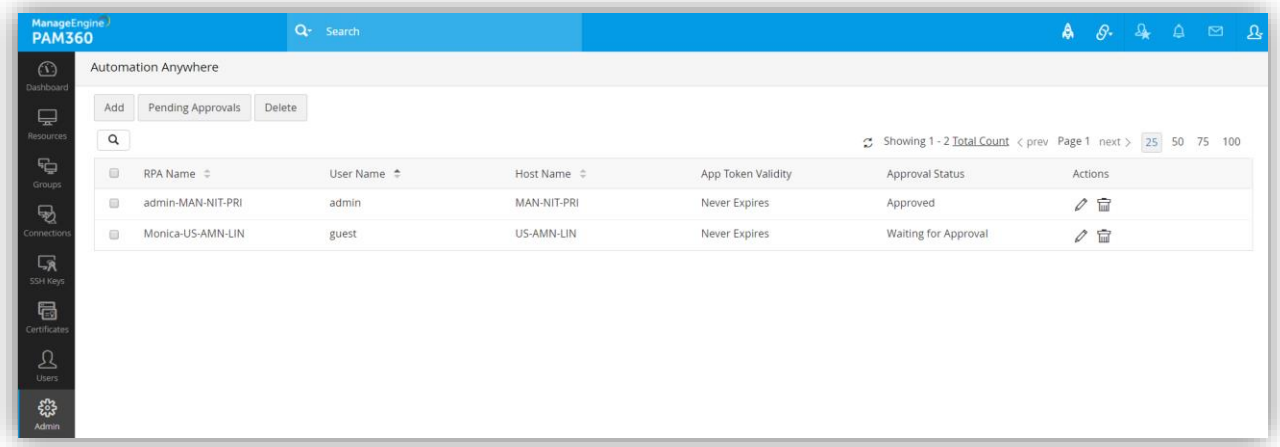
App Token is valid forever. However, you can define a validity period for the App Token in the next step.

v. **App Token Validity: Never Expires** is automatically selected and it will keep the App Token valid forever. Click **Expires On** to set a date for the expiry of the App Token. Click **Save** to add a new entry.

4.2 Editing Entries

To edit an RPA entry, follow the below steps:

1. Click the edit icon under **Actions** beside the required **RPA Name.**
2. Edit the **RPA Name, Host Name** and **App Token**. Once the details are edited, the request will go through the approval mechanism again. The new **App Token** or **Host Name** will be active once the request is approved.



4.3 Approval Workflow for RPA Entries

The **User Name** chosen in the **Add** window can be your own admin user name, another admin user or a non-admin user (Password User or Password Auditor)

Case I - Automatic Approval: If you choose your own user name, the entry will be automatically approved and the App Token will be active right away.

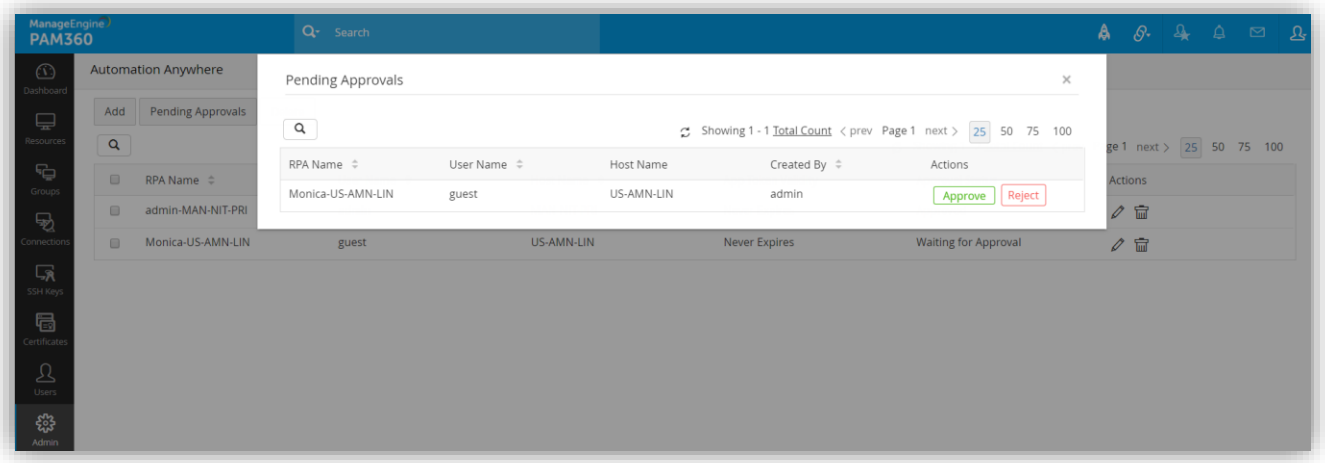
Case II - Awaiting Approval for RPA Privileged Users: If the RPA owner is a user with RPA privilege, then the approval request will be sent to the RPA Owner and will be visible for them under **Pending Requests**. They can review details such as **User Name**, **Host Name**, **Created By** and choose to approve or reject the request. Upon approval, the RPA Owner can either generate a new App Token or use the same one generated when the entry was added. Please note that only the RPA Owner will be able to apply the App Token and use the PAM360 bot in Automation Anywhere. Upon rejection of the request, the RPA entry will be deleted from the menu.

Case III - Awaiting Approval for Users without RPA Privilege: If the RPA owner is not a user with

RPA privilege, then all admins other than the one creating the RPA entry will get the approval request—any one of the admins can approve or reject the request. You can copy the App Token and provide it to the RPA owner after approval from one of the admins.

The App Token will not be valid if one of the following cases is true:

1. The App Token is incorrect.
2. The App Token has expired.
3. Automation Anywhere integration is disabled under **Admin >> Integrations >> Robotic Process Automation**.
4. If the App Token is used from a host different from the one specified while creating the RPA entry.



4.4 Deleting Entries

1. To delete an RPA entry, click the **Delete** icon under **Actions** beside any RPA name. To delete multiple entries, select check boxes beside the RPA names and click **Delete User** from the top bar.
2. Click **Delete** in the confirmation dialog box.

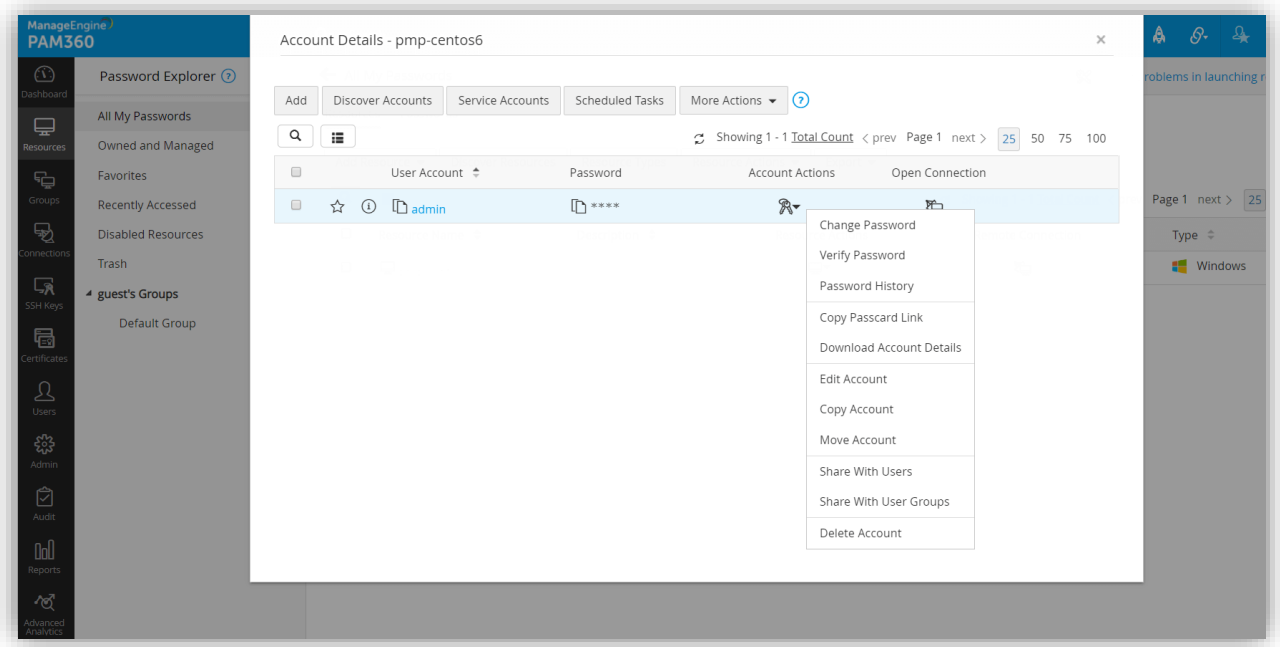
5. Downloading Account Details in PAM360

Automation Anywhere provides an option to add input variables through a text file, in addition to giving the details manually. Follow the below steps to download account details for a particular account in PAM360:

1. Navigate to **Resources** and click a resource name. **Account Details** window will display

all accounts associated with the resource.

2. Click the **Account Actions** drop-down beside an account and choose **Download Account Details** from the drop-down.
3. A text file containing details such as ServerName, Port, ResourceID, AccountID will be exported. The key-value pairs will be separated by the delimiter '=' in the text file.



Integrating PAM360 with Cortex XSOAR

PAM360, a unified Privileged Access Management product from ManageEngine, integrates with Cortex XSOAR by Palo Alto Networks, a robotic process automation (RPA) tool that allows you to build standardized responses using commands created through techniques that incorporate case management, automation, real-time collaboration, and threat intelligence management to serve security teams across the incident lifecycle. At the end of this document, you will have learned the following:

1. Key Benefits of Integration
2. How does the Integration Work?
3. Setting up the PAM360 Instance in Cortex XSOAR
4. Configuring Cortex XSOAR in PAM360
   4.1 Adding Entries
   4.2 Editing Entries
   4.3 Approval Workflow for RPA Entries
   4.4 Deleting Entries

1. Key Benefits of Integration

Through the PAM360 - Cortex XSOAR integration, the commands provided by PAM360 can automate a variety of password-related operations such as creating resources and accounts, fetching passwords, and updating resource and account details. These operations can be used further by Cortex XSOAR to perform any automated tasks.

This integration allows you to securely configure instances in Cortex XSOAR using credentials stored in the PAM360 vault. From the Cortex XSOAR instance, you can reset account passwords, fetch resource and account details without revealing the passwords, enforce automated approval workflows to gain access to passwords.

2. How does the Integration Work?

The PAM360-Cortex XSOAR integration utilizes commands to automatically fetch passwords using resource and account details from PAM360's vault. PAM360 provides various commands covering a variety of automation tasks that can be combined to create a complete endpoint management workflow.

Let's assume a scenario in which an automation task is required to trigger scans on specified endpoints in your environment. The credentials to connect to the endpoints are stored in the PAM360 vault. By integrating PAM360 with Cortex XSOAR, you can create an automated setup that uses the commands provided by PAM360 to retrieve passwords and other account details from the PAM360 vault that can be put to use based on your requirements.

3. Setting up the PAM360 Instance in Cortex XSOAR

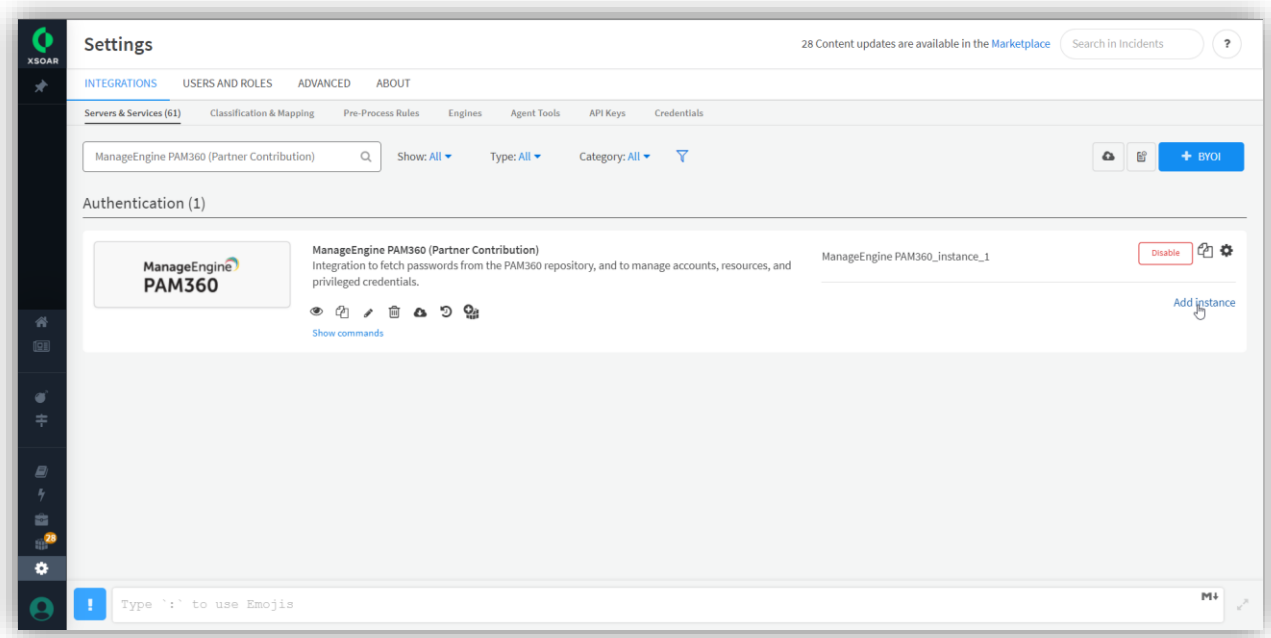
Prerequisite

A working instance of Cortex XSOAR is required to complete the integration with PAM360.

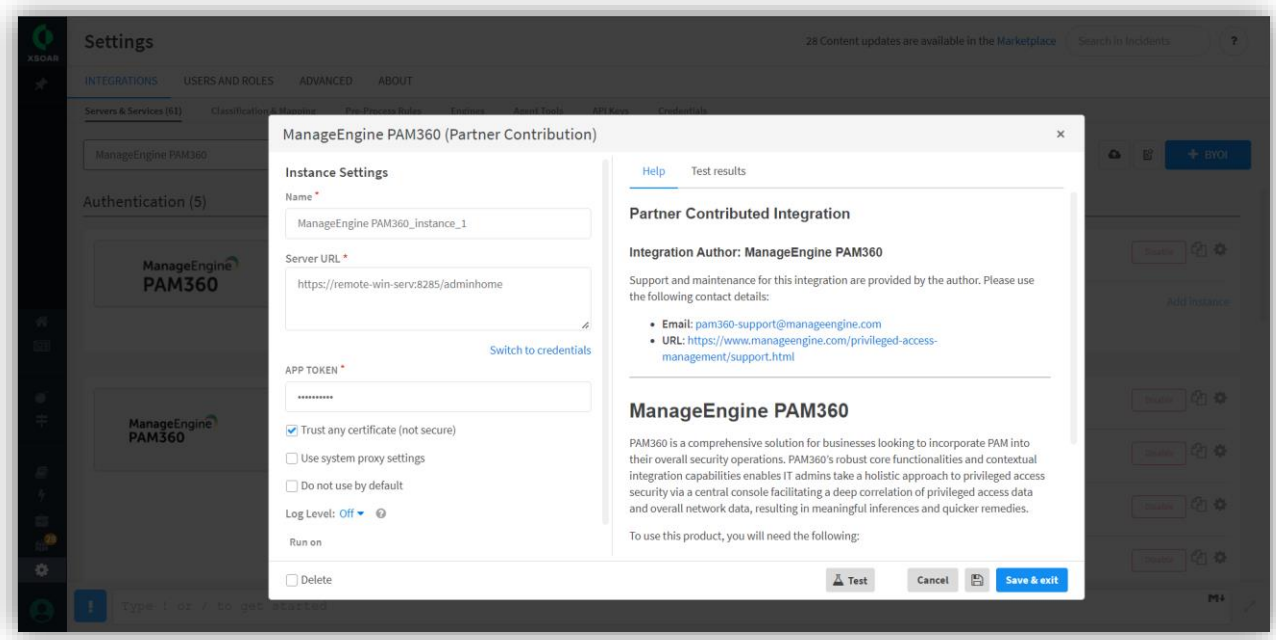
First-time users, click here to sign up for Cortex XSOAR and get started.

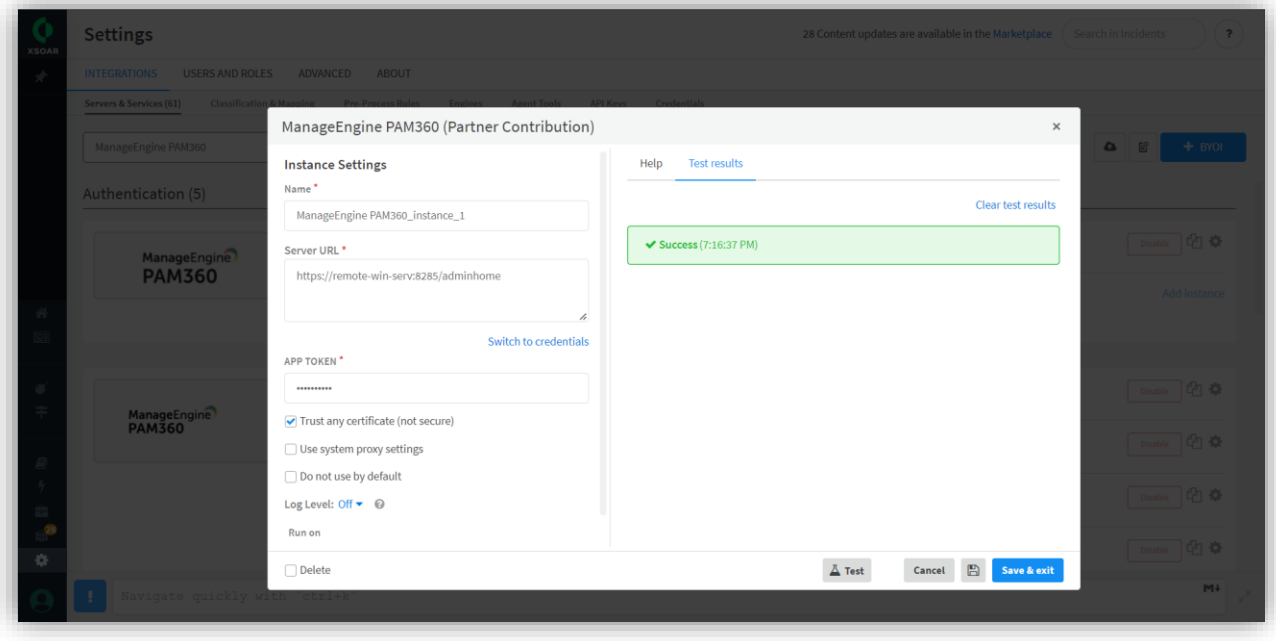
Follow the below steps to set up the Cortex XSOAR portal and add the PAM360 instance in there:

1. Login to the Cortex XSOAR portal and navigate to the **Marketplace** option available in the left pane.
2. Here, search for the ManageEngine PAM360 application and click **Install**.
3. After installation, go to **Settings >> Integration** and you will find it under the **Servers and Services** category.



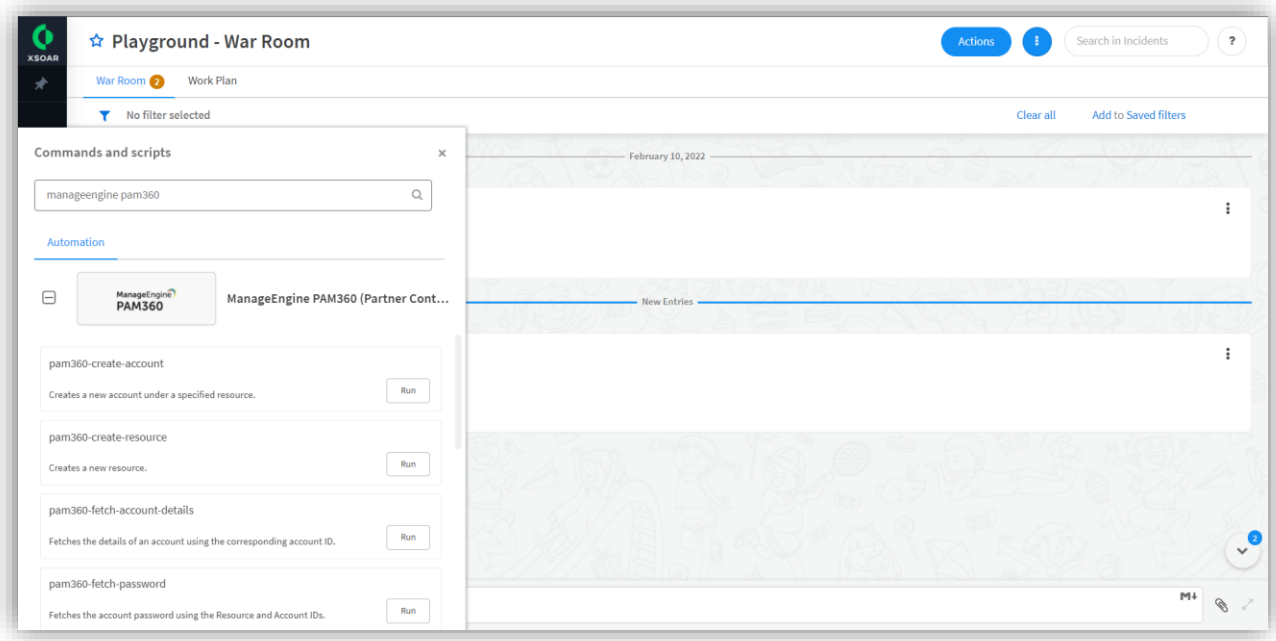
4. To add PAM360 as an instance, under the PAM360 application, click **Add Instance**.
5. Here under **Instance Settings**, add parameters such as name, PAM360 Server URL, and the App Token generated from the PAM360 interface. Once done, click the **Test** option to check the connection. The set up is complete when you see a success message.

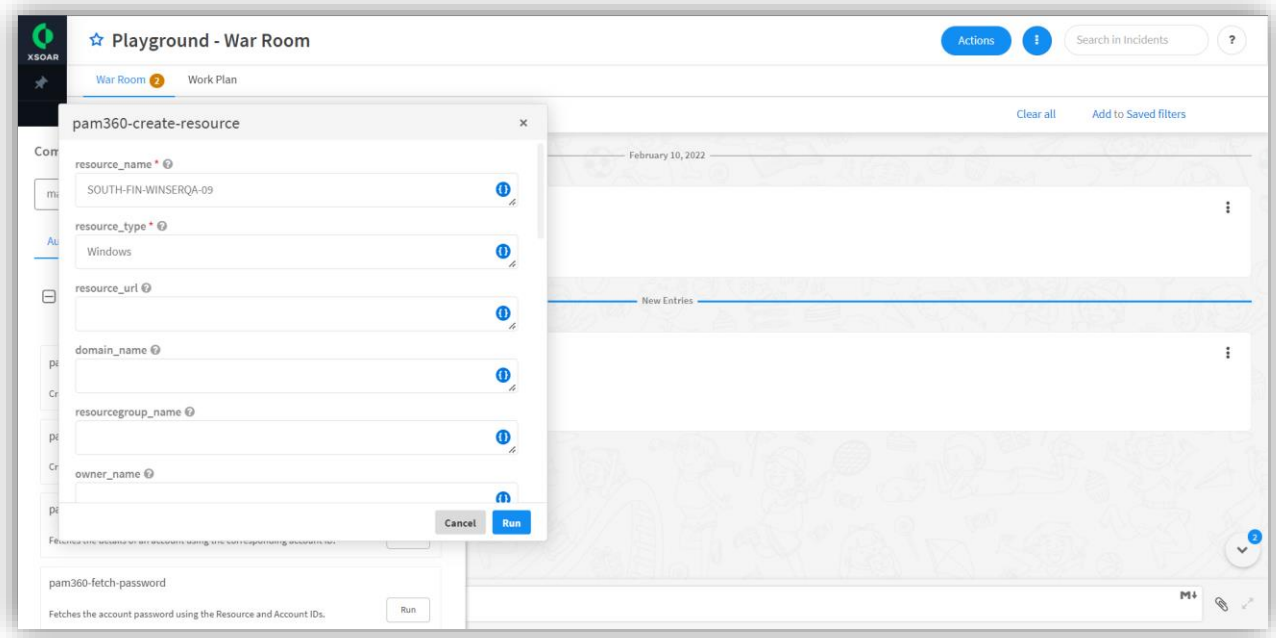


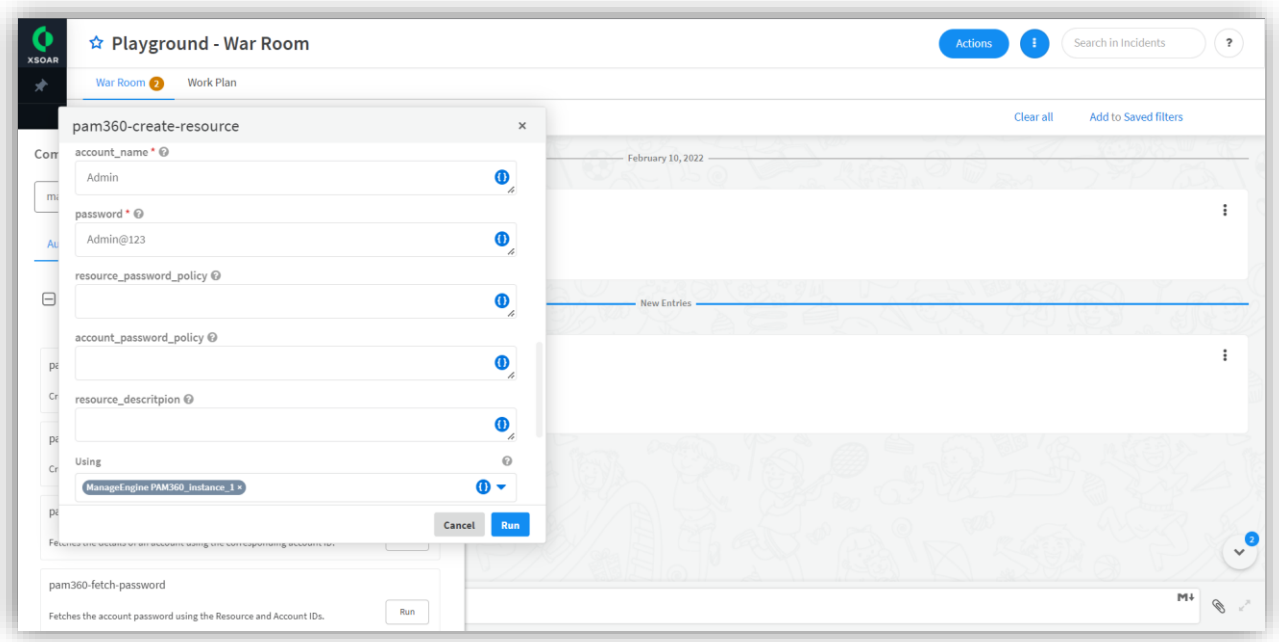


6. Once you have set up the PAM360 Instance in the Cortex portal, you can view and run the PAM360 commands by adding relevant input parameters. PAM360's commands work using the REST API, therefore it is vital to provide appropriate input data for seamless results.
7. In the Playground - War Room page, search for your PAM360 Instance under **Commands and scripts**. Here, you can view all the commands offered by PAM360. Click Run beside each command to add parameters necessary for each command. For example, for the command pam360-create-resource, enter the following attributes for successful creation of a new resource: **Resource Name, Resource Type, Account Name, Account Password**, and choose a valid PAM360 instance added in the Cortex portal.

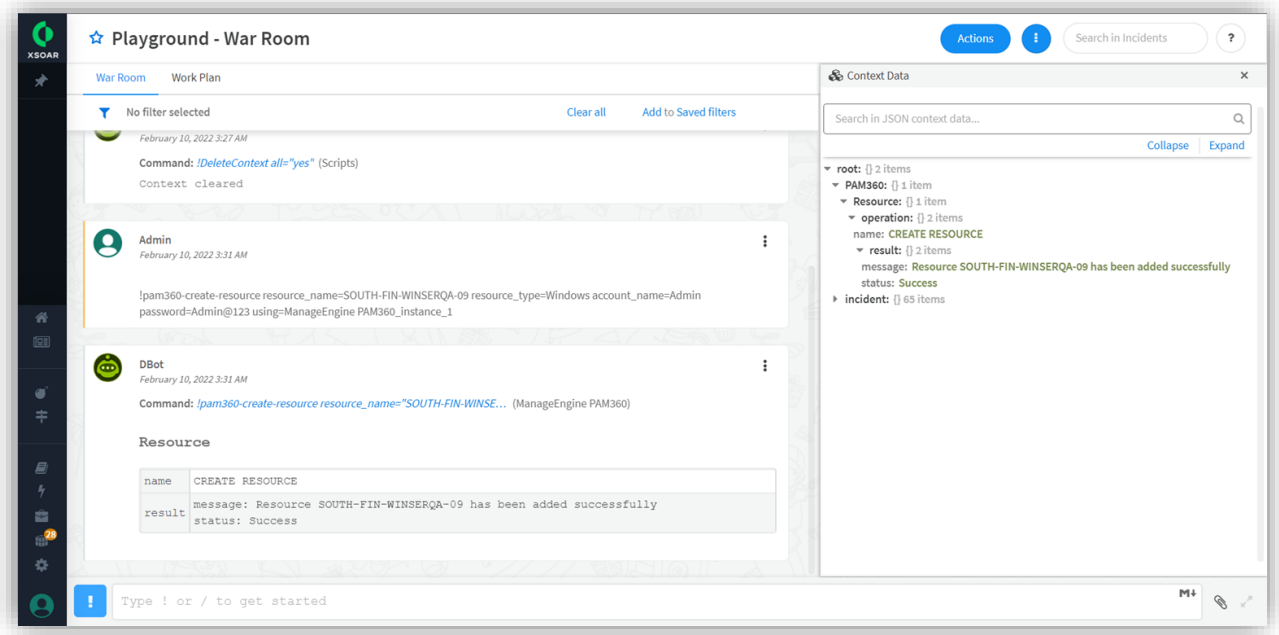
Now, click **Run** to run the command.







8. For each command invoked, the status will be displayed as a **DBot** message in the Playground - War Room page. To view detailed output results of the commands, click the ellipses beside the **Actions** option at the top and click **Context Data.**



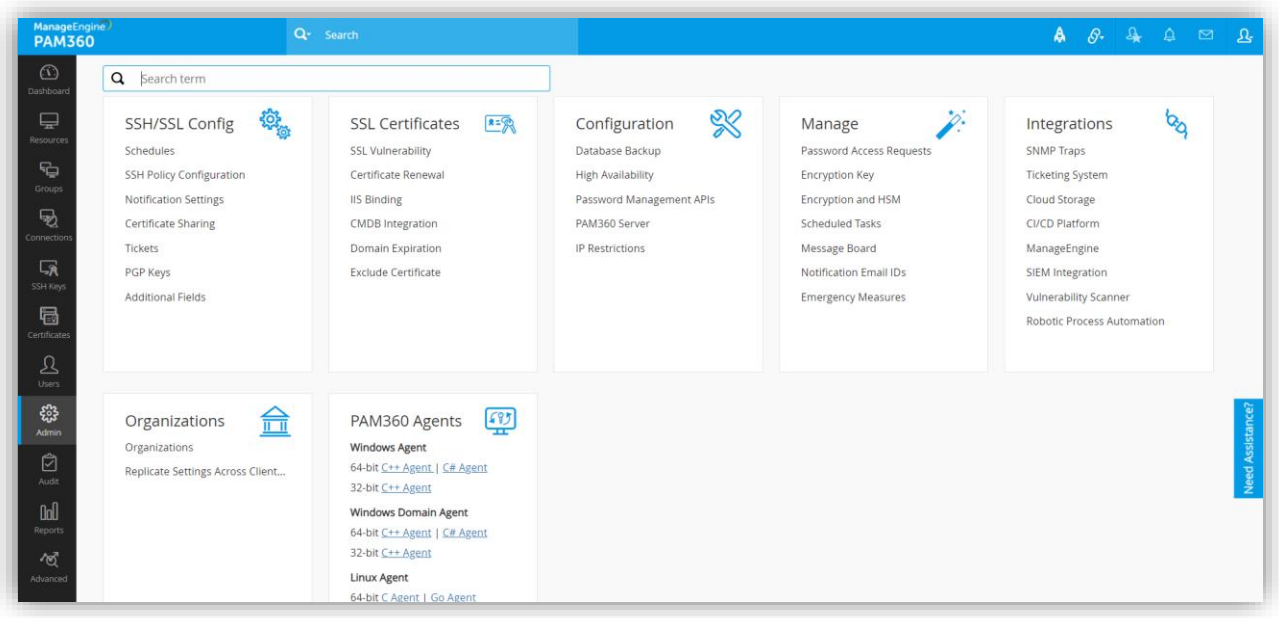
9. Below is a list of commands offered by PAM360. Click each link for samples of input and output data for each command:

Commands	Description
pam360-create-resource	To create resources.
pam360-create-account	To create accounts.
pam360-update-resource	To update the attributes of a resource.
pam360-update-account	To update the attributes of an account.
pam360-list-all-resources	To list all resources owned by and shared to the user.
pam360-list-all-accounts	To list all accounts owned by and shared to the user.
pam360-fetch-account-details	To fetch the details of an account.
pam360-fetch-resource-account-id	To fetch the resource and account IDs.
pam360-fetch-password	To fetch a password.
pam360-update-account-password	To update the password of an account.

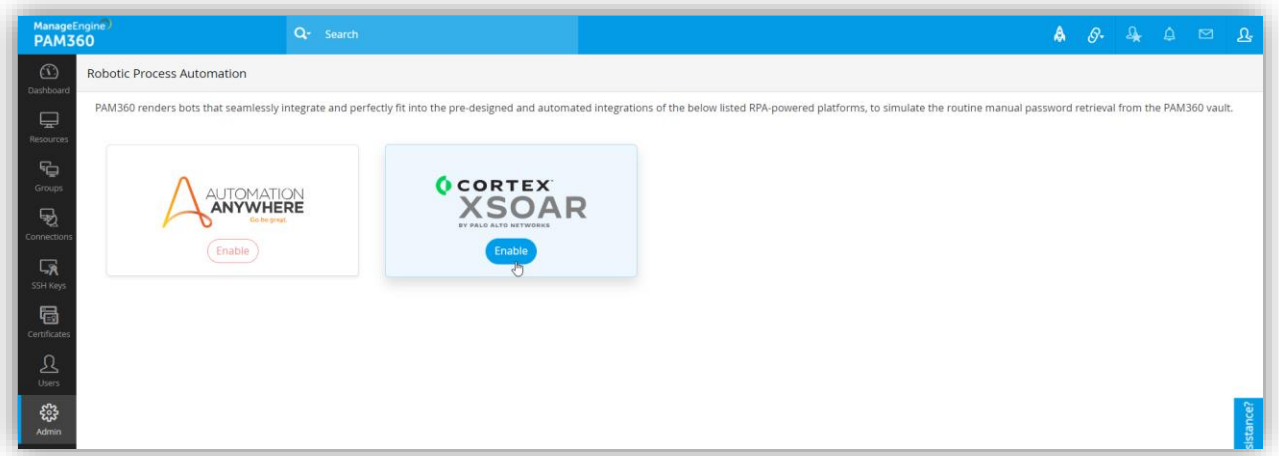
4. Configuring Cortex XSOAR in PAM360

> **Note:** The **Robotic Process Automation** option will be visible only to users with RPA privilege - Administrators, Privileged Administrators and users for whom RPA custom role is enabled

1. Login to PAM360's web interface and navigate to **Admin >> Integrations >> Robotic Process Automation**.



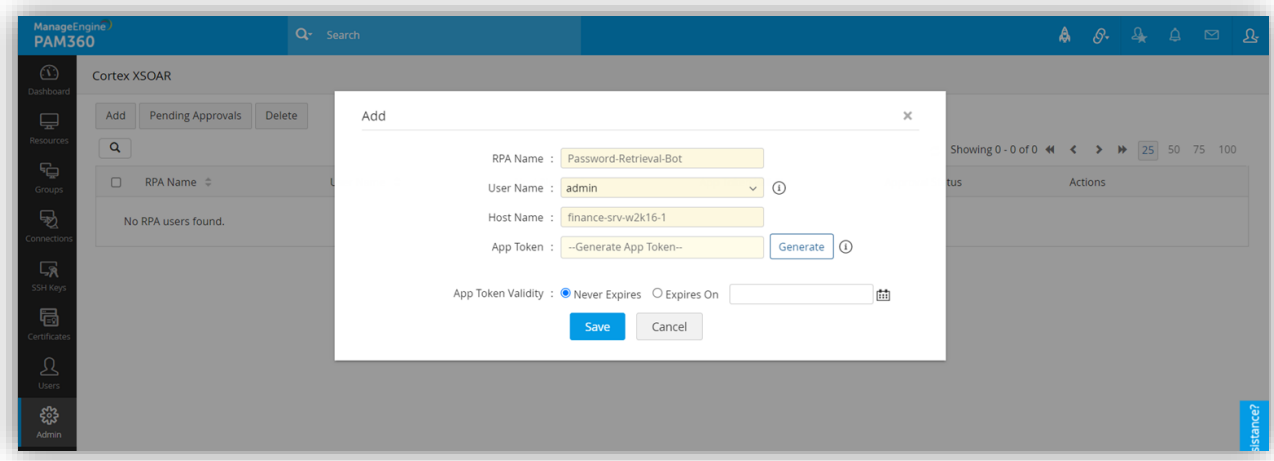
2. Click **Enable** under **Cortex XSOAR**.



3. In the new window, there are three options: **Add, Pending Requests, Delete**.

4.1 Adding Entries

1. Click **Add** and enter the following attributes to add a new RPA entry for a user.



i. **RPA Name:** Enter a unique name for your reference, e.g. Password-Retrieval-Bot.

ii. **User Name:** All users who have web access to PAM360 will be listed in the drop-down. The user selected here will be the one who can use the App Token in Cortex XSOAR from the Host Name specified in the next step. Before the App Token can be used, the request will go through an approval mechanism. Refer to the section 4.3 Approval Workflow for RPA Entries section to know how the approval works for different types of users. Please note that if you choose your own user name, the RPA entry will be auto-approved and the App Token generated will be active right away.

iii. **Host Name:** Enter a **Host Name** from which the selected user can use PAM360 commands after the generated App Token is approved. There can only be one RPA entry for a unique User Name - Host Name combo.

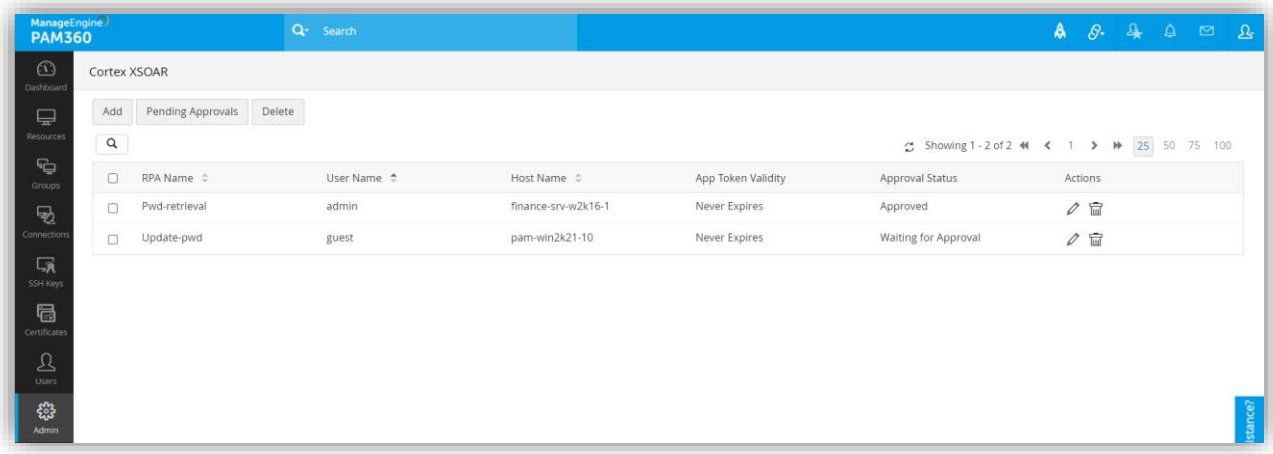
iv. **App Token:** Click **Generate** to generate an App Token. This App Token will become active only after RPA entry request is approved by the selected user. By default, the App Token is valid forever. However, you can define a validity period for the App Token in the next step.

v. **App Token Validity: Never Expires** is automatically selected and it will keep the App Token valid forever. Click **Expires On** to set a date for the expiry of the App Token. Click **Save** to add a new entry.

4.2 Editing Entries

To edit an RPA entry, follow the below steps:

1. Click the edit icon under **Actions** beside the required **RPA Name.**
2. Edit the **RPA Name, Host Name** and **App Token**. Once the details are edited, the request will go through the approval mechanism again. The new **App Token** or **Host Name** will be active once the request is approved.



4.3 Approval Workflow for RPA Entries

The **User Name** chosen in the **Add** window can be your own admin user name, another admin user or a non-admin user (Password User or Password Auditor)

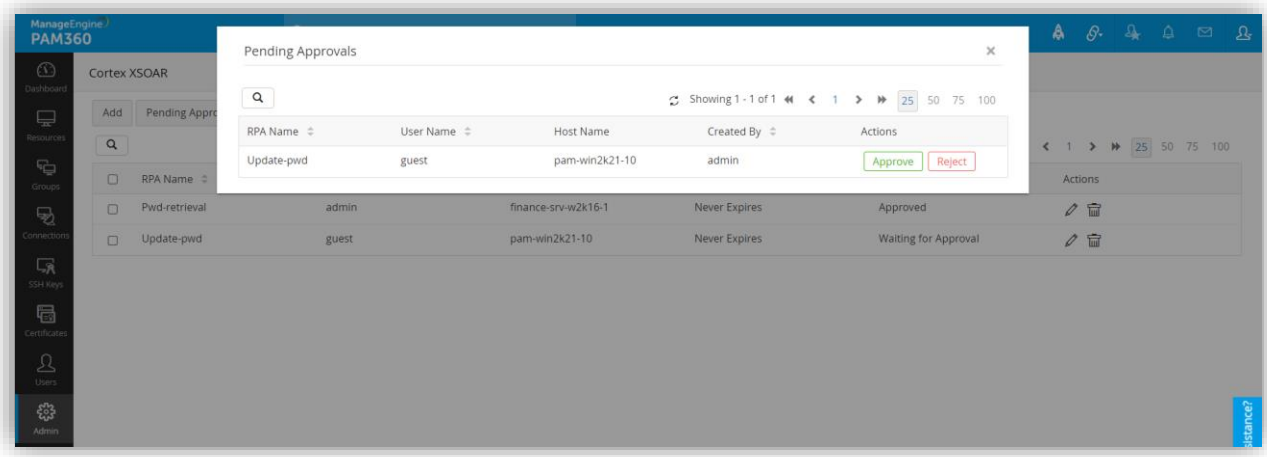
Case I - Automatic Approval: If you choose your own user name, the entry will be automatically approved and the App Token will be active right away.

Case II - Awaiting Approval for RPA Privileged Users: If the RPA owner is a user with RPA privilege, then the approval request will be sent to the RPA Owner and will be visible for them under **Pending Requests**. They can review details such as **User Name**, **Host Name**, **Created By** and choose to approve or reject the request. Upon approval, the RPA Owner can either generate a new App Token or use the same one generated when the entry was added. Please note that only the RPA Owner will be able to apply the App Token and use PAM360 commands in Cortex XSOAR. Upon rejection of the request, the RPA entry will be deleted from the menu.

Case III - Awaiting Approval for Users without RPA Privilege: If the RPA owner is not a user with RPA privilege, then all admins other than the one creating the RPA entry will get the approval request—any one of the admins can approve or reject the request. You can copy the App Token and provide it to the RPA owner after approval from one of the admins.

The App Token will not be valid if one of the following cases is true:

1. The App Token is incorrect.
2. The App Token has expired.
3. Cortex XSOAR integration is disabled under **Admin >> Integrations >> Robotic Process Automation**.
4. If the App Token is used from a host different from the one specified while creating the RPA entry.



4.4 Deleting Entries

1. To delete an RPA entry, click the **Delete** icon under **Actions** beside any RPA name. To delete multiple entries, select check boxes beside the RPA names and click **Delete User** from the top bar.
2. Click **Delete** in the confirmation dialog box.

Integrating PAM360 with Kubernetes

PAM360, a unified Privileged Access Management product from ManageEngine, integrates with Kubernetes, an open-source container orchestration tool that facilitates automation of software deployment, helps to scale and manage applications effectively.
At the end of this section, you will have learned the following:

1. Key Benefits of Integration
2. How does the Integration Work?
3. Configuring Kubernetes Integration in PAM360
4. Fetching and Managing Secrets
5. Mapping Secrets to Resources
6. Limitations
7. Glossary of Terminologies

1. Key Benefits of Integration

This integration helps you to fetch secrets stored in the Kubernetes clusters and manage them from the PAM360 interface—you can fetch, manage, and periodically rotate secrets obtained from multiple Kubernetes clusters. Through the integration, you can achieve collaborative management of the Kubernetes secrets used in your enterprise. Once the fetched secrets are added to the PAM360 repository, you can perform a variety of operations to manage them, such as updating the secrets through cluster sync, rotating the secret keys, and enforcing access control on the Kubernetes resources to provide controlled access to the sensitive secrets. PAM360 records extensive audit trails for all operations performed on the Secrets that are stored in the repository.

2. How does the Integration Work?

The Kubernetes-PAM360 integration utilizes API responses to fetch secrets from the Kubernetes server and bring them into the PAM360 repository as resources, where they can be managed and shared. Secrets from multiple Namespace clusters can be fetched and managed from PAM360.
PAM360 functions like a repository, where secrets from various Kubernetes clusters, invoked for different tasks, can be discovered and stored. The Kubernetes secrets fetched from their respective Namespaces are added as accounts within the resources and stored under the resource type 'Kubernetes'. The accounts are available as downloadable .json files.

Example of a Kubernetes Secret

```
apiVersion: v1
kind: Secret
metadata:
  name: pam-win8-32-0ex097
  namespace: pam360-com
type: Opaque
data:
  admin: dXNlcm5hbWU=
  sysadmin: dXNlcm5hbWU=
  user-5841: dXNlcm5hbWU=
  automation: dXNlcm5hbWU=
  service-acc: dXNlcm5hbWU=
  local-admin: dXNlcm5hbWU=
```

Note: The secret file (.json) may contain single or multiple keys depending on your Kubernetes configuration.

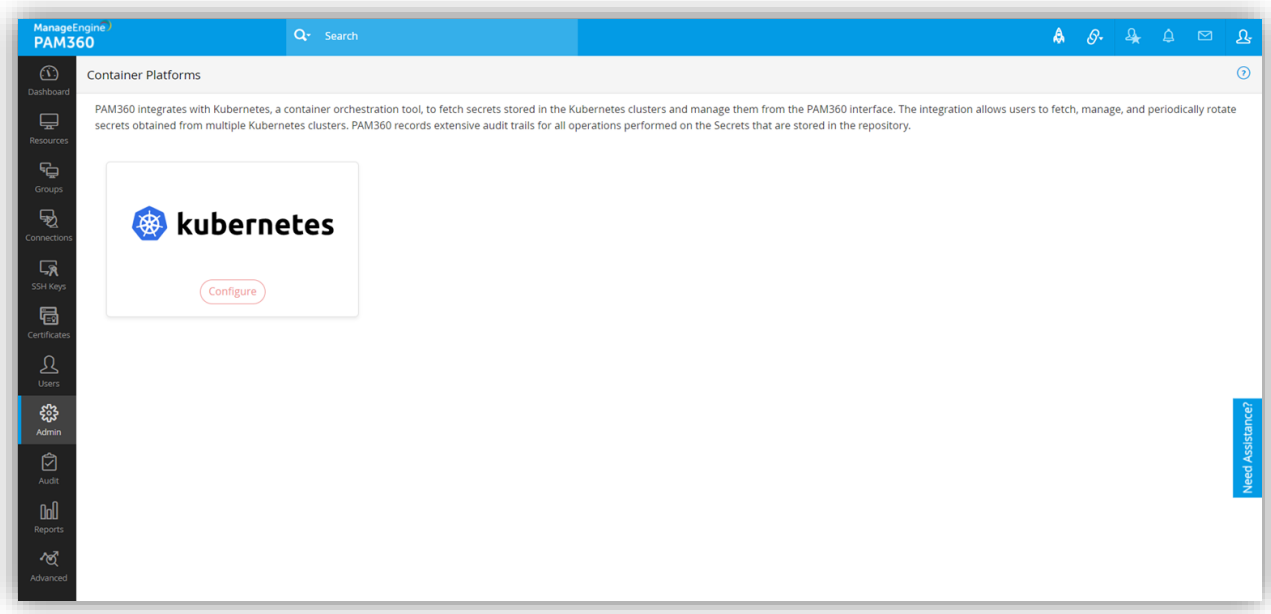
3. Configuring Kubernetes Integration in PAM360

Prerequisites

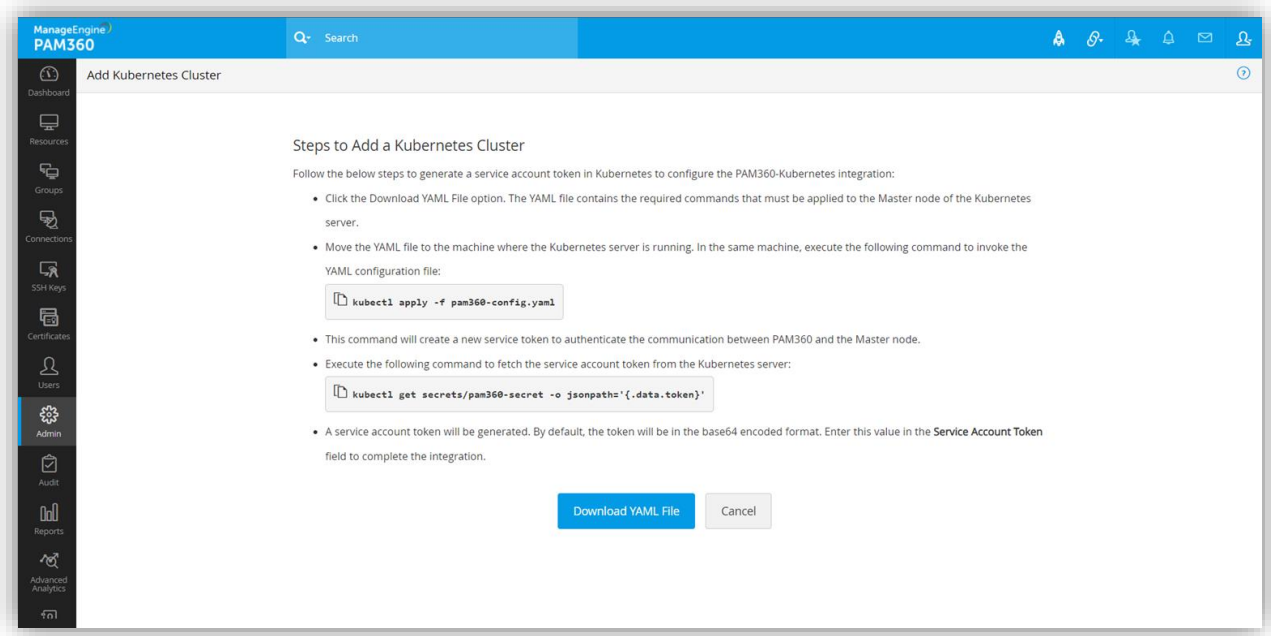
1. Import the Kubernetes server certificate in PAM360
   i. Copy the SSL certificate of the host where Kubernetes is running and paste it under the path **<PAM360 Installation Folder>/bin**.
   ii. From the **<PAM360 Installation Folder>/bin** directory, execute the following command: **importCert.bat <name of the server certificate mentioned above**
   iii. You have successfully added the Kubernetes server certificate to the PAM360 certificate store.

3.1 Steps to Download YAML File from PAM360

1. Navigate to **Admin >> DevSecOps >> Container Platforms.**
2. In the integration page, click **Configure** on the Kubernetes option.



3. To begin the configuration process, you must first download the YAML file from the PAM360 interface. The YAML file contains the necessary commands that must be applied to the Master node of the Kubernetes server. In this window, click **Download YAML File** to proceed.



3.2 Steps to Obtain the Service Account Token in the Kubernetes Server

1. Move the YAML file to the machine where Kubernetes server is running. Execute the following command to invoke the YAML configuration file.

```
kubectl apply -f pam360-config.yaml
```

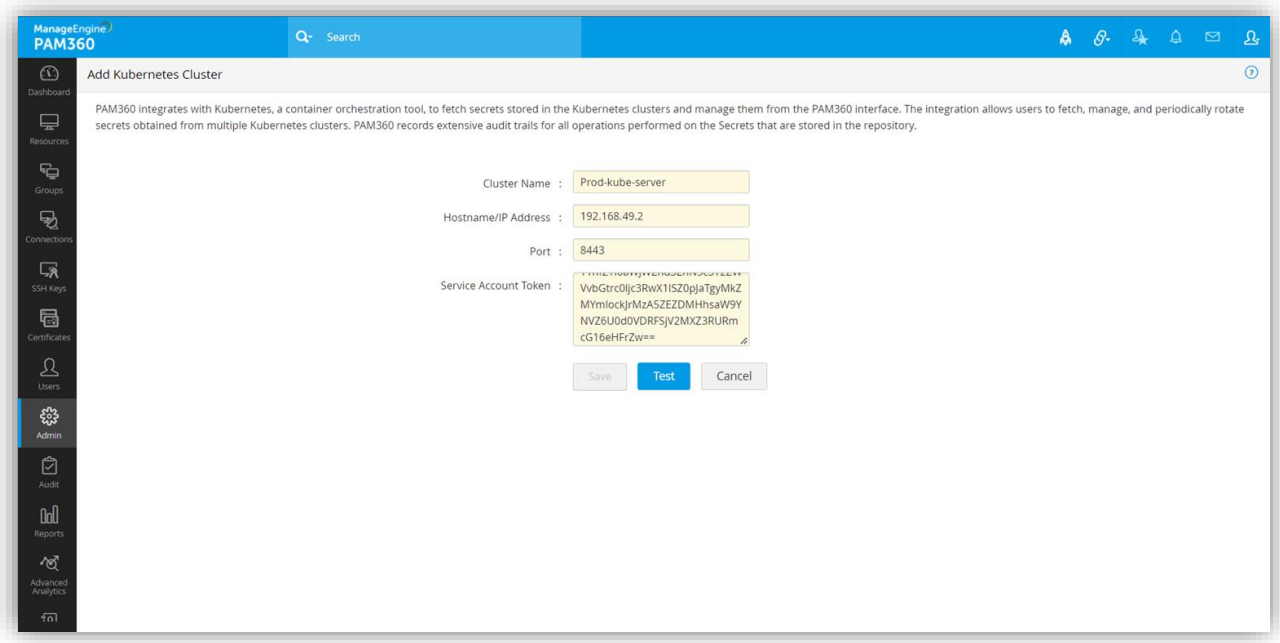
2. This command will create a new service token to authenticate the communication between PAM360 and the Master node.
3. Now, execute the following command to fetch the service account token from the Kubernetes server:

```
kubectl apply -f pam360-config.yaml
```

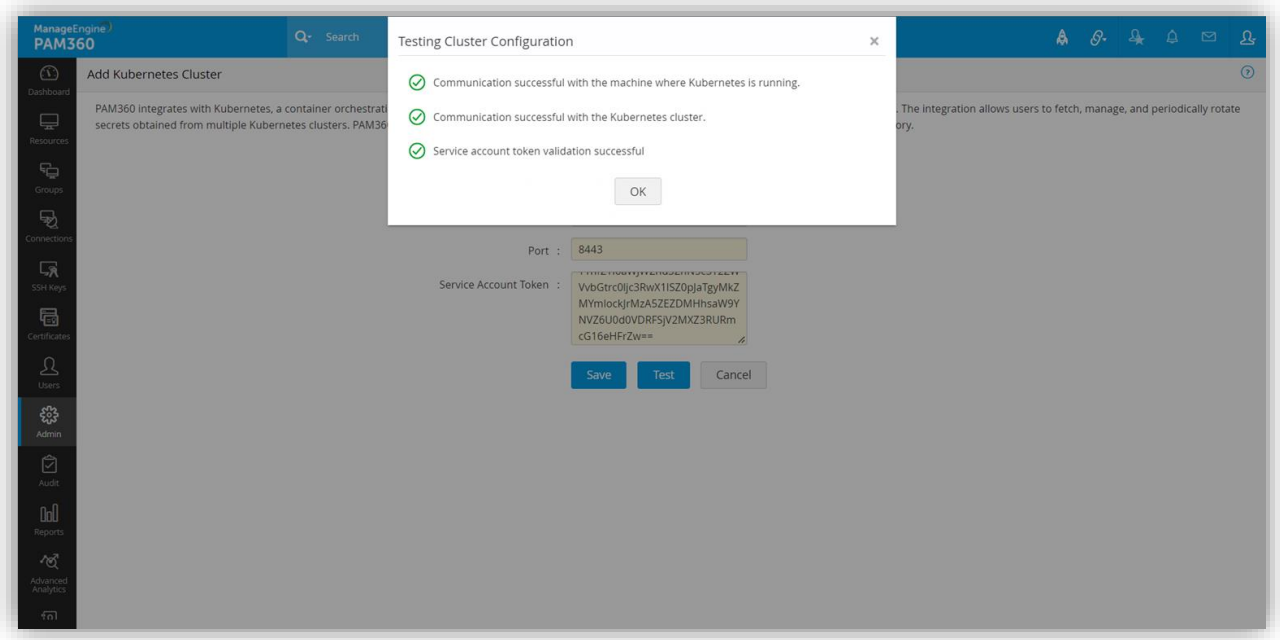
4. A service account token will be generated. By default, the token will be in the base64 encoded format. Copy this service account token to configure the integration in PAM360.

3.3 Steps to Configure the Integration in the PAM360 Interface

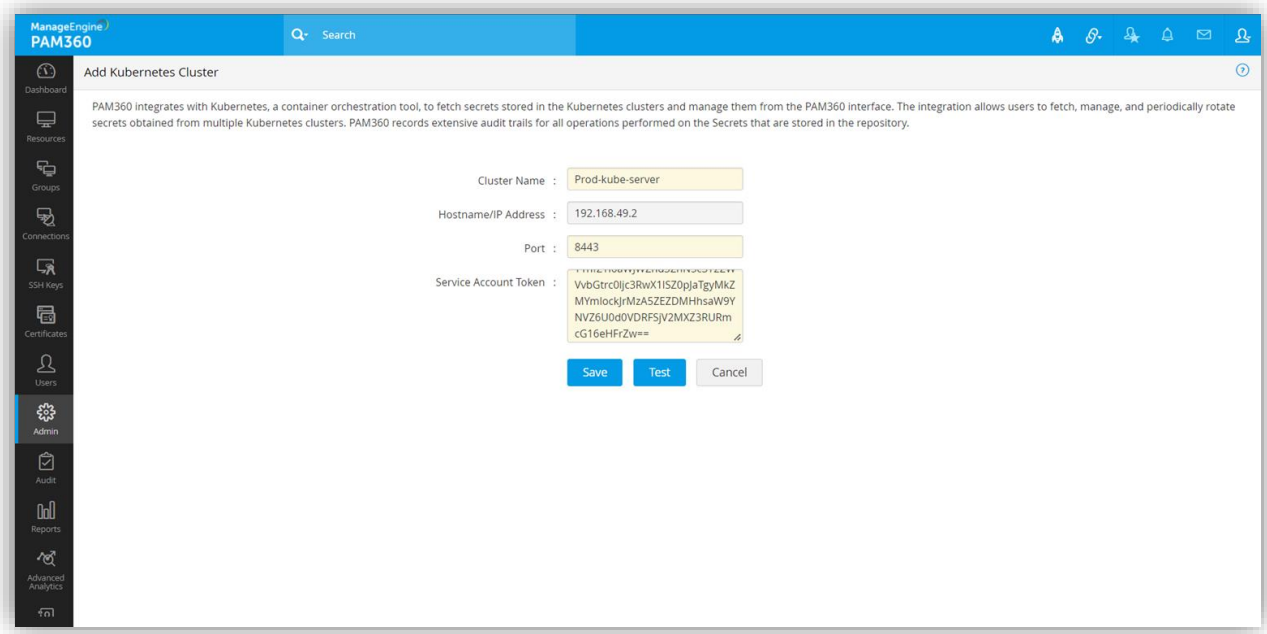
1. Now, open the PAM360 interface once again and navigate to **Admin >> DevSecOps >> Container Platforms** and click **Kubernetes**.
2. In this window, add the following attributes to create a new Kubernetes cluster in PAM360:
   i. Cluster Name
   ii. Hostname of the machine where the Kubernetes server is running
   iii. The Service account token from the previous step.



3. Click **Test**. This operation will test the cluster configuration and ensure that communication between PAM360 and Kubernetes can be established. PAM360 performs three checks before establishing the connection:
    i. Verifies if it can communicate with the host machine where Kubernetes server is running.
    ii. Verifies if it can communicate with the Kubernetes cluster.
    iii. Authenticates the service account token.



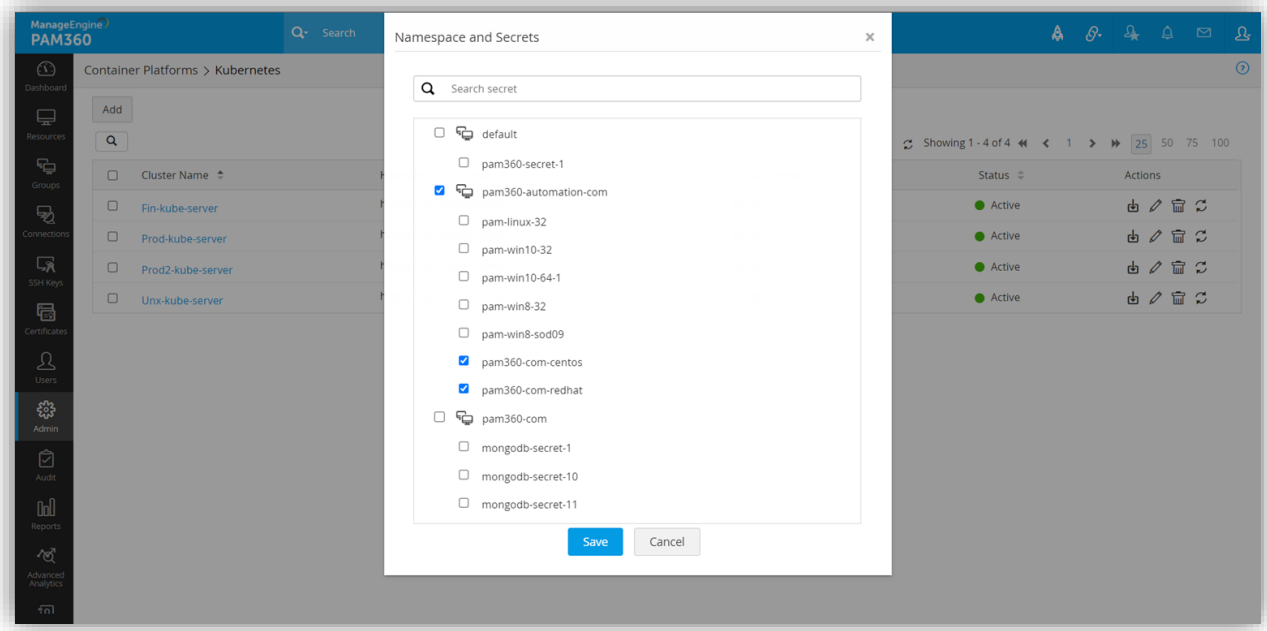
4. Click **Save** to complete the configuration. You can save the configuration details only if the test is successful.



4. Fetching and Managing Secrets

Once you have saved the configuration details, the next step is to fetch secrets from the Kubernetes cluster. Follow the below steps:

1. In the **Fetched Secrets** window that appears, a list of Namespaces and their corresponding secrets are displayed. Select the required Namespaces or individual secrets and Click **Save** to start fetching the secrets.
2. In the **Kubernetes Cluster** page, click the cluster name to display all the details related to the Namespace and the cluster in the **Namespace and Secrets** window.



3. A new cluster with the Kubernetes server details you provided will be displayed on this page, along with the status of the Kubernetes server and the operations to be performed. There are four main operations you can perform on the cluster:
    i. **Fetch**
    ii. **Edit**
    iii. **Delete**
    iv. **Sync Secrets**

    i. Fetch
    Click the **Fetch** icon to fetch Namespaces from the Kubernetes server. The cluster will be named in the format Namespace name - Cluster Name you specified while creating the cluster.

    ii. Edit
    Click the **Edit** icon to change the Kubernetes configuration details.

    iii. Delete
    Click **Delete** to remove the cluster. To add it back, you must follow step 3 and reconfigure it. Please note that the Delete operation will remove only the secret association and not the resources created via this cluster, which will still be available under the Resources tab. We recommend you delete the resources manually to avoid possible conflicts.

    iv. Sync Secrets
    Use this option to update the list of secrets fetched from the Kubernetes cluster already added to PAM360. In other words, if a new set of secrets is added to a cluster in the Kubernetes server, the sync option will fetch all the additional secrets added after the initial fetch operation in PAM360 and keep the cluster information in sync with the Kubernetes server.

Real time scenario

John is an IT admin who manages a critical database. The database key required for authentication is a critical entity that needs to be stored away securely. For this purpose, John saves the database key within multiple Kubernetes secrets. Now, he needs a secure repository to store the Kubernetes secrets and manage them from a single interface.

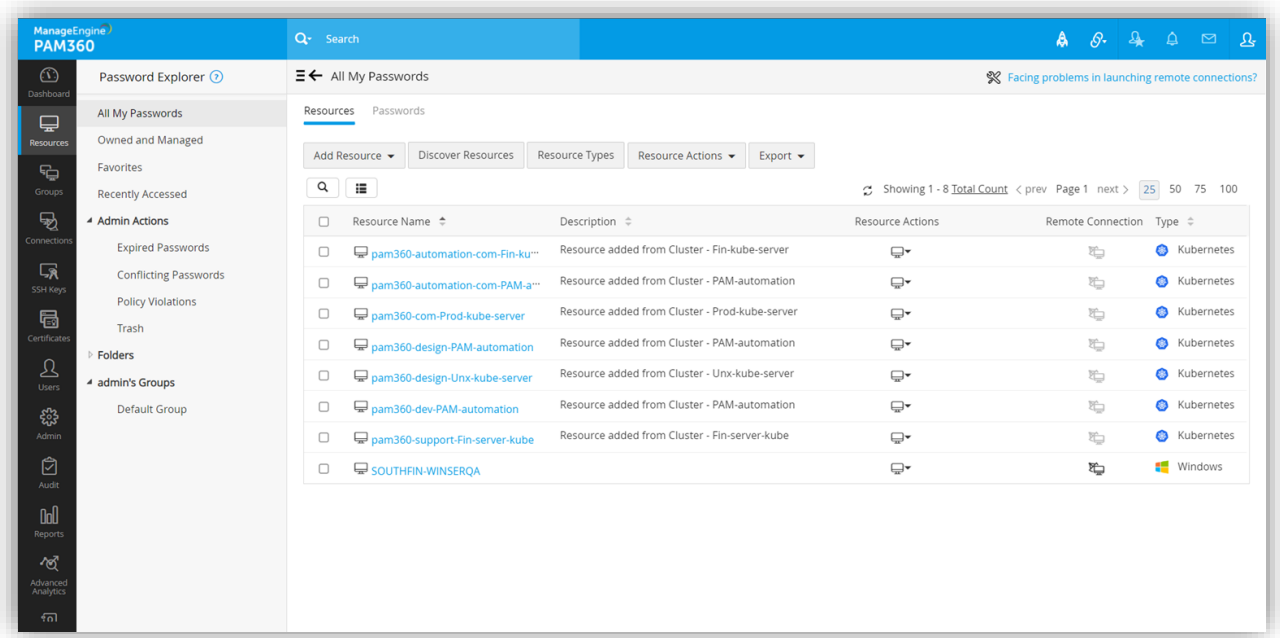
Here comes the PAM360-Kubernetes integration into play. The integration allows John to choose and fetch secrets stored in Kubernetes clusters as needed. During the operation, PAM360 fetches the JSON file that contains the critical secret keys and stores them in a file store within the repository. PAM360 encodes the secret keys contained within the secret files. The product is capable of fetching and storing secrets from multiple Kubernetes clusters. Kubernetes secrets contain machine identities that the system uses to interact with other systems outside the Kubernetes server. Through this integration, PAM360 automates the process of secrets management.

John can also rotate the Kubernetes secrets through a password reset operation from the PAM360 interface. To achieve this, he can map the Kubernetes secrets to existing resources in PAM360 and change the passwords of the resources. This operation will rotate the secret keys stored within the JSON files fetched from Kubernetes. However, the secret keys will not be automatically updated directly in the Kubernetes server.

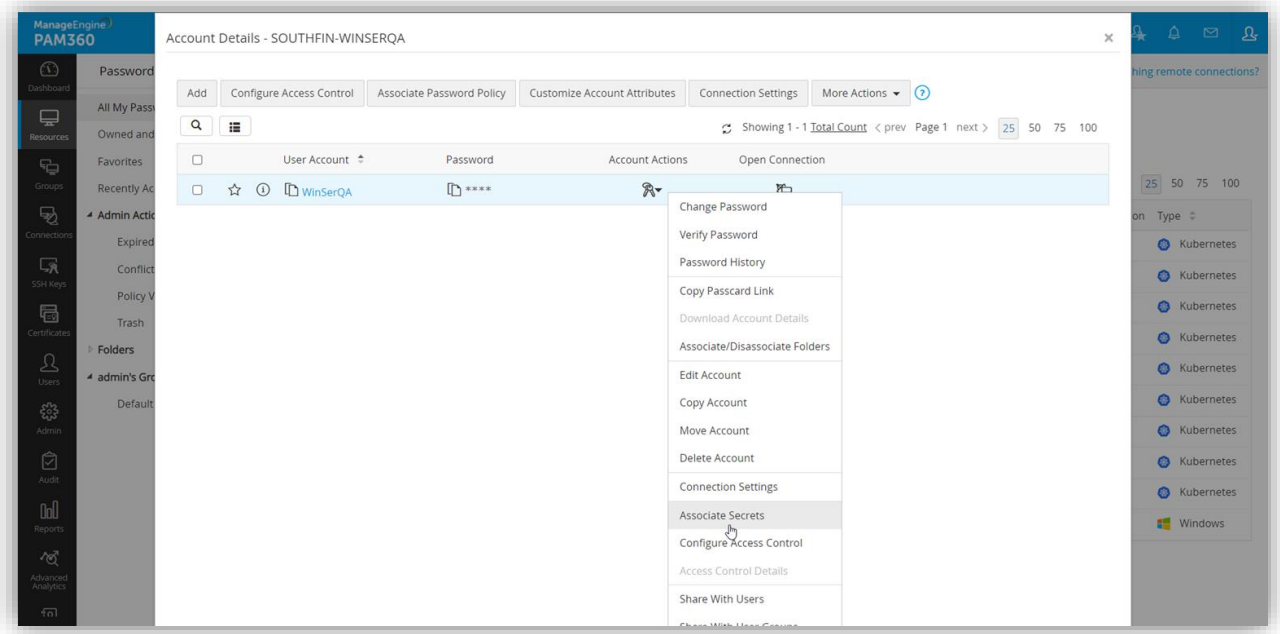
5. Mapping Secrets to Resources

To begin managing the secrets you have fetched, map them to resources in the PAM360 repository.

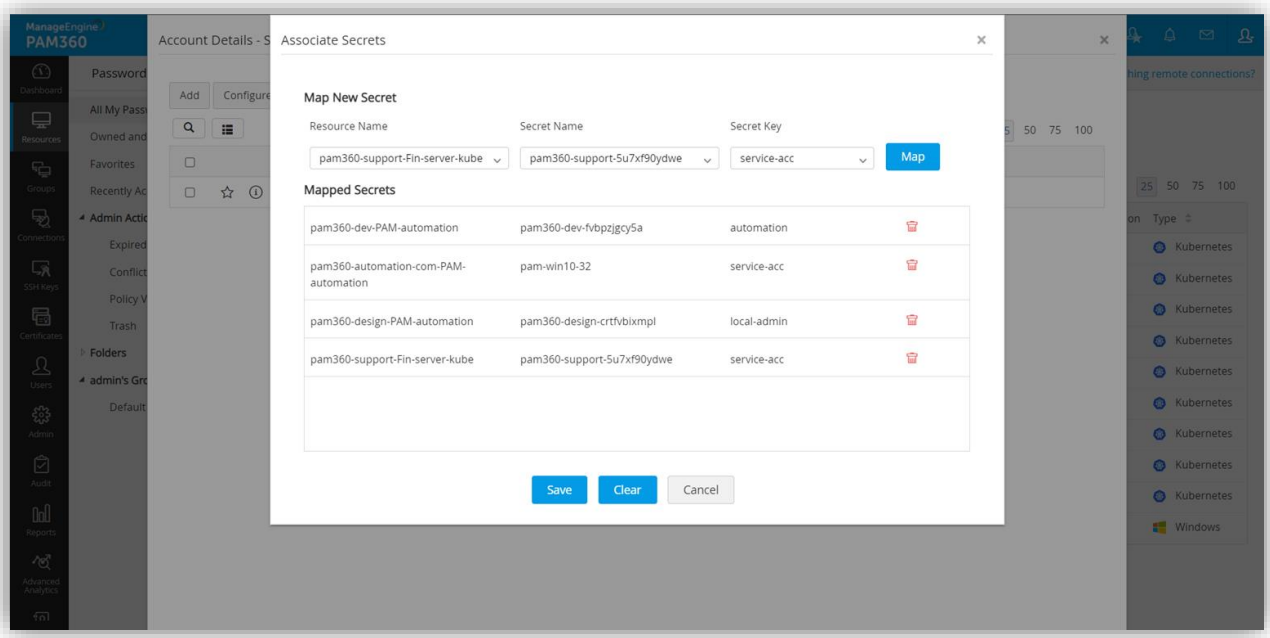
1. Once the secrets are fetched, PAM360 creates individual resources with the following naming convention: **Namespace-Cluster Name**. Navigate to the **Resources** tab to view all Kubernetes resources created by PAM360.
2. The secrets are categorized under the resources based on the Namespace and the Kubernetes Cluster from which they were fetched.



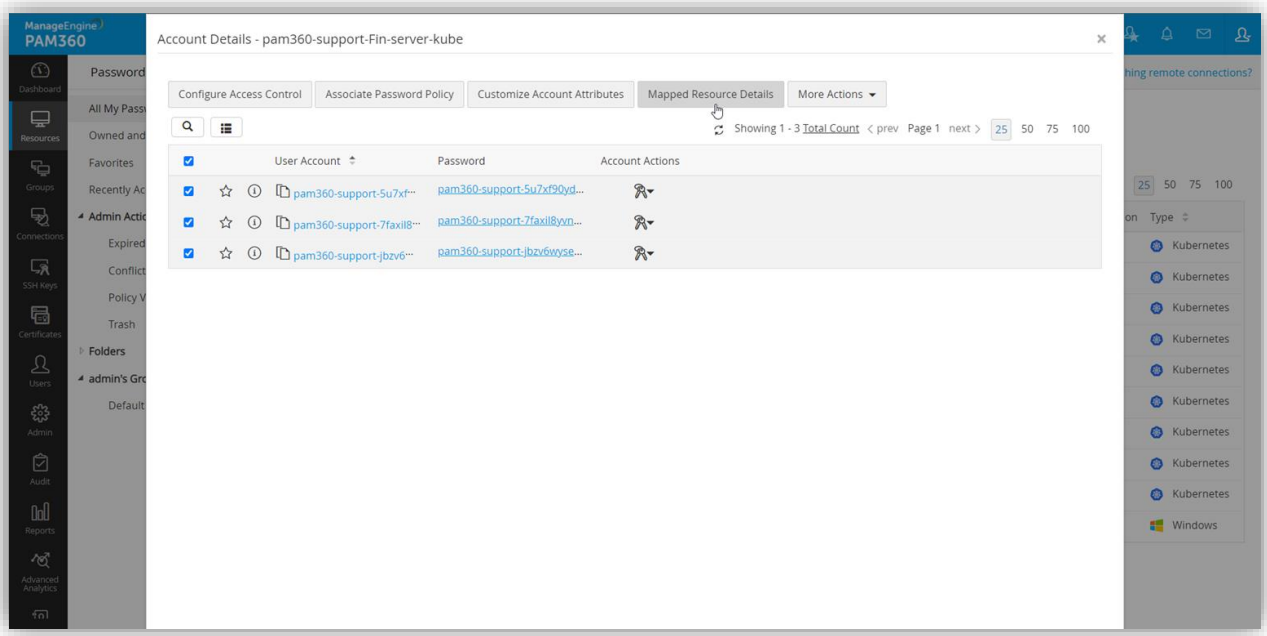
3. You can associate Kubernetes secrets with any resource of any resource type owned by you or shared with you.
4. Select a resource, go to **Account Actions >> Associate Secrets**

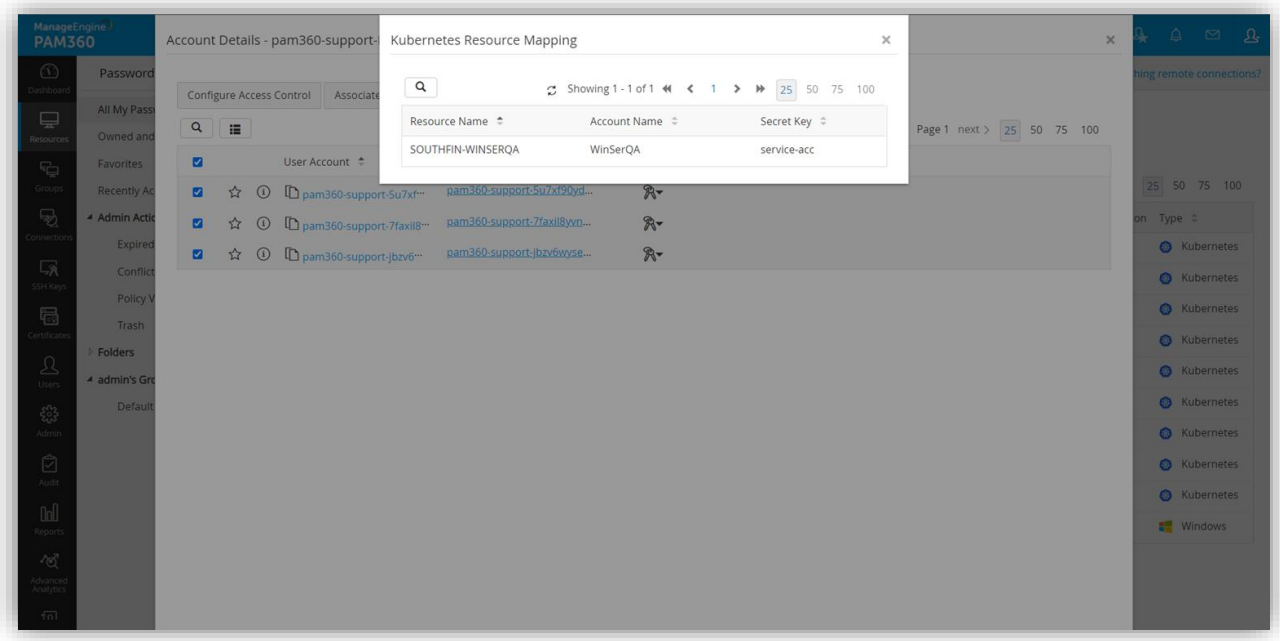


5. In the **Associate Secrets** window, select a resource name from the drop-down, a secret name and a secret key belonging to the secret. Click **Map** and save. You have successfully associated the selected secrets and secret keys with the account. You may map multiple secrets to a resource.



6. Once mapping is complete, you are ready to manage the secrets through the resource. To view mapping details, open any Kubernetes resource and click **Mapped Resource Details**. This window will display all the list of secrets belonging to this Kubernetes cluster and the resource to which they are mapped.





Note: Please note that any password reset operation triggered through the mapped resource will change all of the secret keys mapped to it and the changes will reflect in the Kubernetes server. However, PAM360 will not reset the passwords of the services running inside the Kubernetes clusters.

6. Limitations

1. You must manually map each secret to a resource to manage them from the PAM360 repository. Whenever new secrets are synced from the Kubernetes server through an on-demand fetch, the secrets must be manually mapped to a resource from the Resources tab.
2. PAM360's remote password reset support does not extend to the services running inside the Kubernetes server.
3. The integration offers only a one-way sync—PAM360 can fetch the additional secrets added to the Kubernetes cluster, but it cannot remove the secrets already deleted from the Kubernetes server.
4. PAM360 does not have an automated sync schedule to fetch secrets from the Kubernetes server automatically.

7. Glossary of Terminologies

Term	Description
Container	A portable, executable image that contains software and all of its dependencies.

Secret	An object that contains sensitive data such as a password, a token, or a key.
Cluster	A set of worker machines called nodes that run containerized applications. Every cluster has at least one worker node.
Kubectl	Command line tool used to communicate with a Kubernetes cluster's control plane using the Kubernetes API.
Namespace	A Namespace is an abstract concept that is used to isolate a group of resources residing within a single Kubernetes cluster.

Integrating ManageEngine PAM360 with SIEM Tools

This document discusses the process of integrating PAM360 with various SIEM tools. At the end of this section, you will have learned the following:

1. Key Benefits of Integration
2. How does the Integration Work?
    2.1 Format of the Syslog Messages Sent from PAM360
3. Steps to Integrate a SIEM Tool and Configure Syslog Collection
    3.1 Customizing the Syslog Event Notifications in PAM360

1. Key Benefits of Integration

PAM360 integrates with SIEM tools that help in gathering and processing audit logs for resources, passwords, and users from PAM360 in real time and send them as Syslogs to external log management systems. Specific events for which notifications are to be raised can be tailored from the Audit tab of PAM360.

The following are the SIEM tools that can be currently integrated with PAM360 to collect syslogs:

1. Splunk
2. ManageEngine EventLog Analyzer
3. Sumo Logic
4. Microsoft Sentinel
5. Other Syslog Collectors

Apart from the above SIEM tools, you can set up any other log management tool also to collect audit logs. You can have multiple log management tools configured concurrently.

2. How does the Integration Work?

Once the details of the the collector host, such as the host name and port are given and the integration is enabled, an RFC-3164 compliant Syslog message will be generated and sent to the configured host and port, using the chosen protocol (TCP or UDP). Default facility name will be AUTH, but you can change it to any of the unassigned facility names from the list.

1. **Splunk:** Click here for information on how to view the syslog data sent from PAM360 in

Splunk.

2. **ManageEngine EventLog Analyzer:** Once the collector host is added in PAM360, the PAM360 server will be added as a device in EventLog Analyzer automatically. Refer to section 3 for the configuration steps.
3. **Sumo Logic:** Click here to read more about Sumo Logic's collectors.
4. **Microsoft Sentinel:** Click here to learn how to configure Microsoft Sentinel with PAM360 in detail.

2.1 Format of the Syslog Messages Sent from PAM360

PAM360 uses different Syslog message formats for Resource Audit and User Audit. The RFC-3164 compliant Syslog message indicates the type of audit event at the start of the message, followed by the username and IP address from which the operation was performed. The message typically includes details such as the type of operation, the timestamp, and status. It also displays the name of the PAM360 server where the operation was carried out, along with the resource & account name details. A notable difference between the Syslog messages for MSP and Non-MSP is that the MSP format includes the ORG_NAME in the message.

i. Syslog Format for MSP

Resource Audit

```
[ResourceAudit:LOGGED_IN_USERNAME:IPADDRESS] [OPERATION_TYPE]
[OPERATED_TIME] [STATUS_OF_OPERATION] [PAM360_SERVER_NAME]
[ORG_NAME-RESOURCE_NAME:ACCOUNT_NAME:REASON]
```

User Audit

```
[UserAudit:LOGGED_IN_USERNAME:IPADDRESS] [OPERATION_TYPE]
[OPERATED_TIME] [STATUS_OF_OPERATION] [PAM360_SERVER_NAME]
[ORG_NAME-LOGGED_IN_USERNAME:REASON]
```

ii. Syslog Format for Non-MSP

Resource Audit

```
[ResourceAudit:LOGGED_IN_USERNAME:IPADDRESS] [OPERATION_TYPE]
[OPERATED_TIME] [STATUS_OF_OPERATION] [PAM360_SERVER_NAME]
[RESOURCE_NAME:ACCOUNT_NAME:REASON]
```

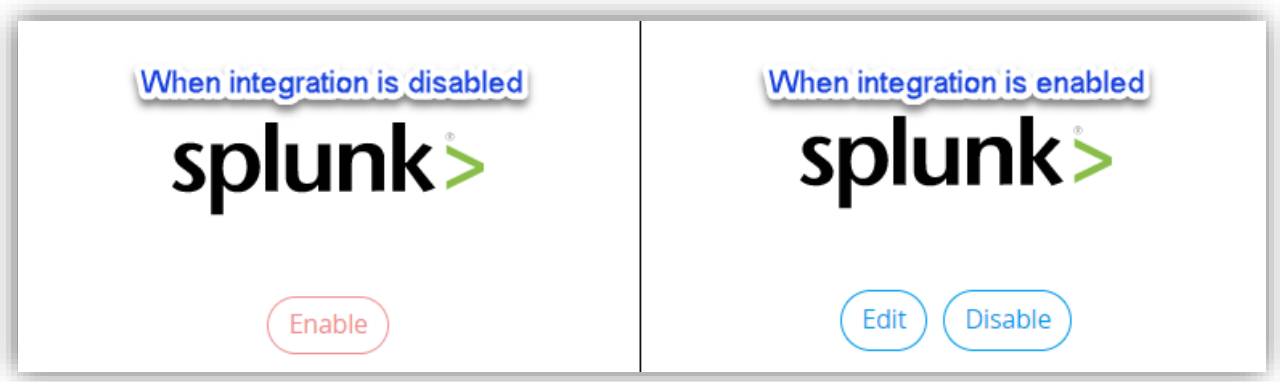
User Audit

> [UserAudit:LOGGED_IN_USERNAME:IPADDRESS] [OPERATION_TYPE] [OPERATED_TIME] [STATUS_OF_OPERATION] [PAM360_SERVER_NAME] [LOGGED_IN_USERNAME:REASON]

3. Steps to Integrate a SIEM Tool and Configure Syslog Collection

Follow the below steps to integrate any SIEM tool with PAM360 and configure syslog collection.

1. Navigate to **Admin >> Integrations >> SIEM Integrations.**
2. In the page displayed, you will see the SIEM tool blocks with the below options. These options remain the same for any SIEM tool you might want to integrate with PAM360.

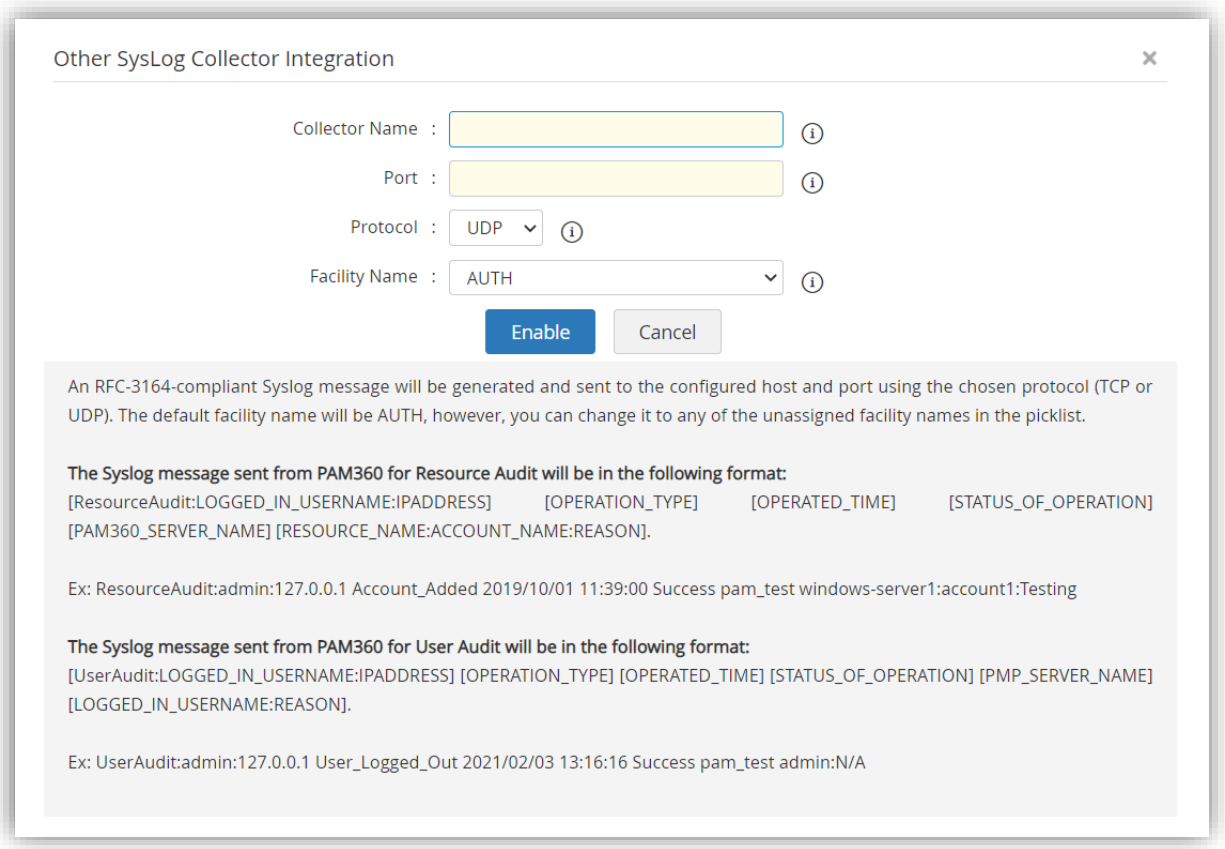


Buttons and Definitions:

Sl. No:	Button	Definition
1	Enable	You will see this option if the integration is disabled. Click this button to enter the required details of the SIEM tool and enable integration.
2	Edit	You will see this option if the integration is enabled. Click this button to update the SIEM tool details, such as the collector name, port, protocol and facility name.

3	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

3. Click **Enable** under the SIEM tool of your choice. If you don't have any of the listed tools, click **Enable** under 'Others' and enter the below details:
   i. Collector Name
   ii. Port
   iii. Protocol (UDP/TCP)
   iv. Facility Name (AUTH is selected by default)



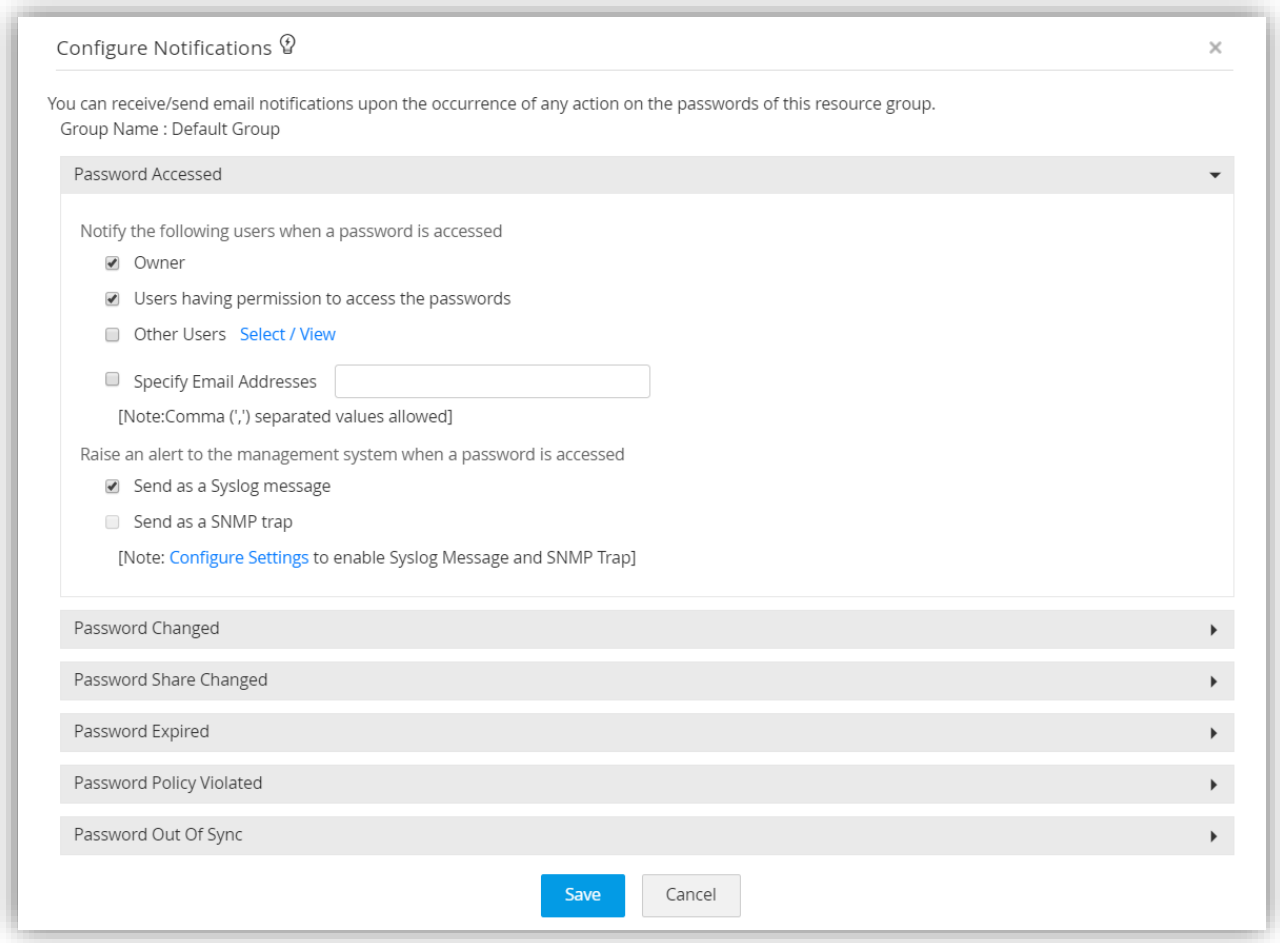
4. Click **Enable**. Now the integration with PAM360 and the SIEM tool of your choice is complete.

3.1 Customizing the Syslog Event Notifications in PAM360

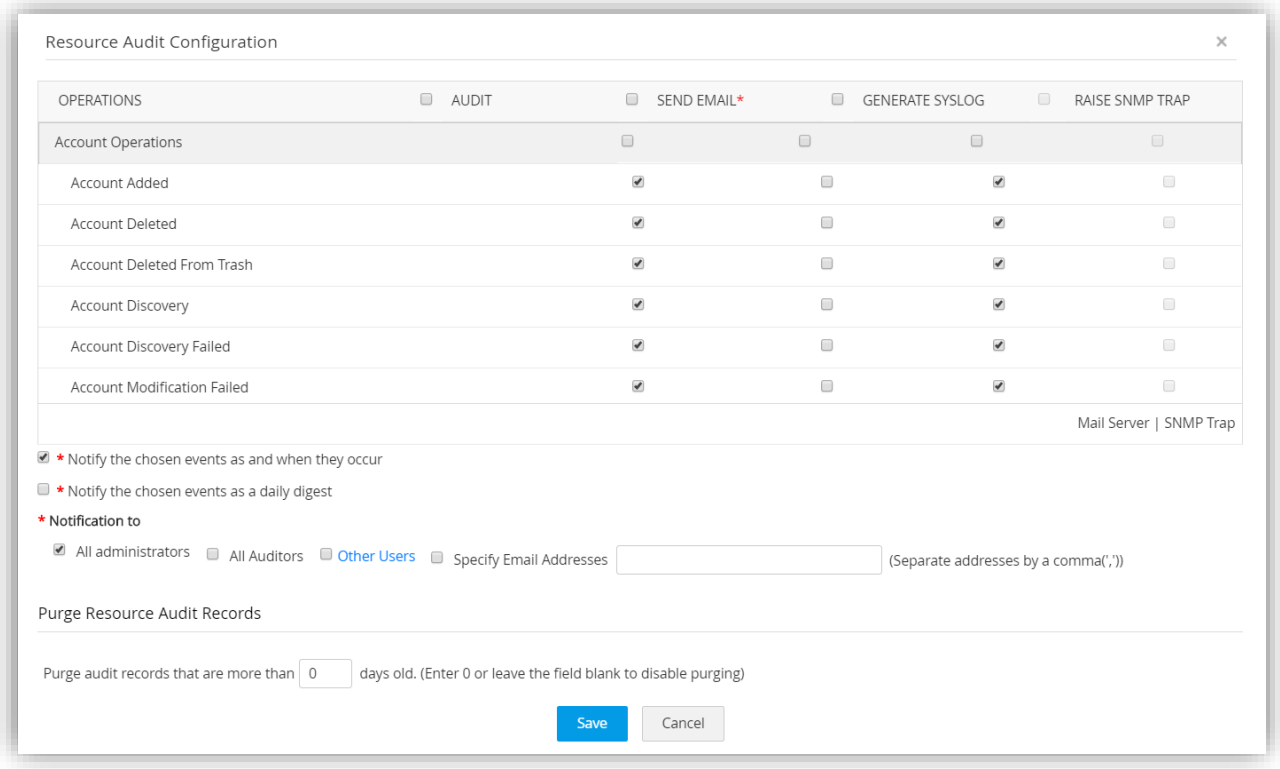
After enabling the integration and configuring the settings, you can customize the events for which you wish to generate the syslog messages.

1. **Password-oriented:** To generate password-related syslog messages, navigate to **Groups**

>> Actions (of desired group) >> Configure Notifications, and select **Send as a Syslog message** for the required password-oriented options.



2. **Operation-oriented:** You can generate syslog messages regarding the account operations inside PAM360. This can be done for both resource audit and user audit. To configure for resource audit, navigate to **Audit >> Resource Audit >> Audit Actions >> Configure Resource Audit.** Similarly, to configure for user audit, navigate to **Audit >> User Audit >> Audit Actions >> Configure User Audit**. The **Generate Syslog** option will be selected for all the operations already. Uncheck the operations which don't need to be recorded.


Resource Audit Configuration
OPERATIONS
AUDIT
SEND EMAIL*
GENERATE SYSLOG
RAISE SNMP TRAP
Account Operations
Account Added
Account Deleted
Account Deleted From Trash
Account Discovery
Account Discovery Failed
Account Modification Failed
Mail Server | SNMP Trap
* Notify the chosen events as and when they occur
* Notify the chosen events as a daily digest
* Notification to
All administrators
All Auditors
Other Users
Specify Email Addresses
(Separate addresses by a comma(','))
Purge Resource Audit Records
Purge audit records that are more than 0 days old. (Enter 0 or leave the field blank to disable purging)
Save
Cancel

Integrating PAM360 with Microsoft Sentinel

PAM360, a unified Privileged Access Management product from ManageEngine, integrates with Microsoft Sentinel, a cloud-native security information and event management (SIEM) solution by Microsoft. This is in addition to the already available integrations with the third-party SIEM solutions such as Splunk, ManageEngine EventLog Analyzer, and Sumo Logic.

At the end of this document, you will have learned the following:

1. Key Benefits of Integration
2. Configuring a PAM360 workspace in Microsoft Sentinel
3. Enabling Microsoft Sentinel integration in PAM360
4. Viewing PAM360 logs in Microsoft Sentinel
5. Troubleshooting Tips

1. Key Benefits of Integration

PAM360's extensive auditing capabilities include gathering and processing audit logs for resources, passwords, and users in real time. The product allows you to tailor notifications for specific events from the Audit tab.

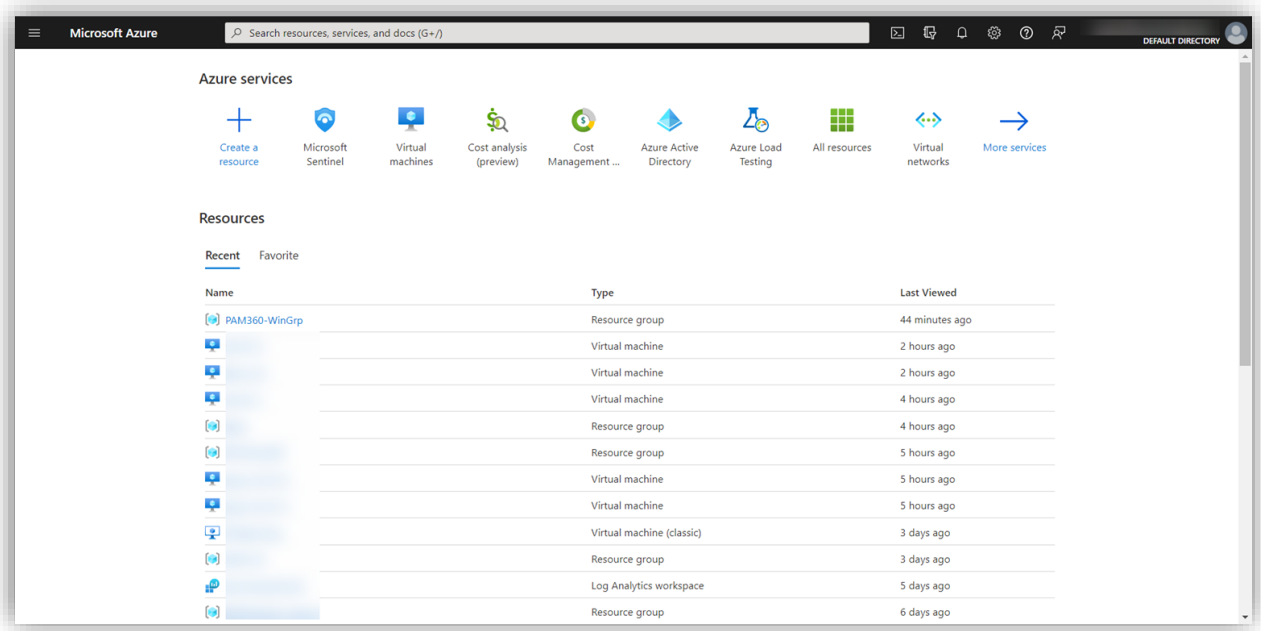
Through the PAM360-Microsoft Sentinel integration, PAM360 sends detailed logs to the SIEM tool as syslogs, enabling you to view PAM360 audit trails from the Microsoft Sentinel interface. Apart from the above-mentioned SIEM tools, you can set up any other log management tool to collect audit logs. It is possible to configure multiple log management tools concurrently.

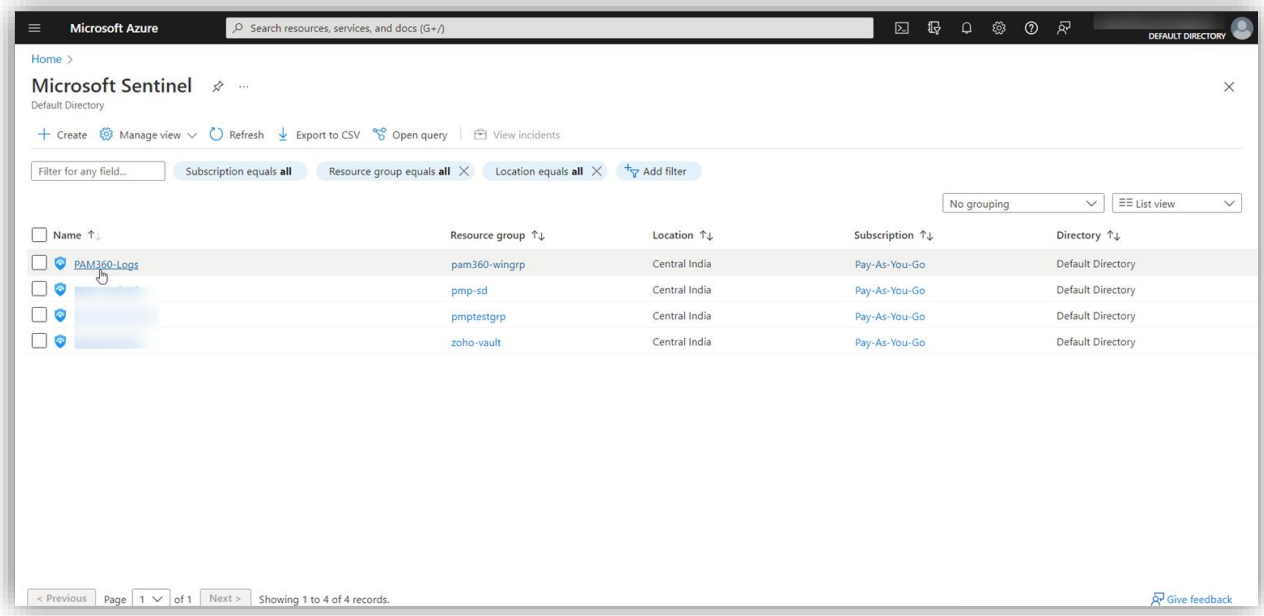
2. Configuring a PAM360 Workspace in Microsoft Sentinel

Prerequisites

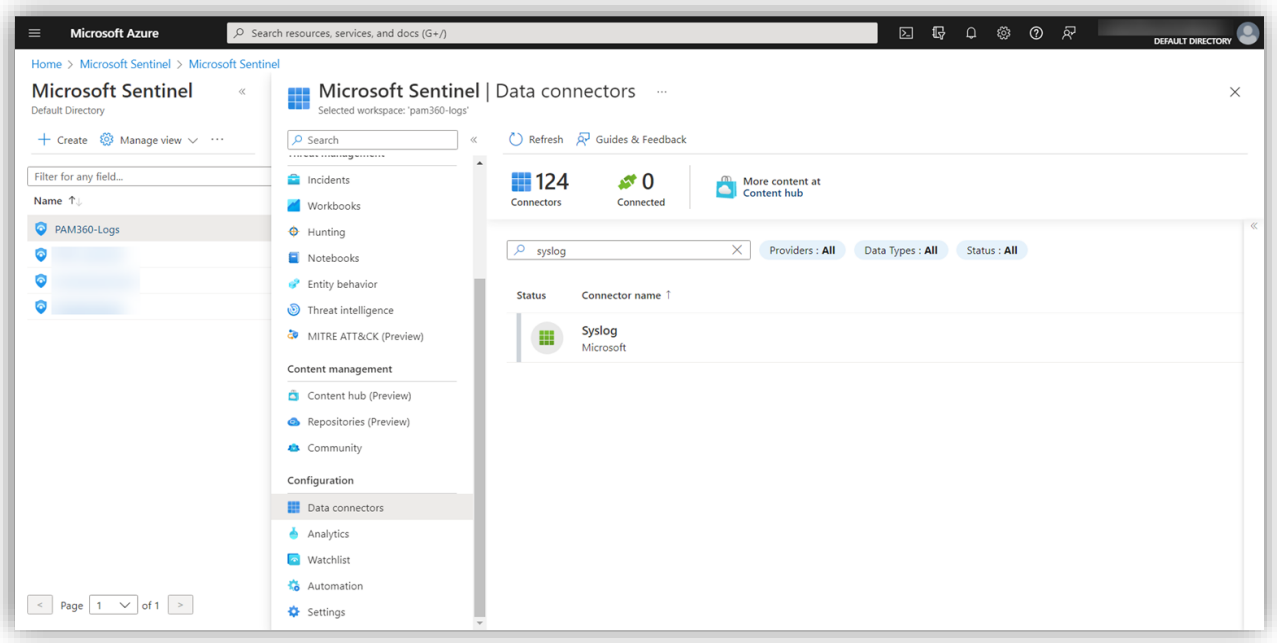
1. Ensure that the PAM360 server has internet access to send syslogs to Microsoft Sentinel.
2. This integration requires a workspace in Microsoft Sentinel. If you don't have one already, create a new workspace for PAM360. Refer to this document for instructions on how to create a new workspace.

1. Log in to the Microsoft Azure Portal. Under **Azure Services**, click **Microsoft Sentinel**.

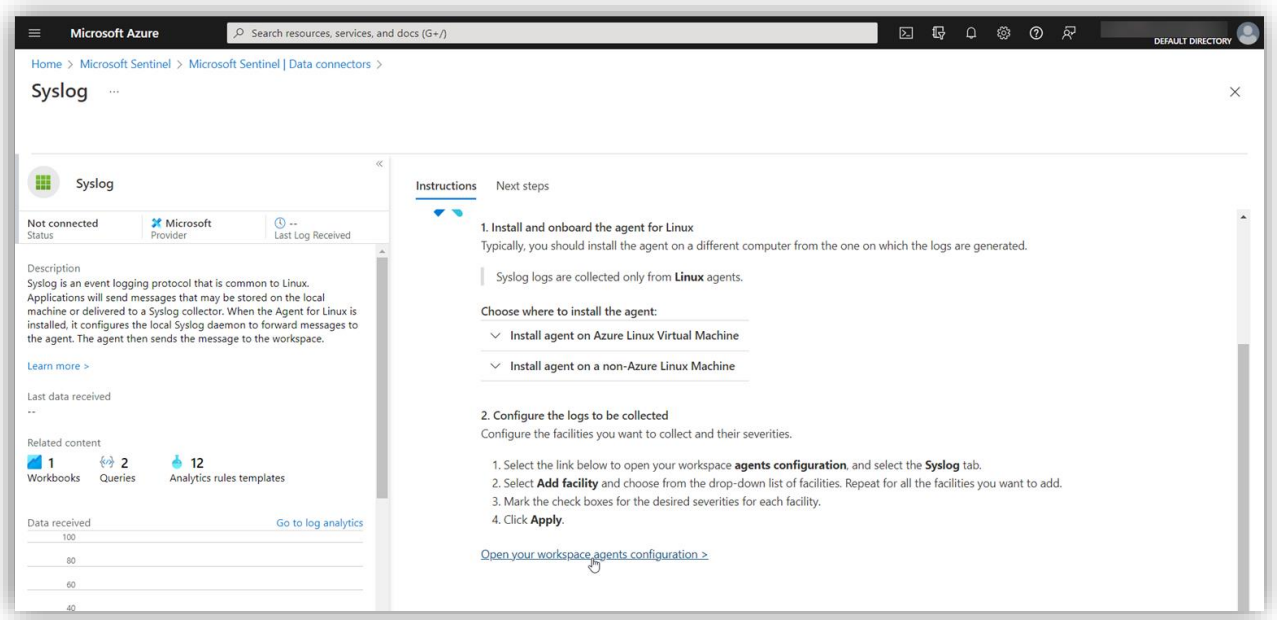




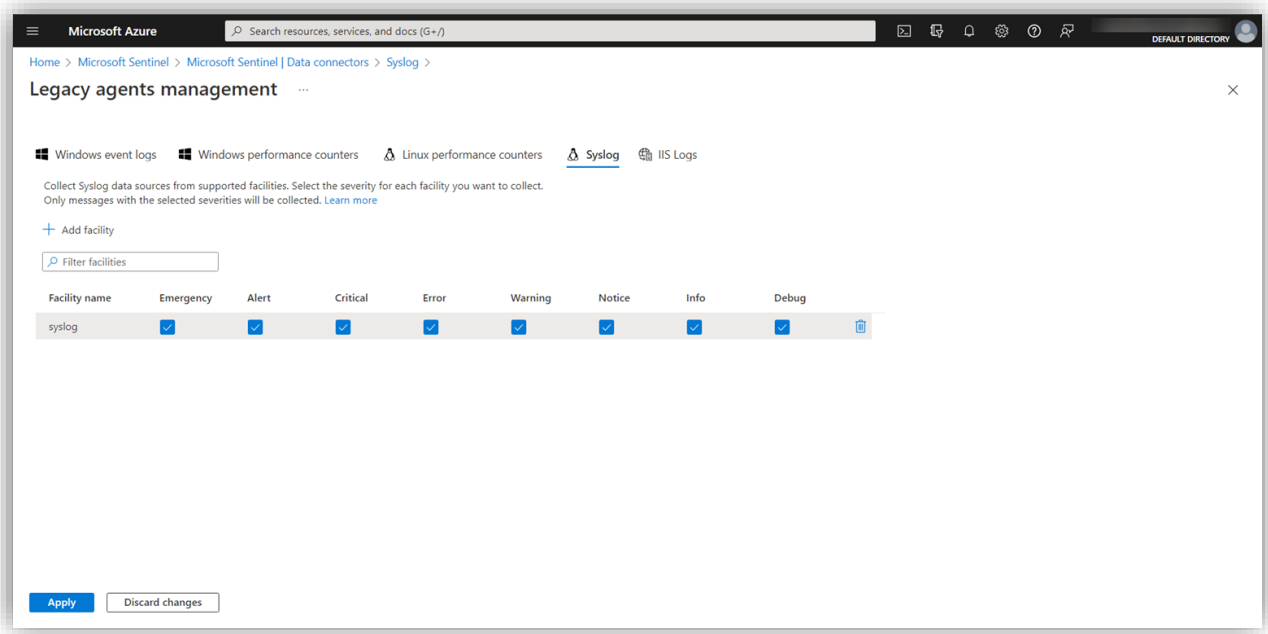
2. Open the newly created workspace. In the left pane, under **Configuration**, click **Data Connectors.**
3. A list of data connectors will be displayed on the right. Enter "syslog" in the search bar on the right. Click the **Syslog** connector to open it using the **Open connector page** option.



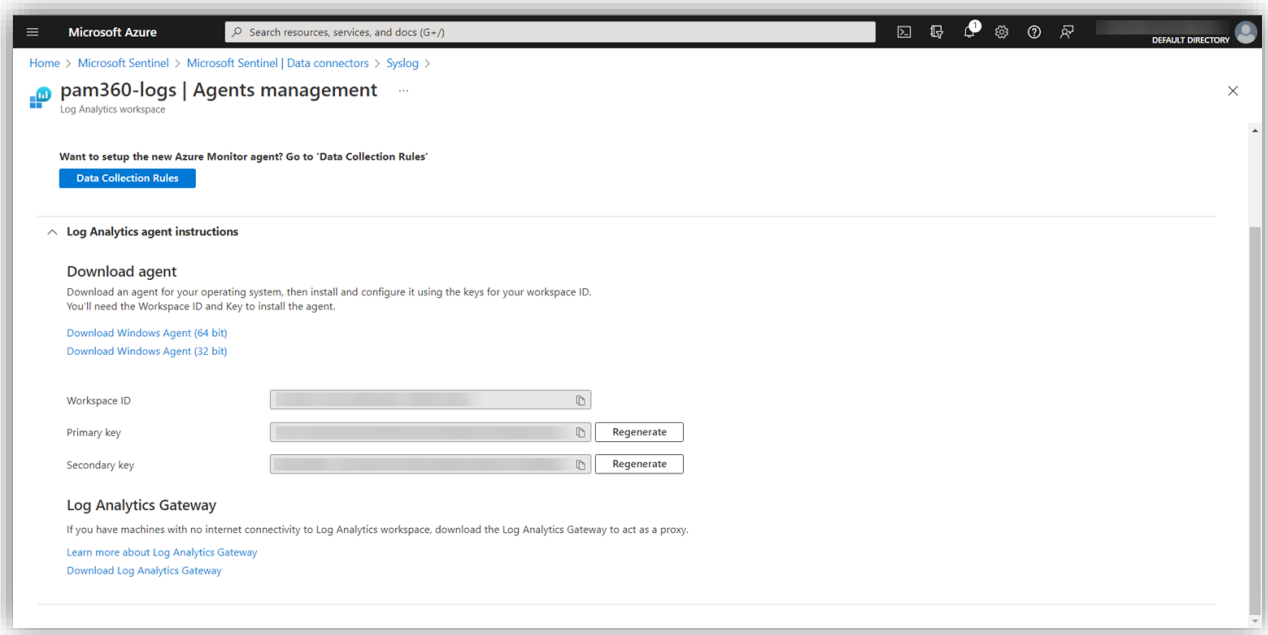
4. The Syslog configuration page will open up. Here, under **Configuration**, you will find two steps. Under step 2 **Configure the logs to be collected**, click the link **Open your workspace agents configuration**.



5. In the **Legacy agents management** page, a list of permission levels will be listed under **Facility**. Add facility for **Syslog**. Select all checkboxes to grant permissions and click **Apply**.



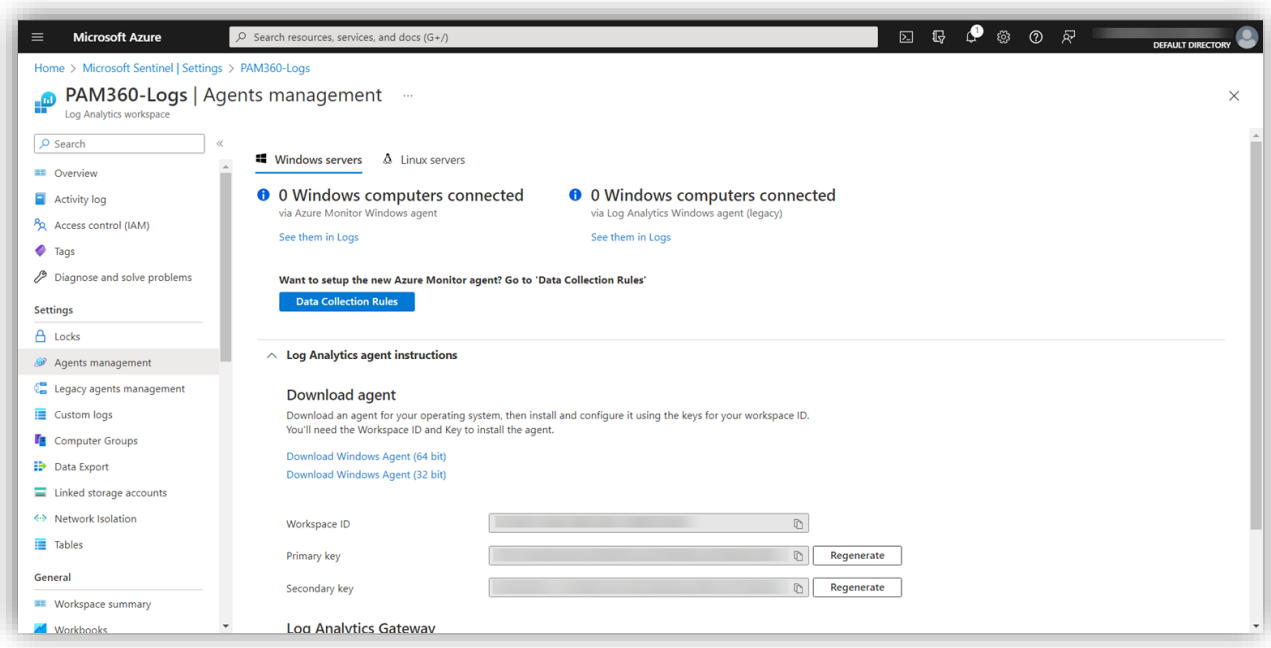
6. Go back to the Syslog configuration page. Under step 1, click the link **Download & install agent for non-Azure Linux machines**. You will be redirected to the **Agents management** page where you can find the Workspace ID and the Primary & Secondary keys under the **Log Analytics agent instructions** menu.
7. Copy and save the Workspace ID and the keys in a safe location as they are necessary to complete the integration in PAM360.



Notes:

i. Please note that the PAM360 - Microsoft Sentinel integration does not require any Azure agents, so you don't need to download any from the **Agents management** page.

ii. You can also obtain the Workspace ID and the Primary/Secondary key by navigating to **Settings >> Agents management**. Here, expand the **Log Analytics agent instructions** menu to view the required information.



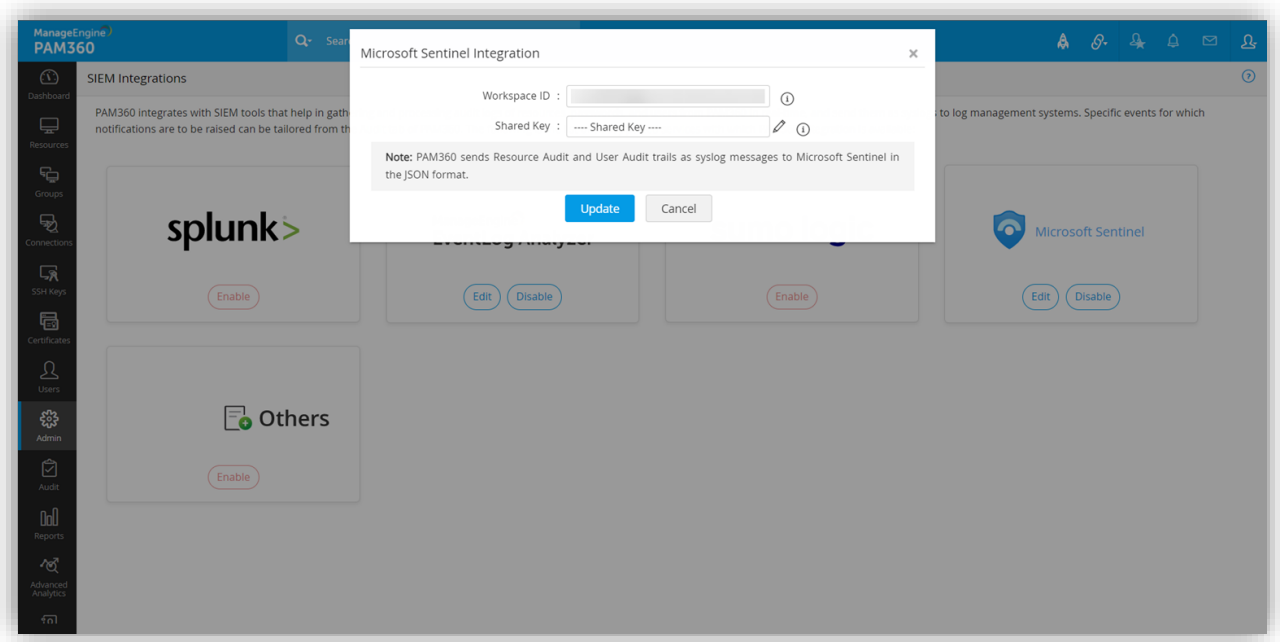
You have successfully configured a workspace for PAM360 in the Microsoft Sentinel portal.

3. Enabling Microsoft Sentinel Integration in PAM360

Follow the below steps to complete the Microsoft Sentinel configuration in PAM360.

1. In the PAM360 interface, navigate to **Admin >> Integrations >> SIEM Integrations**.
2. Under Microsoft Sentinel, click **Enable**. In the dialog box that appears, enter the **Workspace ID** copied from the Microsoft Sentinel portal.
3. In the **Shared Key** field, enter either the Primary or the Secondary key taken from the Microsoft Sentinel portal and click **Enable**.
4. Click **Enable** again in the confirmation dialog box.

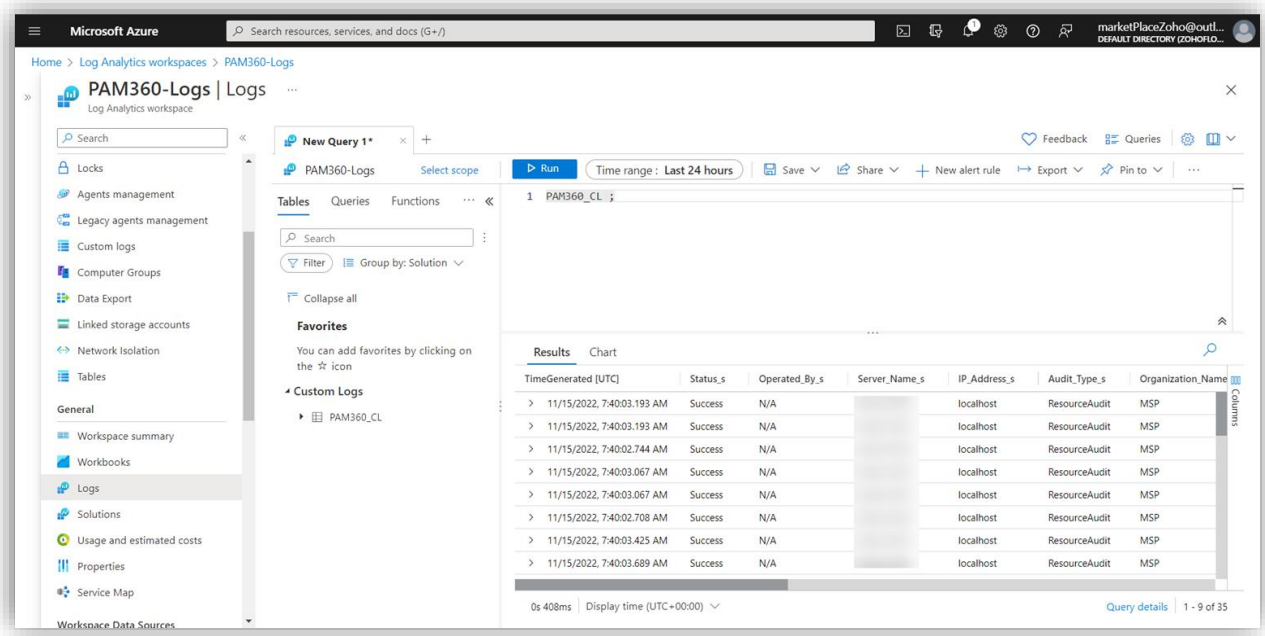
The integration process is now complete. All audit trails that are captured in PAM360 will be transferred to the Microsoft Sentinel portal.



4. Viewing PAM360 Logs in Microsoft Sentinel

To view the PAM360 logs in Microsoft Sentinel, go to the Microsoft Sentinel portal.

1. In the left pane, navigate to **General >> Logs**.
2. Expand the **Custom Logs** menu and verify if a custom log for PAM360 has been created with the name PAM360_CL.
3. Double click the custom log; the command will appear on the terminal to the right. Add a semicolon to the custom log command: **PAM360_CL;**
4. You can choose the required time range and click the **Run** option from the top.
5. Now, all logs captured from PAM360 in the selected time range will appear below.
6. If required, use the **Export** option to export the logs in the CSV format.



5. Troubleshooting Tips

After configuring the integration, if you are still unable to view the PAM360 logs in the Microsoft Sentinel portal, try the below steps:

1. Ensure there is internet connectivity in the machine where the PAM360 server resides.
2. If you have used the Primary key while configuring the integration, edit the configuration details and enter the Secondary key in the **Shared Key** field and save changes. If both the keys fail to work, use the **Regenerate** option to regenerate fresh keys and try to configure again.
3. Check if syslog permissions are enabled under **Legacy agents management >> Facility**.
4. Check if the **Generate Syslog** option is enabled in the PAM360 interface under **Configure Audit** as shown in section 3.1 of SIEM tools.
5. Ensure that you do not delete the custom fields that are auto-generated in the Sentinel portal under **Settings >> Custom Logs** after the integration is enabled in PAM360. In case, you have deleted the custom fields, re-configure the integration with a new workspace to view the logs.

Integrating PAM360 with Vulnerability Scanner

This document discusses the process of integrating PAM360 with the vulnerability management tools. For now, PAM360 integrates with Rapid7 InsightVM. At the end of this section, you will have learned the following:

1. Key Benefits of Integration
2. How does the Integration Work?
3. Prerequisites for Performing the Integration
4. Steps to Configure the Integration
5. Steps to Map InsightVM Services to PAM360 Resource Types
6. Steps to Associate an Account to an InsightVM Service

1. Key Benefits of Integration

ManageEngine PAM360 integrates with Rapid7 InsightVM, a vulnerability management tool that automatically scans and collects data from all endpoints available in a network and identifies the ones that may pose a security risk. The PAM360-InsightVM integration helps you secure and centrally manage the shared credentials that are necessary to run vulnerability scans, right from the PAM360 interface.

2. How does the Integration Work?

PAM360 sources data from InsightVM through their API and using their host name and login credentials. Once the integration is complete, all the services in InsightVM will be populated in PAM360, after which you can associate and manage the InsightVM credentials from the PAM360 interface.

3. Prerequisites for Performing the Integration

Before commencing the integration, verify if all of the below prerequisites are satisfied:

1. PAM360 supports connection via HTTPS only, hence it is mandatory to import a valid SSL certificate in the server. Follow the steps given below to import a certificate in the server:
    i. Stop the PAM360 service.
    ii. Open the command prompt and go to the "<PAM360_Installation_Folder>/bin" directory.
    iii. Execute the following command:

importCert.bat <Path of the certificate used by ADSSP>

iv. Restart the PAM360 service.

2. To remotely update passwords for InsightVM services after integration, you need to have the remote password reset enabled for resources in PAM360. Click here to learn more about setting up remote password reset in PAM360.

4. Steps to Configure the Integration

To enable and configure the PAM360 - InsightVM integration, follow the below steps:

1. Navigate to **Admin >> Integrations >> Vulnerability Scanner.**
2. In the page displayed, you will see the **Rapid7 InsightVM** block with with any of the below options based on whether you have enabled or disabled the integration:

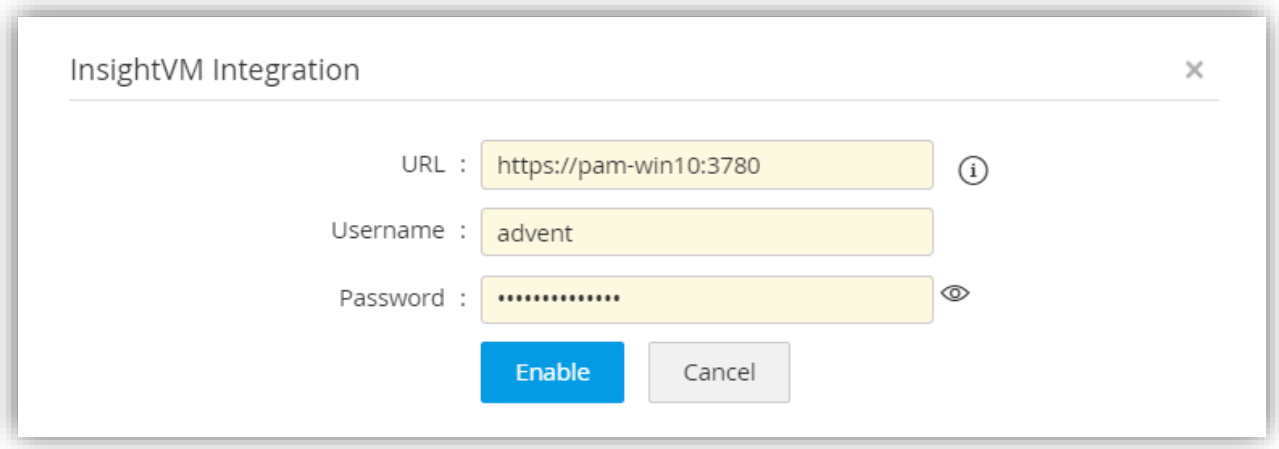




Sl. No:	Button	Definition
1	Enable	You will see this option if the integration is disabled. Click this button to enter required details of the InsightVM server and enable integration.
2	Edit	You will see this option if the integration is enabled. Click this button to update

		the InsightVM URL and login credentials.
3	**Configure**	You will see this option if the integration is enabled. Click this button to view all the InsightVM services populated in PAM360.
4	**Disable**	You will see this option if the integration is enabled. Click this button to disable the integration.

3. Click **Enable** and configure the following details:
   i. URL of the InsightVM server
   ii. User Name
   iii. Password
4. Click **Enable** to save the details.

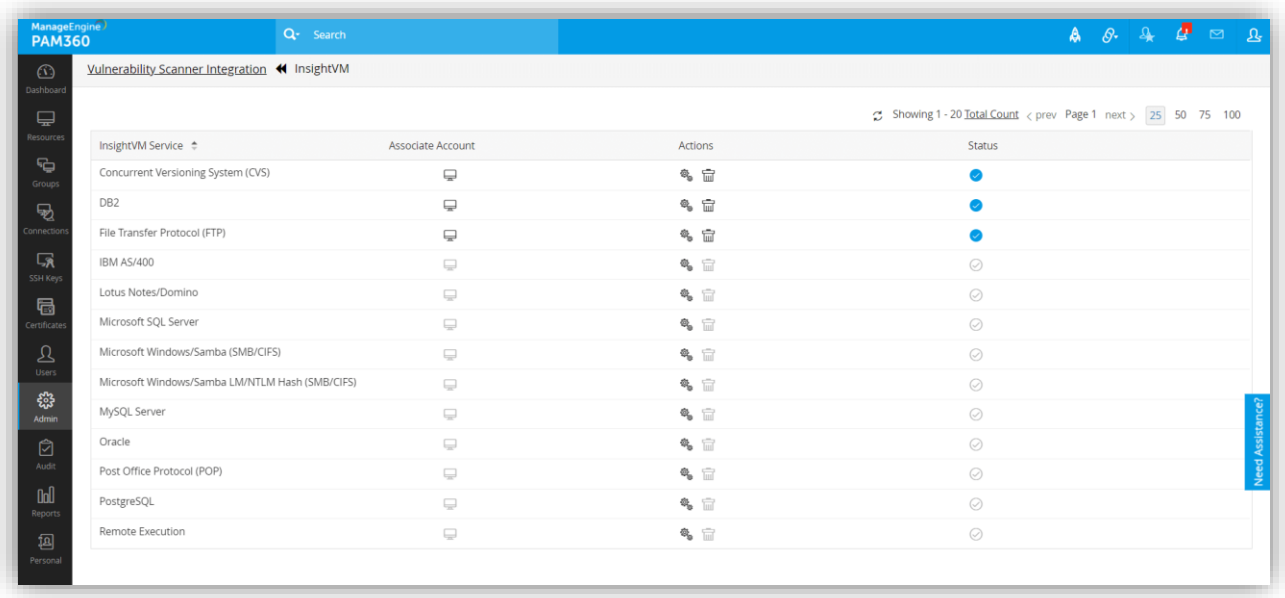


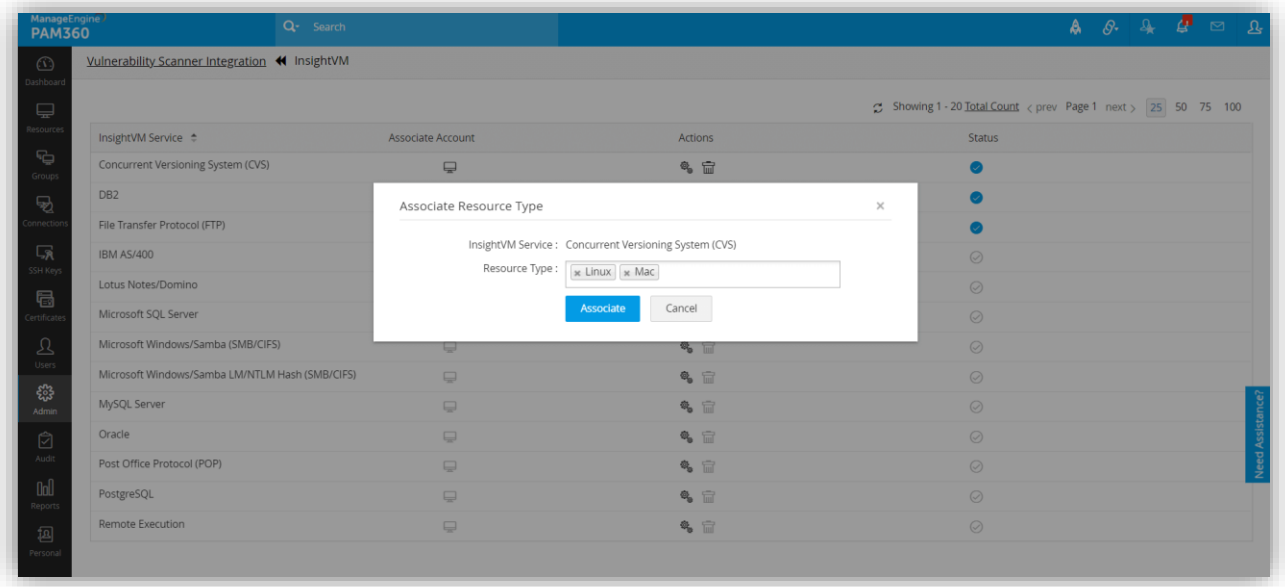
5. Steps to Map InsightVM Services to PAM360 Resource Types

Once the integration is enabled, click **Configure** to view all the InsightVM services in PAM360. Follow the below steps to map an InsightVM service to resource types in PAM360.

1. Click the **Associate Resource Type** option under **Actions** beside the required InsightVM service.

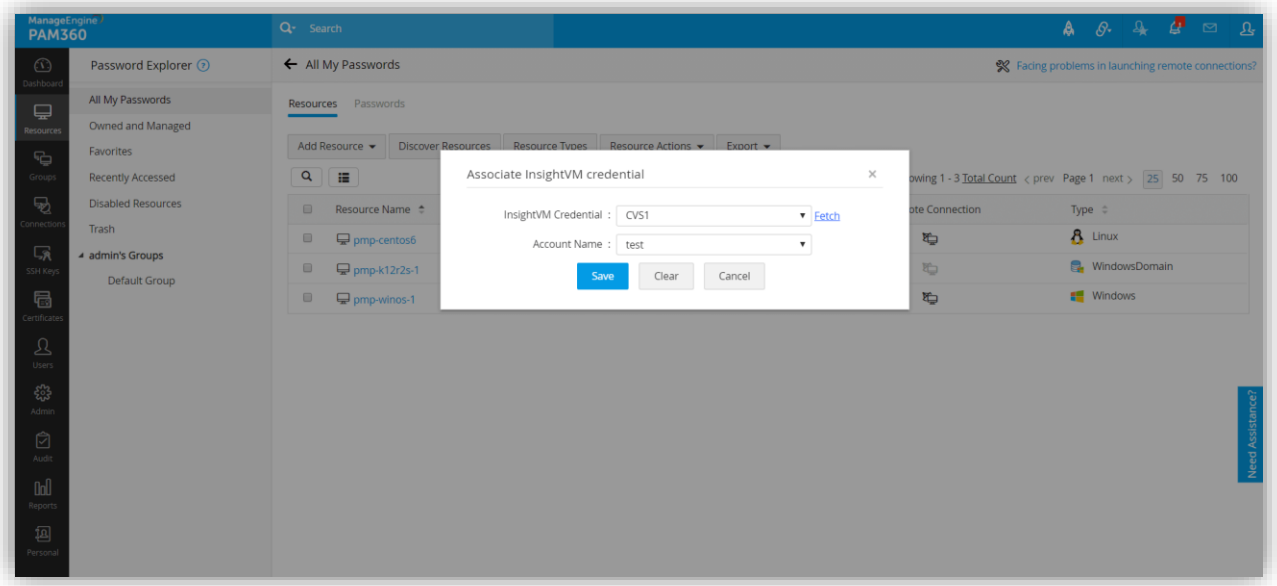
2. In the pop-up that opens, add resource types from PAM360 that are relevant to the selected service. You can map as many resource types to a service as you need. Click **Associate** once you are done.



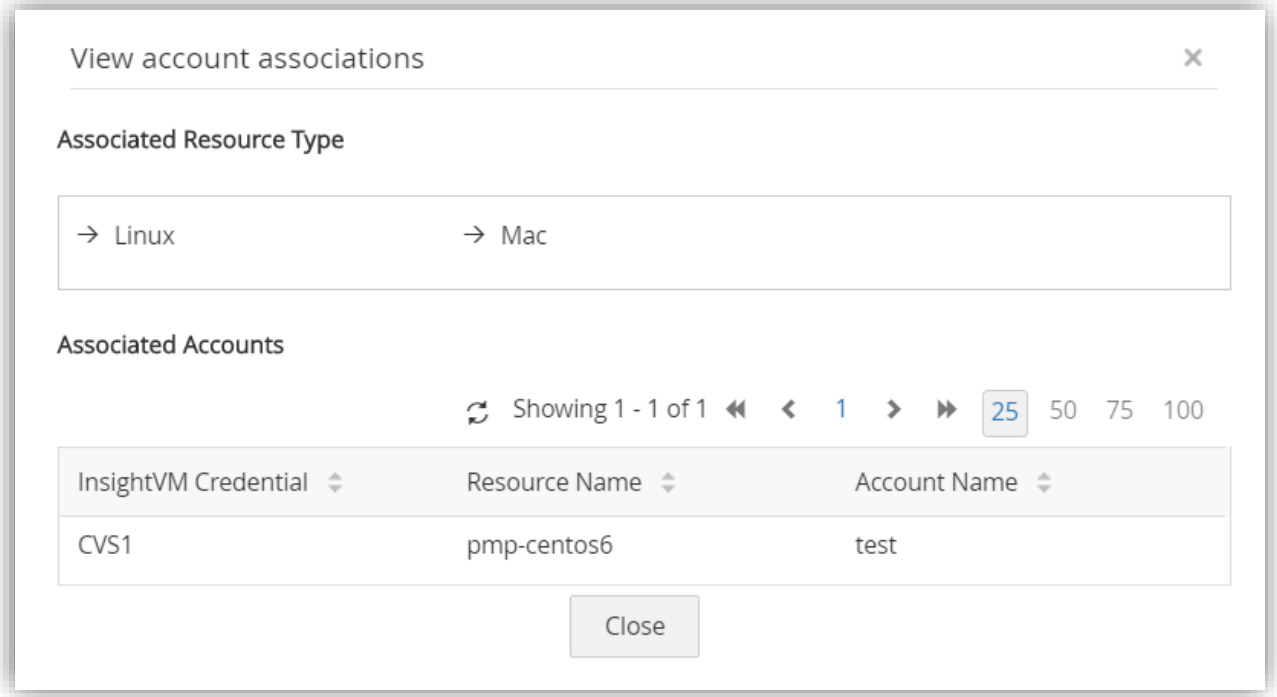


6. Steps to Associate an Account to an InsightVM Service

1. Navigate to the **Resources** tab and click **Resource Actions >> Associate InsightVM credential** beside a resource type that was associated with an InsightVM service.
2. Choose an InsightVM credential from the list of corresponding InsightVM credentials and choose a PAM360 account to be mapped to it.
3. Click **Save**. The selected PAM360 account will be mapped to the selected InsightVM credential.



4. The mapping details of PAM360 accounts with InsightVM services can be reviewed for a particular service, go to **Admin >> Integrations >> Vulnerability Scanner**, click **Configure**. Here, click the **Associate Account** beside the required InsightVM service.



Note: Remote password reset from PAM360 is not supported for the following InsightVM services:

1. Simple Network Management Protocol v2/v1c
2. Simple Network Management Protocol v3
3. SSH key
4. Lotus Notes/Domino
5. Web Site HTTP Authentication

For more information about shared credentials in InsightVM, click here.

Integrating with SafeNet Luna PCIe Hardware Security Module (HSM)

Besides the default encryption method, PAM360 provides support for **SafeNet Luna PCIe** HSM to give administrators the option to enable hardware data encryption for PAM360.

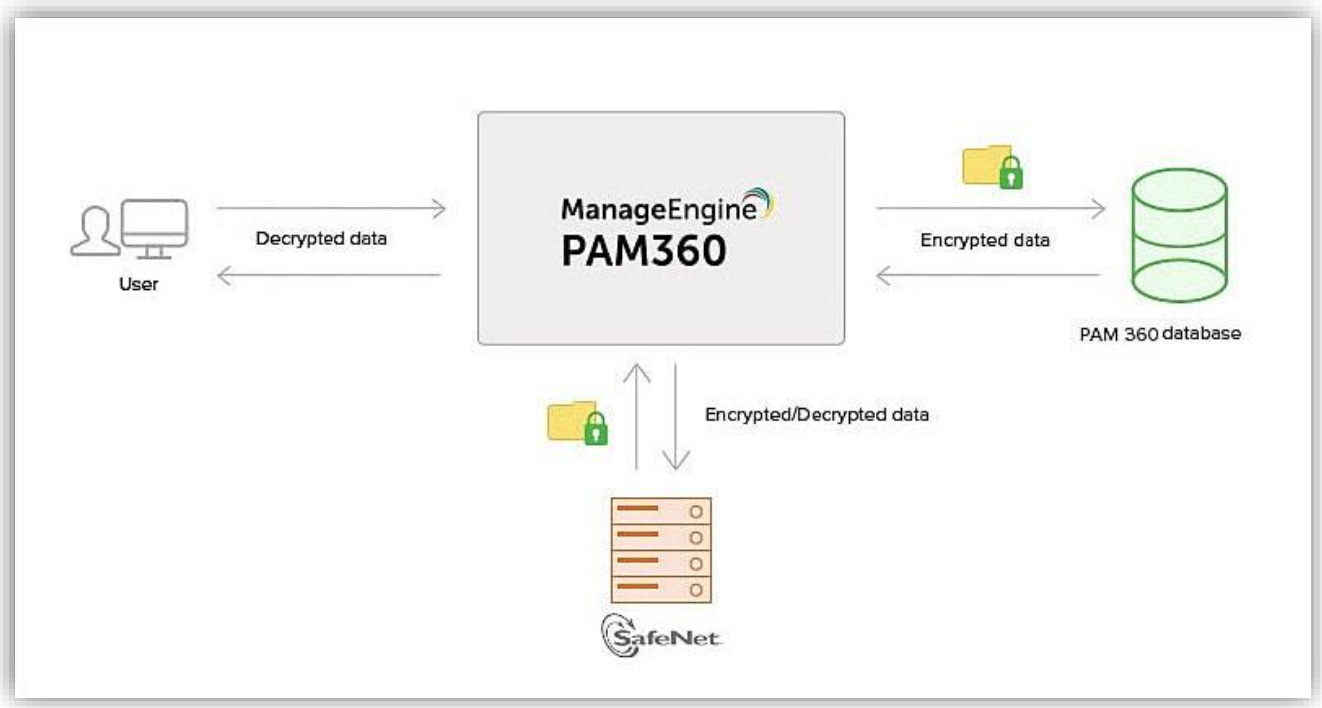
You can integrate PAM360 with the SafeNet Hardware Security Module that can handle all the encryption and decryption methods. In addition to this, SafeNet HSM can also store the encrypted key directly in its hardware module that is fitted to a computer or a network server.

PAM360's integration with SafeNet Luna PCIe HSM allows you to use the HSM to encrypt your data as well as to store it within the device itself.

At the end of this section, you will have learned the following:

1. Workflow
2. Configuring SafeNet HSM for PAM360
3. Migrating to the SafeNet HSM Encryption Method

1. Workflow



2. Configuring SafeNet HSM for PAM360

1. If you choose SafeNet HSM as your encryption method, you first need to configure the HSM device for your network requirements. You can download the SafeNet installation guide for steps on that.
2. After the installation process is complete, use command prompt to choose a slot number and set a password for the HSM. Once the set up is done, this slot number and password will be used to switch encryption methods.
3. After testing the HSM connection, you may continue with the migration process.

3. Migrating to the SafeNet HSM Encryption Method

You can follow the below steps to initiate the migration:

1. Stop the PAM360 service.
2. Open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory.
3. Execute the following command:

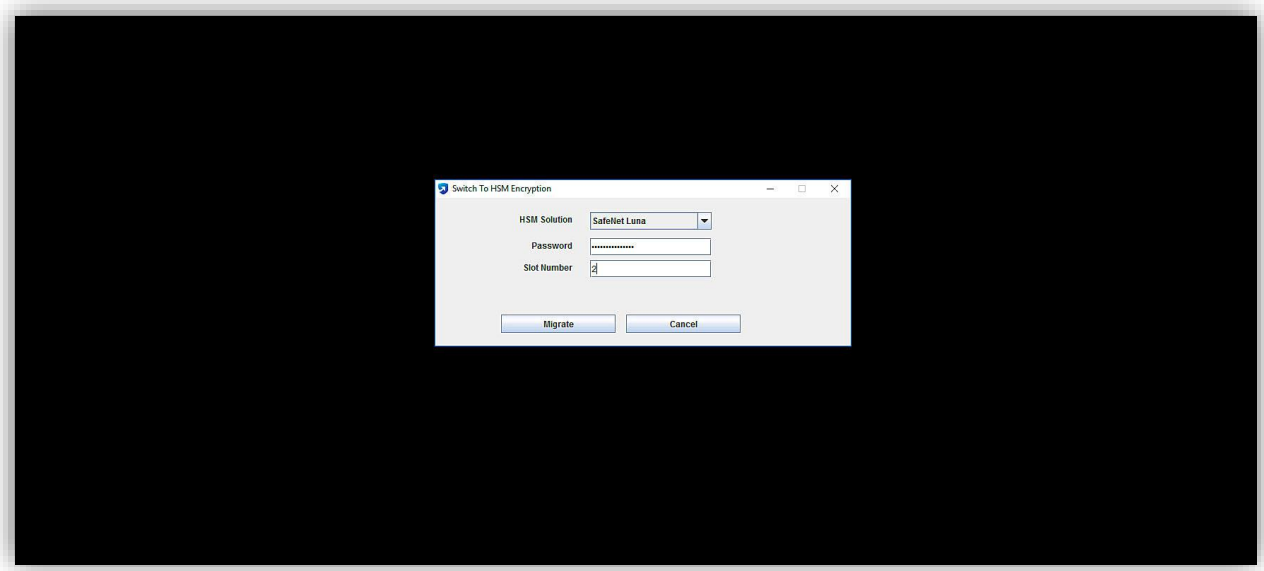
For Windows:

SwitchToHSM.bat

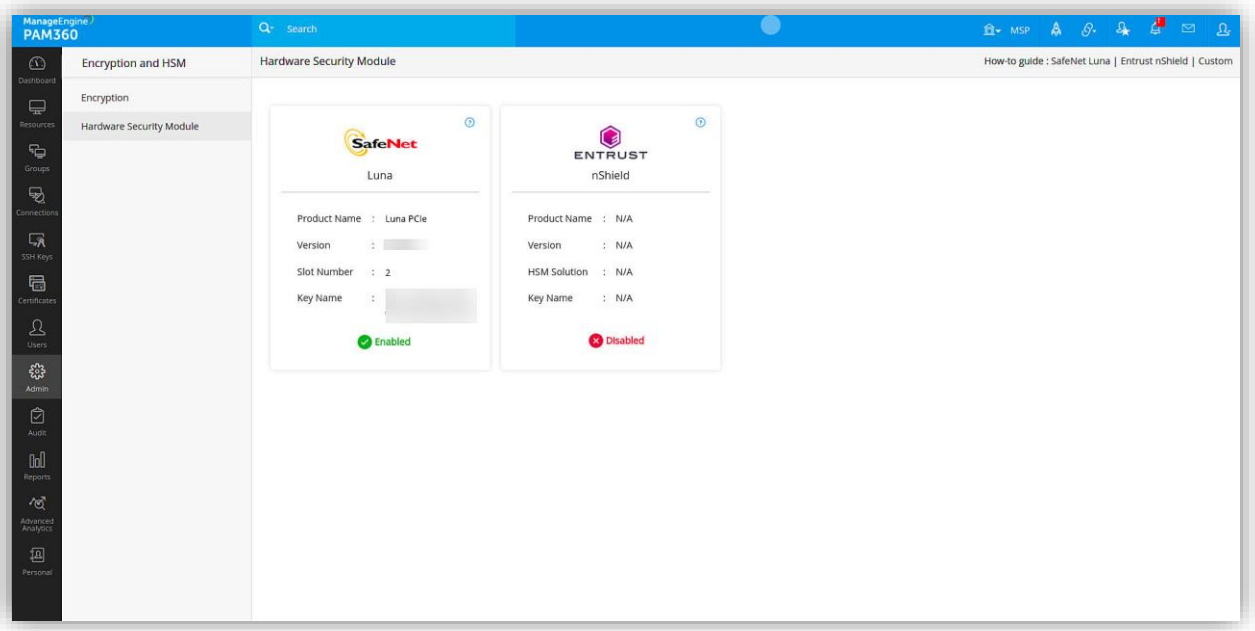
For Linux:

sh SwitchToHSM.sh

4. This will bring up the following dialog box:



5. Here, enter the SafeNet HSM password and slot number in the dialog box and click on **Migrate.**
6. Restart the PAM360 service to complete the migration.
7. To check which method of encryption is currently applied to your data, navigate to the **PAM360 interface and go to Admin >> Configuration >> Encryption and HSM.**



Integration with the Entrust nShield Hardware Security Module (HSM)

Apart from the default encryption method, PAM360 integrates with Entrust nShield HSM, a hardware security module, and provides an option to enable hardware-based data encryption. The integration allows you to utilize hardware-based data encryption for the privileged digital identities and the personal passwords stored in the PAM360 database. You can secure your data encryption key within the HSM to safeguard it locally in your environment. Through this integration, it is also possible to achieve FIPS 140-2 compliance for the privileged identities in your environment and ensure enhanced data security.

PAM360 supports two modes of encryption that encompasses the Entrust nShield HSM:

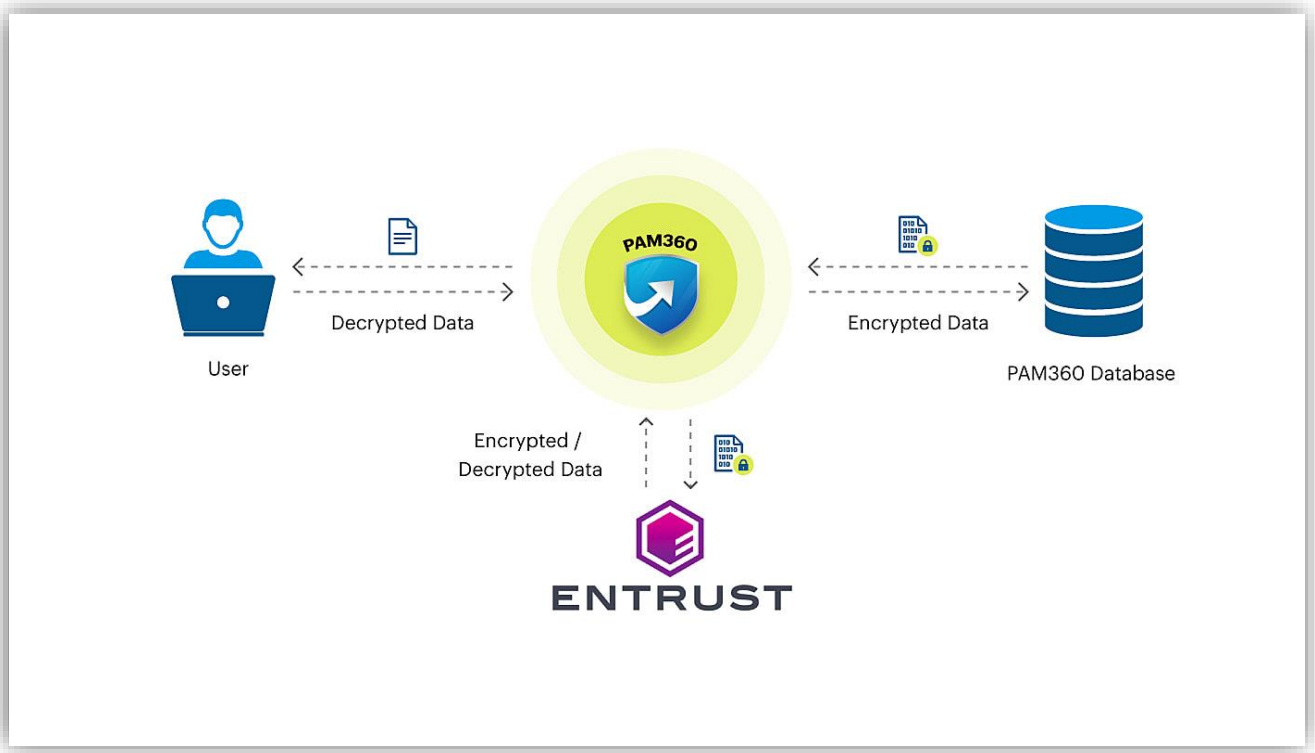
1. Module Only Key
2. Softcards

Read further to learn how to configure them in detail.

1. **Workflow Diagram**
2. **Configuring the Entrust nShield HSM**
3. **Migrating to the Entrust nShield HSM Encryption**

1. Workflow Diagram

The workflow diagram depicting the encryption and decryption workflow between PAM360 and the Entrust nShield HSM is as follows:



2.Configuring the Entrust nShield HSM

2.1 Steps to Install the Entrust nShield HSM

Follow these steps to install and configure PAM360 with the Entrust nShield HSM. The installation must be done on the same server running the PAM360 web server.

2.1.1 Prerequisites

The following are needed for the integration:

1. A working instance of PAM360.
2. An nShield Connect HSM.
3. Good connectivity between the PAM360 instance and nShield's Security World.

2.2 Steps to Install the Security World Software

> **Note:** We recommend you uninstall any existing nShield software before installing the new nShield software.

1. Install and configure the Security World software. For instructions, refer to the Installation Guide and the User Guide for the HSM.

2. Add the Security World utilities path C:\Program Files\nCipher\nfast\bin to the Windows system path.
3. Run the following commands to check connectivity between the machine where PAM360 is running and the nShield Security world.

```
anonkneti <Unit IP>

Output of this command is:

<Unit ESN> < Unit KNETI HASH>

ESN refers to Electronic Serial Number.

To enroll, run the following command:

nethsmenroll  <Unit IP>
```

4. Run the enquiry utility to verify that the HSM is configured properly.

```
C:\Users\Administrator>enquiry
Server

enquiry reply flags none
enquiry reply level Six
serial number ####-####-####
mode operational
...

Module #1

enquiry reply flags none
enquiry reply level Six
serial number ####-####-####
mode operational
...
```

5. Extract and place the world and module files in the path - **C:\ProgramData\nCipher\Key Management Data\local** for Windows and **kmdata/local** for Linux to complete the configuration.
   You can run for example some of the local benchmarking: perfcheck -m1 signing:287
6. As per your organization's security policy, create a Security World, if you don't have one already. As a precaution, create extra ACS cards for each person who has access

privilege and a few spares.
new-world -i -m <module_number> -Q >K/N<

> **Note:** After an ACS card set has been created, the cards cannot be duplicated.

7. Run the nfkminfo utility to confirm the Security World is operational:

```
C:\Users\Administrator>nfkminfo
World
generation 2
state 0x37270008 Initialised Usable ...
...
Module #1
generation 2
state 0x2 Usable
...
Module #1 Slot #0 IC 0
generation 1
phystype SmartCard
...
error OK
...
Module #1 Slot #1 IC 0
generation 1
phystype SoftToken
...
error OK
...
```

Important Notes:

1. The Softcard key is stored as an environmental variable in the path C:\ProgramData\nCipher\Key Management Data\local and it is not saved in the PAM360 database.
2. Based on the encryption mode you have opted for, we highly recommend you to save a copy of the Module only key (or) the Softcard and the Softcard key in a secure location.

3. Migrating to the Entrust nShield HSM Encryption

Follow the below steps to initiate the migration from PAM360 Encryption to the Entrust nShield HSM encryption:

1. Stop the PAM360 service.
2. Open a command prompt and navigate to **<PAM360_SERVER_HOME>\bin** directory.
3. Execute the following command:

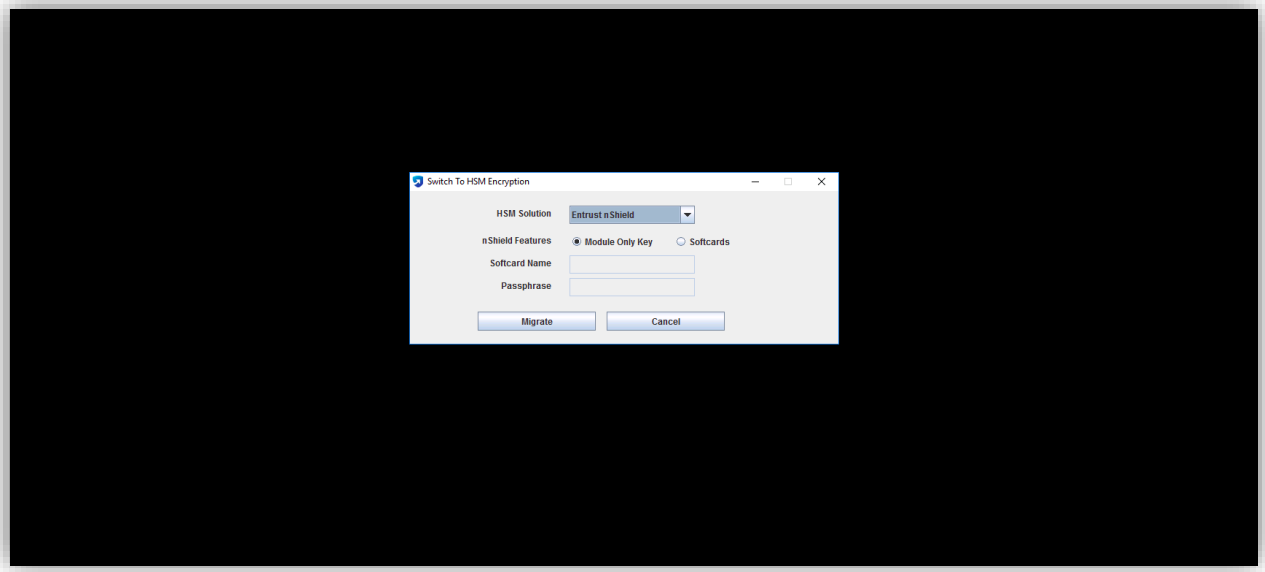
For Windows:

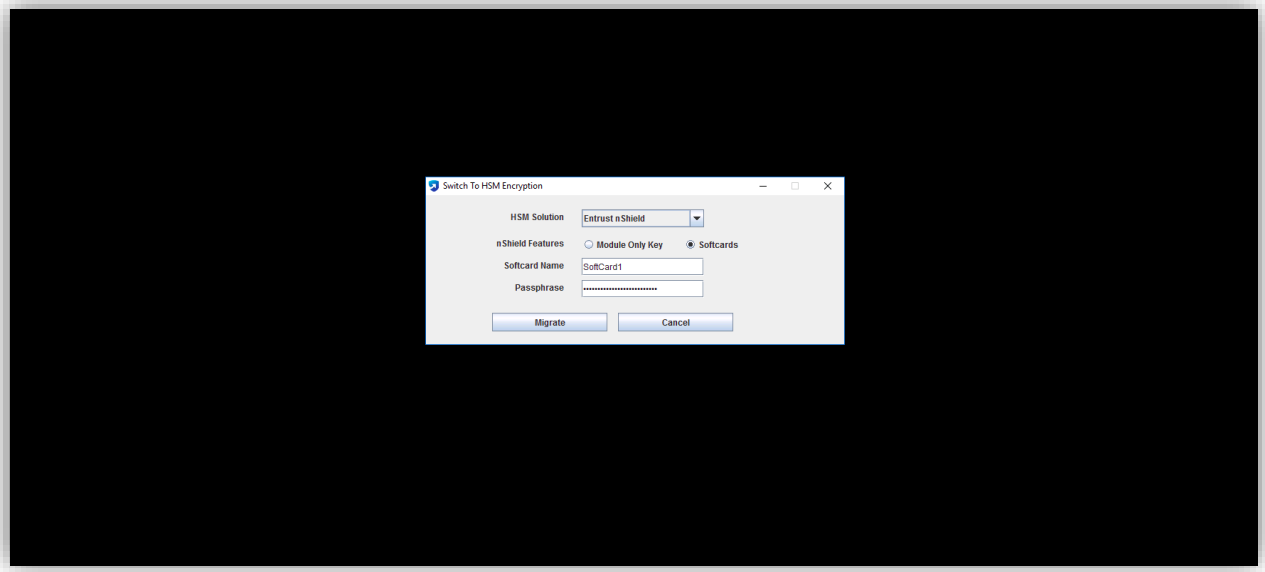
SwitchToHSM.bat

For Linux:

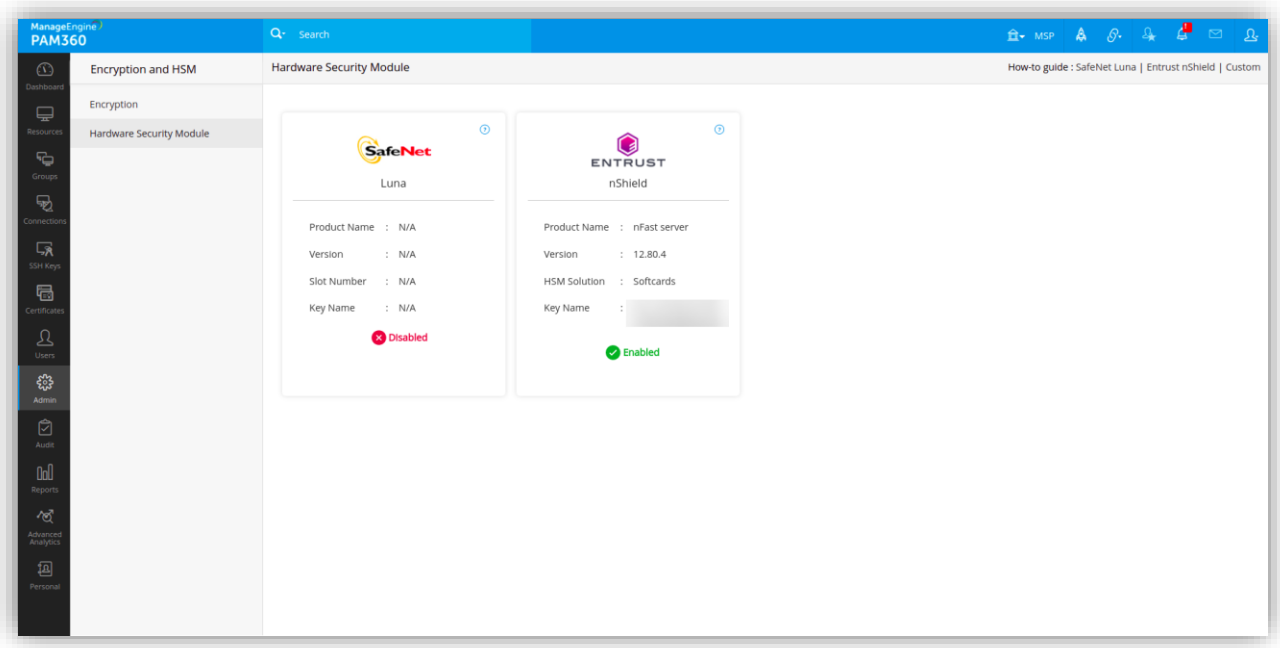
sh SwitchToHSM.sh

4. The command will bring up the following dialog box:





5. Here, choose Entrust nShield from the **HSM Solution** drop-down. In the nShield Features option, choose either Module only key or Softcards.
6. If you choose the **Module Only Key** mode, no need to enter a passphrase. If you choose **Softcards**, enter the Softcard name and its Passphrase.
7. Verify the details and click **Migrate**.
8. To ensure success of the integration, copy this jar file: **nCipherKM.jar** found in your nShield installation folder and paste it in this directory: **<PAM360_Installation_Folder>\lib.**
9. Restart the PAM360 service to complete the HSM migration.
10. To check the method of encryption applied in PAM360, go to the **Admin** tab in the PAM360 interface and select **Configuration >> Encryption and HSM**.



Important Notes:

1. Once you have configured the Entrust nShield HSM as your primary encryption method, you cannot switch back to PAM360 encryption without complete reconfiguration of PAM360. To switch to PAM360 encryption once again and regain some of data from your old build, you can do either of the following:

   i. Export all resources and their passwords from the PAM360 build that is using HSM encryption to use as a backup. Uninstall the old build and install PAM360 anew without HSM encryption. Reinstalling PAM360 will erase your previous data. However, you can import the resources and passwords taken from the previous build to recover some of the data.

   ii. Uninstall the current version and restore an older backup of PAM360 with the PAM360 encryption key.

2. It is not possible to switch encryption modes after the initial configuration.
3. If the current primary encryption method in your PAM360 server is SafeNet Luna HSM, direct transition to the Entrust nShield HSM is not possible without complete reconfiguration of PAM360.

3.1 Steps to Configure the Entrust nShield HSM in a High Availability Setup

If you have High Availability (HA) enabled for PAM360 in your environment, you will have to

reconfigure the HA setup after transitioning to the Entrust nShield HSM as your primary encryption mode.

Follow the below steps to configure the Entrust nShield HSM in a HA setup:

1. Install and configure nShield in the primary and secondary servers and set up high availability as per the steps provided in the following documents, based on the database you use: PostgreSQL / MS SQL.
2. Now, based on the encryption mode you have chosen, do as follows to complete the HSM configuration in a HA setup:
    i. If you have chosen Module only key mode: Copy the key file from the directory path C:\ProgramData\nCipher\Key Management Data\local in the primary server and place it in the aforementioned path in the secondary server.
    ii. If you have chosen Softcards mode: You will find 2 Softcard key files in the directory path C:\ProgramData\nCipher\Key Management Data\local. Copy both the key files and place them in the aforementioned path in the secondary server.
3. Start both the primary and the secondary servers.

Notes:

1. Please ensure that both the primary and secondary servers in the HA setup are running PAM360 build 5550 or above.
2. After switching to the Entrust nShield HSM as the encryption mode, ensure to reconfigure the Application Scaling and Failover Service too, similar to HA.

3.2 Steps to Rotate the HSM Key

As a security best practice, we recommend periodically rotating encryption keys. The same steps used to rotate the PAM360 encryption key will work for the HSM keys as well. Refer to the **section 5** in **Getting Started with PAM360** help section to learn how to rotate the HSM key in both HA and non-HA setups.

4. Troubleshooting Steps

Below is a list of errors that you may encounter in the SwitchToHSM_log.txt log file if there are any discrepancies in the values passed during the integration process. The SwitchToHSM_log.txt file is present under the directory path: <PAM360_Installation_Folder>\logs.

4.1 Exceptions

Exception #1: java.lang.NoClassDefFoundError: com/ncipher/provider/km/nCipherKM|

Problem: The jar file nCipherKM.jar is not available in the directory path: <PAM360_Installation_Folder>\lib.

Solution: Place the nCipherKM.jar file in the Lib folder as mentioned in the step above to rectify the error.

Exception #2: error (st=DecryptFailed) : NFKM_checkpp

Problem: The Softcard passphrase provided during migration was incorrect.

Solution: Please repeat the steps in section 3 with the correct Softcard passphrase.

4.2 Error

Problem: PAM360 service does not start, the following error in present in the the Wrapper.log - **Error: Exception while initializing ManageEngine PAM360 Cryptography. java.lang.Exception: Exception occurred while decrypting**

Solution: The HSM key is not present in the directory path: C:\ProgramData\nCipher\Key Management Data\local as mentioned in the step 3.1.

How to Use Custom Cryptography (Encryption and Decryption) in PAM360

By default, PAM360 encrypts all passwords and other sensitive information using AES-256 symmetrical encryption algorithm and stores only these encrypted data into the password database. The master encryption key is auto-generated and is unique for every installation. In this scenario, the entire encrypt and decrypt methods will reside inside the PAM360 class file. Hence, both the key-generation and encryption logic were handled by PAM360.

Apart from the default cryptography technique, PAM360 now provides an option to use custom cryptography i.e., the encrypt & decrypt methods can now be customized by implementing our Java interface **PAM360EncryptDecrypt** with setter and getter methods, where you can use your own key and encryption logic.

> **Important Note:** Before configuring custom cryptography, take a backup of the PAM360 folder. If the database server is configured in a different machine, ensure that you take a copy of the entire PAM360 database as well. This will avoid data loss, if anything goes wrong during the configuration process. Also, please take necessary precaution with regard to the following aspect:

Personal Password Management

In case, you/other users in your organization have used 'Personal Password Management' in PAM360 with the option of specifying own encryption key, which is NOT stored in PAM360, those data will eventually be lost when you configure custom cryptography and cannot be retrieved later. Therefore, users will have to be advised to use the 'Export Passwords' option in the personal passwords section before configuration.

Steps to implement custom cryptography in an existing PAM360 installation

A brief summary of the steps to configure custom cryptography in PAM360 include writing an implementation class to run your own encryption logic and executing it. Here are the steps in detail:

Step 1: Write your own implementation class

You need to first write your own class implementing the interface **PAM360EncryptDecrypt.java** as explained below.

Please refer to the javadoc for interface PAM360EncryptDecrypt for more details.

Notes:

- **generateCryptographicKey()** method in the class should generate and return a new 32bit key whenever called while **getPam32BitKey()** should return the last generated 32bit key, whenever called.
- **getMSSQLMasterKey()** should return the database master encryption key, that will be used while setting up the MSSQL Always-On cluster as backend. If the return value is null or empty-string, then cluster level nodes' switch-over operations will not be handled.

Step 2: Archive your implementation class

Now, convert your implementation class as **SampleEncryption.jar** and move it to **<PAM360-Installation Folder>/lib** directory.

Step 3: Stop PAM360 server

Stop the server of PAM360 if it is running.

Step 4: Execute the Migrate Cryptography script

Scenario 1: High Availablity/Failover Service is not configured

Execute the **MigrateCryptography.bat** script available in **<PAM360_HOME>\bin** folder and pass your implementation class as argument.

Script Usage: MigrateCryptography.bat com.org.crypto.SampleEncryptDecrypt

Scenario 2: In case of High-Availablity/Failover Service being configured

Here are the steps to be followed for to execute the script if High Availablity or Failover Service has been configured in PAM360:

1. Stop and uninstall secondary server.
2. Configure custom cryptography in Primary by executing **migrateCryptography.bat**.
3. Next, install a fresh secondary instance of PAM360.
4. Now, reconfigure High Availability/ Failover service. The **HAPack.zip** or **FOSPack.zip** will contain the custom encryption jar.

Step 5: Add Custom Cryptography to PAM360ED File

After executing the script, open the file **pam360ed.conf** present inside **<PAM360-Home>/conf** folder. In the file, look for **EDCLASS** and add an entry next to it as specified.

```
EDCLASS=com.adventnet.passtrix.ed.PAM360EncryptDecryptImpl
EDJARS=MyOwnEncDecImpl1.jar,MyOwnEncDecImpl2.jar
```

In the above entry, **MyOwnEncDecImpl1.jar**, **MyOwnEncDecImpl2.jar** are sample cryptography jars. Rename your jar files as required and specify one or more jars in a comma separated format. In case, you are using third party jars, then specify that first followed by your implementation class.

Step 6: Start PAM360 server

After completing the above steps, you need to start PAM360 to give effect to this implementation.

PAM360 Software Development Kit

The PAM360 Software Development Kit (SDK) empowers developers with a predefined set of software requirements tailored for crafting their applications with the PAM360 ecosystem. By furnishing a collection of libraries and meticulous documentation, the PAM360 SDK aids developers in constructing applications compatible with specific platforms, operating systems, programming languages, or frameworks with the required privileged operation to be performed from PAM360.

Comprehensive in scope, the SDK encompasses a rich repository of PAM360 REST API coding examples, facilitating seamless integration of privileged access management functionalities into custom applications. Designed to streamline the development journey, SDKs furnish developers with reusable components and resources, simplifying intricate tasks such as resource access, account management, and user interaction within PAM360.

The SDK was created to allow users to write scripts for applications, microservices, etc, to access PAM360 privileged information without having to write code to directly access the REST APIs. By leveraging the SDK, developers can efficiently embed privileged access management capabilities into their applications, ensuring robust security and seamless functionality within the PAM360 environment.

Essential SDK Terminologies

- **Authentication Token:** A unique token generated during the user creation to access PAM360 with allowed SDK functionalities.
- **SDK Policy:** A mapping method to provide users with the respective PAM360 access in the SDK deployed application.
- **Registration Token:** A token generated during policy creation. This token is used by the user to register their SDK deployed application with PAM360 to gain access to allowed PAM360 privileged actions in their applications.
- **Application:** Any software or service where the SDK will be deployed by the PAM360 users.

Required PAM360 Roles and Permissions

PAM360 users can utilize the SDK if they have been granted access by the administrator and possess a registration token obtained through a registered policy mapped to their user accounts. To grant users SDK access, create a policy for SDK usage, and oversee deployed SDK applications in PAM360, individuals must hold one of the following roles:

1. Privileged Administrator
2. Administrator
3. Custom role with 'SDK Application Management' operation enabled

Setting Up the PAM360 SDK

This help document will walk you through the steps involved in setting up the SDK for the PAM360 users and deploying it on the desired endpoints. It covers the following topics:

1. SDK Environmental Requirements
2. PAM360 SDK Files
3. Registering a Policy in PAM360 for SDK
4. Deploying PAM360 SDK in Services/Applications
5. SDK Application Management

1. SDK Environmental Requirements

To effectively utilize the SDK, ensure the following prerequisites are met as required:

1. **PAM360 Version:** The SDK is compatible with PAM360 version 6700 and above, and requires SDK version 1.0.00 or later.
2. **Development Environment:**
   i. **Java SDK:** Java SDK requires Java application of version 8 or higher.
   ii. **Python SDK:** Python SDK requires Python application of version 3.12 or higher.

2. PAM360 SDK Files

PAM360 provides the following SDK files to empower the development endeavors:

Java SDK

Download the Java SDK from the PAM360 interface by navigating to **Admin >> SDK Management**.

SDK JAR: This core component includes precompiled Java classes and methods of PAM360 APIs that developers can integrate into their projects. It acts like a compressed package containing various class files, resources, and dependent libraries.
Note: This version downloads only the core SDK. Include the following JARS in your project's referenced libraries: commons-logging-1.1.jar, httpclient-4.5.13.jar, httpcore-4.4.9.jar, httpmime-4.5.3.jar and json.jar.

Python SDK

To access the PAM360 Python SDK, navigate to **Admin >> SDK Management** in the PAM360 interface and download the Python SDK.
SDK Package: The Python SDK is bundled as a compressed zip file containing the necessary installable SDK package structured within folders. The `pyproject.toml` file within the SDK package provides installation specifications. Additionally, within the `src` folder, you will find the Python SDK source files essential for integrating with PAM360 APIs.
Note: Post-installation of the SDK, ensure that the requests library version 2.31.0 or higher (https://pypi.org/project/requests/) is installed.

3. Registering a Policy in PAM360 for SDK

To integrate the PAM360 SDK into applications, users need to first obtain the necessary SDK files. Additionally, an administrator must register an SDK policy in PAM360 and map it to the PAM360 user's account. This mapping acts as a bridge to provide the required PAM360 access in the SDK-deployed applications. The registration token associated with the policy grants users' authentication to PAM360 from the SDK-deployed application.

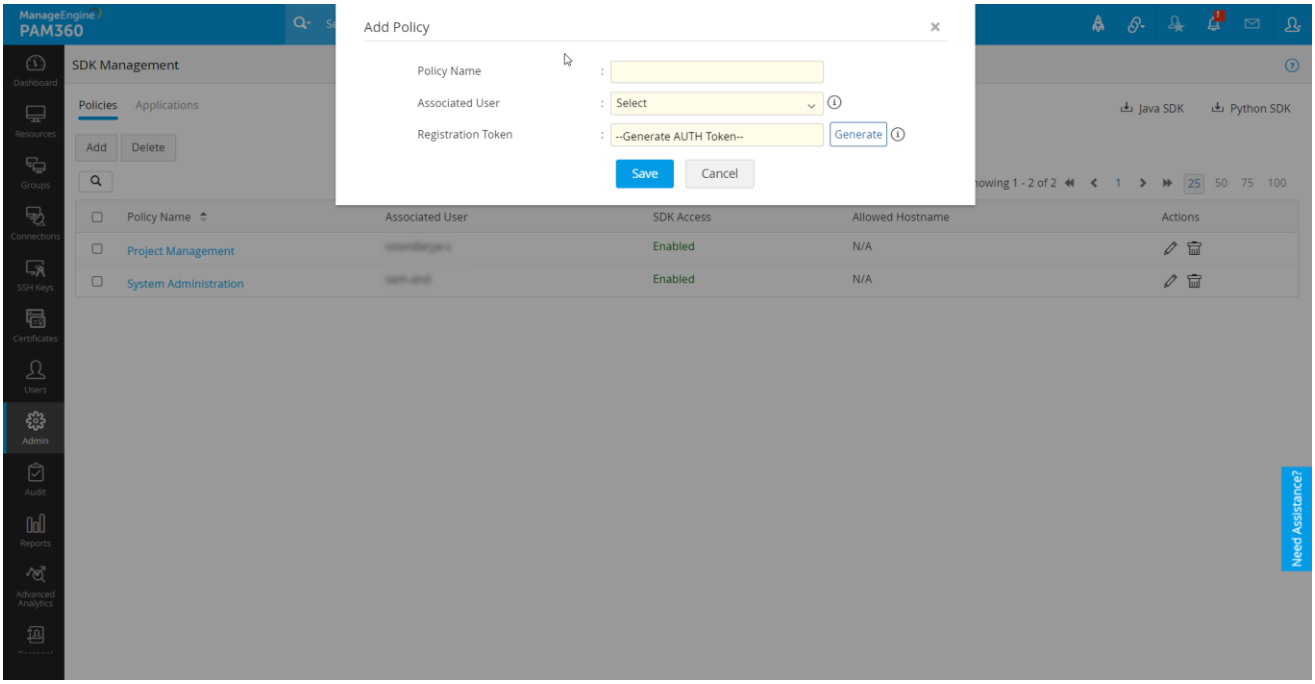
Notes:

i. The user for whom the policy is created should possess the user account with the PAM360 SDK access.

ii. The user can access the PAM360 APIs in their application using the SDK predefined classes and methods based on their role and scope provided in PAM360. For example, a user with the role of Password User can only use the API operations related to the resources and accounts shared with him by the administrator in their application/services.

To register a policy for a user with SDK access,

1. Navigate to **Admin >> DevSecOps >> SDK Management**. This page will display a list of existing policies with details such as the associated user, access status, and allowed hostnames.
2. From the policy tab, click **Add Policy** to create a new policy.
3. In the dialogue box that opens,
   a. **Policy Name:** Enter a descriptive name for the policy.
   b. **Associated User:** Select the user for whom the policy is created to perform the PAM360 operations in their application with the PAM360 SDK.
4. Click **Generate** to create a registration token.
5. Click **Save**. Upon saving the policy, the associated user will receive an email containing the registration token for further SDK usage.



3.1 SDK Policy Management

The PAM360 console allows administrators to perform the following actions on existing policies:

1. Edit policy details
2. Regenerate registration tokens
3. Delete policies

Notes:

i. Deleting an SDK policy will remove all the registered applications associated with the policy.

ii. The number of applications per SDK policy is subject to limitations based on the users' roles in PAM360. Users with the Administrator Type roles can register a maximum of 3 applications per SDK policy. Users with the End-user Type roles can register a maximum of 10 applications per SDK policy.

3.2 How the SDK Policy Works?

Upon SDK deployment by the users, when the SDK sends a request from the deployed application, PAM360 verifies the source of the request associated with a registration token with the policy associated to the user in PAM360 and provides a legitimate and authorized access to the PAM360 interface.

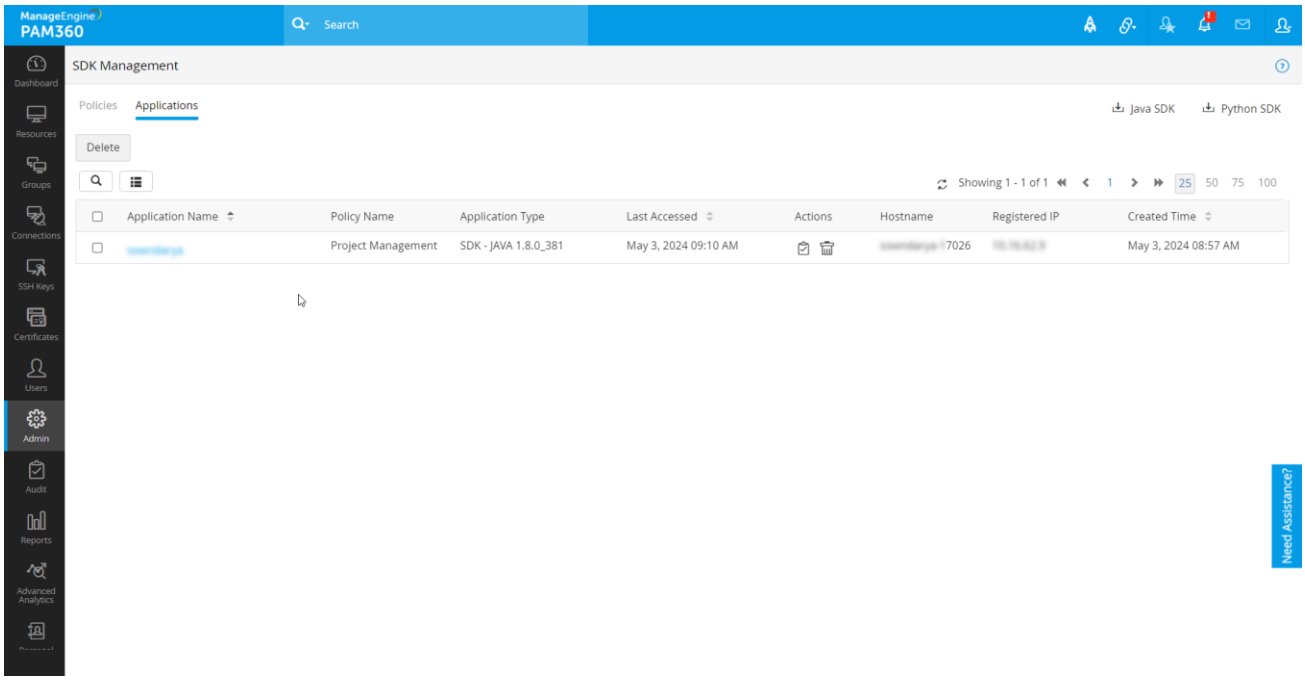
4. Deploying PAM360 SDK in Services or Applications

After completing the administrative tasks mentioned above, users can proceed to use the PAM360 SDK within their desired programming services or applications. Below are the necessary documentation and guidelines for deploying and registering the PAM360 SDK with relevant DevSecOps services or applications, along with sample API codes.
PAM360 Software Development Kit for DevSecOps: Java | Python

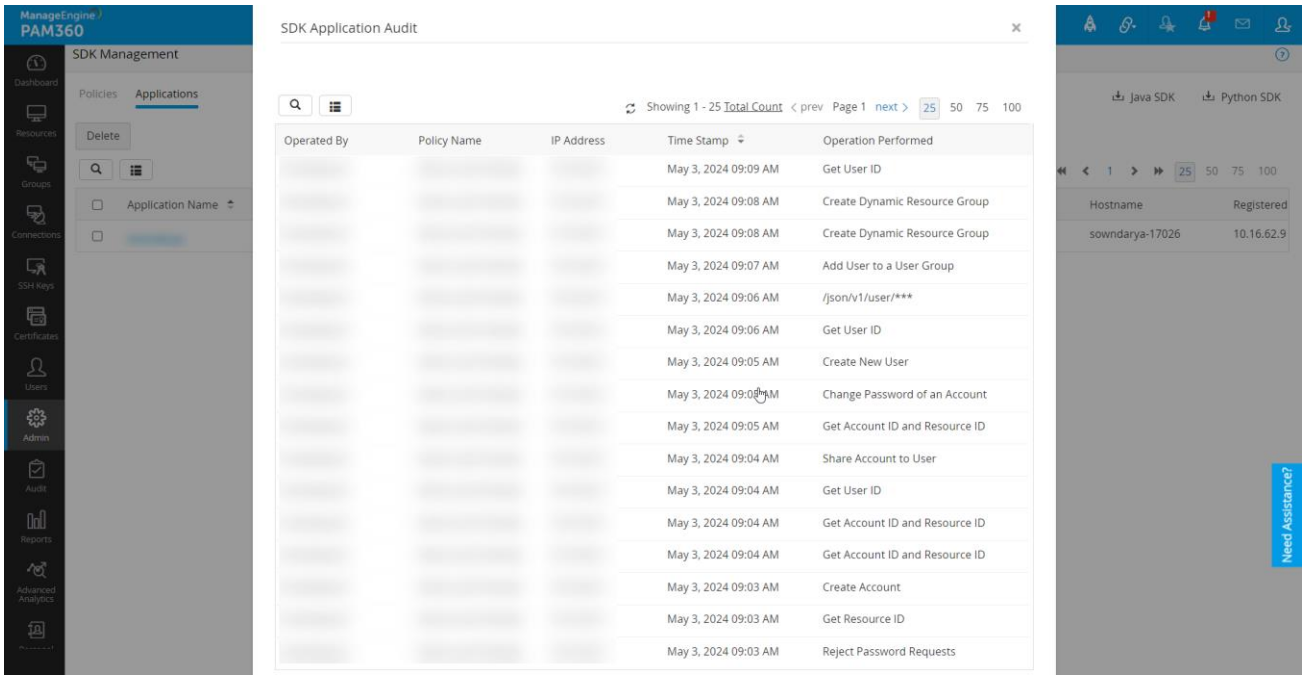
5. SDK Application Management

All applications registered by users with the PAM360 SDK and a registration token are listed here, along with relevant information. Users with respective privileges can view and manage the list of PAM360 registered applications directly from the PAM360 interface.
To access this feature in PAM360:
Navigate to **Admin >> DevSecOps >> SDK Management >> Applications**.

a. Upon navigation, the page will display a list of applications where the PAM360 SDK is deployed. Each application entry includes information such as the registered **Policy Name**, **Application Type**, **Last Accessed**, **Actions**, **Machine Name**, **Registered IP**, **Created Time**, and **Notes**.



b. Administrators can track all PAM360 operations performed in the applications using the **SDK Audit** button located under the **Actions** column. This provides an audit trail of activities performed directly from the SDK deployed applications.



c. Administrators also have the ability to delete applications, which will unlink the SDK from the registered applications. Deleting an application removes the connection, preventing the application from retrieving data from PAM360 unless it is re-registered.

d. Additionally, administrators can edit the application name and add notes for quick identification and reference.

Software Development Kit for DevSecOps - Java

Once a PAM360 user in an organization is provided with the SDK access and a registered token, they can further proceed in using the SDK by registering the relevant PAM360 SDK in their application/services. To do so, follow the below documentation.

1. Java SDK Prerequisites

i. Java SDK requires Java application of version 8 or higher.

ii. Deploy the downloaded PAM360 Java SDK JAR into the lib folder within your application or development service directory.

> **Notes:** Once you are granted SDK access in PAM360, an email containing the authentication token and a link to download the Java SDK will be sent to your registered email address.
>
> Alternatively, you can reach out to your administrator for the Java SDK file.

The core SDK will be downloaded using the provided link. Include the additional JARS (commons-logging-1.1.jar, httpclient- 4.5.13.jar, httpcore-4.4.9.jar, httpmime-4.5.3.jar and json.jar) in the project's referenced libraries.

iii. To ensure a successful SDK registration, add the PAM360 web server certificate to the cacerts folder in the Java installation directory.

2. Registering the Java Application with PAM360

Upon deploying the SDK JAR file to the Java application, prior to initiating the creation of your Java application, certain configuration steps or the provision of necessary information are required to establish a connection, register, or utilize PAM360 functionalities provided by the SDK.

Use the provided sample code with the **ClientRegistrationManager** and **ServiceConfiguration** objects to register your Java application/services with the PAM360 server. This registration

registers your Java application to the PAM360 interface and facilitates the subsequent retrieval of data from the PAM360 repository via available API methods. It is a one-time operation on the machine where the PAM360 SDK is utilized.

```
import com.manageengine.pam360.sdk.exception.SDKException;
import com.manageengine.pam360.sdk.services.ClientRegistrationManager;
import com.manageengine.pam360.sdk.services.ServiceConfiguration;
public class SDKRegistrationExample {
public static void main(String [] args) { ServiceConfiguration config = null; try {
String registrationToken = "#######-####-####-####-############"; String
pamHostName = "CHEST11F-H07";
int pamServerPort = 8282;
config = new ServiceConfiguration(pamHostName, pamServerPort);
ClientRegistrationManager registrationManager = new
ClientRegistrationManager(config);
registrationManager.register(registrationToken);
//To Update a New Registration Token -
registrationManager.update(registrationToken,"");
//To check if there any SDK registered - boolean isRegistered =
registrationManager.isRegistered();
}
catch (SDKException ex) { ex.printStackTrace();
}
}
}
```

i. **registrationToken** - Unique identifier associated with a SDK policy received via an email or from administrator.
ii. **pamHostName** - Specific host from where the PAM360 application operates.
iii. **pamServerPort** - Port number for the communication with the PAM360 server.

2.1 How Does the User Registration Work?

Upon executing the above sample code with the classified ClientRegistrationManager and ServiceConfiguration SDK java objects, the Java application will be registered with the

PAM360 application. In response to the registration, an SDK config file will be created in the folder named sdk_config.

> **Notes:** Make sure to securely store the generated config file. The config file value acts as a primary source of authentication between the Java application and PAM360 while making the API calls from the Java application.

Upon completion, the registered application with the deployed PAM360 SDK will be reflected in the PAM360 web interface. Information such as Policy Name, Application Type, and Accessed Information, along with audit details of actions performed within the application relevant to PAM360, will be accessible. Administrators possess the capability to oversee details of SDK-deployed applications directly from the PAM360 interface.

3. Invoking a PAM360 API via SDK Deployed Application

Below is a sample code for initializing an API via PAM360 SDK from the Java application/services.

E.g., **To Fetch a Password of an Account**

```
import com.manageengine.pam360.sdk.exception.SDKException; import
com.manageengine.pam360.sdk.resources.Password;
import com.manageengine.pam360.sdk.services.ClientRegistrationManager;
import com.manageengine.pam360.sdk.services.PAMService;
import com.manageengine.pam360.sdk.services.ServiceConfiguration;
public class getPasswordOfAccount {
public static void main(String[] args) { ServiceConfiguration config = null; try {
String pamHostName = "CHEST11F-H07"; int pamServerPort = 8282;
config = new ServiceConfiguration(pamHostName, pamServerPort); String
restApiToken = "########-####-####-####-############";
PAMService service = new PAMService(config, restApiToken); Password
password = service.getPasswordInstance();
System.out.println(password.getPasswordOfAccount("ad-services2k19",
"sysadmin"));
}
catch (SDKException ex) { ex.printStackTrace();
}
}
}
```

Refer to this Java Documentation to learn about the available objects, methods, and classes.

4. Java SDK Best Practices

SDK Logs - The PAMSDKLogger is responsible for logging all the internal errors and activities that occur within the PAM360 SDK. This class reports all internal errors that occur in an entity, registration, etc. By default, the SDK-relevant logs are stored in a folder named **sdk_logs** in the PAM360 SDK's deployed Java application. However, for security reasons, you can provide an absolute file path in a preferred directory using the below steps while invoking an API. This is a one-time process; once defined, the same path will be used for logs in the subsequent API calls.

```
import com.manageengine.pam360.sdk.services.PAMSDKLogger;
.
.
PAMSDKLogger logger = new PAMSDKLogger();
logger.setLogLocation("D:\2024\Java\Vault\SDK");
.
.
```

SDK Config -The config file value generated during the application registration acts as a primary authentication source between the Java application and PAM360 while making the API calls from the Java application. By default, while registering the application, the config file will be stored in a folder called **sdk_config** within the Java application. However, for security reasons, you can specify the desired directory path using the below steps while invoking an API. This allows you to store the SDK config file in a location of your choice.

```
import com.manageengine.pam360.sdk.services.DefaultClientConfigHandler;
.
.
ServiceConfiguration config = null; try {
String pamHostName = "CHEST11F-H07"; int pamServerPort = 8282;
config = new ServiceConfiguration(pamHostName, pamServerPort);
config.setConfigurationPath("D:\2024\Java\Vault\SDK")
.
.
```

Software Development Kit for DevSecOps - Python

Once a PAM360 user in an organization is provided with the SDK access and a registered token, they can further proceed in using the SDK by registering the relevant PAM360 SD application/services. To do so, follow the below documentation.

1. Python SDK Prerequisites

i. Python SDK requires Python application of version 3.12 or higher.

ii. Unzip the downloaded Python SDK zip file and use the following command to install the Python SDK package: **pip install <sdk-folder-path>**

Notes:

Once you are granted SDK access in PAM360, an email containing the authentication token and a link to download the Python SDK will be sent to your registered email addr Alternatively, you can reach out to your administrator for the Python SDK file.

Post-installation of the SDK, ensure that the requests library version 2.31.0 or higher (https://pypi.org/project/requests/) is installed.

iii. If the PAM360 web server uses a self-signed certificate, download and deploy it in the desired system directory and update the respective certificate path while creating the se configurations.

2. Registering a Python Application with PAM360

Before you start developing your Python application, it is essential to configure and establish a connection between the PAM360 server and the Python SDK. This process involves steps to register your application and enable it to utilize PAM360 functionalities.

You can use the following sample code, which involves the ClientRegistrationManager and ServiceConfiguration objects, to perform the registration of your Python application PAM360 server. This registration ensures that your application is recognized within the PAM360 interface, allowing you to access data from the PAM360 repository through availab methods. Remember, this registration is a one-time operation on the machine where you're using the PAM360 SDK.

```
import logging
from src.com.manageengine.pam360.sdk.services.registration_utility import
ClientRegistrationManager from
src.com.manageengine.pam360.sdk.services.service_configuration import
ServiceConfiguration
app_logger = logging.getLogger( # Configuration Steps name )
sdk_registration_token = "#######-####-####-####-############" host_name = "CH-
TEN-53D07"
port_no = 8282
certificate_path = "D:\2024\Python\Secure Vault\SDK" # SSL Certificate file Path in
.pem format service_config = ServiceConfiguration(host_name, port_no,
certificate_path)
# Registration Steps try:
sdk_client_name = "Sample Python Application Name" registration_manager =
ClientRegistrationManager(service_config)
registration_manager.register(sdk_registration_token, sdk_client_name)
except SDKRegistrationError as ex: app_logger.error(ex)
```

i. **sdk_registration_token** - Unique identifier associated with a SDK policy received via an email or from administrator.
ii. **host_name** - Specific host from where the PAM360 application operates.
iii. **port_no** - Port number for the communication with the PAM360 server.

Upon running this code, your Python application will be registered with the PAM360 server, enabling it to interact with PAM360 functionalities via API calls.

2.1 How Does the User Registration Work?

Executing the provided sample code with the designated ClientRegistrationManager and ServiceConfiguration SDK Python objects will result in the registration of the Python application with the PAM360 application. Following registration, an SDK config file will be generated and stored in a folder named sdk_config.

Notes: Make sure to securely store the generated config file. This config file serves as the primary authentication method between the Python application and PAM360 when maki calls from the Python application.

Upon successful completion, the registered application utilizing the deployed PAM360 SDK will be visible in the PAM360 web interface. Details such as Policy Name, Applicatio Accessed Information, and audit logs of actions performed within the application relevant to PAM360 will be accessible. Administrators retain the capability to monitor the specifi SDK-deployed applications directly from the PAM360 interface.

3. Invoking a PAM360 API via SDK Deployed Application

Below is a sample code for initializing an API via PAM360 SDK from the Python application/services.

E.g., **To Fetch a Password of an Account**

```
import logging
from com.manageengine.pam360.sdk.exception.pam_exception import SDKError
from com.manageengine.pam360.sdk.services.pam_service import PAMService
from com.manageengine.pam360.sdk.services.service_configuration import
ServiceConfiguration
app_logger = logging.getLogger( try:name )
pam_host_name = "CHEST11F-H07" pam_server_port = 8282
config = ServiceConfiguration( host=pam_host_name, port=pam_server_port,
certificate_path=r"path\to\certificate.pem" # Provide the certificate path while using
a self-signed certificate for the PAM360 web
)
user_api_token = "########-####-####-####-############"
# PAMService is the entry point to all entities
service = PAMService(service_config=config, user_token=user_api_token,
org_name="Client Organisation") # Entity is the entry point to all entity-related
operations
# In this case, Password Entity
password_entity = service.get_password_instance() # Get Password of an Account
under a Resource resource = "ad-services2k19"
account = "sysadmin"
password = password_entity.get_password_account(resource_name=resource,
account_name=account) print(f"Password of {account} Account under {resource}
Resource is {password}")
except SDKError as ex:
app_logger.error(ex)
```

Refer to the Python Documentation to learn about the available classes, objects, functions.

4. Python SDK Best Practices

Virtual Environments - It is recommended to use virtual environments in Python while creating an application. This is for isolating dependencies, simplifying management, ensuri reproducibility, providing sandboxing for testing, enhancing security, and facilitating easy cleanup, making them a best practice for application development, especially when incorp SDK packages.

SDK Logs - The PAMSDKLogger is responsible for logging all internal errors and activities within the PAM360 SDK. This class records any internal errors that occur within an en registration, etc. By default, logs related to the SDK are saved in a folder named **sdk_logs** within the deployed Python application of the PAM360 SDK. However, for security purp have the option to specify an absolute file path in a preferred directory using the below steps while invoking an API. This is a one-time process; once defined, the same path will be logs in the subsequent API calls.

```
from com.manageengine.pam360.sdk.services.pam_sdk_logger import
PAMSDKLogger PAMSDKLogger.set_log_file_path(r"D:\2024\Python\Secure
Vault\SDK")
```

SDK Config -The config file value serves as the primary authentication mechanism between the Python application and PAM360 when making API calls. By default, during applic registration, the config file is stored in a folder named **sdk_config** within the Python application. Yet, for security considerations, you can define a desired path in a preferred directo the below steps while invoking an API. This allows you to store the SDK config file in a location of your choice.

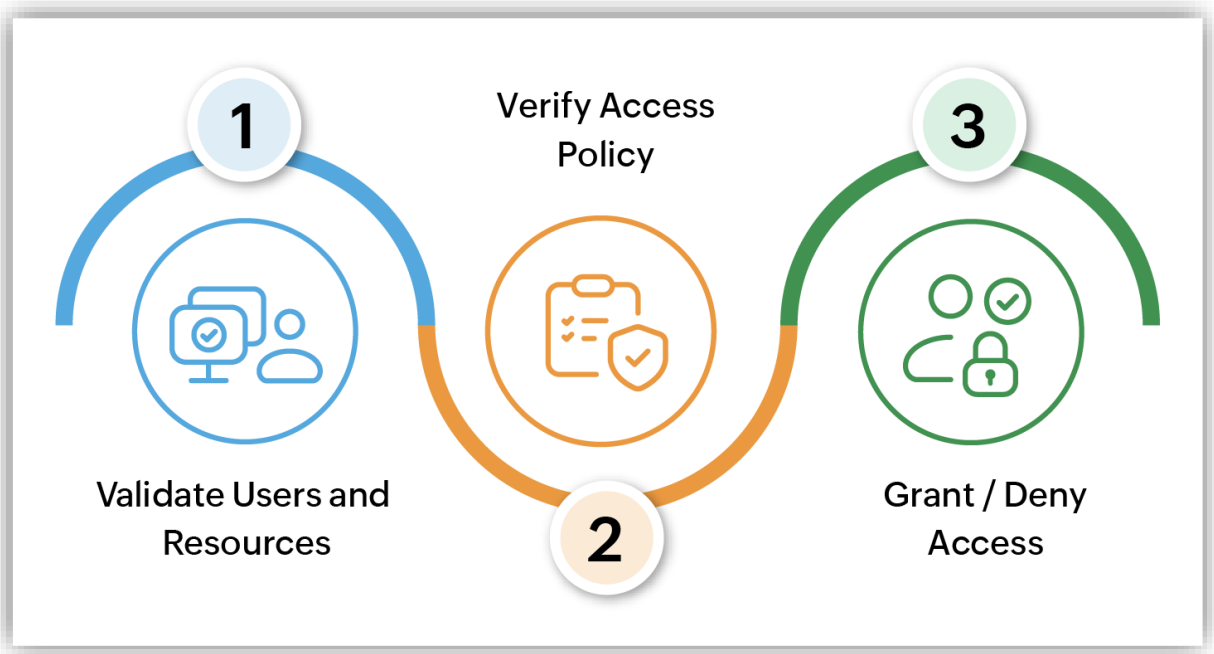
```
from com.manageengine.pam360.sdk.services.service_configuration import
ServiceConfiguration config = ServiceConfiguration(
host=pam_host_name, port=pam_server_port,
certificate_path=r"path\to\certificate.pem"
config_folder_path=r"D:\2024\Python\Secure Vault\SDK"
}
```

Implementing Zero Trust Approach via PAM360

Zero Trust - Policy-Based Access Privilege

Zero Trust is the trending methodology of granting access privileges to users to the resources in an organization by verifying their activities and state with the score-based access policy method instead of trusting them instinctively, irrespective of their identity. The foremost motto of this approach is never to trust and always verify before granting privileges in an organization. By formulating real-time user/resource scores, the Zero Trust approach highlights vulnerable users and non-compliant devices, thus restricting further access privileges to the users and the resources via policy-based access privilege methodologies.

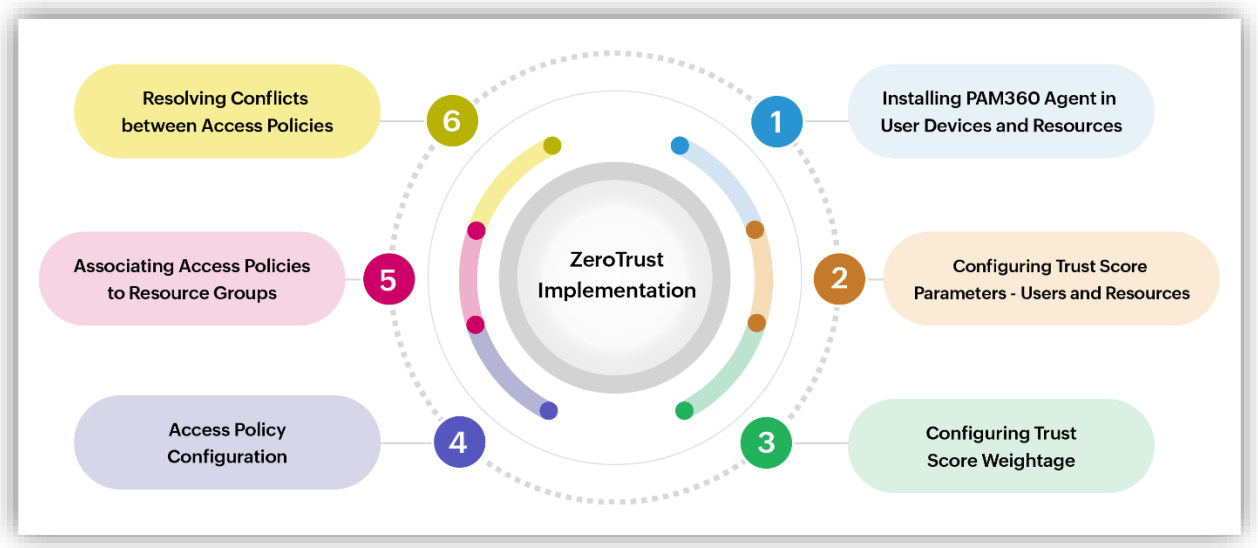
Zero Trust Approach in PAM360



Where does this Zero Trust Approach Benefit the organization?

When an infrastructure of an organization enlarges, managing the privileged resources and user activities gets out of control, and monitoring them throughout will be a tedious process. There comes the Zero Trust approach, which minimizes the risk of data breaches and cyber attacks by eliminating the concept of trust altogether by calculating user and resource trust

scores using predefined conditional parameters with an assist from respective installed agents. This decisive action ensures that only authorized users/devices have access to critical resources, minimizing the risk of data breaches and cyber-attacks.



This document will help you learn more about implementing the Zero Trust approach in your organization via PAM360. Refer to the below sub-sections to learn more about the further Zero Trust implementation process:

1. User Roles
2. Installing PAM360 Agent with Zero Trust Module
3. Configuring Trust Score Parameters
4. Configuring Weightage for Trust Scores
   4.1 Trust Score Details and Usage
5. Zero Trust Access Policies
6. Associating Access Policies to Resource Groups
7. Resolving Conflict between Access Policies
8. Limitations in Policy-Based Access Privilege Functionality

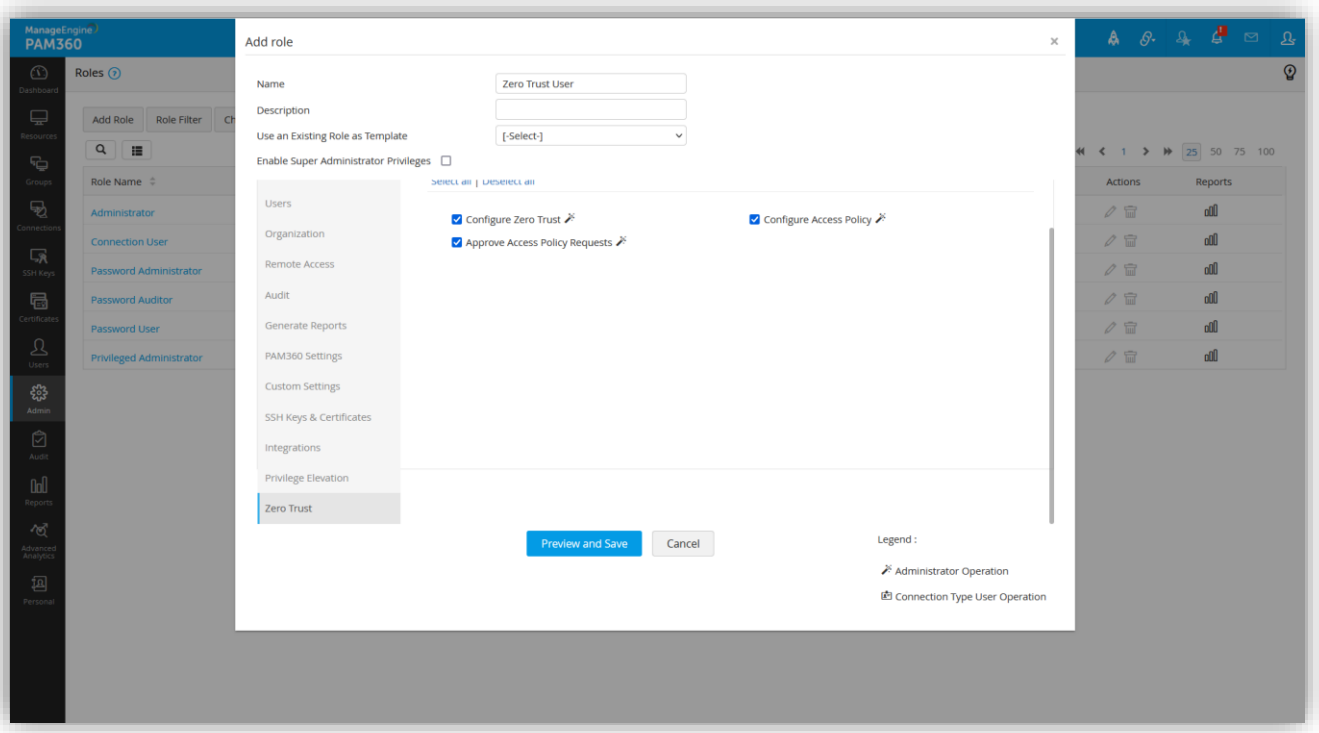
1. User Roles

Zero Trust configuration involves four main operations: configuring parameters and trust score weightage, configuring access policies, approving access policy requests, and resolving conflicts between access policies for a resource. By default, users with:

1. The **Privileged Administrator** role has access to all of these operation privileges.

2. The **Administrator** role can create, manage and resolve conflicts in their access policies, approve access policies and view the access policies created by other administrators.
3. The **Password Administrator** role can perform all operations as **Administrators** except for access policy approval.

If you require a custom user role to meet your specific needs, you can navigate to '**Admin >> Customization >> Roles >> Zero Trust**' and enable the necessary permissions that follow:



1. **Configure Zero Trust** - A user with this role enabled can define parameter values and trust score weightage.
2. **Configure Access Policy** - Can create, manage and resolve conflicts in their access policies and view the access policies created by other administrators.
3. **Approve Access Policy Request** - Can view and approve the access policies created by another administrator along with the operations performed by the **Configure Access Policy** role.

> **Note:** Granting the **Approve Access Policy Request** role will automatically permit the **Configure Access Policy** role to the users.

2. Installing PAM360 Agent with Zero Trust Module

The Zero Trust methodology works in an organization based on access policies defined via a set of score parameters. For the policy-based access privilege feature to fetch data for different parameters from user devices and resources for score validations, an agent with the relevant usage type is to be installed in the respective user devices and resources that come under the Zero Trust approach for privileged access and account governance.

To fetch data for **User Score Parameters**, an agent with the usage type '**User Device**' is to be installed in the user machines. Similarly, an agent with the usage type '**Resource**' should be installed in all the resources with the enabled **Zero Trust Module** to fetch the data for **Resource Score Parameters**.

> **Note:** If you want to implement the policy-based access control via the Zero Trust feature in an agentless approach, you can proceed with user authentication parameters for configuring the parameters, weightage and access policy.

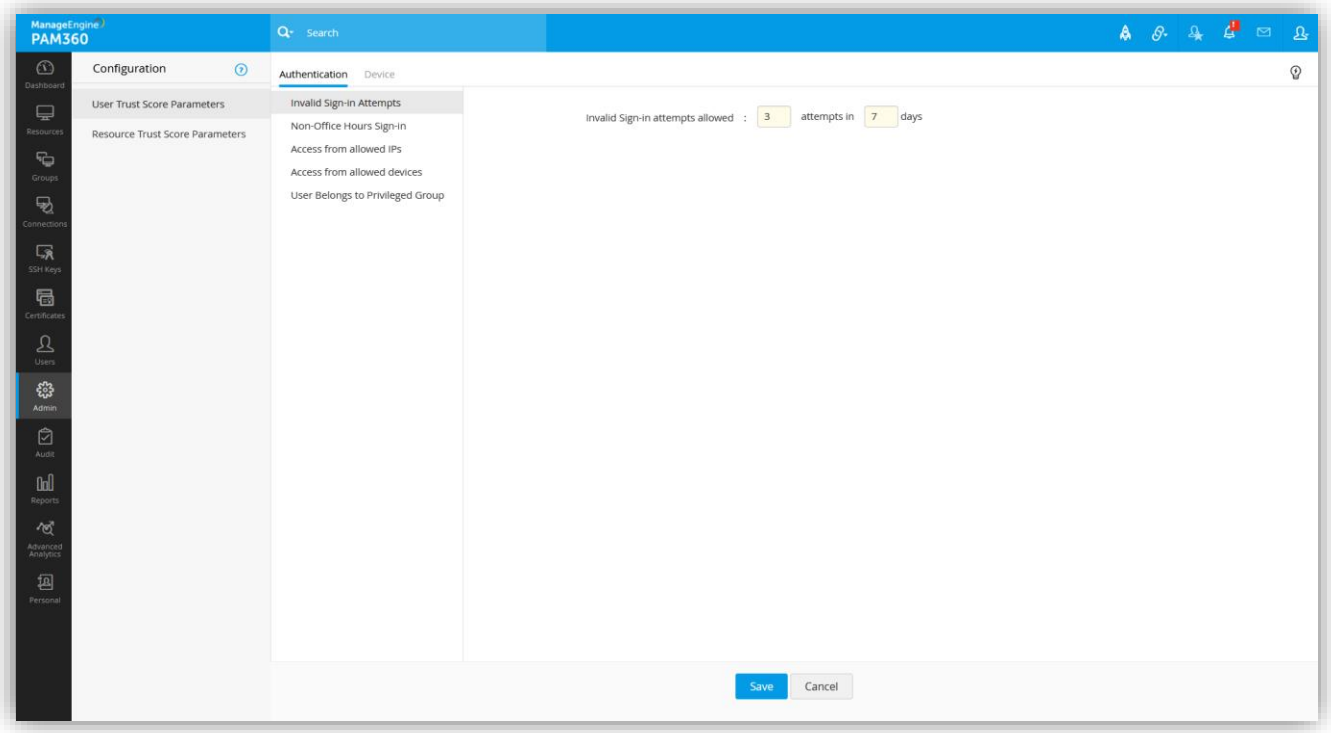
Refer to this help section to learn more about installing the PAM360 agent in the required user devices and resources.

3. Configuring Trust Score Parameters

The Zero Trust approach is micro-segment behavioural analytics of users and resources based on the predefined parameters for the trust score calculation. Nineteen types of parameters revolve around the Zero Trust approach in PAM360 for the trust score calculation. They are organized into two different categories:

- User Score Parameters (user authentication postures and user device configuration/security postures)
- Resource Score Parameters (resource configuration/security postures)

In the **Admin >> Zero Trust >> Configuration** page, you can set the desired baseline passing value for those parameters for the trust score calculation as per your organization's needs. To know more about each parameter in detail and about defining the parametric conditions for trust score calculation, refer to this help document.



Once the Zero Trust approach is implemented in your organization, users must maintain those minimum predefined conditional parameters to maintain their trust scores high, thus granting them access to privileged accounts or elevating their self-privileges based on the administrator's configuration.

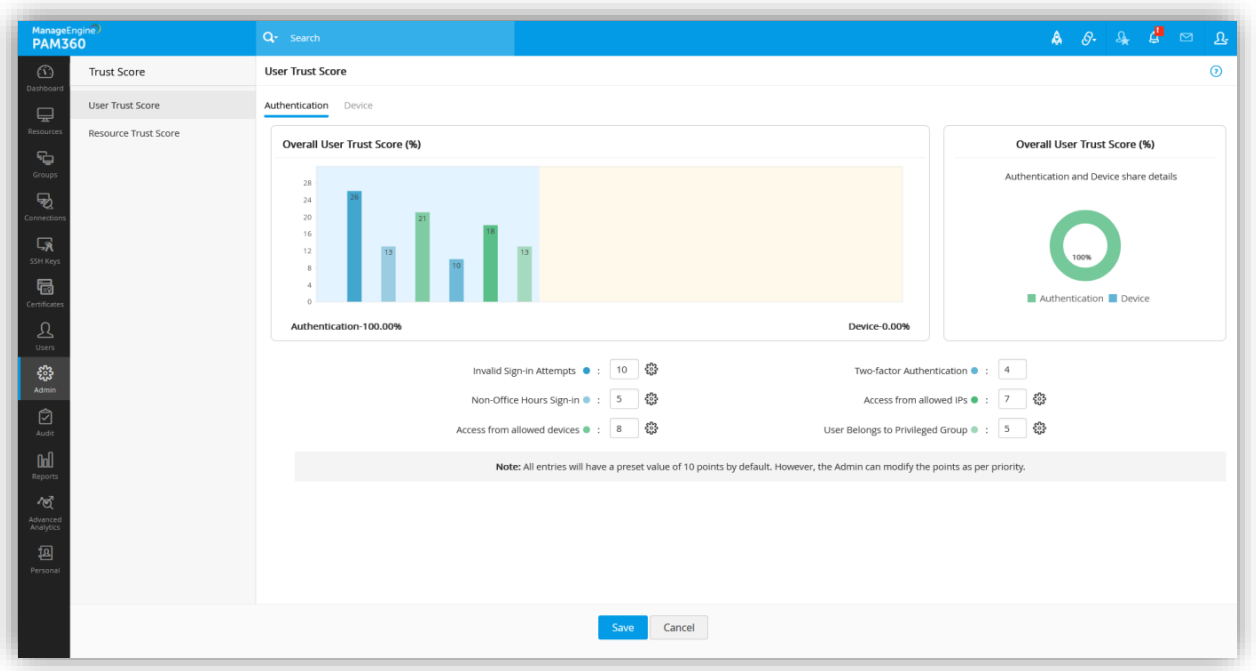
4. Configuring Weightage for Trust Scores

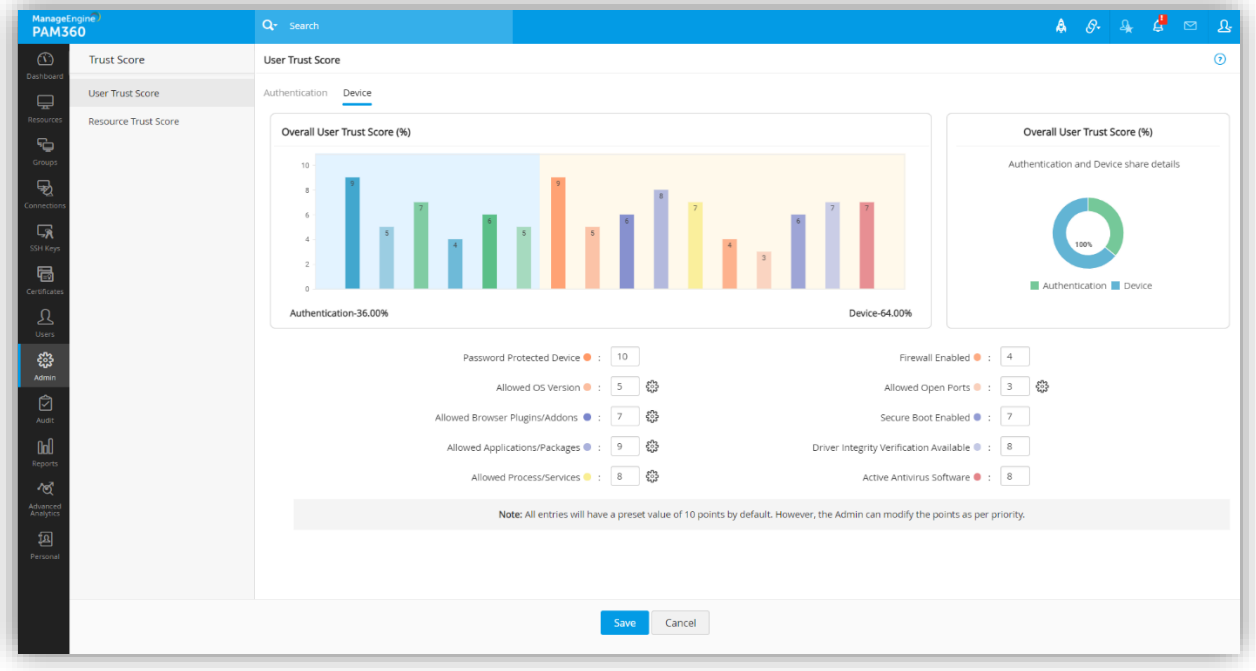
Configuring upon the parameter weightage in this section, the user trust score will be calculated based on user authentication and user device configuration/security postures, and the resource trust score will be calculated based on resource configuration/security postures. The calculated trust scores will be shown in the **Users** and **Resources** tabs beside the respective users and the resources.

To configure the trust score weightage for the user score parameters:

1. Navigate to '**Admin >> Trust Score >> User Trust Score**'.
2. The user trust score is derived using the Authentication and Device parameters of the users. In the **Authentication** and **Device** tabs, enter a weightage value between **0 - 10** in the field beside the respective parameters based on your organization's importance over the parameter.

3. The bar chart presented in the **User Trust Score** window will be updated with the points for each parameter based on the fixed weightage values out of 10, resulting in a total score of 100 that will be considered for the final trust score validation of the user when the respective parametric conditions are met.



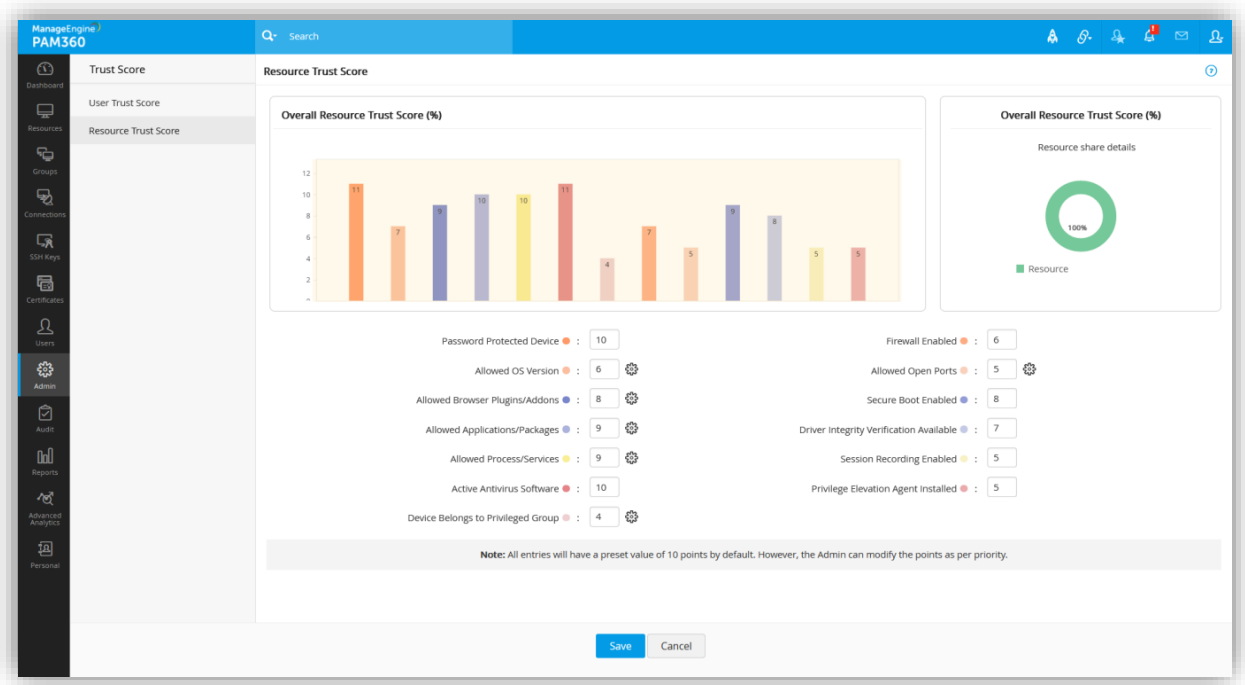


Notes:

i. The **User Trust Score** is a combination of points from the user authentication and user device state based on the configured weightage values.
ii. The user authentication parameter points will be updated only during each PAM360 login.

Similarly, to configure the trust score weightage for the resource score parameters:

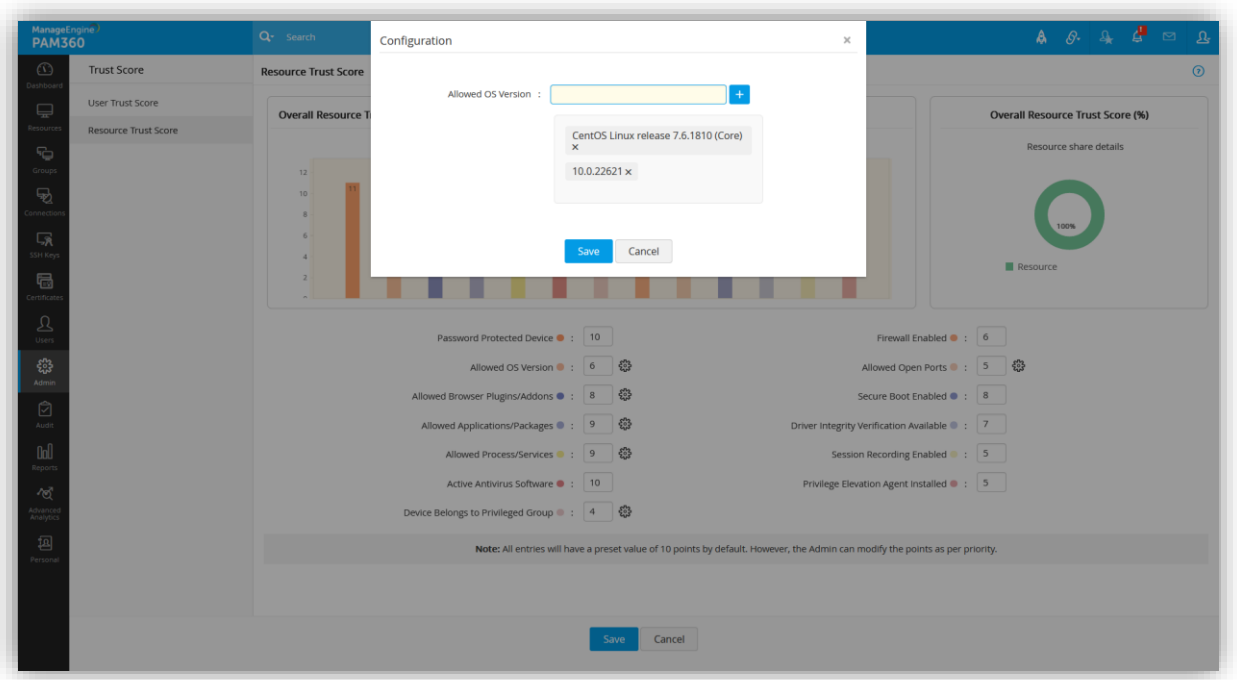
1. Navigate to '**Admin >> Trust Score >> Resource Trust Score**'.
2. Enter a weightage value between **0 - 10** in the field beside the respective parameters.
3. The bar chart presented in the **Resource Trust Score** window will be updated with the points for each parameter based on the fixed weightage values out of 10, resulting in a total score of 100 that will be considered for the final trust score validation of the resource when the respective parametric conditions are met.



From the **Trust Score** page, you can also modify or define the condition parameters that are defined or left in the **Admin >> Zero Trust >> Configuration** page. To do so:

1. Click on the gear icon beside the respective parameter.

2. In the pop-up that opens, modify/define the conditions as required for your organization.
3. Click **Save** to save the newly defined or the modified changes. The respective parameter change will get reflected in the **Admin >> Zero Trust >> Configuration** page.



To know more in detail about how these trust score parameters work, refer to this help document.

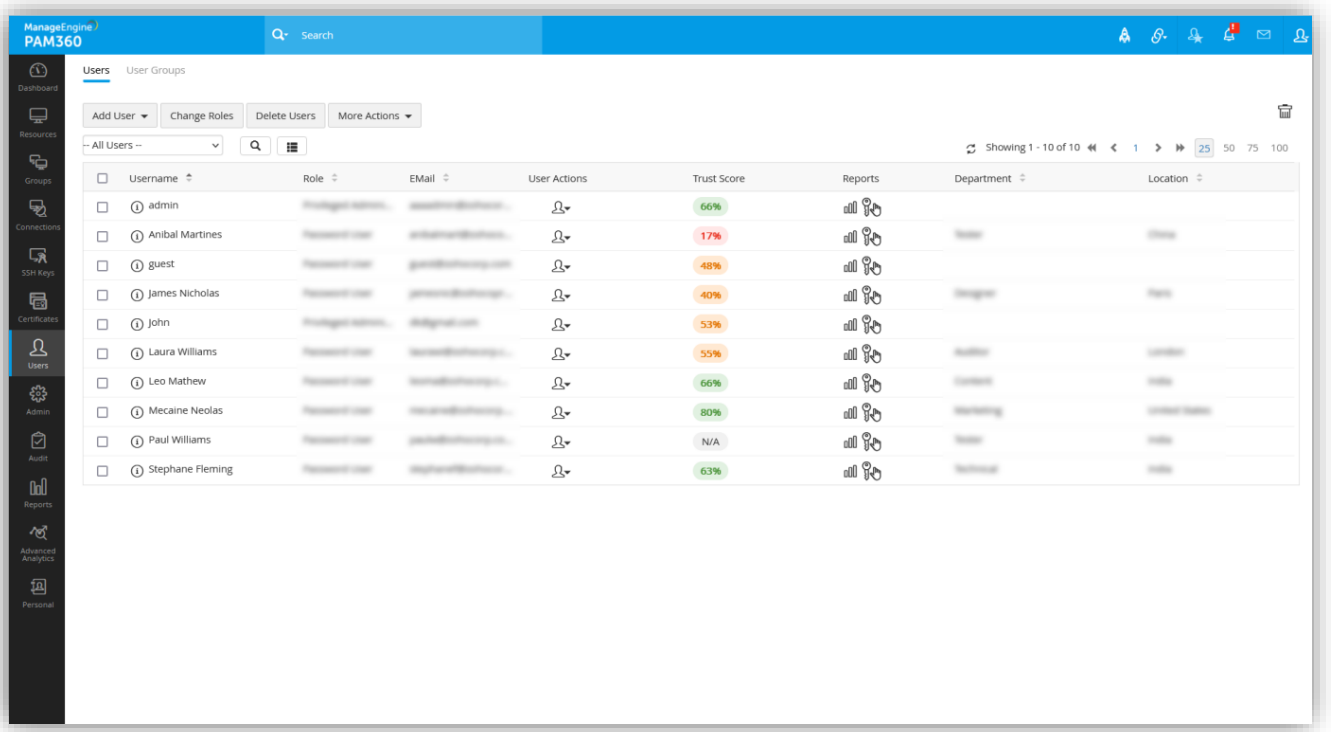
4.1 Trust Score Details and Usage

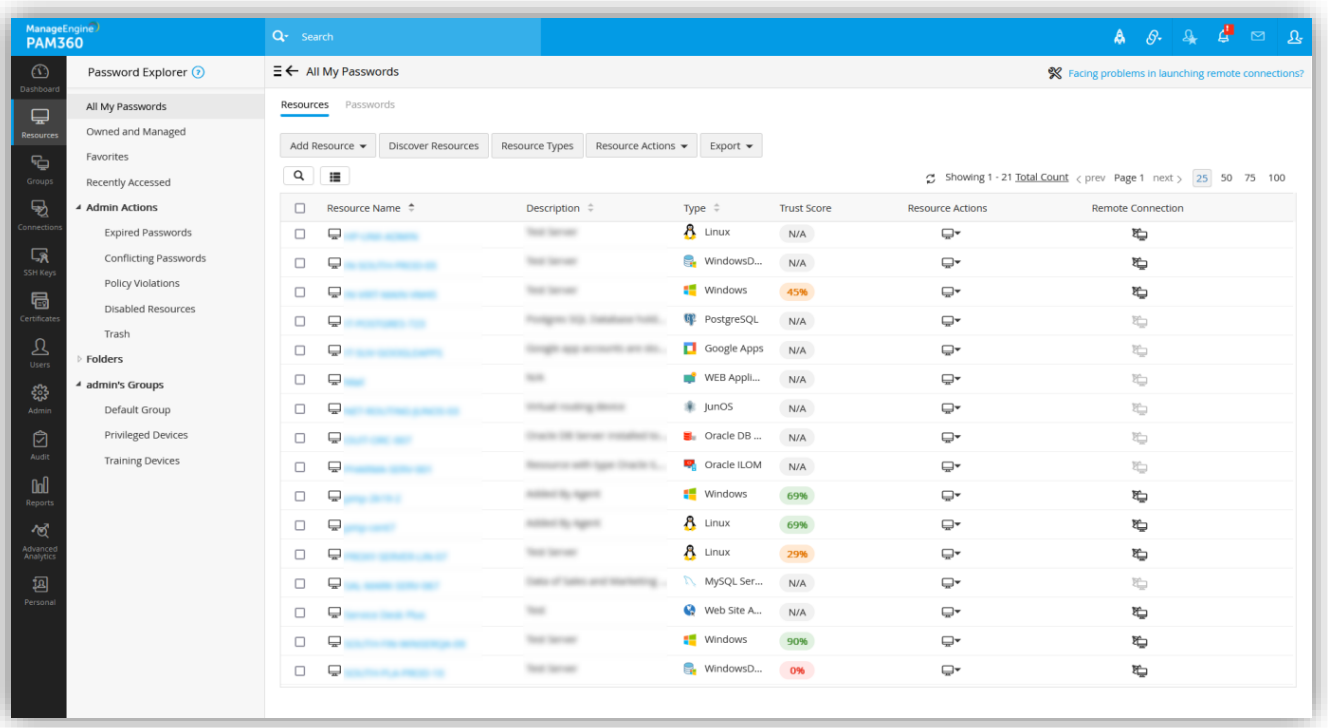
Once you have configured the above sections 2 - 4, you can see the real-time trust scores of the users and the resources in the Users and the Resources tabs based on user authentication and user device and resource activities.

Note:

Even-though without any above configurations, the user trust score will be shown in the PAM360 GUI based on the following conditions that are defined on zero trust upgrade/installation.

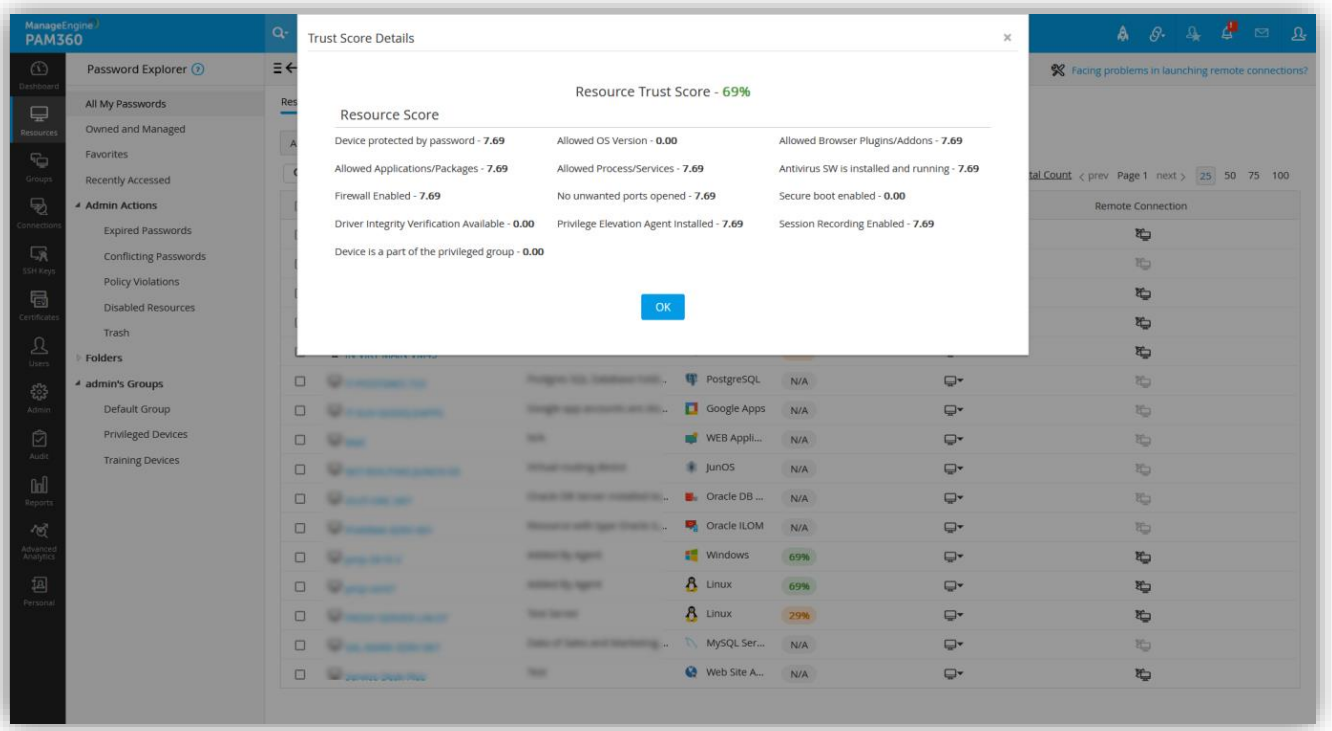
1. Invalid Sign-In Attempts - **3 attempts in 7 days.**
2. Non-Office Hour Sign-In - **09:00 - 18:00**
3. Enabled Two-Factor Authentication.
4. Password Protected Device.
5. Session Recording Enabled.
6. Privileged Elevation Agent installed.





When the user authentication, user device, and resource data fetched meet the conditional and predefined parametric values, the user/resource trust score will be increased based on the configured parameter weightage value. Vise versa, if any of the parameters do not meet the conditional or predefined parameters, the user/resource trust score will decrease based on the fixed weightage values for those parameters.

Click on the respective trust score value to see the configured parameter scores in detail. The parameter configured for the user/resource will be shown here with the score based on the weightage assigned to them.

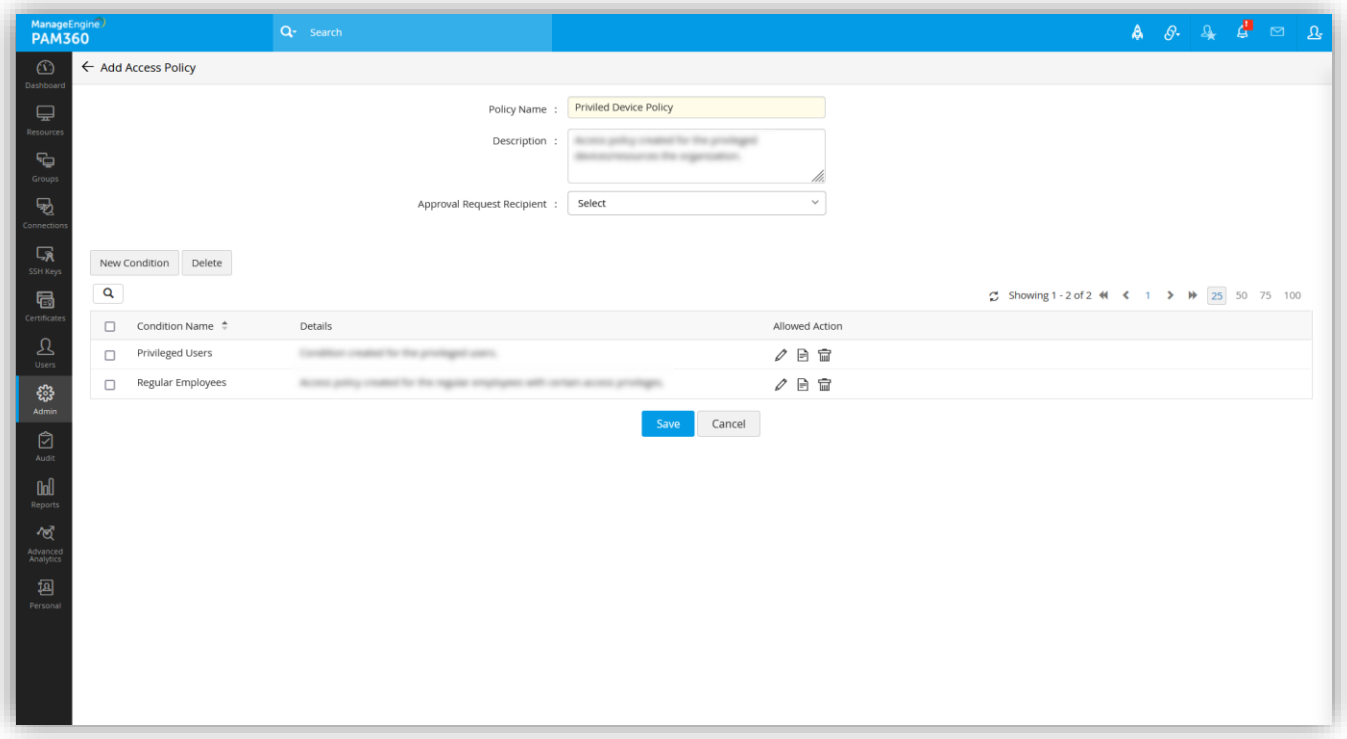


Based on the available trust scores, you can determine the credibility of the resources and the users. If you wish to scrutinize the access privileges and resource governance in a policy-based manner, you can proceed with further access policy configurations that automate the process with a policy-based trust score mechanism.

5. Zero Trust Access Policies

Once you have finished setting up the trust score parameters and the trust score weightage, you can create access policies by which the policy-based access method will be implemented in your organization with the help of generated trust scores. You can create fine-grained dynamic access policies based on your organization's needs and requirements, on which users will be given access privileges to the respective resources.

Navigate to '**Admin >> Zero Trust >> Access Policy**' to create new access policies with desired conditions concerning your requirements. Every access policy created for this zero trust approach is to be approved by another administrator of the organization to check for valid access policy conditions towards the users and the resources.



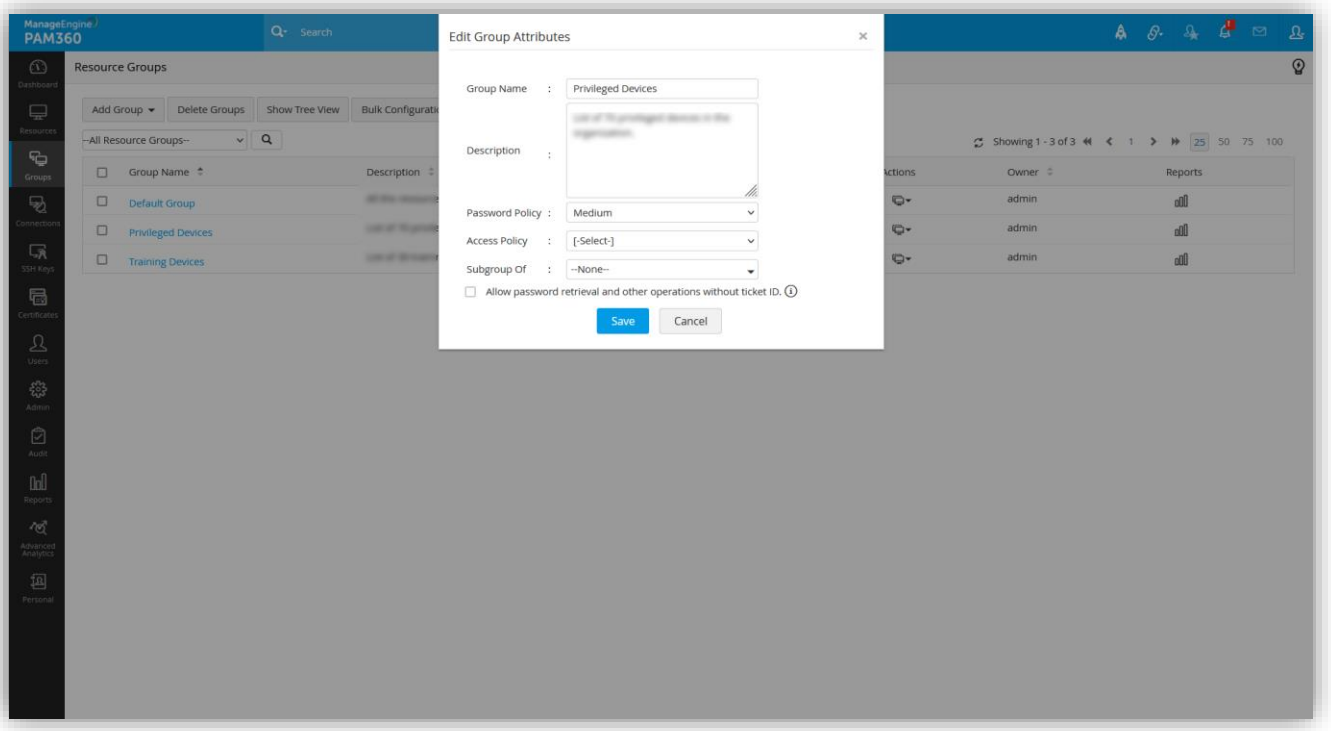
To learn more about creating access policies with various conditions and their limitations, refer to this help document.

6. Associating Access Policies to Resource Groups

Zero Trust is an automated policy-based access privilege approach based on the derived trust scores of the users and the resources. For this approach to work, the users and the resources have to be associated with an access policy with the required set of grant or deny conditions. While configuring the conditions in the access policy, the users will be associated with it using the **Applies To** option. For the users to opt for further privileges and connections using the Zero Trust approach, the configured access policies must be associated with the resources via static resource groups. To do this:

1. Navigate to the **Groups** tab.
2. Click on the **Actions** icon beside the respective static resource group.
3. Select the option **Edit Group Attributes**.
4. In the pop-up that appears, select the respective access policy in the **Access Policy** field that is to be associated with the resource group.
5. Click **Save** to apply the changes.

6. You can also associate an access policy for the resources when you are creating a new resource group post-configuration of access policies.



Now your organization is implemented with the Zero Trust approach for granting access privileges, remote connections, and elevated privileges to users. Under this approach, whenever a user requests access, their trust score is evaluated alongside the trust score of the resource they seek to access. The access policy conditions that have been configured are then used to determine whether the user is permitted access or not. If all the criteria in the access policy are satisfied, the user is permitted the access they require. However, if any of the access policy criteria fail, the system will either audit, issue a warning, request a reason, or deny the user access request, depending on the configuration of the access policy.

Note:

If an existing access policy is modified and in a pending approval/suspended state, then the access policy with the conditions that exist before the modification will be active in the respective resource groups.

Refer to this help document for real-time Zero Trust implementation process in an organization.

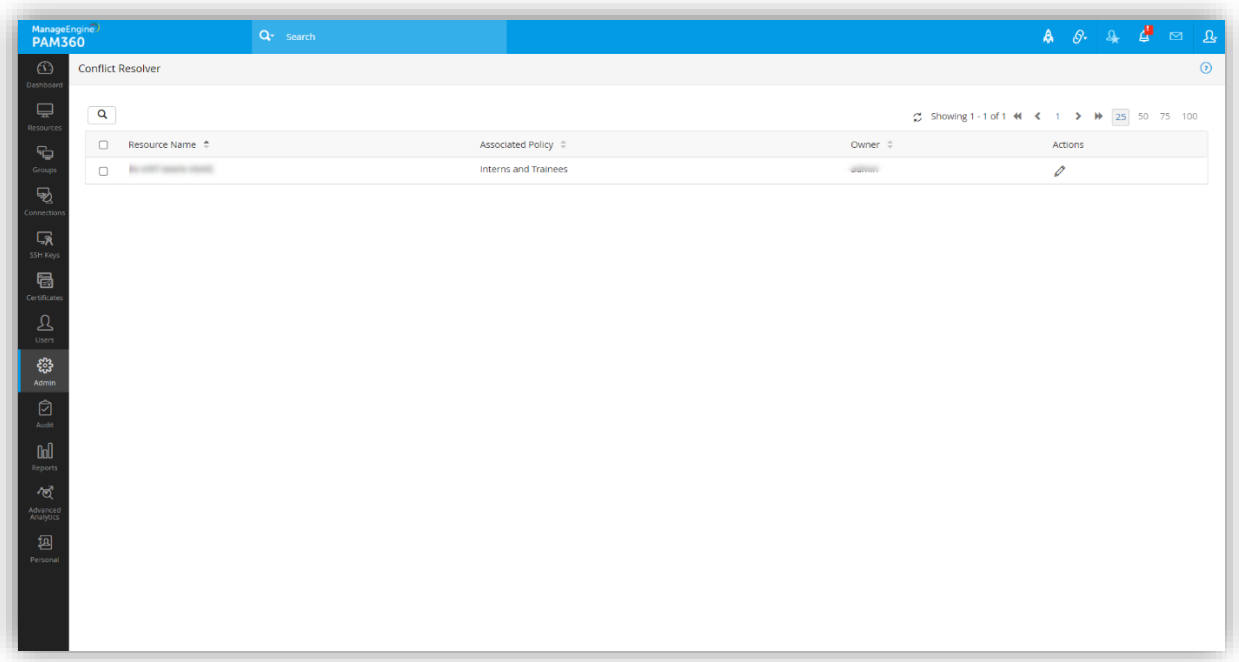
7. Resolving Conflict between Access Policies

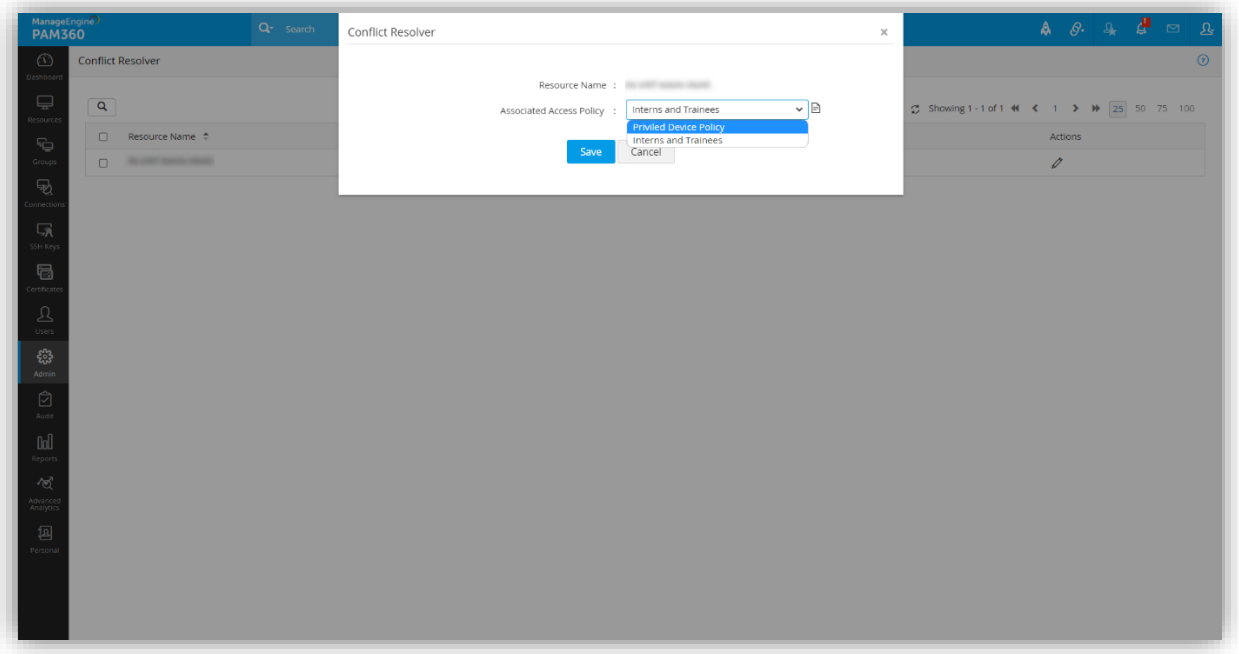
In the Zero Trust approach, when a resource is present in multiple static resource groups, and each of the resource groups is associated with different Zero Trust access policies, there will be a conflict between the access policies of that resource. **Admin >> Zero Trust >> Conflict Resolver** page will show all the available access policy conflicts on the resources in the Zero Trust configuration.

Consider a resource '**pam-server-1**' grouped in static resource groups '**Privileged Devices**' and '**Shared Devices**'. At first, the resource group '**Privileged Devices**' was associated with an access policy '**Regular Employees**', and later the '**Shared Device**' was associated with an access policy '**Contractual Employees**'.

In above such cases, the access policy for a resource will always be applied based on the most recent resource group mapping. So, the resource '**pam-server-1**' will be applied with the access policy '**Contractual Employees**' configured via the resource group '**Shared Device**'. If you want to change the access policy of a resource back to any other access policy, do the steps that follow:

1. Navigate to '**Admin >> Zero Trust >> Conflict Resolver**'.
2. Click on the **Actions** icon beside the respective resource for which you want to change the access policy from the recently applied one.
3. In the pop-up that appears, select the desired access policy in the **Associated Access Policy** field.
4. Click the document icon beside the **Associated Access Policy** field to see the access policy criteria in detail.
5. Click **Save** to apply the respective access policy to the resource.





8. Limitations in Policy-Based Access Privilege Functionality

1. When multiple users share a device in an organization, we recommend configuring user authentication parameters solely for the device. Because on a user device shared with multiple users, any device-related unauthenticated operation performed by a user will lead the user device to restrict access for all other users.
2. The designated approver for the access policy must review and approve it, as approval cannot be delegated to other administrators.

3. The access policy is not applicable for mobile applications, browser add-ons, and REST API users, and any activities performed through them will not affect the trust score of the user and resource.
4. Access policy conditions are now limited to static resource groups only.
5. User authentication parameters are calculated from the PAM360 audits; if the audit data is purged, the user authentication could be impacted based on fixed parameter weightage.
6. The allow access privilege is currently supported for the primary landing server.
7. The resource trust score validation will be bypassed for currently logged-in AD/LDAP and Azure accounts.
8. A user can attain VNC and SFTP connections irrespective of the access policy configured for a resource.
9. Our access policy condition now only permits the allowed access for password reset and not for key rotation.

Configuring Trust Score Parameters for Zero Trust Approach

The Zero Trust methodology here employs micro-segmentation and behavioural analytics to calculate a trust score for users and resources based on predetermined parameters. To access resources configured with policy-based access control, users must met multiple conditional parameters defined by administrators or users with custom access policy roles. This documentation provides a detailed explanation of the trust score parameters and their implementation within the policy-based access approach.

PAM360 utilizes a total of nineteen conditional and predefined parameters to determine the users' and resources' trust scores. These parameters are divided into two categories, one for users and the other for resources, and have been assigned weightage to calculate the respective user and resource trust score. Based on these parameters and their assigned weightage, PAM360 calculates the trust score for both users and resources.

User Trust Score Parameters

Conditional Parameters to be Defined by the Administrator	
Authentication	**Device**
Invalid Sign-In Attempts	Allowed OS Version
Non-Office Hours Sign-In	Allowed Open Ports
Access from Allowed IPs	Allowed Browser Plugins/Addons
Access from Allowed Devices	Allowed Applications/Packages
User Belongs to Privileged Group	Allowed Processes/Services

Predefined Parameters Based on Default Device Data	
Authentication	**Device**
Two-Factor Authentication	Password Protected Device
	Active Antivirus Software
	Firewall Enabled
	Secure Boot Enabled
	Driver Integrity Verification Available

Resource Trust Score Parameters

Conditional Parameters to be Defined by the Administrator
Allowed OS Version
Allowed Open Ports
Allowed Browser Plugins/Addons
Allowed Applications/Packages
Allowed Process/Services
Resource Belongs to Privileged Group

Predefined Parameters Based on Default Application/Device Data
Password Protected Device
Active Antivirus Software
Firewall Enabled
Secure Boot Enabled
Driver Integrity Verification Available
Session Recording Enabled
Privilege Elevation Agent Installed

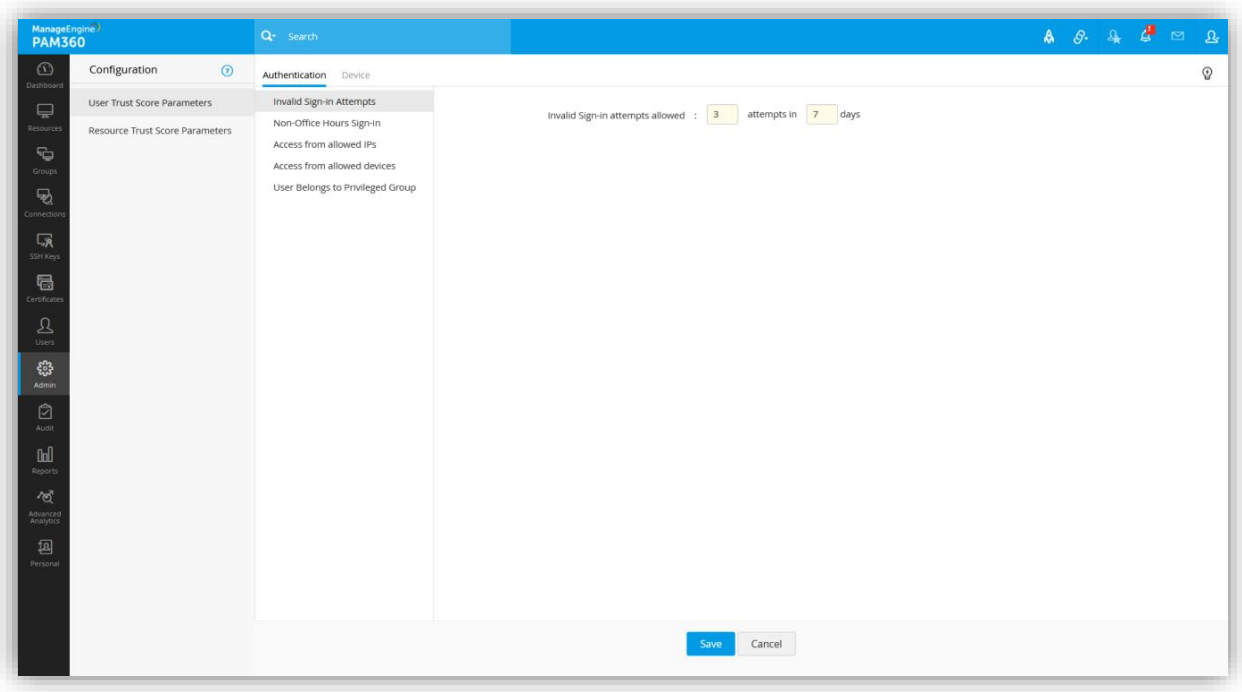
1. Conditional Parameters to be Defined by the Administrator

Navigate to **Admin >> Zero Trust >> Configuration** to define the conditional parameters' baseline values for the user (user authentication + user device) and resource trust score calculation.

a. User Authentication Parameters

i. **Invalid Sign-In Attempts** - Here you can define the allowed number of unsuccessful login attempts per defined day a user can make.
E.g., Invalid Sign-in attempts allowed: **3** attempts in **7** days.
In case a user has attempted to sign in more than three times with incorrect credentials, they fail to fulfill the specified condition. Consequently, this parameter will be assigned a score of 0 in the user trust score calculation, regardless of its weightage assigned.

The following parameters work similarly for the respective trust score calculation.



ii. **Non-Office Hour Sign-In** - This parameter defines the user login to the PAM360 application during the specified working hours. By default, the working hours will be from **09:00 - 18:00** for all the PAM360 users.

If you want to change this parameter value diversely for different users, do the steps that follow:

1. Click the **Add Sign-In** button.
2. In the pop-up that opens, select the respective user group to whom the working hours are to be changed.
3. Enter the Sign-In hours as per the organization's requirement, select **Enable** and click **Save**.
4. If you select **Disable**, the default Sign-In hours **09:00 - 18:00** will be applicable for those users.

Note:

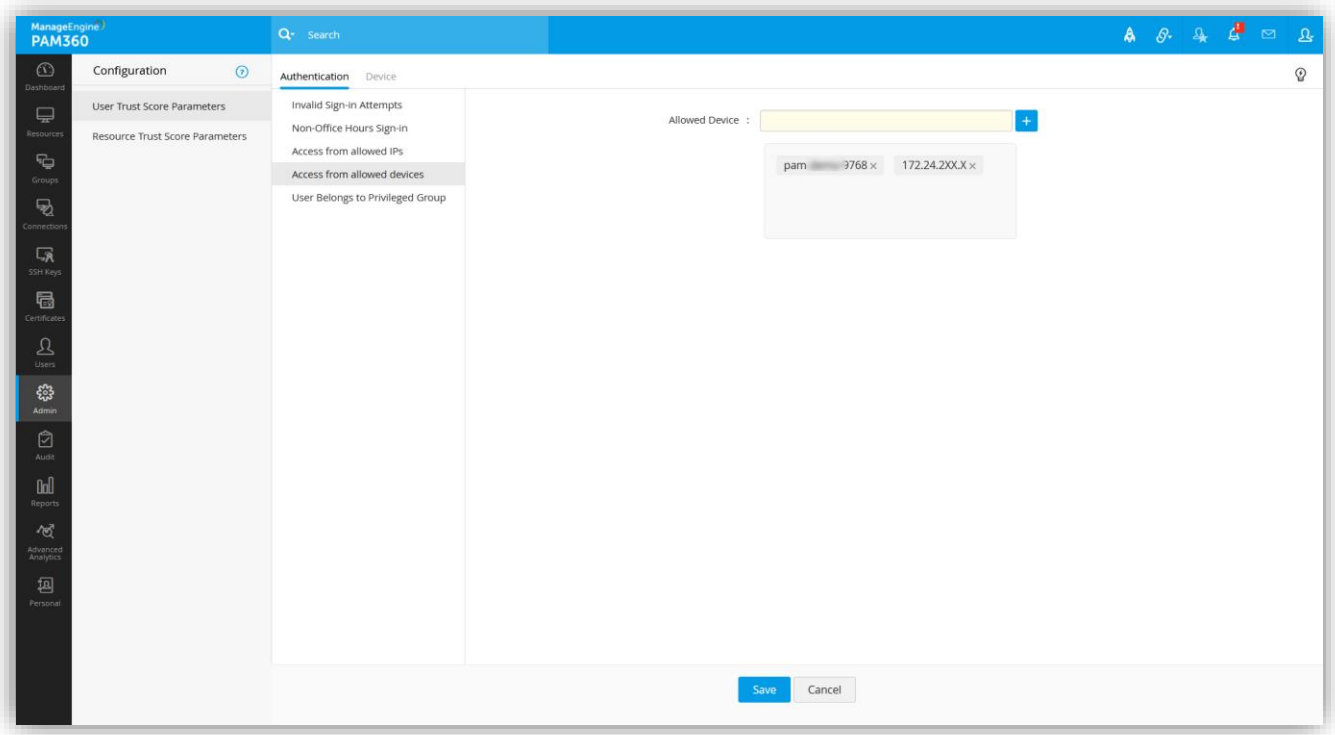
Ensure to set the sign-in hours as per your device time conversion with the PAM360 configured server time. If you fail to set the correct sign-in hours as per your PAM360 server's time conversion, it might result in a reduced trust score with a score value of 0 for this parameter.

E.g., PAM360 server time - 5:00 (US) | User-machine time - 10:00 (UK).

The work shift of the user in the UK is 10:00 - 17:00. Then the Sign-In hours set here should be 5:00 - 12:00.

iii. **Accessing from Allowed IPs** - Here you can define the allowed users' IP addresses in the range that accesses the PAM360 application.
E.g., Access from Allowed IP: **172.24.2XX.X** to **172.24.2YY.Y**.
If a user presents in the above IP range and accesses the PAM360 application, the parametric condition will be met, and the parameter score will be added to the overall user trust score. Non-compliance with this parameter will lead the parameter score to 0, irrespective of the assigned parameter weightage in the trust score page.

iv. **Accessing from Allowed Devices** - Similar to the allowed IP parameter, here you can define the IP addresses or the device names that are allowed to access the PAM360 application authorized by the organization. E.g., Allowed Device: **pam-server3592**.



Note: If you need to monitor limited allowed machines or a machine that is different from the above-provided IP range, you can use this parameter with the respective IP addresses or the device names.

v. **User Belongs to Privileged Group** - In this parameter, you can add the user group with the users who are part of the privileged group in an organization. The users present in the added user group will have an added advantage of an additional user trust score without any condition and just being considered a privileged user.

b. User Device/Resource Parameters

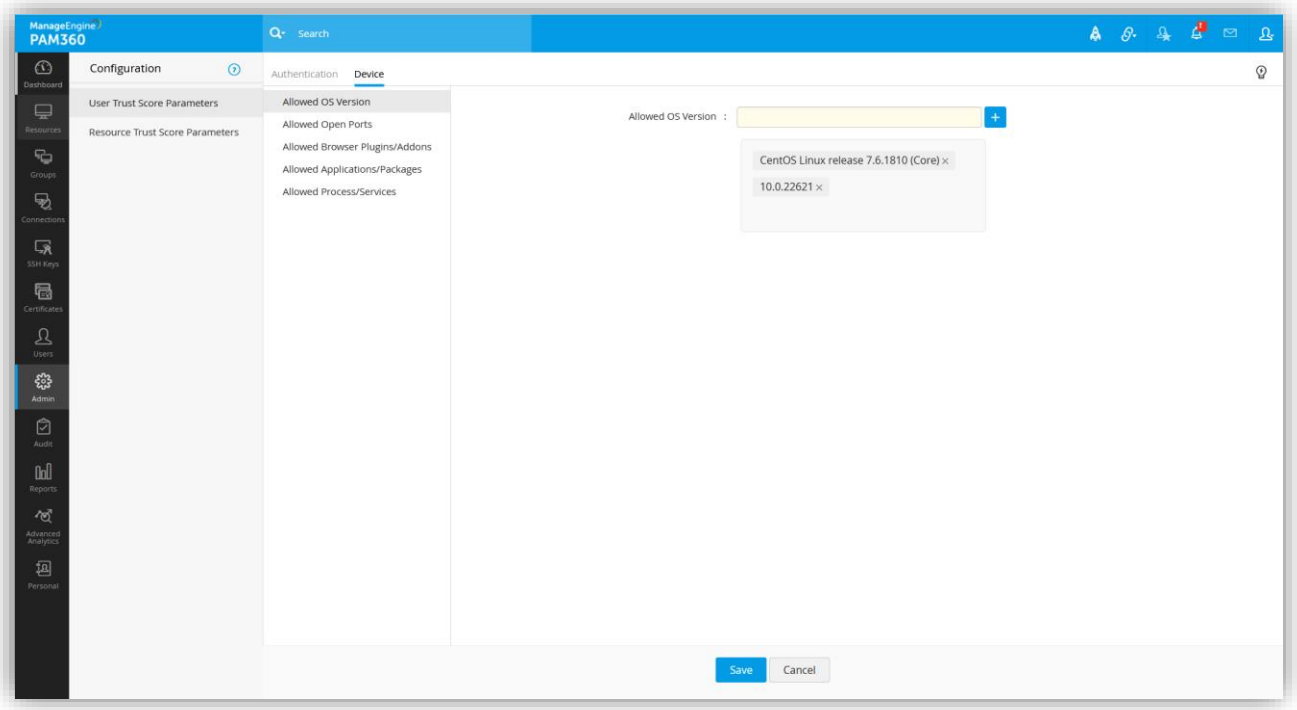
By default, all the devices/resources in an organization will be configured with a set of open ports, browser plugins/add-ons, applications/packages, and processes and services. To find out the respective details from a device/resource in an organization and to enter those in a specific acceptable format in the below parameters section, do the steps that follow:

1. Download this zip file and extract it to any of the desired devices.
2. Open the respective folder **Windows** or **Linux** based on your Operating System (OS) where you have extracted the zip.

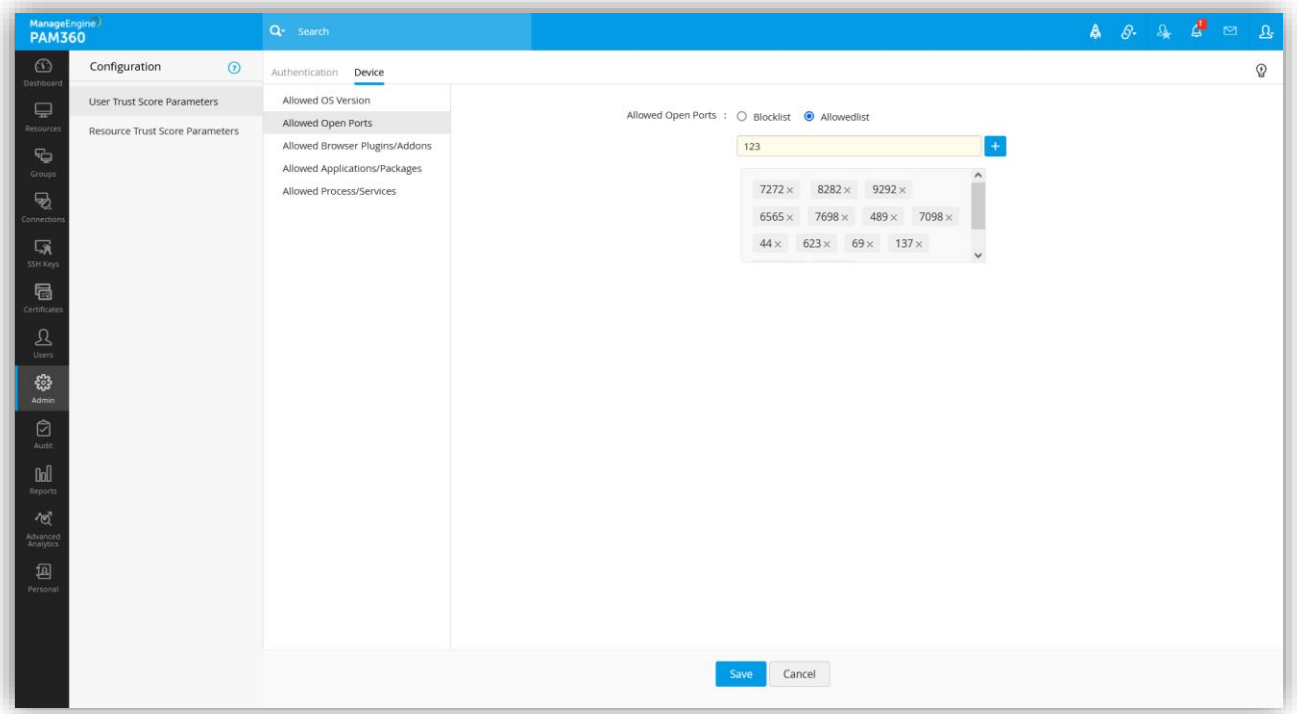
3. Execute the bash/ sh/ bat/ ps1 file '**fetch_configuration_details**' with the run as administrator privilege.
4. Upon execution, an output file with the name '**query_result.txt**' is generated in the same folder location.
5. Open the **query_result.txt** file to check for the default device data or system properties for defining the respective score parameter. Use the search option to search the value of the respective parameter with the relevant below ids:
   a. Antivirus_status
   b. Application_and_packages
   c. Chrome_extensions
   d. Disk_encryption_status
   e. Firefox_addons
   f. Firewall_status
   g. OS_version
   h. Open_ports
   i. Process_and_services
   j. Secure_boot_status

Note: The parameters received through the output file are the default set of open ports, browser plugins/add-ons, applications/packages and processes and services configured for the device/resource. You can use these parameters to define the below conditional values.

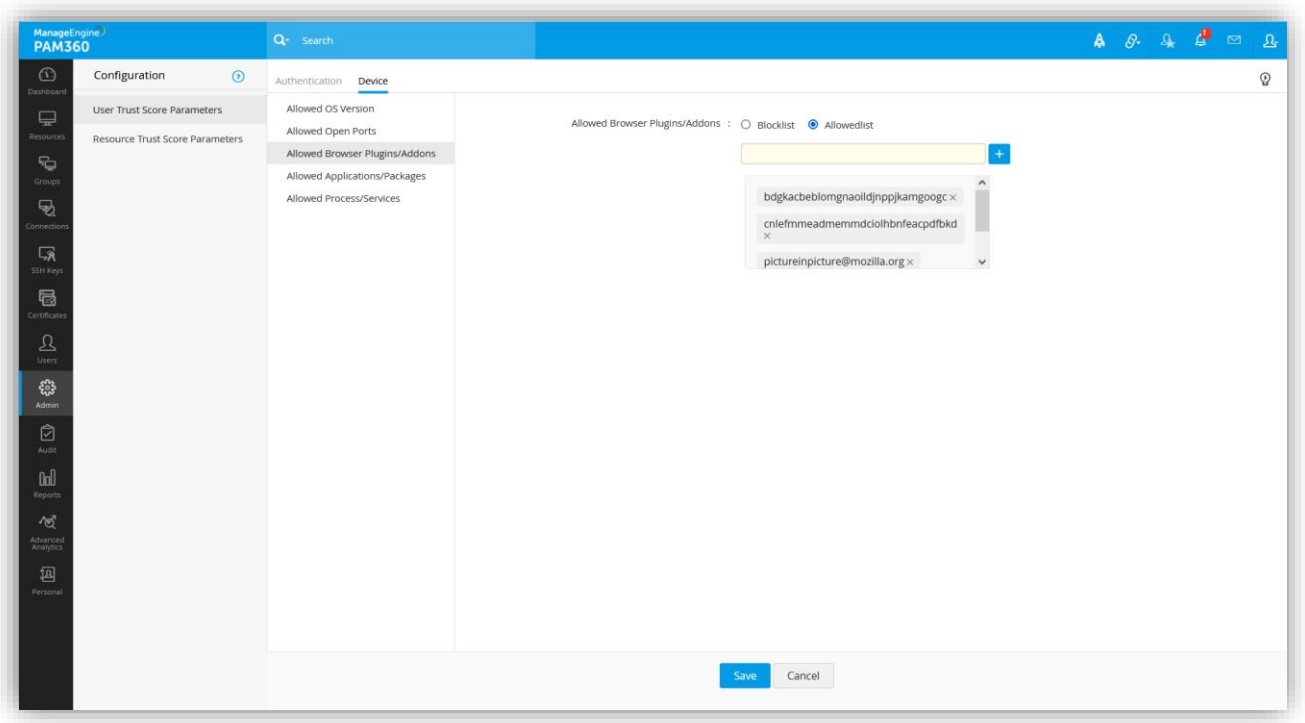
i. **Allowed OS Version** - Here you can define the OS version that is allowed to be used by your organization's users. If a logged-in device/resource deviates from the list of the predefined OS version, it will impact the respective trust score irrespective of the trust score weightage.
E.g., 10.0.22621



ii. **Allowed Open Ports** - Here you can specify the ports that PAM360 users are allowed to access within this field. Users can provide a list of allowed or blocked ports, and if a user tries to access a port that is block-listed or not included in the allowed list, their trust score will be reduced based on the weightage given to this parameter.
E.g., 8282, 7272, 9292, 6565

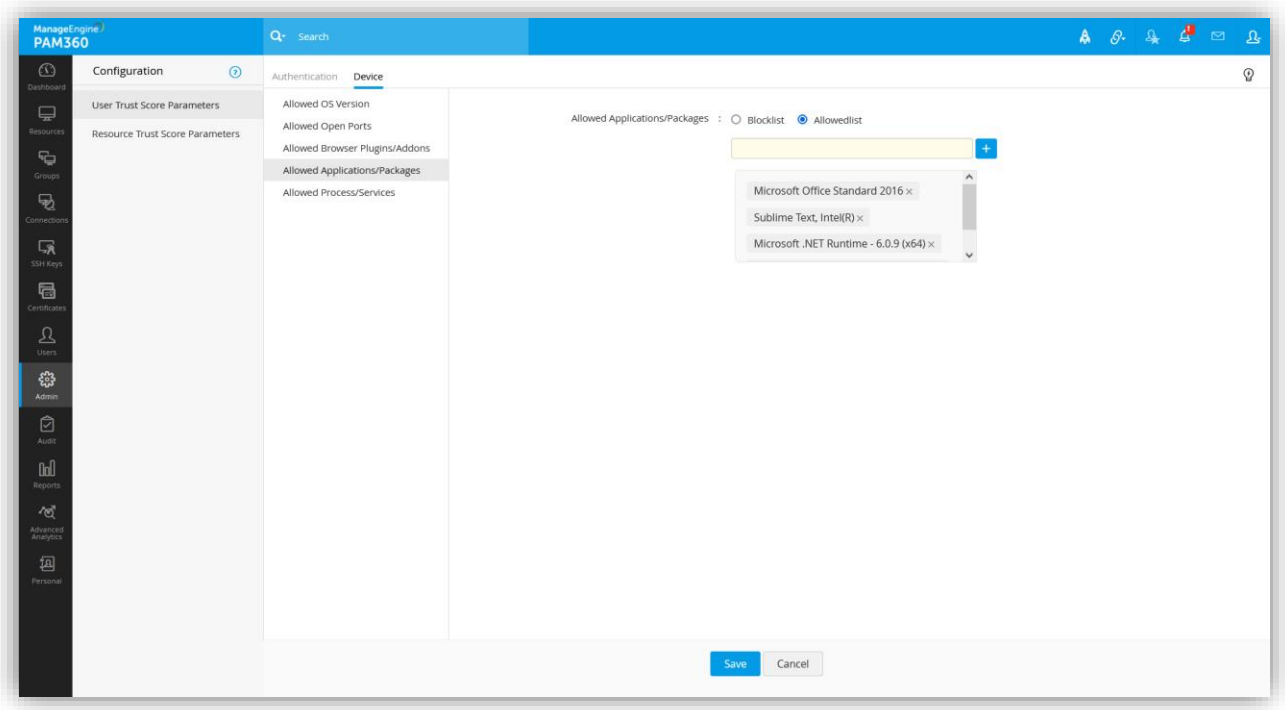


iii. **Allowed Browser Plugins/Addons** - Using this parameter you can define the allowed browser plugins/add-ons to be used by the users who are going to be the part of policy-based access control method. Based on your organization's favorable, you can use the blocked/allowed list methods to list the plugins and add-ons.
E.g., bdgkacbeblomgnaoildjnppjkamgoogc, pictureinpicture@mozilla.org, firefox-compact-light@mozilla.org



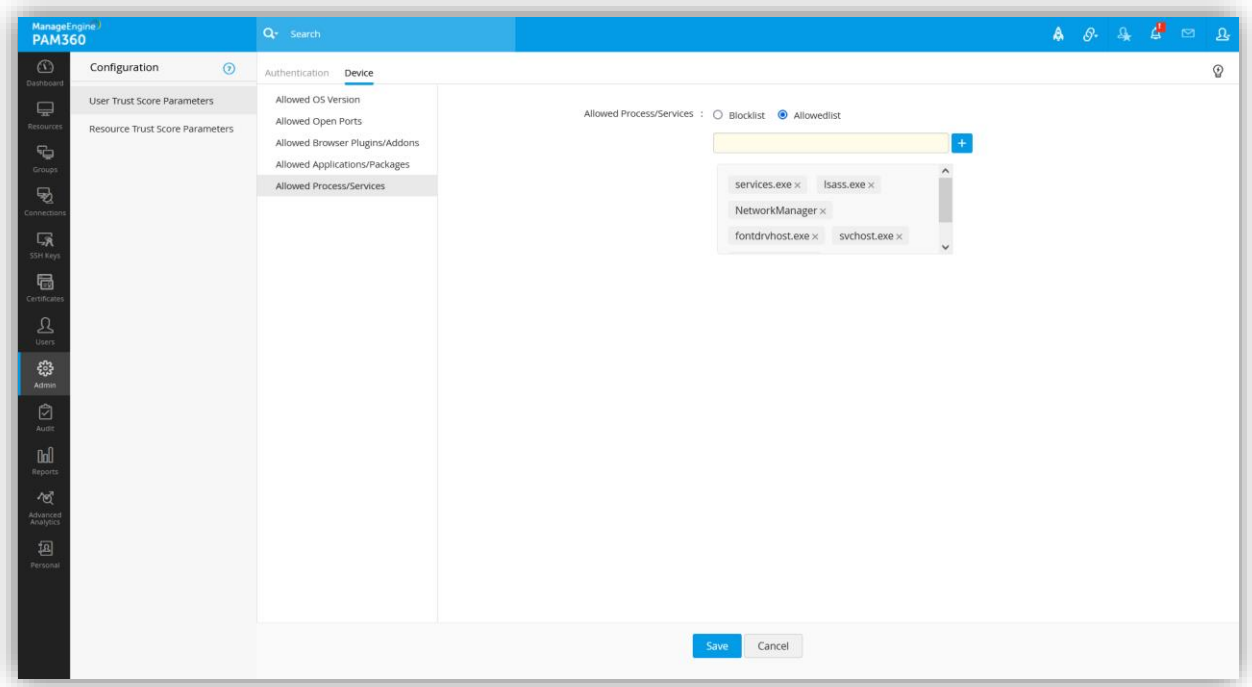
Note: The allowed/blocked browser plugins/add-ons are only applicable to the web browsers **Chrome** and **Firefox**.

iv. **Allowed Applications/Packages** - Here you can define the applications/packages that are allowed to be installed and used in the user devices/resources. This can be accomplished by either providing a list of allowed or blocked applications/packages. Based on the installed applications and packages, the respective trust score will vary upon the provided weightage to this parameter.
E.g., Microsoft Office Standard 2016, Sublime Text, Intel(R) Wireless Manageability Driver, Microsoft .NET Runtime - 6.0.9 (x64)



v. **Allowed Processes/Services** - In this parameter, you can specify the processes/services that are permitted to run on the users' devices or resources. This can be attained by creating a list of allowed or restricted processes/services. The trust score for the respective user device/ resource parameter will be adjusted based on the processes/services that are running.

E.g., services.exe, lsass.exe, NetworkManager



vi. **Privileged Resource Group** (Resource Parameter) - In this parameter, you can add the resource group with the resources that are part of the privileged devices in an organization. The resources present in the added resource group will have an added advantage of an additional resource trust score without any condition and just being present in the privileged device group.

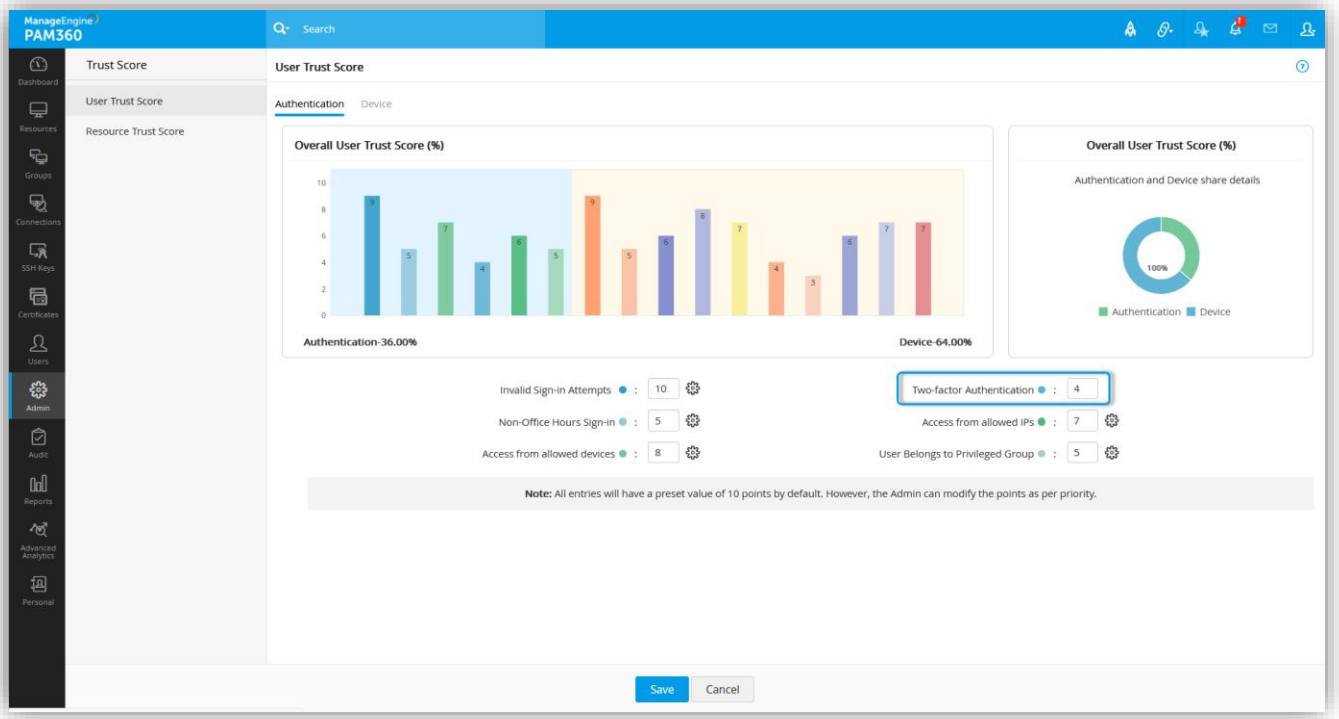
Notes:

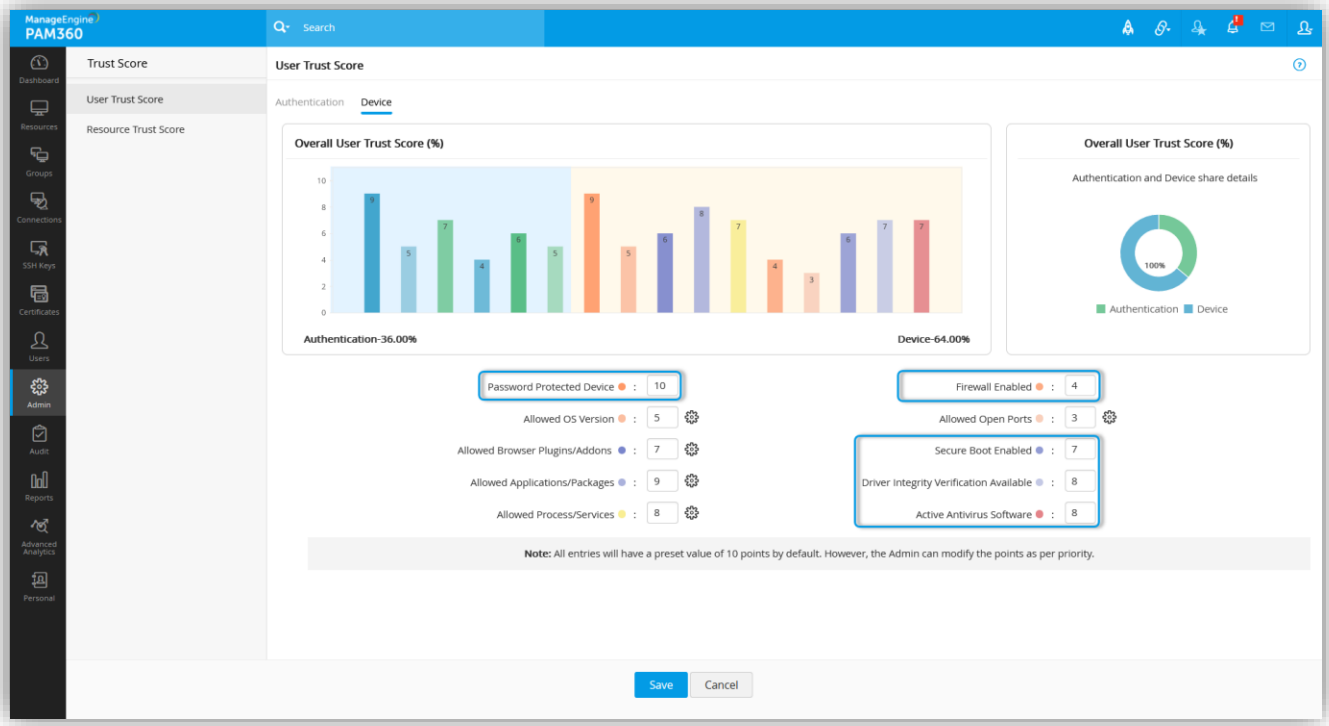
i. For the parameters that contain allowed and blocked lists, you should provide valid input values. An empty parameter with a given weightage in the Trust Score page will consider the parameter as met for the respective trust score calculation.

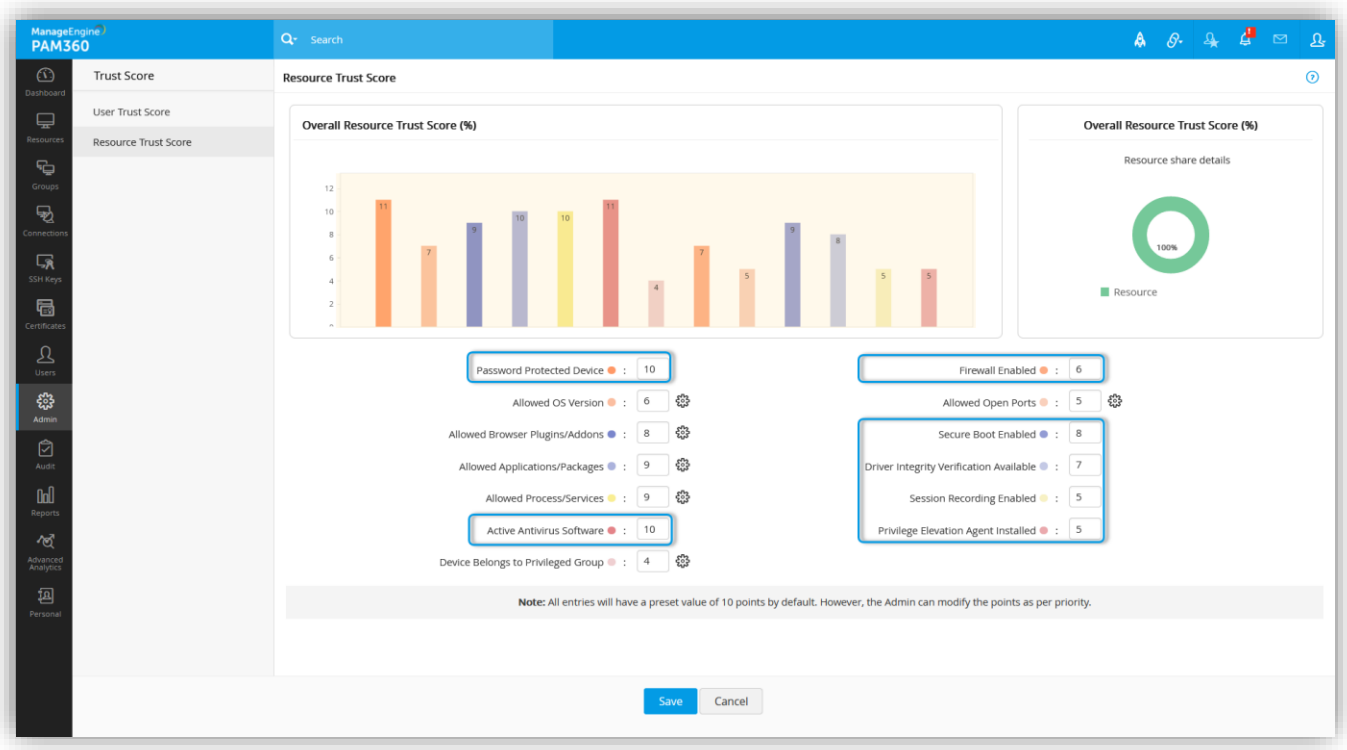
ii. The characters entered in the parameter allowed list and the blocked list are case-sensitive.

2. Predefined Parameters

Below are the parameters that cannot be configured or defined by the administrator. They are from predefined application/system properties. You can add a weightage for those properties on the Trust Score page for the trust score calculation as per your organization's needs and requirements. If you consider any of these parameters to be unchecked for the trust score calculation, enter a value of 0 in the Trust score weightage section else, you can provide a value of 1-10 based on your organization's importance over the parameter.


ManageEngine
PAM360
Search
Trust Score
User Trust Score
Resource Trust Score
User Trust Score
Authentication
Device
Overall User Trust Score (%)
Authentication-36.00%
Device-64.00%
Overall User Trust Score (%)
Authentication and Device share details
100%
Authentication
Device
Invalid Sign-in Attempts : 10
Non-Office Hours Sign-in : 5
Access from allowed devices : 8
Two-factor Authentication : 4
Access from allowed IPs : 7
User Belongs to Privileged Group : 5
Note: All entries will have a preset value of 10 points by default. However, the Admin can modify the points as per priority.
Save
Cancel


ManageEngine
PAM360
Search
Trust Score
User Trust Score
Resource Trust Score
User Trust Score
Authentication
Device
Overall User Trust Score (%)
Authentication-36.00%
Device-64.00%
Overall User Trust Score (%)
Authentication and Device share details
100%
Authentication
Device
Password Protected Device : 10
Allowed OS Version : 5
Allowed Browser Plugins/Addons : 7
Allowed Applications/Packages : 9
Allowed Process/Services : 8
Firewall Enabled : 4
Allowed Open Ports : 3
Secure Boot Enabled : 7
Driver Integrity Verification Available : 8
Active Antivirus Software : 8
Note: All entries will have a preset value of 10 points by default. However, the Admin can modify the points as per priority.
Save
Cancel



i. **Two-Factor Authentication** (Only for User Authentication) - Two-Factor Authentication (2FA) mentioned here represents the one used in the PAM360 for an additional way of identity. This 2FA parameter will act as an added score point for the user where the TFA is mandated for PAM360 login with a configured weightage value.

Note: We recommend you always enable the 2FA in PAM360 for an added layer of identity verification for greater security reasons.

ii. **Device Protected by Password** - This parameter verifies if the user's device or resource has password protection. If password protection is detected, the relevant score will be calculated based on its assigned weightage. If password protection is not detected, the score for this parameter will be zero, regardless of its assigned weightage.

iii. **Antivirus SW is Installed and Running** - This parameter evaluates whether an antivirus program is installed and active on the user's device or resource. If an antivirus program is present and operational, it will contribute towards the score calculation. Conversely, the absence of an antivirus program will result in a reduced parameter score, which will impact the overall trust score accordingly. At this early stage of Zero Trust release, PAM360 has the capability to evaluate only a specific set of antivirus that is deployed in

the resources/user machines. If your antivirus is not in the below-mentioned list, it is recommended to enter the weightage value as '0' to avoid unnecessary score reduction.

a. Microsoft Defender
b. Avast
c. AVG
d. Bitdefender
e. Kaspersky
f. McAfee
g. Sophos
h. Symantec
i. Trend Micro

iv. **Firewall Enabled** - This parameter examines whether a firewall is active on the user's device or resource. If a firewall is detected, the parameter will be considered for score calculation toward the final trust score value. Conversely, if no firewall is detected on the user's configured device or resource, the parameter will not be considered and will result in a parameter score of zero, regardless of its assigned weightage.

v. **Secure Boot Enabled** - The secure boot feature is to block the loading of malicious applications during device or resource startup. This particular parameter assesses the Secure Boot system summary status. If it is turned on, the parameter's score will be considered and added to the final trust score calculation. However, if the Secure Boot system summary status is changed to off on any user device or resource under the policy-based access control, the parameter will fail and receive a parameter score of zero, irrespective of its assigned weightage.

vi. **Device Integrity Verification Available** - The integrity verification feature in operating systems examines the system files and drivers for malicious or corrupted applications. If the user's device or resource has this feature available, the parameter will be considered as met, and the assigned weightage score will be added to the final trust score calculation.

Note: If you have any uncertainty over the status of the above parameters in any of the resources or user machines, you can perform the above steps in the respective user device/resources to check for the parameter status.

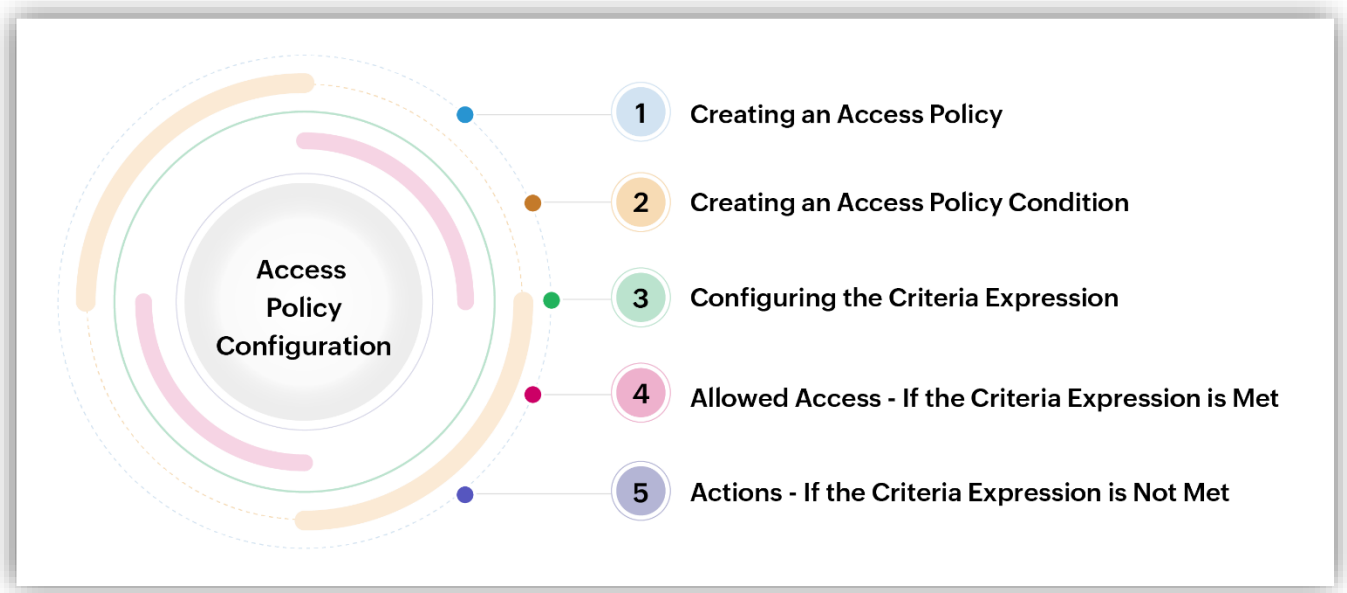
vii. **Session Recording Enabled** (Only for Resource Trust Score) - This parameter represents the one that is enabled for the resources in PAM360 to play back the remote sessions. Assigning a weightage to this parameter will check for the configured resources for the session recording feature. If the session recording is enabled for the accounts of the resource, the parameter score will be added to the overall resource trust score.

Note: This parameter will be met for the resource trust score calculation only when all the accounts in a resource have the enabled session recording in PAM360.

viii. **Privilege Elevation Agent Installed** - Assigning a weightage to this parameter acts as an added trust score to the specific resources that are installed with the Self-Service Privilege Elevation module along with the Zero Trust module.

Access Policy Configuration for Zero Trust Approach

Post establishing the trust score parameters and weightage, you can create access policies to implement the policy-based access method in the organization, utilizing the generated user and resource trust scores. These access policies can be tailored to meet the specific needs and requirements of the organization, allowing users to be granted appropriate access privileges to the corresponding resources in a detailed and dynamic manner.



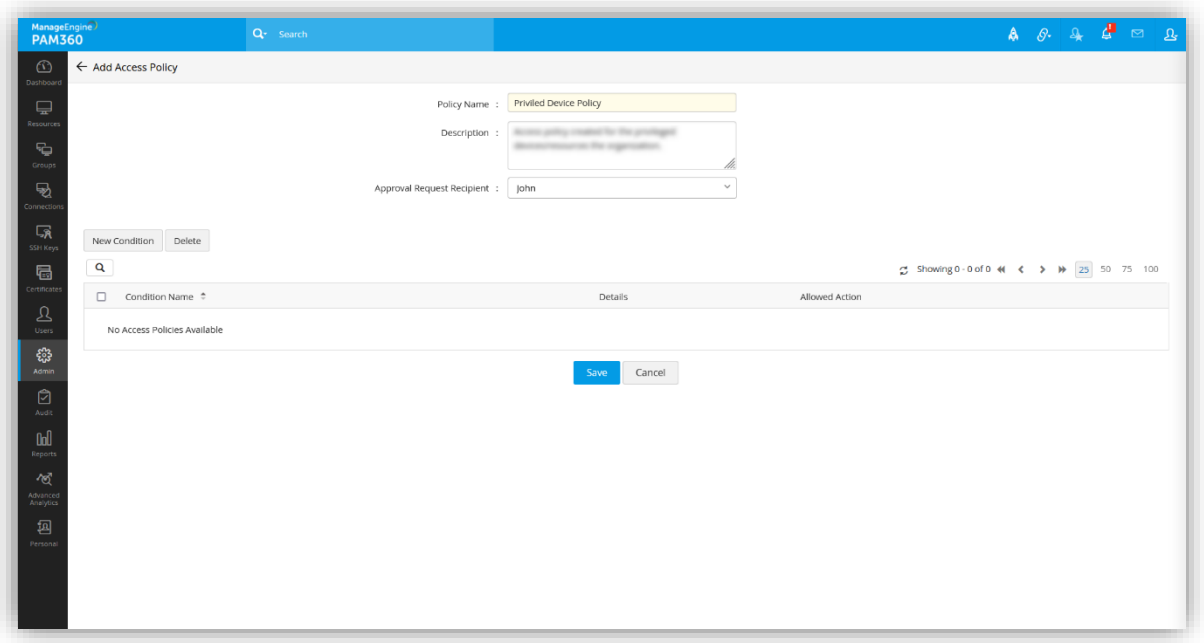
Navigate to '**Admin >> Zero Trust >> Access Policy**' to create the new access policies with desired conditions concerning your requirements. Every access policy created for this zero trust approach is to be approved by another administrator of the organization to check for valid access policy conditions towards the users and the resources.

Note: The access policy created with multiple conditions for a resource does not apply to the owner of the resource except for the condition with **Self-Service Privilege Elevation** access.

1. Creating an Access Policy

To create an access policy for implementing policy-based access privilege, do the steps that follow:

1. Navigate to '**Admin >> Zero Trust >> Access Policy**'.
2. In the page that opens, click **Add** to create an **Access Policy**.
3. On the page that opens:
   a. Enter the **Policy Name** and **Description**.
   b. Select the approver(s) from the **Approval Request Recipient** field who will approve this access policy for further implementation.



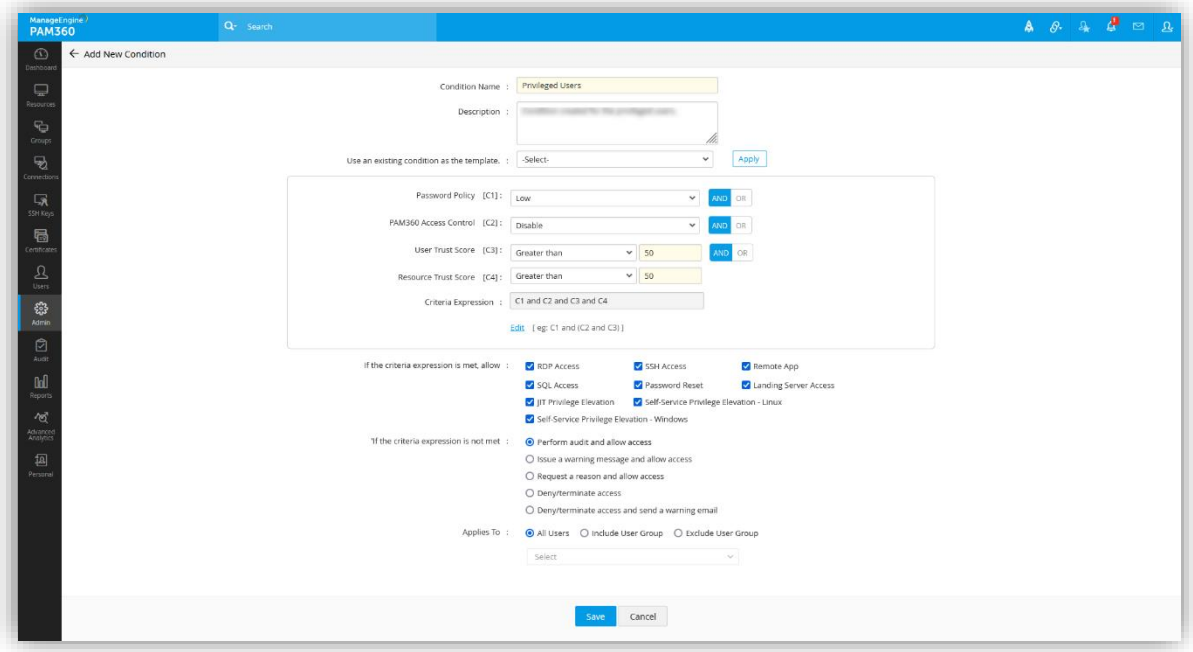
Note: A minimum of one condition is required to create an access policy.

1.a Creating an Access Policy Condition

To create a condition in an access policy, do the steps that follow:

1. Click **New Condition** to create a condition.
2. On the page that opens, fill in the necessary fields that follow:
   a. **Condition Name** - Enter a condition name of your choice.
   b. **Description** - Enter a detailed description of the condition for future reference.
   c. **Use an existing condition as the template** - If you have created conditions previously for any access policies, they will be listed in this field. You can use it from the drop-

down as a template for this new condition.



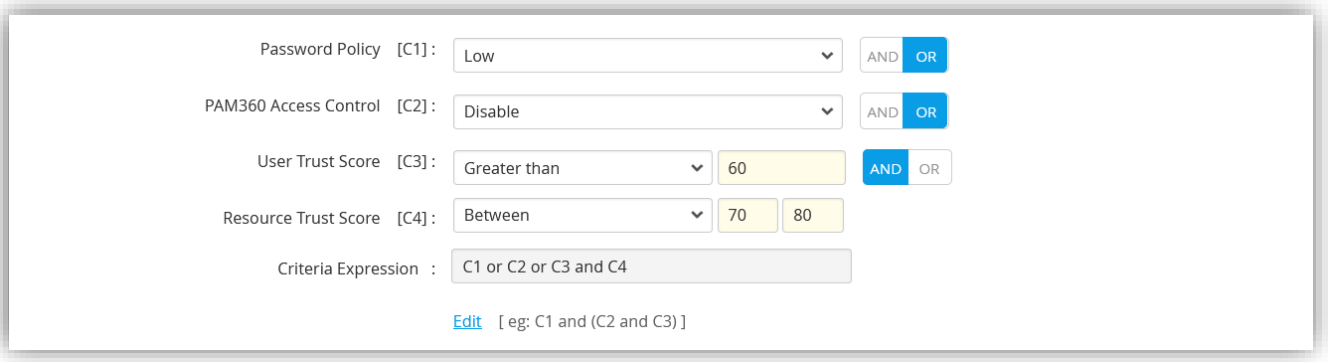
Notes:

i. You can create multiple conditions in an access policy concerning your requirements.

ii. If there are multiple conditions in an access policy, the user/resource should meet all the configured criteria in the conditions of the access policy to get the respective access privileges.

1.b Defining Criteria and Criteria Expression

Now you have to provide the criteria for this access policy condition that have to be met to get further allowed access privileges via this access policy condition:



1. **Password Policy [C1]** - In this field, you can choose the strength of the password policy. The password policy is to ensure the password strength of the accounts to which the access privilege is to be given to the users.

   How does it work?

   If you select the lower strength as criteria C1 and the resource to which this access policy is applied has a higher strength, criteria C1 will be accepted. However, if you choose higher strength and the resource to which this access policy is applied has a lower strength of password policy level, the criteria will not be satisfied.
2. **Password Access Control [C2]** - You can also choose the access control status required for an account or resource to grant access privileges. Access control status for the accounts or resources ensures a controlled level of access by the administrator posts zero trust access policy conditions.

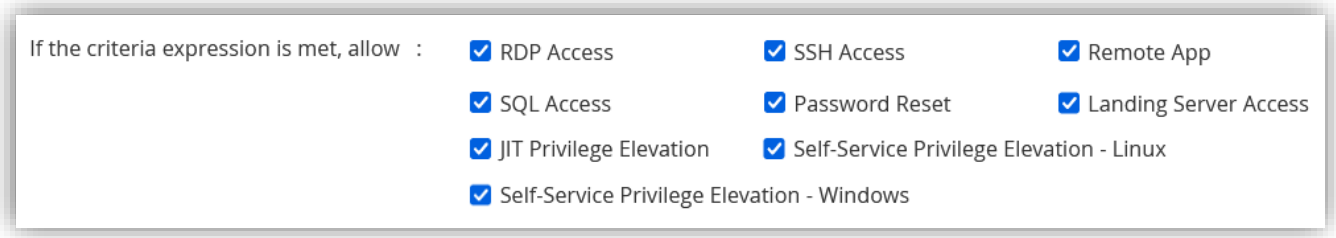
   How does it work?

   If you select **Disable**, the criteria will be considered valid regardless of the access control configuration at the account or resource level where this access policy is implemented. However, if you select **Enable** and the accounts or resources covered by this access policy do not have configured access control, then the criteria will not be satisfied.
3. **User Trust Score [C3]** - Here, you can define the minimum trust score of the user who tries to get access privileges via this access policy. You can either provide a greater-than value or an in-between value as criteria C3.
4. **Resource Trust Score [C4]** - Similar to the user trust score, here you can define the resource trust score of the resources to which the access privilege is given via this access policy. You can either provide a greater-than value or an in-between value as criteria C4.
5. **Criteria Expression** - Using this criteria expression option, you can customize your way of criteria' (C1, C2, C3, and C4) importance in the condition of an access policy. Either you can use the **AND/OR** button to maintain it, or you can use the **Edit** option to set your criteria importance manually. **E.g.,** [C1 or (C2 and C3) or C4]

1.c Allowed Access If the Criteria Expression is Met

You can enable the access privileges here based on the respective users' requirements to which the condition is to be applied. If the above-defined criteria expression is satisfied, the user associated with this condition is given access privileges that you enabled in this condition.

Note: A minimum of one allowed access is required to save the access policy condition.



i. **RDP Access** - Enabling this checkbox will permit users to take RDP sessions to the resources configured under this access policy when they meet the defined criteria expression.

ii. **SSH Access** - This option will permit users to take SSH sessions to the resources configured under this access policy when they meet the defined criteria expression.

> **Note:** Users will be restricted to attain all SSH, Telnet, and Legacy SSH connections when they fail to meet the criteria expression configured with enabled SSH access.

iii. **Remote App** - Enabling this access will permit users to connect to the remote applications configured in the target resources when they meet the defined criteria expression.

iv. **SQL Access** - Enabling this checkbox will permit users to take SQL sessions to the SQL resources configured under this access policy when they meet all the defined criteria.

v. **Password Reset** - This access will grant permission to the users to do remote password reset when the respective user and resource meet the defined criteria expressions.

> **Note:** If you have any scheduled password reset configured, it will not be affected by the access policy conditions configured via zero trust. Even if the user/resource fails to meet the configured criteria expression, the password reset will be performed through the scheduled password reset.

vi. **Landing Server Access** - Enabling this will allow users to remotely access the IT assets in your data centers configured with a primary landing server if the criteria expression is satisfied.

Note: To attain the access privilege to a resource configured via the landing server, both the landing server and target resources should meet the defined criteria expression if they are associated with policy-based access privilege conditions.

vii. **JIT Privilege Elevation** - This option provides Just-In-Time privilege elevation access to accounts in PAM360 if all the criteria are satisfied according to the expression added for this condition.

viii. **Self-Service Privilege Elevation - Linux** (If resource configured with Self-Service Privilege Elevation) - Enabling this option will allow users to execute privileged commands with an elevated account privilege without sharing the passwords of the high-privileged user accounts if the provided criteria expression is satisfied. To learn more about configuring Self-Service Privilege Elevation in Linux, click here.

Notes:

i. If you are enabling this access privilege in a condition, it is required to enable SSH Access for this access privilege to work for a user.

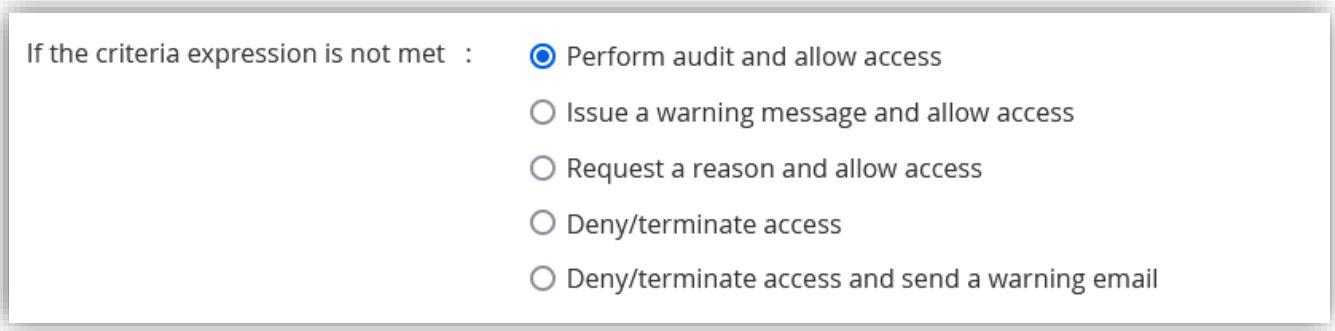
ii. If you are allowing users to take remote sessions via external SSH clients such as Remote Connect, PuTTY, etc., for Self-Service Privilege Elevation - Windows/Linux, it is required to neglect the **User Trust Score [C3]** criteria. The user authentication parameters cannot be validated for such cases.

ix. **Self-Service Privilege Elevation - Windows** (If resource configured with Self-Service Privilege Elevation) - Enabling this option will allow users to run certain types of files/applications (.cmd, .exe, .msc, .msi, and .bat) with elevated account privileges without sharing the password of the higher privilege account if the criteria expression is satisfied. To learn more about configuring Self-Service Privilege Elevation, click here.

Note: If you are enabling this access privilege in any condition, it is required to enable RDP Access for this access privilege to work for a user.

1.d Actions If the Criteria Expression is Not Met

The operation you select in this section will be performed when the user/resource fails to meet the above-defined criteria expression of a condition.



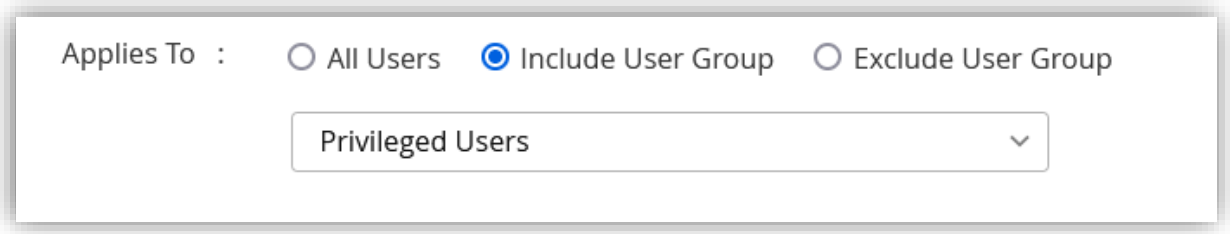
a. **Perform audit and allow access** - This option involves conducting an audit of the user's and resource's activity and then granting access to the requested if they fail to meet the criteria expression defined in the access policy condition.
b. **Issue a warning message and allow access** - If the criteria expression configured in an access policy condition is not satisfied, this option permits users' access to the resource but also sends a warning message to the user to alert them.
c. **Request a reason and allow access** - Enabling this option involves asking the user to provide a reason for their access request if they fail to meet the configured criteria expression of a condition. If the user provides a reason, the access privilege is permitted with the given reason; otherwise, the access is denied.

> **Note:** All the above three options are verified during the initial stages before granting the user access to the respective resource. If any of the criteria gets failed post permitted to access, the session will continue without any reason or warning, and this action will be in effect from the impending sessions.

d. **Deny/terminate access** - This option involves denying access to the resource entirely, and the user is not allowed to access the resource when the criteria expression is not satisfied.
e. **Deny/terminate access and send a warning email** - If the configured criteria expression of the condition is not met, this option involves denying access to the resource and sending a warning email to the user to alert them.

Note: The above two operations will be performed during the initial validation and active privileged sessions of the resources. If the configured criteria expression fails during an active privileged session, the respective enabled operation (terminate or warning message with a termination) will be performed.

Applies To: This option allows you to include or exclude users from the condition based on your policy-based access privilege requirements. By associating users with the condition, you can enforce the respective access policy for the users via relevant user groups.



To learn how to create an access policy that involves multiple conditional cases, you can refer to this real-time scenario help document.

2. Mindful While Creating Multiple Conditions in an Access Policy

1. While creating the access policy conditions, you can enforce it to all the users in the organization or a few specific users via user groups. If you want to exclude a few users from the access policy where they have already been included through different user groups, using the same condition template, you can add a new condition with the option '**Exclude User Group**'.
2. If there are two below conditions in an access policy applied for the same user:
   a. If the user trust score is greater than 70, allow RDP and SSH access. Else perform an audit and provide access.
   b. If the user trust score is greater than 50, allow RDP access. Else deny/terminate access.

It works in a way that - RDP access will be allowed for the user trust score greater than 50 or will deny/terminate the session if it is less than 70. SSH access will not be allowed for the user since it is not enabled in one of the conditions.

Note: If an allow access privilege is not enabled for a user in any of the conditions of an access policy, then it will be considered a disabled privilege for the access policy. In the above cases, we recommend you create unique access policies for RDP and SSH access for the same user with diverse criteria.

3. In an access policy with multiple conditions that have varying criteria and actions for the same user, the privileged access calculation for that access policy will always consider the action from the condition that has the higher precedence action. E.g., Deny/terminate, Exclude User Group.
4. The criteria expression [C1 or C2 and C3 and C4] is always verified from right to left, irrespective of the AND/OR condition. You can use the edit criteria expressions option and use the '()' brackets to define precedence to the criteria validation. E.g., [C1 or (C2 and C3) or C4]
5. For the resource configured with Self-Service Privilege Elevation on Windows or Linux, the trust score of the logged-in user account will be considered for access policy criteria calculation and not the trust of the user account that is used to elevate the privilege.

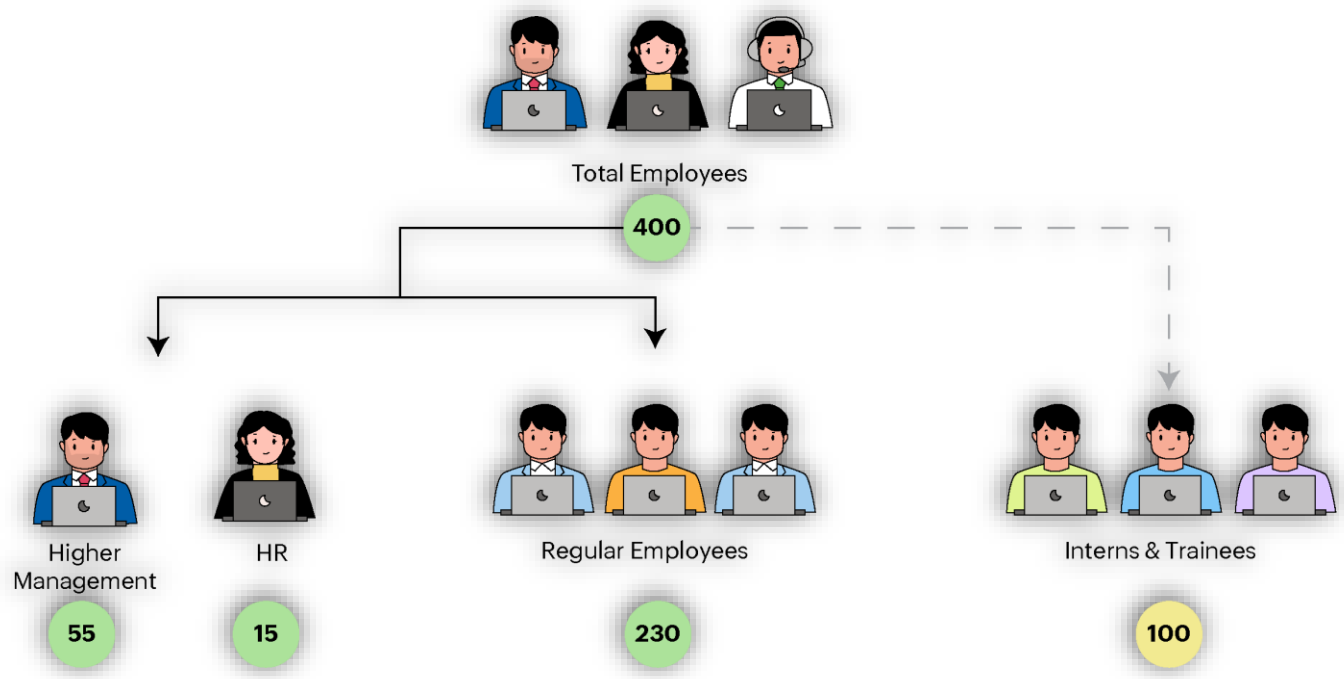
Practical Implementation Scenario and Use Cases

Zero Trust security is a security model that assumes that all users, user devices, and resources are untrusted by default. This approach requires organizations to verify the identity of all users, devices, and resources before granting users access to resources with the organization's data, thus resulting in safeguarding the organization's data from threats and anomalies.

Implementing Zero Trust can seem daunting, but it is crucial for organizations to adopt a Zero Trust model to protect their sensitive data from external breaches and cyberattacks. From this document, you will explore a practical Zero Trust implementation scenario in an organization and examine case studies that led to the result of successful Zero Trust implementations.

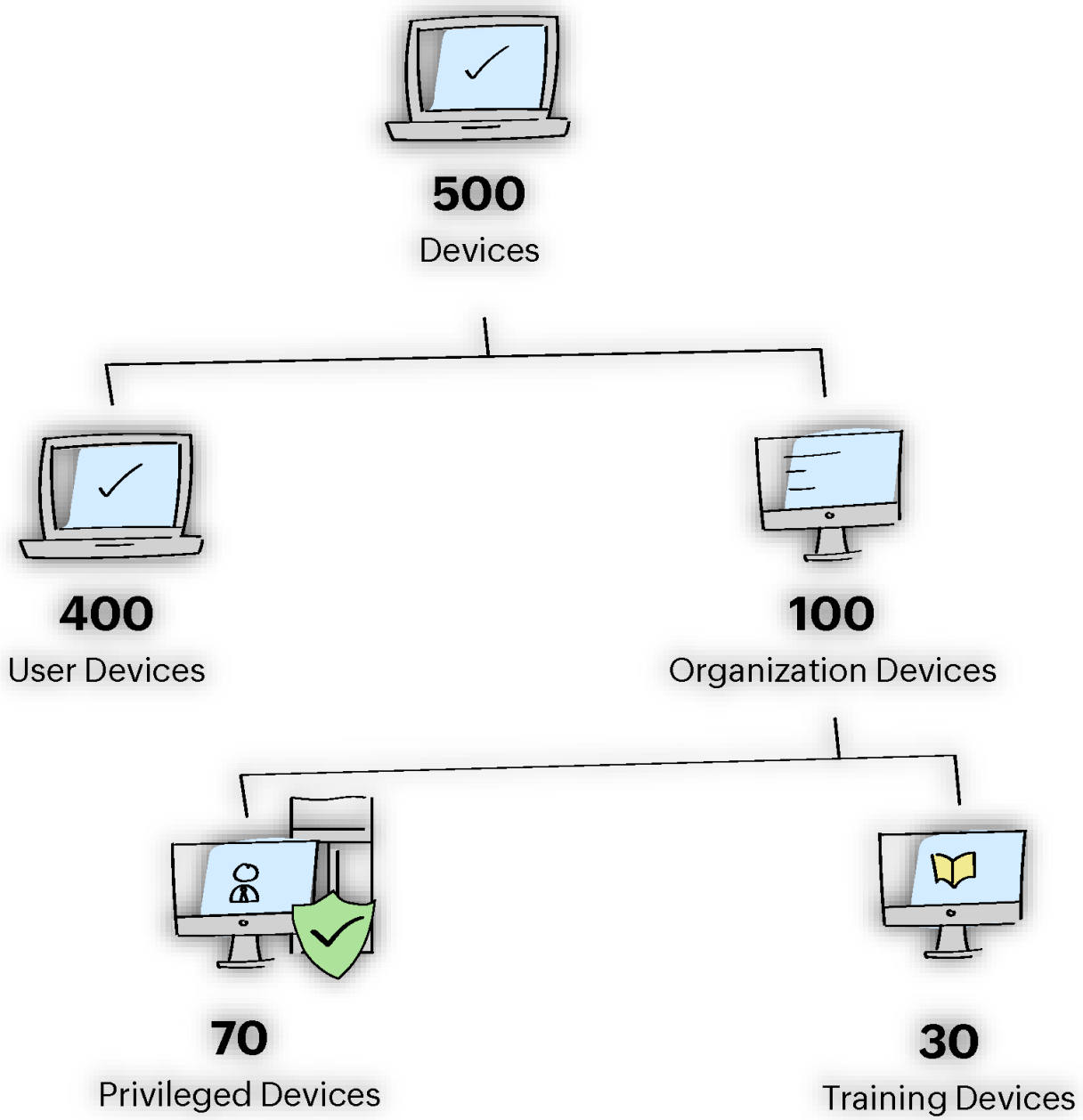
1. Zero Trust Implementation Scenario in an Organization

Imagine an organization with the below hierarchical scenario and strength:



a. People from **Higher Management** and the **HR** are grouped in the user group - '**Privileged Users**'.
b. **Regular Employees** are grouped into the user group - '**Regular Employees**'.

c. **Interns and Trainees** are grouped in a user group - '**Interns and Trainees**'.



a. **Organization Devices** include **Privileged Devices** and **Training Devices**.
b. **Privileged Devices** are grouped in the resource group - '**Privileged Devices**'.
c. **Training Devices** are grouped in the resource group - '**Training Devices**'.

Case: John - The IT administrator of the above organization is struggling to manage and grant access privileges to many individuals, including regular employees, interns, trainees, and higher management and human resources personnel. Additionally, he faces challenges in managing user and privileged devices, protecting against threats from sophisticated attackers

and algorithms, restricting access to non-compliant devices, and monitoring user activity and access to privileged devices.

Without an approach like Zero Trust, these difficulties can lead to security vulnerabilities and unauthorized access to sensitive information. Hence John plans to enforce the policy-based access privilege (Zero Trust approach) via PAM360.

Organization Requirements

1. Regular employees should have access to all the privileged devices with prerequisite conditions except the training devices.
2. Interns and trainees should have a strict access policy for accessing the training devices for training and validation purposes.
3. People from higher management and HR should always have access to all the devices in the organization with certain access conditions.
4. All devices that include highly privileged accounts should be checked continuously for security.
5. Regular employees, interns, and trainees should be given access to their respective allocated devices based on the user activities and device/resource state.
6. Granting access to organization resources should be automated in a high-end workflow with enhanced security criteria.

Step 1 - Installing Zero Trust Agent

To validate the user device and resource credibility using the user device and resource state, some certain parameters from them should be fetched for validation. To fetch those details for validation to policy-based access privilege, John will:

1. Install the PAM360 agent of **Usage type - 'User Device'** in the user devices.
2. Install the PAM360 agent of **Usage type - 'Resources'** in the organization resources **Zero Trust Module**.

Step 2 - Configuring Trust Score Parameters

John will then navigate to the **Admin >> Zero Trust >> Configuration** page to define conditional parameters for the user authentication, user device, and resources for calculating trust scores based on the organization's requirements and standards. John defines the following conditional parameters (**only for reference**) that follow:

Note: To know more about configuring parameters in detail, refer to this help section.

User Score Parameters

Authentication	
Invalid Sign-In Attempts	5 attempts in 7 days
Non-Office Hour Sign-In	09:00 to 18:00
Access from Allowed IPs	172.24.2XX.X to 172.24.2YY.Y
Access from Allowed Devices	192:YY:YYY:YY pam-2k694
User Belongs to Privileged Group	Privileged Users

Device	
Allowed OS Version	10.0.22621
Open Ports	135 445 623 3306 4567 5040 7680 8020 8027 8028 8383 8443 9292 9293 9295 16992 49664 49665 49666 49667 4567 7680 8028 8443 9292 9293 9295 16992 49664 49665 49666 49667 49668 49669 49673 49670 69 123 5050 61856 137 138 1900 56744 69 123 60504 63906 1900 49667 56743 57457 1900 56742
Allowed Browser Plugins/Addons	bdgkacbeblomgnaoildjnppjkamgoogc cnlefmmeadmemmdciolhbnfeacpdfbkd

	pictureinpicture@mozilla.org firefox-compact-light@mozilla.org
Allowed Applications/Packages	7-Zip 22.01 (x64) Mozilla Firefox (x64 en-US) Notepad++ (64-bit x64) Microsoft Office Standard 2016 Sublime Text Intel(R) Wireless Manageability Driver Microsoft .NET Runtime - 6.0.9 (x64) Dell Power Manager Service FortiClient VPN Microsoft Office Standard 2016
Allowed Processes/Services	smss.exe csrss.exe wininit.exe services.exe lsass.exe WUDFHost.exe fontdrvhost.exe svchost.exe NetworkManager

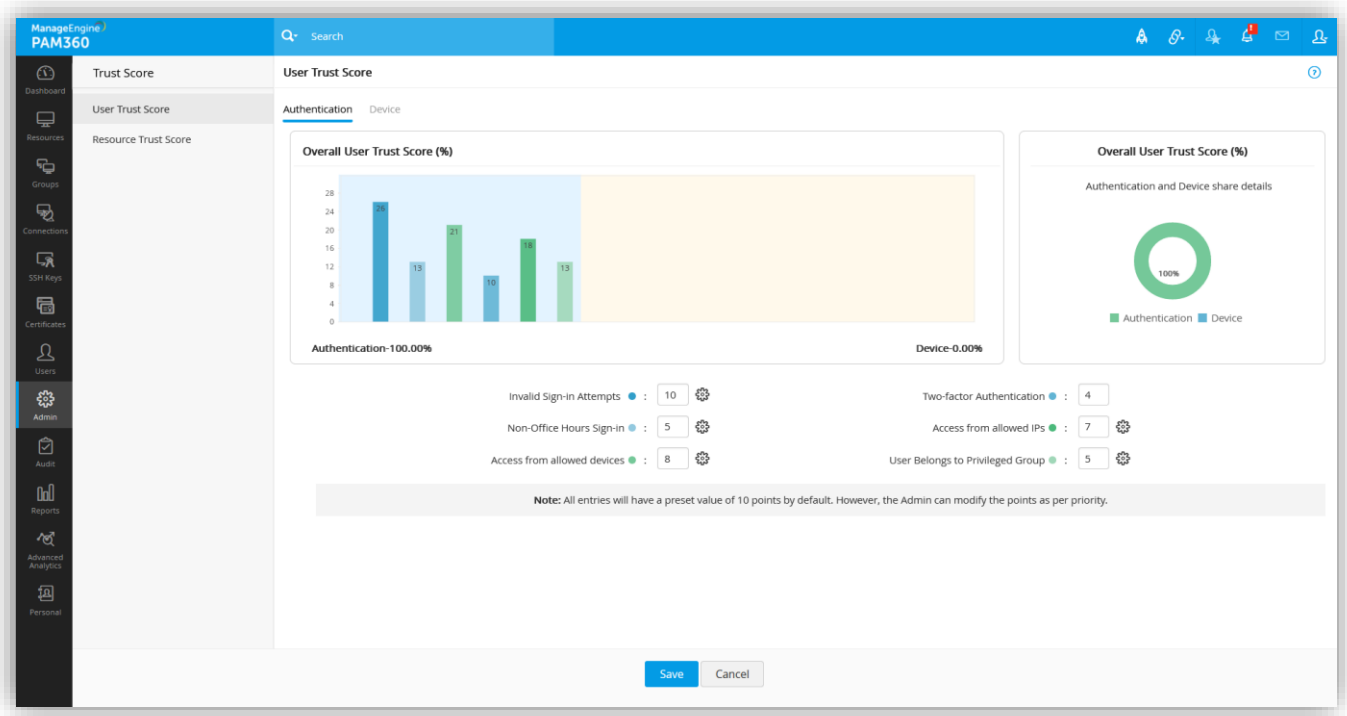
Resource Score Parameters

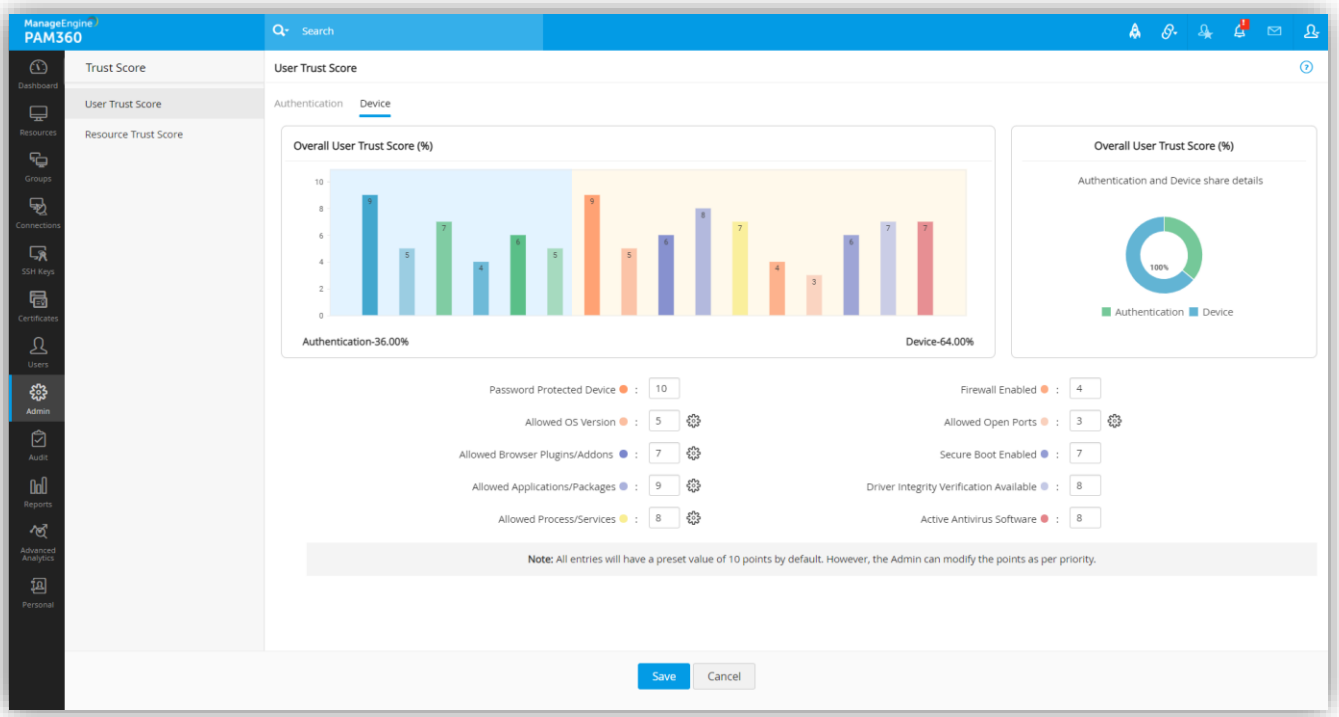
Resource	
Allowed OS Version	10.0.22621
Open Ports	7272 45623 5355 8282 51444 63906 6565 9292
Allowed Browser Plugins/Addons	firefox-compact-dark@mozilla.org expressionist-balanced-colorway@mozilla.org nmmhkkegccagdldgiimedpiccmgmieda
Allowed Applications/Packages	Mozilla Firefox (x64 en-US) Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.40664 Intel(R) Wireless Manageability Driver Microsoft .NET Runtime - 6.0.9 (x64) Java 8 Update 361 (64-bit) Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31326
Allowed Processes/Services	WUDFHost.exe winlogon.exe fontdrvhost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe svchost.exe IntelCpHDCPSvc.exe

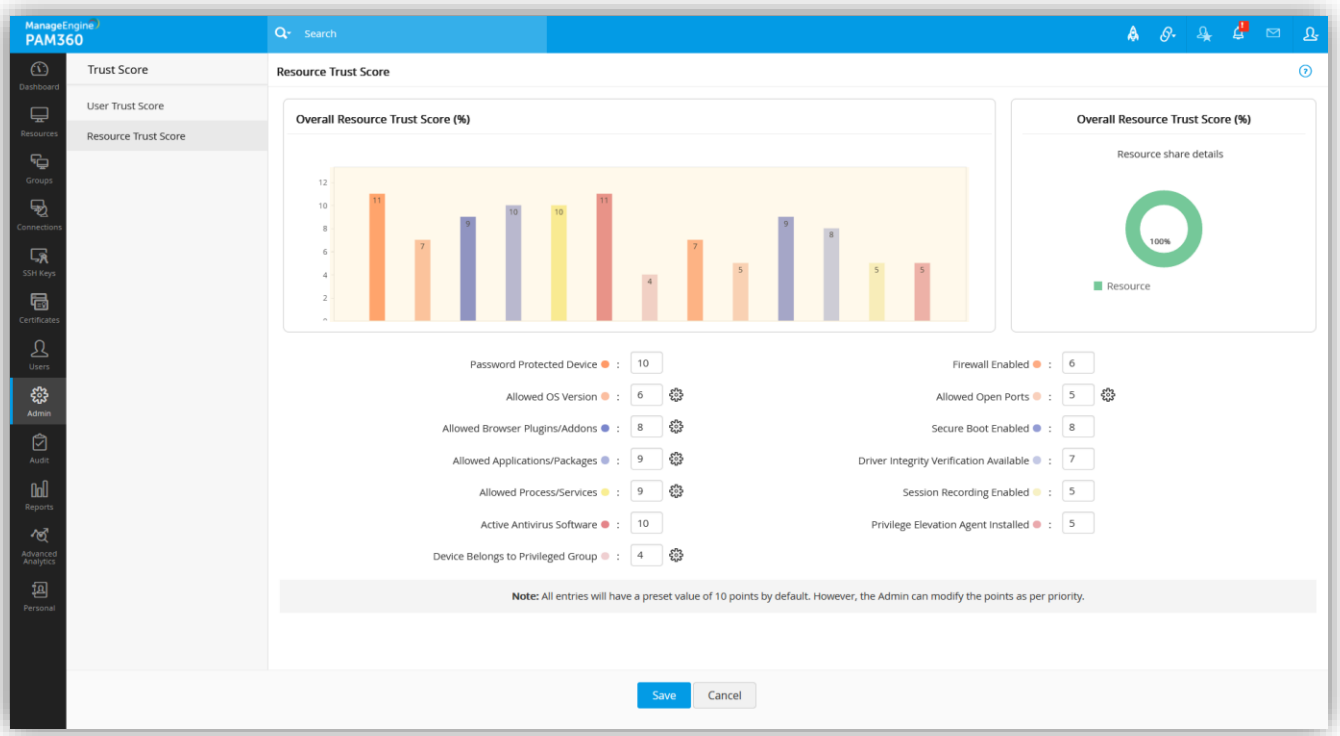
Device Belongs to Privileged Group	Privileged Devices

Step 3 - Configuring Trust Score Weightage

Now, John navigates to **Admin >> Zero Trust >> Trust Score** page to set the weightage value **(0-10)** for the conditional and the predefined parameters (fetched from the user device and resource via installed agents) for the trust score calculation. For the user trust score and the resource trust score calculation, John sets the below weightage based on the organization's importance.



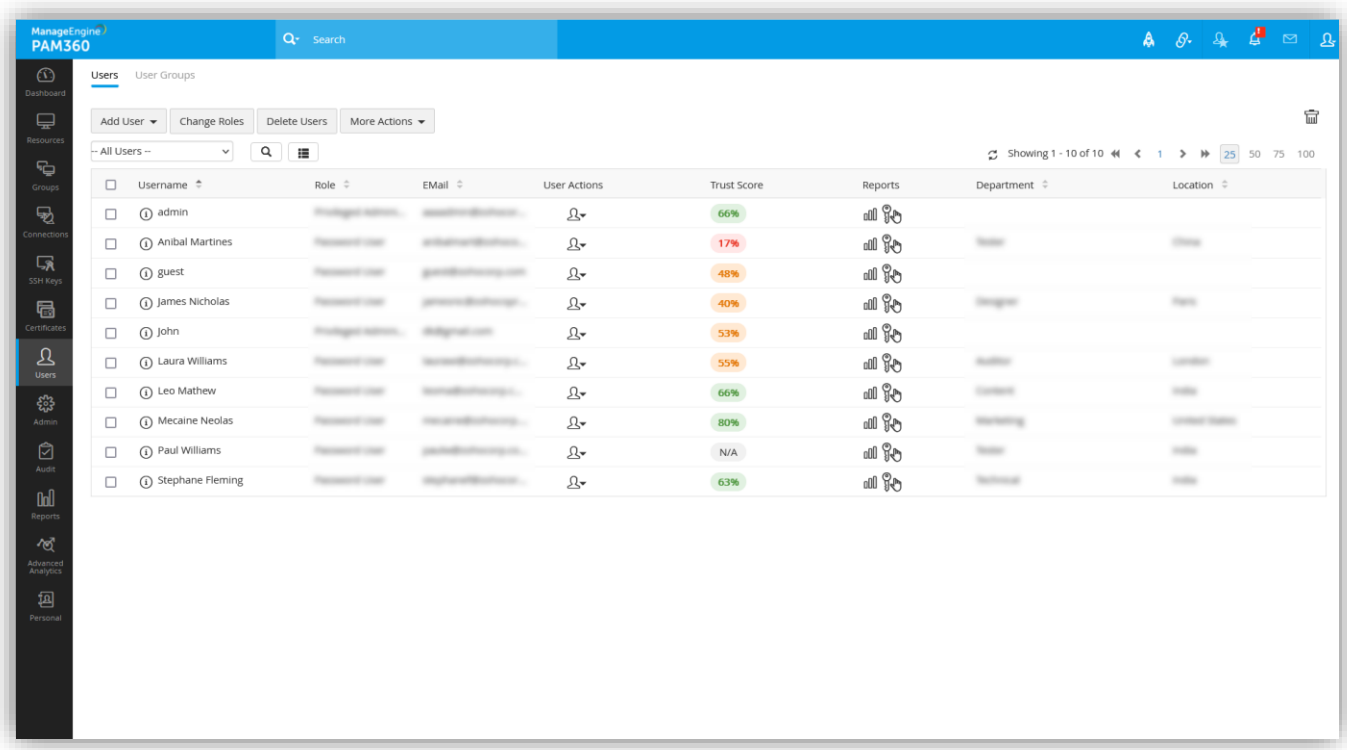


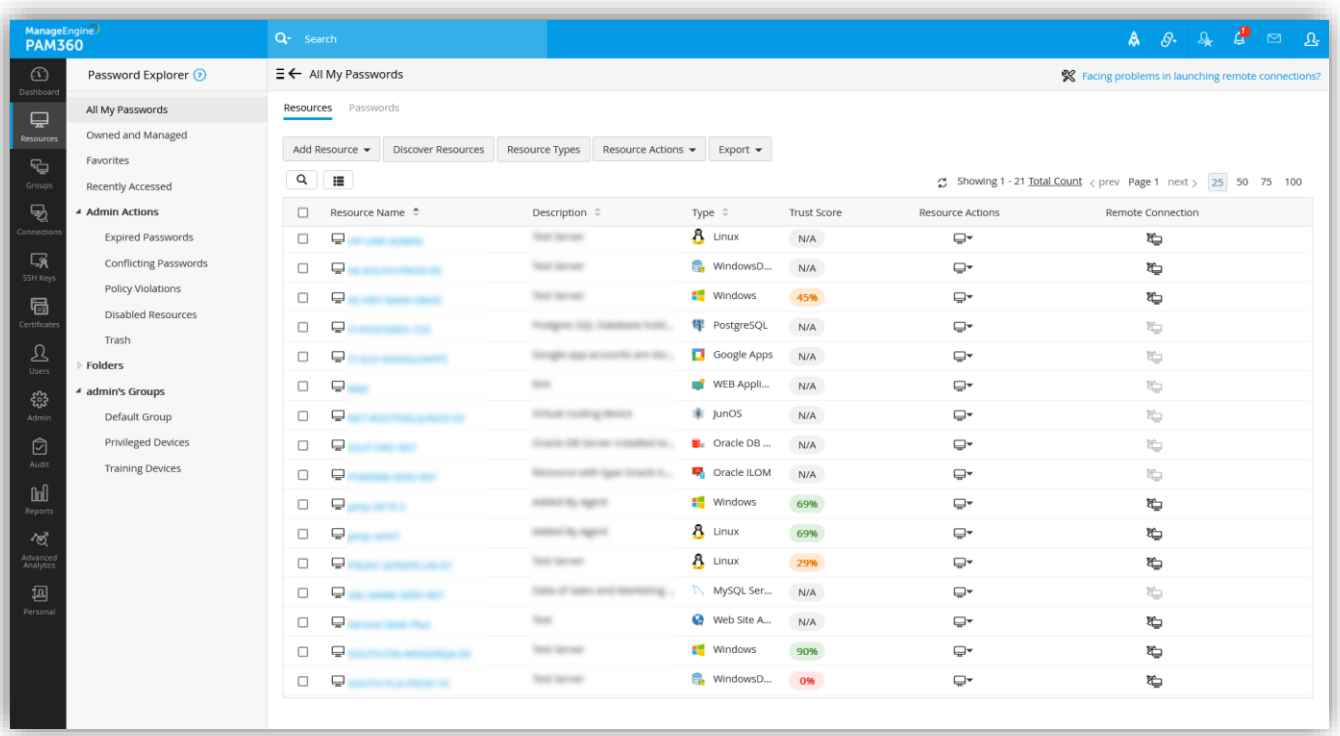


Based on the fixed weightage values in the respective fields, the bar charts will show the points for each parameter. The parameter points will be consolidated and calculated out of 100 as per the value of assigned weightage in the respective fields.

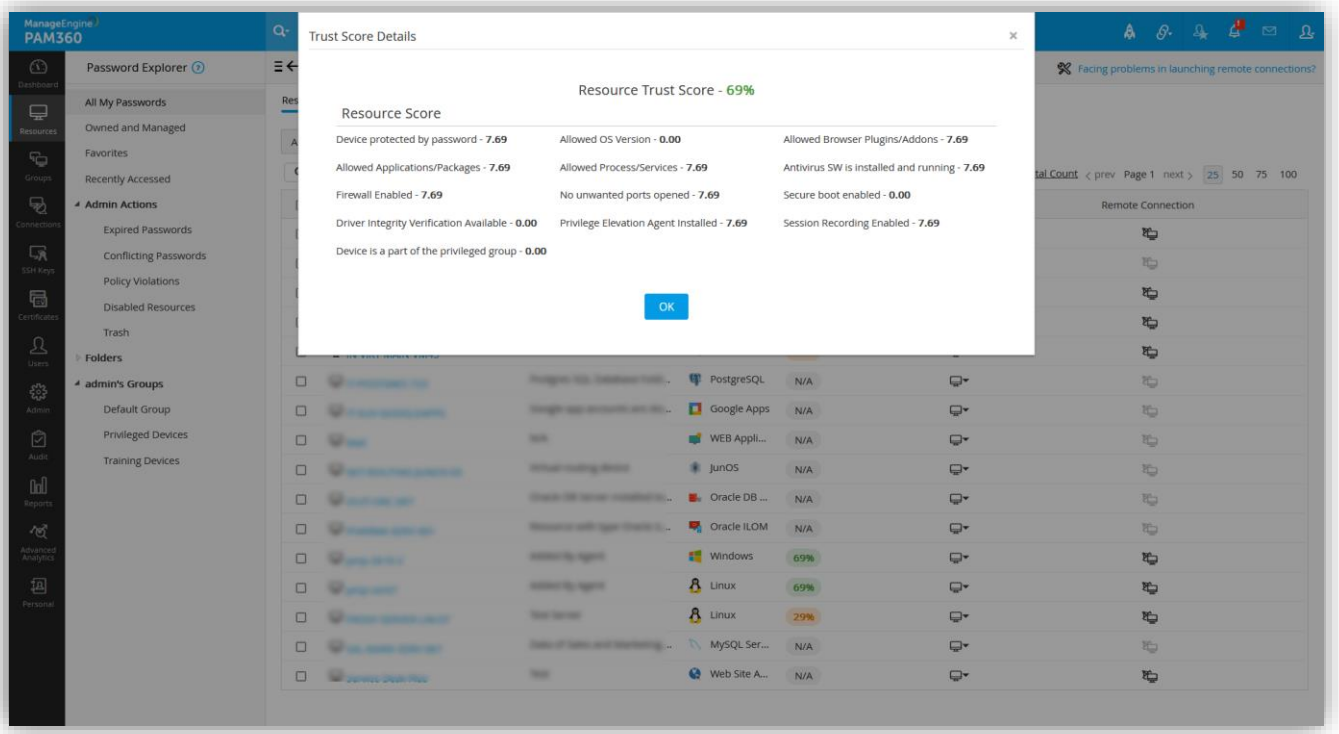
For example, if the user configured under a policy-based access privilege method logged in during non-predefined working hours, as shown in the bar chart, 5 points will be reduced from the user trust score. Similarly, if a privileged device configured under a policy-based access privilege method is not installed with antivirus, as shown in the bar chart, 11 points will be reduced from the resource trust score.

On the **Users** and **Resources** tab, the final trust scores for users and resources will be displayed based on all parameters' validation.





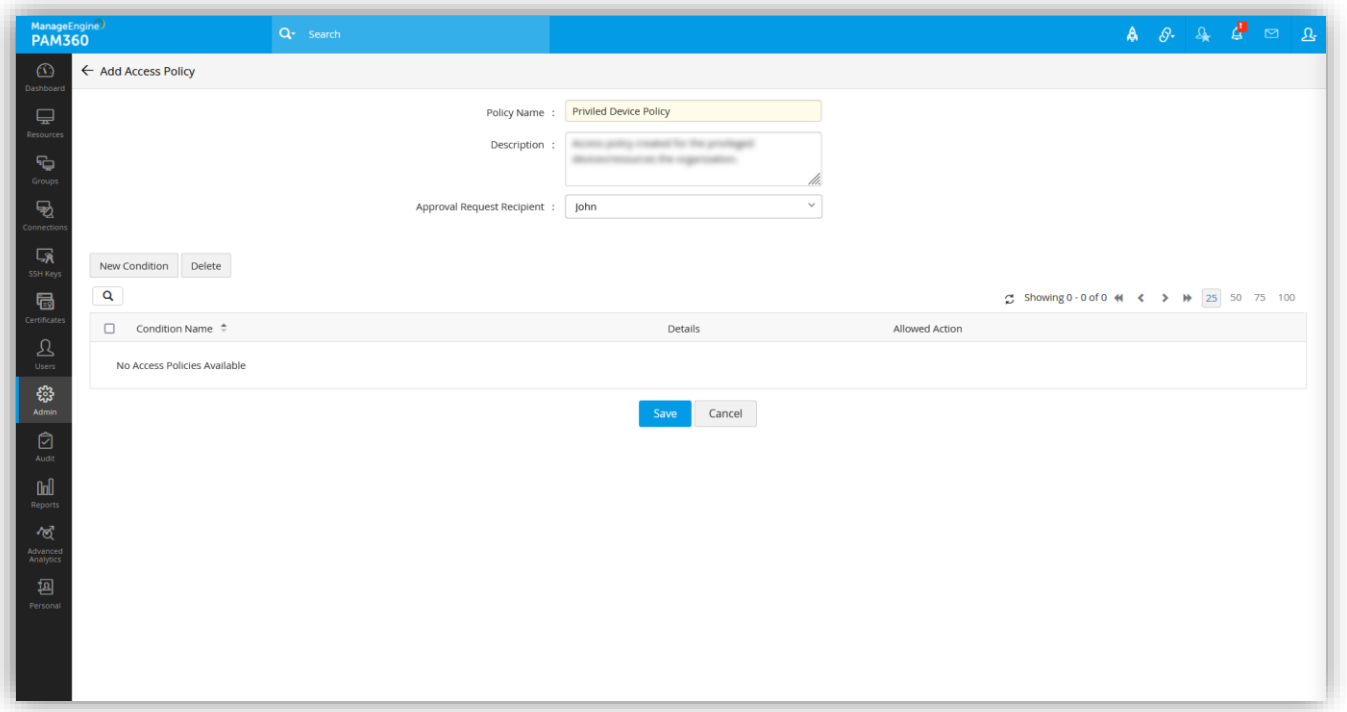
By clicking on the respective trust score value, John can see the parameter that is met or not met by the users as configured by him.



Step 4 - Configuring Zero Trust Access Policies

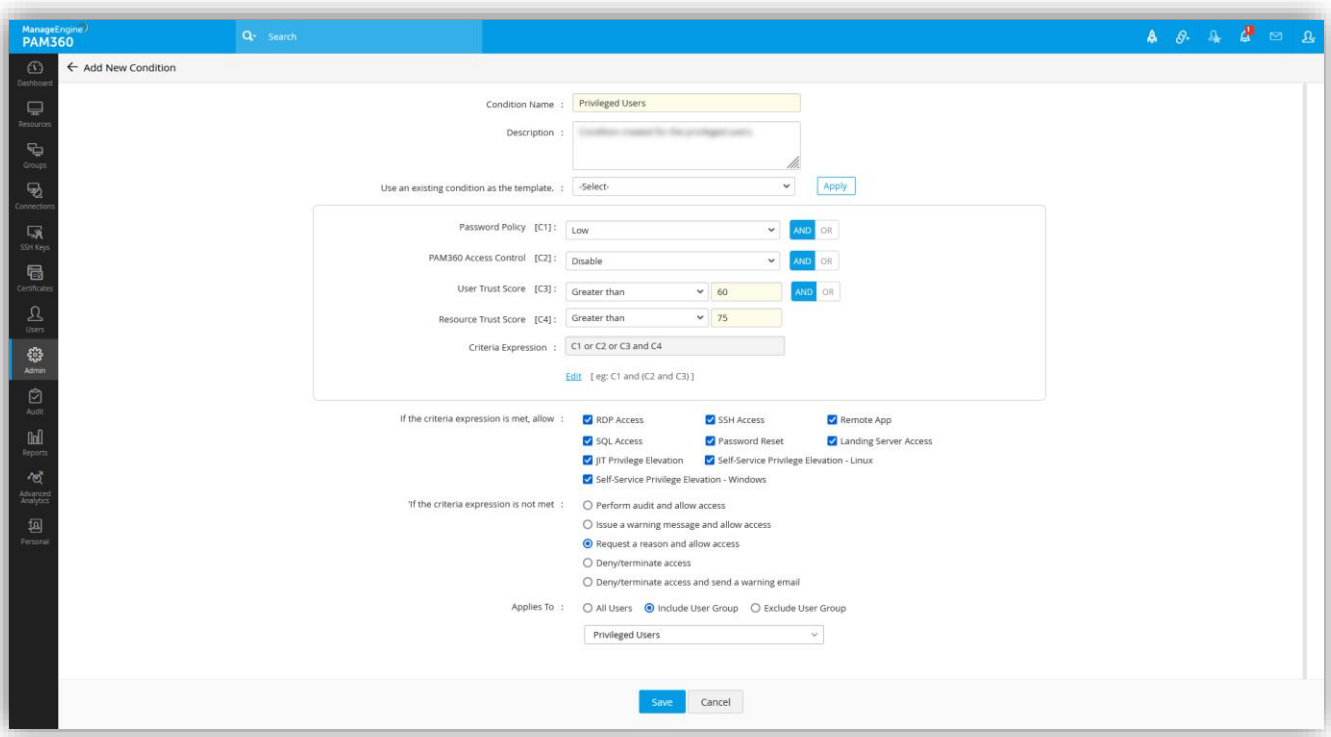
John now creates the two access policies with multiple conditions based on his organization's requirements. To do so, John navigates to '**Admin >> Zero Trust >> Access Policy >> Add**' and adds the below access policies.

1. Privileged Device Policy



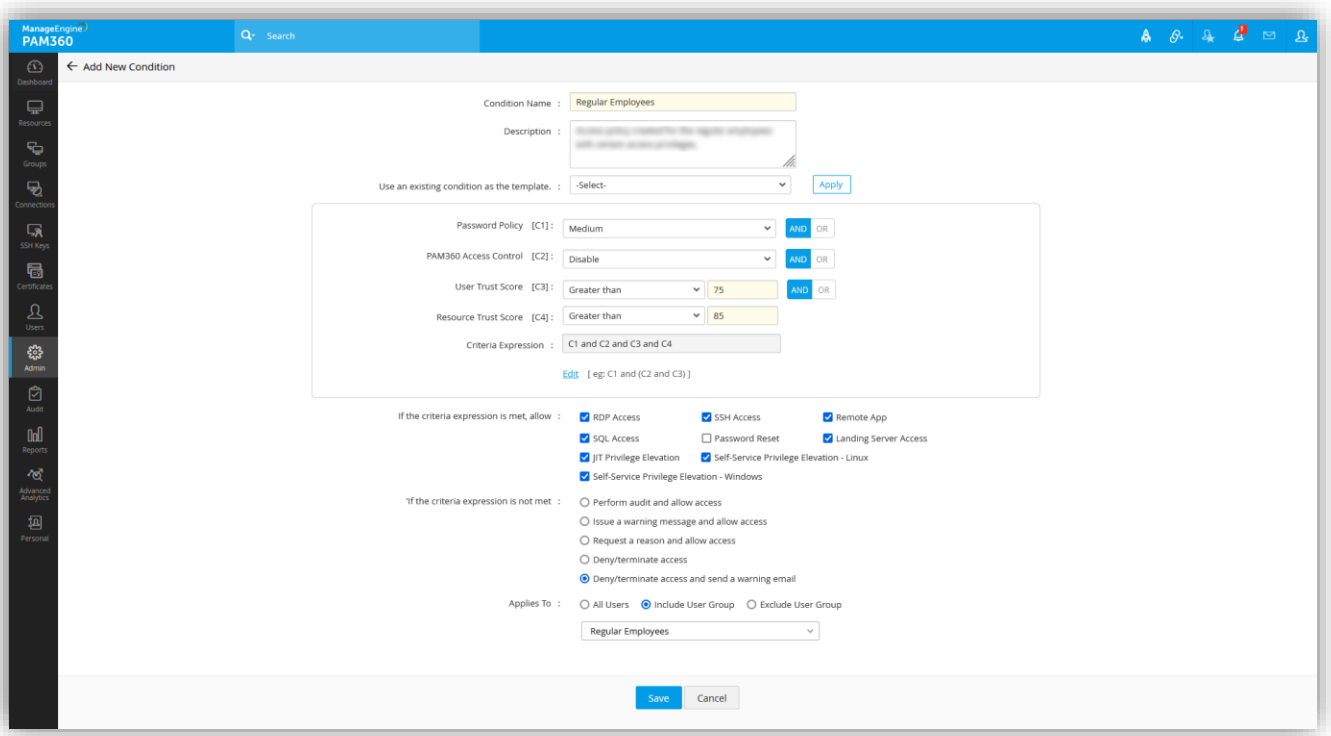
Condition I:

For the users from the '**Privileged Users**' user group, if the user trust score is above 60 and the resource trust score is above 75, provide RDP, SSH, SQL, landing server, remote app, password reset, and privilege elevation access. Else, Request a reason and allow access.

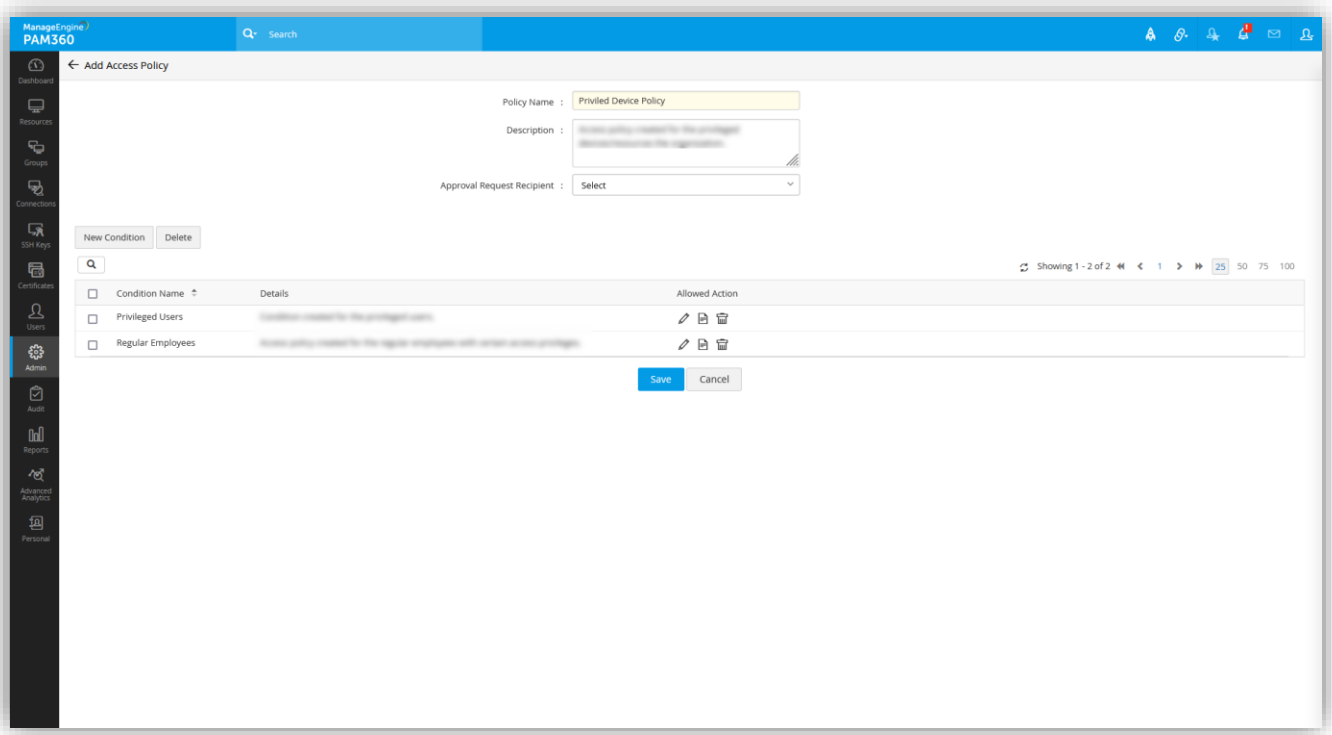


Condition II:

For the users from the '**Regular Employees**' user group, if the user trust score is above 75 and the resource trust score is above 85, provide RDP, SSH, SQL, landing server, remote app, and privilege elevation access. Else, Deny /terminate access and send a warning email.



After adding upon the conditions, John selects an approval recipient (another user with the administrator privilege) and saves this access policy for the further approval process.

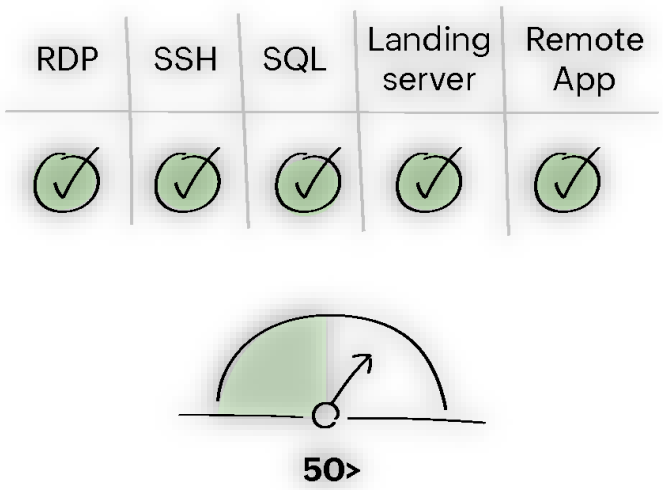


2. Training Policy

Condition I:

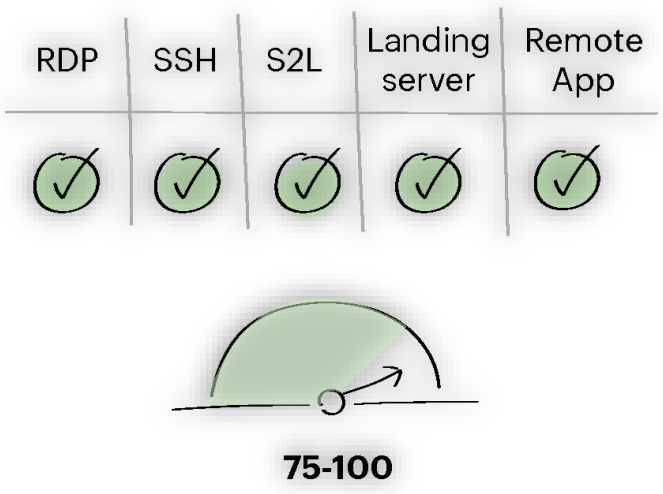
For the users from the '**Privileged Users**' user group, if the user and resource trust scores are above 50, provide RDP, SSH, SQL, landing server, remote app, password reset, and privilege elevation access. Else, Perform audit and allow access.





Condition II:

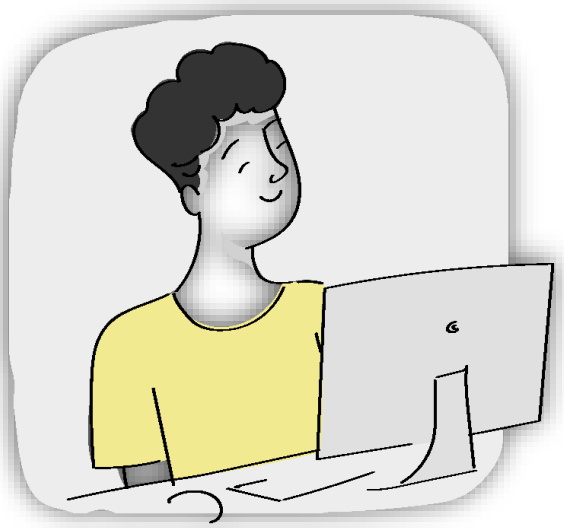
For the users from the '**Regular Employees**' user group, if the user and resource trust scores are between 75 and 100, provide RDP, SSH, SQL, landing server, remote app, password reset, and privilege elevation access. Else, Issue a warning message and provide access.

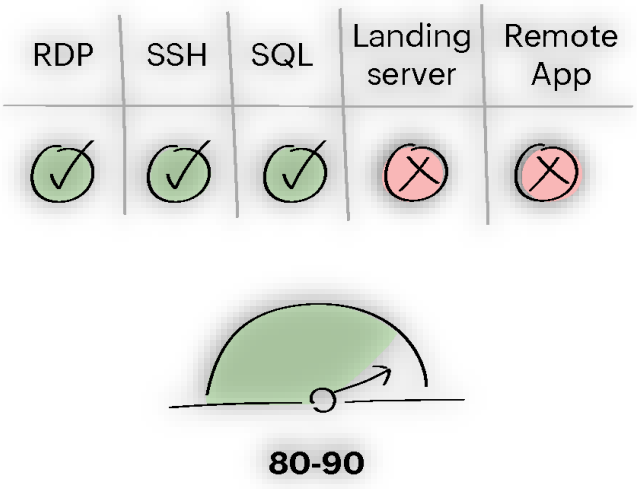




Condition III:

For the users from the '**Interns and Trainees**' user group, user and resource trust scores are between 80 and 90, provide RDP, SSH, and SQL access. Else, Deny / Terminate access and send a warning email.



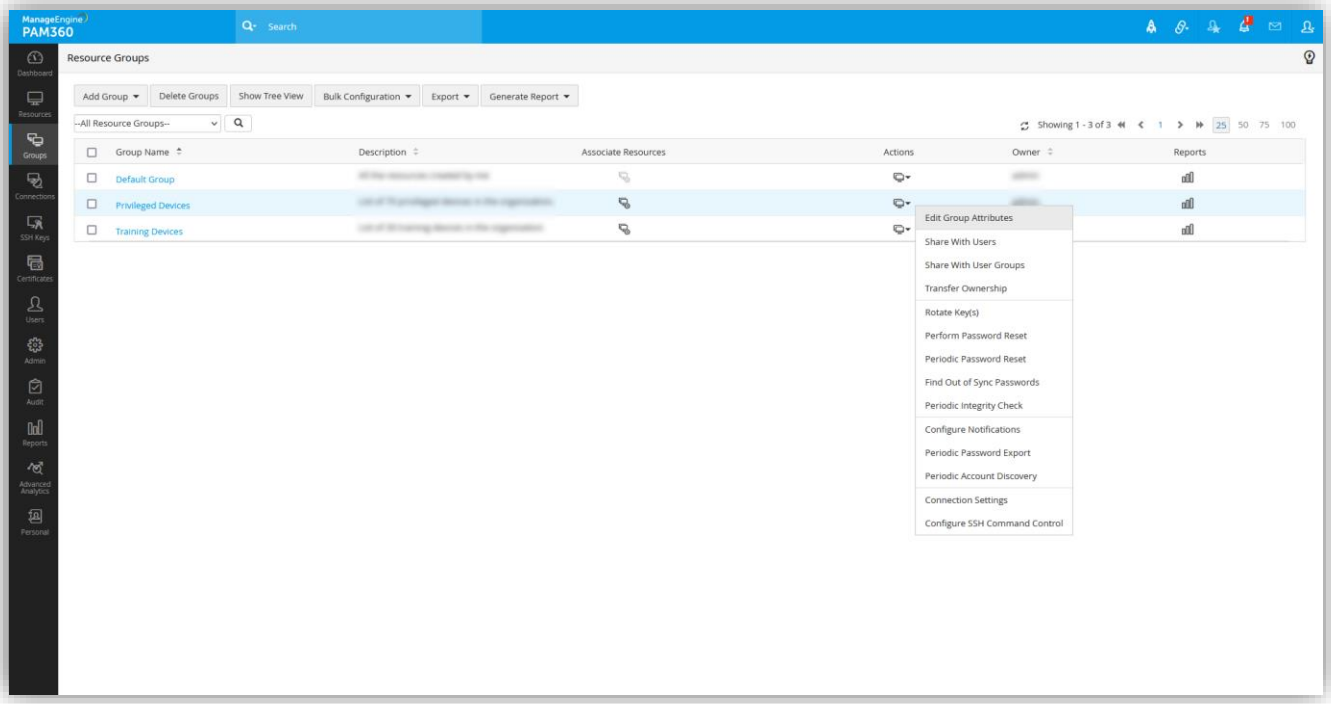


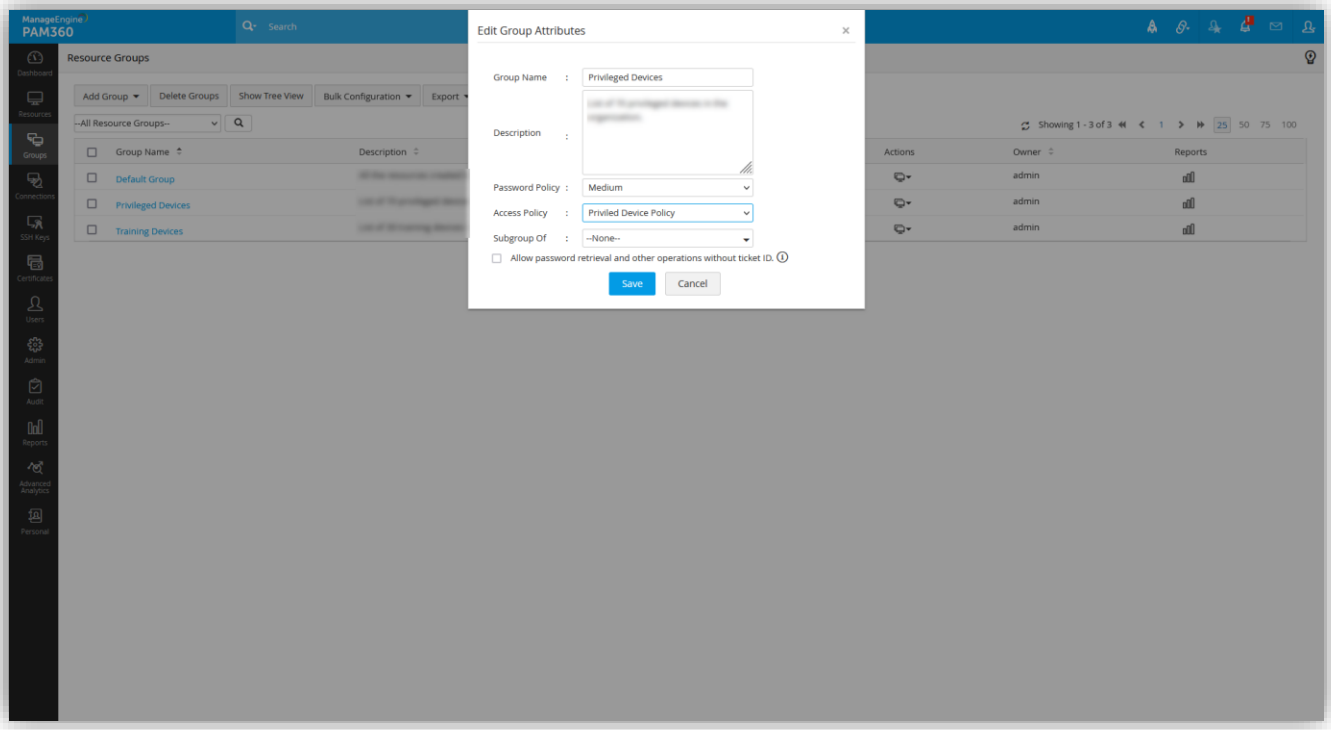
John adds the above conditions for the training devices and saves the access policy with the approver detail. Once the selected approvers of each access policy approve the access policies, John can further proceed with associating the access policies to the respective static resource groups.

Step 5 - Associating Access Policies with Static Resource Groups

John now navigates to the **Groups** tab and associates the configured Zero Trust access policies with the respective resources via static resource groups. John will associate the access policy '**Privileged Device Policy**' with the resource group '**Privileged Devices**' and the access policy '**Training Policy**' with the resource group '**Training Devices**' based on the prerequisites.

Upon completing the above steps, the policy-based access privilege method will be active for the organization via PAM360 using the Zero Trust approach.





Step 6 - Resolving Conflicts between Access Policies

In some scenarios, the few resources are grouped in multiple static resource groups with diverse access policies. In such cases, resources grouped in more than one resource group may result in conflict if their access policies are different.

Consider a case where another administrator in the organization creates a new static resource group with a new access policy of multiple conditions that includes five of the 70 privileged devices of the organization. The access policy for those five devices will automatically be changed to the newly applied access policy via a different resource group and displayed in the **Conflict Resolver**.

Now, John or the other administrator navigates to '**Admin >> Zero Trust >> Conflict Resolver**' and changes the access policy at the resource level from the **Actions** option beside the respective resource based on their final decision over the respective access policy.

2. How Policy-Based Access Privilege Benefits an Organization - Use Cases

Scenario 1

Detail -

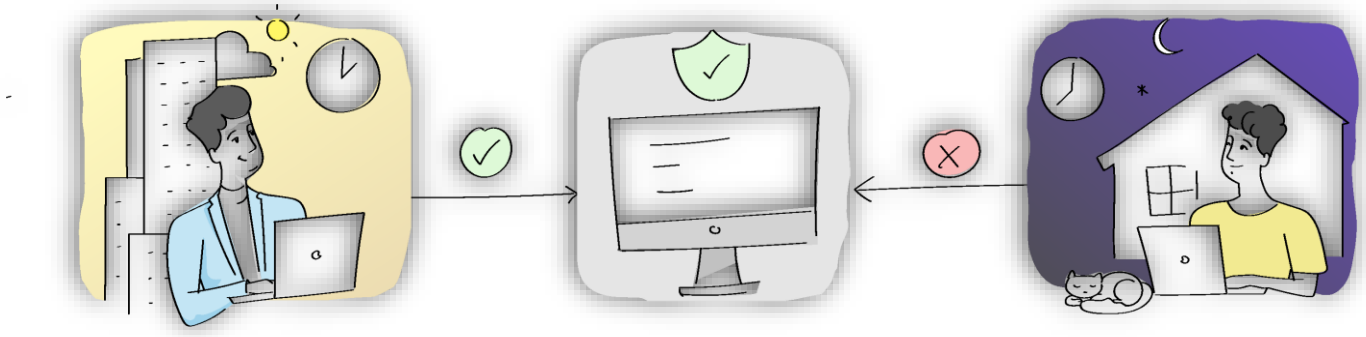
Consider an organization with an Offshore Development Center (ODC) for product maintenance and management purpose. According to the organization's ODC policies, the users are allowed only to work in their respective time zones and network with their assigned resources and are restricted from using external devices for project purposes.

Case -

The administrator has configured the policy-based access with the predefined parameters based on the ODC policies. A user of the organization has forgotten to complete a few application processes and tries to access it outside the network with an external machine on an open network, which might result in external intrusions and affect the project design and data.

Zero Trust Action -

Through the policy-based access privilege method, the parameters such as - Non-Office Hour Sign-in, Accessing from allowed IPs, etc., fail to meet the predefined conditions, thus decreasing the user trust score values, thus further resulting in restricting the user to access the privileged devices in the organization.



Scenario 2

Detail -

Imagine an organization with enormous privileged resources with more than one account in each. All those resources are shared with the organization users for internal project requirements and purposes via the PAM360 Zero Trust approach.

Case -

Consider a resource 'pam-demo-machine' shared with different users for performing privileged actions. A user with access to the resource installs an application and starts the application process that was block-listed by the administrator. The installed application has malware and is ready to be moved into the organization's network by disabling the antivirus and other device defenders.

Zero Trust Action -

The application installed by the user deviates from the configured Zero Trust policy-based access by failing to meet the predefined parameters such as - Allowed Applications/Packages, Allowed Processes/Services, Antivirus Software is installed and running, Firewall Enabled, etc. This results in reduced device score values, thus resulting in live session termination and also restricting other shared users from using that particular resource to avoid further data breaches and cyber-attacks.

PAM360 Integration with Zoho Flow

PAM360 integration with Zoho Flow, a robust automation platform that helps expand PAM360's integration capabilities across 800+ business applications, thus paving the way for workflow automation across multiple business functions, especially on HR and ITSM. A perfect example of this integration is the automated onboarding and offboarding of users onto/from PAM360 via a recruitment/ATS application.

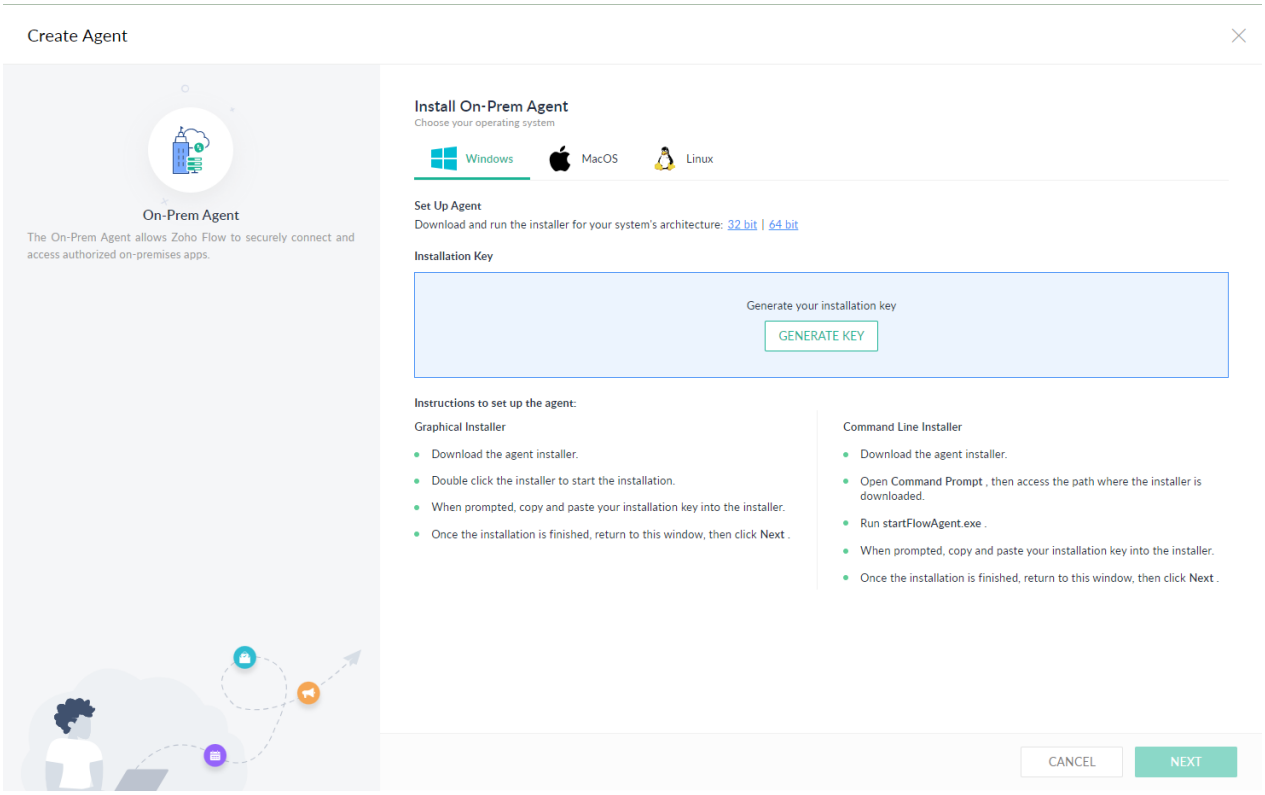
PAM360 can process dedicated actions triggered from any application in Zoho Flow's diverse app gallery. With this integration capability, PAM360 users can craft custom workflows within Zoho Flow, linking PAM360 to a wide array of applications using the PAM360 APIs. This includes tasks like user creation, user group management, account control, and sharing of privileged accounts and resources.

Working with Zoho Flow Agent

To create workflow automation in PAM360 on-premise application via Zoho Flow, a Zoho Flow agent is required that allows creating the required workflows, which include triggers and actions of on-premises applications, allowing them to exchange data between your cloud apps as well as the other on-premises applications in a secured manner.
Follow the below steps to download and install the Zoho Flow agent in the PAM360 installed server based on your operating system.

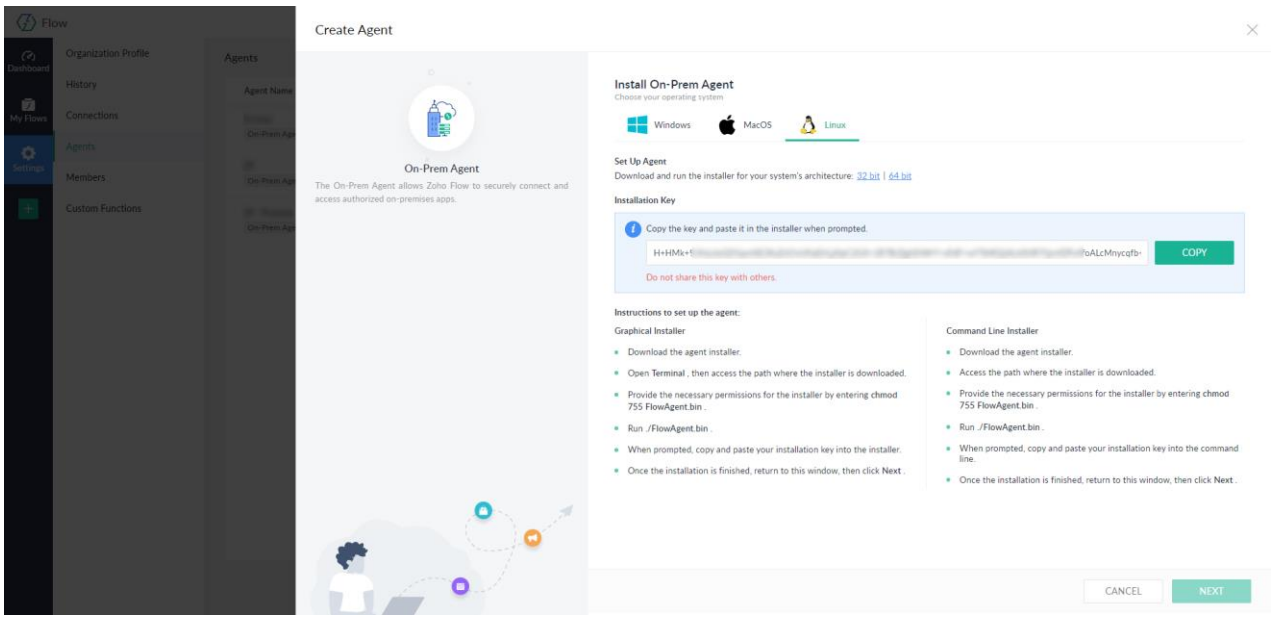
a. Downloading the Zoho Flow Agent Installer File

Log in to the Zoho Flow application.
Navigate to **Settings >> Agent** and click **CREATE AGENT**.
On the page that appears, select **On-Prem Agent** and click **NEXT**.



Now, navigate to the tab **Windows** or **Linux** and download your Zoho Flow agent installer file based on your system's architecture (**32-bit | 64-bit**).
Click **GENERATE KEY** to generate a unique key for this agent. In the window that opens, click **Accept** to continue.

Note: The installation key can be generated by the administrator or the organization owner only.



b. Installing the Zoho Flow Agent - In Windows

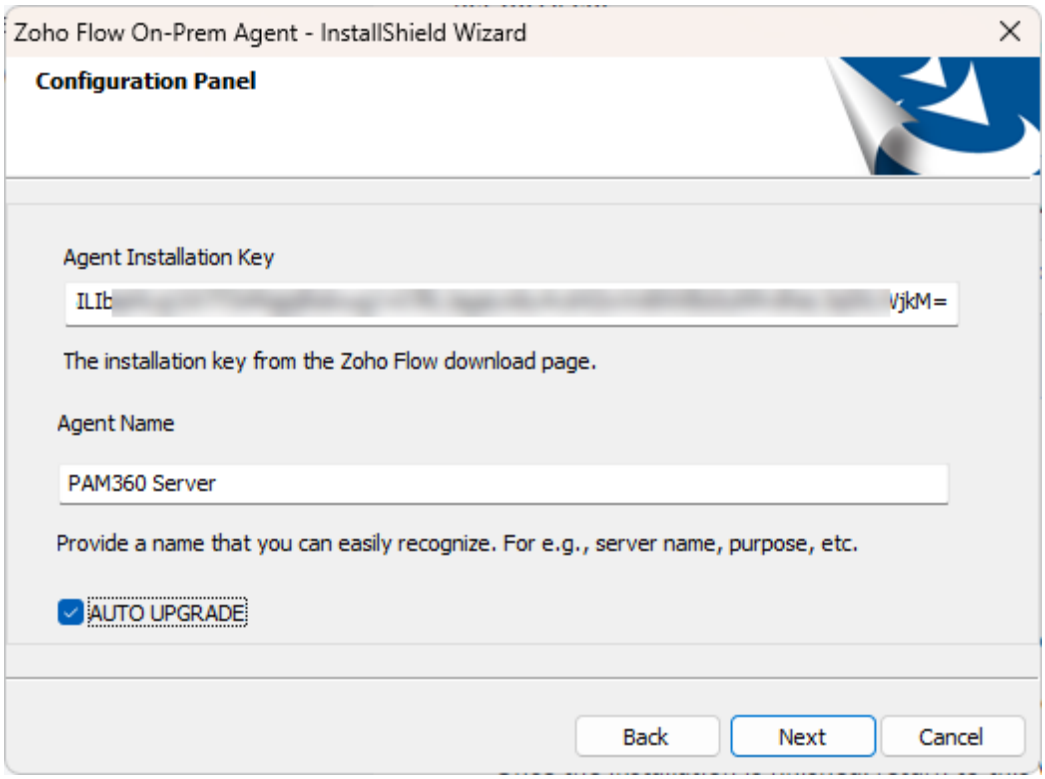
Navigate to the agent file downloaded path and launch the **FlowAgent.exe** as an administrator to start with the installation.

(or)

Open the **Command Prompt** as an administrator, navigate to the agent file directory path, and execute the command **start FlowAgent.exe**.

In the **Zoho Flow On-Prem Agent InstallShield Wizard** that opens, click **Next** and agree to the terms and conditions to continue with the installation.

In the **Configuration Panel** page, enter the **Agent Installation Key** copied from the **Create Agent** page from the **Zoho Flow** site.

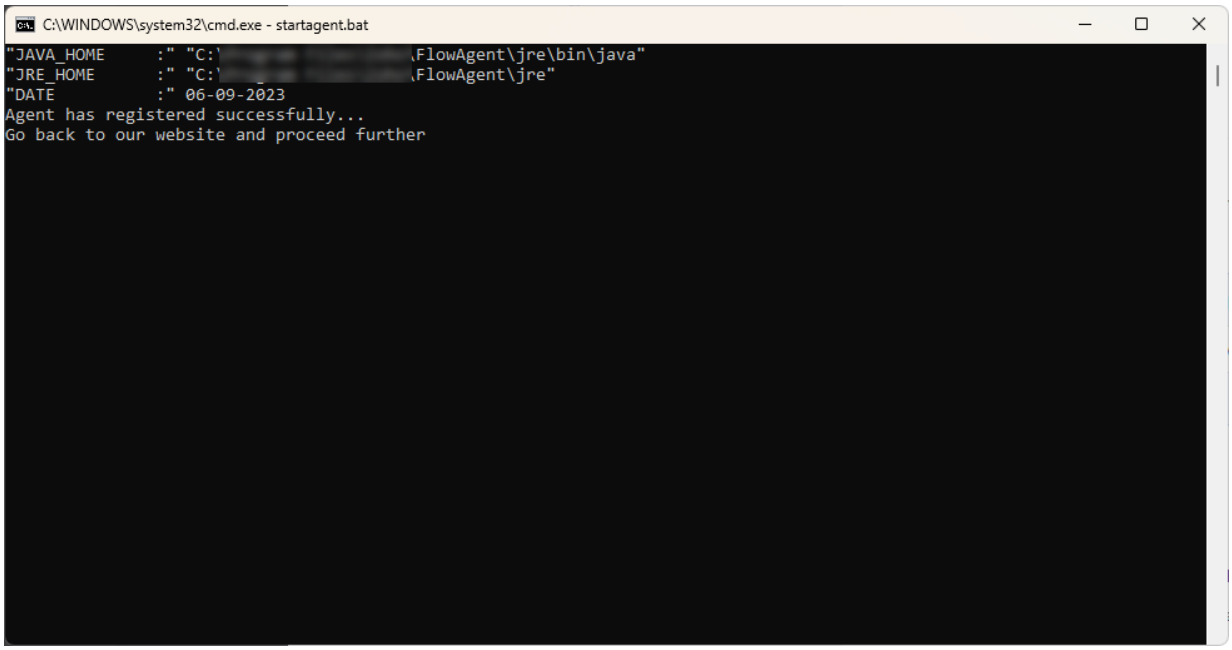


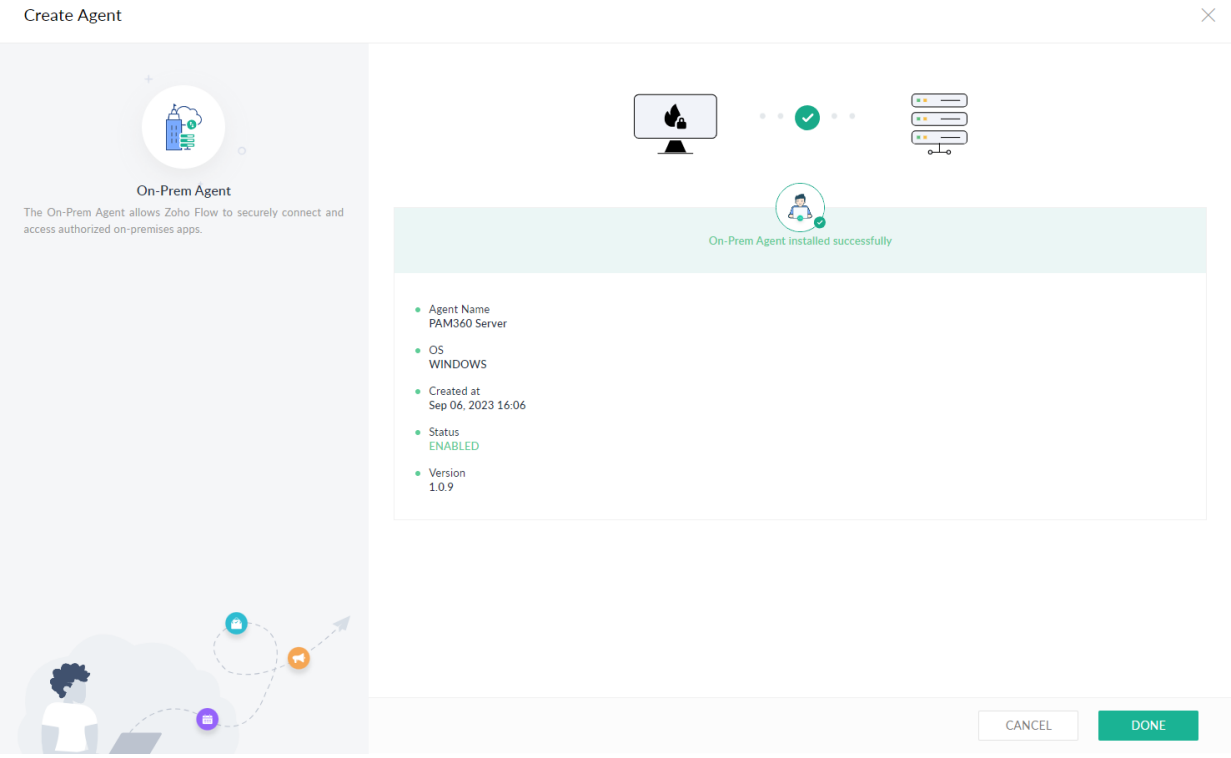
Change the destination location to the desired path where the agent installation files are to be placed.

Configure **the Proxy Details** if required and click **Next**.

Finally, click **Install** to proceed with the installation and enable the checkbox to start the Zoho Flow agent.

Once you are done with the installation, return to the Zoho Flow Create Agent window and click **Next**.





c. Installing the Zoho Flow Agent - In Linux

i. Installation using Graphical Installer

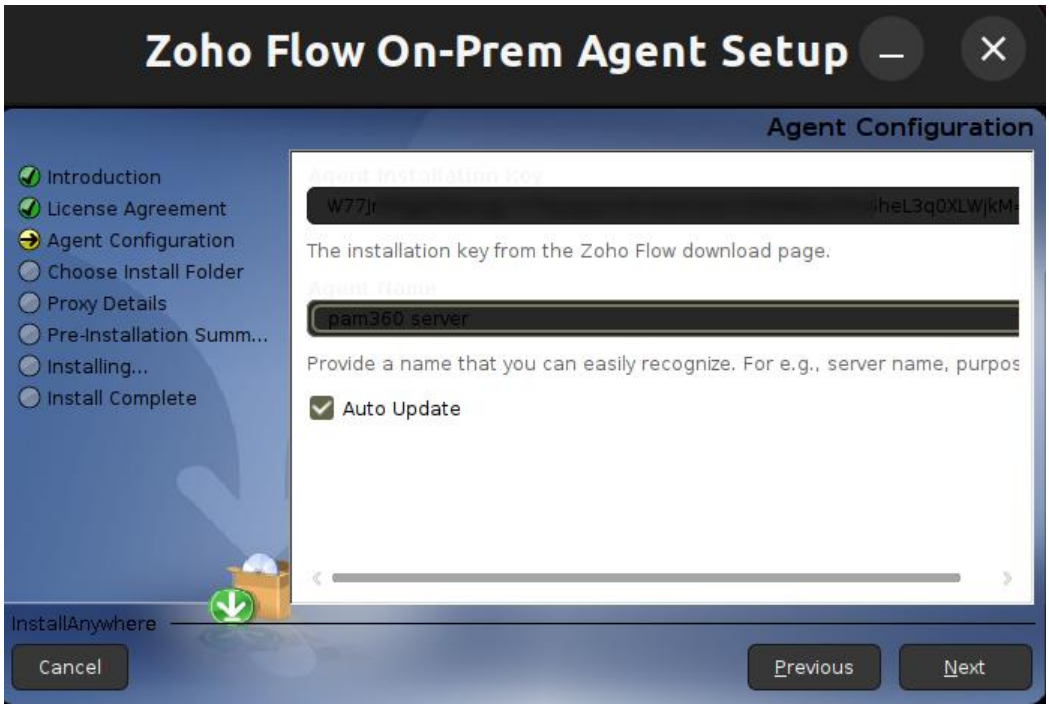
Open the terminal and navigate to the path where the Zoho Flow agent installer is downloaded.

Provide the necessary permissions for the installer by executing the command: **chmod 755 FlowAgent.bin**.

Now, execute the command **-./FlowAgent.bin**.

In the **InstallAnywhere** dialogue that opens, click **Next** and agree to the terms and conditions to continue with the installation.

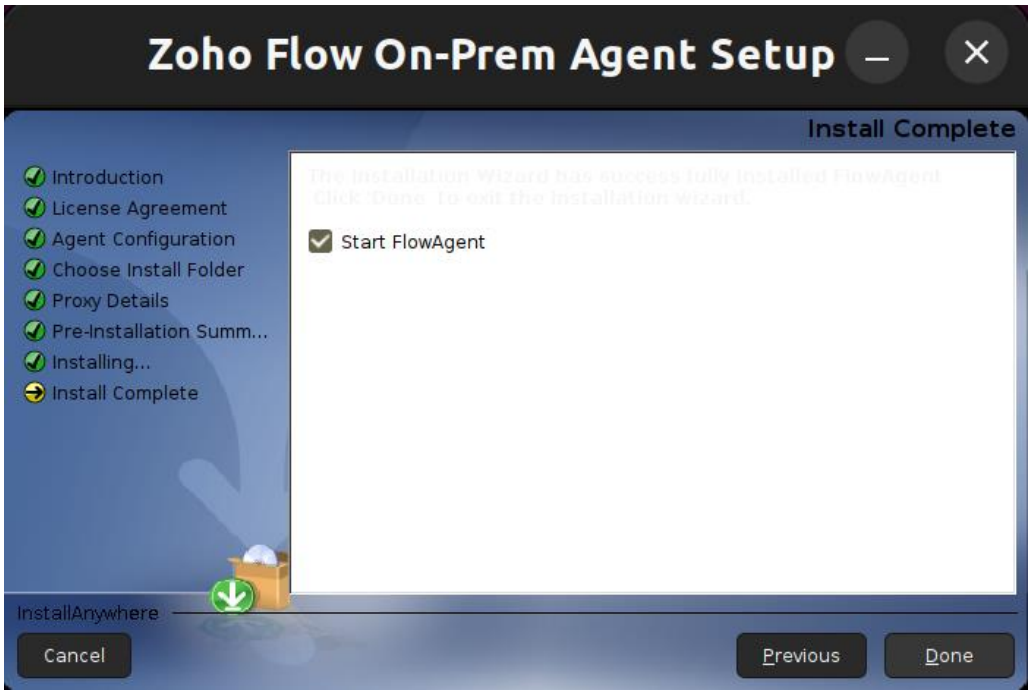
In the **Agent Configuration** page, enter the **Agent Installation Key** copied from the **Create Agent** page from the **Zoho Flow** site and provide an agent name.



Change the destination location to the desired path where the agent installation files are to be placed.

Configure the **Proxy Details** if required and click **Next**.

Finally, click **Install** to proceed with the installation and enable the checkbox to start the Zoho Flow agent.



Once you are done with the installation, return to the Zoho Flow **Create Agent** window and click **Next**.

ii. Installation using Command Line Interface

Open the terminal and navigate to the path where the Zoho Flow agent installer is downloaded.

Grant the necessary permissions to the installer by entering the following command: **chmod 755 FlowAgent.bin**

Execute the agent installer by entering the following command:**./FlowAgent.bin**.

When prompted, enter the agent installation key (copied from the **Create Agent page** from the **Zoho Flow** site) and also provide a name for the agent.

Specify the desired installation path for the agent.

If required, configure the proxy details.

Review the installation details, and then press enter to proceed.

Once the installation process is complete, return to Zoho Flow and click **Next**.

d. Post-Agent Installation Steps

The installed agents should always be updated to ensure a continuous workflow automated between the applications. We always recommend using the auto-update for seamless operations in the automated workflows.

To manage the agent update:

Navigate to **Settings >> Agent** and click **VIEW DETAILS** beside the respective agent.

In the pop-up that opens, enable or disable the **Auto-Update** feature using the provided toggle button.

> **Note:** By default, the agent installed will be enabled with the Auto-Update post-installation.

To delete the agent:

Navigate to **Settings >> Agent** and click the delete icon beside the **VIEW DETAILS** button.

You will be listed with the details of the workflow configured relevant to the agent. Ensure once and confirm the deletion process.

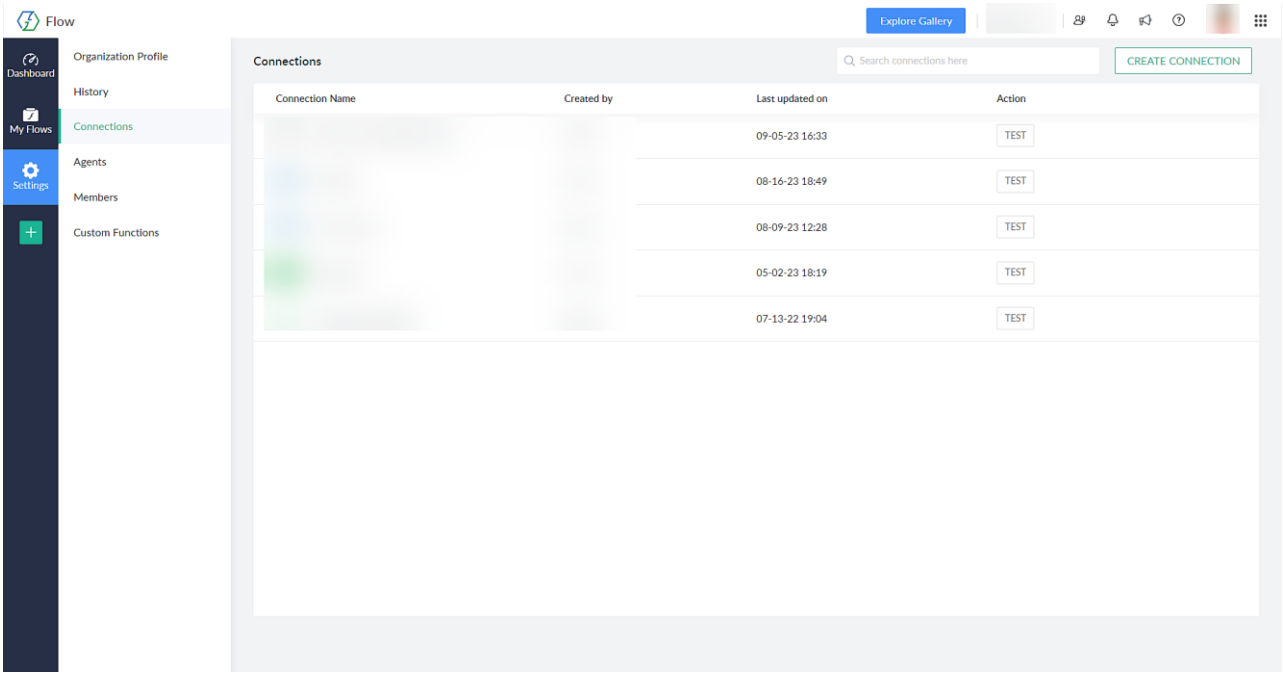
Integrating PAM360 with Zoho Flow

PAM360 seamlessly processes action requests from any application available within Zoho Flow's extensive app gallery. This, in turn, allows PAM360 users to craft customized flows within Zoho Flow, establishing connections between PAM360 and a wide range of applications using PAM360 APIs.

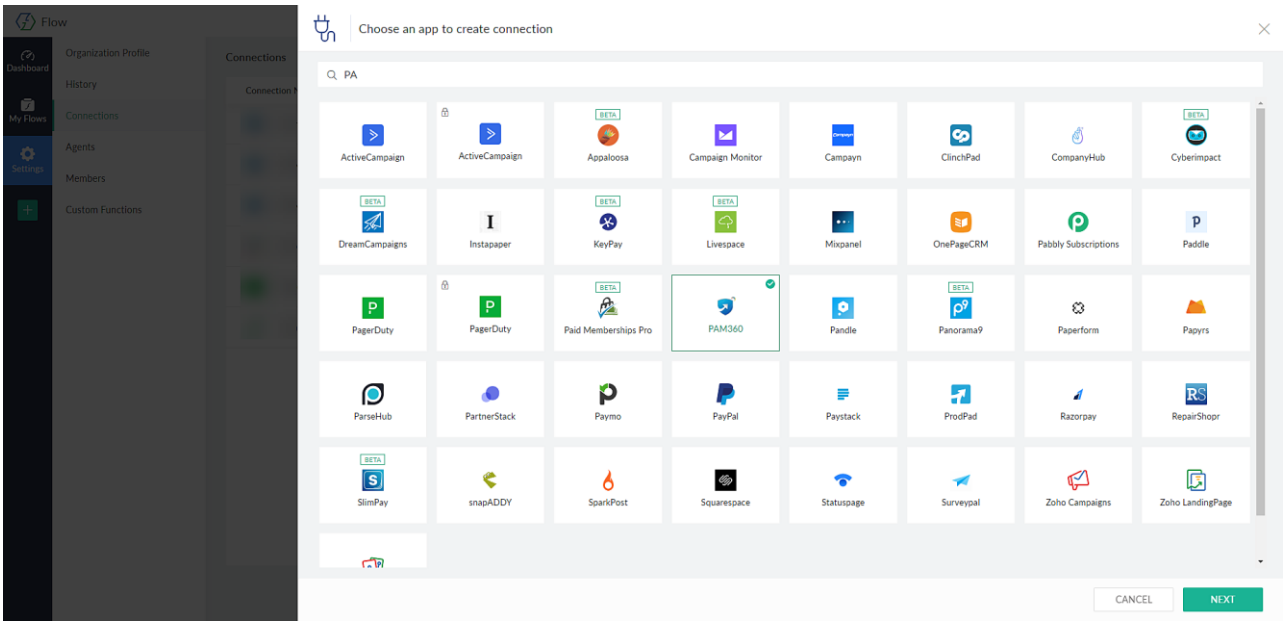
The first step to accessing PAM360 through Zoho Flow is to integrate PAM360 with the Zoho Flow application. The following steps educate you on creating a PAM360 connection in Zoho Flow and creating the required trigger events.

1. Steps to Integrate PAM360 with Zoho Flow

Login to the Zoho Flow application, navigate to the **Settings** section, and select **Connections**. From there, initiate the connection creation process by clicking on **CREATE CONNECTIONS**.



This action triggers a pop-up that presents an extensive list of applications available in Zoho Flow. In the search bar, look out for **PAM360**, then proceed to select the app and advance by clicking **Next**.

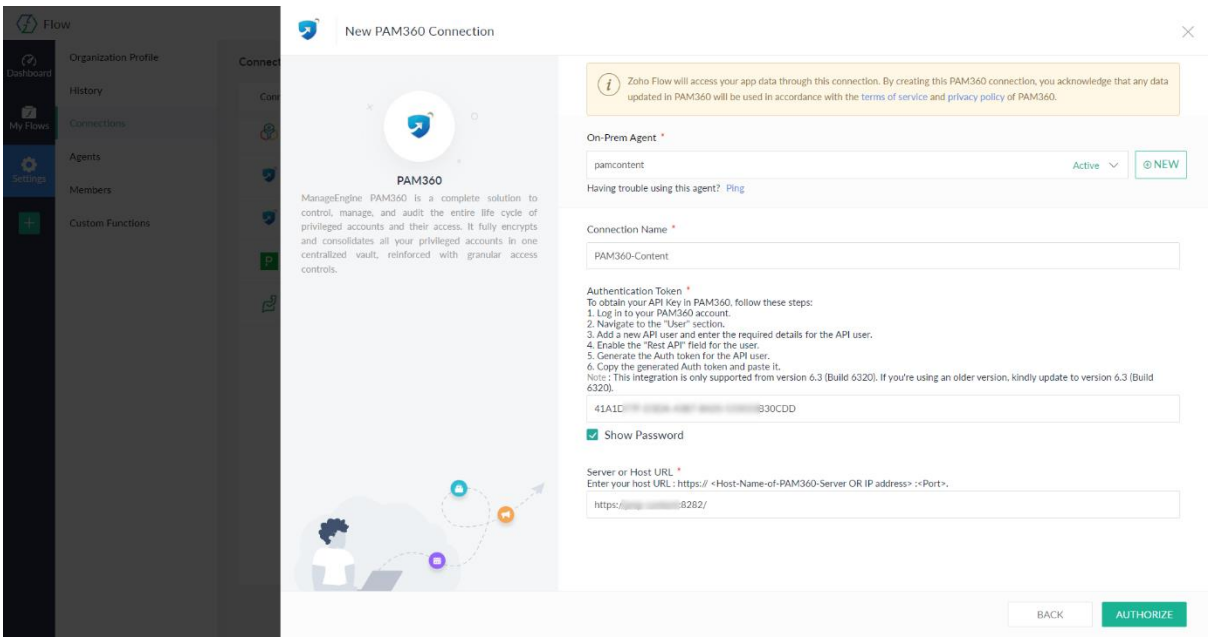


On the new page that appears,

Select the **On-Prem Agent** installed in the PAM360 server and enter a **Connection Name**.

Enter the **Authentication Token** of your PAM360 REST API user responsible for the further flow management, and enter the PAM360 application **Server or Host URL**.

Finally, click **AUTHORIZE** to complete.



Please note that the application integrating with PAM360 for automation capabilities should be added as a new connection in Zoho Flow. For this, navigate to **'Settings >> Connections >> CREATE CONNECTION'**.

2. Supported API Actions in PAM360 to Integrate with Other Applications via Zoho Flow

The following operations can be performed in PAM360 (via RESTful API call) with the assisted triggers available in the other applications in Zoho Flow without manual intervention.

Add user to user group
Create user
Fetch account
Fetch resource group
Fetch user
Fetch user group
Lock user
Share/revoke account to/from user
Share/revoke account to/from user group
Share/revoke resource group to/from user
Share/revoke resource group to/from user group
Share/revoke resource to/from user
Share/revoke resource to/from user group
Unlock user

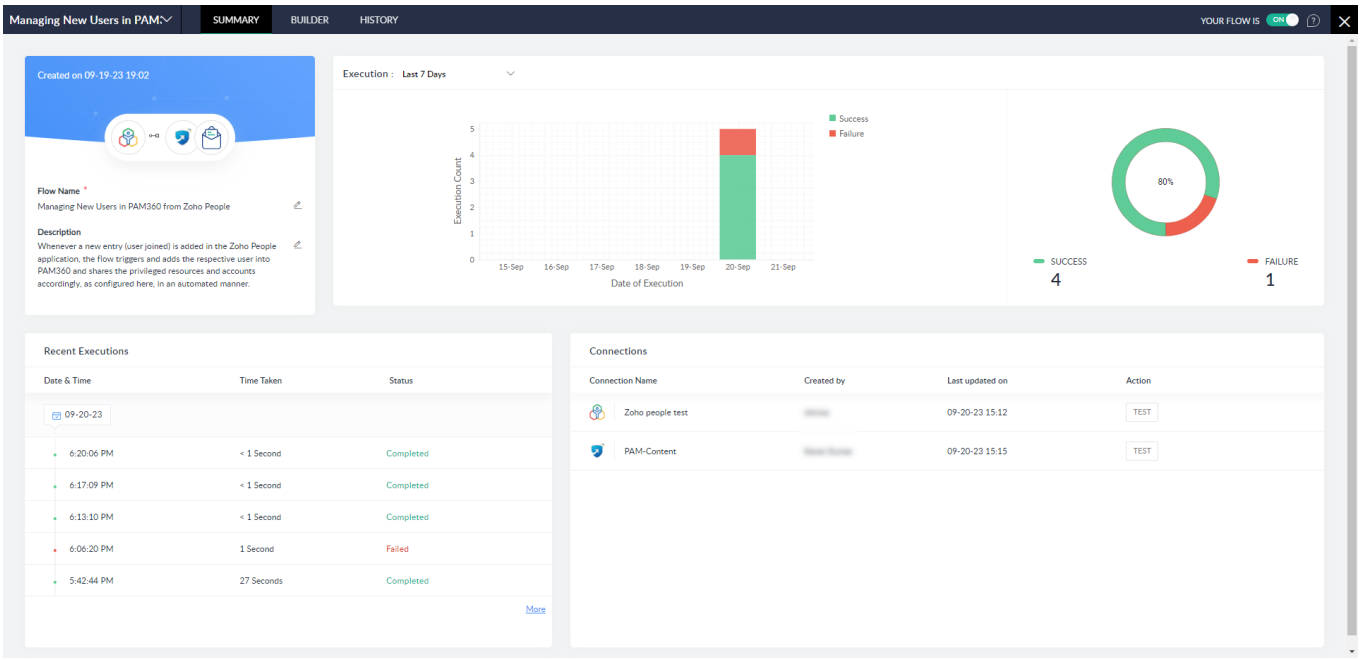
3. Creating a Flow with PAM360 and Other Applications

Refer to the upcoming help section - **How PAM360 Integration with Zoho Flow Aids in Real-Time?** for a detailed explanation of the flow creation process in Zoho Flow.

4. Flow Details and Management

After setting up a flow between PAM360 and an application in Zoho Flow, tasks will be automatically performed in PAM360 based on the respective triggers activated from the application. One can access the complete details of the tasks performed from the Summary tab of the flow dashboard, which includes:

1. Flow details
2. Connection details
3. Flow execution details based on the selected period
4. Recent executions with date and time stamps



Flow Rerun

There are two types of retry mechanisms for the failed flow executions.

Auto Rerun - For Zoho Flow internal errors and API errors from the application used in your connection.

Manual Rerun - Failed due to flow configuration or other similar errors.

Auto Rerun - Zoho Flow employs an automatic rerun mechanism following a task failure, aiming to pick up from the exact point of the previous error. The process continues at regular intervals if the executions continue to encounter issues. Failed tasks undergo a maximum of 8 retry attempts in 24 hours before being marked unsuccessful.

If you modify your flow before an upcoming rerun, all future reruns will adhere to the edited configuration. Turning off the flow between reruns halts the rerun process, but if you re-enable it before the next scheduled rerun, the process will resume.

Auto Rerun is not applicable under the following circumstances:

Triggers, including Webhook triggers and Real-time app triggers.
When a flow is switched off.
When a flow is deleted.
When the task has previously run successfully.

Manual Rerun - For manual reruns, Zoho Flow offers two options:

1. **Resume:** This choice allows for an immediate continuation of the flow execution from the point of failure.
2. **Restart:** This option initiates the flow execution from the beginning, starting from the task following the trigger. All steps, including successful ones, will be re-executed. However, this may lead to some actions failing, potentially resulting in duplicate entries and further errors, ultimately leading to failed executions. Please note that the restart will not function if significant changes have been made to the flow (such as altering the trigger or action) after the initial failure.

To manually rerun a failed execution:

- Log in to the Zoho Flow application.
- Navigate to the desired flow in **My Flows**, then click on the **History** tab. (You can also access your organization's flow history from **Settings >> History**.)
- Select the failed executions for rerun using the checkboxes.
- If you prefer to continue the execution from the step that originally failed, click on **Run** (the default option, **Resume**, will be selected). Alternatively, use the dropdown arrow next to **Run** and select **Restart** to initiate the flow executions from their triggers.

To know more about the rerun mechanism and other common problems that you might encounter in Flow creation and execution, refer to the below articles for comprehensive information.

How PAM360 Integration with Zoho Flow Aids in Real-Time?

The PAM360 integration with Zoho Flow enhances the PAM360 workflow automation capabilities through RESTful APIs. This, in turn, extends support for tasks like user management, account control, and secure sharing of privileged resources. Users can utilize this powerful combination for more productive and secure privileged access management workflows.

Please go on and read about how this integration helps organizations achieve real-time workflow automation.

Consider an organization with the below scenario -

- A vast number of employees shared with diverse nature of privileged resources based on their department, designation, and team requirements.
- The organization uses an HR tool (let's assume it is Zoho People) for user data management and PAM360 for IT assets and privileged resource management.

Organization requirements -

- Employees newly joined the organization should be added as users in PAM360 with the respective user groups.
- People with higher designations who join the organization should be added as users in PAM360 and shared with the privileged resources.
- Users from the third-party vendor should be added as users in PAM360 and shared with relevant resources for a limited period, and the access should be revoked after the allowed period.



With the above scenario, it will be hectic for the HR and IT people to govern the resources and account to the newly joined/third-party users. Here comes the PAM360 integration with Zoho Flow into play - it automates the entire resource allocation and revocation tasks based on the organization's needs and requirements.

1. Prerequisites to Create a Workflow in Zoho Flow

The Zoho Flow agent is to be installed.

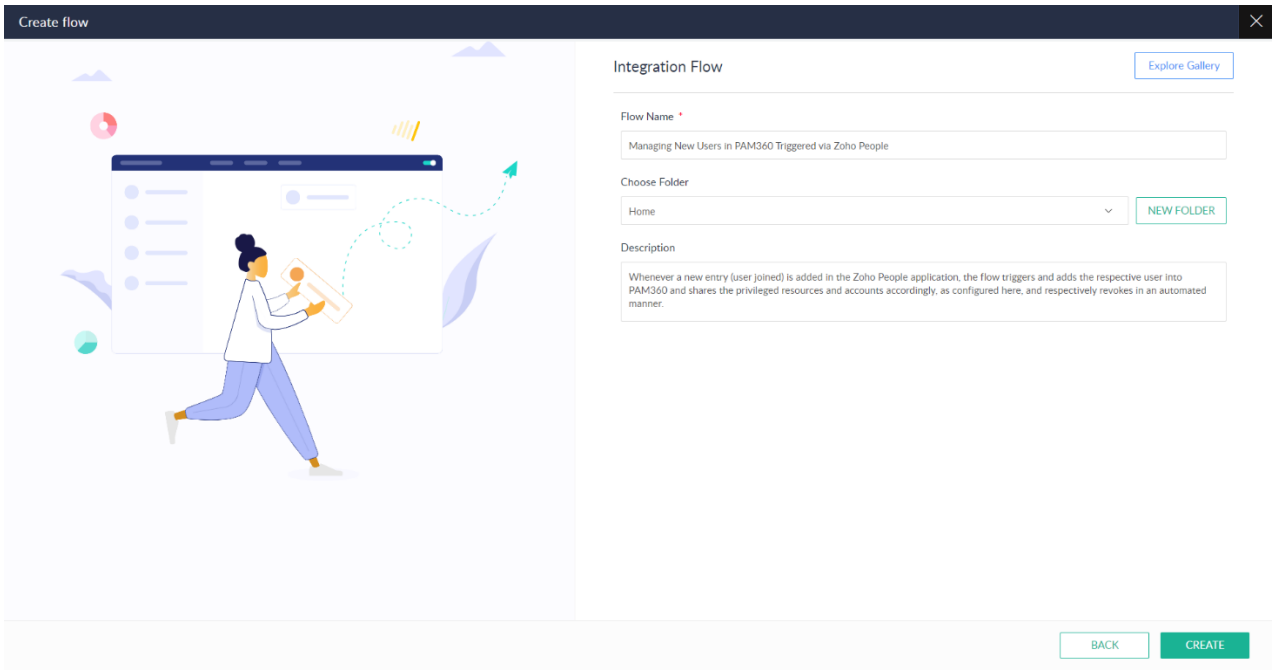
PAM360 and the respective application (here - Zoho People) are to be added as a connection in the Zoho Flow application.

2. Creating a Workflow in Zoho Flow

Navigate to the **My Flows** tab in the Zoho Flow application and click **+CREATE**.

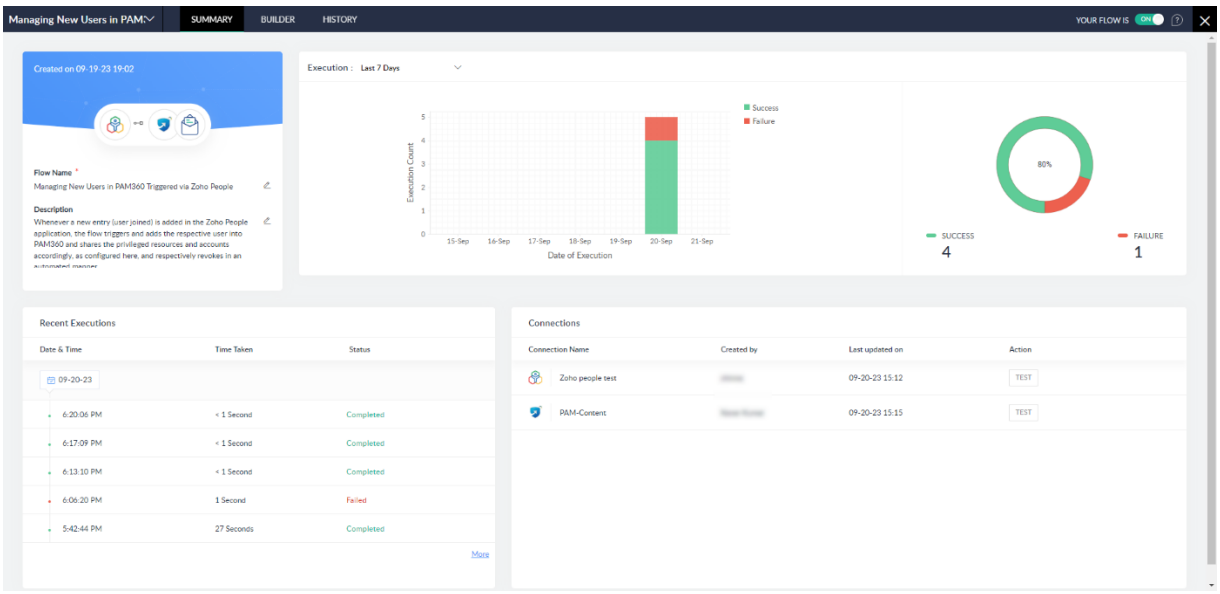
In the window that appears, Select the **Integration Flow** and click **NEXT**.

In the window that appears, enter the required basic information about the flow, such as flow name, location path, and description, and click **CREATE**.

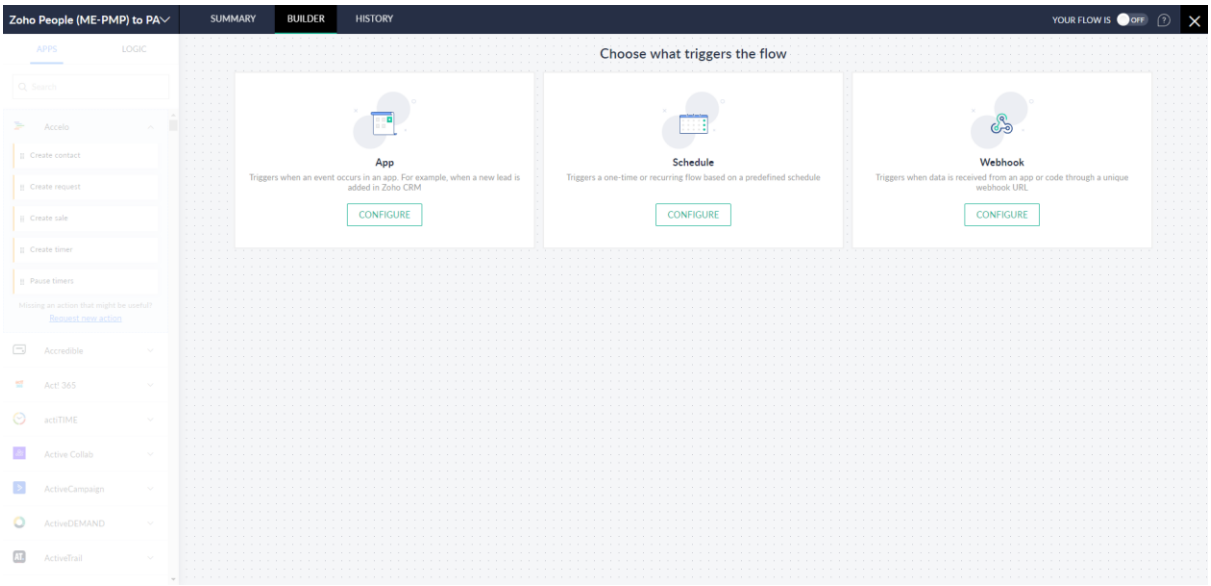


Now, a flow will be created successfully, and you will have access to three different tabs of the flow:

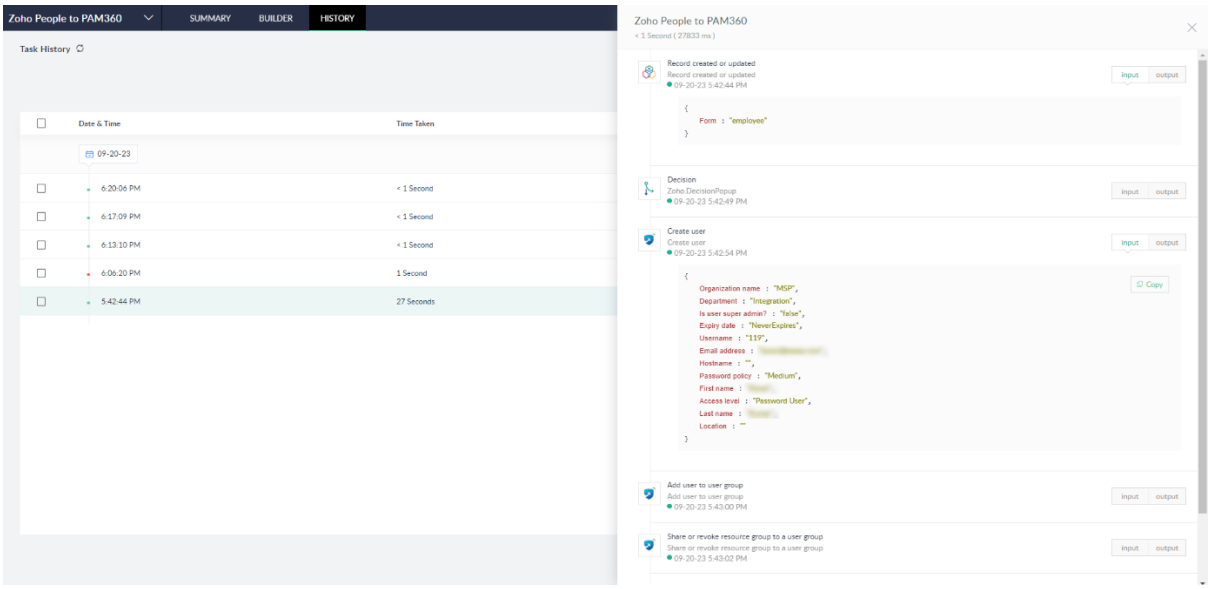
SUMMARY - This is where you will find the list of flow executions with the respective date, timestamps, and execution status.



BUILDER - Here, you will be crafting your required tasks that are to be automated with PAM360 and other applications in this flow.



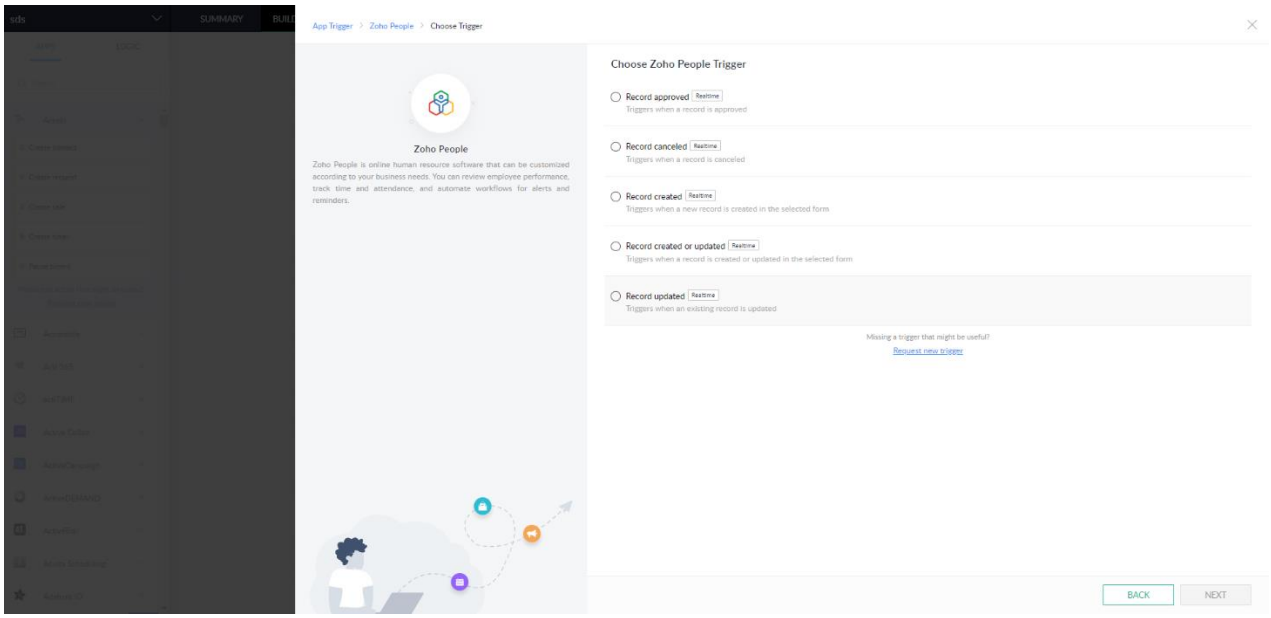
HISTORY - You will find here the comprehensive information of flows executed at each interval with their respective inputs and output details.



To create a flow from the **BUILDER** window, click **CONFIGURE** under the **App**. You can also configure **Schedule** triggers based on your requirements.

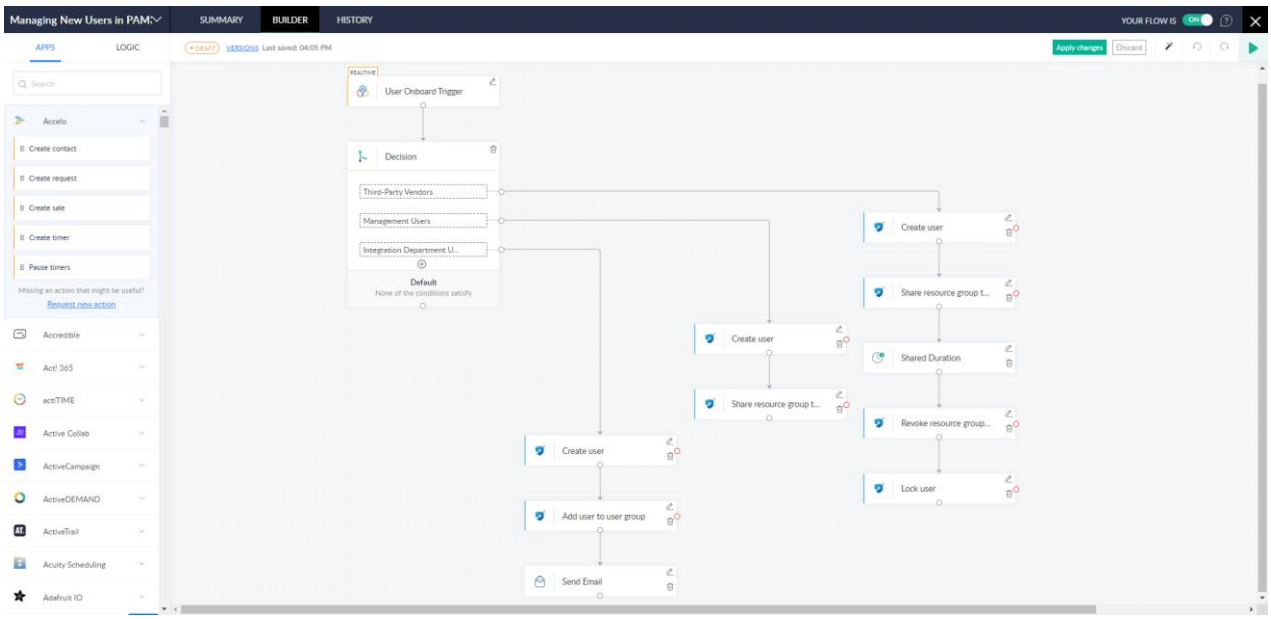
In the new page that slides over, select the application (here - **Zoho People**) to which the PAM360 is to be connected for automated user management capabilities.

Select the type of trigger that you need for managing the users between Zoho People and PAM360 (here - **Record created or updated**).



Now select the Zoho People connection that you created earlier, provide a variable name, and select the required form from the Zoho People application (here - **Employee**).

Now, using the **APPS** and **LOGIC** section from the left pane, create your flow accordingly and switch on the flow using the toggle button at the top right corner.

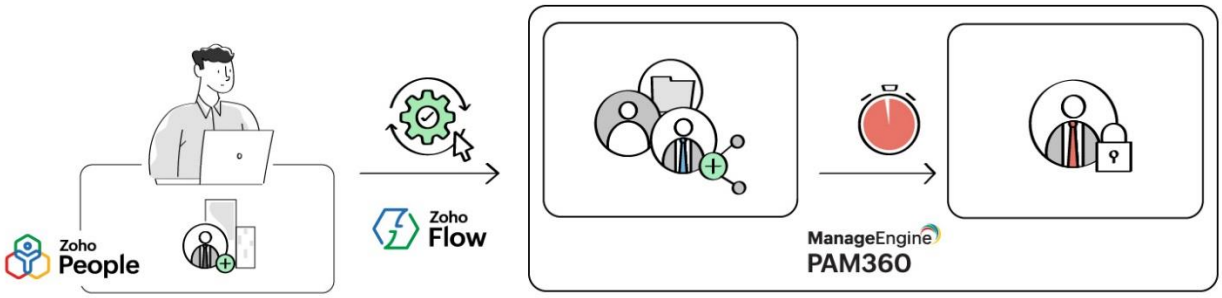


Refer to the Zoho Flow articles on flow creation for in-depth details.

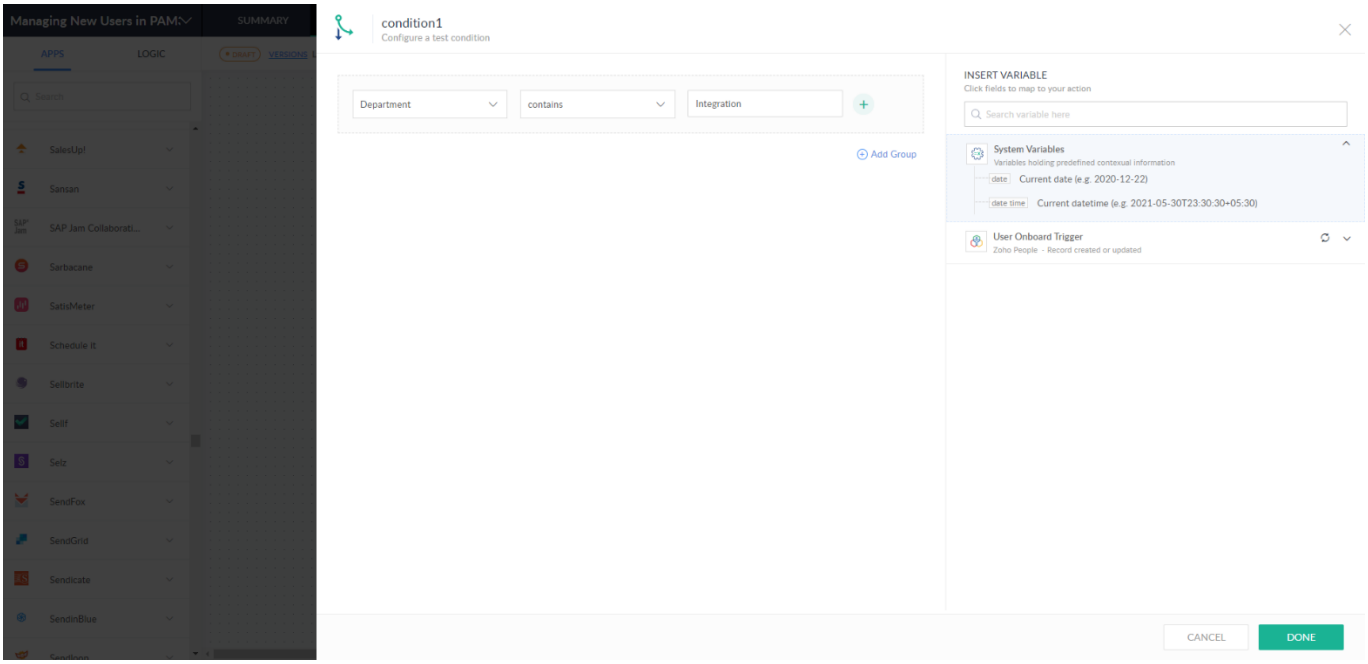
3. How does the above Flow Work for the Aforementioned Scenario?

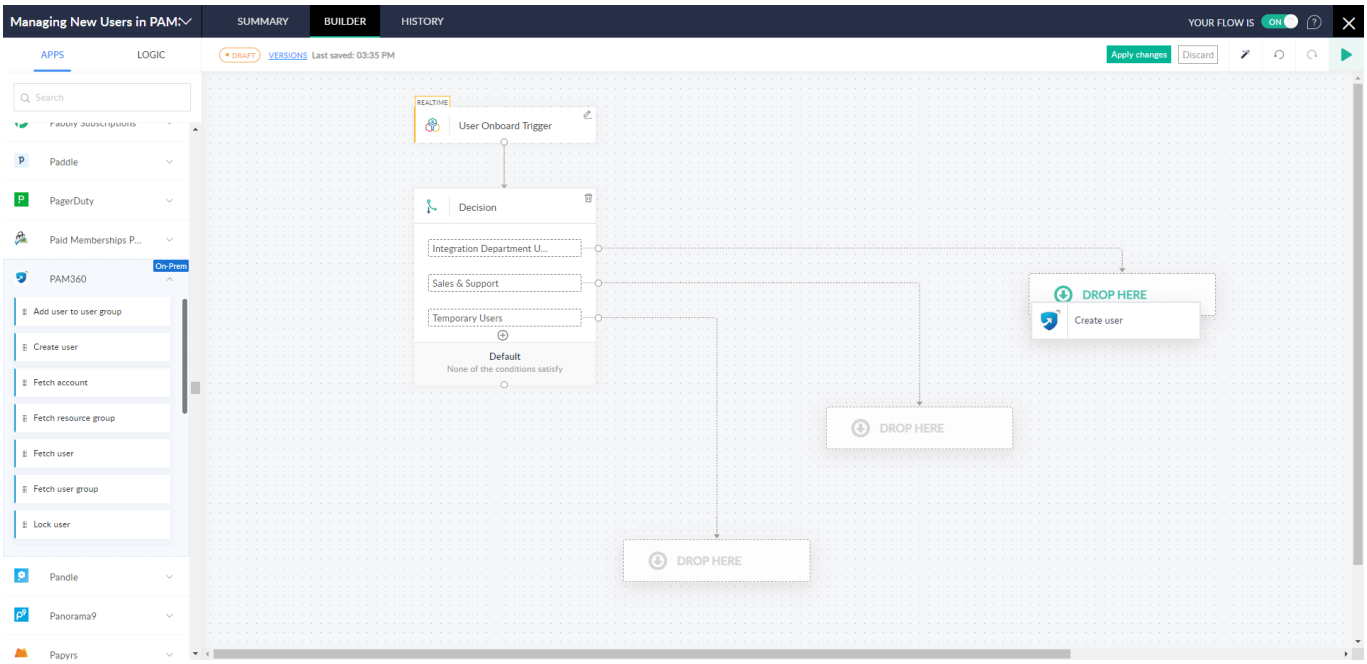
When a new user is added to the **Zoho People Employee's** form data, the flow trigger gets initiated. According to the flow's decision logic, it checks for the user department. If the

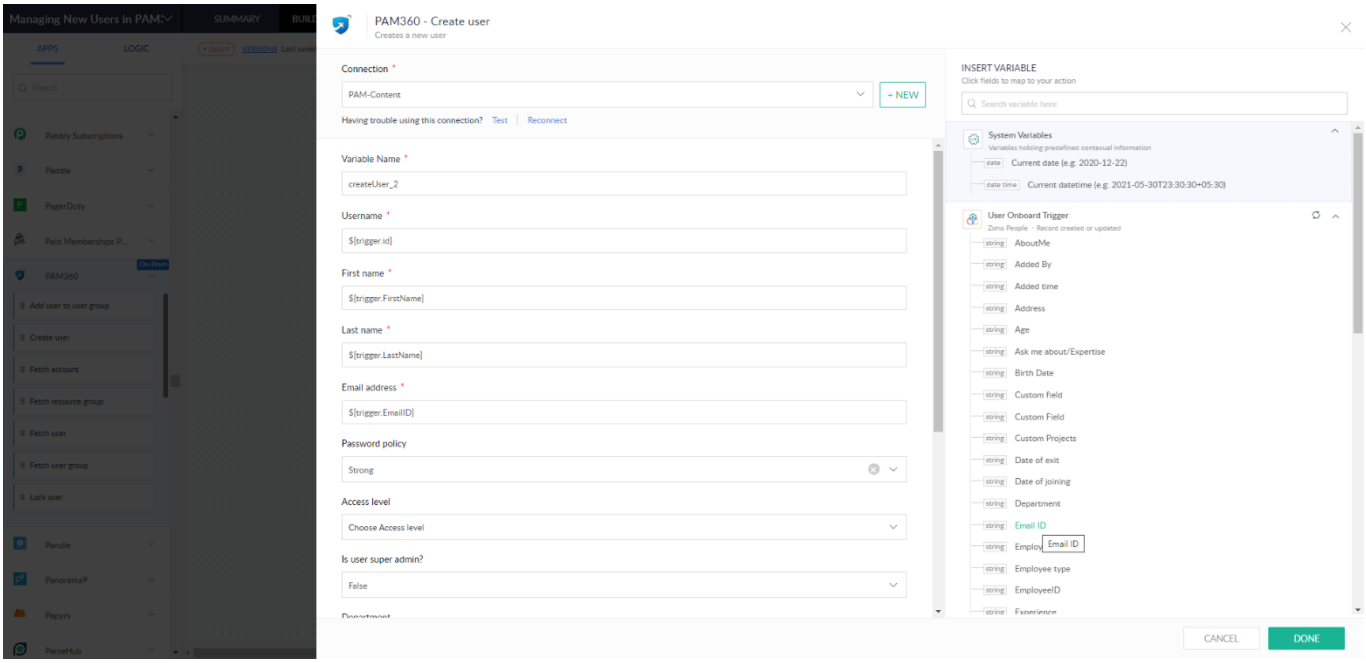
required conditions are satisfied, the user will be added to PAM360 and shared with the relevant privileged resources based on the flow attributes configuration.

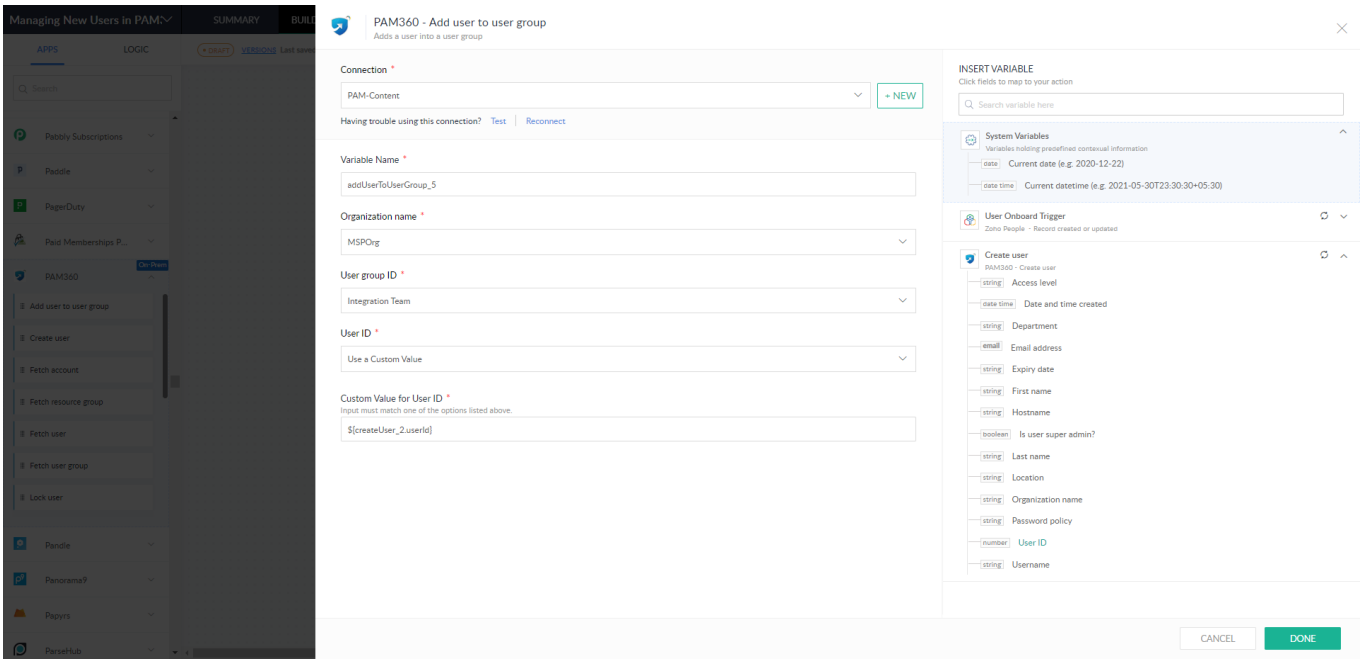


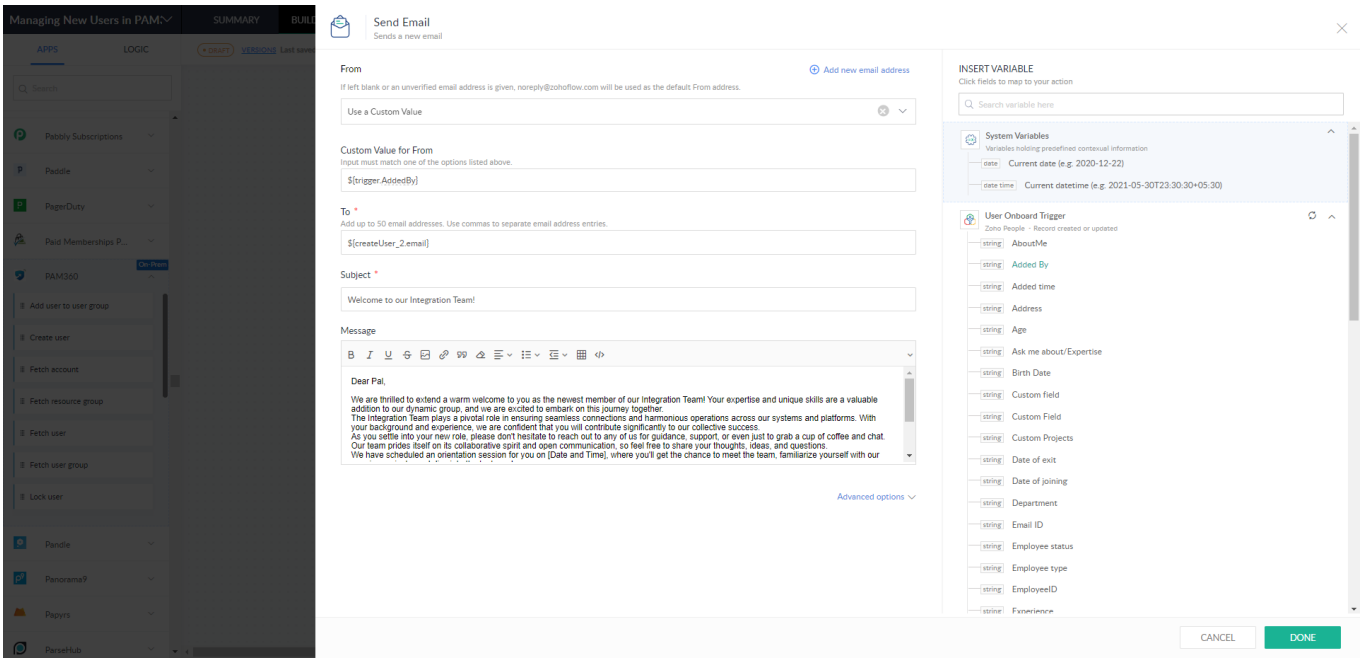
The below images are for the sample references for mapping the attributes for each task in the flow as per your requirement.

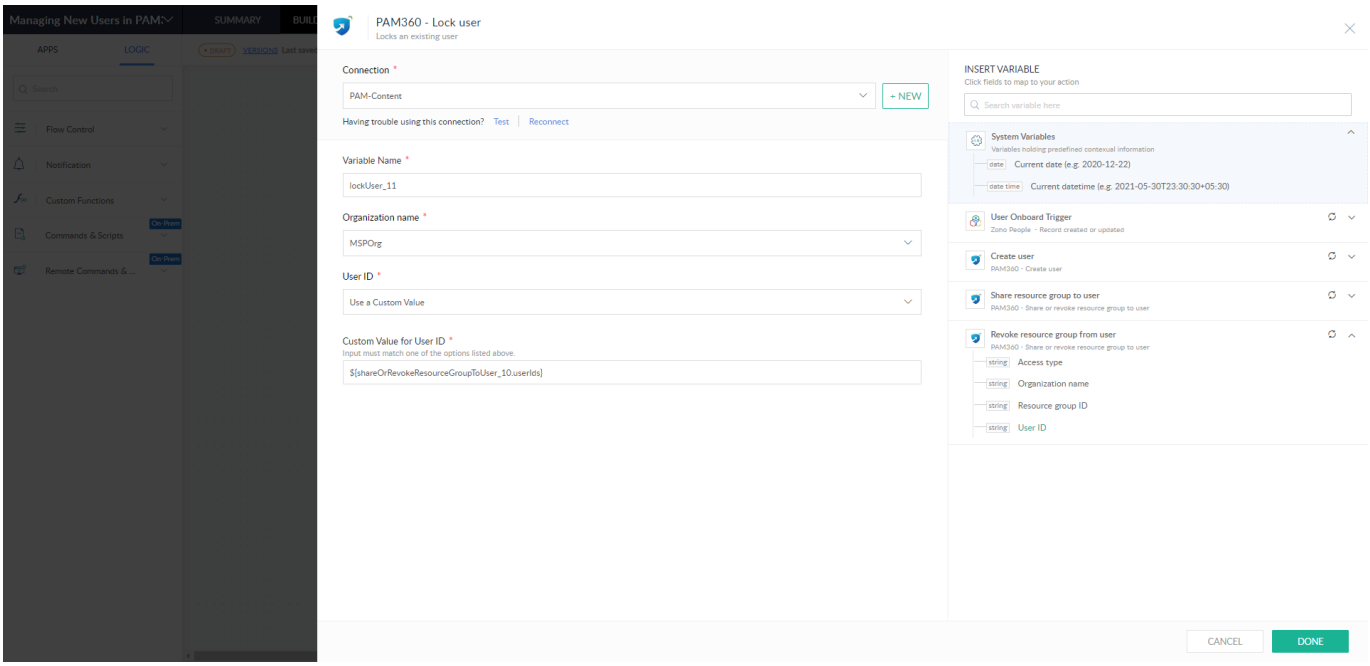



Managing New Users in PAM
SUMMARY
BUILDER
HISTORY
YOUR FLOW IS ON
APPS
LOGIC
DRAFT
VERSIONS Last saved: 03:35 PM
Apply changes
Discard
Search
Paddle
PagerDuty
Paid Memberships P...
PAM360
On-Prem
Add user to user group
Create user
Fetch account
Fetch resource group
Fetch user
Fetch user group
Lock user
Pandle
Panorama9
Papyrs
REALTIME
User Onboard Trigger
Decision
Integration Department U...
Sales & Support
Temporary Users
Default
None of the conditions satisfy
DROP HERE
Create user
DROP HERE
DROP HERE


PAM360 - Create user
Creates a new user
Connection *
PAM-Content
+ NEW
Having trouble using this connection? Test | Reconnect
Variable Name *
createUser_2
Username *
${trigger.id}
First name *
${trigger.FirstName}
Last name *
${trigger.LastName}
Email address *
${trigger.EmailID}
Password policy
Strong
Access level
Choose Access level
Is user super admin?
False
INSERT VARIABLE
Click fields to map to your action
Search variable here
System Variables
Current date (e.g. 2020-12-22)
Current datetime (e.g. 2021-05-30T23:30:30+05:30)
User Onboard Trigger
Zoho People - Record created or updated
AboutMe
Added By
Added time
Address
Age
Ask me about/Expertise
Birth Date
Custom field
Custom Field
Custom Projects
Date of exit
Date of joining
Department
Email ID
Employee type
EmployeeID
CANCEL
DONE


Managing New Users in PAM
SUMMARY
APPS
LOGIC
PAM360 - Add user to user group
Adds a user into a user group
Connection *
PAM-Content
+ NEW
Having trouble using this connection? Test | Reconnect
Variable Name *
addUserToUserGroup_5
Organization name *
MSPOrg
User group ID *
Integration Team
User ID *
Use a Custom Value
Custom Value for User ID *
Input must match one of the options listed above.
${createUser_2.userId}
INSERT VARIABLE
Click fields to map to your action
Search variable here
System Variables
Variables holding predefined contextual information
date Current date (e.g. 2020-12-22)
date time Current datetime (e.g. 2021-05-30T23:30:30+05:30)
User Onboard Trigger
Zoho People - Record created or updated
Create user
PAM360 - Create user
string Access level
date time Date and time created
string Department
email Email address
string Expiry date
string First name
string Hostname
boolean Is user super admin?
string Last name
string Location
string Organization name
string Password policy
number User ID
string Username
CANCEL
DONE


Managing New Users in PAM
SUMMARY
APPS
LOGIC
Send Email
Sends a new email
From
Add new email address
If left blank or an unverified email address is given, noreply@zohoflow.com will be used as the default From address.
Use a Custom Value
Custom Value for From
Input must match one of the options listed above.
${trigger.AddedBy}
To *
Add up to 50 email addresses. Use commas to separate email address entries.
${createUser_2.email}
Subject *
Welcome to our Integration Team!
Message
Dear Pal,
We are thrilled to extend a warm welcome to you as the newest member of our Integration Team! Your expertise and unique skills are a valuable addition to our dynamic group, and we are excited to embark on this journey together.
The Integration Team plays a pivotal role in ensuring seamless connections and harmonious operations across our systems and platforms. With your background and experience, we are confident that you will contribute significantly to our collective success.
As you settle into your new role, please don't hesitate to reach out to any of us for guidance, support, or even just to grab a cup of coffee and chat. Our team prides itself on its collaborative spirit and open communication, so feel free to share your thoughts, ideas, and questions.
We have scheduled an orientation session for you on [Date and Time], where you'll get the chance to meet the team, familiarize yourself with our
Advanced options
INSERT VARIABLE
Click fields to map to your action
Search variable here
System Variables
Variables holding predefined contextual information
date Current date (e.g. 2020-12-22)
date time Current datetime (e.g. 2021-05-30T23:30:30+05:30)
User Onboard Trigger
Zoho People - Record created or updated
string AboutMe
string Added By
string Added time
string Address
string Age
string Ask me about/Expertise
string Birth Date
string Custom field
string Custom Field
string Custom Projects
string Date of exit
string Date of joining
string Department
string Email ID
string Employee status
string Employee type
string EmployeeID
CANCEL
DONE



Similarly, as shown in this scenario, an organization can use this PAM360-Zoho Flow integration with the diversely available applications in Zoho Flow and create flows that reduce the tremendous human interventions in real-time using the available workflow automation methodology.

Configuring Different APIs

For applications and scripts in your infrastructure that communicate with other applications using a password, you no longer have to hard-code the password in a configuration file or a script. They can securely query PAM360 to retrieve the password whenever they need, so that administrators are free to apply good practices like periodic rotation to such passwords as well, without worrying about having to update them manually in many places.

Here in this section you will learn about the following topics:

1. Prerequisites to Configure the APIs
2. Workflow of the Steps involved in API Management
3. Types of APIs Supported
4. Command Line Interface (CLI) for Scripts Over Secure Shell (SSH)
5. RESTful API

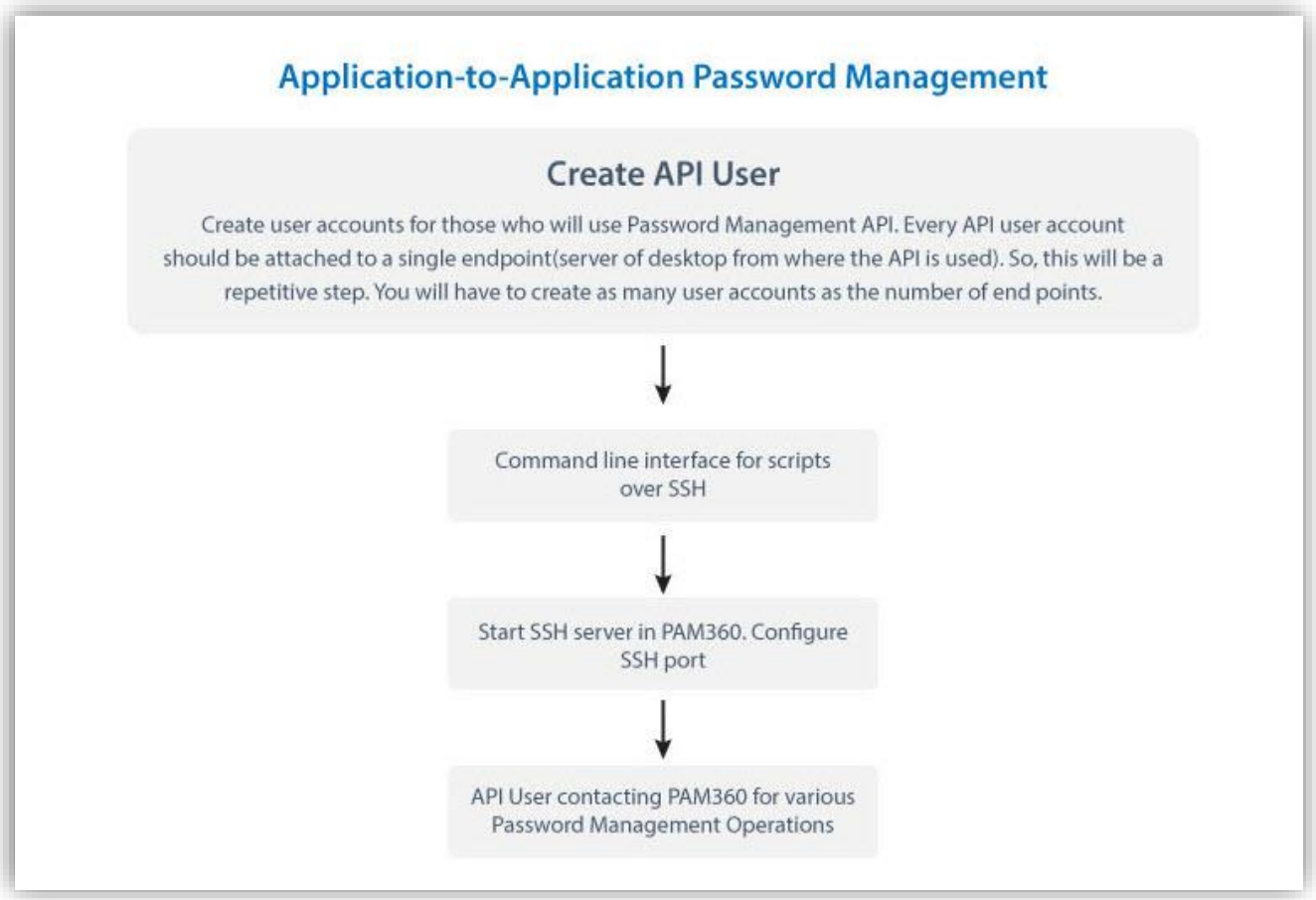
1. Prerequisites to Configure the APIs

The following are the important points to be assured before configuring and using the APIs:

- User accounts that use only the PAM360 APIs have to be created in PAM360. Every API user account should be attached to a single endpoint (server or desktop from where the API is used, so the user accounts are uniquely identified as user@hostname).
- An API user can use either the SSH CLI, or the RESTful APIs.
- The **SSH CLI** users are authenticated using PKI authentication. So, the following should be supplied to each user, depending on the type of API used:
    - ➤ An OpenSSH format public key, corresponding to the private key of user@host, for using SSH CLI.
- PAM360 has built in SSH server that can be configured to run on specific ports.
- Once the API users are created and the SSH servers is enabled, PAM360 is ready to serve the API users.
- Administrators can provide access to passwords to API users in the same way as it is done for other users. API users can only access passwords that they have permission to, through the API.

2. Workflow of the Steps involved in API Management

The following diagram illustrates the summary of steps involved in API management in PAM360:



3. Types of APIs Supported

PAM360 provides two API flavors:

1. Command Line Interface (CLI) for scripts over secure shell (SSH)
2. RESTful API

The SSH CLI use PKI authentication for allowing access to the PAM360 application through the API.

4. Command Line Interface (CLI) for Scripts Over Secure Shell (SSH)

Setting up CLI for Scripts over SSH involves the following steps:

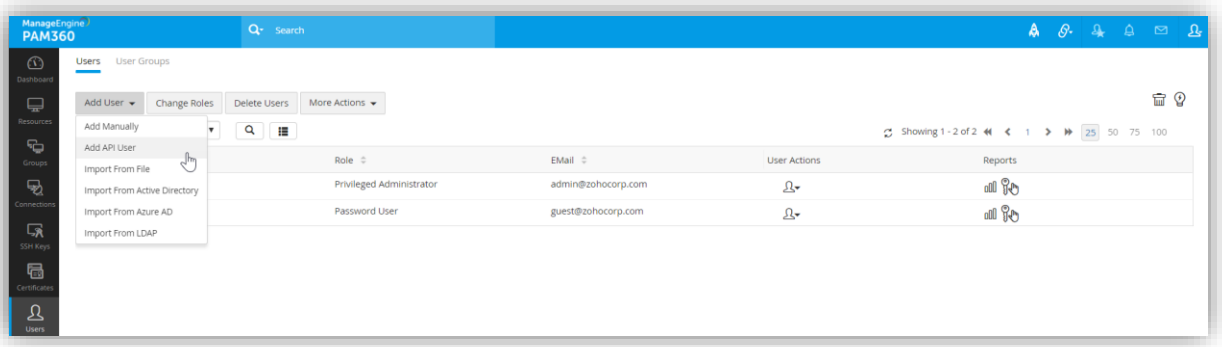
1. **Creating API User Accounts in PAM360.**
2. **Configurations on the Server Side and Starting the SSH Server.**
3. **Configurations on the Client Side to Enable Applications Access to PAM360.**

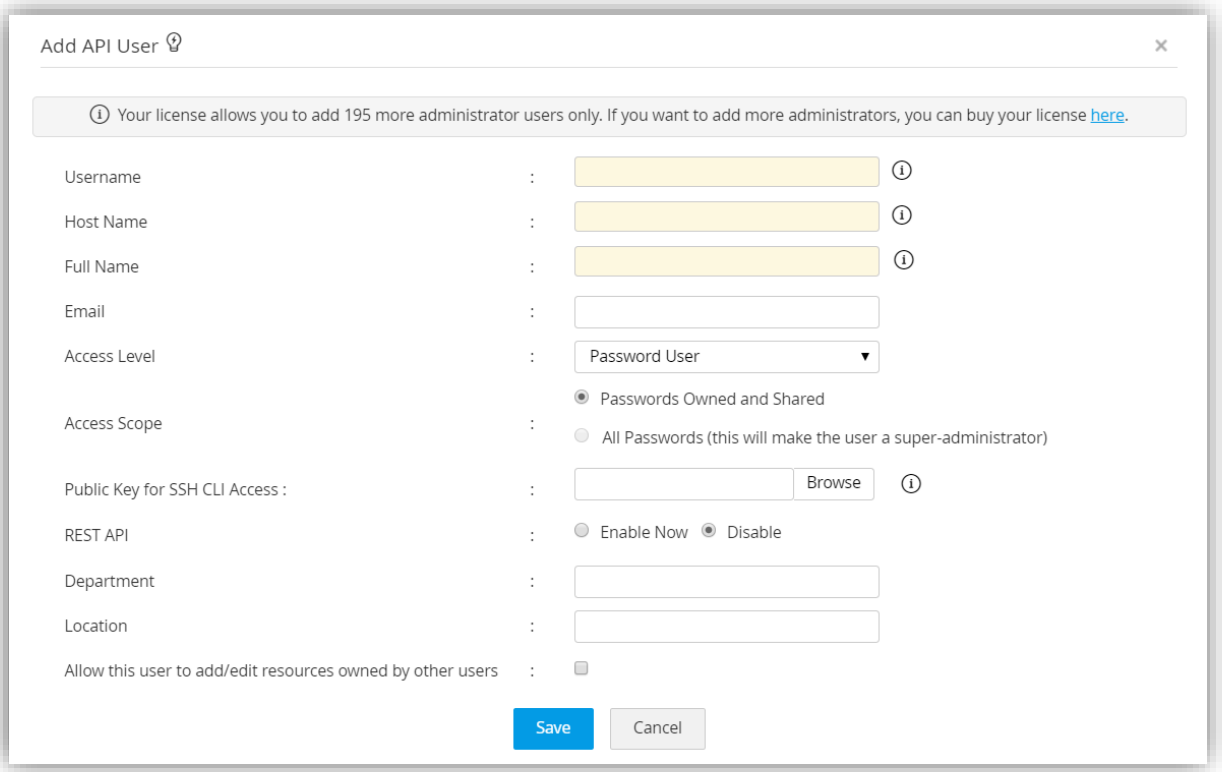
4.1 Creating API User Accounts in PAM360

This is the first step in the process to configure and use password management APIs for Application-to-Application Password Management. As mentioned above, user accounts have to be created in PAM360 to those who will use only the password management API. Every API user account should be attached to a single endpoint (server or desktop from where the API is used, so the user accounts are uniquely identified - for example, as user@hostname)

To create an API user account:

1. Navigate to **Users** tab.
2. Click **Add User** and select **Add API User** from the drop down.





3. Enter the user name in the respective text field. This name identifies the API user. It is

important that the same name should be used as the 'Common Name' (CN) in the corresponding SSL certificate. In MSP edition, in addition to the 'Common Name'(CN), the Organization Name (O) in the certificate should be same as the organization display name in PAM360.

4. Enter the name of the host from where the API user would access PAM360 for password management operations. Internally, the user name and the host together is used to uniquely identify the API user. For example, a user with the name 'test' from the host 'test-server' will be considered as 'test@test-server' to uniquely identify the API user.
5. 'Full Name' refers to the name with which the API user would be identified in the external world. That means, in reports, audit trails and such other places where activities are traced to users. By default, the 'User Name' - 'Host Name' combination with the suffix "API User" is used as 'Full Name'. In the above example, it will be test@test-server - API User. However, if you want to have a different name, you are free to define that.
6. You can use **Access Scope** to change an Administrator/Password Administrator/Privileged Administrator into a Super Administrator by choosing the option **All Passwords in the system.** When you do so, they will be able to access all passwords in PAM360 without any restriction. Conversely, a Super Administrator can be changed to his earlier role of Administrator/Password Administrator/Privileged Administrator by choosing the option **Passwords Owned and Shared.**
7. SSH connects and logs into the specified host with the user name specified above. The user must prove his identity to the remote machine using public key authentication. If you wish to make use of the SSH CLI access, browse and select the open SSH format public key of the CLI user.

   If you want to create SSH format private-public key afresh,

   a. Open a command prompt and run the command ssh-keygen.
   b. By default, the private key is stored in id_rsa file. The public key is stored in id_rsa.pub. These two files are stored under the directory specified in the command prompt by default.
   c. If you want, you can store them under a different location. You need to import the id_rsa.pub. It will be stored in PAM360 under <PAM360_HOME>/<user name>/.ssh/authorized_keys]
   d. If you want to have an extra layer of security, you can use passphrase on the SSH key. Once you enter and confirm a passphrase, the passphrase is added to the key. You will have to enter the passphrase everytime when you use the SSH key.
   e. Once you generate the key, specify the location of the public key. (browse and locate in the user addition GUI)
   f. The following snapshot explains the above sequence:

- Generating public/private rsa key pair.
- Enter file in which to save the key (/home/xyz/.ssh/identity): /home/xyz/.ssh/pam360_identity
- Enter passphrase (empty for no passphrase): *enter your passphrase here*
- Enter same passphrase again: *repeat your passphrase*
- Your identification has been saved in /home/xyz/.ssh/pam360_identity.
- Your public key has been saved in /home/xyz/.ssh/pam360_identity.pub.
- The key fingerprint is:

  22:71:3c:ff:7e:df:59:ad:72:47:d1:16:bd:e2:e9:2d xyz@xyz

The above example shows how to generate the key pair using open SSH. You may use any other standard tool to generate the keys as you wish.

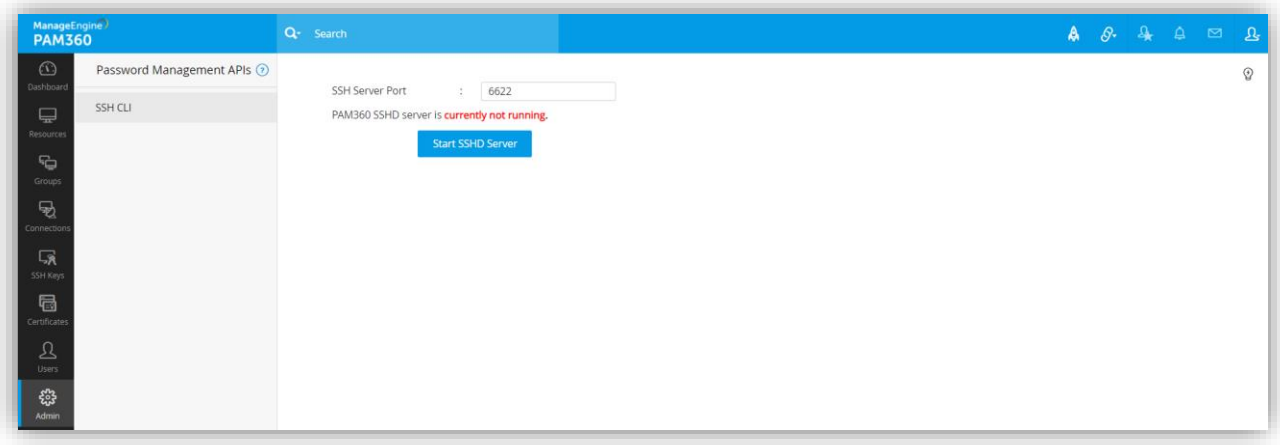
Note: The API user creation is specific to the host from where the application would contact PAM360 for passwords. That means, user and host are tied with other. If you want to make use of Password Management API from more than one host, you need to create as many API users as the number of hosts. Conversely, if you wish to have many users on a single host, then again you need to create as many API users as needed.

4.2 Configurations on the Server Side and Starting the SSH Server

PAM360 comes with an inbuilt SSH server. By default, it occupies 6622. You may configure it to run on any other desired port, if you wish to do so. You need to start the SSH server.

To configure the SSH server port and to start it,

1. Navigate to **Admin >> Configuration >> Password Management API.**
2. In the UI that opens, select **SSH-CLI** from the left pane.



3. Edit the **SSH-CLI server port** and click **Start SSHD Server**.

4.3 Configurations on the Client Side to Enable Applications Access to PAM360

Once you have created API users and also started SSH server in PAM360, API users can access PAM360 for the passwords that are allotted to them. Note that the ownership and sharing mechanism of PAM360 applies in the case of API users too. That means, the API users will be able to access only those passwords that are allotted to them. Using Password Management APIs, users can retrieve, modify and create accounts.

How does Password access workflow on the client-side work?

Each user creates SSH public-private key pair for authentication purposes. The server knows the public key and the user knows the private key. The file <PAM360_HOME>/<user name>/.ssh/authorized_keys lists the public keys that are permitted for logging in. When the user logs in, the SSH program tells the server which key pair it would like to use for authentication. The server checks if this key is permitted, and if so, sends the user a challenge, a random number, encrypted by the user's public key. The challenge can only be decrypted using the proper private key. The user's client then decrypts the challenge using the private key, proving that user knows the private key but without disclosing it to the server. Once the authentication is successful, the user is permitted to do password management operations.

API User Contacting PAM360 for various password operations

As explained above, the API users will be allowed to access PAM360 for password retrieval and other operations only from the host in which they were configured to function. That is, during user creation, you would have entered the name of the host from where the API user would access PAM360 for password management operations. The API user will be allowed to access PAM360 only from the specified host.

To retrieve passwords or to do any other password management operation, the applications running in the host should access the SSH server that runs with PAM360. The SSH server, in turn, connects to PAM360 for password operations.

The SSH server can be accessed using any standard openSSH command. As explained below, along with the command, you need to append PAM360-specific commands to carry out the required password management operations.

ssh **-q** [-p port] user@hostname [-i private_key] **[PAM360 specific command]**

Example:

ssh -q -p 6622 test@test-server -i /home/guest/id_rsa [PAM360 specific command]

For MSP Edition use the below command:

ssh **-q** [-p port] ORGNAME/user@hostname [-i private_key] **[PAM360 specific command]**

Example:

ssh -q -p 6622 MANAGEENGINE/test@test-server -i /home/guest/id_rsa [PAM360 specific command]

4.3.1 PAM360 specific commands to be included in your application for application-to-application password management:

For automatic A-to-A password management, you need to use specific commands in your application invoking the API. Use the give commands for the following operations:

1. **For Password Retrieval**
2. **For Password Reset**
3. **For Creating a New Resource and a User Account**

1. For Password Retrieval

ssh **-q** [-p port] user@hostname [-i private_key] RETRIEVE --resource=**<RESOURCE NAME As present in PAM360>** --account=**<ACCOUNT NAME As Present in PAM360>** --reason=**<REASON For Password Access>** --ticketid=**<TICKET ID For Password Access>**

Example:

ssh -q -p 6622 test@test-server -i /home/guest/id_rsa RETRIEVE --resource=test-server --account=root --reason=Testing password retrieval using ssh client API --ticketid=7

2. For Password Reset

2.1 **For Local Password Reset:**

ssh -q [-p port] user@hostname [-i private_key] RESET_LOCAL --resource=<RESOURCE NAME AS PRESENT IN PAM360> --account=<ACCOUNT_NAME As Present in PAM360> --newpassword=<NEW PASSWORD> --reason=<Reason for Password Reset> --ticketid=<TICKET ID For Password Reset>

Example:

ssh -q -p 6622 test@test-server -i /home/guest/id_rsa RESET_LOCAL --resource=test-server --account=root--newpassword=rootnew --reason=Rotating Password --ticketid=7

2.2 For Remote Password Reset:

ssh -q [-p port] user@hostname [-i private_key] RESET_REMOTE --resource=<RESOURCE NAME AS PRESENT IN PAM360> --account=<ACCOUNT_NAME As Present in PAM360> --newpassword=<NEW PASSWORD> --reason=<Reason for Password Reset> --ticketid=<TICKET ID For Password Reset>

Example:

ssh -q -p 6622 test@test-server -i /home/guest/id_rsa RESET_REMOTE --resource=test-server --account=root --newpassword=rootnew --reason=Rotating Password --ticketid=7

3. For Creating a New Resource and a User Account

ssh -q [-p port] user@hostname [-i private_key] CREATE --resource=<RESOURCE NAME To Be Created> --account=<ACCOUNT NAME to be created>--newpassword=<PASSWORD of the Account being added> --resourcetype=<Type of the Resource Being Added> --notes=<Reference Notes>

Example:

ssh -q -p 6622 test@test-server -i /home/guest/id_rsa CREATE --resource=testresource --account=testaccount --newpassword=test password--resourcetype=Windows --notes=A New resource is added

Refer to this document for more details.

Troubleshooting Tips

1. When I executed the above command, I did not get any response from PAM360.

Remove the -q option in the above commands. You will receive warning/error messages on the screen.

For example, to retrieve password, execute the command as:

ssh [-p port] user@hostname [-i private_key] RETRIEVE --resource=<RESOURCE NAME As present in PAM360> --account=<ACCOUNT NAME As Present in PAM360> --reason=<<REASON For Password Access>

Contact PAM360 support with the message you see on the screen.

2. When I try to retrieve a password from PAM360 Secondary Server in High Availability mode, I do not get the required password

Every time after adding a new API user, the entire **sshd** folder available under <PAM360_Primary_Installation_Folder> has to be copied and pasted under **<PAM360_Secondary_Installation_Folder>**. If this is done, you will be able to access the passwords from PAM360 Secondary.

4.3.2 Accessing PAM360 Secondary for A-to-A Password Management (HA Mode - SSH CLI)

If you have configured high availability setup in PAM360, when the Primary Server goes down, applications can seamlessly connect to the Secondary for A-to-A Password Management. For this to work, you need to make the following simple configuration:

1. Go to **<PAM360_Primary_Installation_Folder>.**
2. Copy the **'sshd'** directory and paste it under **<PAM360_Secondary_Installation_Folder>**.

> **Important Note:** The sshd folder has to be copied and pasted as explained above every time you create a new API user.

As mentioned earlier, PAM360 comes with an inbuilt SSH server. It has to be started in the PAM360 secondary installation as explained below:

If you have configured high availability setup in PAM360, when the Primary Server goes down, applications can seamlessly connect to the Secondary for A-to-A Password Management. For this to work, you need to make the following simple configuration:

1. Stop PAM360 Primary Server.
2. Connect to PAM360 Secondary's Web-Interface.
3. Go to **Admin >> Configuration >> Password Management API >> SSH CLI.**
4. Change the SSH-CLI server port, if you want to (by default it occupies 6622).
5. Click **Start SSHD Server.**

4.3.3 Commands for accessing PAM360 Secondary Server

For automatic A-to-A password management, you need to use the following commands in your application:

1. For Password Retrieval:

ssh **-q** [-p port] user@**PAM360_Secondary_hostname** [-i private_key] RETRIEVE --resource=<RESOURCE NAME As present in PAM360> --account=<ACCOUNT NAME As Present in PAM360> --reason=<REASON For Password Access>

Example:

*ssh **-q** -p 6622 **test@test-secondary-server** -i /home/guest/id_rsa RETRIEVE --resource=**test-server** --account=**root** --reason=**Testing password** retrieval using ssh client API*

Once the above configuration is done, password access in high availability mode will be seamless. However, as write operations are not permitted when Primary Server is down, applications would only be able to RETRIEVE passwords. They will not be allowed to carry out password reset and resource/account creation.

RESTful API

Introduction

PAM360 APIs allow you to connect, interact and integrate with PAM360 directly. The APIs belong to the REpresentational State Transfer (REST) category. PAM360 APIs use the GET, PUT, and POST methods to offer a wide range of operations such as creating resources and adding accounts to them, adding SSL certificates and SSH keys, associating SSH keys with resources, retrieving passwords, retrieving resource/account details, updating passwords programmatically, sharing resources/accounts to users and so on.

Prerequisite

Creating API user accounts is the first step in the process of configuring RestAPIs for Application-to-Application password management. Click here to know how to create an API user account.

APIs Summary

Methods Used to Invoke APIs

GET

To fetch resources, accounts, passwords, account/resource details

PUT

To change a password

POST

To create new resource and accounts

How to Make Use of the APIs?

Invoking the APIs

The APIs can be invoked via HTTP POST, GET and PUT requests. All parameters in the request should be form-urlencoded. For all the APIs you need to pass the AUTH token, which is mandatory.

Supported Format

PAM360 supports the **JSON** format and the URL structure for it is given below:

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

PAM360 provides a wide range of APIs to:

1. Get the Resources Owned and Shared to a User
2. Get the Accounts that are Part of a Resource
3. Get Details of an Account
4. Get the Password of an Account that is Part of a Resource
5. Change the Password of an Account
6. Create a New Resource
7. Get the Account ID and Resource ID
8. Get the Resource ID using the Resource Name
9. Delete a Resource in PAM360
10. Request Password Approval by the Admin
11. Get the List of Password Requests
12. Reject a Password Request
13. Approve a Password Request
14. Check-in the Password Approved by the Admin
15. Checkout the Password Approved by the Admin
16. Generate Password
17. Create a New User
18. Edit Resources
19. Delete an Account Under a Specific Resource
20. Get License Keys, Files, Digital Certificates, Documents, Images, etc.
21. Create Accounts Under a Specific Resource

22. Edit an Account Under a Specific Resource
23. Delete a User
24. Create an API User
25. Create a New SSH Key
26. Delete an SSH Key
27. Fetch all the SSH keys
28. Fetch a Particular SSH Key
29. Export an SSH Key
30. Get SSH Keys for a User
31. Fetch All Associated Users
32. Get an SSL Certificate
33. Get all SSL Certificates
34. Get all SSL Certificate Expiry
35. Get SSL Certificate Details
36. Get SSL Certificate Keystore
37. Get SSL Certificate Passphrase
38. Add an SSL Certificate
39. Delete an SSL Certificate
40. Perform SSL Certificate Discovery
41. Perform SSL Certificate Discovery (for a range of IP addresses)
42. Create CSR
43. Get CSR List
44. Sign CSR
45. Create SSL Certificate
46. Get the ID of a User
47. Delete a User with their Username
48. Add a User to a User Group
49. Lock a User
50. Unlock a User
51. Import an SSH Key
52. Associate an SSH Key
53. Dissociate an SSH Key
54. Create Static and Dynamic Resource Groups

55. Get Audit Details
56. Share a Resource to a User
57. Share an Account to a User
58. Share a Resource to a User Group
59. Share an Account to a User Group
60. Fetch User Group ID
61. Configure Remote Password Reset for Linux Resources
62. Deploy an SSL Certificate
63. Share SSL Certificate to User
64. Share SSL Certificate to User Group
65. Share SSL Certificate Group to User
66. Share SSL Certificate Group to User Group
67. Revoke SSL Certificate from User
68. Revoke SSL Certificate from User Group
69. Revoke SSL Certificate Group from User
70. Revoke SSL Certificate Group from User Group
71. Create SSL Certificate Group
72. Delete SSL Certificate Group
73. Edit SSL Certificate Group
74. Generate an Agent Install Key
75. Get Password Policies
76. Get all Resource Types
77. Associate a Resource to a Resource Group
78. Dissociate a Resource from a Resource Group
79. Fetch Resource Groups Associated to a Resource
80. Delete a Resource Group
81. Fetch Resource Group ID
82. Reset Two-Factor Authentication

Note: Please note that each API call made to the PAM360 server requires the authentication token (AUTHTOKEN) to be passed in the **request header** only.

1. Get the Resources Owned and Shared to a User

Description

To get the list of resources which are owned by or shared to an API user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources
```

Sample Output

In the output (as shown in the sample below), you will get all the resources owned and shared by the specific API user.

{ "operation" : { "name" : "GET RESOURCES" , "result " : { "status" : "Success", "message" : "Resources fetched successfully" }, "totalRows":3, "Details": { { "RESOURCE DESCRIPTION":"CentOS Machine", "RESOURCE NAME":"CentOS Machine", "RESOURCE ID":"301", "RESOURCE TYPE":"Linux", "NOOFACCOUNTS" : "3" }, { "RESOURCE DESCRIPTION":"Cisco IOS Device", "RESOURCE NAME":"Cisco IOS Device", "RESOURCE ID":"302", "RESOURCE TYPE":"Cisco IOS", "NOOFACCOUNTS":"2" }, { "RESOURCE DESCRIPTION":"Weblogic Data Source Password", "RESOURCE NAME":"WebLogic Server", "RESOURCE ID":"303", "RESOURCE TYPE":"WebLogic Server", "NOOFACCOUNTS":"2" } } } }

2. Get the Accounts that are Part of a Resource

Description

To get the list of accounts and resource details present in the resource. Resource ID can be obtained from the GET RESOURCES API (explained above).

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/303/accounts
```

Sample Output

In the output (as shown in the sample below), you will get all the resources owned and shared by the specific API user.

{ "operation":{ "name":"GET RESOURCE ACCOUNTLIST", "result ":{ "status": "Success , "message":"Resource details with account list fetched successfully" }, "Details":{ "RESOURCE ID":"303", "RESOURCE NAME":"MSSQL server", "RESOURCE DESCRIPTION" :"WebLogic Data source password", "RESOURCE TYPE":"MS SQL server", "DNS NAME":" sqlserver-l", "PASSWORD POLICY":"Strong", "DEPARTMENT": "SQL Server DBA" , "LOCATION":"Level 10", "RESOURCE URL":"http://sqlserver-1/", "RESOURCE OWNER": "admin", "CUSTOM FIELD":{ "CUSTOMFIELDVALUE":"78336298", "CUSTOMFIELDTYPE":"Numeric", "CUSTOMFIELDLABEL":"License No" , "CUSTOMFIELDCOLUMNNAME":"COLUMN_LONG1" }, { "CUSTOMFIELDVALUE":"Sep 10, 2013", "CUSTOMFIELDTYPE" : "Date", "CUSTOMFIELDLABEL":" Installed Date", "CUSTOMFIELDCOLUMNNAME" "COLUMN_DATE1" }, { "CUSTOMFIELDVALUE":"Tese123$*%%, "CUSTOMFIELDTYPE":"Password", "CUSTOMFIELDLABEL":"Resource Password", "CUSTOMFIELDCOLUMNNAME":"COLUMN_SCHAR1" }, { "CUSTOMFIELDVALUE":"YES" "CUSTOMFIELDTYPE":"Character", "CUSTOMFIELDLABEL":"Secure Resource", "CUSTOMFIELDCOLUMNNAME":"COLUMN_CHAR1" } }, "ACCOUNT LIST": { { "ISFAVPASS": "false", "ACCOUNT NAME":"sysdba", "PASSWDID":"308", "PASSWORD STATUS":"[In Use]", "ACCOUNT ID":"308" }, { "ISFAVPASS":"false", "ACCOUNT NAME":"system", "PASSWDID":"307" "PASSWORD STATUS":"*****", "ACCOUNT ID":"307" } } } }

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources
```

3. Get Details of an Account

Description

To get the details of an account that is part of a resource, you need to pass both Resource ID and Account ID to fetch the required details.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/303/accounts/307
```

Sample Output

{ "operation":{ "name":"GET RESOURCE ACCOUNT DETAILS", result":{ status":"Success", message":"Account details fetched successfully" }, "Details":{ "DESCRIPTION":"", "LAST ACCESSED TIME":"N/A", "LAST MODIFIED TIME":"Sep 10, 2013 3:33 PM", "PASSWORD STATUS":"*****", "PASSWDID":"307", "CUSTOM FIELD":[{ "CUSTOMFIELDVALUE": "56455567", "CUSTOMFIELDTYPE":"Numeric", "CUSTOMFIELDLABEL":"Account LIC Number", "CUSTOMFIELDCOLUMNNAME":"COLUMN_LONG1" }, { "CUSTOMFIELDVALUE": "Sep 10, 2013", "CUSTOMFIELDTYPE":"Date", "CUSTOMFIELDLABEL":"Acc creation date", "CUSTOMFIELDCOLUMNNAME":"COLUMN_DATE1" }, { "CUSTOMFIELDVALUE": "Test12345", "CUSTOMFIELDTYPE":"Password", "CUSTOMFIELDLABEL":"Secondary Password", "CUSTOMFIELDCOLUMNNAME":"COLUMN_SCHAR1" }, { "CUSTOMFIELDVALUE": "YES", "CUSTOMFIELDTYPE":"Character", "CUSTOMFIELDLABEL":"Secure Account", "CUSTOMFIELDCOLUMNNAME":"COLUMN_CHAR1" }] } } }

4. Get the Password of an Account that is Part of a Resource

Description

To get the password of an account that is part of a resource, you need to pass both Resource ID and Account ID to fetch the required details.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/password
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

In case the setting at your end demands a reason to be supplied for retrieving a password, you need to pass the following details as input. If the ticketing system is enabled, you need to pass ticket ID for validation.

```
INPUT_DATA={"operation":{"Details":{"REASON":"Need the password to Login Windows Server","TICKETID":"7"}}}
```

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/303/accounts/307/password
```

```
curl -X GET -k -H "Content-Type: text/json" -H
"AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" https://<Host-Name-of-
PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/2/accounts/2/password --data-urlencode
```

Sample Output

```
{ "operation":{ "name":"GET PASSWORD", "result":{ "status": "Success",
"message":"Password fetched successfully" },
"Details":{ "PASSWORD":"fqxdB7ded@4" } } }
```

Note: If there occurs any problem on retrieving password, the reason will be displayed as part of the message.

5. Change the Password of an Account

Description

To change the password of an account that is part of a resource, you need to pass both Resource ID and Account ID to fetch the required details. If the ticketing system is enabled, you need to pass ticket ID for validation.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account
ID>/password
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Input Data

You need to pass input data such as new password, reset type and reason. Reset type should be either LOCAL or REMOTE.

```
INPUT_DATA={
"operation":{
"Details":{
"NEWPASSWORD":"Test@12345$",
"RESETTYPE":"LOCAL",
"REASON":"Password Expired",
"TICKETID":"7"
}}}
```

Sample Request

```
curl -X PUT -k -H "AUTHTOKEN<<Authtoken_generated_from_PAM360>>"
https:/<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/2/accounts/2/password --data-urlencode
INPUT_DATA={"operation":{"Details":{"NEWPASSWORD":"Test12345$","RESETTYPE
":"LOCAL","REASON":"test","TICKETID":"7"}}}
```

Sample Output

```
{"operation":{"name":"CHANGE
PASSWORD","result":{"status":"Success","message":"Password changed
successfully"}}}
```

Note: If there occurs any problem with changing password, the reason will be displayed as part of the message.

6. Create a New Resource

Description

To create a new resource in PAM360.

Input Data

You need to pass input data such as name of the resource, account name, resource type, password, URL, description, notes and any other additional fields at the resource and account levels. You can add as many as 40 custom fields (20 each at resource and account levels). Of these, resource name, account name, resource type and password are mandatory.

```
INPUT_DATA={
"operation":{
"Details":{
"RESOURCENAME":"Windows Server",
"ACCOUNTNAME":"Administrator",
"RESOURCETYPE":"Windows",
"PASSWORD":"Test123#@!",
"NOTES":"Testing API",
"RESOURCEURL":"http://windowsserver/adminconsole",
"RESOURCEPASSWORDPOLICY":"Strong",
"ACCOUNTPASSWORDPOLICY":"Strong",
"RESOURCECUSTOMFIELD":[
{
"CUSTOMLABEL":"Secure Resource",
"CUSTOMVALUE":"YES"
}],
"ACCOUNTCUSTOMFIELD":[
{
"CUSTOMLABEL":"Secure Account",
"CUSTOMVALUE":"YES"
}]}}}
```

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H
"content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources --data-urlencode
"INPUT_DATA={\"operation\":{\"Details\":{\"RESOURCENAME\":\"Windows
Server\",\"ACCOUNTNAME\":\"Administrator\",\"RESOURCETYPE\":\"Windows\",\"
PASSWORD\"
:\"Test@123\",\"RESOURCEPASSWORDPOLICY\":\"Strong\",\"ACCOUNTPASSWOR
DPOLICY\":\"Strong\",\"RESOURCECUSTOMFIELD\":[{\"CUSTOMLABEL\":\"Secure
Resource\",\"CUSTOMVALUE\":\"YES\"}],\"ACCOUNTCUSTOMFIELD\":[{\"CUSTOM
LABEL\":\"Secure Account\",\"CUSTOMVALUE\":\"YES\"}]}}}"
```

Sample Output

```
{"operation":{
"name":"CREATE RESOURCE",
"result":{
"status":"Success",
"message":"Resource Windows Server has been added successfully"
}}
```

Note: If you want to add a new resource under Administrator/Password Administrator/Privileged Administrator an additional parameter "OWNERNAME" having the value of that particular user should be added to the resource details. While adding the resource to AD user, the username must be in the format "Domain-Name\\UserName".

```
INPUT_DATA={ "operation":{ "Details":{ "RESOURCENAME":"Windows Server",
"ACCOUNTNAME":"Administrator", "RESOURCETYPE":"Windows",
"PASSWORD":"Test@123", "NOTES":"Testing API",
"RESOURCEURL":"http://windowsserver/adminconsole", "OWNERNAME":"admin",
"RESOURCECUSTOMFIELD":[ { "CUSTOMLABEL":"Secure Resource",
"CUSTOMVALUE":"YES" } ], "ACCOUNTCUSTOMFIELD":[ {
"CUSTOMLABEL":"Secure Account", "CUSTOMVALUE":"YES" } ] } } }
```

Note: If you want to add a resource to a static resource group, an additional parameter "RESOURCEGROUPNAME" having the value of that particular resource group should be added to the resource creation input. If the group already exists, this resource will be added to that group; otherwise, a new group with the name specified here will be created.

```
INPUT_DATA={ "operation":{ "Details":{ "RESOURCENAME":"Windows Server",
"ACCOUNTNAME":"Administrator", "RESOURCETYPE":"Windows",
"PASSWORD":"Test123#@!", "NOTES":"Testing API",
"RESOURCEURL":"http://windowsserver/adminconsole",
"RESOURCEGROUPNAME":"Windows Servers", "RESOURCECUSTOMFIELD":[ {
"CUSTOMLABEL":"Secure Resource", "CUSTOMVALUE":"YES" } ],
"ACCOUNTCUSTOMFIELD":[ { "CUSTOMLABEL":"Secure Account",
"CUSTOMVALUE":"YES" } ] } } }
```

Note: You can also add files as a separate resource in PAM360. To add a file as a new resource, the 'Content-Type' in the request has to be modified as shown in the sample below. Once you have modified, you just have to pass the file along with it.

```
INPUT_DATA={ "operation":{ "Details":{ "RESOURCENAME":"Active Directory",
"ACCOUNTNAME":"Administrator", "RESOURCETYPE":"License Store",
"PASSWORD":"Test123#@!", "NOTES":"Testing API",
"RESOURCEURL":"http://windowsserver/adminconsole" } } }
```

Sample Request

```
curl -X POST -k -H "Content-Type: multipart/form-data" -F
'file=@standalonesample.txt' -F
'INPUT_DATA={"operation":{"Details":{"RESOURCENAME":"Windows
erver","ACCOUNTNAME":"Administrator","RESOURCETYPE":"File Store",
"PASSWORD":"Test123#@!","NOTES":"Testing
API","RESOURCEURL":"http://windowsserver/adminconsole"}}}' 'https://<Host-
Name-of-PAM360-Server OR IP address>ort>/
restapi/json/v1/resources?AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

7. Get the Account ID and Resource ID

Description

To get the account ID and resource ID, you need to pass the resource name and account name in the URL.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/getResourceIdAccountId?
RESOURCENAME=(Resourcename)&ACCOUNTNAME=(Account name)
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" "https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/getResourceIdAccountId?RESOURCENAME=MSSQLServer&ACCOUNTNAME=system"
```

Sample Output

```
{"operation":{"name":"GET_RESOURCEACCOUNTID","result":{"status":"Success","message":"Resource ID and account ID fetched successfully for the given resource name and account name." },
"Details":{"RESOURCEID":"303","ACCOUNTID":"307" }}}
```

8. Get the Resource ID using the Resource Name

Description

To fetch the resource ID, you can provide the resource name alone in the URL.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/resourcename/{RESOURCENAME}
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/resourcename/test
```

Sample Output

```
{"operation":{"name": "GET_RESOURCEID","result":{"status": "Success","message": "Resource ID fetched successfully for the given resource name."},
"Details":{"RESOURCEID": "1"}}
```

9. Delete a Resource in PAM360

Description

To delete a resource for the given resource ID. Resource ID can be obtained from the GET RESOURCES API (explained above).

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/{resourceid}
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

DELETE

Input Data

None

Sample Request

```
curl -X DELETE -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/2
```

Sample Output

```
{ "operation":{ "name":"DELETE RESOURCE" "result":{"status":"Success"
"message":"Resources deleted successfully."} }
```

10. Request Password Approval by the Admin

Description

Method to request the admin for password access approval. The account id has to be passed for the same in the URL.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/accounts/{accountid}/requestpassword
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

In case the setting at your end demands a reason to be supplied for requesting a password, you need to pass the following details as input. INPUT_DATA= { "operation" : { "Details" : { "REASON" : "asdefefe"}}}

Sample Input

```
{ "operation":{ "Details":{ PASSWDID":"1" "REASON":"Testing" } } }
```

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H
"Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/accounts/7/requestpassword?INPUT_DATA= {
"operation" : { "Details":{ "REASON" : "Testing"}}}
```

Sample Output

```
{ "operation":{ "name":"REQUEST_PASSWORD" ,"result":{"status":"Success"
,"message":"Request to view password have been raised successfully" },
"Details":{"STATUS" : "WAITING FOR APPROVAL / CHECKOUT" ; } } }
```

11. Get the List of Password Requests

Description

Method to get the list of password requests to be approved or rejected by the admin who is logged in.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/accounts/passwordaccessrequests
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Input

```
INPUT_DATA= { "operation" : { "Details" : { "REASON" : "Testing", "TICKETID" : "7"}}}
```

Sample Request

```
curl -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/passwordaccessrequests
```

Sample Output

{
"operation":{
"name":"GET_PASSWORDREQUEST"
"result":{
"status":"Success"
"message" : "Password Request fetched successfully"
}
"Details": {
"REQUESTER USERID":"2"
"REQUESTED BY":"guest"
"REQUESTED BY FULLNAME" : "Guest guest"
"PASSWORDREQUESTLIST" : [
{
"ACCOUNT ID" : "1"
"ACCOUNT NAME" : "ACCOUNT1"
"RESOURCE ID":"1"
"RESOURCE NAME":"apt-server1"
"PASSWD ID" : "1"
"STATUS":""
"REQUESTED TIME":"Nov 27
"REASON" : "For connecting the machine and update the PAM360 server".
}{
"ACCOUNT ID" : "2"
"ACCOUNT NAME" : "ACCOUNT2"
"RESOURCE ID":"2"
"RESOURCE NAME":"apt-server2"
"PASSWD ID" : "2"
"STATUS":""
"REQUESTED TIME":"Nov 28
"REASON" : "For connecting the machine and update the PAM360 server".
}]}}}

Note: Requester ID is the same as the ID of the user who has requested the password.

12. Reject a Password Request

Description

Method for the admin to reject the password requests. This requires the account ID and requester ID to be passed in the URL.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/reject
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Sample Input

```
{ "operation":{ "Details":{ "PASSWDID":"1" "REQUESTEDID" : "2" (userid of the request raised user) } } }
```

Note: Requester ID is the same as the ID of the user who has requested the password.

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/7/requester/34/reject
```

Sample Output

```
{ "operation":{ "name" : "ADMIN_REQUEST_REJECT""result" : {"status" : "Success""message": "Password Rejected successfully" } } }
```

13. Approve a Password Request

Description

Method for the admin to approve the password requests. Here, the account ID and the Requester ID are required to be passed in the URL.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/approve
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

None

Note: Requester ID is the same as the ID of the user who has requested the password. REQUESTEDID can be obtained from the GET PASSWORDREQUEST API(REQUESTER USERID).

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/7/requester/34/approve
```

Sample Output

```
{ "operation" : { "name" : "ADMIN_REQUEST_APPROVE""result" : { "status" : "Success""message": "Password Approved successfully" } } }
```

14. Check-in the Password Approved by the Admin

Description

Method to check-in the password approved by the admin. The account and requester IDs have to passed in the URL for the same.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/{accountid}/requester/{requesterid}/checkin
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

```
{ "operation":{ "Details":{ "PASSWDID" : "1" "REQUESTEDID" : "2" (userid of the request raised user) } }
```

Note: Requester ID is the same as the ID of the user who has requested the password.

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/7/requester/34/checkin
```

Sample Output

```
{ "operation":{"name" : "ADMIN_REQUEST_CHECKIN""result" : {"status" : "Success""message" : "Password have been checked in successfully" } } }
```

15. Checkout the Password Approved by the Admin

Description

Method to checkout the password after being approved by the admin after request. The account ID had to be passed for the same in the URL.

URL

```
https://:<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/{accountid}/checkout
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

On account of customized settings that demand reason for password checkout, you need to pass the following as input. INPUT_DATA= { "operation" : { "Details":{ "REASON" : "asdefefe"}}}

Sample Input

```
{ "operation":{ "Details":{ "REASON":"N/A" } } }
```

Sample Request

```
curl -X POST -k-H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/7/checkout?INPUT_DATA= { "operation" : { "Details" : { "REASON" : "N/A"}}}
```

Sample Output

```
{ "operation": { "name" : "REQUEST_CHECKOUT""result" : { "status" :
"Success""message" : "Password have been checked out successfully"
"Details":{"STATUS" : "***** [checkIn]" } } }
```

16. Generate Password

Description

Method to generate passwords using existing policies in PAM360.

URL

```
https:// <Host-Name-of-PAM360-Server OR IP address>
:<Port>/restapi/json/v1/passwords/generate
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

INPUT_DATA={ "operation" : { "Details" : { "POLICY" : "Strong"}}}

Sample Output

```
{ "operation": { "name": "GENERATE PASSWORD", "result": { "status": "Success",
"message": "Password generated successfully." },
"Details": { "PASSWORD": "u%mdh7gfN" } } }
```

17. Create a New User

Description

To add a new user to PAM360. This API allows you to create users without any obligatory enforcement of a password.

URL

https:// <Host-Name-of-PAM360-Server OR IP address> :<Port>/restapi/json/v1/user

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName=<<org display name>>

HTTP Method

POST

Input Data

INPUT_DATA={"operation": {"Details":{"USERNAME":"jason1", "FIRSTNAME":"Jason","LASTNAME":"J","FULLNAME":"JasonThomas","EMAIL":"jason@opmanager.com","POLICY":"Strong","ROLE":"Password User","ISSUPERADMIN":"true|false","PASSWORD":"Test@123","DEPARTMENT":"NOC","LOCATION":"Level 10 - South Wing","ISAPIUSER":"false","HOSTNAME":"admin-2100","EXPIRYDATE":"yyyy-mm-dd|NeverExpires"}}}

Input Data

(Applicable from build 6700 and above only)

Notes:

1. User accounts can be created with the following access as required: Web Access, REST and Application Access or REST API only access depending upon the requirements.

2. Utilizing the ISAPIUSER parameter enables the creation of an exclusive REST API user.

```
INPUT_DATA=
{
"operation":{
"Details":{
//User Details
"FIRSTNAME":"Jason",
"LASTNAME":"J",
"USERNAME":"Jason",
"EMAIL":"jason@opmanager.com",
"ROLE":"administator",
"DEPARTMENT":"NOC",
"LOCATION":"Level 10 - South Wing",
"ISSUPERADMIN":false,
//Web Access - To provide the user with PAM360 web access
"WEBACCESS":true,
"POLICY":"Strong",
"PASSWORD":"Test@123",
"ENABLEMOBILEACCESS":true,
"ENABLEADDONACCESS":true,
"REMOTECONNECTACCESS":true,
"REMOTECONNECTVIASSHPROXY":false,
"LANGUAGECODE":"english",
"ENABLETWOFACTOR":true,
"RSAUSERNAME":"Jason",
"RADIUSUSERNAME":"Jason",
"PHONEFACTOR_USERNAME":"Jason",
"DUOUSERNAME":"Jason",
"PRIMARYCONTACT":"Mobile",
```

Sample Output


```
{
"operation":{
"result": {
"message": "User Created Successfully.",
"status": "Success",
},
"Details": {
"USERID": "302"
},
"name": "CREATE_USER"
}
}
```


18. Edit Resources

Description

Method to edit resources.

URL

```
https://severname:port/restapi/json/v1/resources/{RESOURCEID}
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Input Data

(Optional inputs are given in grey)

Sample Input

Note: If you want to edit resource type, an additional parameter "RESOURCETYPE" having the value of that particular resource type should be added to the input. While editing 'Resource Type' cannot be changed from Key Store, File Store, License Store, Rackspace, and AWS IAM to other resource types and viceversa.

```
{ "operation" : { "Details": { "RESOURCENAME" : "Test", "LOCATION" : "4th floor",
"RESOURCEURL" : "http://test", "RESOURCEPASSWORDPOLICY":"Strong",
"DEPARTMENT" : "Test", "RESOURCEDESCRIPTION" : "Created for quality
assurance", "RESOURCETYPE" : "Windows", "RESOURCECUSTOMFIELD" : [ {
"CUSTOMLABEL" : "Secure Resource", "CUSTOMVALUE" : "YES" } ] } } }
```

Sample Request

```
curl -X PUT -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/1 --data-urlencode
"INPUT_DATA={\"operation\":{\"Details\":{\"RESOURCENAME\":\"Test\",\"LOCATIO
N\":\"4thfloor\",\"RESOURCEURL\":\"http://test\",\"RESOURCEPASSWORDPOLICY\
":\"Strong\",\"DEPARTMENT\": \"Test\", \"RESOURCEDESCRIPTION\" : \"Created for
quality assurance\", \"RESOURCECUSTOMFIELD\" : [{\"CUSTOMLABEL\" : \"Secure
Resource\", \"CUSTOMVALUE\" : \"YES\" }]}}}"
```

Sample Output

```
{"operation":{ "name":"EDIT RESOURCE",
"result":{"status":"Success","message":"Resource Test modified successfully."}}}
```

19. Delete an Account under a Specific Resource

Description

To delete an account under a specific resource.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

DELETE

Sample Request

```
curl -X DELETE -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/1/accounts/1
```

Sample Output

```
{ "operation":{
"name":"DELETE ACCOUNT",
"result":{"status":"Success","message":"Account Test123 deleted successfully."}}}
```

20. Get License Keys, Files, Digital Certificates, Documents, Images, etc.

Description

To get files, keys, certificates, etc. that are either an individual resource or a part of other resources.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/downloadfile
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

In case the setting at your end demands a reason to be supplied for downloading the file, you need to pass the following details as input. If the ticketing system is enabled, you need to pass ticket ID for validation.

```
{"operation":{
"Details":{
"REASON":"Need the key file to connect the remote host", //optional when reason is forced
"TICKETID":"7", // optional when ticketing system is enabled
"ISCUSTOMFIELD":"true" //optional Need to be given if the file to be downloaded is account/resource additional field file type
"CUSTOMFIELDTYPE":"ACCOUNT / RESOURCE" // optional -If its account additional field it must be ACCOUNT or if its resource
additional field it must be RESOURCE
"CUSTOMFIELDLABEL" : "LicenseFIle" // optional - Name of the resource/account additional field
}}}
```

Sample Request

```
curl -i -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>"https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/1501/accounts/3601/downloadfile
```

21. Create Accounts under a Specific Resource

Description

To create multiple accounts that are associated with a specific resource ID.

Input Data

You need to pass input data such as account list, name of the accounts, passwords, description.

```
INPUT_DATA={"operation":{
"Details":{
"ACCOUNTLIST": [
{
"ACCOUNTNAME":"bestest047",
"PASSWORD":"Pa$$Word@123",
"ACCOUNTPASSWORDPOLICY":"Strong",
"NOTES":"IT Security - BES PAM360 API Test"
},
{
"ACCOUNTNAME":"bestest048",
"PASSWORD":"Pa$$Word@123",
"ACCOUNTPASSWORDPOLICY":"Strong",
"NOTES":"IT Security - BES PAM360 API Test"
}]}}}
```

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H
"Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/1/accounts --data-urlencode
"INPUT_DATA={\"operation\":{ \"Details\":{ \"ACCOUNTLIST\": [{
\"ACCOUNTNAME\":
\"bestest047\",\"PASSWORD\":\"Pa$$Word@123\",\"ACCOUNTPASSWORDPOLICY
\":\"Strong\",\"NOTES\":\"IT Security - BES PAM360 API
Test\"},{\"ACCOUNTNAME\":\"bestest048\",
\"PASSWORD\":\"Pa$$Word@123\",\"ACCOUNTPASSWORDPOLICY\":\"Strong\",\"
NOTES\":\"IT Security - BES PAM360 API Test\"}]}}}"
```

Sample Output

```
{"operation":
{"name":"ADD ACCOUNTS","result":
{"status":"Success","message":"Account added successfully"},
"Details":[
{"bestest047":{"STATUS":"Account added successfully"},
"bestest048":{"STATUS":"Account added successfully"}}]}}
```

22. Edit an Account under a Specific Resource

Description

To edit an user account under a specific resource.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/<Resource ID>/accounts/<Account ID>/
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Sample Input

```
{ "operation" : {"Details" : {
"ACCOUNTNAME" : "Test account",
"ACCOUNTPASSWORDPOLICY":"Strong",
"NOTES":"Created for quality assurance",
"ACCOUNTCUSTOMFIELD" : [
{
"CUSTOMLABEL" : "Secure Account",
"CUSTOMVALUE" : "YES"
} ] } } }
```

Sample Request

```
curl -X PUT -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H
"Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/1/accounts/1 --data-urlencode
"INPUT_DATA={\"operation\":{ \"Details\":{\"ACCOUNTNAME\" : \"Test
account\",\"ACCOUNTPASSWORDPOLICY\":\"Strong\",\"NOTES\":\"Created for
quality assurance\", \"ACCOUNTCUSTOMFIELD\" : [{\"CUSTOMLABEL\" : \"Secure
Account\", \"CUSTOMVALUE\" : \"YES\"}]}}}"
```

Sample Output

```
{"operation":{ "name":"EDIT ACCOUNT",
"result":{"status":"Success","message":"Account Test account modified
successfully"}}}
```

23. Delete a User

Description

Method to delete a specific user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/{userid}
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

DELETE

Sample Request

```
curl -X DELETE -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H "Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/307
```

Sample Output

```
{"operation":{"name":"DELETE USER","result":{"status":"Success","message":"User Michael deleted Successfully"}}}
```

24. Create an API User

Description

Method to create an API user.

URL

```
https:// <Host-Name-of-PAM360-Server OR IP address> :<Port>/restapi/json/v1/user
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

```
INPUT_DATA={"operation":{"Details":{"USERNAME":"jason","FULLNAME":"Jason Thomas","EMAIL":"jason@opmanager.com","POLICY":"Strong","ROLE":"Password User","ISSUPERADMIN":"true|false","DEPARTMENT":"NOC","LOCATION":"Level 10 - South Wing","ISAPIUSER":"true","HOSTNAME":"admin-2100","EXPIRYDATE":"yyyy-mm-dd|NeverExpires"}}}
```

Sample Output

```
{"operation":{"name":"CREATE_USER","result":{"status":"Success","message":"SUCCESS"},
"Details":{"AUTHTOKEN":"7DxxxAB-CAxxB-44xx5-8xx9-9317xxxxxEF0"}}}
```

25. Create a New SSH Key

Description

To create a new SSH key.

URL

```
https:// <Host-Name-of-PAM360-Server OR IP address>
:<Port>/api/pki/restapi/createsshkey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data has to be passed as input:

```
{"operation":{"Details":{"keyName":"keytest",
"passPhrase":"passPhrase",
"comment":"comment",
"length":"2048",
"keyType":"ssh-rsa"}}}
```

Sample Request

```
https://< Host-Name-of-PAM360-Server OR IP address
>:<Port>/api/pki/restapi/createsshkey?INPUT_DATA={"operation":{"Details":{"keyNa
me":"keytest","passPhrase":"passPhrase","comment":"comment","length":"2048","
keyType":"ssh-rsa"}}}
```

Sample Response

```
{ "name": "CreateSSHKey",
"result": {
"status": "Success",
"message": "New SSH key created successfully" }
}
```

Note: Following are the key types that can be used to create new SSH keys:

- sh-rsa (key length: 1024/2048/4096)
- ssh-dss (key length: 1024)
- d25519 (no specific key length)
- ecdsa (key length: 256/384/521)

26. Delete an SSH Key

Description

To delete a particular SSH key.

URL

```
https://< Host-Name-of-PAM360-Server OR IP address >:<Port>/api/pki/restapi/deleteSSHKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

DELETE

Input Data

The following data has to be passed as input:

```
{"operation":{"Details":{"key_name":"newkey1","withoutDisassociation":"true"}}}
```

Sample Request

```
https://< Host-Name-of-PAM360-Server OR IP address >:<Port>/api/pki/restapi/deleteSSHKey?INPUT_DATA={"operation":{"Details":{"key_name":"newkey1","withoutDisassociation":"true"}}}
```

Sample Response

```
{ "name": "DeleteSSHKey","result": { "status": "Success","message": "SSH keys newkey1 deleted successfully"}}
```

27. Fetch all the SSH Keys

Description

To fetch all the discovered SSH keys.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllSSHKeys
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllSSHKeys
```

Sample Response

```
{ "name": "GetAllSSHKeys", "result": { "status": "Success", "message": "All SSH Keys fetched successfully" }, "totalRows": 1, "details": [ { "KeyName": "testkey", "KeyType": "ssh-rsa", "KeyLength": "2048", "FingerPrint": "SHA256:v28/AlRYrpBKjAp4JoTRphLOkFdVb1ummVcyFHSfC5I", "isPassphraseAvailable": false, "CreatedBy": "mm", "CreationTime": "Today" } ] }
```

28. Fetch a Particular SSH Key

Description

To fetch a particular SSH key from the discovered keys.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getSSHKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The name of the operation and key to be passed as input

```
{"operation":{"Details":{"keyName":"key"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/getSSHKey?INPUT_DATA={"operation":{"Details":{"
keyName":"key"}}}
```

Sample Response

```
{ "name": "GetSSHKey", "result": { "status": "Success", "message": "SSH Key testkey
fetched successfully" }, "details": [ { "KeyName": "testkey", "KeyType": "ssh-rsa",
"KeyLength": "2048", "FingerPrint":
"SHA256:v28/AlRYrpBKjAp4JoTRphLOkFdVb1ummVcyFHSfC5I",
"isPassphraseAvailable": false, "CreatedBy": "mm", "CreationTime": "Today" } ] }
```

29. Export an SSH Key

Description

To export a particular SSH key.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/exportSSHKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The name of the operation and key have to be passed as input.

```
{"operation":{"Details":{"keyName":"key"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/exportSSHKey?INPUT_DATA={"operation":{"Details":{"keyName":"key"}}}
```

Sample Response

```
Key file
```

30. Get SSH Keys for a User

Description

To get all the SSH keys associated with a particular user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getSSHkeysforuser
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

The username and resource name have to be passed as input.

```
{"operation":{"Details":{"userName":"test","resourceName":"172.21.xxx.xx"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getSSHkeysforuser?&INPUT_DATA={"operation":{"Details":{"userName":"test","resourceName":"172.21.xxx.xx"}}}
```

Sample Response

```
{ "name": "GetSSHKeysForUser", "result": { "status": "Success", "message": "SSH keys for user test of resource pam-centos6 fetched successfully" }, "details": "testkey,testkey1" }
```

31. Fetch all Associated Users

Description

To fetch all the users associated with SSH keys.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllAssociatedUsers
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllAssociatedUsers
```

Sample Response

```
{ "name": "GetAllAssociatedUsers", "result": { "status": "Success", "message": "All associated users fetched successfully" }, "totalRows": 1, "details": [ { "UserName": "test", "ResourceName": "pam-centos6" } ] }
```

32. Get a Certificate

Description

To obtain a certificate from PAM360's certificate repository.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getCertificate
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

The operation details and the name of the certificate fetched have to be passed as input.

```
{"operation": { "Details" : { "common_name" :
"*.google.com","serial_number":"XXXXXXXXXXXXXX" // optional to provide serial
number to fetch certificate details}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/getCertificate?INPUT_DATA={"operation":{"Details":
{"common_name":"*.google.com","serial_number":"XXXXXXXXXXXXXX"}}}
```

Sample Response

```
Certificate object
```

33. Get all Certificates

Description

To obtain all the certificates from PAM360's certificate repository.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/getAllSSLCertificates
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data (Optional)

```
INPUT_DATA={"operation":{"Details":{"withExpiryDaysLessThan":"500","withKeyLen
gth":"1024","withSignatureAlgorithm":"SHA1"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllSSLCertificates?INPUT_DATA={"operation":{"Details":{"withExpiryDaysLessThan":"500","withKeyLength":"1024","withSignatureAlgorithm":"SHA1"}}}
```

Sample Response


```
{ "name": "GetAllSSLCertificates", "result": { "status": "Success", "message": "All SSL Certificates fetched successfully" }, "totalRows": 2, "details": [ { "CertID": 1, "DNS Name/FQDN": "paytm.com", "Port": 443, "Common Name": "*.paytm.com", "Issuer": "GeoTrust Inc.", "FromDate": "Oct 13, 2015", "ExpiryDate": "Aug 27, 2017", "KeyStrength": "2048", "SignatureAlgorithm": "SHA256withRSA" }, { "CertID": 302, "DNS Name/FQDN": "204.141.32.155", "Port": 443, "Common Name": "*.zoho.com", "Issuer": "Sectigo Limited", "FromDate": "Jul 2, 2019", "ExpiryDate": "Apr 30, 2021", "KeyStrength": "2048", "SignatureAlgorithm": "SHA256withRSA" } ] }
```


34. Get all Certificate Expiry

Description

To get the expiry dates of all the certificates.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllSSLCertsExpiryDate
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getAllSSLCertsExpiryDate
```

Sample Response

```
{ "name": "GetAllSSLCertificatesExpiryDate", "result": { "status": "Success", "message": "Certificates expiry date fetched successfully" }, "totalRows": 2, "details": [ { "Common Name": "*.paytm.com", "ExpiryDate": "Aug 27, 2017" }, { "Common Name": "*.zoho.com", "ExpiryDate": "Apr 30, 2021" } ] }
```

35. Get Certificate Details

Description

To get the details of a particular certificate.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getCertificateDetails
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

The operation details and the name of the certificate have to be passed as input.

```
{"operation": {"Details":{"common_name":"*.google.com"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getCertificateDetails?INPUT_DATA={"operation":{"Details":{"common_name":"*.google.com"}}}
```

Sample Response


```
{ "name": "GetCertificateDetails", "result": { "status": "Success", "message": "Details of certificate *.zoho.com fetched successfully" }, "details": [ { "certtype": "Domain", "certificateTemplate": "N/A", "endpoint": { "hostName": "*.zoho.com", "port": "443", "expiry_date": "2021-04-30 05:29:59.0", "from_date": "2019-07-02 05:30:00.0", "certSignAlg": "SHA256withRSA", "Sans": "*.zoho.com,zoho.com", "serial": "8c0b04e91a1796d86d1de5e89c8b3c5c", "fingerPrint": "aeecb6227dc8adef18a8fb99465739996e2782a8", "keyalg": "RSA", "PublicKeyLength": 2048, "PrivateKey": false, "isAWS": false }, "isCertInstalledMulipleServers": false, "issuer": { "cname": "Sectigo RSA Domain Validation Secure Server CA", "org": "Sectigo Limited", "orgunit": "-" }, "issuedto": { "cname": "*.zoho.com", "org": "-", "orgunit": "Domain Control Validated" }, "intermediate": {}, "ipaddress": "204.141.32.155", "CertificateId": "302" } ] }
```


36. Get Certificate Keystore

Description

To get the key store file of a particular certificate.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getCertificateKeyStore
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

The name of the operation and the common name of the keystore file have to be passed as input.

```
{"operation" : { "Details" : {"common_name" :
"apitest","serial_number":"XXXXXXXXXXXXXX" //optional to provide serial number
to fetch the keystore file}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/getCertificateKeyStore?INPUT_DATA={"operation":{
"Details":{"common_name":"apitest","serial_number":"XXXXXXXXXXXXXX"}}}
```

Sample Response

```
KeyStore File Object
```

37. Get Certificate Passphrase

To get the private key passphrase of a certificate.

URL

```
https://< Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/getCertificatePassphrase
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Input Data

The following data has to be passed as input:

```
{"operation":{"Details":{"common_name":"mycert","serial_number":"XXXXXXXXXXXXXX"}}}
```

Sample Request

```
https://< Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/getCertificatePassphrase?INPUT_DATA={"operation":{"Details":{"common_name":"mycert","serial_number":"XXXXXXXXXXXXXX"}}}
```

Sample Response

```
{ "name": "GetCertificatePassphrase","result": {"status": "Success","message": "Private key passphrase of certificate mycert is 123456789"}}
```

38. Add a Certificate

To add a certificate to PAM360's certificate repository.

URL

```
https://< Host-Name-of-PAM360-Server OR IP address >:<Port>/api/pki/restapi/addCertificate
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data has to be passed as input:

input data:
{"operation":{"Details":{"fileType":"KEYSTORE","PASSWORD":"PASSWORD"}}}

Note: The fileType specified in the input data can be either CERTFILE or KEYSTORE. For CERTFILE fileType, the PASSWORD field need not be specified.

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H 'Content-Type: multipart/form-data' -F INPUT_DATA='{"operation":{"Details":{"fileType":"KEYSTORE","PASSWORD":"PASSWORD"}}}' -F File=@D:/certs/newcert.keystore https://< Host-Name-of-PAM360-Server OR IP address >:<Port>/api/pki/restapi/addCertificate
```

Sample Response

```
{ "name": "AddCertificate",
"result":
{{"Status":"Success",
"Message": "Certificate newcert.com added successfully"}}}
```

39. Delete a Certificate

Description

To delete a certificate from PAM360's certificate repository.

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/deleteCertificate

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

DELETE

Input Data

The operation name and the common name of the certificate have to be passed as input.

```
{"operation": {"Details":{"common_name" : "apitest","serial_number" :
"XXXXXXXXXXXXXX" //optional to provide serial number to delete a certificate}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/deleteCertificate?INPUT_DATA={"operation":
{"Details":{"common_name":"apitest","serial_number":"XXXXXXXXXXXXXX" //
optional to provide serial number to fetch certificate details}}}
```

Sample Response

```
{"name":"DeleteCertificate","result":{"status":"Success","message":"Certificate
apitest deleted successfully."}}
```

40. Perform SSL Certificate Discovery

Description

To discover a particular SSL certificate.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/sslCertSingleDiscovery
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The name/IP address of the host and port number have to be passed as input.

```
{"operation":{"Details":{"HOST":"de-ubuntu10-
1","TIMEOUT":"300","PORT":"<Port>"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/sslCertSingleDiscovery?INPUT_DATA={"operation":{
"Details":{"HOST":"de-ubuntu10-1","TIMEOUT":"300","PORT":"<Port>"}}}
```

Sample Response

```
{ "name": "Get SSL Discovery", "totalRows": 1, "details": { "zoho.com": [ "SUCCESS",
"SSL Certificate already available, *.zoho.com certificate found at port 443" ] } }
```

41. Perform SSL Certificate Discovery (For a Range of IP Addresses)

Description

To discover a set of SSL certificates.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/sslCertRangeDiscovery
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The start and end IP addresses, port number and time-out have to be passed as input.

```
{"operation":{"Details":{"StartIpAddress":"192.xxx.xxx.x",
"EndIpAddress":"192.xxx.xxx.x",
"TIMEOUT":"3",
"PORT":"443"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/sslCertRangeDiscovery?INPUT_DATA={"operation":{"Details":{"StartIpAddress":"192.xxx.xxx.0","EndIpAddress":"192.xxx.xxx.3","TIMEOUT":"3","PORT":"443"}}}
```

Sample Response

```
{ "name": "Get SSL Discovery", "totalRows": 4, "details": { "192.168.216.1": [ "FAILURE", "Connection failed,no certificate found at port 443" ], "192.168.216.0": [ "FAILURE", "Connection timed out,no certificate found at port 443" ], "192.168.216.2": [ "FAILURE", "Connection timed out,no certificate found at port 443" ], "192.168.216.3": [ "FAILURE", "Connection timed out,no certificate found at port 443" ] } }
```

42. Create CSR

Description

To create a certificate signing request.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/createCSR
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data need to be passed as input.

```
{"operation":{"Details":{"CNAME":"mytestcert",
"ALT_NAMES":"test",
"ORGUNIT":"zohocorp",
"ORG":"manageengine",
"LOCATION":"chennai",
"STATE":"Tamilnadu",
"COUNTRY":"IN",
"PASSWORD":"zohocorp",
"VALIDITY":"888",
"VALIDITY_TYPE":"days",
"ALG":"RSA",
"LEN":"4096",
"SIGALG":"SHA256",
"StoreType":"PKCS12"}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/createCSR?INPUT_DATA={"operation":{"Details":{"CNAME":"mytestcert", "ALT_NAMES":"test", "ORGUNIT":"zohocorp", "ORG":"manageengine", "LOCATION":"chennai", "STATE":"Tamilnadu","COUNTRY":"IN", "PASSWORD":"zohocorp", "VALIDITY":"888", "VALIDITY_TYPE":"days", "ALG":"RSA", "LEN":"4096", "SIGALG":"SHA256", "StoreType":"PKCS12"}}}
```

Sample Response

```
{"name":"CreateCertificate","result":{"status":"Success","message":"CSR saved successfully"}}
```

43. Get CSR List

Description

To get CSR list

HTTPS Method

GET

Input Data

```
INPUT_DATA={"operation":{"Details":{"common_name":"testcsr"}}} (optional)
```

Note: Without INPUT_DATA all the CSR will be fetched. But with INPUT_DATA, the CSR matching the common_name criteria alone will be fetched.

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Sample Request

```
https://<HostName>:8282/api/pki/restapi/getCSRList
```

Sample Response


```
{ "name": "GetCSRList", "result": { "status": "Success", "message": "Fetched all CSRs successfully" }, "totalRows": 1, "details": [ { "CREATED_BY": "admin", "KEYALGORITHM": "RSA", "KEYSTORE_TYPE": "JKS", "isPassword": true, "CSR_ID": 1, "CREATED_DATE": "May 15, 2020 19:51", "LOGIN_ID": 301, "KEY_STRENGTH": 2048, "DOMAIN_NAME": "testcsr", "VALIDITY": "30", "SIGNATURE_ALGORITHM": "SHA256withRSA" } ] }
```


44. Sign CSR

Description

To sign CSR

HTTPS Method

POST

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA={"operation":{"Details":{"serverName":"pam360-w12r2-1","caName":"pam360-w12r2-1-ca","templateName":"DomainController","CSR_ID":"1"}}}
```

Sample Request

```
https://<HostName>:8282/api/pki/restapi/signCSR
```

Sample Response

```
{"name":"SignCSR","result":{"status": "Success","message":"Successfully
testdomain.com certificate signed"}}
```

45. Create Certificate

Description

To create an SSL certificate.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/createCertificate
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data have to be passed as input:

{"operation":{"Details":{"CNAME":"mytestcert",
"ALT_NAMES":"test",
"ORGUNIT":"zohocorp",
"ORG":"manageengine",
"LOCATION":"chennai",
"STATE":"Tamilnadu",
"COUNTRY":"IN",
"PASSWORD":"zohocorp",
"VALIDITY":"888",
"VALIDITY_TYPE":"days",
"ALG":"RSA",
"LEN":"4096",
"SIGALG":"SHA256",
"StoreType":"PKCS12"}}}

Sample Request

https://<Host-Name-of-PAM360-Server OR IP address>
:<Port>/api/pki/restapi/createCertificate?INPUT_DATA={"operation":{"Details":{"CN
AME":"mytestcert", "ALT_NAMES":"test", "ORGUNIT":"zohocorp",
"ORG":"manageengine", "LOCATION":"chennai",
"STATE":"Tamilnadu","COUNTRY":"IN", "PASSWORD":"zohocorp",
"VALIDITY":"888", "VALIDITY_TYPE":"days", "ALG":"RSA", "LEN":"4096",
"SIGALG":"SHA256", "StoreType":"PKCS12"}}}

Sample Response

{"name":"CreateCertificate","result":{"status":"Success","message":"Certificate
saved successfully"}}

46. Get the ID of a User

Description

To get the ID of a user by passing their username.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/getUserId
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>
```

HTTP Method

GET

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/getUserId?USERNAME=user1
```

Sample Response

```
{ "operation": { "name":"get_USERID", "result": { "status":"Success","message":"User Id for the specified username  have been fetched successfully"},"Details":{"USERID":"1"}}}
```

47. Delete a User with their Username

Description

To delete a user by passing their username.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user?USERNAME=(username)
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>
```

HTTP Method

DELETE

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user?USERNAME=admin1
```

Sample Response

```
{"operation":{"name":"DELETE USER","result":{"status":"Success","message":"User admin1 deleted successfully"}}}
```

48. Add a User to a User Group

Description

To add a user to a user group by passing their username and the user group to which they should be added.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/addUserToUserGroup?USERNAME=(username)&USERGROUPNAME=(usergroupname)
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

POST

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-ServerORIP address>:<Port>/restapi/json/v1/user/addUserToUserGroup?=admin1&USERGROUPNAME=TestGroup
```

Sample Response

```
{"operation":{"name":"ADD USER TO USERGROUP","result":{"status":"Success","message":"User admin1 added to User Group TestGroup successfully"}}}
```

49. Lock a User

Description

To lock a user by passing their username.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/lock?USERNAME=(username)
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

PUT

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/lock?USERNAME=apiuser
```

Sample Response

```
{"operation":{"name":"LOCK USER","result":{"status":"Success","message":"User account apiuser locked successfully."}}}
```

50. Unlock a User

Description

To unlock a user by passing their username.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/unlock?USERNAME=(username)
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

PUT

Input Data

None

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/unlock?USERNAME=apiuser
```

Sample Response

```
{"operation":{"name":"UNLOCK USER","result":{"status":"Success","message":"User account apiuser unlocked successfully."}}}
```

51. Import an SSH Key

Description

To import an SSH key.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/addSSHKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data is to be passed as input:

```
{ "operation": { "Details": { "keyName":"testkey","passphrase":"passtrix" } } }
```

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H 'Content-Type: multipart/form-data' -F INPUT_DATA={"operation":{"Details":{"keyName":"testkey","passphrase":"passtrix"}}} -F File=@D:/certs/keys/test1-passtrix/test1_Jul-21-2017-15_56.key https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/addSSHKey
```

Sample Response

```
{ "name":"addSSHKey","result": { "status":"SUCCESS","message":"Key imported successfully" } }
```

52. Associate an SSH Key

Description

To associate an SSH key.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/associateKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data is to be passed as input:

```
{ "operation": { "Details": {
"keyName":"testkey","resourceName":"test.csez.zohocorpin.com","userName":"tes
t" } } }
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/associateKey?INPUT_DATA={"operation":{"Details":{
"keyName":"testkey","resourceName":"test.csez.zohocorpin.com","userName":"tes
t"}}}
```

Sample Response

```
{ "name": "associateKey", "result": { "status": "Success", "message": "Key associated
successfully" } }
```

53. Dissociate an SSH Key

Description

To dissociate an SSH key.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/dissociateKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data is to be passed as input:

```
{ "operation": { "Details": {
"keyName":"testkey","resourceName":"test.csez.zohocorpin.com","userName":"tes
t" } } }
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/dissociateKey?INPUT_DATA={"operation":{"Details":
{"keyName":"testkey","resourceName":"test.csez.zohocorpin.com","userName":"te
st"}}}
```

Sample Response

```
{ "name": "dissociateKey", "result": { "status": "SUCCESS", "message": "Key
dissociated successfully." } }
```

54. Create Static and Dynamic Resource Groups

Description

To create both static and dynamic resource groups in PAM360.

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resourcegroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

The following data must be passed as input to create a static resource group:

```
INPUT_DATA={
"operation": {
"Details": {
"GROUPNAME": "CG1",
"DESCRIPTION": "description",
"PARENTGROUPID": 306,
"GROUPTYPE":"STATIC",
"POLICY": "Low",
"NoHelpDeskRetrieval": "false"
}}}
```

The following data must be passed as input to create a dynamic resource group:

```
INPUT_DATA={
"operation": {
"Details": {
"GROUPNAME": "CG3",
"DESCRIPTION": "description",
"PARENTGROUPID": 3002,
"POLICY": "Low",
"NoHelpDeskRetrieval": "false",
"GROUPTYPE":"DYNAMIC",
"andor": "and",
"NoOfCriteria": 2,
"condition_1": "RESOURCENAME",
"operator_1": "CONTAINS",
"valuefield_1": "a",
"condition_2": "LOGINNAME",
"operator_2": "CONTAINS",
"valuefield_2": "e"
}}}
```

Sample Request

```
curl -X POST -k -H "AUTHTOKEN:<<Authtoken_generated_from_PAM360>>" -H
"Content-Type: text/json" https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resourcegroup --data-urlencode
"INPUT_DATA={\"operation\": {\"Details\": {\"critgroup\": \"CG1\",\"critdesc\":
\"description about CG1\",\"RuleCriteria\": \"Low\",\"NoHelpDeskRetrieval\":
\"false\",\"andor\": \"and\",\"NoOfCriteria\": 2,\"condition_1\":
\"RESOURCENAME\",\"operator_1\": \"CONTAINS\",\"valuefield_1\":
\"win\",\"condition_2\":
\"LOGINNAME\",\"operator_2\":\"CONTAINS\",\"valuefield_2\": \"PAM360\"}}}"
```

Sample Output

```
{ "operation": { "name":"CREATE RESOURCE GROUP", "result": { "status":"Success",
"message":"Group CG1 has been added successfully."}}}
```

55. Get Audit Details

Description

To get the audit details in PAM360.

URL

```
https://<Host-Name-of-PAM360-
ServerORIPaddress>:<Port>/restapi/json/v1/audit?AUDITTYPE=<<Resource/User>>&
STARTINDEX=&LIMIT=&DURATION=<<TODAY / YESTERDAY/ LAST_7_DAYS >>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP method

GET

Input Data

None

Sample Request

```
https://localhost:<Port>/restapi/json/v1/audit?AUDITTYPE=Resource&STARTINDEX=1&LIMIT=2&DURATION=YESTERDAY
```

Sample Response

```
{
"operation":
"name": "GET_AUDIT",
"result":
"status": "Success",
"message": "Audits fetched successfully." },
"totalRows": 2,
"Details":
"AUDITID": "3002",
"RESOURCENAME": "Not Applicable",
"ACCOUNTNAME": "N/A",
"OPERATIONTYPE": "CI/CD Settings Updated",
"OPERATEDBY": "admin",
"IPADDRESS": "localhost",
"USERNAME": "N/A",
"LASTACCESSEDTIME": "2019-01-03 14:51:06.666",
"REASON": "Jenkins Authtoken Modified.",
"NAME": "N/A",
"CLIENT": "Web Client"
},
"AUDITID": "2113",
"RESOURCENAME": "test",
"ACCOUNTNAME": "test",
"OPERATIONTYPE": "Password Verification Failed",
"OPERATEDBY": "System",
"IPADDRESS": "localhost",
"USERNAME": "N/A",
"LASTACCESSEDTIME": "2019-01-03 01:45:00.107",
"REASON": "PAM360 could not verify the password integrity.",
"NAME": "N/A",
"CLIENT": "Web Client"
}]}}
```


56. Share a Resource to a User

Description

To share a resource to a user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<resourceid>/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Input Data

```
{"operation":{"Details":{"ACCESSTYPE": "modify","USERID":"1"}}}
```

Allowed accesstypes: view, modify, fullaccess, revoke

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/1/share
```

Sample Response

```
{"operation":{"name":"SHARE RESOURCE","result":{"status":"Success","message":"Read and Modify permission granted to user successfully."}}}
```

57. Share an Account to a User

Description

To share an account to a user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<resourceid>/accounts/<accountid>/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Input Data

```
{"operation":{"Details":{"ACCESSTYPE":"modify","USERID":"1"}}}
```

Allowed accesstypes: view, modify, revoke

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/11/share
```

Sample Response

```
{"operation":{"name":"SHARE ACCOUNT","result":{"status":"Success","message":"View and Modify permission granted to user successfully."}}}
```

58. Share a Resource to a User Group

(This API works from PAM360 build 5100 and above only)

Description

To share a resource to a user group

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<resourceid>/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA={"operation":{"Details":{"ACCESSTYPE":"view","USERGROUPID":"1"}}}
```

Allowed accesstypes: view, modify, fullaccess, revoke

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/1/share
```

Sample Response

```
{ "operation": { "result": { "message": "Read Only permission granted to user group(s) successfully.", "status": "Success" }, "name": "SHARE RESOURCE" } }
```

59. Share an Account to a User Group

(This API works from PAM360 build 5100 and above only)

Description

To share an account to a user group

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<resourceid>/accounts/<accountid>/share

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>

HTTP Method

PUT

Input Data

INPUT_DATA={"operation":{"Details":{"ACCESSTYPE":"view","USERGROUPID":"1"}}}

Allowed accesstypes: view, modify, fullaccess, revoke

Sample Request

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/1/accounts/1/share

Sample Response

{ "operation": { "result": { "message": "Read Only permission granted to user group(s) successfully.", "status": "Success" }, "name": "SHARE ACCOUNT" } }

60. Fetch UserGroupID

(This API works from PAM360 build 5100 and above only)

Description

To fetch the UserGroupID of a user group

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/getUserGroupId?USERGROUPNAME=<usergroupname>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>
```

HTTP Method

GET

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/getUserGroupId?USERGROUPNAME=<usergroupname>
```

Sample Response

```
{"operation":{"name":"GET_USERGROUPID","result":{"status":"Success","message":"Usergroup Id for the specified usergroup name have been fetched successfully.
"},"Details":{"USERGROUPID":"1"}}}
```

61. Configure Remote Password Reset for Linux Resources

(This API works from PAM360 build 5100 and above only)

Description

To configure remote password reset for Linux resources

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/configureremotepasswordreset
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

POST

Input Data

```
{"operation": { "Details": { "REMOTEMODE":"ssh|telnet", // Default value - ssh
"LINUX_SSHTELNETPORT":"22", "LINUX_USERPROMPT":"$",
"LINUX_LANDINGSERVER":"test", "RESOURCEIDENTIFIER":"linux | others", // Default
value - linux "WDRESOURCEID":"1", "WDACCOUNTID":"1",
"REMOTELOGINACCOUNT":"test", "AUTHENTICATION":"passauth | keyauth", //
Default value -passauth "ELEVATIONTYPE":"su | sudo", // Default value - sudo
"ROOTACCOUNT":"root", "LINUXROOTUSERPROMPT":"#",
"RESOURCEIDS":["301","302","601"], "RESOURCETYPE":"Linux",
"REMOVEENTER":"true | false" // Default value - false}}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/restapi/json/v1/resources/configureremotepasswordreset
```

Sample Response

```
{"operation":{ "result":{ "message": "Password reset details configured for the
matching resources.", "status": "Success"}, "Details":{ "CONFIGURATION RESULT":[{
"STATUS": "SUCCESS", "RESOURCENAME": "pam360-os1.win.domain.com",
"RESOURCEID": "3"},{ "STATUS": "SUCCESS", "RESOURCENAME": "DC-
u16.lin.domain.com", "RESOURCEID": "4"}]}, "name": "CONFIGURE REMOTE
PASSWORD RESET"}}
```

62. Deploy an SSL Certificate

(This API works from PAM360 build 5300 and above only)

Description

To Deploy SSL Certificate.

HTTPS Method

POST

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA={"operation":{"Details":{"common_name":"testcert","serial_number":"
xxxxxxxx","serverName":"testmachine"}}}
```

Note: It is optional to provide the server name. The server name allows you to deploy certificates to that particular server. Without the server name, the certificates are deployed to all the saved servers from the client.

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/deployCertificate
```

Sample Response

{"result": {
"message": "Certificate deployment is successful.",
"status": "Success"
},
"name": "DeployCertificate",
"totalRows": 1,
"deployStatus": [
{
"server": "testmachine",
"message": "Certificate testcert of format CER and PFX deployed in testmachine successfully.",
"status": "Success"
}]}

63. Share SSL Certificate to User

(This API works from PAM360 build 5300 and above only)

Description

To share SSL certificate to user.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/shareCertificateToUser
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{
"common_name":"certificate","serial_number":"179ae1f45a8" ,"userId":"301"}}}
```

Sample Response

```
{   "result": {
"message": "Certificate shared successfully.",
"status": "Success"
},   "name": "ShareCertificate"}
```

64. Share SSL Certificate to User Group

(This API works from PAM360 build 5300 and above only)

Description

To share SSL certificate to user group.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/shareCertificateToUserGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{
"common_name":"certificate","serial_number":"179ae1f45a8"
,"userGroupId":"301"}}}
```

Sample Response

```
{ "result": { "message": "Certificate shared successfully.", "status": "Success" },
"name": "ShareCertificate" }
```

65. Share SSL Certificate Group to User

(This API works from PAM360 build 5300 and above only)

Description

To share SSL certificate group to user.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/shareCertificateGroupToUser
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{ "certificate_group_name":"certificate"
,"userId":"301"}}}
```

Sample Response

```
{ "result": { "message": "Certificate shared successfully.", "status": "Success" },
"name": "ShareCertificate" }
```

66. Share SSL Certificate Group to User Group

(This API works from PAM360 build 5300 and above only)

Description

To share SSL certificate group to user group.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/shareCertificateGroupToUserGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{ "certificate_group_name":"certificate" ,"userGroupId":"301"}}}
```

Sample Response

```
{ "result": { "message": "Certificate shared successfully.", "status": "Success" }, "name": "ShareCertificate" }
```

67. Revoke SSL Certificate from User

(This API works from PAM360 build 5300 and above only)

Description

To revoke SSL certificate from user.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/revokeCertificateFromUser
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{ "common_name":"certificate","serial_number":"179ae1f45a8" ,"userId":"301"}}}
```

Sample Response

```
{ "result": { "message": "Access to certificate revoked successfully.", "status": "Success" }, "name": "RevokeCertificate" }
```

68. Revoke SSL Certificate from User Group

(This API works from PAM360 build 5300 and above only)

Description

To revoke SSL certificate from user group.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/revokeCertificateFromUserGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{
"common_name":"certificate","serial_number":"179ae1f45a8"
,"userGroupId":"301"}}}
```

Sample Response

```
{ "result": { "message": "Access to certificate revoked successfully.", "status":
"Success" }, "name": "RevokeCertificate" }
```

69. Revoke SSL Certificate Group from User

(This API works from PAM360 build 5300 and above only)

Description

To revoke SSL certificate group from user.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/revokeCertificateGroupFromUser
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA:{"operation":{"Details":{ "certificate_group_name":"certificate"
,"userId":"301"}}}
```

Sample Response

{ "result": { "message": "Access to certificate revoked successfully.", "status": "Success" }, "name": "RevokeCertificate" }

70. Revoke SSL Certificate Group from User Group

(This API works from PAM360 build 5300 and above only)

Description

To revoke SSL certificate group from user group.

HTTPS Method

POST

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/revokeCertificateGroupFromUserGroup

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

Input Data

INPUT_DATA:{"operation":{"Details":{ "certificate_group_name":"certificate" ,"userGroupId":"301"}}}

Sample Response

{ "result": { "message": "Access to certificate revoked successfully.", "status": "Success" }, "name": "RevokeCertificate" }

71. Create SSL Certificate Group

(This API works from PAM360 build 5300 and above only)

Description

To create an SSL certificate group.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/createCertificateGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA={"operation":{"Details":{
"group_name":"NAME","group_description":"This is the description for the group certificate","group_mail":"pam360@zohocorporation.com","ssl_details":"301,202"}
}}
```

Sample Response

```
{"result":{"message":"Certificate group added successfully.","status":"Success"},"name":"createCertificateGroup"}
```

72. Delete SSL Certificate Group

(This API works from PAM360 build 5300 and above only)

Description

To delete SSL certificate group.

HTTPS Method

DELETE

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/deleteCertificateGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA={"operation":{"Details":{ "group_name":"NAME"}}}
```

Sample Response

```
{"result":{"message":"The certificate group is deleted successfully.","status":"Success"},"name":"deleteCertificateGroup"}
```

73. Edit SSL Certificate Group

(This API works from PAM360 build 5300 and above only)

Description

To edit SSL certificate group.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/api/pki/restapi/editCertificateGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Input Data

```
INPUT_DATA={"operation":{"Details":{ "group_name":"NEW
NAME","group_description":"This is new description for the group
certificate","group_mail":"pam360@zohocorporation.com","ssl_details":"1,2,3"}}}
```

Sample Response

```
{"result":{"message":"The certificate group is updated
successfully.","status":"Success"},"name":"editCertificateGroup"}
```

74. Generate an Agent Install Key

(This API works from PAM360 build 5300 and above only)

Description

To generate an agent install key.

HTTPS Method

POST

URL

```
https://<Host-Name-of-PAM360-Server OR IP
address>:<Port>/api/pki/restapi/generateInstallKey
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

Sample Response

```
{ "result": { "message": "Agent install key fetched successfully", "status": "Success" },
"name": "GetAgentInstallKey", "totalRows": 1, "AgentInstallKey":
"20570b9e0ceaa936" }
```

75. Get Password Policies

(This API works from PAM360 build 5300 and above only)

Description

To list all the password policies in the organization.

HTTPS Method

GET

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/passwords/policies
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

Sample Response

{ "operation":{ "result":{ "message": "Password Policies fetched successfully", "status": "Success" }, "Details":{ "ORGANIZATION": "CHAKRIORG", "POLICIES":[{ ENFORCE MIXED CASE": "false", " PASSWORD MAX LENGTH": "8", " ENFORCE SPL CHARS": "false", " POLICYNAME": "Low", " ENFORCE NUMERALS": "false", " NO OF SPL CHARS REQUIRED": "0", " DEFAULTPOLICY": "false", " CHECK DICTIONARY WORD": "false", " NUMBER OF LOWERCASE CHARACTERS REQUIRED": "0", " REUSE OF OLD PASSWORDS": "Don't allow last 1 passwords", " CHECK ANAGRAM OF LOGINNAME": "false", POLICYID": "10000000000001", CHECK SEQUENCE": "false", DESCRIPTION": "Password with less strict constraints", " ENFORCE STARTING WITH AN ALPHABET": "false", " CHECK REPEATED SUBSTRING": "false", " PASSWORD CAN CONTAIN LOGINNAME": "false", " NUMBER OF UPPERCASE CHARACTERS REQUIRED": "0", " CHECK SIMILARITY OF PASSWORDS": "false", " PASSWORD VALIDITY PERIOD": "0", " NUMBER OF NUMERALS": "0", " PASSWORD MIN LENGTH": "4" }, { " ENFORCE MIXED CASE": "true", " PASSWORD MAX LENGTH": "10", " ENFORCE SPL CHARS": "false", " POLICYNAME": "Medium", " ENFORCE NUMERALS": "true", " NO OF SPL CHARS REQUIRED": "0", " DEFAULTPOLICY": "false", " CHECK DICTIONARY WORD": "false", " NUMBER OF LOWERCASE

CHARACTERS REQUIRED": "1", " REUSE OF OLD PASSWORDS": "Don't allow last 5 passwords", " CHECK ANAGRAM OF LOGINNAME": "false", " POLICYID": "10000000000002", " CHECK SEQUENCE": "false", " DESCRIPTION": "Password with few strict constraints", " ENFORCE STARTING WITH AN ALPHABET": "true", " CHECK REPEATED SUBSTRING": "false", " PASSWORD CAN CONTAIN LOGINNAME": "true", " NUMBER OF UPPERCASE CHARACTERS REQUIRED": "1", " CHECK SIMILARITY OF PASSWORDS": "true", " NUMBER OF PASSWORDS TO CHECK FOR SIMILARITY": "1", " PASSWORD VALIDITY PERIOD": "180", " NUMBER OF NUMERALS": "1", " PASSWORD MIN LENGTH": "6" }, { ENFORCE MIXED CASE": "true", " SEQUENCE LENGTH": "5", " PASSWORD MAX LENGTH": "16", " ENFORCE SPL CHARS": "true", POLICYNAME": "Strong", " ENFORCE NUMERALS": "true", " CHECK NUMERIC SEQUENCE": "true", " KEYBOARD LAYOUT": "QWERTY", " DESCRIPTION": "Password with strict constraints", " ENFORCE STARTING WITH AN ALPHABET": "true", " NUMBER OF PASSWORDS TO CHECK FOR SIMILARITY": "1", " PASSWORD VALIDITY PERIOD": "30", " DICTIONARY NAME": "Common Words", CHECK CONSECUTIVE SEQUENCE": "true", " NO OF SPL CHARS REQUIRED": "1", " DEFAULTPOLICY": "true", " CHECK DICTIONARY WORD": "true", " NUMBER OF LOWERCASE CHARACTERS REQUIRED": "1", " REUSE OF OLD PASSWORDS": "Don't allow last 10 passwords", " CHECK ANAGRAM OF LOGINNAME": "false", " CHECK ALPHABET SEQUENCE": "true", " POLICYID": "10000000000003", " CHECK KEYBOARD SEQUENCE": "true", " CHECK OBVIOUS SUBSTITUTION": "false", " CHECK SEQUENCE": "true", " CHECK REPEATED SUBSTRING": "true", " PASSWORD CAN CONTAIN LOGINNAME": "true", " NUMBER OF UPPERCASE CHARACTERS REQUIRED": "1", " CHECK SIMILARITY OF PASSWORDS": "true", " NUMBER OF NUMERALS": "1", " PASSWORD MIN LENGTH": "8" }, { " ENFORCE MIXED CASE": "true", " PASSWORD MAX LENGTH": "32", " ENFORCE SPL CHARS": "true", POLICYNAME": "Offline Password File", " ENFORCE NUMERALS": "true", " NO OF SPL CHARS REQUIRED": "1", " DEFAULTPOLICY": "false", " CHECK DICTIONARY WORD": "false", " NUMBER OF LOWERCASE CHARACTERS REQUIRED": "1", " REUSE OF OLD PASSWORDS": "Don't allow last 10 passwords", " CHECK ANAGRAM OF LOGINNAME": "false", " POLICYID": "10000000000004", " CHECK SEQUENCE": "false", " DESCRIPTION": "Policy for offline password access", " ENFORCE STARTING WITH AN ALPHABET": "false", " CHECK REPEATED SUBSTRING": "false", " PASSWORD CAN CONTAIN LOGINNAME": "true", " NUMBER OF UPPERCASE CHARACTERS REQUIRED": "1", " CHECK SIMILARITY OF PASSWORDS": "false", " PASSWORD VALIDITY PERIOD": "30", "

NUMBER OF NUMERALS": "1", " PASSWORD MIN LENGTH": "16" }, { " ENFORCE MIXED CASE": "true", " SEQUENCE LENGTH": "3", " PASSWORD MAX LENGTH": "10", " ENFORCE SPL CHARS": "false", " POLICYNAME": "test", " ENFORCE NUMERALS": "true", " CHECK NUMERIC SEQUENCE": "true", " KEYBOARD LAYOUT": "QWERTY", " DESCRIPTION": "testing", " ENFORCE STARTING WITH AN ALPHABET": "true", " NUMBER OF PASSWORDS TO CHECK FOR SIMILARITY": "1", " PASSWORD VALIDITY PERIOD": "180", " DICTIONARY NAME": "Common Words", " CHECK CONSECUTIVE SEQUENCE": "false", " NO OF SPL CHARS REQUIRED": "0", " DEFAULTPOLICY": "false", " CHECK DICTIONARY WORD": "true", " NUMBER OF LOWERCASE CHARACTERS REQUIRED": "1", " REUSE OF OLD PASSWORDS": "Don't allow last 5 passwords", CHECK ANAGRAM OF LOGINNAME": "true", CHECK ALPHABET SEQUENCE": "true", " POLICYID": "10000000000011", " CHECK KEYBOARD SEQUENCE": "true", " CHECK OBVIOUS SUBSTITUTION": "true", " CHECK SEQUENCE": "true", " CHECK REPEATED SUBSTRING": "true", " PASSWORD CAN CONTAIN LOGINNAME": "true", " NUMBER OF UPPERCASE CHARACTERS REQUIRED": "1", " CHECK SIMILARITY OF PASSWORDS": "true", " NUMBER OF NUMERALS": "1", " PASSWORD MIN LENGTH": "6" }] }, "name": "GET PASSWORD POLICIES" } }

76. Get all Resource Types

(This API works from PAM360 build 5400 and above only)

Description

To list all the resource types in the organization.

HTTPS Method

GET

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/resourcetypes

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

Input Data

```
INPUT_DATA={ "operation":{ "Details":{
"RESOURCETYPE_CONTAINING":["brocade"], } } }
```

Sample Response

{ "operation":{ "result":{ "message": "Resource Types fetched successfully", "status": "Success" }, "Details":{ "RESOURCETYPES":[{ "COMMAND_SET":["Brocade"], "ISSYNCSUPPORTED": "false", "CUSTOMRESOURCETYPE": "Windows", "ISCERTIFICATE": "false", "CATEGORY": "network", "SYNCTYPE": "CustomCli", "ISDEFAULT_SUPPORTED_RESOURCETYPE": "true", "OSID": "40", "RESOURCE_ATTRIBUTES":["DNS Name / IP Address", "Group Name", "Resource Description", "Department", "Resource URL", "Location", "Password Policy", "Resource Name"], "ACCOUNT_ATTRIBUTES":["Password Policy", "Private Key", "Notes", "User Account", "User Account Password"], "RESOURCETYPE": "Brocade", "DEFAULTRESOURCETYPE": "false" }, { "COMMAND_SET":["Brocade SAN Switch"], "ISSYNCSUPPORTED": "false", "CUSTOMRESOURCETYPE": "Windows", "ISCERTIFICATE": "false", "CATEGORY": "network", "SYNCTYPE": "CustomCli", "ISDEFAULT_SUPPORTED_RESOURCETYPE": "true", "OSID": "42", "RESOURCE_ATTRIBUTES":["DNS Name / IP Address", "Group Name", "Resource Description", "Department", "Resource URL", "Location", "Password Policy", "Resource Name"], "ACCOUNT_ATTRIBUTES":["Password Policy", "Private Key", "Notes", "User Account", "User Account Password"], "RESOURCETYPE": "Brocade SAN Switch", "DEFAULTRESOURCETYPE": "false" }, { "COMMAND_SET":["Brocade VDX"], "ISSYNCSUPPORTED": "false", "CUSTOMRESOURCETYPE": "Windows", "ISCERTIFICATE": "false", "CATEGORY": "network", "SYNCTYPE": "CustomCli", "ISDEFAULT_SUPPORTED_RESOURCETYPE": "true", "OSID": "41", "RESOURCE_ATTRIBUTES":["DNS Name / IP Address", "Group Name", "Resource Description", "Department", "Resource URL", "Location", "Password Policy", "Resource Name"], "ACCOUNT_ATTRIBUTES":["Password Policy", "Private Key",

"Notes", "User Account", "User Account Password"], "RESOURCETYPE": "Brocade VDX", "DEFAULTRESOURCETYPE": "false" }], "ORGANIZATIONNAME": "MSPOrg" }, "name": "GET RESOURCE TYPES" } }

77. Associate a Resource to a Resource Group

(This API works from PAM360 build 5400 and above only)

Description

To associate a resource to a resource group.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/<groupId>/associateResources
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

POST

Input Data

```
{ "operation": {"Details": { RESOURCEIDS:[1, 2] }}}
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/<groupId>/associateResources
```

Sample Response

{ "operation": { "result": { "message":"Resource added to group successfully.","status":"Success"}, "Details": { "1": { "status":"Success"}, "2":{ "status":"Success" }}, "name":"ASSOCIATE RESOURCES" }}

78. Dissociate a Resource from a Resource Group

(This API works from PAM360 build 5400 and above only)

Description

To dissociate a resource from a resource group.

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/<groupId>/disassociateResources

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>

HTTP Method

POST

Input Data

{ "operation": {"Details": { RESOURCEIDS:[1, 2] }}}

Sample Request

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/<groupId>/disassociateResources

Sample Response

{ "operation": { "result": { "message":"Resource removed from group successfully.","status":"Success" }, "Details":{ "1":{ "status":"Success"}," 2":{ "status":"Success" }}, "name":"DISASSOCIATE RESOURCES" }}

79. Fetch Resource Groups Associated to a Resource

(This API works from PAM360 build 5400 and above only)

Description

To fetch resource groups that are associated to a resource.

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<ResourceId>/associatedGroups

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName= <<org display name>>

HTTP Method

GET

Sample Request

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/<ResourceId>/associatedGroups

Sample Response

{ "operation": { "result":{ "message":"Associated groups fetched successfully","status":"Success"}, "Details":{ "ASSOCIATED GROUPS":[{ "GROUP ID":301,"GROUP NAME":"Default Group"}]}, "name":"GET ASSOCIATED GROUPS" }}

80. Delete a Resource Group

(This API works from PAM360 build 5400 and above only)

Description

To delete a particular resource group.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup?RESOURCEGROUPID=<resourcegroupid>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName= <<org display name>>
```

HTTP Method

DELETE

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup?RESOURCEGROUPID=<resourcegroupid>
```

Sample Response

```
{ "operation":{ "name":"DELETE RESOURCE GROUP","result": { "status":"Success","message":"Resource Group deleted successfully." }}}
```

81. Fetch Resource Group ID

(This API works from PAM360 build 5400 and above only)

Description

To fetch the ID of a resource group.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/getResourceGroupId?RESOURCEGROUPNAME=<resourcegroupname>&USERID=<userid>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

GET

Parameters

```
RESOURCEGROUPNAME=<resourcegroupname> USERID=<userid>
```

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/getResourceGroupId?RESOURCEGROUPNAME=<resourcegroupname>&USERID=<userid>
```

Sample Response

```
{ "operation":{ "name":"GET RESOURCE GROUP ID","result": { "status":"Success","message":"Resource Group Id for the specified Resource Group name have been fetched successfully."} ,"Details":{"RESOURCEGROUPID":"1" }}}
```

82. Reset Two-Factor Authentication

(This API works from PAM360 build 5400 and above only)

Description

To reset two-factor authentication for a username.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/resetMFA?USERNAME=<username>
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
```

HTTP Method

PUT

Parameters

USERNAME=<username>

Sample Request

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/resetMFA?USERNAME=<username>
```

Sample Response

```
{
"operation":{
"result":{
"message": "Two Factor Authentication reset successfully",
"status": "Success"
},
"name": "Reset MFA"
}
}
```

83. Edit an User Account

(This API works from PAM360 build 5400 and above only)

Description

To edit an user account.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/{userid}
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
{
"operation": {
"Details": {
"FIRSTNAME": "Jason",
"LASTNAME": "J",
"EMAIL": "jason@opmanager.com",
"POLICY": "Strong",
"ROLE": "Password User",
"ISSUPERADMIN":false,
"DEPARTMENT": "NOC",
"LOCATION": "Level 10 - South Wing",
"WEBACCESS":true,
"ENABLEMOBILEACCESS": false,
"ENABLEADDONACCESS": false,
"REMOTECONNECTACCESS":true,
"REMOTECONNECTVIASSHPROXY":false,
"LANGUAGECODE": "English",
"ENABLETWOFACTOR": false,
"RADIUSUSERNAME": "Jackson",
"RSAUSERNAME": "Jackson",
"PHONEFACTOR": "Jackson",
"DUOUSERNAME": "Jackson",
"PRIMARYCONTACT": "Mobile",
"MOBILE_COUNTRYCODE": "91",
"MOBILE":"9876543210",
"LANDLINE": "12312311",
```

```
"LANDLINE_COUNTRYCODE": "355",
"LANDLINE_EXT": "907",
"RESTAPIACCESS": true,
"SDKACCESS":true,
"ISAPIUSER":true,
"EXPIRYDATE": "yyyy-mm-dd",
"OWNERNAMEOPTION": true,
"HOSTCHECK":true,
"HOSTNAME":"john-1234"
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "User edited successfully.",
"status": "true"
},
"Details": {},
"name": "EDIT_USER"
}
}
```

84. Regenerate Authentication Token

(This API works from PAM360 build 5400 and above only)

Description

To regenerate the authentication token of the user.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user/regenerateAuthtoken
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

None

Sample Output

```
{
"operation": {
"result": {
"message": "Authtoken regenerated successfully.",
"status": "true",
"statusCode": 20000
},
"Details": {
"AUTHTOKEN": "37F5E238-7E33-4F59-87AE-FDFEF82D1AE0"
},
"name": "REGENERATE_AUTHTOKEN"
}
}
```


85. Fetch All Users

(This API works from PAM360 build 6320 and above only)

Description

To fetch all user details.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/user
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

GET

Note: The default limit, 100, will be applied if the "limit" is not specified.

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"limit": 3,
"startIndex": 1,
"searchValue": "admin@zohocorp.com",
"searchColumn":
"userId|userName|email|role|department|location|orgName|isApiUser|isTfaEnabled|isSuperAdmin|isUserLocked",
"searchOperator": "contains|doesNotContain|equals|notEquals|startsWith|endsWith"
}
}
}
```

Sample Output

{
"operation": {
"result": {
"message": "User(s)' details have been fetched successfully.",
"status": "Success",
"statusCode": 20000
},
"Details": [
{
"role": "Privileged Administrator",
"isApiUser": false,
"isSuperAdmin": false,
"userName": "admin",
"isTfaEnabled": false,
"userId": 1,
"isAddonAccessEnabled": true,
"isUserLocked": false,
"dateCreated": "2023-06-15 11:27:21.11",
"trustScore": "66",
"location": "",
"department": "",
"isMobileAccessEnabled": true,
"email": "aaaadmin@zohocorp.com"
},
{
"role": "Password User",
"isApiUser": false,
"isSuperAdmin": false,

"userName": "guest",
"isTfaEnabled": false,
"userId": 2,
"isAddonAccessEnabled": true,
"isUserLocked": false,
"dateCreated": "2023-06-15 11:27:21.11",
"trustScore": "N/A",
"location": "",
"department": "",
"isMobileAccessEnabled": true,
"email": "guest@zohocorp.com"
},{
"role": "Administrator",
"isApiUser": true,
"isSuperAdmin": false,
"userName": "apiAdmin",
"isTfaEnabled": false,
"userId": 301,
"isAddonAccessEnabled": false,
"isUserLocked": false,
"dateCreated": "2023-06-15 11:37:50.345",
"trustScore": "N/A",
"location": "",
"department": "",
"isMobileAccessEnabled": false,
"email": ""
}],"name": "GET_USER(S)",
"totalRows": 3}}

86. Fetch All User Groups

(This API works from PAM360 build 6320 and above only)

Description

To fetch all the user groups.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/userGroup
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

GET

Note: The default limit, 100, will be applied if the "limit" is not specified.

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"limit": 3,
"startIndex": 1,
"searchValue": "sample",
"searchColumn": "userGroupId|userGroupName|description",
"searchOperator": "contains|doesNotContain|equals|notEquals|startsWith|endsWith"
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "User group(s)' details have been fetched successfully.",
"status": "Success",
"statusCode": 20000
},
"Details": [
{
"userGroupName": "Sample",
"userGroupId": 301,
"dateCreated": "2023-06-01 12:48:35.862",
"description": "For sample purpose"
}
],
"operationName": "GET_USERGROUP(S)",
"totalRows": 1
}
}
```


87. Bulk Share Resource Groups to Users

(This API works from PAM360 build 6320 and above only)

Description

To share resource groups to users in bulk.

URL

https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/share

Header

AUTHTOKEN=<<Authtoken_generated_from_PAM360>>

orgName=<<org diaplay name>>

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"resourceGroupIds": ["301","302","601"],
"userIds":["1","2"],
"accessType":"view|modify|fullaccess|revoke"
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_RESOURCEGROUP(S)"
}
}
```


88. Bulk Share Resource Groups to User Groups

(This API works from PAM360 build 6320 and above only)

Description

To share resource groups to user groups in bulk.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resourcegroup/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"resourceGroupIds": ["301","302","601"],
"userGroupIds": ["1","2"],
"accessType":"view|modify|fullaccess|revoke"
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_RESOURCEGROUP(S)"
}
}
```

89. Bulk Share Resources to Users

(This API works from PAM360 build 6320 and above only)

Description

To share resources to users in bulk.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"resourceIds": ["301","302","601"],
"userIds": ["1","2"],
"accessType":"view|modify|fullaccess|revoke"
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_RESOURCE(S)"
}
}
```


90. Bulk Share Resources to User Groups

(This API works from PAM360 build 6320 and above only)

Description

To share resources to user groups in bulk.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/resources/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"resourceIds": ["301","302","601"],
"userGroupIds": ["1","2"],
"accessType":"view|modify|fullaccess|revoke"
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_RESOURCE(S)"
}
}
```

91. Bulk Share Accounts to Users

(This API works from PAM360 build 6320 and above only)

Description

To share accounts to users in bulk.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"accountIds": ["301","302","601"],
"userIds":["1","2"],
"accessType":"view|modify|remoteapponly|revoke",
"remoteAppIds":["1","2"], //in case of remoteapponly accessType
"resourceId":1 //in case of remoteapponly accessType
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_ACCOUNT(S)"
}
}
```


92. Bulk Share Accounts to User Groups

(This API works from PAM360 build 6320 and above only)

Description

To share accounts to user groups in bulk.

URL

```
https://<Host-Name-of-PAM360-Server OR IP address>:<Port>/restapi/json/v1/accounts/share
```

Header

```
AUTHTOKEN=<<Authtoken_generated_from_PAM360>>
orgName=<<org diaplay name>>
```

HTTP Method

PUT

Input Data

```
INPUT_DATA=
{
"operation": {
"Details": {
"accountIds": ["301","302","601"],
"userGroupIds":["1","2"],
"accessType":"view|modify|remoteapponly|revoke",
"remoteAppIds":["1","2"], //in case of remoteapponly accessType
"resourceId":1 //in case of remoteapponly accessType
}
}
}
```

Sample Output

```
{
"operation": {
"result": {
"message": "Revoke action triggered. Refer Audit for more details.",
"status": "Success",
"statusCode": 20001
},
"operationName": "SHARE_ACCOUNT(S)"
}
}
```

Reports

The information on the entire password management process in your enterprise is presented in the form of comprehensive reports in PAM360. The status and summaries of the different activities such as password inventory, policy compliance, password expiry, user activity etc. are provided in the form of tables and graphs, which assist the IT administrators in making well-informed decisions on password management.

PAM360 provides about fourteen canned reports classified under four types. In addition, there is a provision to create custom reports.

The following types of reports are available in PAM360:

1. Canned Reports
    1.1 Password Reports
    1.2 User Reports
    1.3 General Reports
    1.4 Compliance Reports
    1.5 Scheduling Report Generation
    1.6 Steps to Terminate an Existing Schedule
2. Custom Reports
    2.1 Steps to Create Custom Reports
    2.2 Custom Reports - Use Case

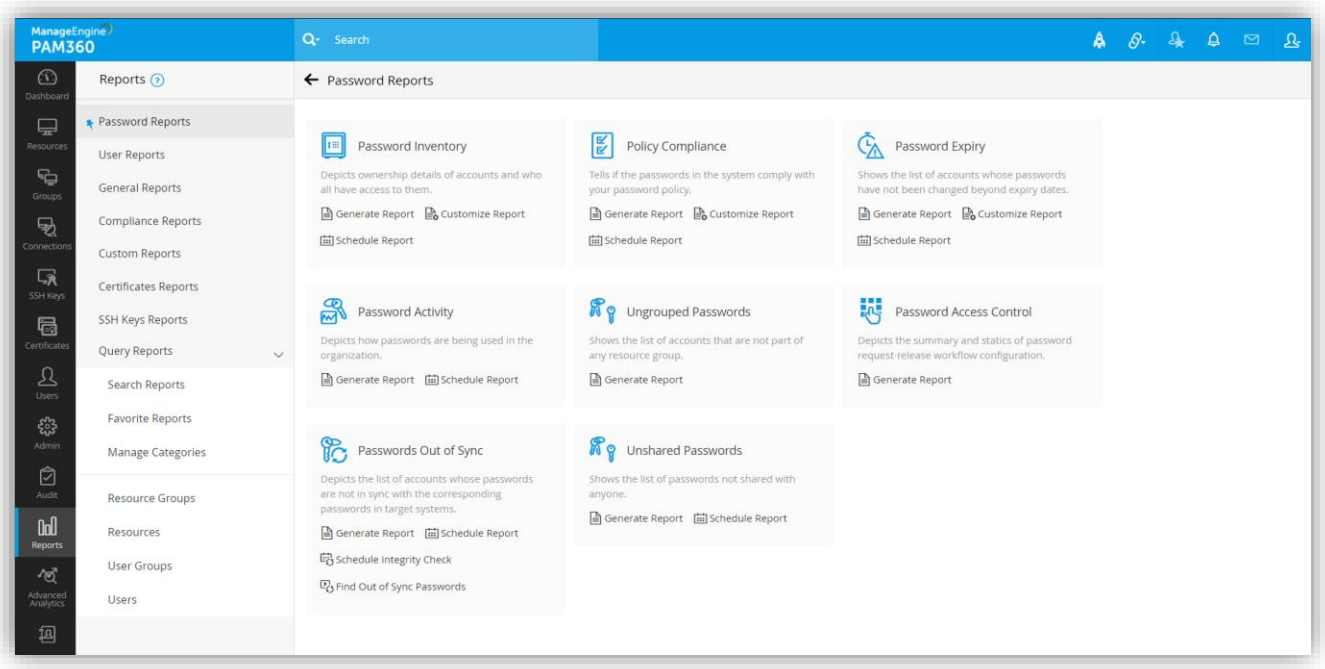
1. Canned Reports

PAM360 provides four types of canned reports:

1.1 Password Reports

All details related to device properties such as hardware properties, firmware details, audit details of the devices, etc., are presented using Password reports. To access Password reports:

1. Navigate to **Reports >> Password Reports.**



2. You will see multiple report types under this report category. The following table describes each report type in detail:

Report Name	What does it Convey	Additional Information
Password Inventory Report	This report provides a snapshot of details about the total number of resources, passwords, resource types and users present in PAM360. Besides, it provides details about the ownership of each password/resource and details about the time at which the passwords were accessed. There are three sections in this report: **Password Inventory - Summary Report** This section lists down the details in summary about the total number of resources, total number of passwords, total number of users and total number of resource types. **Password Distribution by Resource Type**	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links **"Export to PDF"/Export to XLS** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
	This section provides a pie-chart showing the number of resources based on the resource types. **Password Inventory- Detailed Report** This section lists down the details of all the resources passwords, resource types and users present in PAM360. Besides, it provides details about the ownership of each password/resource and details about the time at which the passwords were accessed.	
PolicyCompliance Report	This report provides a snapshot of details about the passwords that comply to the password policy set by the administrator and the ones that do not comply. Besides, it provides details about the ownership of each password. Also, in the case of the passwords which are found to be non-compliant, details about non-compliance are also provided. This helps in taking the required corrective action immediately to make them compliant. There are three sections in this report: **Password Policy Compliance Summary** This section lists down the details in summary about the total number of passwords, total number of passwords that comply to the policy and total number of passwords that are non-compliant. **Policy Violation by Resource Type** This section provides a pie-chart showing the number of passwords that are non-compliant to the defined policy based on	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links "Export to PDF"/Export to XLS and "Email this Report" to do the required operation.

Report Name	What does it Convey	Additional Information
	the resource type. **List of Password Policies** This section lists down all policies that have been created. Details about each policy can be easily viewed by simply clicking on the name of each policy. **Policy Compliance Status** This section lists down the compliance details of all the resources (whether they are compliant with the defined policy or not). It also depicts the number of violations in each resource and the ownership details of resources and passwords in tabular form. You can make a search in this report by clicking the icon present at the top-right hand corner of the table.	
Password Expiry Report	This report provides information about the validity details of passwords. In other words, it provides details about the passwords that have expired and the passwords that are valid. There are three sections in this report: **Password Expiry - Summary** This section lists down the details in summary about the total number of passwords, total number of expired passwords and total number of valid passwords. **Resource Types and Expiry Status** This section provides a pie-chart showing the number of expired passwords in each resource type. **Expiry Status of Passwords**	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
	This section lists down the expiry/validity details of all the resources. It also depicts the number of expired/valid passwords in each resource and the ownership details of resources and passwords in tabular form. You can make a search in this report by clicking the icon present at the top-right hand corner of the table.	
Password Activity Report	This report provides information about the usage details of all passwords in the system. It provides details about the passwords that were most accessed during a specific time period, the ones that were least accessed, average access per day, per week, passwords that were frequently reset etc. There are six sections in this report: **Activity Statistics - Summary Report** This section lists down the details in summary about the total number of passwords, average access per day/ per week, average password age, the number of passwords for which reset is supported, number of passwords that were reset using agents, number of passwords that were reset without agents, number of failures in password reset **Most Accessed Passwords** This section provides a graph showing the top 10 passwords that were accessed most. **Frequently Reset Passwords** This section provides a graph showing the top 10 passwords that were reset most. **Least Accessed Passwords**	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
	This section provides a graph showing the least accessed 10 passwords. **Rarely Changed Passwords** This section provides a graph showing the least reset 10 passwords. **Password Activity Details** This section provides the following details about the passwords that are in sync with the target systems: Date of creation of the password, number of times the password had been accessed from the date of creation, number of time the password underwent changes, the time at which the password was accessed/changed last, the frequency at which the password is being accessed every day, the frequency at which the password is being changed every week etc. **List of resources for which access control workflow has been activated** This section lists all the resources for which password access control workflow has been activated **List of resources for which access control workflow has been deactivated** This section lists all the resources for which password access control workflow has been deactivated **List of resources for which access control workflow has not been configured** This section lists all the resources for which password access control workflow has not been configured at all	

Report Name	What does it Convey	Additional Information
Password Access Control - Resource	This report provides a detailed summary of how password request-release workflow configuration for resources is configured and used. The report contains the details of resources for which Resource-level access control is configured. In addition, the report provides a list of password access requests raised, approved and denied in the specified number of days (a minimum of 5 and a maximum of 30 days). You can also view the list of passwords checked out and checked in during a specified number of days. The report contains the following sections: **Access Control Activated** This section lists all the resources for which Resource-level Access Control is activated. **Automatic Approvals** This section lists all the resources for which an auto-approval time frame is configured. **Access Control Not Configured** This section lists all the resources for which Access Control is not configured. **Access Control Deactivated** This section lists all the resources for which Access Control is currently deactivated. **Excluded Accounts From Resource Access Control** This section lists all the resources which are currently excluded from Resource-level Access Control.	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links **Export to PDF**, **Export to XLS** or **Email this Report** to do the required operation.

Report Name	What does it Convey	Additional Information
	List of password access requests raised in the last X no. of days This section lists all the password access requests raised in the specified number of days. **List of password access requests approved in the last X no. of days** This section lists all the password access requests approved in the specified number of days. **List of password access requests denied in the last X no. of days** This section lists all the password access requests denied in the specified number of days. **List of passwords checked out in the last X no. of days** This section lists all the passwords checked out in the specified number of days. **List of passwords checked in during the last X no. of days** This section lists all the passwords checked in during the specified number of days.	
Password Access Control - Account	This report provides a detailed summary of how password request-release workflow configuration for accounts is configured and used. The report contains the details of resources for which Account-level access control is configured. In addition, the report provides a list of password access requests raised, approved and denied in the specified number of days (a minimum of 5 and a maximum of 30 days).	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links **Export to PDF**, **Export to XLS** or **Email this Report** to

Report Name	What does it Convey	Additional Information
	You can also view the list of passwords checked out and checked in during a specified number of days. The report contains the following sections: **Access Control Activated** This section lists all the accounts for which Account-level Access Control is activated. **Automatic Approvals** This section lists all the accounts for which an auto-approval time frame is configured. **Access Control Deactivated** This section lists all the accounts for which Access Control is currently deactivated. **List of password access requests raised in the last X no. of days** This section lists all the password access requests raised in the specified number of days. **List of password access requests approved in the last X no. of days** This section lists all the password access requests approved in the specified number of days. **List of password access requests denied in the last X no. of days** This section lists all the password access requests denied in the specified number of days. **List of passwords checked out in the last X no. of days**	do the required operation.

Report Name	What does it Convey	Additional Information
	This section lists all the passwords checked out in the specified number of days. **List of passwords checked in during the last X no. of days** This section lists all the passwords checked in during the specified number of days.	
Passwords Out of Sync Report	Passwords of resources such as servers, databases, network devices and other applications are stored in PAM360. It is quite possible that someone who have administrative access to these resources could access the resource directly and change the password of the administrative account. In such cases, the password stored in PAM360 would be outdated and will not be of use to the users who access PAM360 for the password. PAM360 provides option for checking the integrity of passwords at any point of time on demand and also at periodic intervals. You can create a scheduled task for carrying out the integrity check at periodic intervals. Click **"Schedule Report"** and fill in the details. You can also generate this report at any point of time by clicking the link **"Generate Report"**. When you do so, you will get the results of the automatic integrity check done by PAM360 at 1 AM every day for all the accounts for which remote synchronization has been enabled. The results of the current day's check done at 1 AM will be depicted in the report.	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
	In case, you want to carry out integrity check at any moment on demand to get latest details, you need to click the option **"ScheduleIntegrity Check"**. PAM360 will try to establish connection with the target systems for all the accounts for which remote password reset has been enabled. Once the connection is established, it tries to login with the credentials stores in PAM360. If login does not succeed, PAM360 concludes that the password is out of sync. In case, PAM360 is not even able to establish connection with the system due to some network problem, it will not be taken as password out of sync. A consolidated notification would be emailed to all the administrators and auditors. The Passwords Out of Sync report provides information if the passwords in the system are in sync with the corresponding passwords in the target systems. There are two sections in this report: **Password Integrity Statistics** This section lists down the statistical details in summary about the total number of passwords for which reset is supported, passwords for which reset is done using agents, number of passwords that were reset using agents, number of passwords in the system are in sync with the corresponding passwords in the target systems, number of passwords that are out of sync etc. **Passwords Out of Sync Distribution** This section displays a pie-chart that portrays the distribution of passwords (that are out of sync) across resource types.	

Report Name	What does it Convey	Additional Information
	Passwords Out of Sync Details This section provides an expanded list of passwords, mentioning which of them are not in sync, who owns them, and their resource type.	
Ungrouped Passwords Report	Provides complete details about the password access control workflow scenario of your organizations. List of resources for which access control has been enabled, resources for which access control is activated/deactivated, resources for which the requests are automatically approved, list of password release requests approved/denied etc are depicted through this report.	This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links "Export to PDF"/Export to XLS and "Email this Report" to do the required operation.
Unshared Passwords	Passwords stored in PAM360. Certain passwords may not be shared with anyone. Such unshared passwords are listed in this report.	

1.2 User Reports

Report Name	What does it Convey	Additional Information
User Access Report	This report provides details about all users in the system with reference to password and resource access. This report has three sections: **User Statistics - Summary Report** This report can be generated in the form of PDF and can be emailed to	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
	required recipients. Click the links "Export to PDF" and "Email this Report" to do the required operation. Details such as the number of new users added during the last five days, users deleted, role change, number of invalid login attempts, users who carried out password reset during the past five days, users who did not login during the last five days, total number of users/user groups in the system, user roles etc are presented as part of this report. **User Activity Summary Report** The actions performed by users on passwords such as password retrieval, password reset etc captured as part of this summary report. This report provides the number of such actions done by each user. Similarly, the number of password actions performed by members of each user group are also depicted. **User Access Details** The resources and resource groups that are owned by/shared to each user are depicted as part of this report. The privileges allowed for the user are also listed. **User Group Access Details** The list of users who are members of the group, resource groups that are owned by/shared to the user group are depicted as part of this report.	
User Activity Report	This report provides details about the password usage of all the users in the	This report can be generated in the form of

Report Name	What does it Convey	Additional Information
	system. This report has the following sections: **Activity Statistics - Summary Report** The total number of passwords accessed by users and user groups during a specified time period are depicted in the form of graphs. **Most Active Users - Login/Access/Reset** The list of the top 10 users who performed most login attempts, most password access and most password resets. **Least Active UsersUsers - Login/Access/Reset** The list of 10 users who performed least login attempts, least password access and least password resets. **User Activity Details** All details about users, including the total number of login attempts made, number of invalid attempts, number of passwords accessed, number of passwords reset are depicted.	PDF or spreadsheet and can also be emailed to required recipients. Click the links **"Export to PDF"/Export to XLS and "Email this Report"** to do the required operation.
Ungrouped Users	Users in PAM360 can be grouped into user groups. Certain users may not be a part of any user group. Such users and the passwords owned by them are listed in this report.	

1.3 General Reports

Report Name	What does it Convey	Additional Information

Executive Report	This report provides a snapshot of all password access and user activities in the system. It is a combined report of Password and User reports. It provides details, in summary, about the following: Password Statistics, Password Activity, Password Policy, Password Expiry, Password Out of Sync, User Statistics and User Activity.	This report can be generated in the form of PDF and can be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

1.4 Compliance Reports

Report Name	What does it Convey	Additional Information
PCI DSS Compliance Report The PCI DSS stands for Payment Card Industry Data Security Standard. It is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It represents a set of rules that need to be adhered to by businesses that process credit cardholder information, to ensure data is protected. The PCI Data Security Standard is comprised of 12 general requirements designed to: • Build and maintain a secure network • Protect cardholder data • Ensure the maintenance of	This reports the violations in your network from the requirements of Payment Card Industry (PCI) Data Security Standard (DSS), relevant to the use and management practices of shared administrative, software and service account passwords of various systems. PCI DSS requirements **2,3,7,8,10 & 12** are covered in this report. **Note:** In order to adhere to "all" the requirements of the PCI DSS standard completely, you will need other tools and security procedures to be implemented.	You have the option to generate separate compliance reports for each PCI DSS requirement 2,3,7,8,10 & 12. You can also generate a consolidated PCI DSS report too. This report can be generated in the form of PDF and can be emailed to required recipients. Click the links **"Export to PDF"** and **"Email this Report"** to do the required operation.

Report Name	What does it Convey	Additional Information
vulnerability management programs • Implement strong access control measures • Regularly monitor and test networks • Ensure the maintenance of information security policies This standard is governed by PCI Security Standards Council https://www.pcisecuritystandards.org/		
ISO/IEC 27001 Compliance Report ISO/IEC 27001 is a specification developed to "provide a model for establishing, operating, monitoring, reviewing, maintaining, and improving an information security management system (ISMS). Simply put, ISO 27001 is a robust framework that helps you protect information such as financial data, intellectual property or sensitive customer information. The standard also stresses on the selection of adequate security controls that help protect information assets. In all, ISO 27001 has ten short clauses and also an Annex A. The Annex A alone specifies numerous control frameworks. Among them, A.9 deals with "Access Control." The clause basically requires the use of • A robust information security policy is in effect to ensure only authorized users have access to	This report communicates an organization's compliance level in relation to the control requirements as outlined in the clause A.9. The compliance will be based on various factors such as stringent password policies for privileged accounts in the enterprise, authentic audit records, strong authentication mechanisms, secure privileged access, and data security levels. A consolidated ISO/IEC 27001 compliance report will include information about the controls listed under A.9.1, A.9.1.1, A.9.1.2, A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3, A.9.3.1, A.9.4, A.9.4.1, A.9.4.2 and A.9.4.3. There are also option to generate separate compliance reports for requirements listed under	1. This report can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links "Export to PDF"/Export to XLS and "Email this Report" to do the required operation. 2. These compliance reports help address requirements only in select clauses of each security standards. In order to adhere to "all" the requirements of ISO 27001 other tools and security

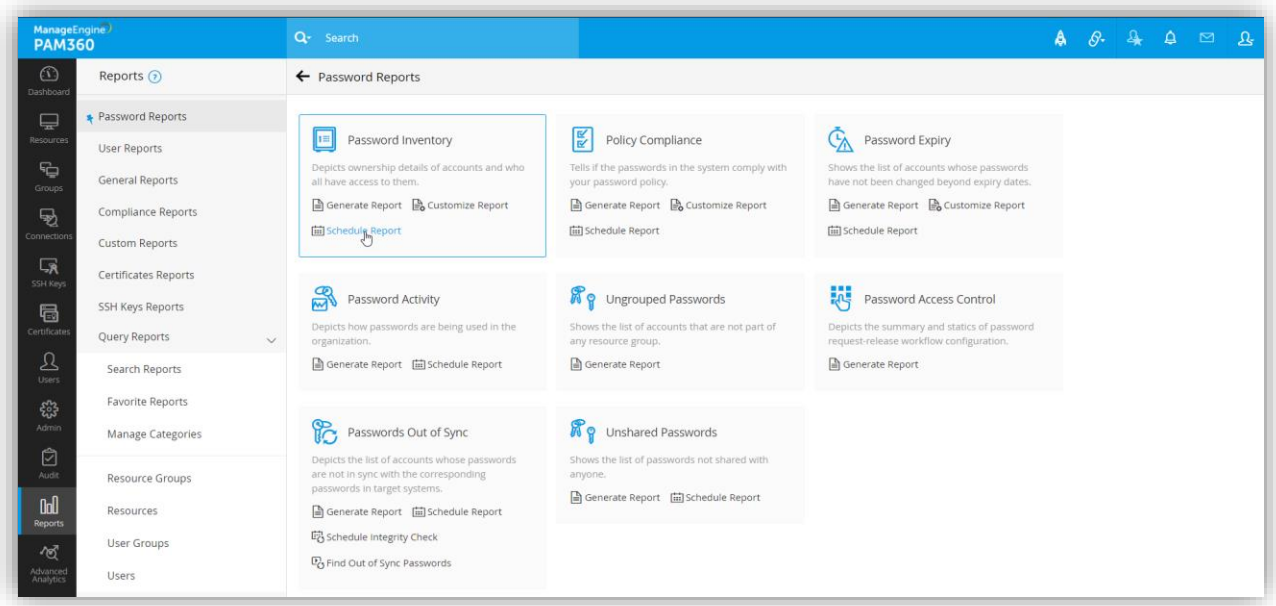
Report Name	What does it Convey	Additional Information
critical systems. • All users are uniquely identified and have established accountability for all privileged activities. • Access is only allowed to systems through secure mechanisms. • Sensitive information is protected with cryptographic controls.	each sections given above.	procedures should be implemented.
NERC CIP Compliance Report The NERC CIP standards is a set of requirements designed to ensure the security and eliability of the power systems. The North American Electric Reliability Corporation (NERC) introduced the Critical Infrastructure Protection (CIP) standards mainly to protect the critical assets such as electric utilities generation and transmission systems in the power grid. Broadly, NERC CIP has nine sections that cover various physical, virtual, and organizational measures that must be enforced to secure the bulk power system. In particular, the clauses CIP-004-3a, CIP-005-3a, and CIP-007-3a mandate. • A regular review of authorized personnel with access to critical systems. • Granular access controls based on functional roles.	This reports shows an organization's level of compliance with select requirements of clauses CIP-004-3a, CIP-005-3a, and CIP-007-3a. The report will help auditors understand the various security measures implemented in the concerned organization, such as privileged access control policies, authentication checks for privileged users, user activity auditing, privileged session recording & monitoring, and password policy enforcement. Apart from a consolidated NERC CIP report, there are also options to generate separate compliance reports for requirements specific to each clauses, i.e. CIP-004-3a, CIP-005-3a, and CIP-007-3a.	This reports can be generated in the form of PDF or spreadsheet and can also be emailed to required recipients. Click the links **"Export to PDF"/Export to XLS** and **"Email this Report"** to do the required operation. These compliance reports help address requirements only in select clauses of each security standards. In order to adhere to "all" the requirements of NERC CIP, other tools and security procedures should be implemented.

Report Name	What does it Convey	Additional Information
• Robust authentication methods. • Comprehensive auditing of security events. • Monitoring of user activity during privileged sessions. • Use of strong passwords with reliable complexities.		

1.5 Scheduling Report Generation

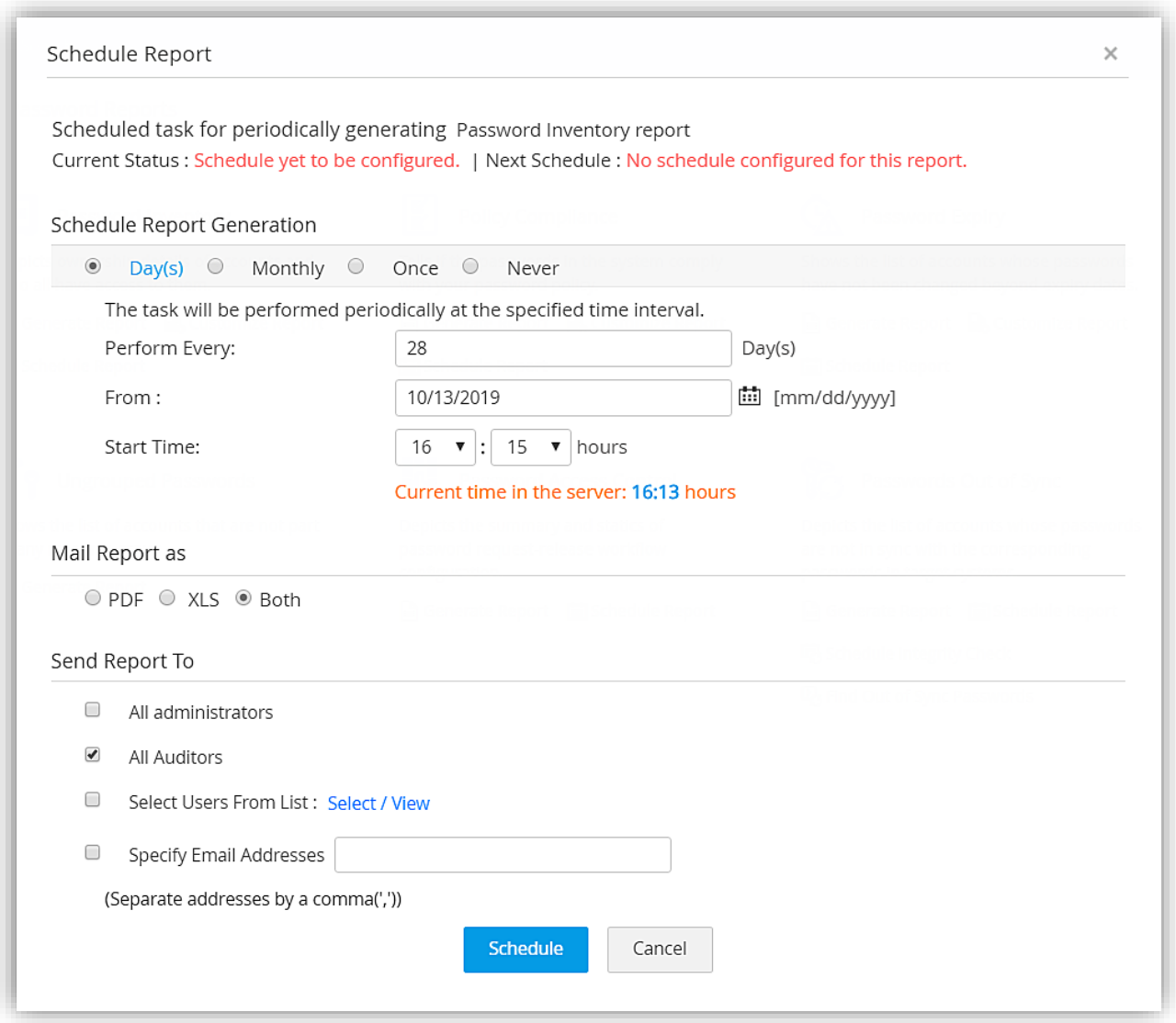
All reports can be scheduled to be generated at periodic intervals. The reports thus generated can be sent via email to required recipients. To create a schedule for any report:

1. Navigate to **Reports** tab.
2. Click the link **Schedule Report** available under the name of each report.

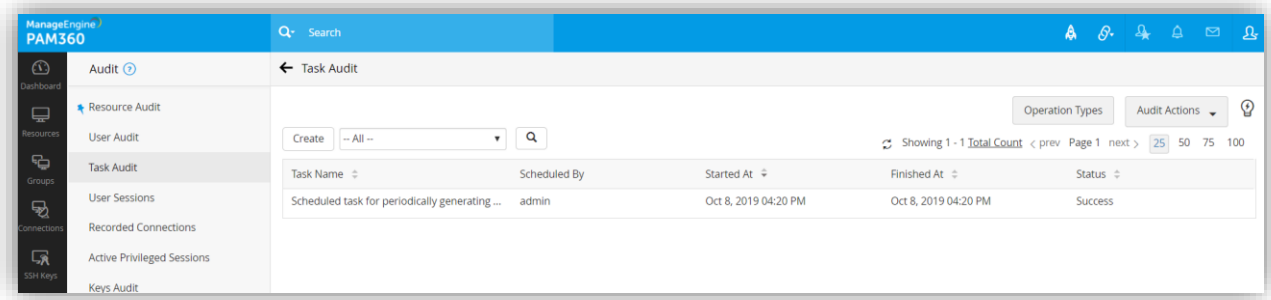


3. In the pop-up form that opens, select the required schedule from the provided terms - Days / Monthly / Once / Never.
4. Next, enter the date / time at which the schedule has to commence.

5. Choose the format in which the report has to be mailed to the recipients, PDF or XLS or both.
6. Select the recipients to whom the report should be mailed to, from the given options.
7. You can also enter the list of email ids to which the report has to be emailed.
8. Click **Schedule**.

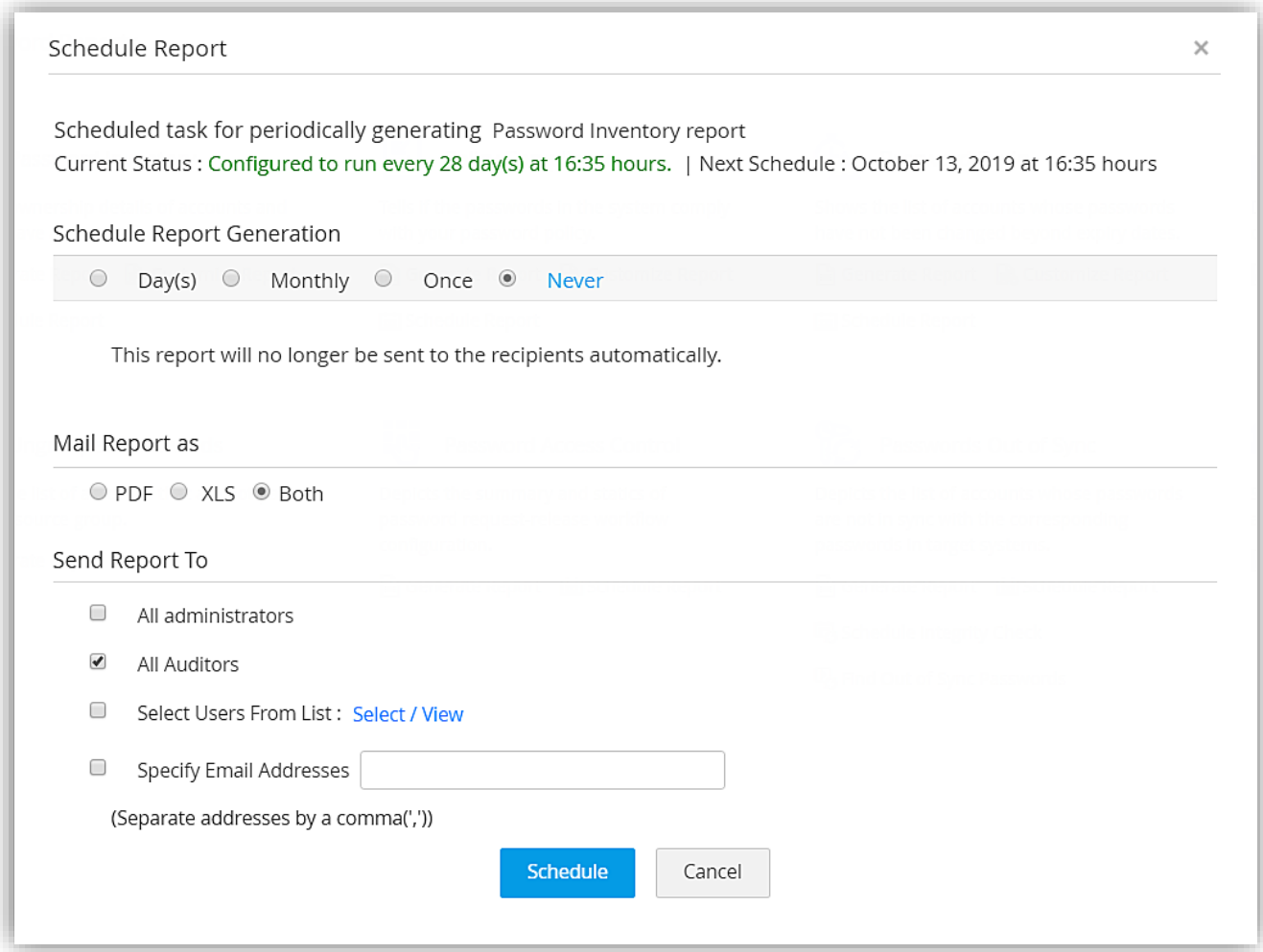


The result of the scheduled task created here are audited and can be viewed from the **Task Audit** section.



1.6 Steps to Terminate an Existing Schedule

1. Click the link **Schedule Report** available under the name of report (for which the schedule has to be terminated).
2. In the window that opens, select the option **Never**.
3. Click **Schedule**. The schedule will be terminated.



2. Custom Reports

You can create customized reports out of the four canned reports (Password Inventory, Password Compliance, Password Expiry and Password Integrity) and two audit reports (Resource Audit and User Audit). You can specify certain criteria and create customized reports as per your needs.

The custom reports have been designed to bring out specific information from the PAM360 database as per your needs. The canned reports provide a snapshot of details in general. On the other hand, you can create a custom report out of this canned report to get specific details.

Examples

Example: 1

For instance, let us take the case of creating a custom report out of Password Inventory Report. Assume that you want to get a report on the resources owned by 'User A' in 'Network Administration' department. You can create a custom report from the 'Password Inventory Report' by specifying the criteria as Resources from 'Department' 'Network Administration' AND 'Owner' name as 'User A'.

The real power of the custom reports lies in the fact that you can specify criteria expression and cull out information catering to your more specific needs.

Example: 2

Assume that your need is to take a list of all the sensitive passwords belonging to the resource types Windows and Windows Domain, Linux and Cisco, owned by a particular administrator - say John. Also, you want to get details on the share permissions for those passwords - with whom the passwords have been shared.

Here, the following are the conditions:

- Sensitive accounts with names 'administrator' on Windows and Windows Domain, 'root' on Linux and 'enable' on Cisco are to be identified
- Among such accounts, only those that are owned by john are to be identified

So, the criteria will be as follows:

To identify the 'administrator' accounts on Windows/Windows Domain, the criteria is

- **Resource Type** starts with Windows (take this as column C1)
- **Account Name** is administrator (take this as column C2)

To identify the 'root' accounts on Linux, the criteria is

- **Resource Type** is Linux (take this as column C3)
- **Account Name** is root (take this as column C4)

To identify the 'enable' accounts on Cisco devices, the criteria is

- **Resource Type** contains Cisco (take this as column C5)
- **Account Name** is root (take this as column C6)

To identify the resources owned by john

- **Owner** is John (take this as column C7)

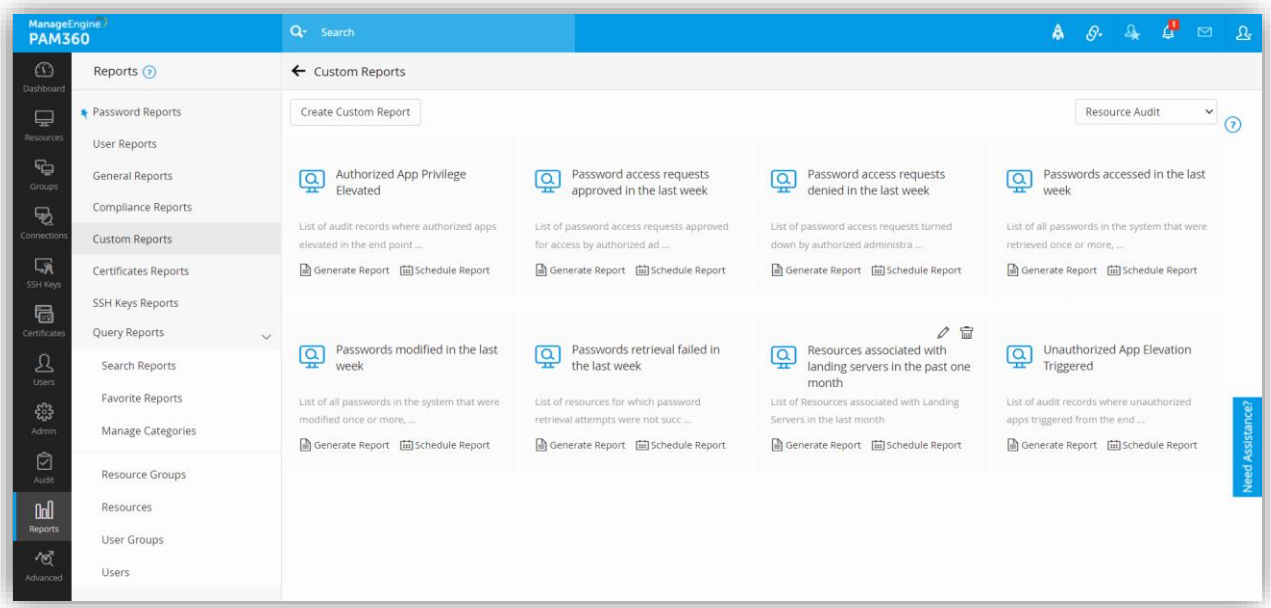
Now, you need to specify the criteria expression to combine the above factors:

((C1 and C2) or (C3 and C4) or (C5 and C6)) and C7

That means, you want to identify the resources/accounts complying to any and all the criteria listed above and finally match the ownership.

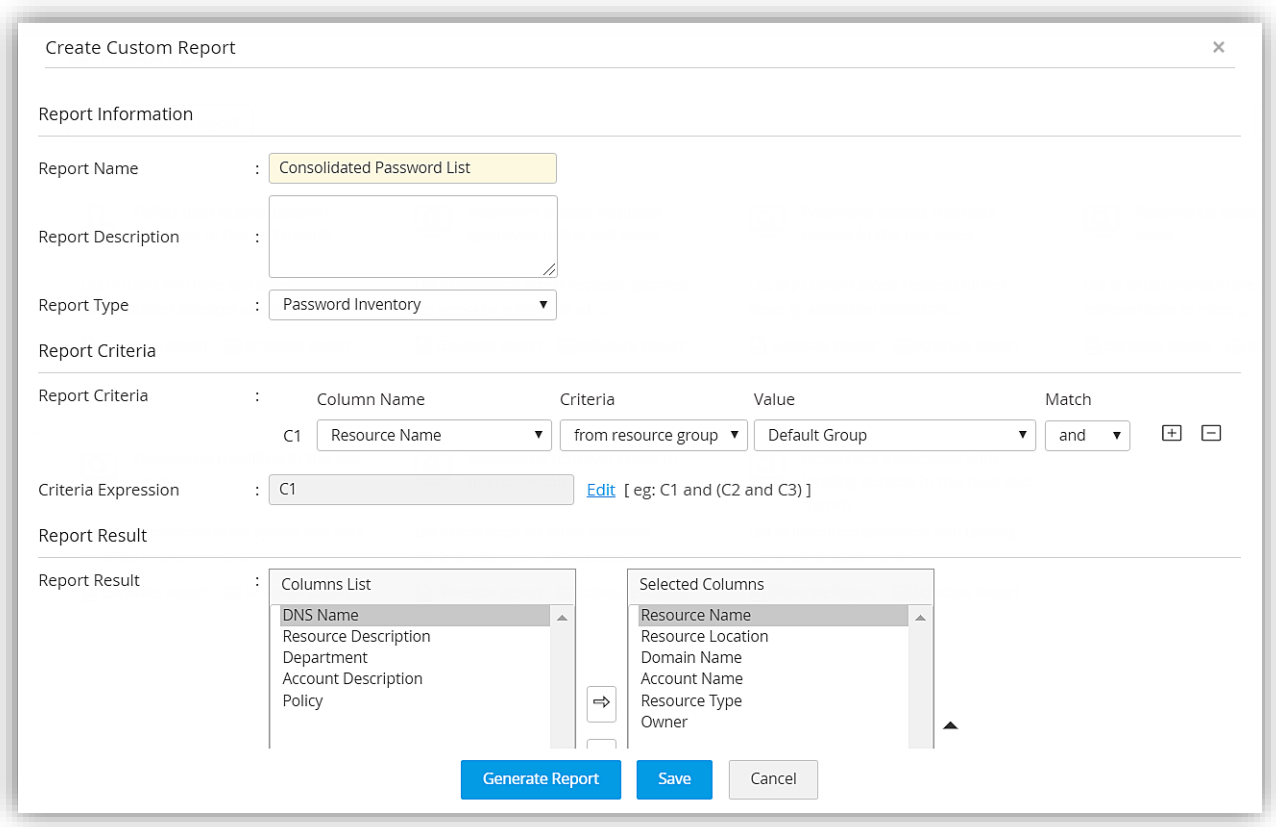
2.1 Steps to Create Custom Reports

1. Navigate to **Reports >> Custom Reports**.
2. Click the link **Create Custom Reports** available on top left hand corner.



3. In the pop-up form that opens, provide a name for the custom report being created; enter description for easy identification of the report.
4. Select the type of report out of which you wish to create the custom report.

5. **Specify the criteria** based on which the custom report has to be created. Refer to the example above on specifying the criteria. In case, you want to specify multiple values for the same **column name, enter the entries in comma separated form**. In the example above, in case, you want to generate the report pertaining to two departments - Network Administration **and** Finance departments, enter the values for the column **'Department'** as Network Administration,Finance.
6. To specify advanced criteria, edit the **control expressions** field; you can specify advanced conditions using expressions.
7. To control the number and order of columns to be displayed in the custom report. From **Select Columns** on LHS, choose the required columns. Use the up, down arrows on the RHS to control the arrangement of the columns in the report
8. Click **Save** to save the entries.
9. Click **Generate Report** to generate the customized report.



2.2 Custom Reports - Use Case

By leveraging the power of the custom reports, you can meet many of your auditing requirements with ease. Following is just one use case:

Exit Audit Report

Continuously assessing the vulnerability with respect to password access is one of the important auditing requirements. When an administrator, who had active access to the privileged passwords leaves the organization, it is imperative to assess the vulnerability. This requires taking a list of all the passwords that were accessed by the particular user during a specified time period and then initiate steps to change the passwords.

Taking a report on all the password management operations performed by the particular administrator during a specified time period, could serve as 'Exit Audit Report'. Custom reports help you generate a report to achieve this precisely. All that you need to do is to get the report out of the 'Resource Audit'.

- Specify the time period for the custom report.
- Select the criteria as **Operation Type** contains (C1) (just leave the criteria field blank to represent that you want to take a report on all operations).
- **'Operated by' 'User A'** (C2) who is leaving the organization.

The resultant report will provide you with a list of password management operations performed by the particular administrator during the time range specified.

Custom Reports out of 'Resource Audit' and 'User Audit' would prove highly useful as you would be able to meet most of your auditing requirements by properly leveraging them.

The resultant report will provide you with a list of password management operations performed by the particular administrator during the time range specified.

Query Reports

You can create query reports to get specific data from PAM360 database, by either writing your own SQL query or customizing a SQL query from existing reports under this category.

With query reports, you can use SQL statements to query the database directly, fetch information from provided tables, and format the data into a report. For instance, using queries, you can create reports for the following sample scenarios (Scope not limited to this list):

1. Passwords that haven't been changed after being used for auto-logon to target system
2. Passwords that haven't been changed at all after resource creation.
3. List of identical user groups (Groups that have the same set of users)

This section walks you through the following topics:

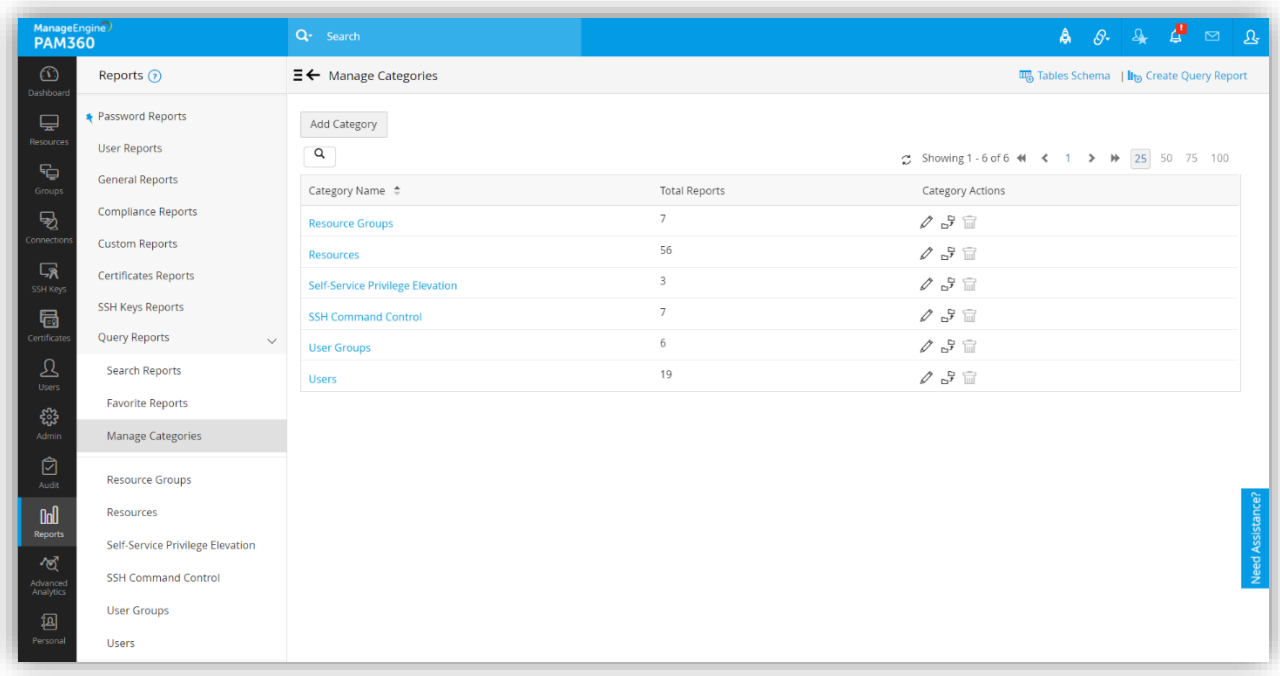
1. **Creating Query Reports**
2. **Use Case Scenarios**
3. **Scheduling Query Reports**
4. **Terminating an Already Created Schedule**
5. **Creating Favorite Reports**
6. **Managing Categories**

1. Creating Query Reports

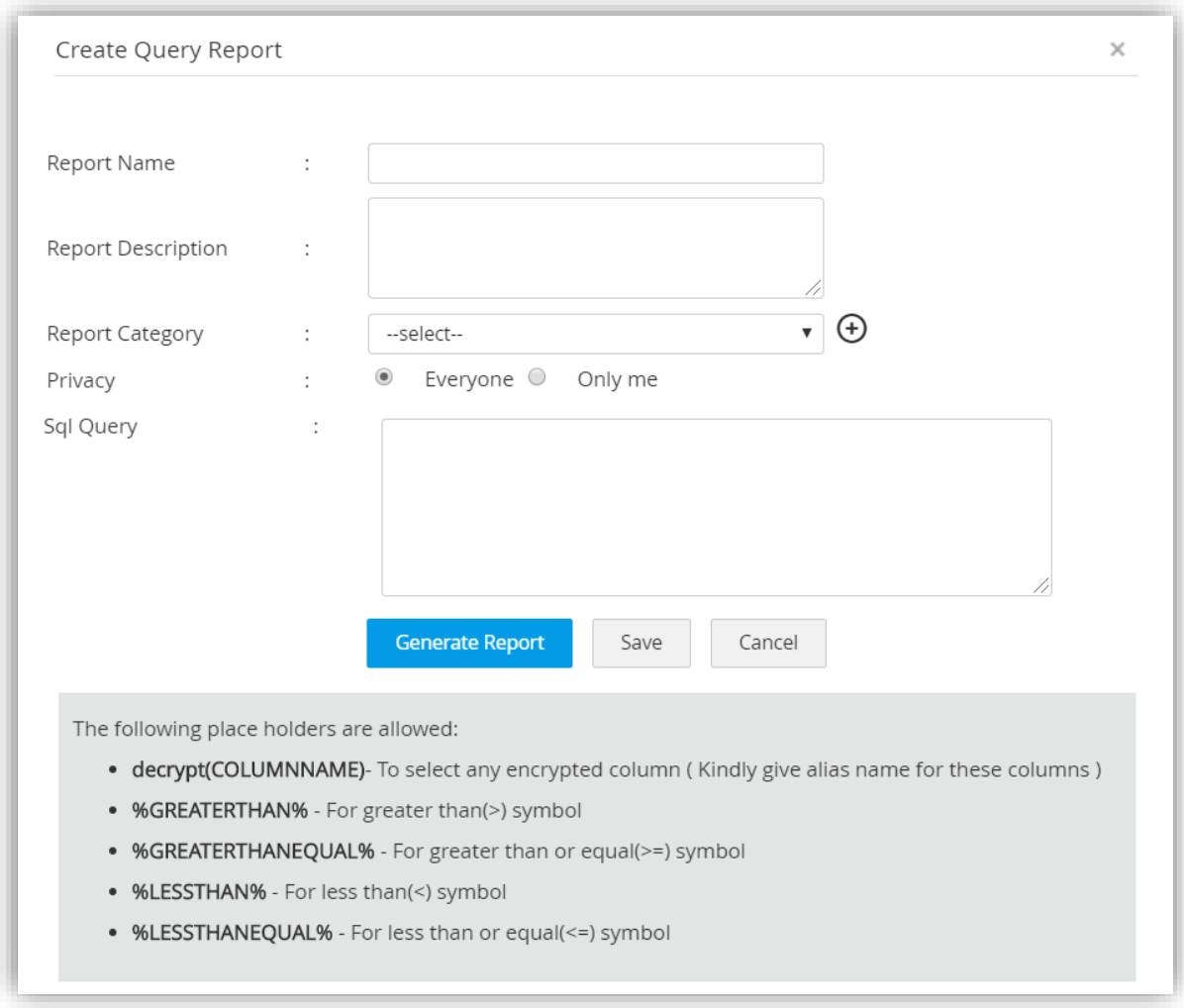
You can run query reports in PAM360 in two ways, either by using default queries or by constructing your own SQL query by referring to the Tables Schema displayed in the product GUI. Default query reports can be found under pre-defined categories - Resource Groups, Resources, User Groups, and Users.

You can use these default reports as such or edit the queries and save them as new reports. Or, to create a new query from scratch using your own SQL query, follow the steps given below:

1. Navigate to **Reports >> Query Reports**.
2. Click **Create Report** available on top right corner.



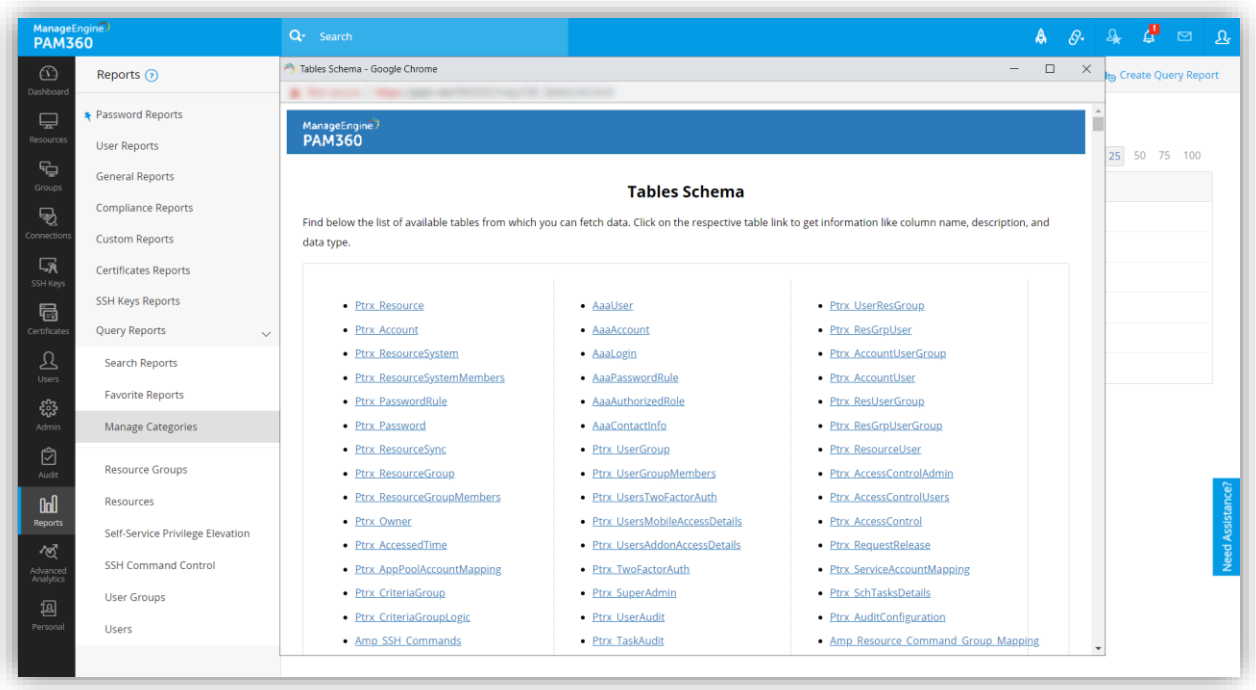
3. In the GUI that opens, provide a name for the query report being created; also enter a description for easy identification of the report.



4. Next, select **Report Category** for the report. You can either choose one of the pre-defined categories or add a new category. To create a new category, click on **Add New** option beside the Report Category field.

5. Set **Privacy** for the report - **Everyone** (or) **Only me** - depending on data sensitivity and need.

6. Enter the SQL query to get the required information from the database. To know the available database tables from which you can query information, refer to the **Tables schema** given at the top left hand corner of the UI as shown below:



7. Once you have entered the query, click **Generate Report**. If you have created the report for future use, click **Save**. The report will be saved.

8. While writing your own SQL query, following are the placeholders that can be used:

   decrypt(COLUMNNAME) - To select any encrypted column While using encrypted columns, remember to give them alias names.

   How to know whether a column is encrypted? To know which columns are encrypted, go to **Query Reports >> Tables Schema**.

   In the dialog box that opens up, scroll down to the list that displays the column name, description, and data type of each table. Under data type, look for **SCHAR**. Columns of the data type SCHAR are encrypted.

Column name	Description	Data type
RESOURCEID **(PK)**	Unique Identifier of the Resource	BIGINT
PASSWDRULEID	Table header	BIGINT
RESOURCENAME	The Resource Name which is a unique name for a System or Service	SCHAR
DOMAINNAME	Domain Name of the resource	CHAR
SSHPORT	SSH connection port	BIGINT
ALACCID	Unique identifier of the Auto Logon Account	BIGINT
RESOURCEDESC	Any additional details about the resource.	CHAR
LOCATION	Any additional details about the resource.	CHAR
DEPARTMENT	Any additional details about the resource.	CHAR
IPADDRESS	IP address of the resource	CHAR
RESOURCEURL	Resource URI of the resource	CHAR
LASTMONITORSYNCTIME	Last Monitor Sync Time	BIGINT
COLUMN_LONG1	Column for custom long attribute.	BIGINT
COLUMN_LONG2	Column for custom long attribute.	BIGINT
COLUMN_LONG3	Column for custom long attribute.	BIGINT
COLUMN_LONG4	Column for custom long attribute.	BIGINT
COLUMN_CHAR1	Column for custom char attribute.	CHAR
COLUMN_CHAR2	Column for custom char attribute.	CHAR
COLUMN_CHAR3	Column for custom char attribute.	CHAR

Other placeholders:

- **%GREATERTHAN%** - For greater than(>l) symbol
- **%GREATERTHANEQUAL%** - For greater than or equal(>=) symbol
- **%LESSTHAN%** - For less than(<) symbol
- **%LESSTHANEQUAL%** - For less than or equal(<=) symbol

2. Use Case Scenarios

Find below the SQL statements written for a few use case scenarios:

Use Case Scenario 1:

Passwords that haven't been changed after being used for auto-logon to target system.

This report helps you to ascertain whether the passwords checked-out by users for auto-logon to a target system, were reset after use. Resetting a password after user access is critical, since it is possible the user may have noted down the password for future use. Therefore, using this query report, you can get the list of passwords not yet reset after auto-logon and update them instantly

For PGSQL:

```
SELECT Ptrx_Resource.RESOURCENAME AS "Resource Name",
Ptrx_Account.LOGINNAME AS "Account Name",
Ptrx_DummyPwdNotChan.retrievedtime AS "Lastaccessedtime",
Ptrx_ResourceSystem.OPERATINGSYSTEM AS "Type", Ptrx_Resource.LOCATION AS
"Location", Ptrx_Resource.RESOURCEDESC AS "Description" FROM (SELECT
accountid, retrievedtime FROM (SELECT Ptrx_DummyPwdRetr.accountid AS
accountid,Ptrx_DummyPwdRetr.accessedtime AS retrievedtime,
Ptrx_DummyPwdChanged.time AS time FROM (SELECT RESOURCEID, ACCOUNTID,
max(LASTACCESSEDTIME) AS accessedtime FROM Ptrx_UserAudit inner join
Ptrx_AuditConfiguration on
Ptrx_AuditConfiguration.CONF_ID=Ptrx_UserAudit.OPERATIONTYPE WHERE
Ptrx_AuditConfiguration.OPERATION_TYPE='Password Retrieved' AND REASON LIKE
'%auto logon helper reason%' GROUP BY RESOURCEID,ACCOUNTID )
Ptrx_DummyPwdRetr LEFT JOIN ( SELECT ACCOUNTID ,max(LASTACCESSEDTIME)
AS time FROM Ptrx_UserAudit inner join Ptrx_AuditConfiguration on
Ptrx_AuditConfiguration.CONF_ID=Ptrx_UserAudit.OPERATIONTYPE WHERE
Ptrx_AuditConfiguration.OPERATION_TYPE ='Password Changed' GROUP BY
ACCOUNTID) Ptrx_DummyPwdChanged ON
Ptrx_DummyPwdRetr.accountid=Ptrx_DummyPwdChanged.accountid AND
Ptrx_DummyPwdChanged.time %GREATERTHAN%
Ptrx_DummyPwdRetr.accessedtime ) AS Ptrx_DummyPwdRetrAndChan WHERE
Ptrx_DummyPwdRetrAndChan.time IS NULL ) AS Ptrx_DummyPwdNotChan INNER
JOIN Ptrx_Account ON
Ptrx_DummyPwdNotChan.accountid=Ptrx_Account.ACCOUNTID INNER JOIN
Ptrx_Resource ON Ptrx_Resource.RESOURCEID=Ptrx_Account.RESOURCEID INNER
JOIN Ptrx_ResourceSystemMembers ON
Ptrx_ResourceSystemMembers.RESOURCEID =Ptrx_Resource.RESOURCEID INNER
JOIN Ptrx_ResourceSystem ON
Ptrx_ResourceSystem.OSID=Ptrx_ResourceSystemMembers.OSID ORDER BY
Ptrx_Resource.RESOURCENAME
```

Use Case Scenario 2:

Password that haven't been changed at all after resource creation.

Use this report to determine the list of passwords that have not been reset even once after resource creation in PAM360. Periodic password resets are important and this report helps track all the resources that have outdated passwords. You can also rewrite the following query

to find out the passwords haven't been changed for resources, added during a particular period.

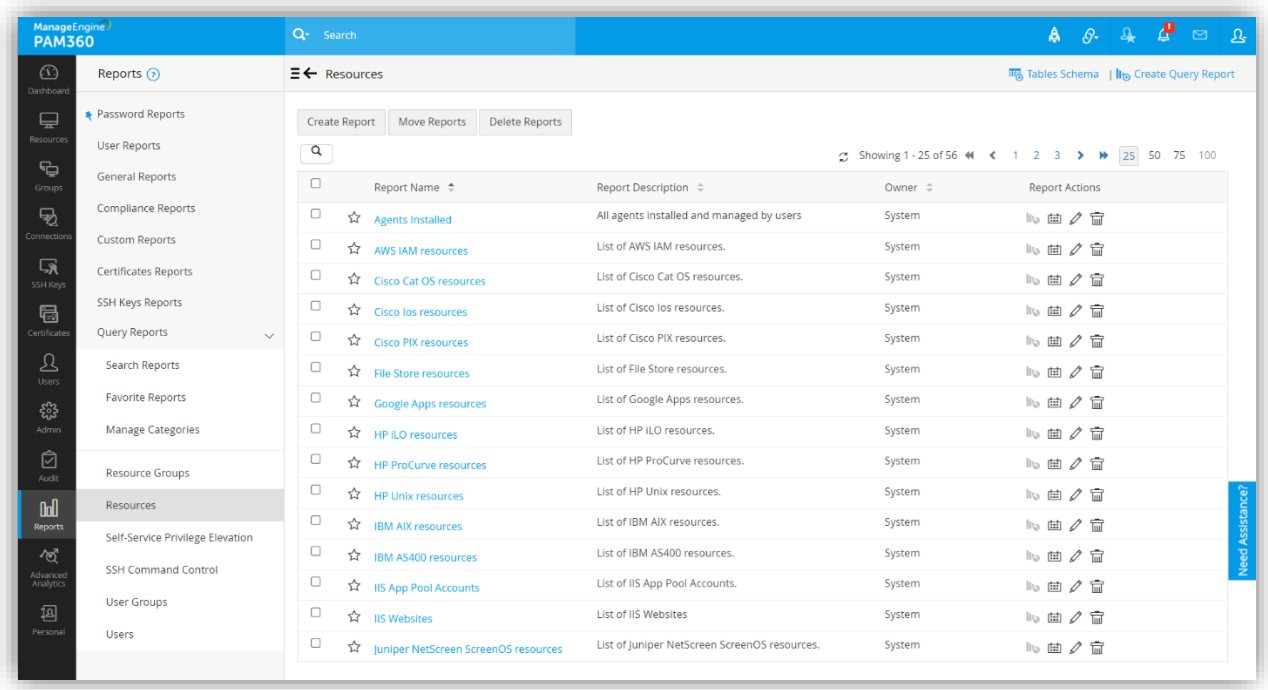
For PGSQL:

```
SELECT Ptrx_Resource.RESOURCENAME AS "Resource Name",
Ptrx_Account.LOGINNAME AS "Account Name",
Ptrx_ResourceSystem.OPERATINGSYSTEM AS "Type", Ptrx_Resource.LOCATION AS
"Location", Ptrx_Resource.RESOURCEDESC AS "Description" FROM ( SELECT
Ptrx_Account.ACCOUNTID AS accountid, Ptrx_Resource.RESOURCEID FROM
Ptrx_Account INNER JOIN Ptrx_Resource ON
Ptrx_Resource.RESOURCEID=Ptrx_Account.RESOURCEID WHERE accountid NOT IN
(SELECT Ptrx_UserAudit.ACCOUNTID FROM Ptrx_UserAudit FULL OUTER JOIN
(SELECT accountid,lastaccessedtime,OPERATION_TYPE FROM Ptrx_UserAudit inner
join Ptrx_AuditConfiguration on
Ptrx_AuditConfiguration.CONF_ID=Ptrx_UserAudit.OPERATIONTYPE WHERE
Ptrx_AuditConfiguration.OPERATION_TYPE LIKE 'Account Added') AS
Ptrx_DummyAccAdded ON
Ptrx_UserAudit.ACCOUNTID=Ptrx_DummyAccAdded.accountid AND
Ptrx_UserAudit.lastaccessedtime %GREATERTHAN%
Ptrx_DummyAccAdded.lastaccessedtime WHERE
Ptrx_DummyAccAdded.OPERATION_TYPE LIKE 'Password Changed' AND
Ptrx_UserAudit.lastaccessedtime BETWEEN Ptrx_DummyAccAdded.lastaccessedtime
AND (Ptrx_DummyAccAdded.lastaccessedtime::timestamp::date)+INTERVAL '5' day )
) AS Ptrx_DummyPwdNotChan INNER JOIN Ptrx_Account ON
Ptrx_DummyPwdNotChan.accountid=Ptrx_Account.ACCOUNTID INNER JOIN
Ptrx_Resource ON Ptrx_Resource.RESOURCEID=Ptrx_Account.RESOURCEID INNER
JOIN Ptrx_ResourceSystemMembers ON
Ptrx_ResourceSystemMembers.RESOURCEID =Ptrx_Resource.RESOURCEID INNER
JOIN Ptrx_ResourceSystem ON
Ptrx_ResourceSystem.OSID=Ptrx_ResourceSystemMembers.OSID ORDER BY
Ptrx_Resource.RESOURCENAME
```

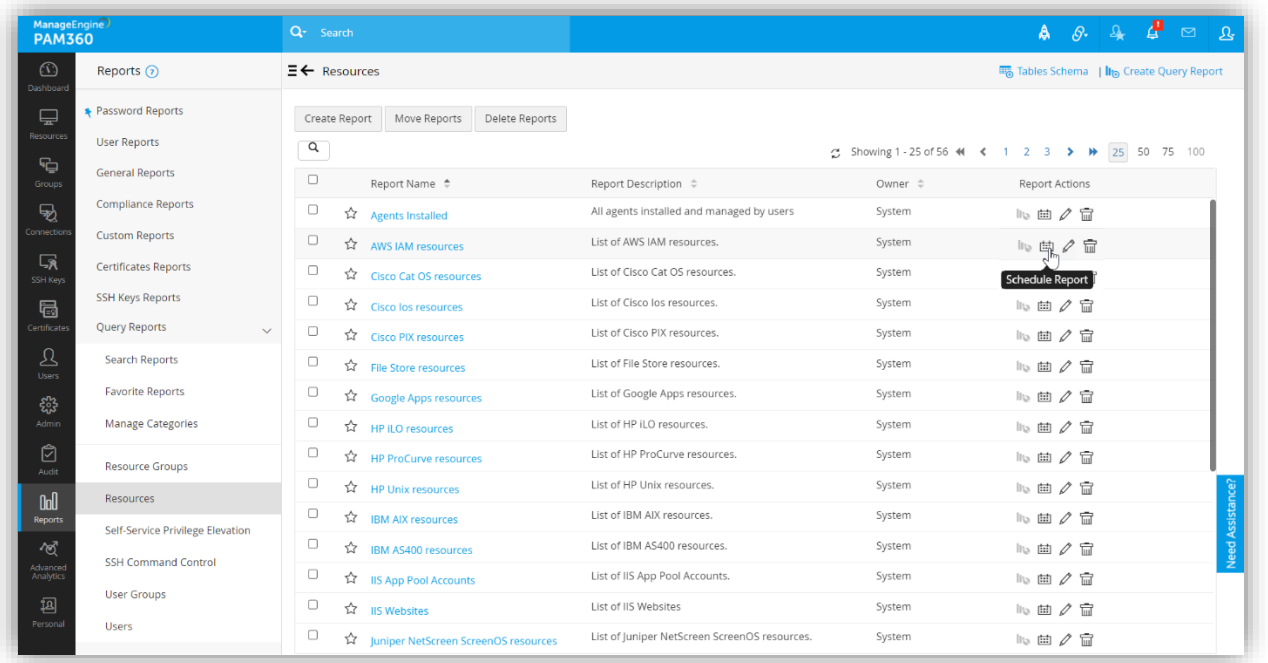
3. Scheduling Query Reports

Once you have created and saved a query report, you can also schedule them to be automatically generated on a periodic basis. Following are the steps required to schedule a report:

1. Navigate to **Reports >> Query Reports >> Resources**. (As shown in the left-hand side of the image below)

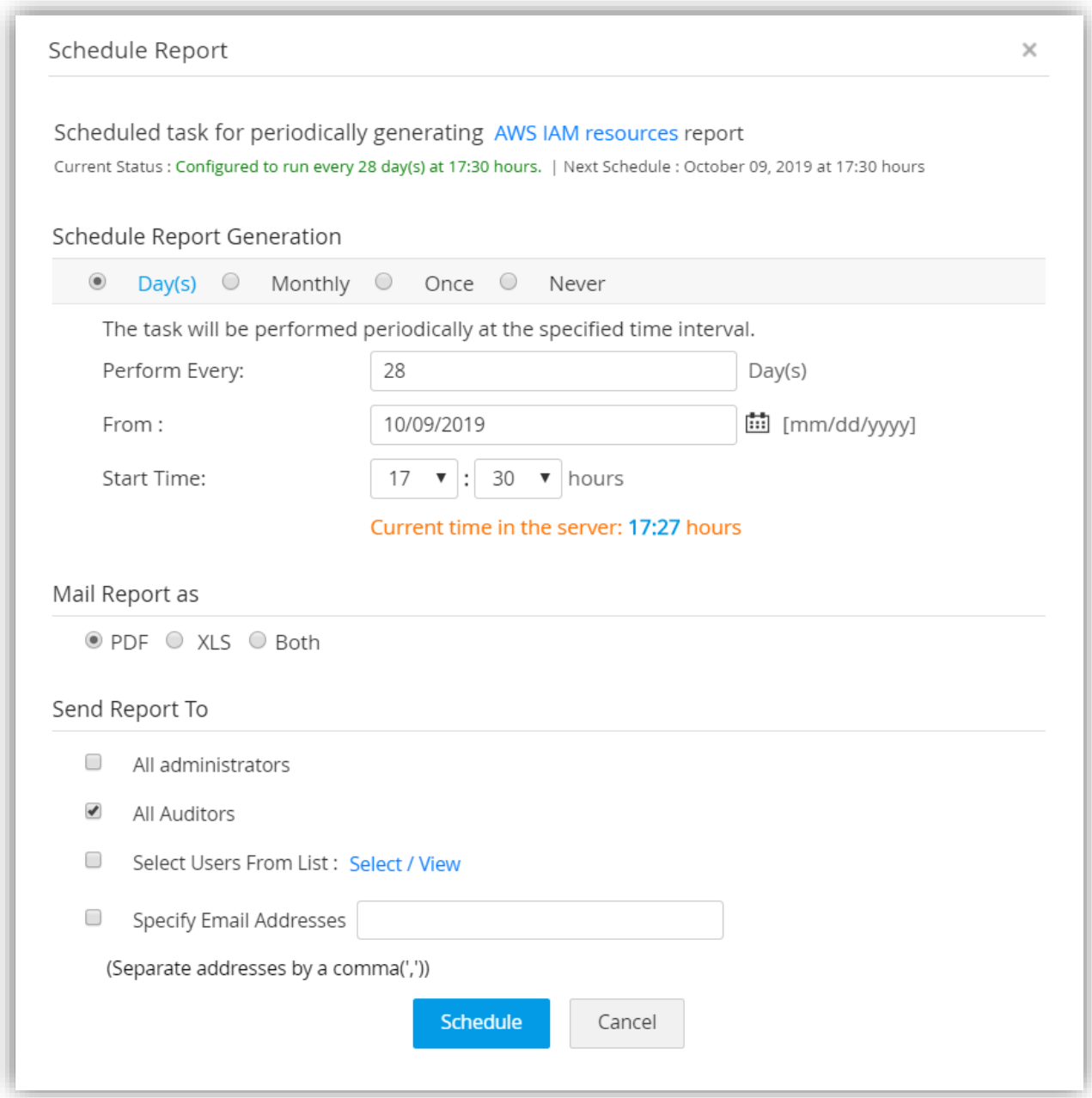


2. Locate the required report and click on the **Schedule Report** icon under Report Actions column beside the report.



3. In the pop up form that opens, select the required schedule - **day(s)/monthly/once**, and also provide the **date/time** at which the schedule has to commence.

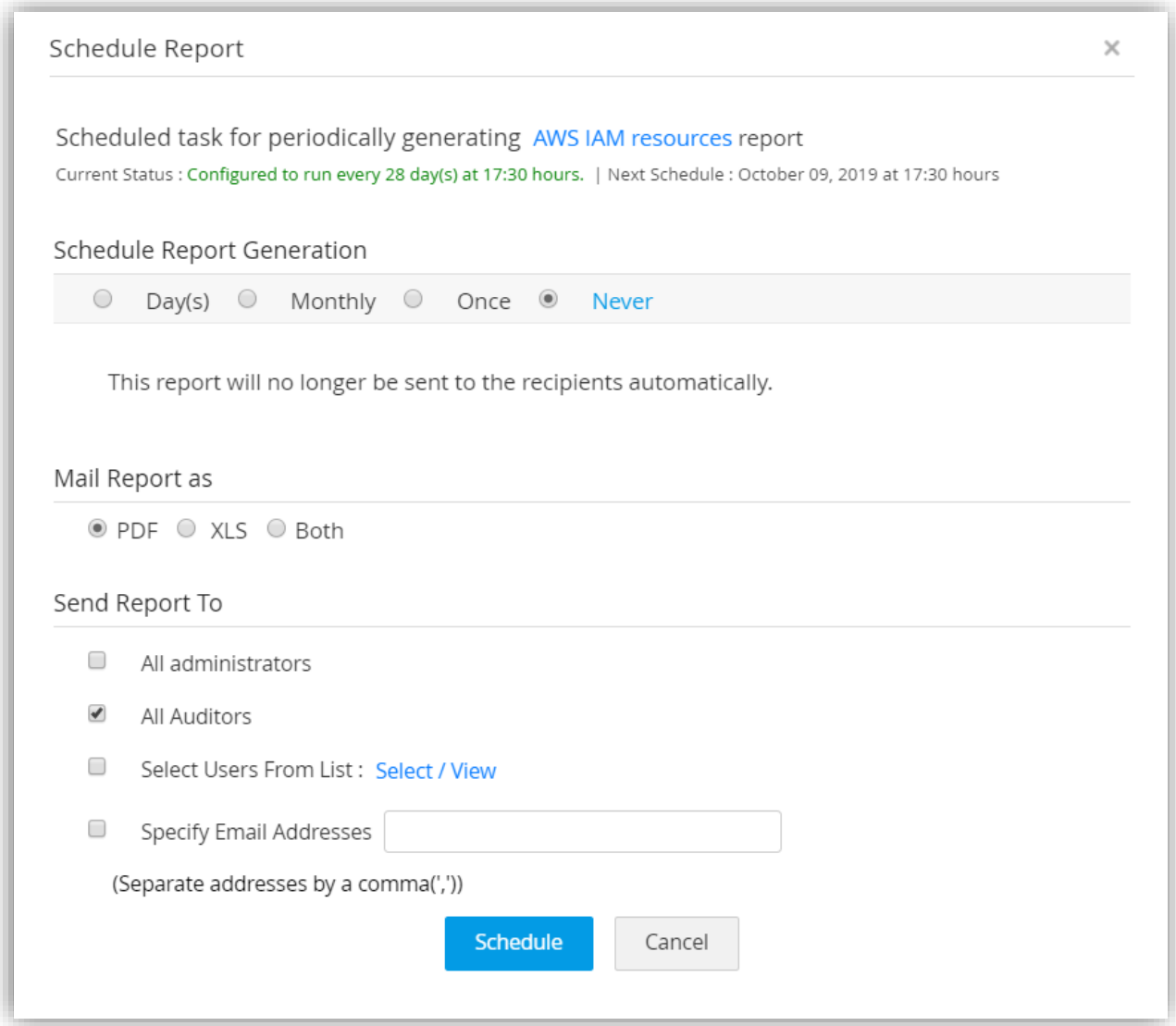
4. Next, choose the format in which the report has to be mailed to the recipients, PDF or XLS or both.
5. Select the recipients to whom the report should be mailed to, from the given options. You can also provide a custom list of email ids instead.
6. Click **Schedule.**



4. Terminating an Already Created Schedule

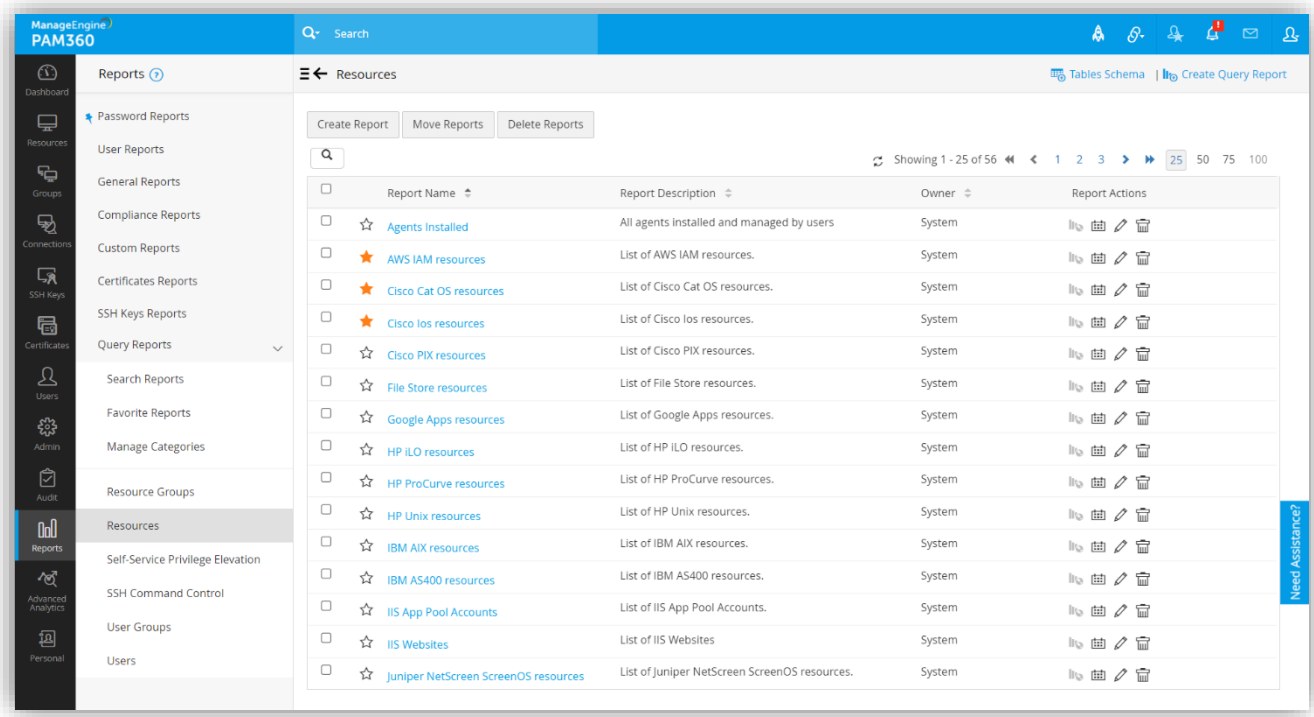
1. Click on the **Schedule Report** icon under **Report Actions** column beside the report.
2. In the pop-up form that opens, select the option **Never**.

3. Click **Schedule**. The schedule will be terminated.



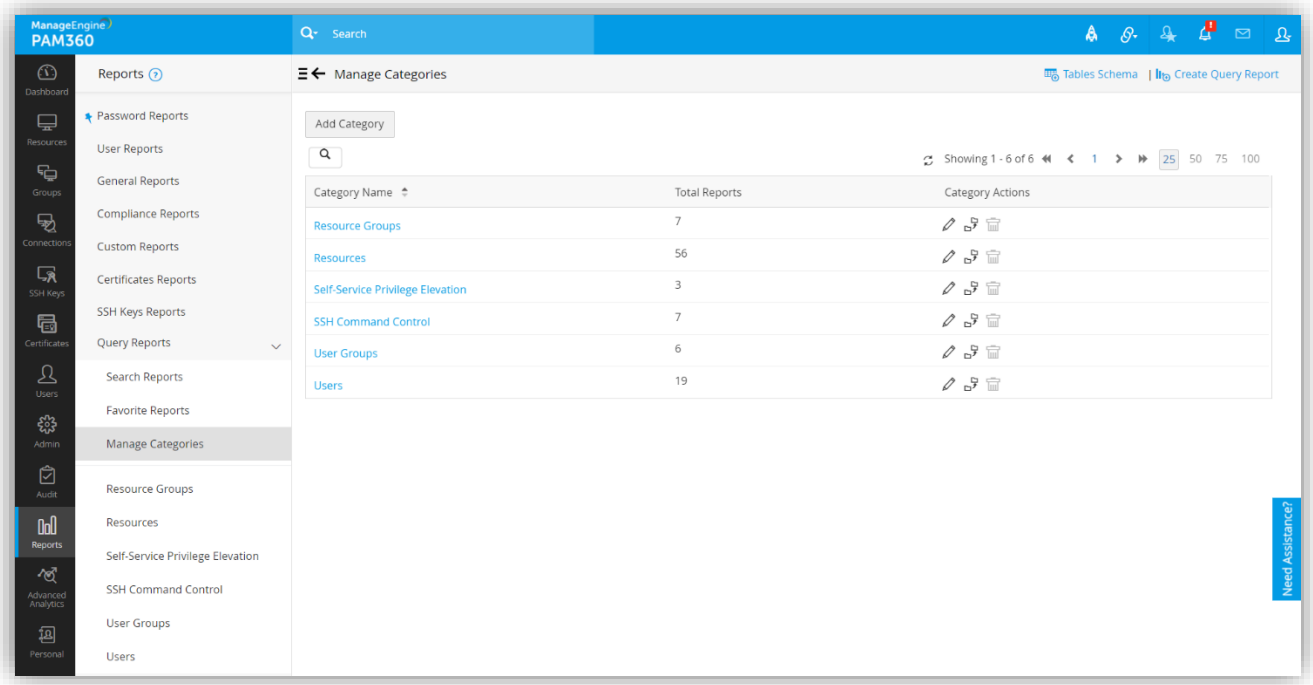
5. Creating Favorite Reports

To easily locate a frequently used or critical report, you can mark the report as favorite by clicking on Mark as Favorite star icon shown before the name of each report.



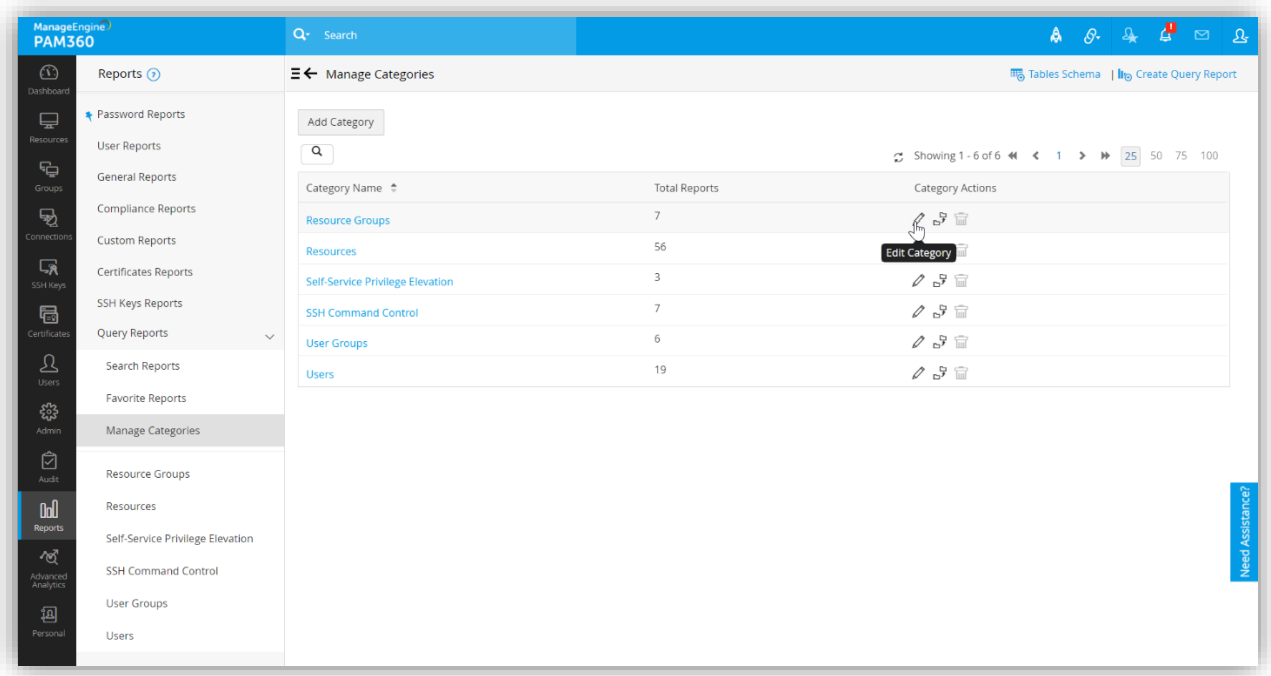
6. Managing Categories

To add/modify/delete categories, go to **Reports >> Query Reports >> Manage Categories**. (As shown in the left-hand side of the image below)

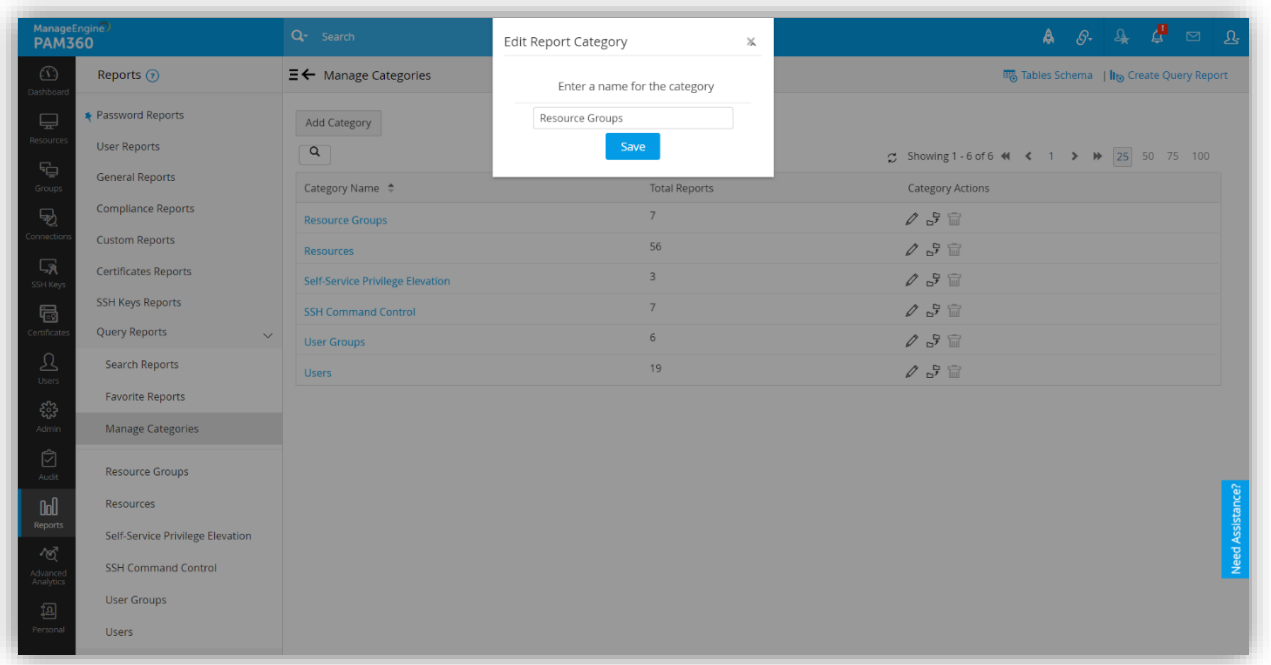


6.1 Editing a Category

1. Click the **Edit Category** icon present against the desired category, under **Category Actions** column.



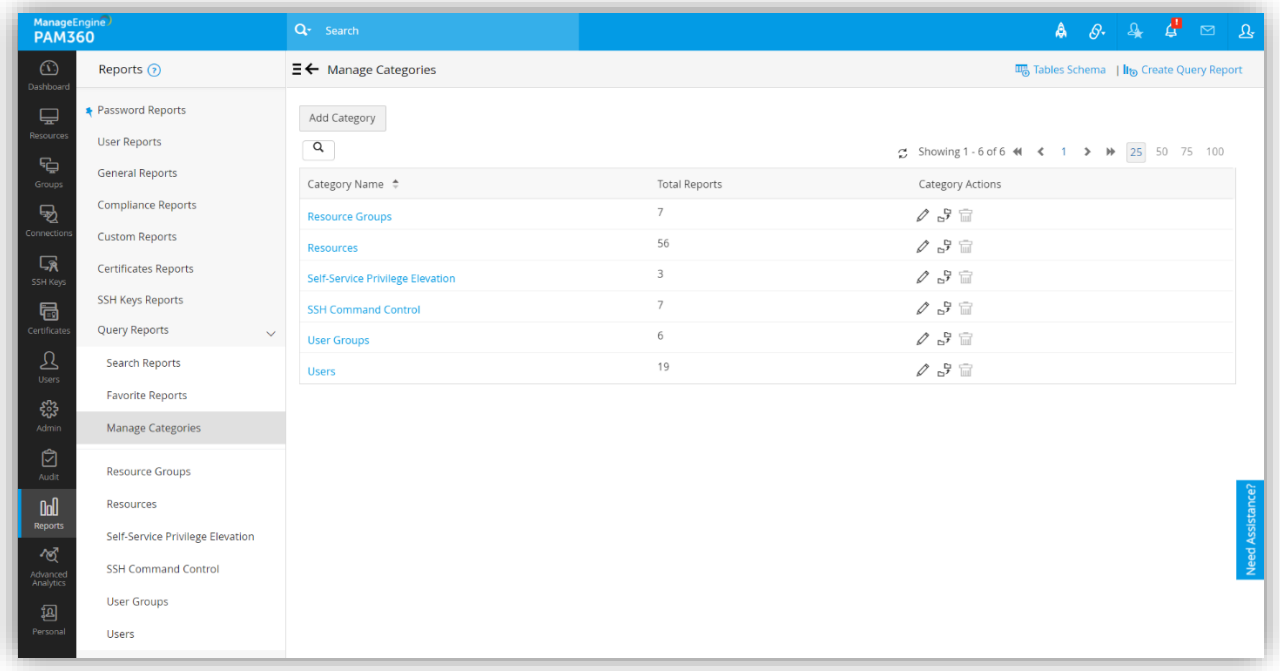
2. In the pop-up form that opens, you can change the **name for the category** and click **Save.**



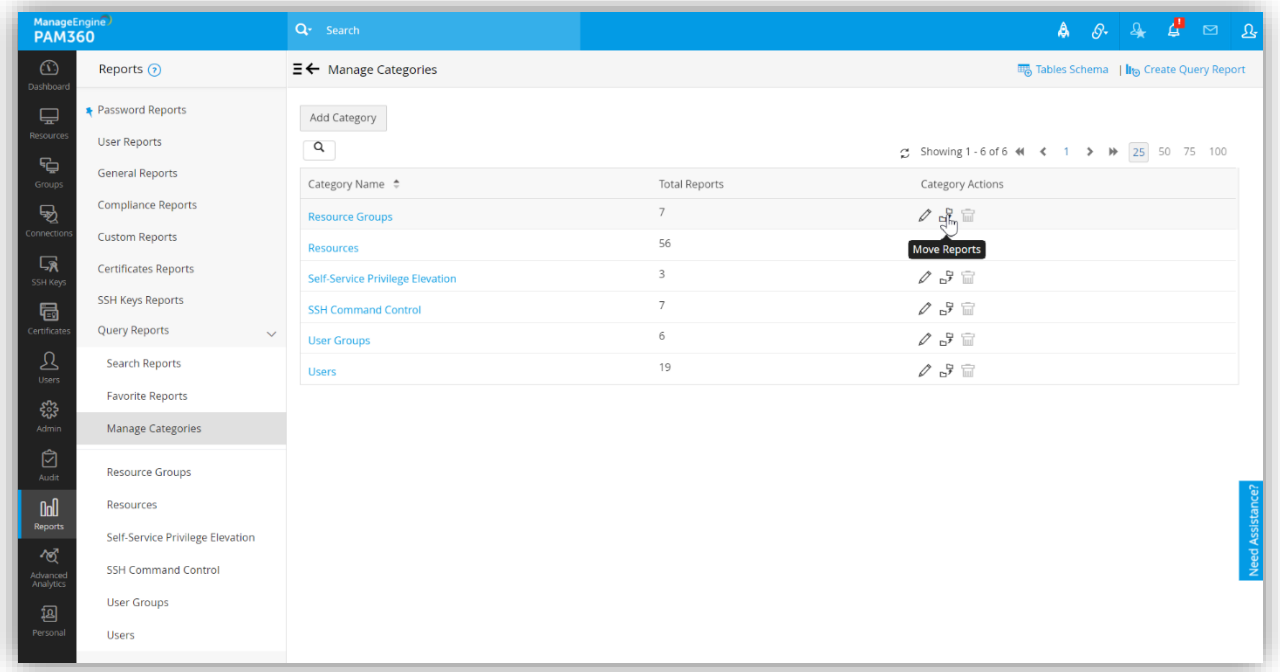
6.2 Deleting a Category

1. Click the **Delete Category** icon present against the desired category, under **Category**

Actions column.



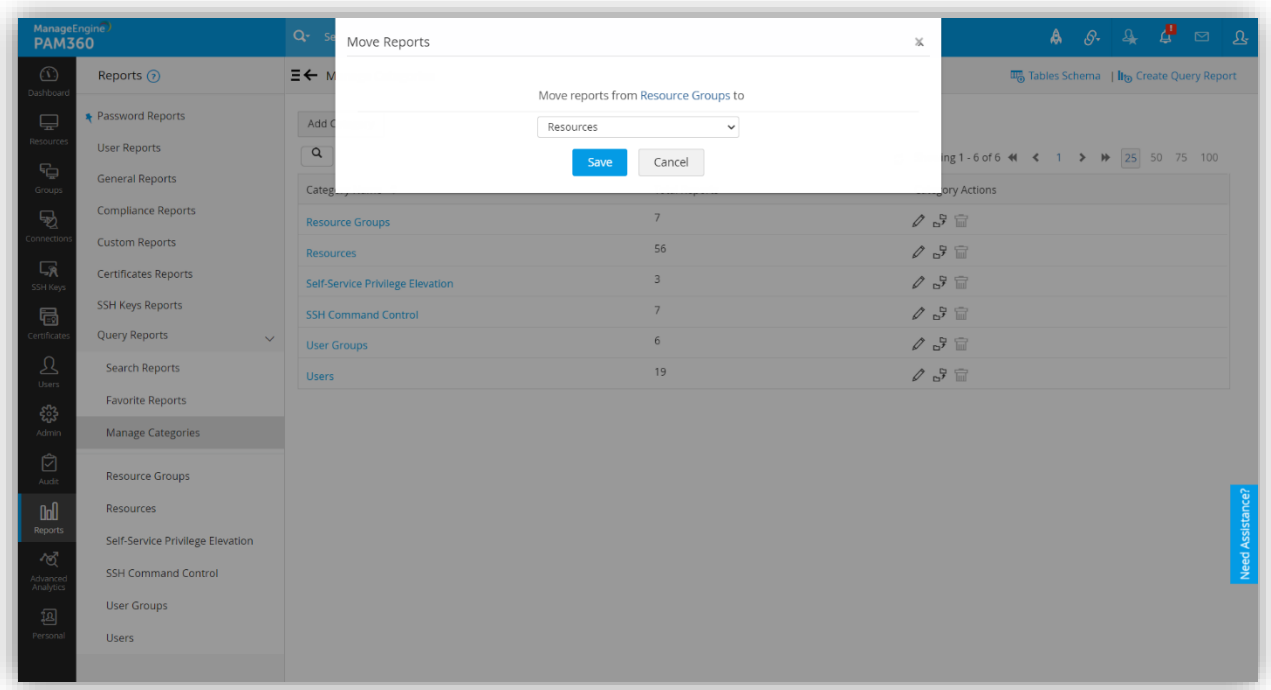
2. In the pop-up form that appears, Click **Ok.**



Note: In order to delete a category, you have to first ensure that no reports exist under it. If there are reports, you can move them to another category.

6.3 Moving Reports from One Category to Another

1. Click the **Move Reports** icon present against the desired category, under **Category Actions** column.
2. In the pop-up form that opens, choose the category to which the reports must be moved and click **Save**.



Audit and Notifications

As PAM360 deals with sensitive passwords, it is important to have a complete record of who accessed what resource and when along with trails about every single action performed by the users within the application. All operations performed by the users are audited with the timestamp and the IP address from where they accessed the application.

Audit in PAM360 has been classified into three types:

1. **Resource Audit** - all operations pertaining to resources, resource groups, accounts, passwords, shares and policies performed in PAM360.
2. **User Audit** - all operations performed by users in PAM360.
3. **Task Audit** - records of various scheduled tasks created in PAM360.

PAM360 audit is quite comprehensive and almost all actions are audited. In case your requirement is to audit only specific operations, PAM360 provides flexible options for focused auditing as well. There is also option to send notifications to required recipients whenever a desired event (audit trail of your choice) occurs in PAM360.

1. Resource Audit

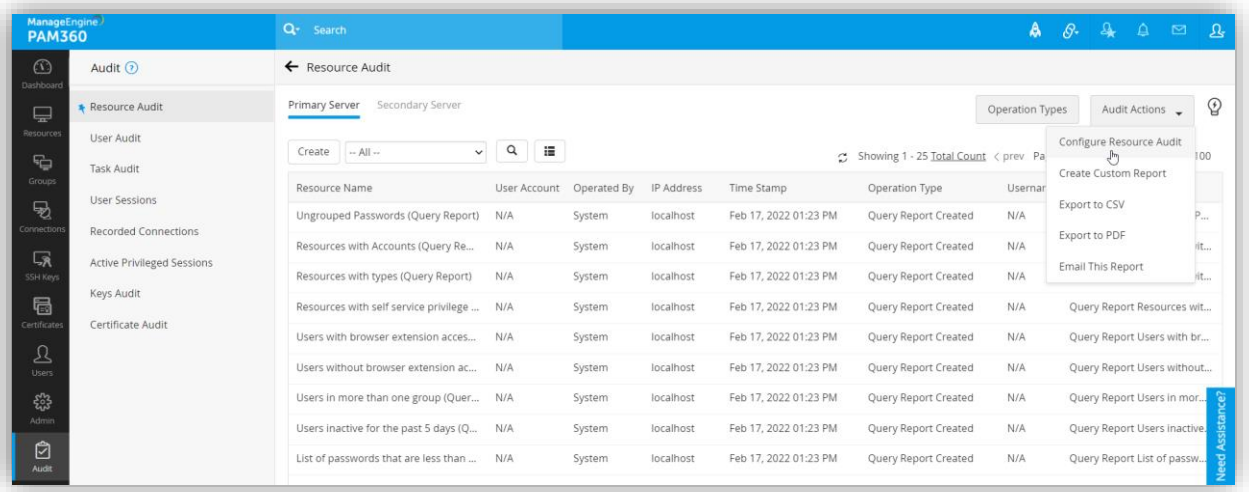
All operations pertaining to 'resources' performed in PAM360 are captured under 'Resource Audit'.

To view Resource Audit:

Navigate to **Audit >> Resource Audit.**

To record only specific operations in Resource Audit:

1. Navigate to **Audit >> Resource Audit**.
2. Click the **'Configure Audit'** icon under the **Audit Actions** drop-down.
3. In the **Resource Audit Configuration** UI that opens, select the operations for which you want audit records to be generated. Leave the checkbox against all other operations blank.



To receive notifications, traps, syslog messages on generation of audit records:

PAM360 provides the flexibility of sending separate notifications as and when the chosen event occurs.

1. If you want to receive instant email notifications, SNMP traps or syslog messages on the occurrence of a desired event, you can select the respective check-boxes against the required audit operation.
2. If you do not want your inbox to be flooded with notification emails, you can customize to receive a single notification every day (containing information about all the events generated on the day) in the form of a daily digest and you can also specify the list of recipients for notifications.
3. Click **Save.**

To purge resource audit trials:

Almost all operations pertaining to resources performed in PAM360 are audited and the audit data is stored in the database. Therefore, the resource audit record grows at a faster rate. To help you maintain disk space, an additional option to purge audit records is given in the same **Resource Audit Configuration** UI. If you do not need audit records that are older than a specified number of days, you can choose to purge them.

To configure resource audit purging,

1. Go to **Resource Audit >> Audit Actions >> Configure >> Purge Resource Audit Records.**
2. Then, specify the number of days upto which the audit records should be retained in PAM360. For instance, if you enter 90, audit records that are more than 90 days old will be automatically purged by PAM360.
3. Click **Save**.

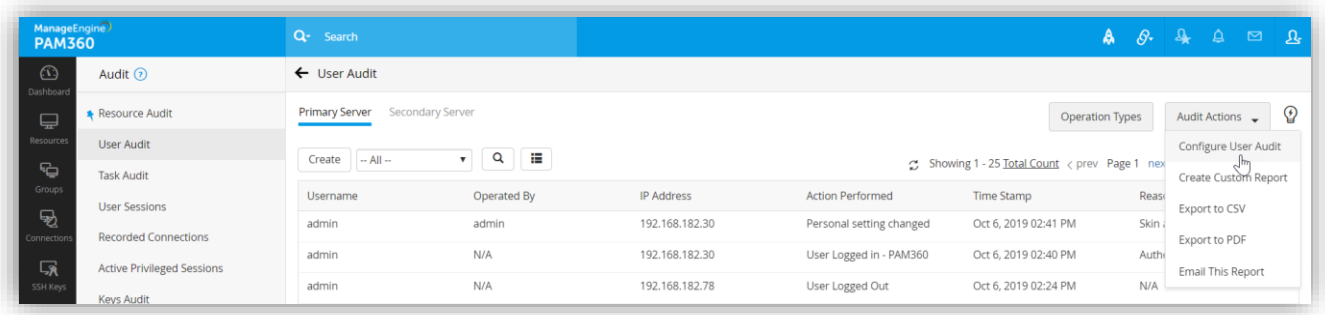
(Applicable from build 5400 onwards)

Note: You can choose to retain or delete specific audit records based on the operation type under **Purge Audit**. Use the check boxes to select the type of audit records that you wish to purge. The audit types that are left unselected will be retained permanently as a part of your audit trail.

To export resource audit trails as PDF/CSV report:

The Audit Trails could be exported as a **PDF/CSV** file and stored in a secure location for reference purposes.

To export Audit Trials as a report, click the button **Export to PDF** or **Export to CSV** as required, under **Resource Audit >> Audit Actions**.



Resource Audit Filters

You can create customized views of audit trails by adding filters and choosing to display only those audit records that are of interest to you.

To create an audit filter,

- Click the button **Create**.
- Select the required column names from the drop-down and enter your criteria (If you want to enter operation type as criteria, click the link **'View Operation Types'**, refer to the list and enter the required name as it is).
- Click **Save**.

2. User Audit

All operations performed in PAM360 by an PAM360 user are captured under User Audit.

To view User Audit:

Navigate to **Audit >> User Audit**.

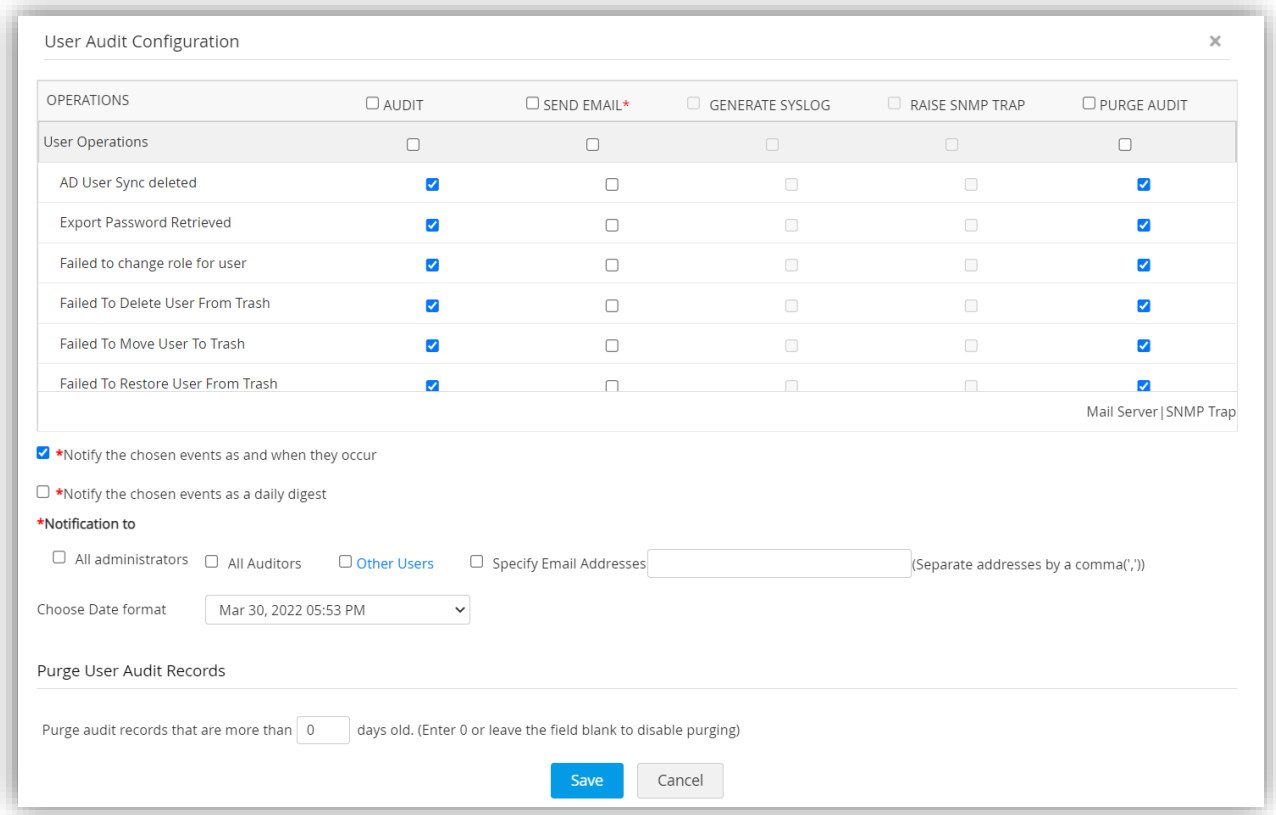
To record only specific operations in user audit

1. Click the **Configure Audit** icon from **Audit** actions in the **User Audit** page.
2. In the dialog box that opens, select the specific operation for which you want audit record to be generated. Leave the checkbox against all other operations blank.

To receive notifications on generation of audit records:

PAM360 provides the flexibility of sending separate notifications to each and every occurrence of the chosen event.

1. If you want to receive notifications, SNMP traps or syslog messages on the occurrence of a particular event, you can select the respective check-boxes against the required operation.
2. If you do not wish your inbox to be flooded with notification emails, you can choose to receive a single notification every day about all the events generated on the day and you can also specify the list of recipients for notifications.
3. Click **Save.**



To purge user audit trials:

Almost all operations pertaining to resources performed in PAM360 are audited and the audit data is stored in the database. Therefore, the resource audit record grows at a faster rate. To help you maintain disk space, an additional option to purge audit records is given in the same **Resource Audit Configuration** UI. If you do not need audit records that are older than a specified number of days, you can choose to purge them.

To configure resource audit purging,

1. Go to **User Audit >> Audit Actions >> Configure >> Purge User Audit Records**.
2. Then, specify the number of days upto which the audit records should be retained in PAM360. For instance, if you enter 90, audit records that are more than 90 days old will be automatically purged by PAM360.
3. Click **Save**.

(Applicable from build 5400 onwards)

Note: You can choose to retain or delete specific audit records based on the operation type under **Purge Audit**. Use the check boxes to select the type of audit records that you wish to purge. The audit types that are left unselected will be retained permanently as a part of your audit trail.

To export user audit trails as PDF/CSV report:

The Audit Trails could be exported as a **PDF/CSV** file and stored in a secure location for reference purposes. To export Audit Trials as a report, click the button **Export to PDF** or **Export to CSV** as required, under **User Audit >> Audit Actions**.

User Audit Filters:

You can create customized views for filtering and viewing only those audit records by specifying your criteria.

To create an audit filter,

- Click the link **Add** present beside **'Manage Custom Filters'**.
- Select the required column names from the drop-down and enter your criteria (If you want to enter operation type as criteria, click the link **'View Operation Types'**, refer to the list and enter the required name as it is).
- Click **Save.**

3. Task Audit

Records of various scheduled tasks created and executed in PAM360 under 'Task Audit'.

To view Task Audit

Navigate to **Audit >> Task Audit.**

To record only specific operations in task audit:

1. Click the **'Configure Audit'** icon from the Audit actions in the Task Audit page.
2. A UI will open. Select the specific operation for which you want audit record to be generated. Leave the checkbox against all the other operations blank.

To receive notifications, traps, syslog messages on generation of audit records:

PAM360 provides the flexibility of sending separate notifications as and when the chosen event occurs.

1. If you want to receive notifications, SNMP traps or syslog messages on the occurrence of a specific event, you can select the respective check-boxes against the required operation.
2. If you do not want your inbox to be flooded with notification emails, you can customize to receive a single notification every day in the form of a daily digest and you can also specify the list of recipients for notifications.
3. Click **Save.**

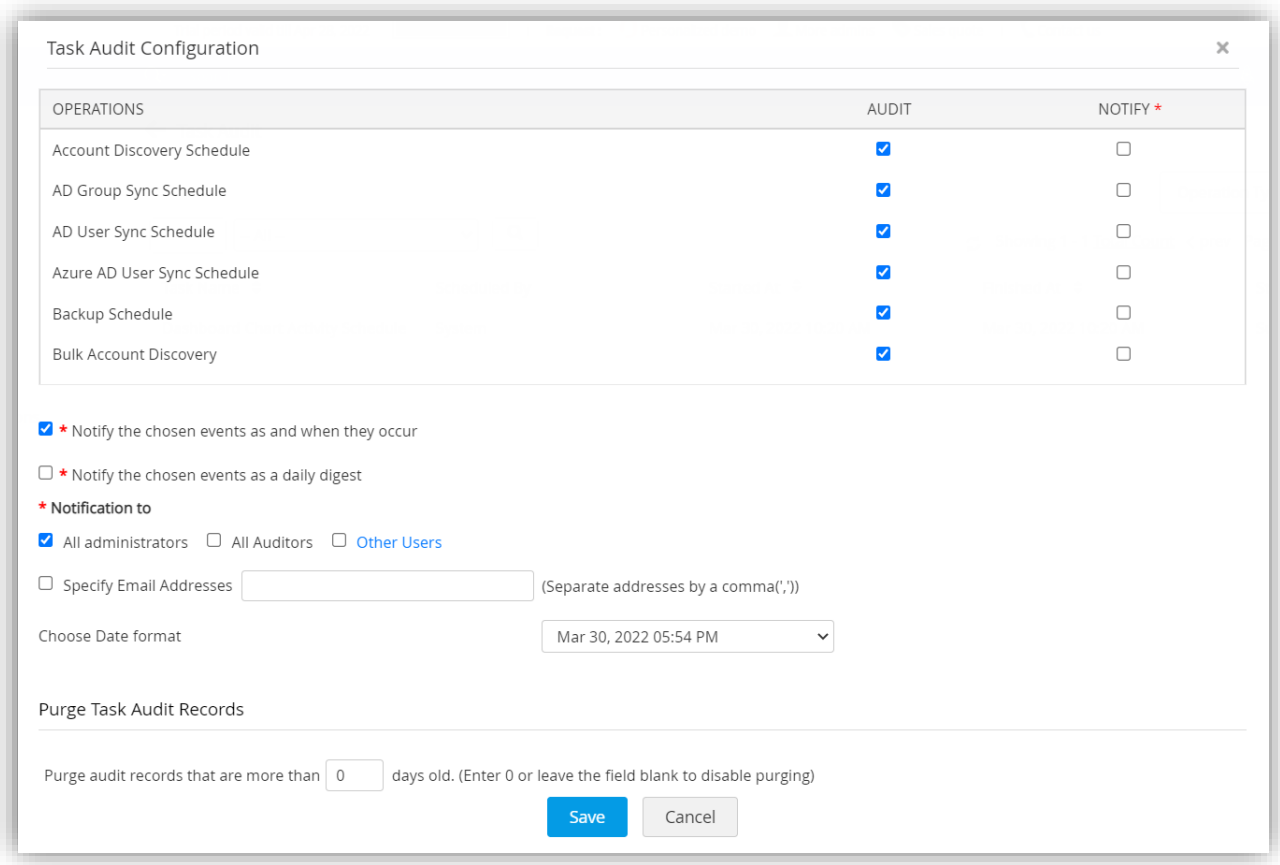
To purge task audit trials:

Almost all operations pertaining to resources performed in PAM360 are audited and the audit data is stored in the database. Therefore, the resource audit record grows at a faster rate. To help you maintain disk space, an additional option to purge audit records is given in the same **Resource Audit Configuration** UI. If you do not need audit records that are older than a specified number of days, you can choose to purge them.

1. Go to **Task Audit >> Audit Actions >> Configure >> Purge User Audit Records**.
2. Then, specify the number of days upto which the audit records should be retained in PAM360. For instance, if you enter 90, audit records that are more than 90 days old will be automatically purged by PAM360.
3. Click **Save.**

(Applicable from build 5400 onwards)

Note: You can choose to retain or delete specific audit records based on the operation type under **Purge Audit**. Use the check boxes to select the type of audit records that you wish to purge. The audit types that are left unselected will be retained permanently as a part of your audit trail.



To export task audit trails as PDF/CSV report:

The Audit Trails could be exported as a **PDF/CSV** file and stored in a secure location for reference purposes. To export Audit Trials as a report, click the button Export to PDF or **Export to CSV** as required, under **Task Audit >> Audit Actions**.

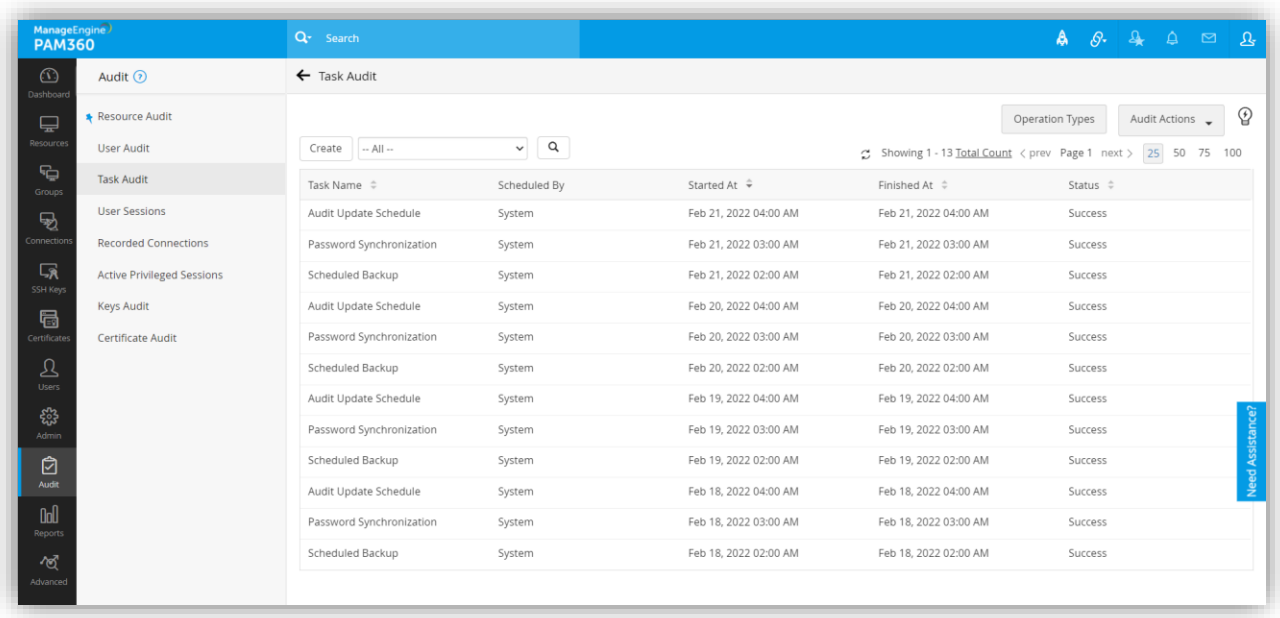
3.1 Task Audit Filters

You can create customized views for filtering and viewing only those audit records that are of interest to you by specifying your criteria.

To create an audit filter:

1. Click the link **Add** present beside **'Manage Custom Filters'**.

2. Select the required column names from the drop-down and enter your criteria (If you want to enter operation type as criteria, click the link **'View Operation Types'**, refer to the list and enter the required name as it is).
3. Click **Save.**



1. Does PAM360 record attempts by users to view and retrieve passwords?

Yes, PAM360 helps in establishing strong accountability for all operations carried out within the application. Therefore, all the operations performed by the users including the password viewing, retrieval and copying actions are audited by PAM360. The list of operations that are audited with timestamp and IP address includes:

i. User accounts created, deleted and modified.

ii. Users logging in and off the application.

iii. Resources and passwords created, accessed, modified and deleted.

2. How are the audit logs protected against modification?

All the audit records are stored in the MySQL database. To ensure security, the MySQL server has been configured not to accept connections from remote hosts. In addition, the password to access the MySQL server is randomly generated for every PAM360 installation. So, unless people gain entry into the database, the audit records cannot be modified.

4. User Sessions

The audits of all the operations a user performed during his active session will be listed. And

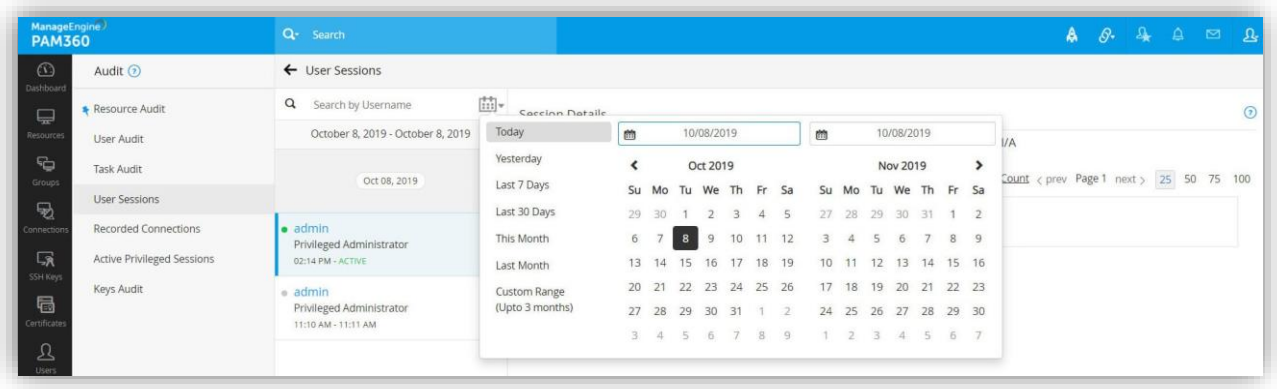
these audits can be viewed by selecting a particular user session of a specific date range. There is also an option to terminate any active user session by the administrators.

> **Note**: All the user session audits are tracked only from version 9500. So, any audits prior to v9500 will not be listed.

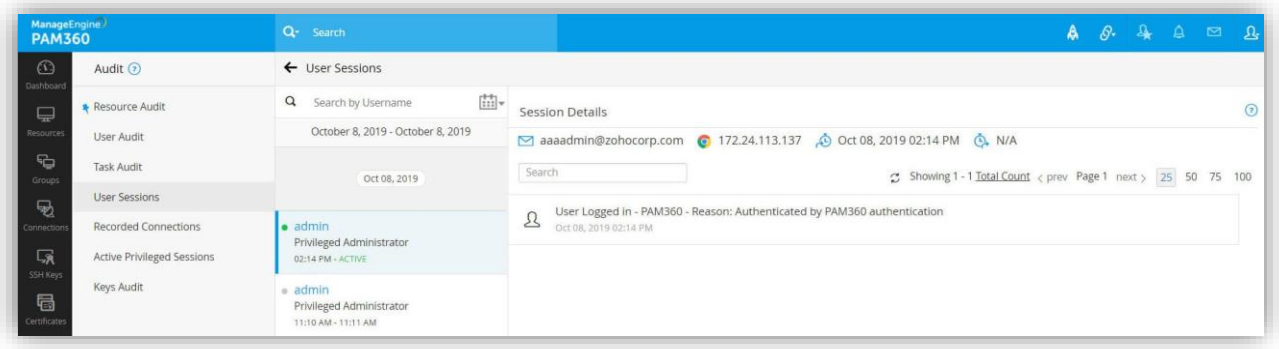
All audits pertaining to 'User Sessions' within the chosen date range are captured under 'Audit » User Sessions'.

To view User Sessions:

1. Navigate to **Audit » User Sessions**.
2. Choose a particular date by double clicking on the specific date for which you want to view the user sessions or a range of dates by selecting a start date and end date from the '**date range picker**'. The range between the start date and end date cannot be more than 3 months.



3. By default, the current date will be chosen as both start and end dates.
4. After choosing the date range, all the user sessions performed on the chosen date range will be listed.
5. Upon clicking a particular user session, the audits of all the operations the user performed during the chosen session will be listed.



To search a particular 'User Session' or 'Audits':

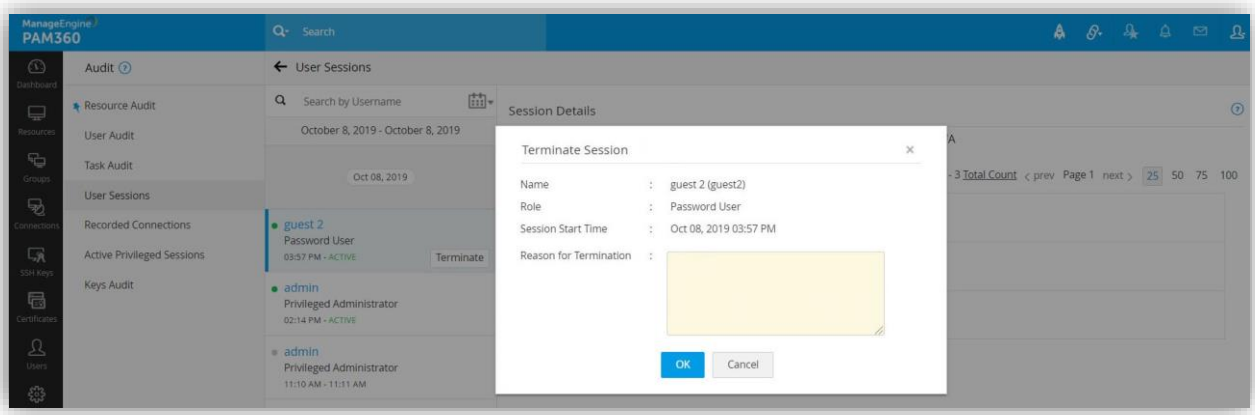
1. Navigate to **Audit >> User Sessions**.
2. Search a particular user session by entering the username - first name, last name or full name in the search field.
3. You can also search a particular audit by entering the keywords in the search field.

To terminate 'User Sessions',

1. Navigate to **Audit >> User Sessions.**
2. You can terminate any active user session by clicking the '**Terminate**' button present beside the '**User Session**' and providing a reason.
3. Click '**OK**'. The session will be terminated.

Notes:

1. Only Administrators / Password Administrators / Privileged Administrators will be able to terminate any user session.
2. The Org Manager's session can be terminated by the administrators of their MSP org only.


ManageEngine
PAM360
Search
Audit
Resource Audit
User Audit
Task Audit
User Sessions
Recorded Connections
Active Privileged Sessions
Keys Audit
User Sessions
Search by Username
October 8, 2019 - October 8, 2019
Oct 08, 2019
guest 2
Password User
03:57 PM - ACTIVE
Terminate
admin
Privileged Administrator
02:14 PM - ACTIVE
admin
Privileged Administrator
11:10 AM - 11:11 AM
Session Details
Terminate Session
Name : guest 2 (guest2)
Role : Password User
Session Start Time : Oct 08, 2019 03:57 PM
Reason for Termination :
OK
Cancel
Total Count
prev
Page 1
next
25
50
75
100

PAM360 Mobile Application - Android

PAM360's Android mobile application makes the product's robust and efficient features more accessible by helping you manage and control your enterprise's privileged accounts and passwords through your mobile device. The Android application encrypts and stores all your data using AES-256 encryption; therefore, accessing your enterprise accounts through your Android device is as secure as accessing PAM360's desktop installation.

Furthermore, all communication between your PAM360 server and the Android application happens over an encrypted channel, secured using the HTTPS protocol over SSL.

> **Note:** The PAM360 Android application requires a valid working instance of the ManageEngine PAM360 web application.

At the end of this topic, you will have learned the following:

1. Significant Features
2. How does Secure Authentication Work in the PAM360 Mobile Application?
3. Getting Started with the Application
    - 3.1 Application Overview
    - 3.2 Installation and Authentication
4. PAM360 Android Application - Navigation Menu
    - 4.1 Enterprise Filters
    - 4.2 Password Access Requests
    - 4.3 Advanced Search
    - 4.4 Resource Groups
    - 4.5 SSH Keys
    - 4.6 Certificates
    - 4.7 Personal
    - 4.8 Settings
5. Setting Up Secure Offline Mode
6. Uninstalling the Mobile Application

1. Significant Features

PAM360's Android application comes with a comprehensive set of features that can help you seamlessly take control of your privileged accounts, even when you are away from the desktop installation.

- View and manage all passwords that are owned or managed by you.
- Approve/reject password requests and monitor who checks out passwords directly from the PAM360 Android application. Also, send password requests, and perform password check in and check out through the mobile application.
- Incorporate ticket ID validation through PAM360's ticketing system integration to secure your access approval workflow even further.
- View and manage your SSH keys and SSL certificate details at any time.
- Store and manage your critical personal information such as credit card numbers for on-the-go access. PAM360's Android application encrypts your personal data using the advanced AES-256 encryption algorithm.
- Save important passwords offline to access them even when you do not have access to the Internet.

2. How does Secure Authentication work in the PAM360 Mobile Application?

The application offers Two-Factor Authentication for enhanced security. Once enabled, users have to authenticate themselves through two successive stages to access the mobile interface. There are three ways of doing the first level of authentication: PAM360's native authentication using Active Directory/LDAP/Azure AD credentials, or via SAML SSO. The second level of authentication can be done through any of the Two-Factor Authentication provisions supported by PAM360. After the Two-Factor Authentication is complete, PAM360 prompts you to set up a passphrase for your account, with a minimum of 8 characters, used for mobile authentication. All your offline data is encrypted using the advanced AES-256 encryption algorithm. Please note that the application does not store your passphrase, and it is mandatory to enter the passphrase during login.

Administrators can selectively allow or restrict mobile application access to users. Navigate to **Admin >> Users >> More Actions** and click the **Restrict Mobile Access** option. The users with the restriction cannot log in to their PAM360 accounts through the Android application.

Similarly, administrators can allow users to cache passwords in their mobile devices. Go to **Admin >> General Settings >> User Management** and select **Allow password caching for offline access via mobile**. Leave this option unchecked to restrict users from accessing passwords offline.

3. Getting Started with the Application

3.1 Application Overview

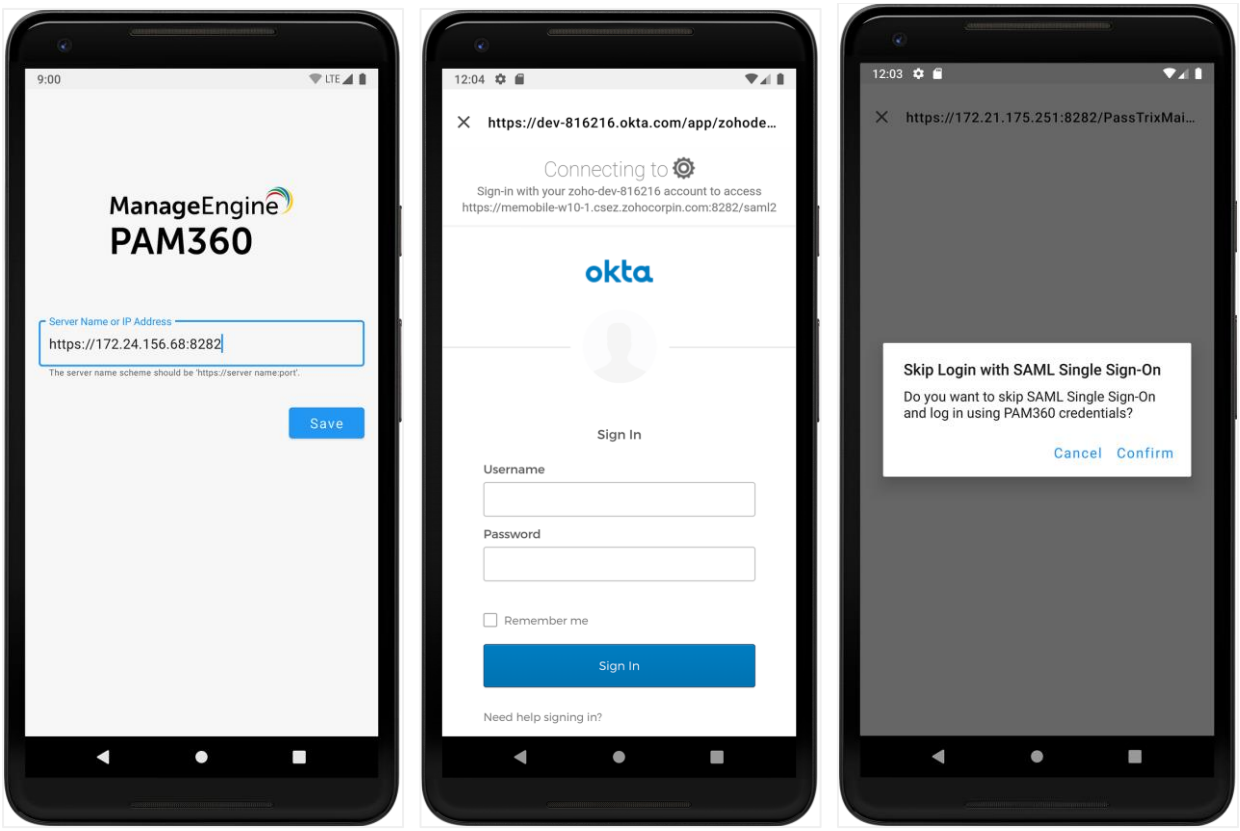
Supported Devices	All Android devices
Compatibility	Requires Android version 5.0 and above
Size	5.3 Mb (approx)
Languages Supported	English, French, German, Japanese, Polish, Simplified Chinese, Spanish, Traditional Chinese, Turkish, Portuguese, Italian, Russian, and Dutch. **Note**: Please select your desired language on the PAM360 desktop installation and the mobile device.

3.2 Installation and Authentication

Follow the below steps to download and install the PAM360 mobile application:

1. Go to the Play Store and search for ManageEngine PAM360 or click this direct link.
2. Click **Install** to install the application on your device.
3. After successful installation, enter the following details to get started with the mobile application:

    i. Enter the **Server Name** or **IP address** in which PAM360 is running, along with the **Port**. If your PAM360 server is installed in a physical network, ensure that the PAM360 server and the mobile application are connected to the same network. However, if your PAM360 server is hosted in the cloud, your mobile application will work from a different network as well.



ii. To login, enter the username & password of your PAM360 account. The Android application supports three ways of authentication; login through PAM360's native authentication, through Active Directory/LDAP/Azure AD authentication, and via SAML SSO. To login using Active Directory/LDAP credentials, select your domain name from the drop-down list. If SAML single sign on is enabled in your PAM360 server, a browser window opens within the application.

iii. Here, enter your SAML SSO credentials to login. To skip the SAML SSO login, close the browser window and you will be redirected to the application's login page.

iv. Set up a passphrase for your account.

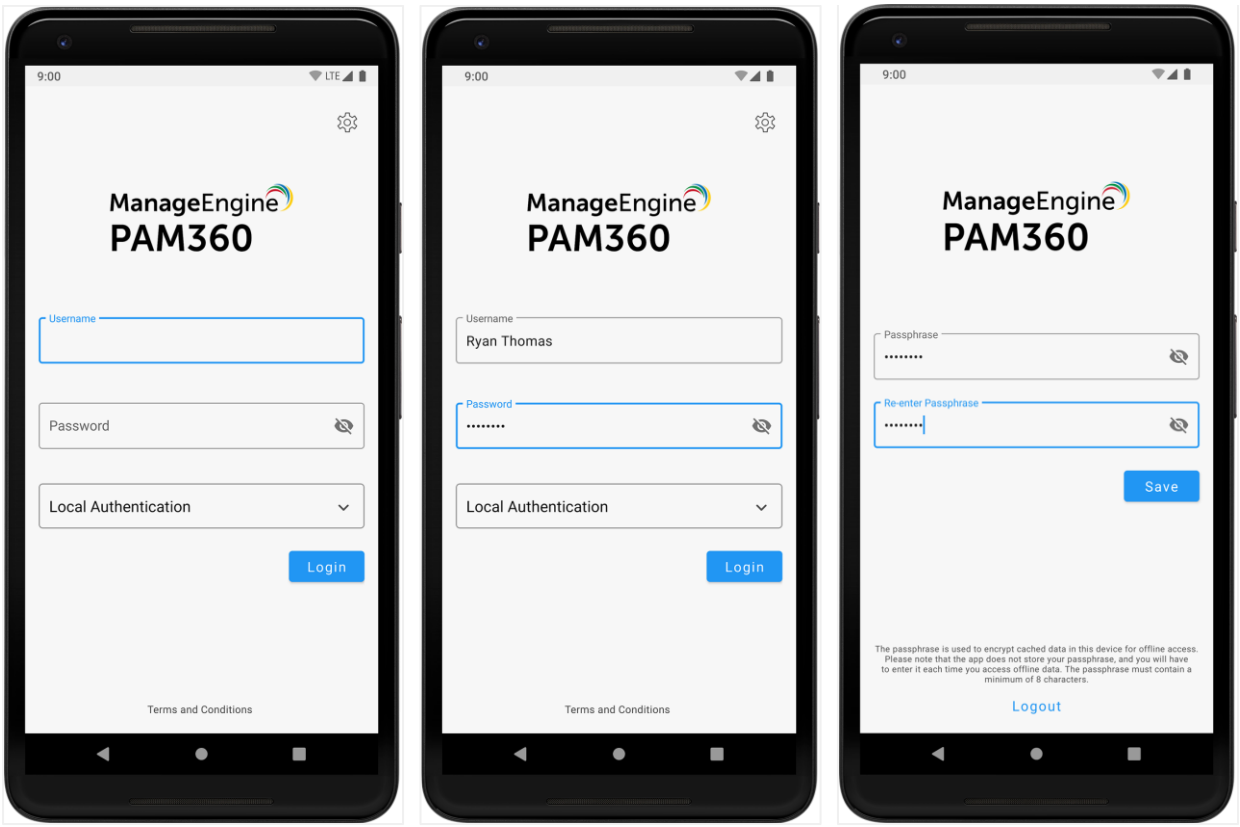
Notes:

i. Please note that the application does not store your passphrase, and it is mandatory to enter the passphrase during login, each time you access the mobile application. You have a total of five attempts to enter the correct passphrase, after which you will be logged out of the application automatically. If you have enabled **Swift Login** options, you can use the **Forgot Passphrase** option in this page to login using that instead.

ii. If you are using the application in online mode and fail to provide the correct passphrase during the allowed attempts, the application will log you out and you have to log in again and set up a new passphrase to access the mobile application again.

iii. In case you fail to enter the correct passphrase while using offline mode, you cannot access the application until you log in through the online mode and change the passphrase again.

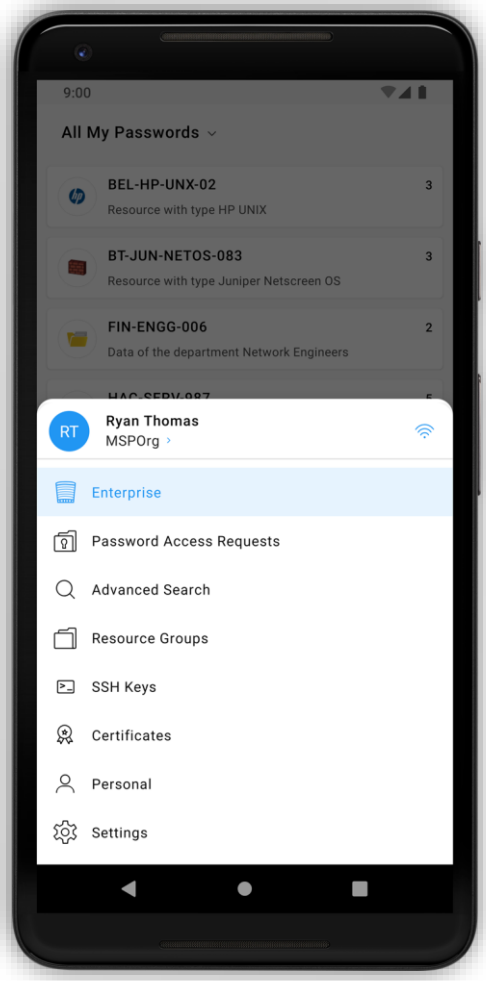
iv. Please note that every time you set up a new passphrase, all the offline password cache you have saved and settings you have customized will be deleted from your device.



4. PAM360 Android Application - Navigation Menu

Once you have signed into your PAM360 account through the Android application, you will see the Navigation Menu on the main screen with the following options that will help you navigate the Android application efficiently:

1. Enterprise Filters
2. Password Access Requests
3. Advanced Search
4. Resource Groups
5. SSH Keys
6. Certificates
7. CSR
8. Personal
9. Settings



i. Choosing Client Organization as an MSP User

If you are an MSP user, PAM360's Android application allows you to manage the administrative passwords of all your clients separately from a single management console. The application neatly segregates client organizations into different sections, which you can tap to view all the passwords belonging to that particular organization. As MSP admin, even though you can view the names of the organizations you manage, you will be able to view the data on all your customers only if you add their resources or if they share their resources with you. Your clients will be able to view the data belonging to their organization only.

As an MSP user, you can choose a client organization and view all the resources under it. To do so:

1. Tap the hamburger icon to open the **Navigation Menu**. Here, tap on the organization name to display all the available client organizations.
2. Tap the client organization name to display all the resources specific to the selected organization. Please note that the mobile interface will display only the resources specific to the selected organization.

4.1 Enterprise Filters

By default, the application displays a list of all the resources on the main screen. From here, tap on any resource to view the accounts associated with it. Tap the hamburger icon at the bottom left corner to open the Navigation Menu. In this menu, tap the **Enterprise** option to open the **All My Passwords** page. To view the **Enterprise Filters**, tap the downward arrow beside **All My Passwords**. The **Enterprise Filters** list displays a list of resources owned or managed by you, categorized as below:

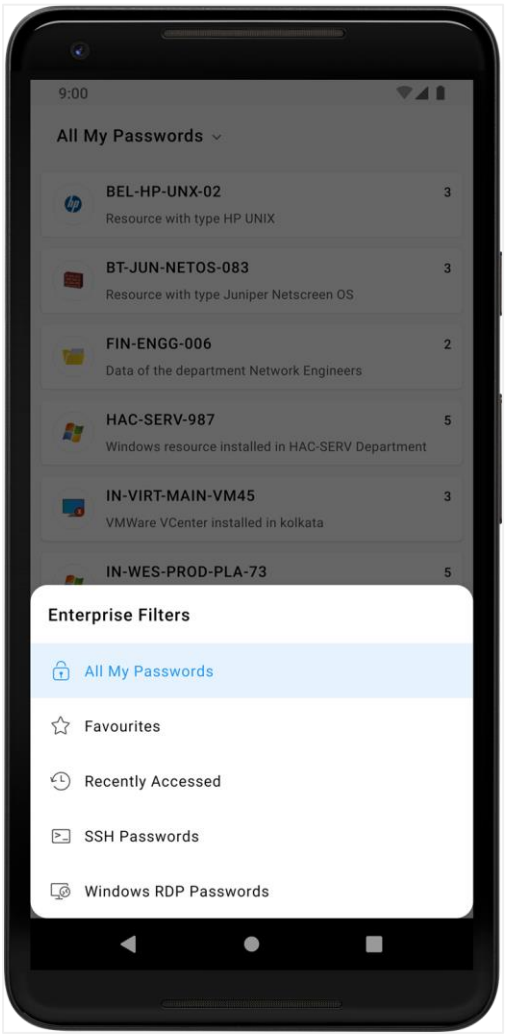
i. All My Passwords
ii. Favorites
iii. Recently Accessed
iv. SSH Passwords
v. Windows RDP Passwords

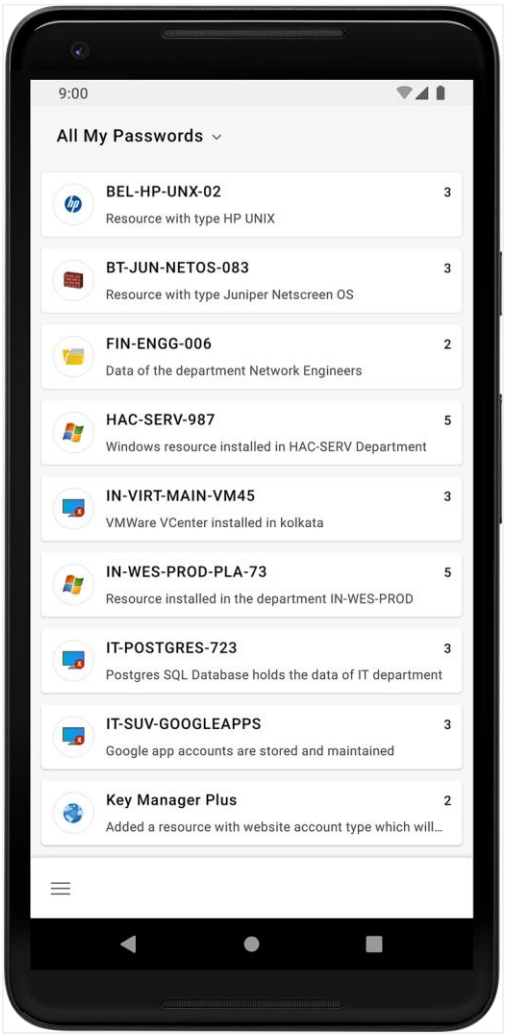
Each menu has a dedicated Search icon that allows you to locate accounts within the menu. The application loads the list of accounts as and when you scroll through the list. When you search for an account using a keyword, the application searches for the keyword only in the already loaded list; to search through all available accounts, scroll to the end of the list to load all accounts.

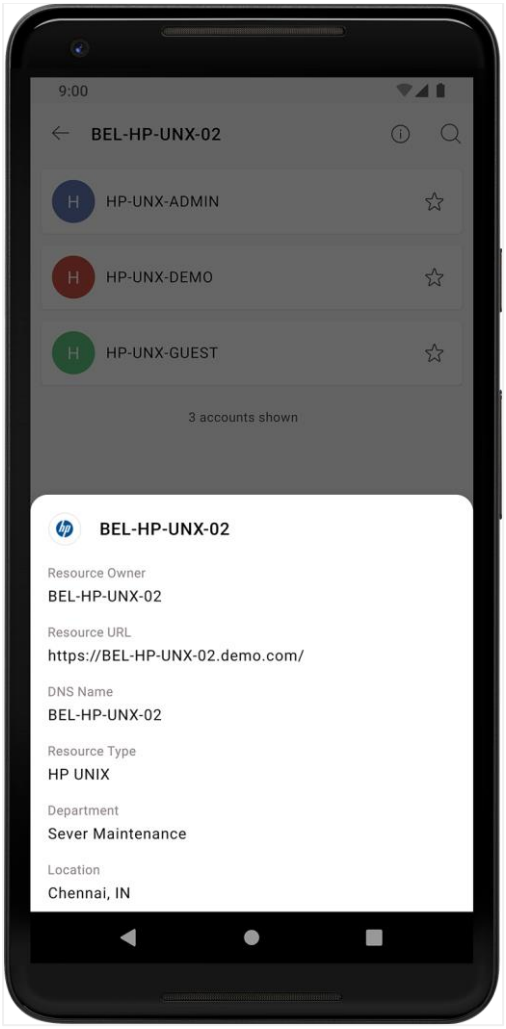
i. All My Passwords

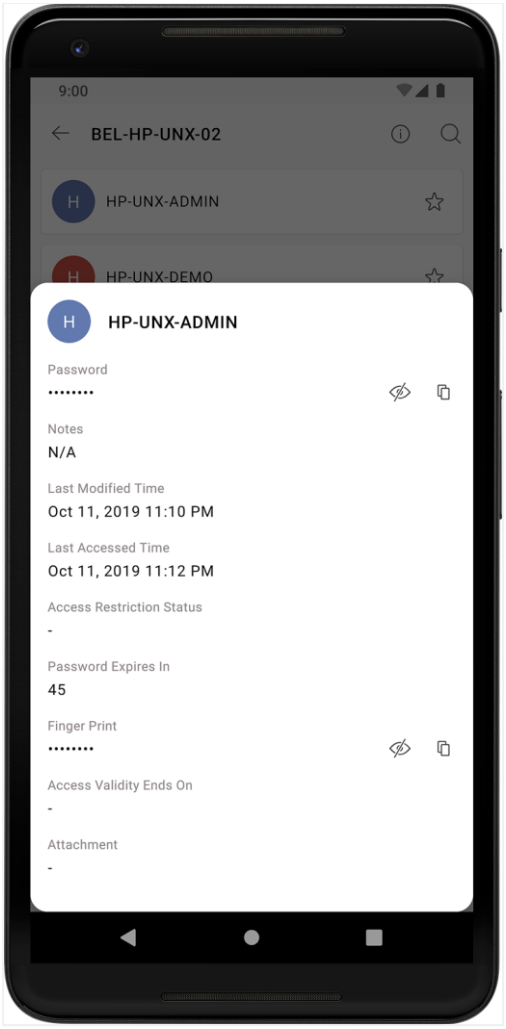
This category lists all resources and accounts that are owned and managed by you. Tap on any resource/account name to view the resource/account details such as resource owner, resource URL, DNS name, resource type, passwords, resource name, account notes, and last accessed time. To view the password of a particular account, tap on the eye icon beside the password. Tap the Search icon to search for any account within the selected resource, using

a search keyword.



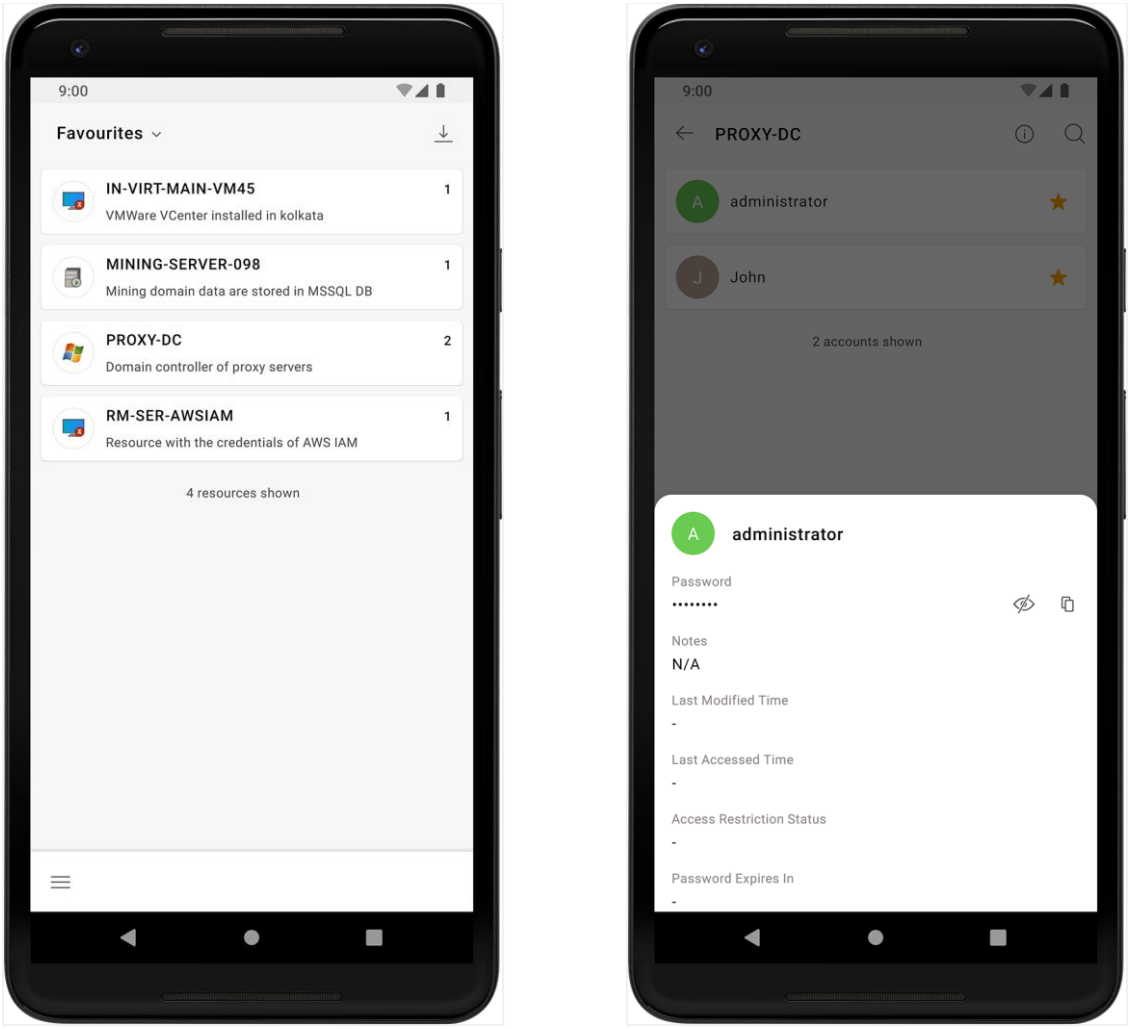






ii. Favorites

This option is to have quick access to the list of passwords that you marked as Favorites. To mark any password as your favorite, tap the star icon beside the required password in any category. Marking passwords as Favorites helps you locate a particular account and its password easily, without the need to scroll through the entire list every time. Tap the Search icon to search for any account within the selected resource, using a search keyword.

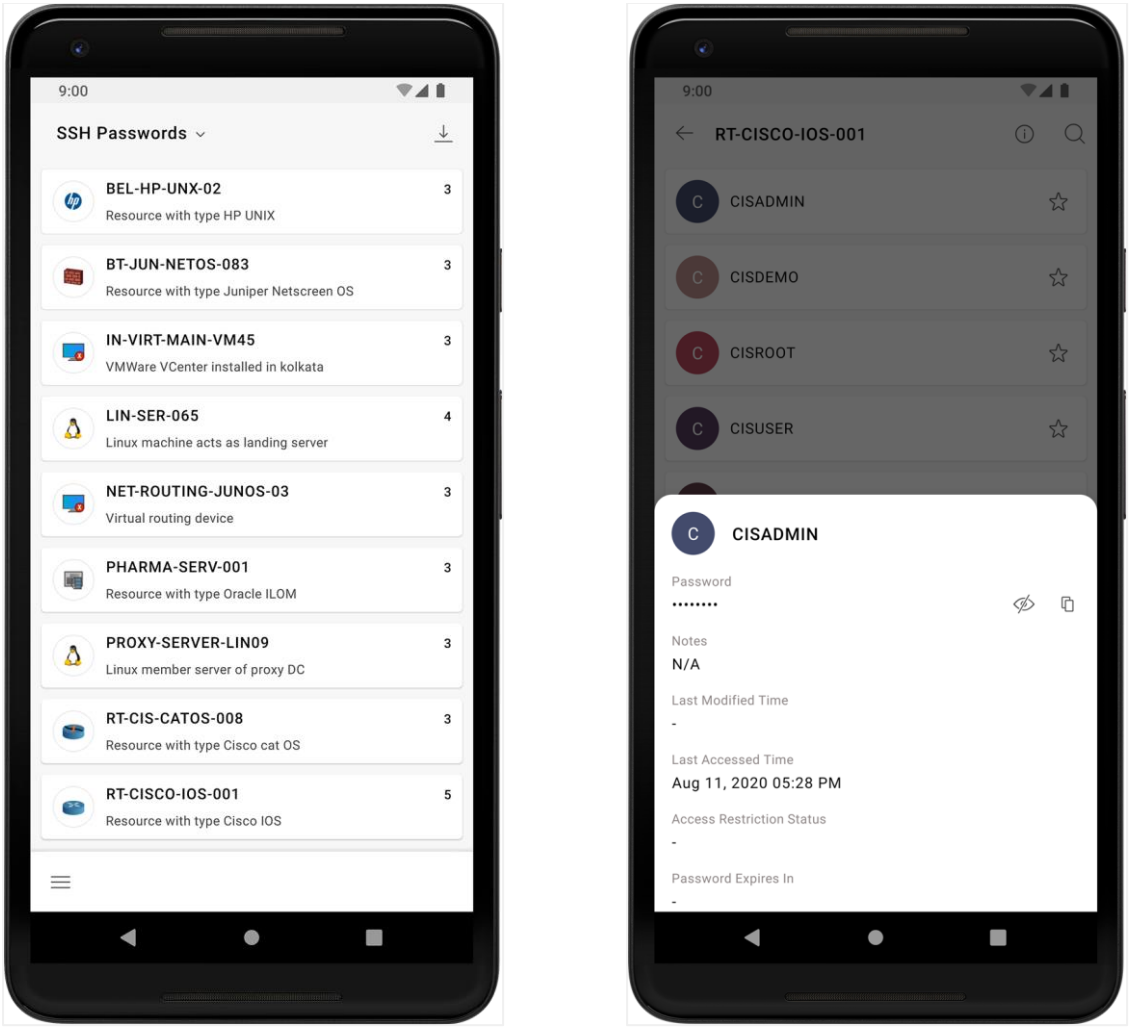


iii. Recently Accessed

This menu helps you view only the list of resources and passwords that you have recently viewed or used. From the list, you can tap on any resource to view its accounts and their corresponding details. Tap the Search icon to search for any account within the selected resource, using a search keyword.

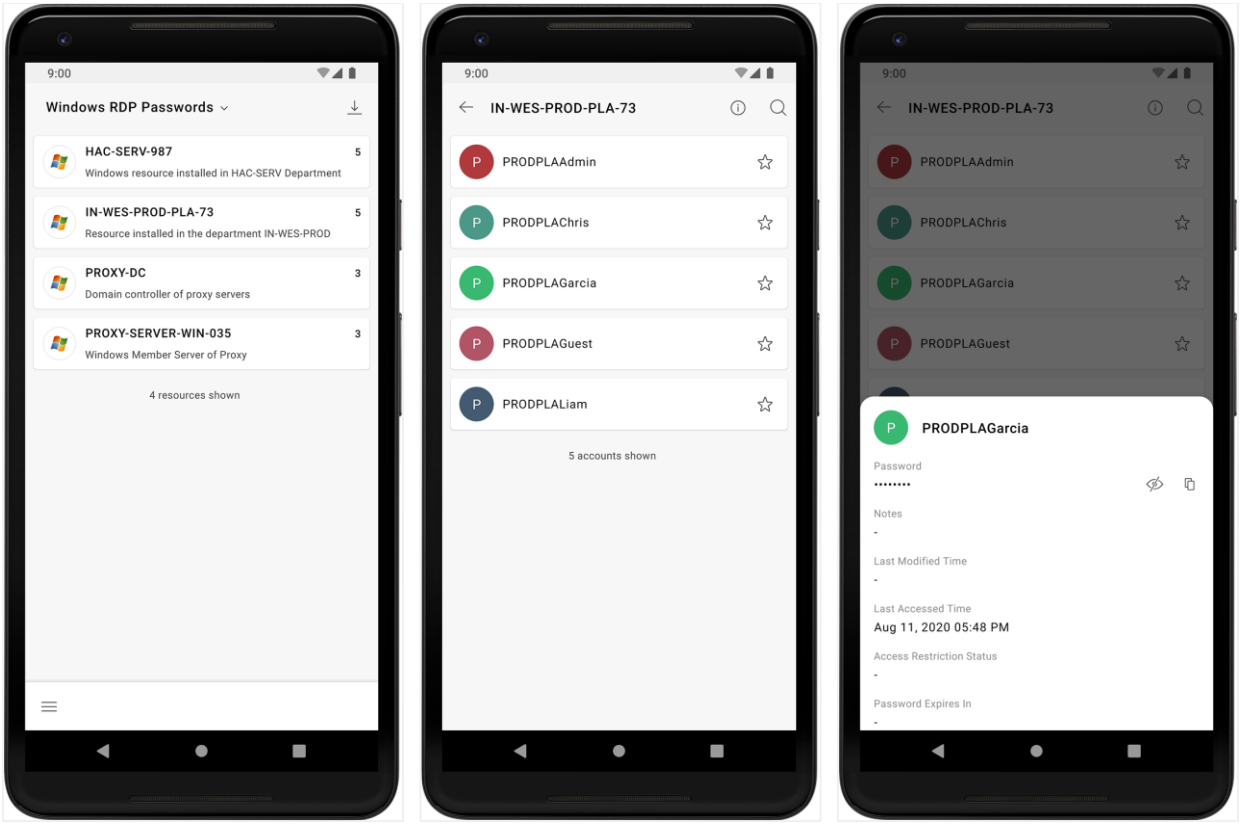
iv. SSH Passwords

This option gives you a consolidated view of all the resources that you can access through an SSH connection. Tap on any resource on this list to view its user accounts. Tap on any account to view the account details, such as the masked password, last modified time, last accessed time, and password expiry date. Tap the Search icon to search for any account within the selected resource, using a search keyword.



v. Windows RDP Passwords

If your network contains a list of resources of various OS types, the Windows RDP Passwords option will help you to view only the list of Windows resources and their corresponding accounts. Tap on any resource/account name to view the resource/account details such as resource owner, resource URL, DNS name, resource type, passwords, resource name, account notes, and last accessed time. To view the password of a particular account, tap on the eye icon beside the password.

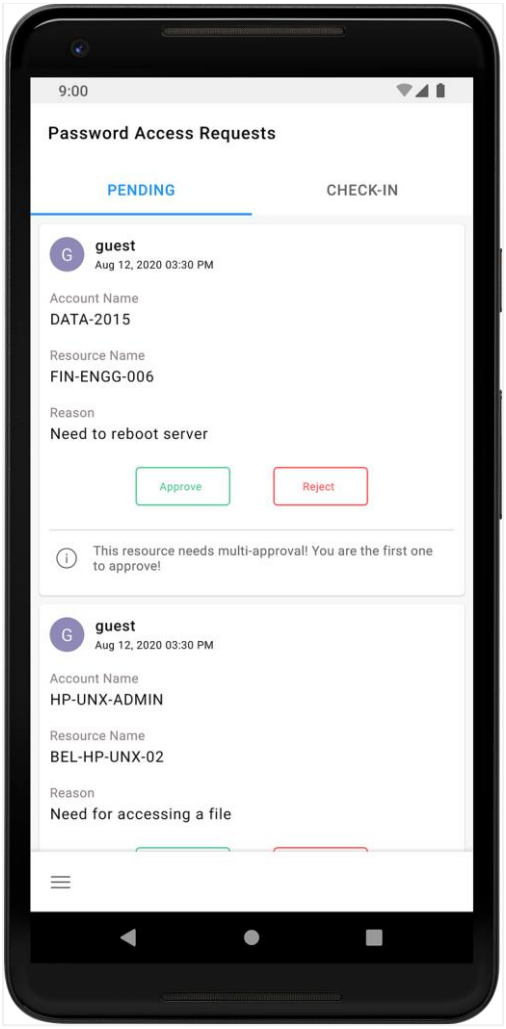


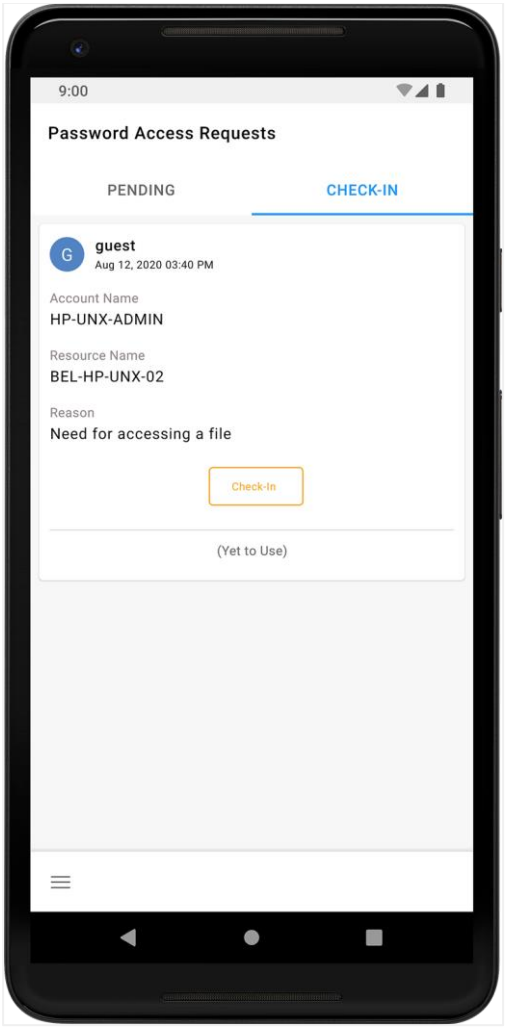
4.2 Password Access Requests

PAM360 provides an access control mechanism that allows administrators to grant password access to users for a specific period. Admins can start granting exclusive privileges once a password is ready to share, and only one user is allowed to use a particular password at a single point in time. Through PAM360's Android application, administrators can view the list of pending password access requests from other users and act upon them.

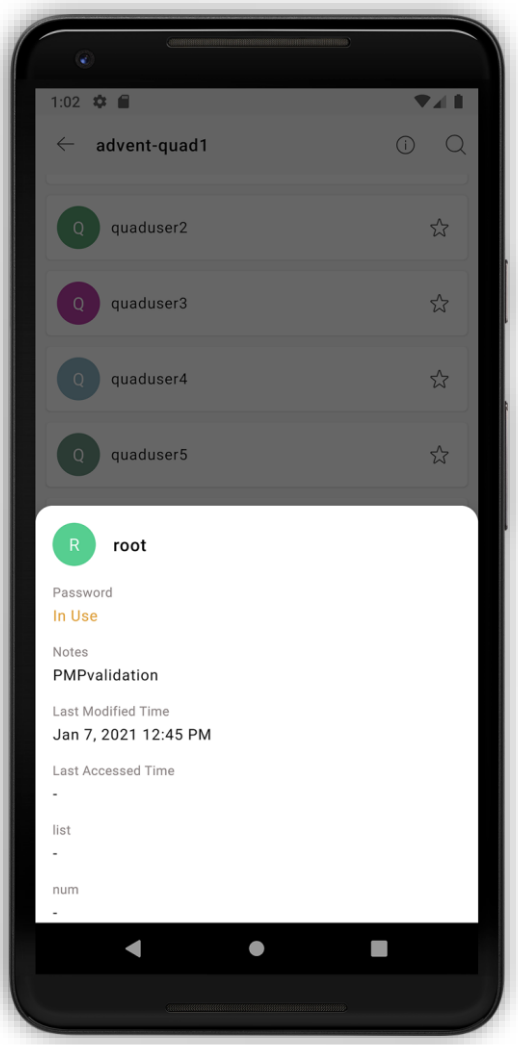
As an administrator, the **Password Access Requests** tab offers two sections:

1. **Pending** - to view the list of password access requests.
2. **Check-In** - to view the passwords that are currently in use and yet to be checked in.

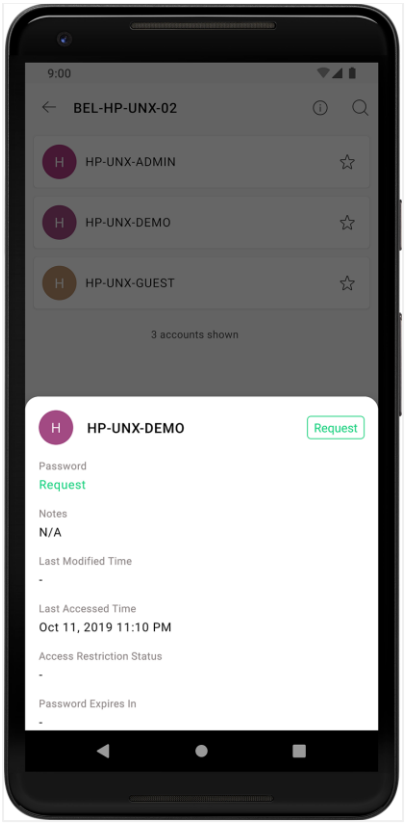


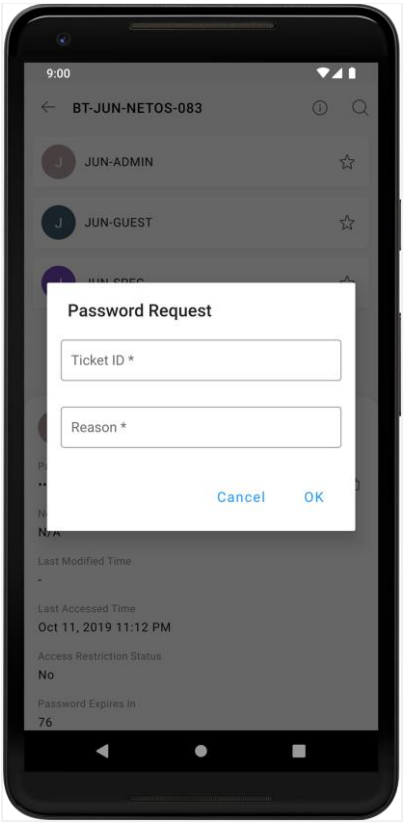


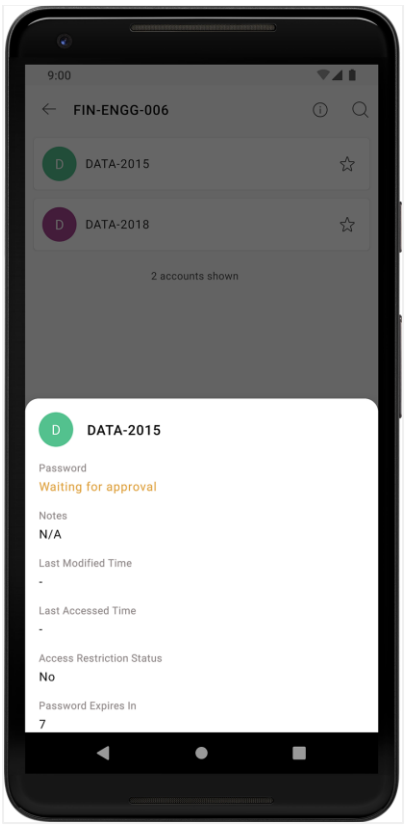
To send a password access request, tap an account, and tap the **Request** option in the account details section. Once your request has gone through, the status will change to **Waiting for Approval**. Once an admin has approved your password request, you will be notified of the same, and the password will be available for **Check Out**. Once you check out the password for use, the status changes to **In Use**. Other users can see this status change in both the **Check-In** tab and the **Account Details** section of the particular account. To give up access to the password, tap the **Check-In** option. Now, the password is checked back into the PAM360 vault.

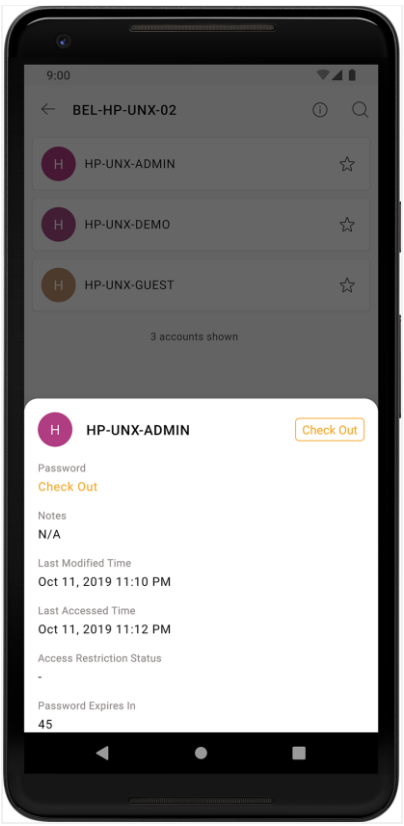


Once you check in the password and give up your access, you must go through the request-release workflow once again, if you should need access to it again. PAM360's Android application also supports ticketing desk integration. Through the integration, PAM360 will prompt users to provide a ticket ID along with their request. Then, PAM360 will validate whether the ticket ID entered by the user exists in the ticketing system or not and only then grant access to the user to view the password.



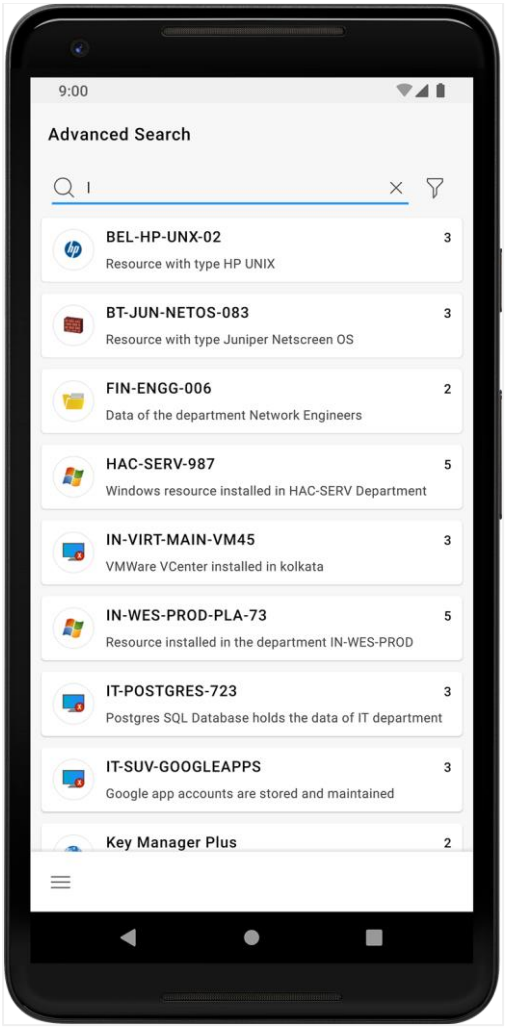


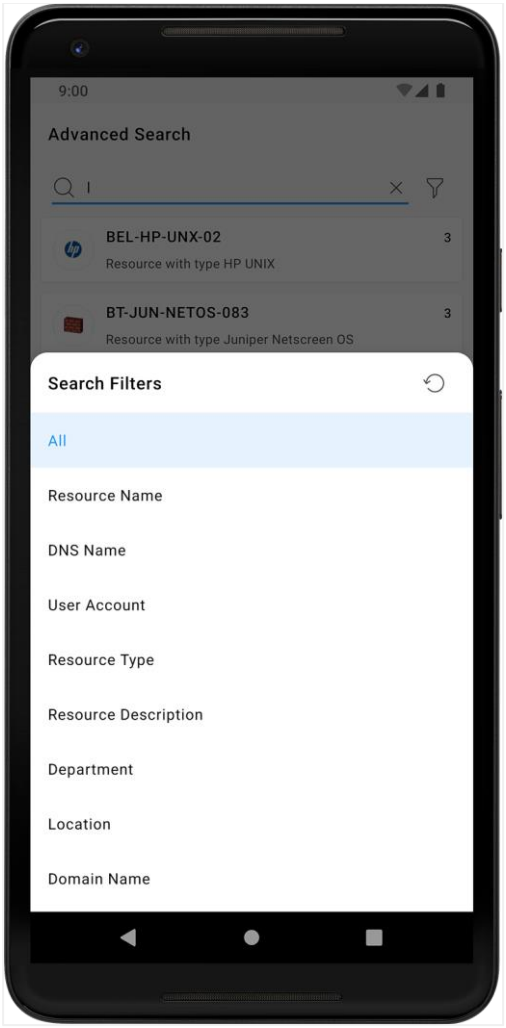




4.3 Advanced Search

Advanced Search in PAM360's Android application is a handy feature that can help you find any particular user or resource instantly. Tap **Advanced Search** from the navigation menu to either enter a keyword like **Name, Department, Location**, or use one of the many search filters available to tailor your search better. The available search filters are **Resource Name, DNS Name, User Account, Resource Type, Resource Description, Department, Location, Domain Name, and Resource URL**. In addition to these default fields, if you have created any additional fields in PAM360's desktop installation, those custom column names will also appear as filters in Advanced Search.



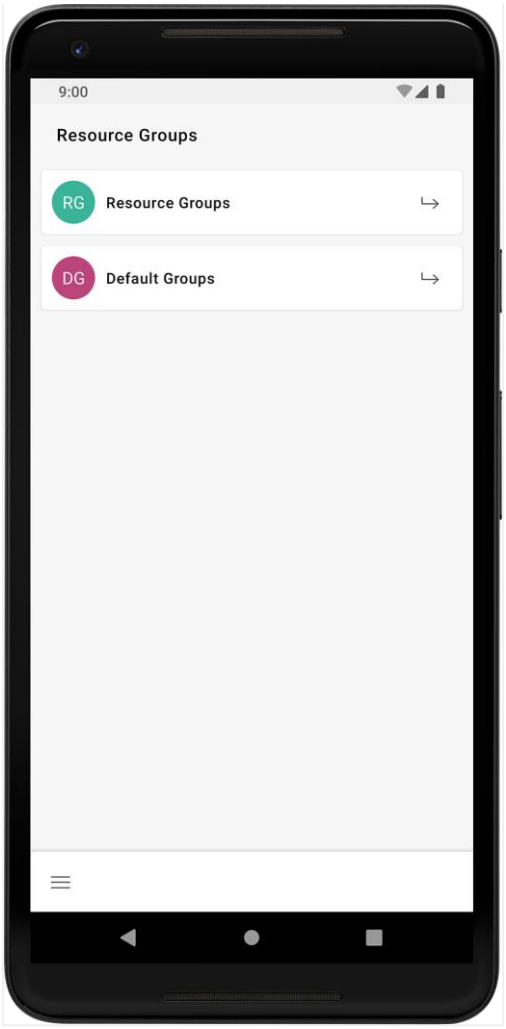


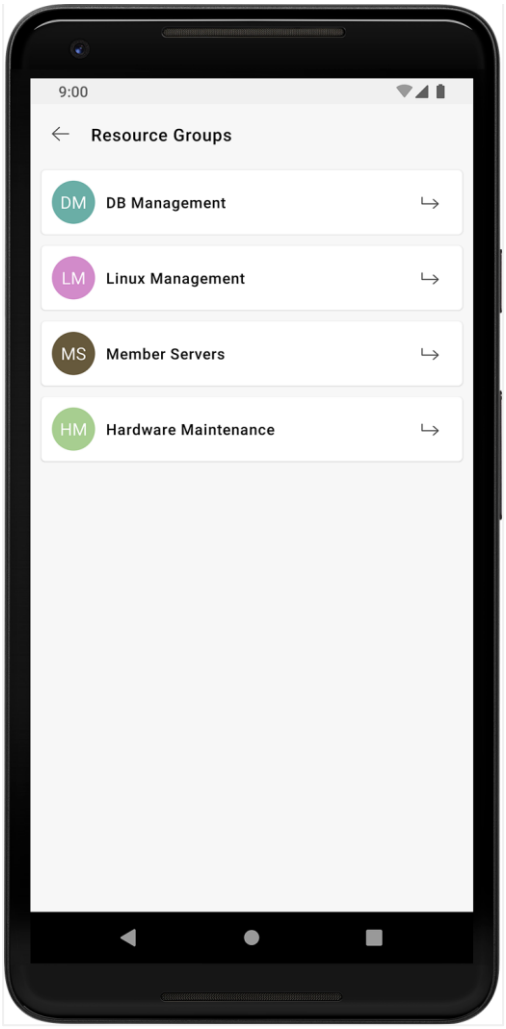
4.4 Resource Groups

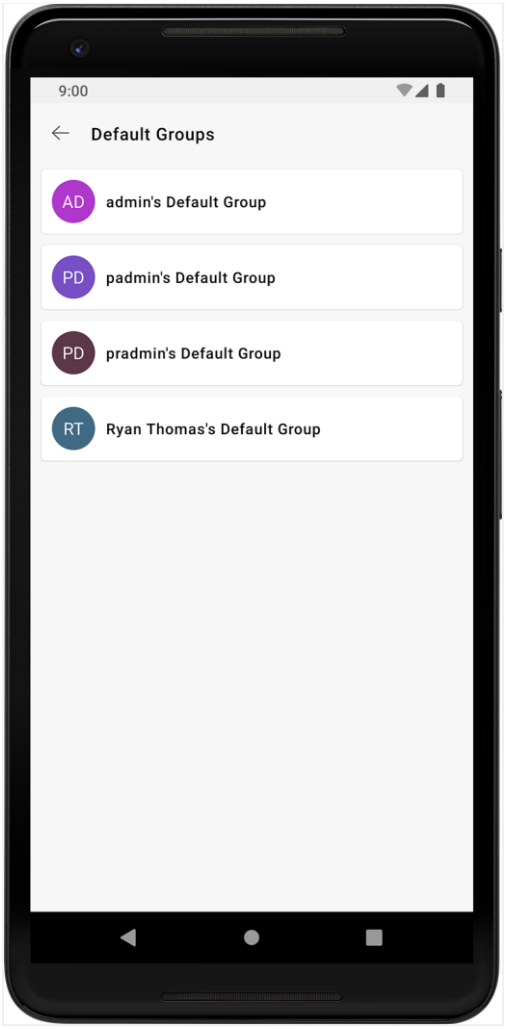
Administrators can create resource groups to combine similar resources for easier management. The grouping can be done either by specifying individual resources (Static group) or by specifying a set of criteria (Dynamic group). In the case of a dynamic or a criteria-based group, whenever a newly added resource matches the criteria of an existing group, PAM360 automatically adds the resource to this group. You can share the resource groups with other users or user groups. Users to whom the groups are shared can see the passwords of only the resources that are part of the shared group at that time.

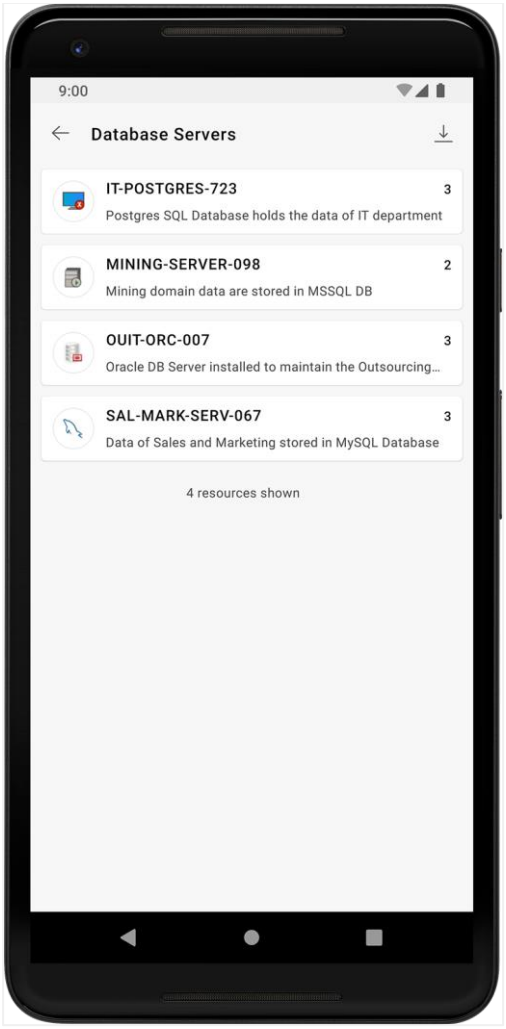
Tap the **Resource Groups** option from the navigation menu to view all the resource groups that are owned or managed by you. If a resource group has a subgroup, it will be indicated by a

right arrow icon; to view the subgroups, simply tap the arrow icon. If you wish to view the resources within a resource group, tap the name of the required resource group. Similarly, tap a resource name within the resource group to view the accounts that belong to the selected resource, and the account name to view the account details.



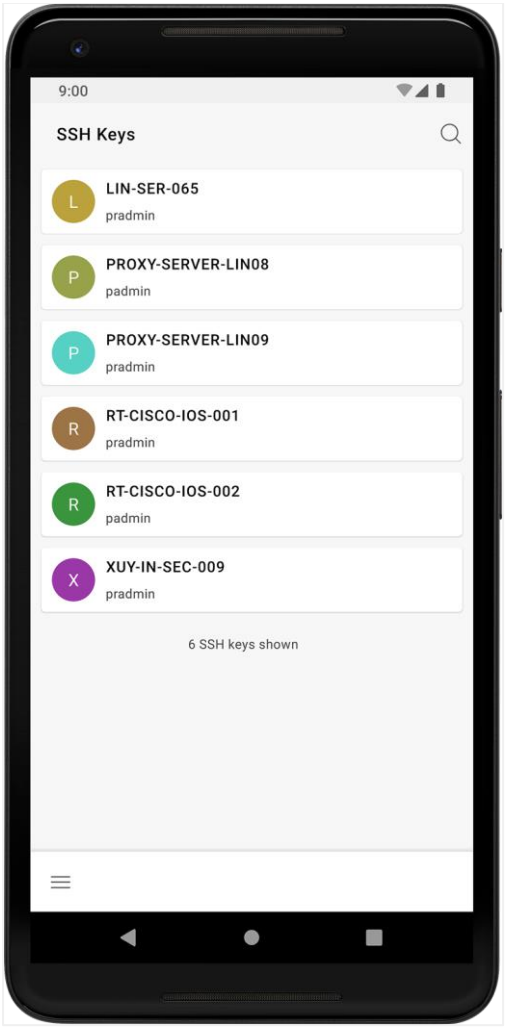


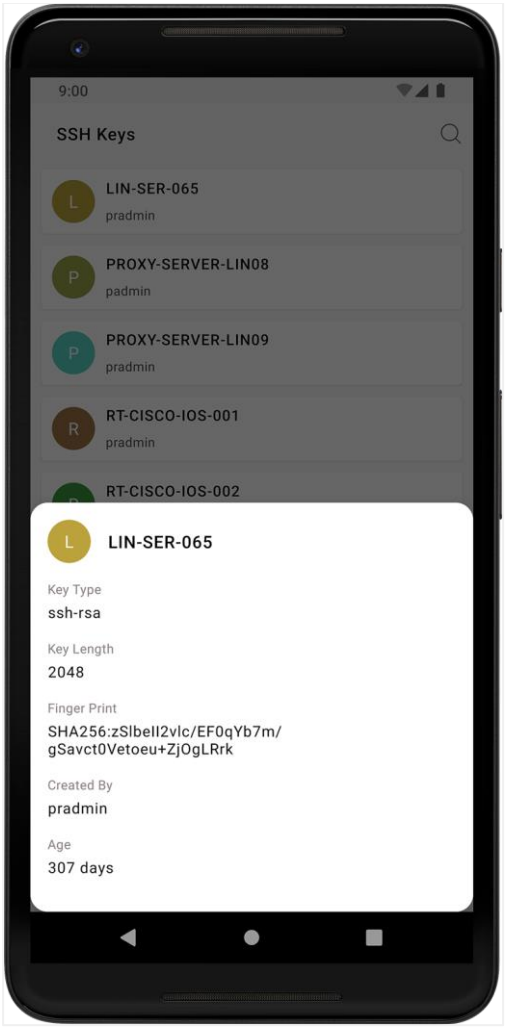




4.5 SSH Keys

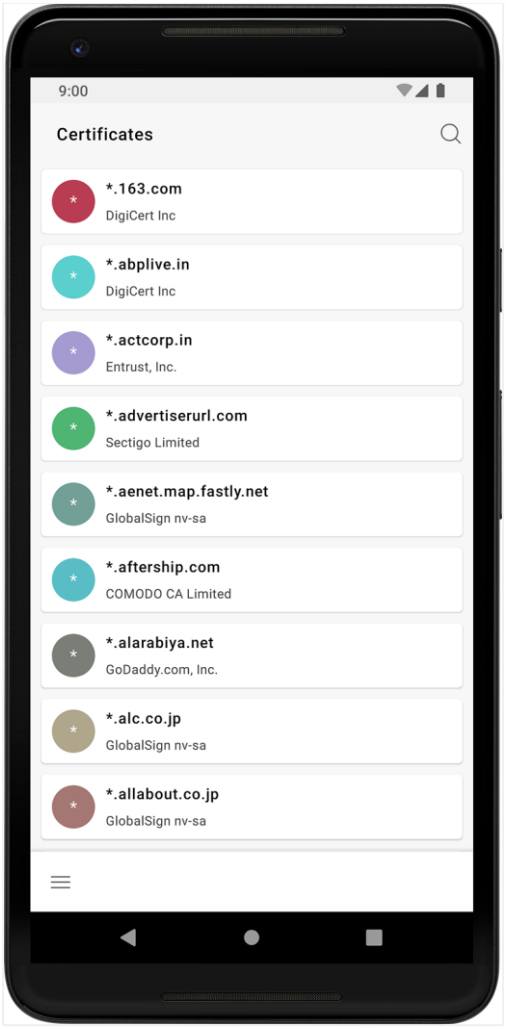
Tap the SSH Keys option from the navigation menu to view all the SSH keys that you are managing in the PAM360 repository. Tap any SSH key to view key details such as **Key Type, Key Length,** the key's **Fingerprint, Username** of the user who created the key, and **Age of the key.**

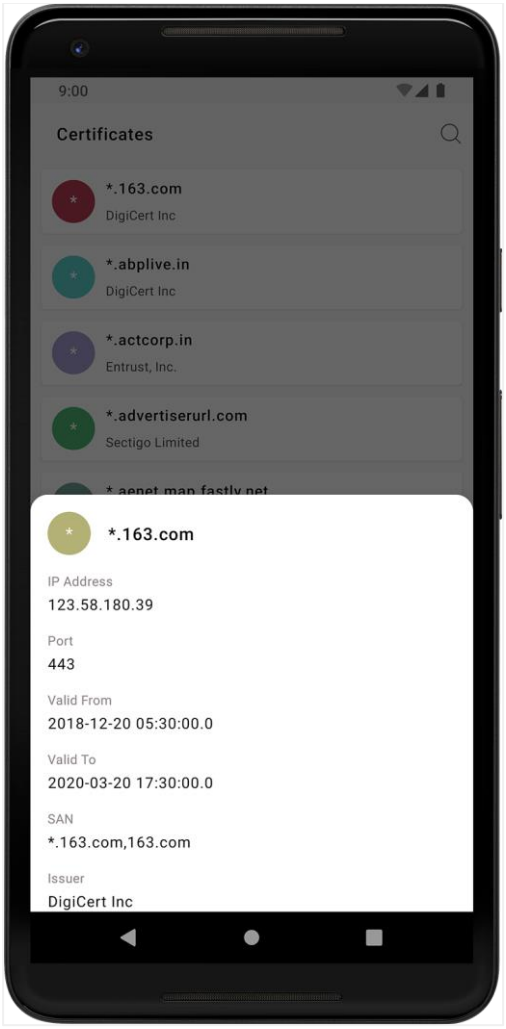




4.6 Certificates

Tap the Certificates option from the navigation menu to view all the SSL certificates that you are managing in the PAM360 repository. Tap any SSL certificate from the list to view the following certificate details: **Common Name, Port, Validity period, SAN, Issuer, Signature Algorithm, Finger Print, Serial Number, Key Algorithm, Key Size, Issuer.**



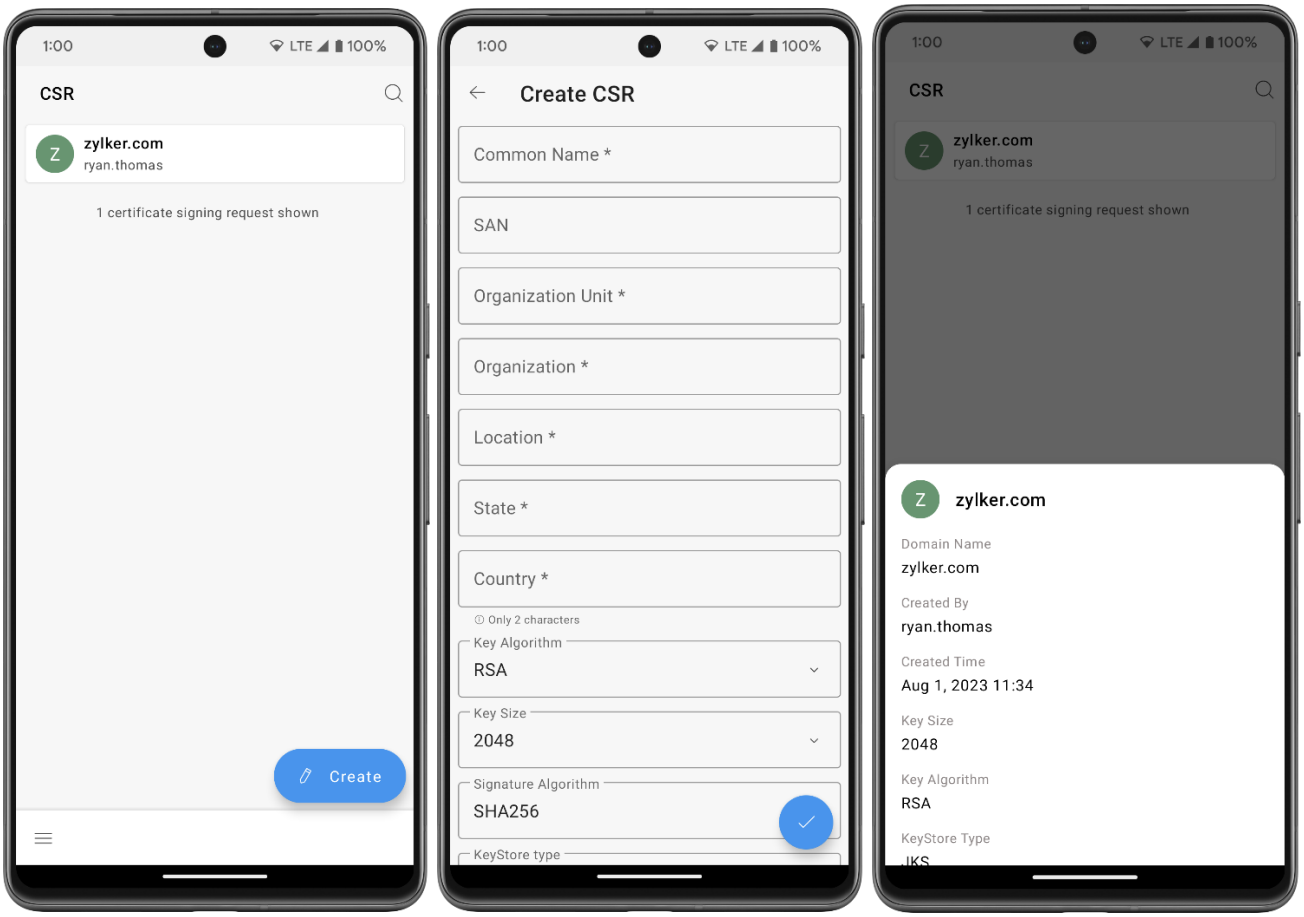


4.7 CSR

PAM360 mobile application allows you to view the Certificate Signing Requests (CSR) created in the web interface. Tap the CSR button from the navigation menu to view the CSR list. You can also create CSR in the mobile application by following the steps given below.

1. Tap **CSR** from the navigation menu and select **Create**.
2. Specify the required details such as Common Name, SAN, Organization Unit, Organization, Location, State, and Country.
3. Select the Key Algorithm, Key Size, Signature Algorithm, and KeyStore type.
4. Choose a Validity Type (Days, Hours, or Minutes) and mention the Validity.
5. Type the Store Password or tap the Generate Password icon to generate a key store password.
6. Enter the Expiry Notification Email address and tap the **Tick** button.

Your CSR will be added to the list. You can view it anytime from the CSR list.



4.8 Personal

Apart from storing enterprise passwords, PAM360's Android application allows you to store personal passwords in the PAM360 repository. The application provides four default categories: **Web Accounts, Banking, Credit Cards,** and **Contacts.** Among these categories, you can save your utmost personal data such as your personal email account information, credit card numbers, and other banking data, contact addresses, and phone numbers.

In addition to the default categories, add any number of additional custom fields to your **Personal** tab from the desktop application to store other information. For instance, if you wish to store details about the properties that you own, then add a custom category named **Properties**.

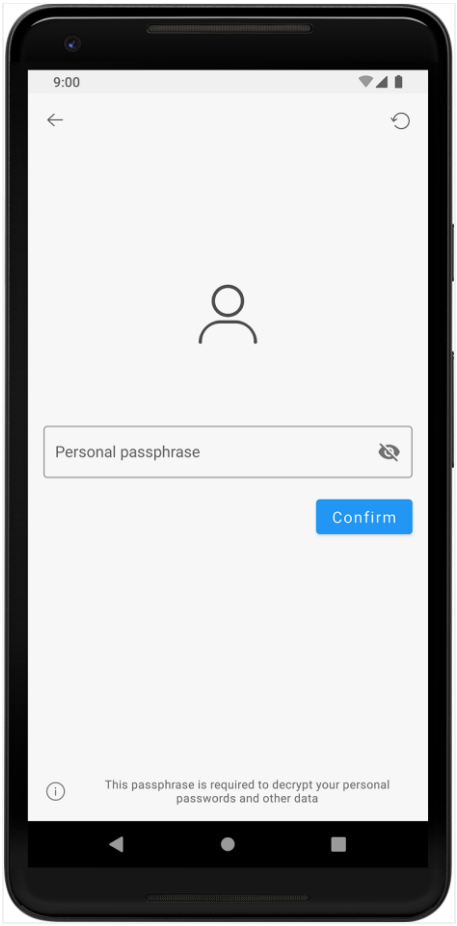
The application stores your personal data in a private repository that only you can access through the **Personal** tab. All information stored here is encrypted independently and hidden from all other users, including the administrator. While adding account details to the **Personal** tab, there is an option to add **Tags**. Under this attribute, add keywords that can be used to search for the account under a particular category. Tap the Search icon and enter a keyword that was previously added as a tag to locate the account you are looking for.

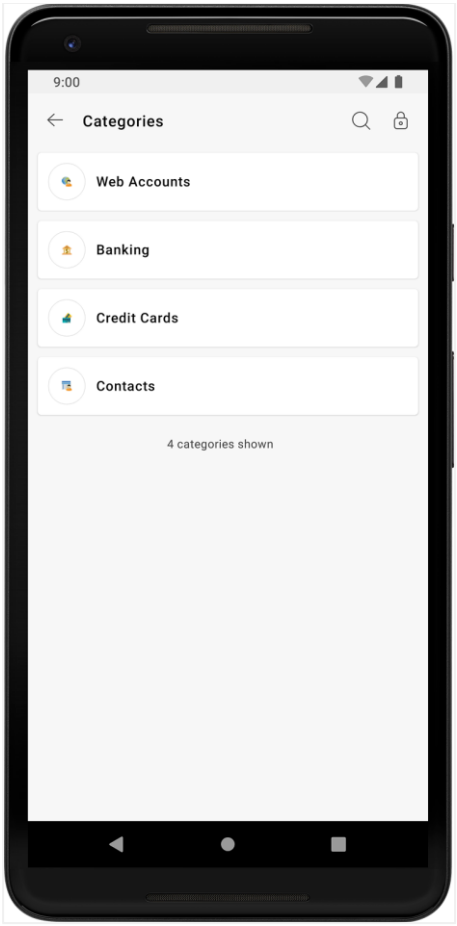
Note: To utilize the Personal tab on the PAM360 mobile application for managing personal information, the 'Allow users to manage their personal passwords' option should be enabled in the PAM360 web application.

4.8.1 Setting up a Personal Passphrase

To use the Personal tab in the application, you must set up a valid passphrase in PAM360's desktop installation and activate your Personal repository; do ensure the passphrase you provide matches the complexity rules enforced by your organization, if any. Once you set up your passphrase, you must enter it every time you need access to your personal passwords. Tap the refresh icon available at the top in case there is a change in the status of the personal passphrase. For example, if you try to login to your personal repository before setting up a passphrase, the application will not let you in. Once you create a passphrase in the desktop application, you can hit refresh in this page and login with your newly created passphrase right away, without moving out of the Personal tab.

Please note that if you forget or misplace the passphrase used for your Personal repository, you cannot reset the passphrase or retrieve your personal data without it.





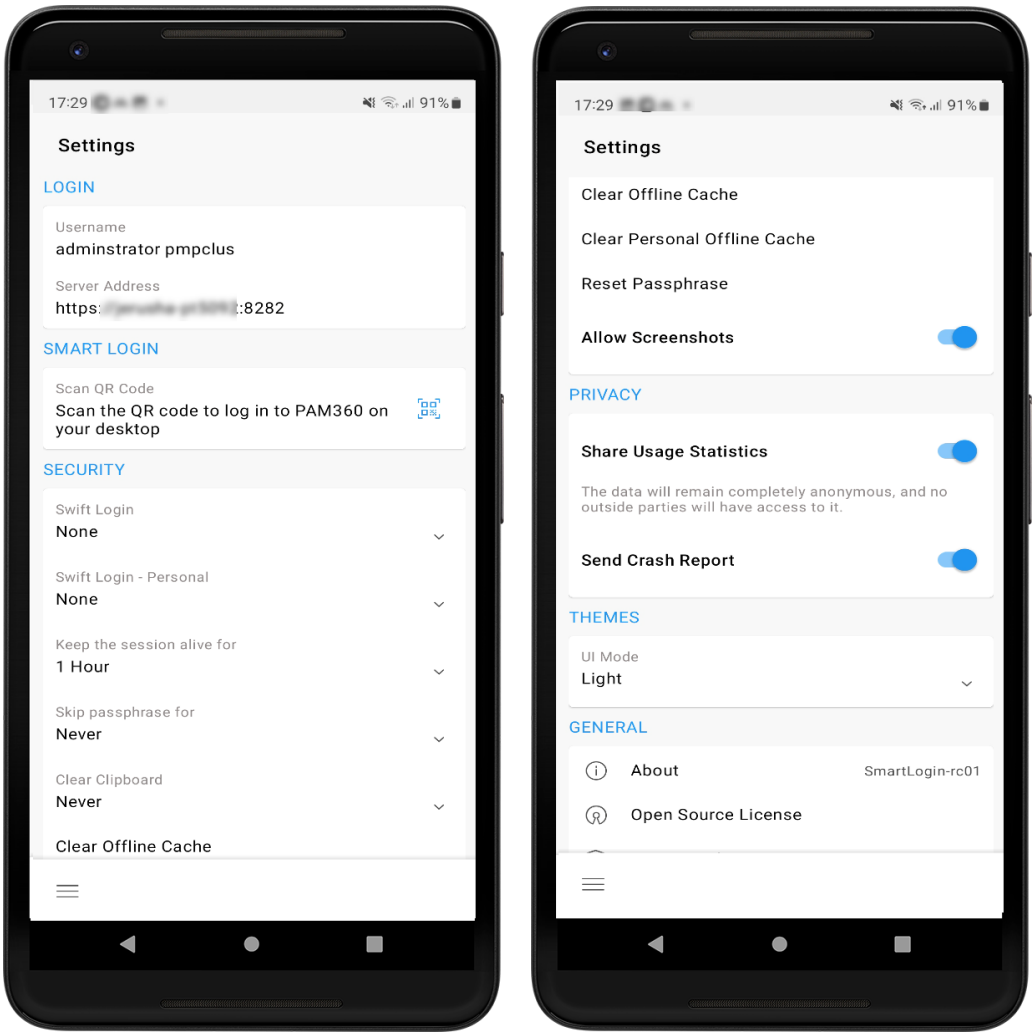
Alternatively, PAM360's Android application provides a **Swift Login** option that will allow you to quickly access Personal passwords instead of entering the passphrase every time. You can set up three different authentication methods for Swift Login: **Fingerprint, Pin,** or via **Credentials**. Click here to learn how to set up Swift Login in the Android application.

4.8.2 Exiting the Personal Tab

To exit the **Personal** tab, tap the lock icon at the top right corner. You will return to the **All My Passwords** section and the **Personal** tab will be locked. To enter the Personal tab again, you must supply the passphrase again.

4.9 Settings

The Settings menu offers a comprehensive collection of options that are split categorically for ease of use. Use this menu to customize various security options, view login details, privacy policy of the Android application, and more.



4.9.1 Login

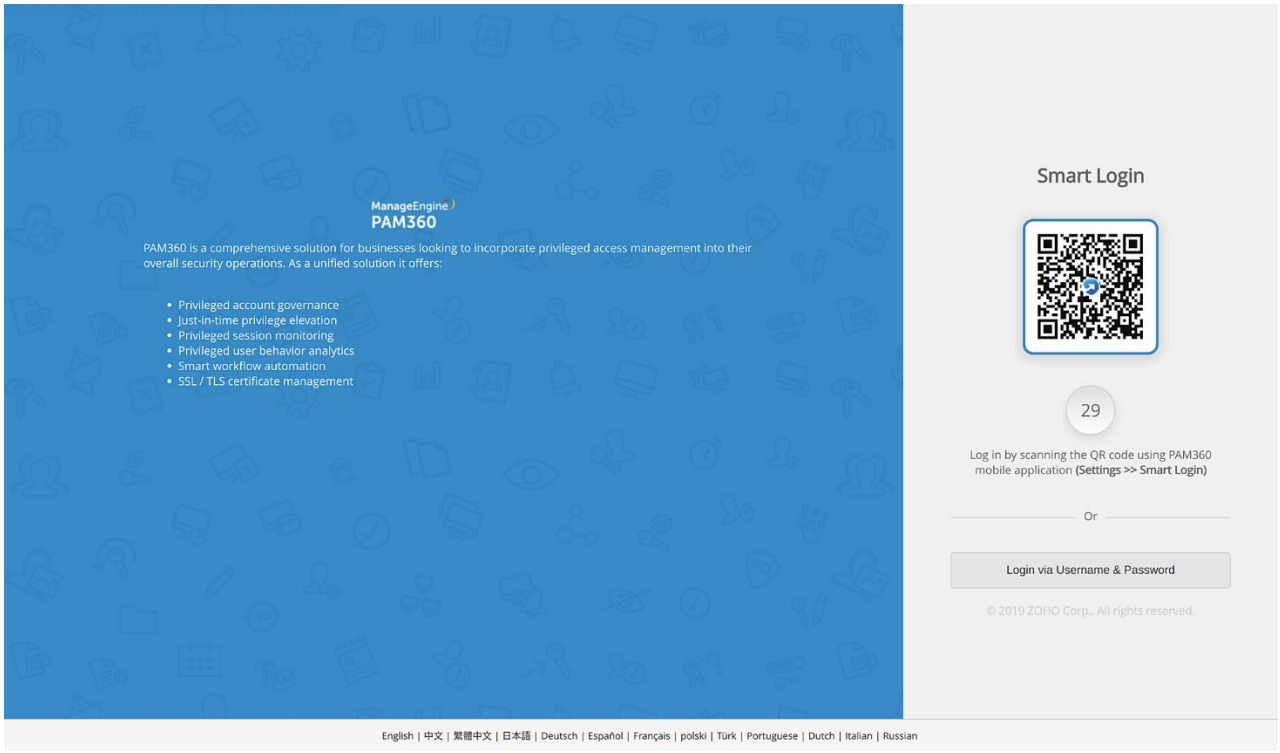
The **Login** section displays the **Username** and **Server** address to which PAM360 is currently connected. If the High Availability feature is turned on in your environment, then the Android application will also display the secondary server details on the **Settings** page. If the primary server is down, you can connect it to the secondary server for uninterrupted service.

4.9.2 Smart Login

The Smart Login feature enables seamless access to the PAM360 web interface by simply scanning the QR code presented on the PAM360 webpage. This direct login approach streamlines the process, providing password less authentication and substantially minimizing the effort required for web login, all while maintaining robust security measures.

1. Head to the PAM360 login webpage and select the **Smart Login** option.

2. Using the QR scanner available in the **Smart Login** section, scan the QR code displayed on the PAM360 web interface.



3. By doing so, you will be logged in to your PAM360 account.

4.9.3 Security

The **Security** section has the following options:

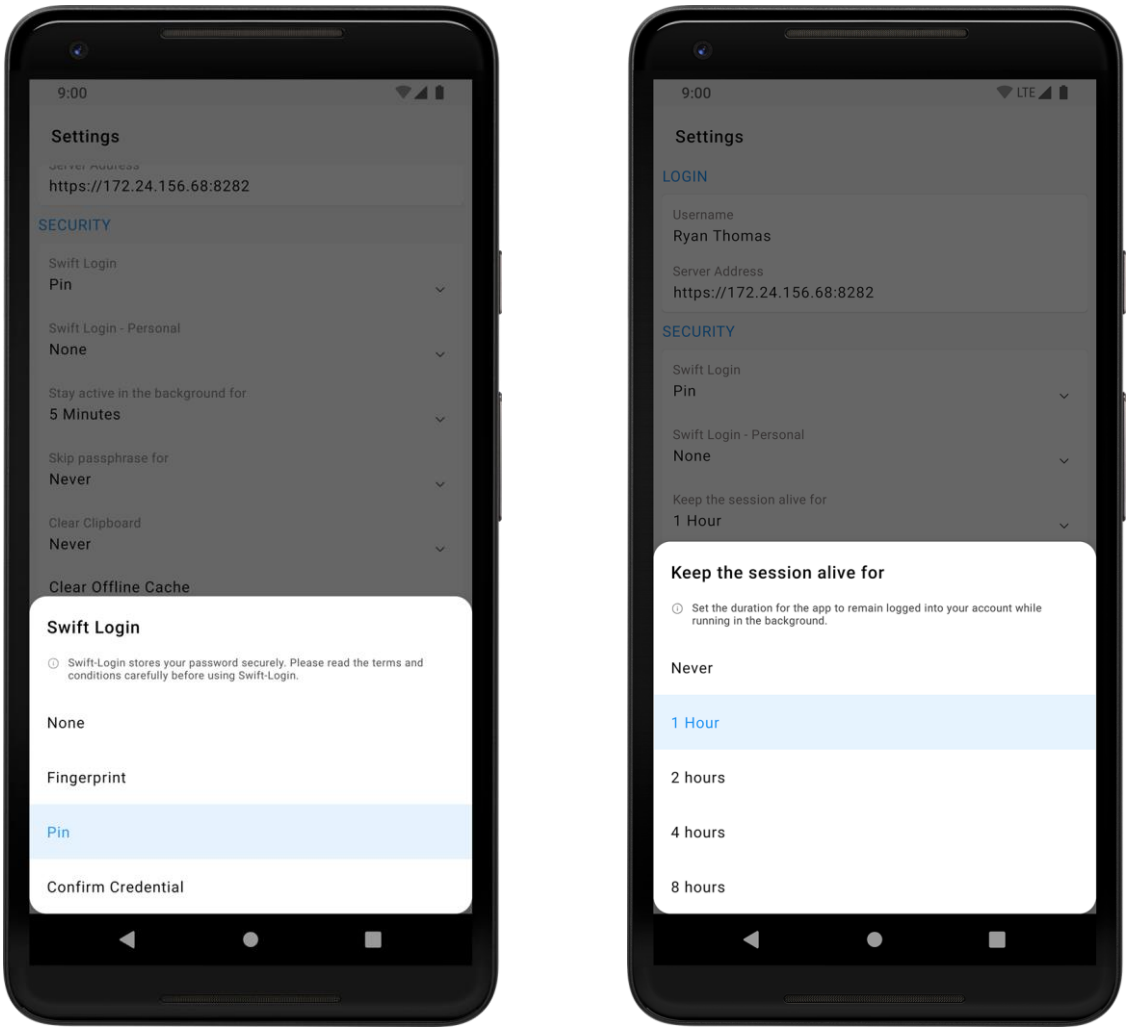
i. Swift Login

You can set up three different authentication methods for Swift Login: **Fingerprint, Pin,** or via **Credentials**. Use this option to log in quickly to the Android application using the local authentication on your phone.

ii. Swift Login - Personal

Tap this option to set up Swift Login for your personal passwords saved in the application.

> **Note:** To allow login Fingerprint in the mobile application, go to **Admin >> General Settings >> User Management** and enable the **Enable logins to mobile apps with fingerprint authentication** option.

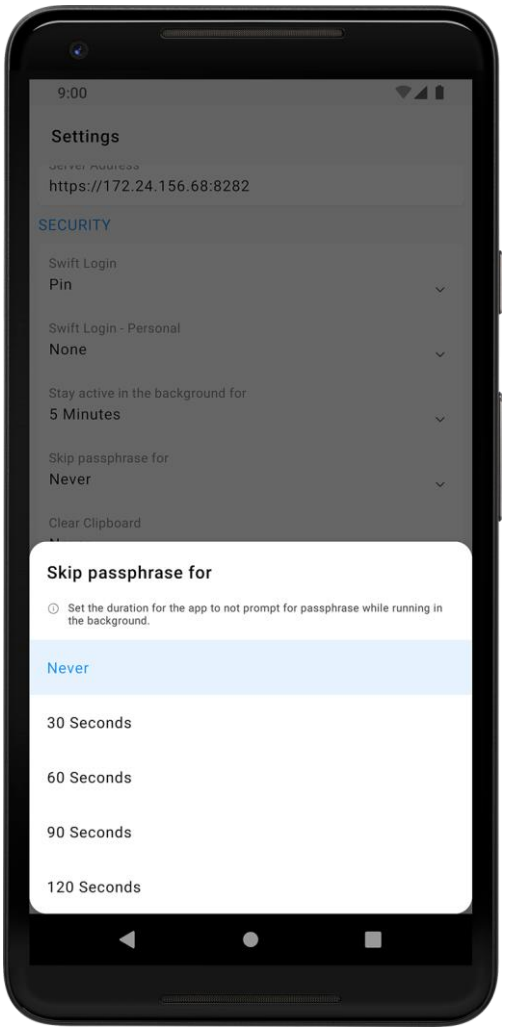


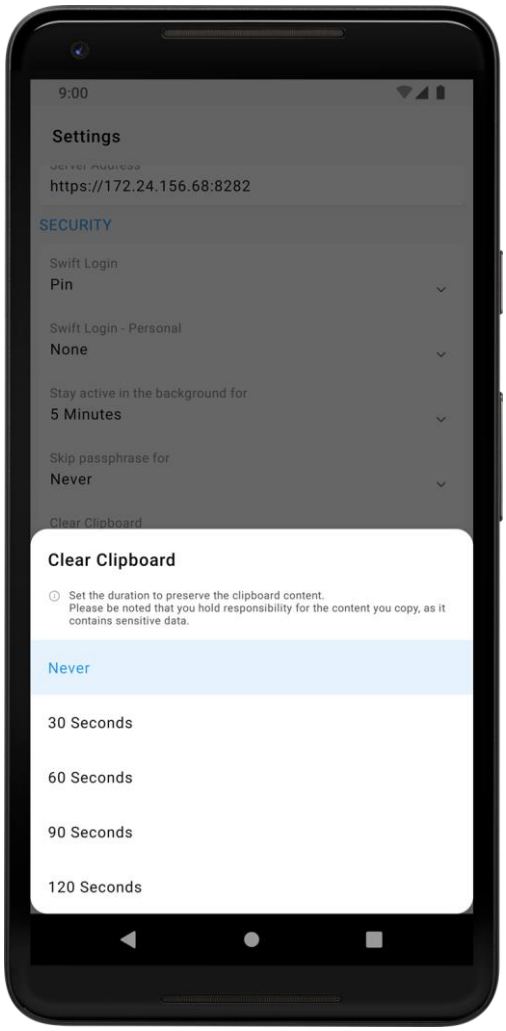
iii. Keep the session alive for

Set the duration for how long the application should remain logged in to your account when the application goes into the background. You can choose any one duration ranging from **1 to 8 hours**. This option is helpful when you want to switch between PAM360 and other apps multiple times within a short span of time. Alternatively, tap **Never** to log out as soon as the application goes into the background.

iv. Skip passphrase for

If you leave the application, however briefly, without logging out, it will prompt you to enter your passphrase again to get back in. Set a duration for the application to not prompt for the passphrase while running in the background. You can choose any one duration ranging from **30 to 120 seconds**. Alternatively, tap **Never** to always prompt for a passphrase during login.





v. Clear Clipboard

PAM360's Android application can preserve any data you copy from within the application for a specified duration. To copy any password, tap the copy icon that is present beside the password. Tap the **Clear Clipboard** option to set a duration to preserve content you have copied to the clipboard. You can choose any one duration ranging from **30 to 120 seconds**. Alternatively, tap **Never** to never save any copied content in the clipboard.

vi. Clear Offline Cache

Tap this option to clear all offline cache. This action will delete all your enterprise passwords that are saved offline.

vii. Clear Personal Offline Cache

Tap this option to clear all personal offline cache. This action will delete all your personal passwords that are saved offline.

viii. Reset Passphrase

Tap this option to reset your passphrase for mobile authentication. Please note that

resetting the passphrase will erase all the cached data from this device. This includes both enterprise and personal offline data unless you have set a different passphrase for your personal data. In that case, only the enterprise offline data will be erased.

ix. **Allow Screenshots**

Using the toggle button, you choose to allow or disallow screenshots within the application.

4.9.4 Privacy

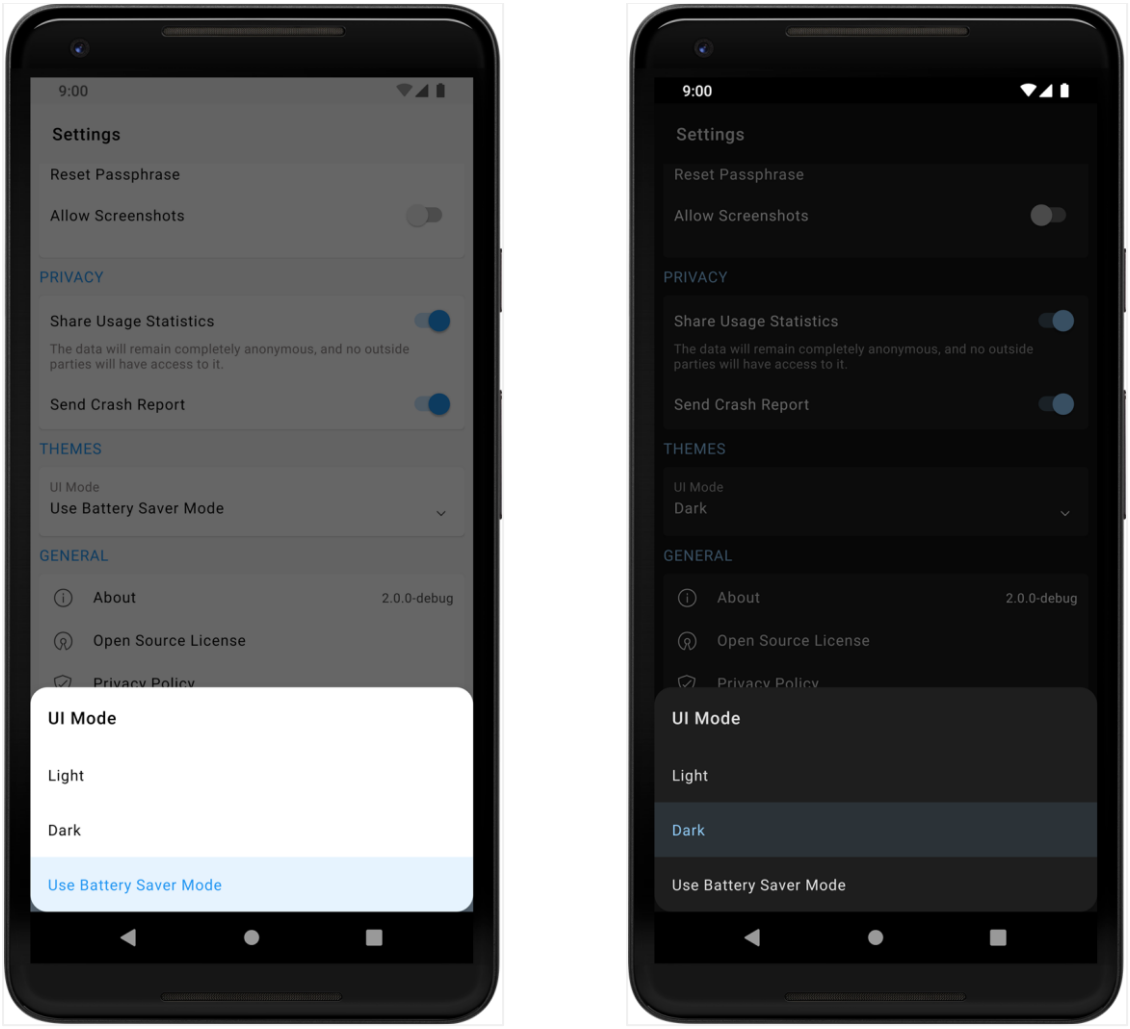
Apart from the above options, you can choose to share **Usage Statistics** or **Crash Reports** to ManageEngine by using toggle buttons under Privacy.

Usage statistics data gives an insight into usability data such as what features of the application you use more, how frequently, etc. This type of data is used as research to learn user behavior, gather pain points, if any, and enhance the application's performance and user experience based on the data.

Crash reports are detailed system logs that capture the state of the application when the crash happens. Collecting and analyzing this data will help us learn what caused the application to crash and rectify it in the next version.

4.9.5 Themes

To change the Android application's theme, tap the drop-down under **Themes >> UI Mode**. Here, you can choose **Light/Dark** mode or choose to use the **Battery Saver Mode**.

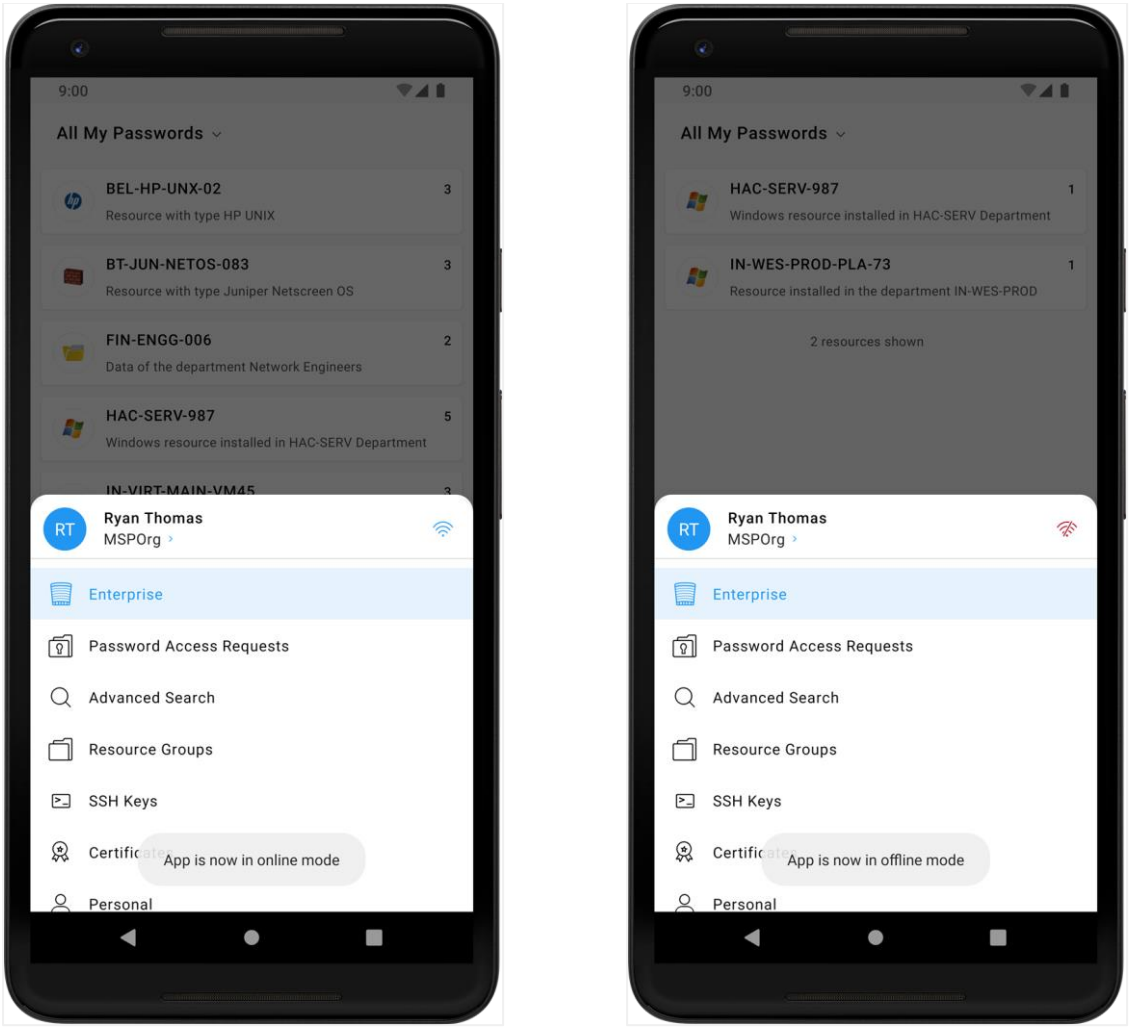


5. Setting up Secure Offline Mode

PAM360's Android application offers a secure offline mode that allows you to access passwords even when you do not have access to the internet.

To access passwords in the offline mode, download the required passwords first; only the passwords which are downloaded before going offline would be available for access in the offline mode. Apart from downloading individual passwords, the application allows you to download a group of passwords from the Enterprise Filters, such as the **Favorites, Recently Accessed, Windows RDP Passwords,** and **SSH Passwords.** Additionally, you can download resource groups and personal passwords. To download passwords for offline access, go to the Enterprise Filters, and click the downward arrow beside the required list of passwords.

> **Note:** Secure Offline Mode will work only if the **Allow password caching for offline access via mobile** option is enabled in General Settings.



6. Uninstalling the Mobile Application

To uninstall the mobile application, follow the below steps:

1. Locate the ManageEngine PAM360 application on your device, long press the icon, and click **Uninstall**.
2. Tap **Ok** in the confirmation pop-up.

Now, the PAM360 mobile application is successfully uninstalled. Once you uninstall the application, all PAM360-related data is removed from the device.

Technical Support

If you face any issue with the mobile application, get in touch with our technical support team.

Toll free number: +1-888-720-9500
Email ID: pam360-support@manageengine.com

Download PAM360 iPhone app	Download PAM360 Android app
	

PAM360 Mobile Application - iOS

PAM360's mobile application for iOS brings the solution's comprehensive enterprise password management features to your fingertips, thereby making on-the-go management of your enterprise's privileged accounts and passwords more accessible through your mobile device. Since the iOS application uses advanced AES-256 encryption to encrypt all your data, accessing your enterprise accounts through your iOS device is just as secure as PAM360's desktop installation. The mobile application also secures all communication between your PAM360 server and the iOS application using the HTTPS protocol over SSL.

> **Note:** The PAM360 iOS application requires a valid working instance of the ManageEngine PAM360 web application.

At the end of this document, you will have learned the following:

1. Salient Features
2. How does Secure Authentication Work in the PAM360 Mobile Application?
3. Getting Started with the Application
   - 3.1 Application Overview
   - 3.2 Installation and Authentication
4. PAM360 iOS Application - Navigation Menu
   - 4.1 Enterprise
   - 4.2 Requests
   - 4.3 Advanced
   - 4.4 Personal
   - 4.5 Settings
5. Uninstalling the Mobile Application

1. Salient Features

PAM360's iOS application comes with an all-encompassing set of features that can help you take control of your privileged accounts, even when you are away from the desktop installation.

- View and manage all passwords that are owned or managed by you.
- Approve/reject password requests and monitor who checks out passwords directly from the PAM360 iOS application. Also, send password requests, and perform

password check in and check out through the mobile application.

- Incorporate ticket ID validation through PAM360's ticketing system integration to secure your access approval workflow even further.
- View and manage your SSH keys and SSL certificate details at any time.
- Store and manage your critical personal information such as credit card numbers for on-the-go access. PAM360's iOS application encrypts your personal data using the advanced AES-256 encryption algorithm.
- Save important passwords offline to access them even when you do not have access to the Internet.

2. How does Secure Authentication work in the PAM360 Mobile Application?

The application offers Two-Factor Authentication (TFA) for enhanced security. Once enabled, users have to authenticate themselves through two successive stages to access the mobile interface. There are three ways of doing the first level of authentication: PAM360's native authentication using Active Directory/LDAP/Azure AD credentials, or via SAML SSO. The second level of authentication can be done through any of the Two-Factor Authentication provisions supported by PAM360. After the Two-Factor Authentication is complete, PAM360 prompts you to set up a passphrase for your account, with a minimum of 8 characters, used for mobile authentication. All your offline data is encrypted using the advanced AES-256 encryption algorithm. Please note that the application does not store your passphrase, and it is mandatory to enter the passphrase during login.

Administrators can selectively allow or restrict mobile application access to users. Navigate to **Admin >> Users >> More Actions** and click the **Restrict Mobile Access** option. The users with the restriction cannot log in to their PAM360 accounts through the iOS application.

Similarly, administrators can allow users to cache passwords in their mobile devices. Go to **Admin >> General Settings >> User Management** and select **Allow password caching for offline access via mobile**. Leave this option unchecked to restrict users from accessing passwords offline.

3. Getting Started with the Application

3.1 Application Overview

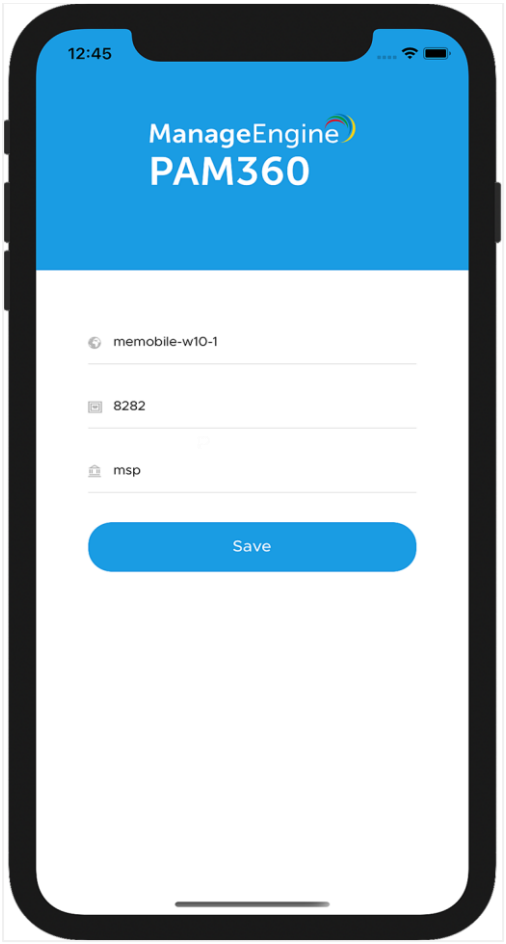
Supported Devices	**iPhone, iPod Touch**
Compatibility	Requires iOS 13.0 or higher.

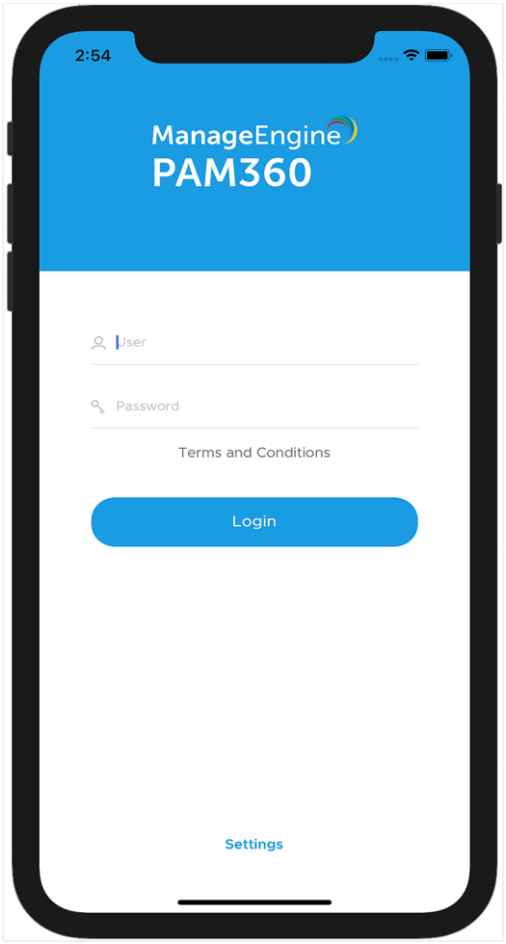
Size	19.5 Mb (approx)
Languages Supported	English, French, German, Japanese, Polish, Simplified Chinese, Spanish, Traditional Chinese, Turkish, Portuguese, Italian, Russian, and Dutch. **Note**: Please select your desired language on the PAM360 desktop installation and the mobile device.

3.2 Installation and Authentication

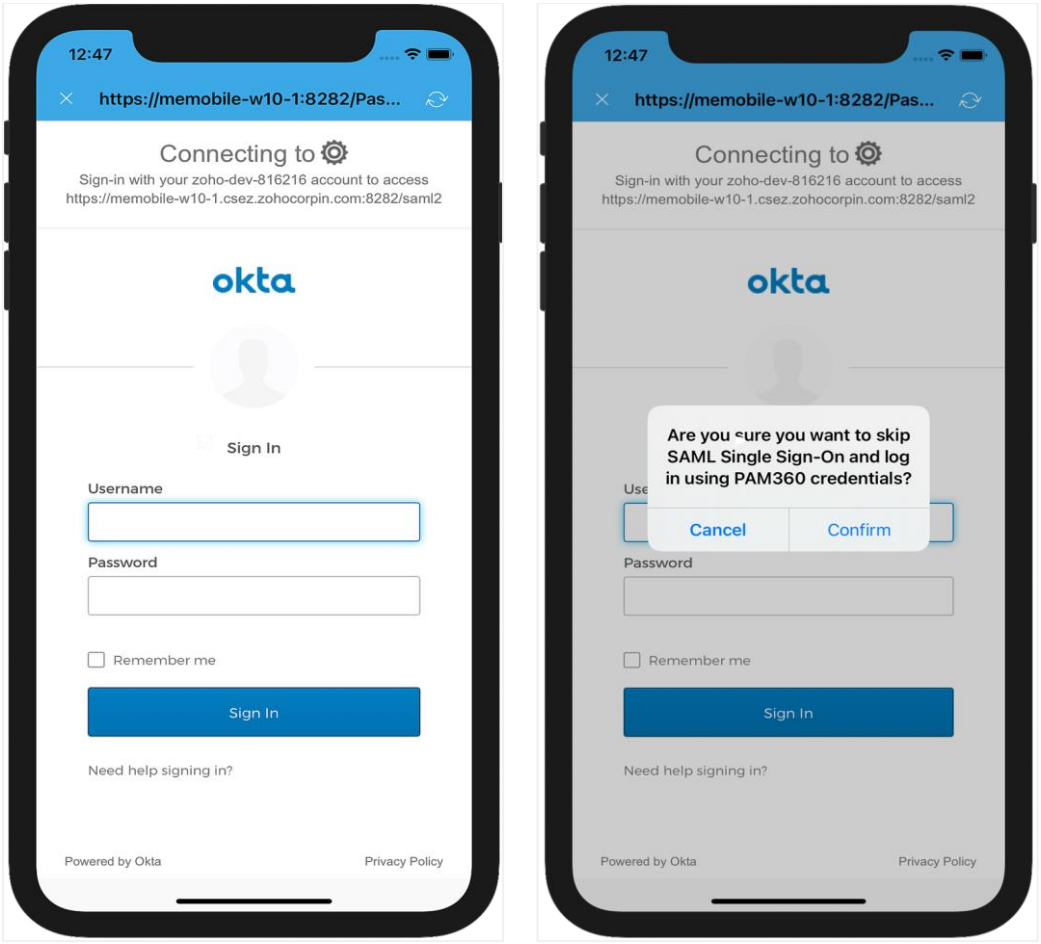
Follow the below steps to download and install the PAM360 mobile application:

1. Go to the App Store and search for ManageEngine PAM360 or click this direct link.
2. Click **Install** to install the application on your device.
3. After successful installation, enter the following details to get started with the mobile application:
    i. Enter the **Server Name** or **IP address** in which PAM360 is running, along with the **Port**. If your PAM360 server is installed in a physical network, ensure that the PAM360 server and the mobile application are connected to the same network. However, if your PAM360 server is hosted in the cloud, your mobile application will work from a different network as well.



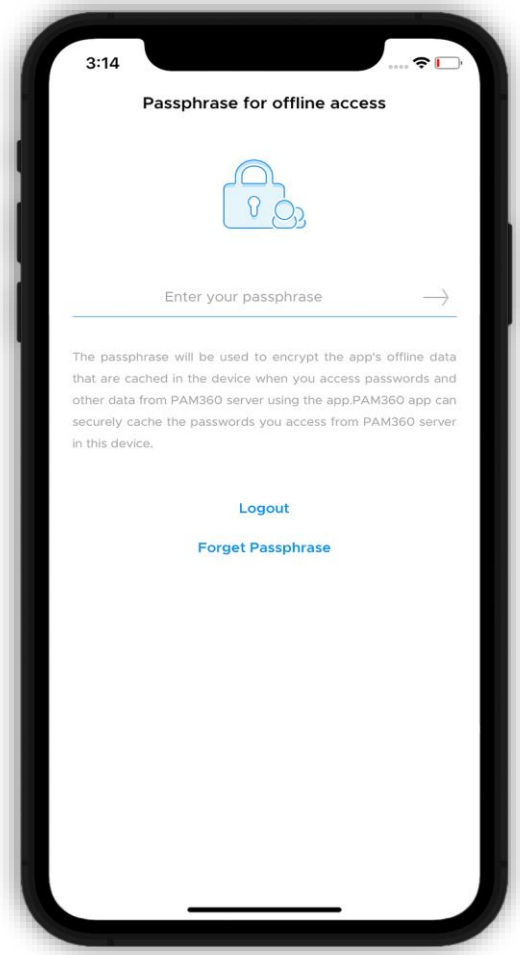


ii. To login, enter the username & password of your PAM360 account. The iOS application supports three ways of authentication; login through PAM360's native authentication, through Active Directory/LDAP/Azure AD authentication, and via SAML SSO. To login using Active Directory/LDAP credentials, select your domain name from the drop-down list. If SAML single sign on is enabled in your PAM360 server, a browser window opens within the application.



iii. Here, enter your SAML SSO credentials to login. To skip the SAML SSO login, close the browser window and you will be redirected to the application's login page.

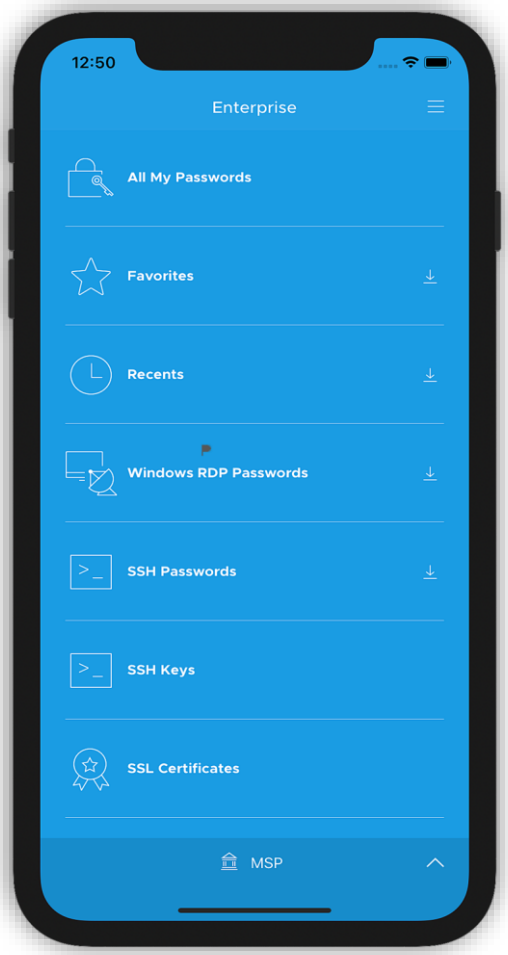
iv. Set up a passphrase for your account. Please note that the application does not store your passphrase, and it is mandatory to enter the passphrase during login, each time you access the mobile application. You have a total of five attempts to enter the correct passphrase, after which you will be logged out of the application automatically. If you have forgotten your login passphrase, tap the **Forgot Passphrase** option to set up a new one.



4. PAM360 iOS Application - Navigation Menu

Once you have signed into your PAM360 account through the iOS application, you will see the Navigation Menu on the main screen with the following options that will help you navigate the iOS application efficiently:

1. Enterprise
2. Requests
3. Advanced
4. Personal
5. Settings



i. Choosing Client Organization as an MSP User

If you are an MSP user, PAM360's iOS application allows you to manage the administrative passwords of all your clients separately from a single management console. The application neatly segregates client organizations into different sections, which you can tap to view all the passwords belonging to that particular organization. As MSP admin, even though you can view the names of the organizations you manage, you will be able to view the data on all your customers only if you add their resources or if they share their resources with you. Your clients will be able to view the data belonging to their organization only.

As an MSP user, you can choose a client organization and view all the resources under it. To do so:

1. Tap the hamburger icon to open the **Navigation Menu**. Here, tap on the organization name to display all the available client organizations.
2. Tap the client organization name to display all the resources specific to the selected

organization. Please note that the mobile interface will display only the resources specific to the selected organization.

4.1 Enterprise

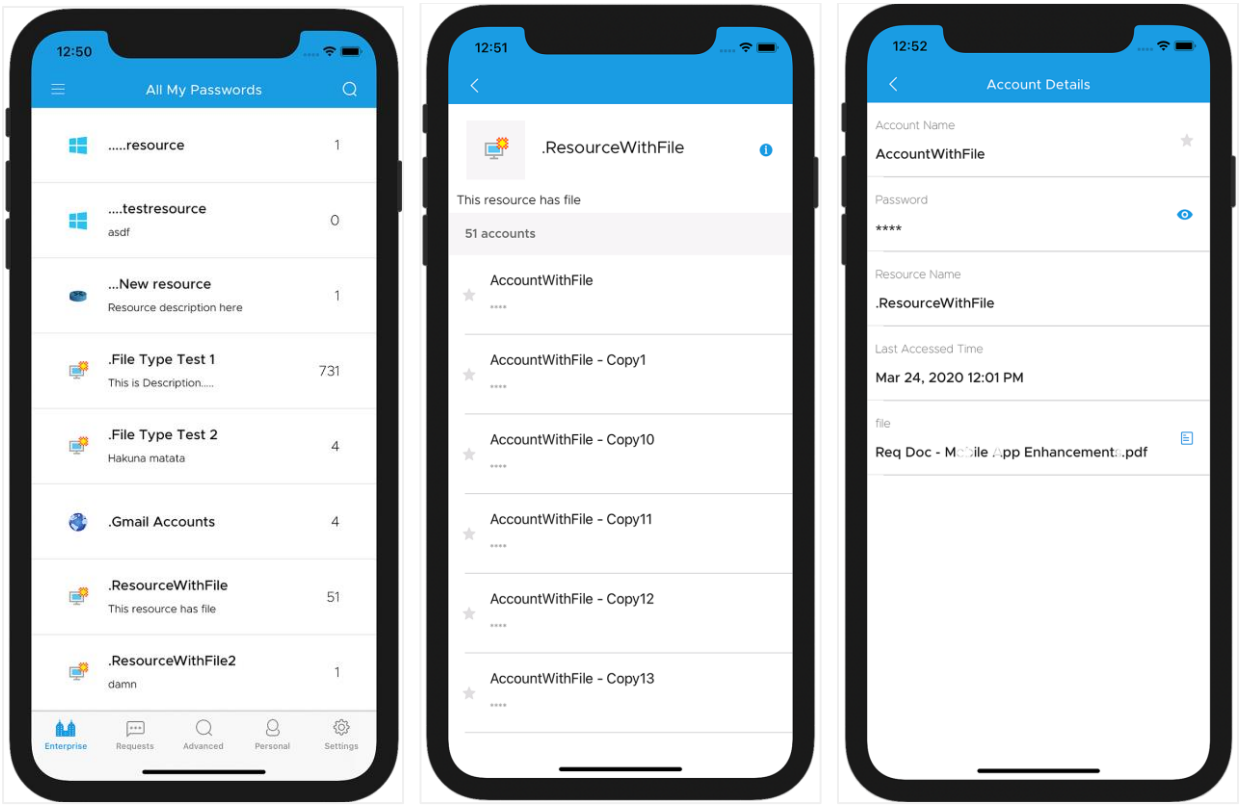
By default, the application displays a list of all the resources on the main screen. From here, tap on any resource to view the accounts associated with it. Tap the hamburger icon at the top left corner to open the Enterprise menu. This menu displays a list of resources owned or managed by you, categorized as below:

i. All My Passwords
ii. Favorites
iii. Recents
iv. Windows RDP Passwords
v. SSH Passwords
vi. SSH Keys
vii. SSL Certificates
viii. Resource Groups

Each menu has a dedicated Search icon that allows you to locate accounts within the menu. The application loads a list of accounts as and when you scroll. When you search for an account using a keyword, the application searches for the keyword only in the already loaded list; to search through all available accounts, scroll to the end of the list to load all the accounts.

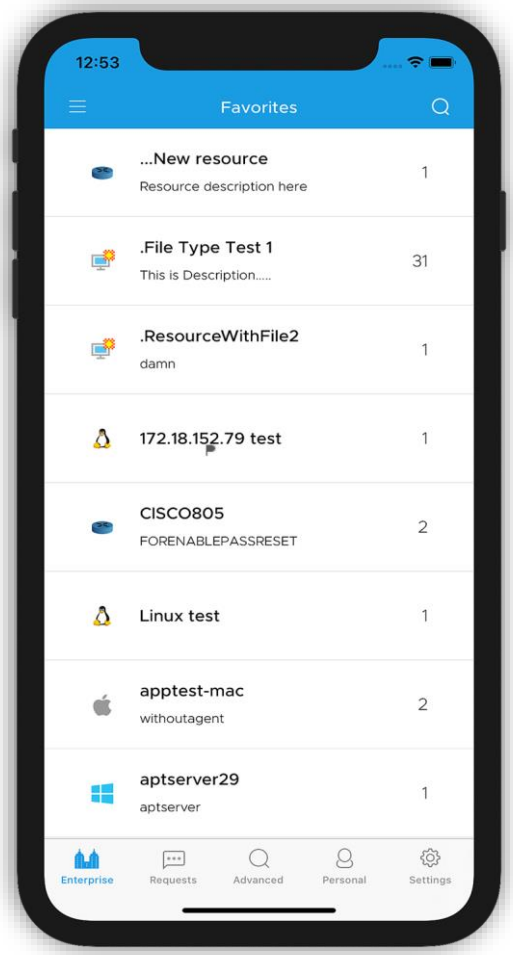
i. All My Passwords

This category lists all resources and accounts that are owned and managed by you. Tap on any resource/account name to view the resource/account details such as resource owner, resource URL, DNS name, resource type, passwords, resource name, account notes, and last accessed time. To view the password of a particular account, tap on the eye icon beside the password. Tap the Search icon to search for any account within the selected resource, using a search keyword.



ii. Favorites

This option is to have quick access to the list of passwords that you marked as Favorites. To mark any password as your favorite, tap the star icon beside the required password in any category. Marking passwords as Favorites helps you locate a particular account and its password easily, without the need to scroll through the entire list every time. Tap the Search icon to search for any account within the selected resource, using a search keyword.

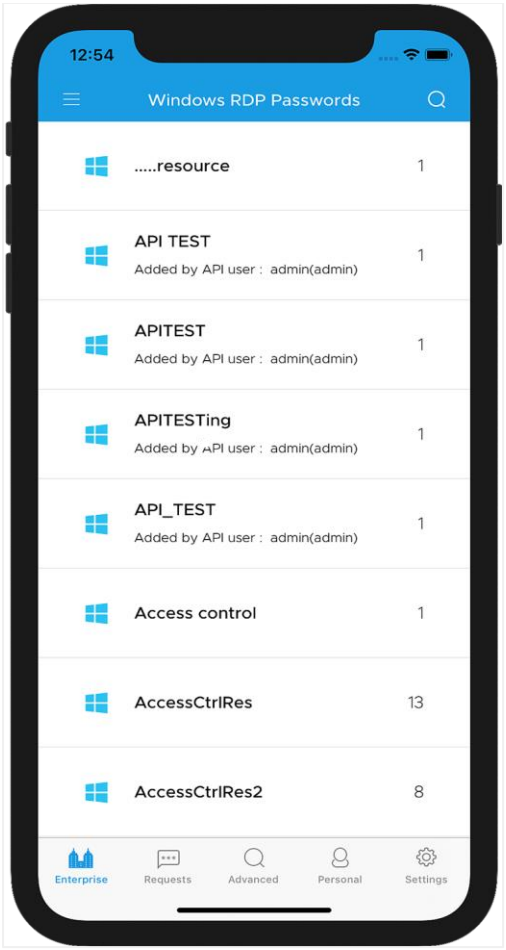


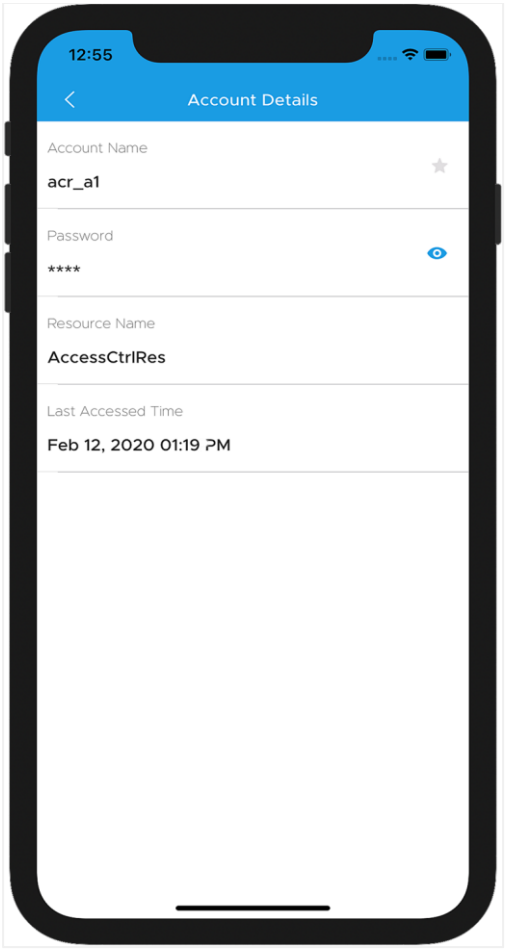
iii. Recents

This menu helps you view-only the list of resources and passwords that you have recently viewed or used. From the list, you can tap on any resource to view its accounts and their corresponding details. Tap the Search icon to search for any account within the selected resource, using a search keyword.

iv. Windows RDP Passwords

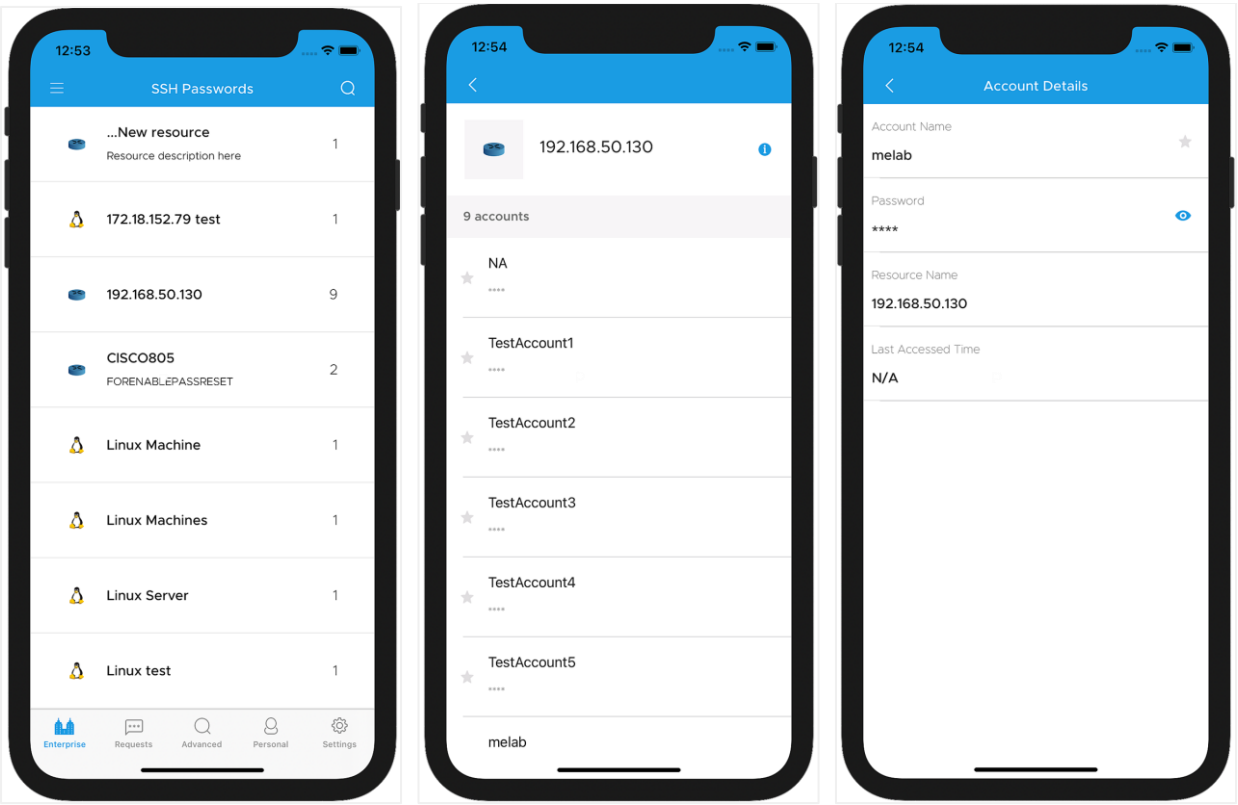
If your network contains a list of resources of various OS types, the Windows RDP Passwords option will help you to view only the list of Windows resources and their corresponding accounts. Tap on any resource/account name to view the resource/account details such as resource owner, resource URL, DNS name, resource type, passwords, resource name, account notes, and last accessed time. To view the password of a particular account, tap on the eye icon beside the password.





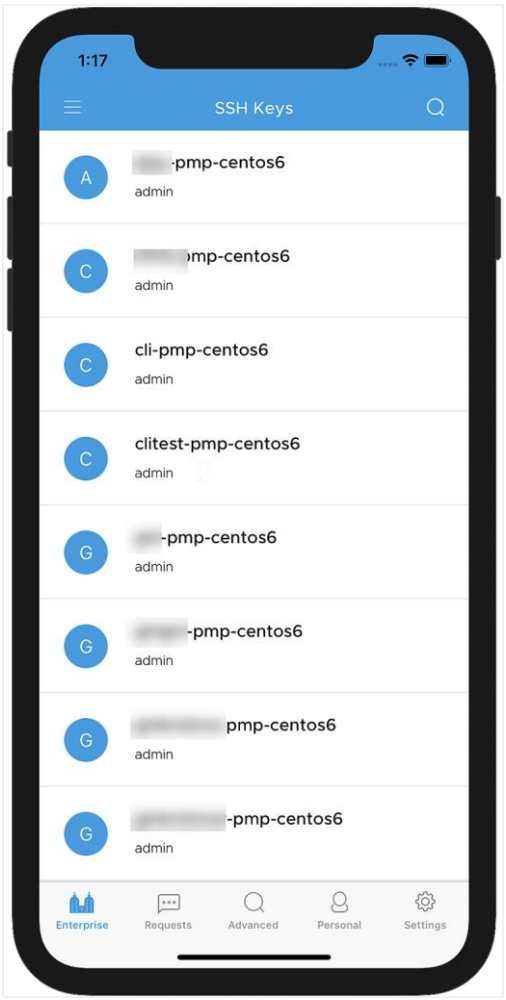
v. SSH Passwords

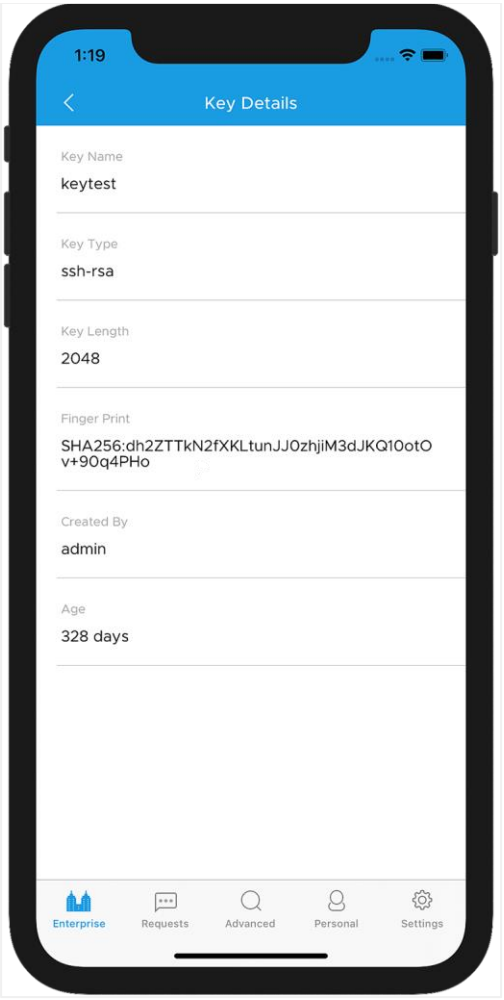
This option gives you a consolidated view of all the resources that you can access through an SSH connection. Tap on any resource on this list to view its user accounts. Tap on any account to view the account details, such as the masked password, last modified time, last accessed time, and password expiry date. Tap the Search icon to search for any account within the selected resource, using a search keyword.



vi. SSH Keys

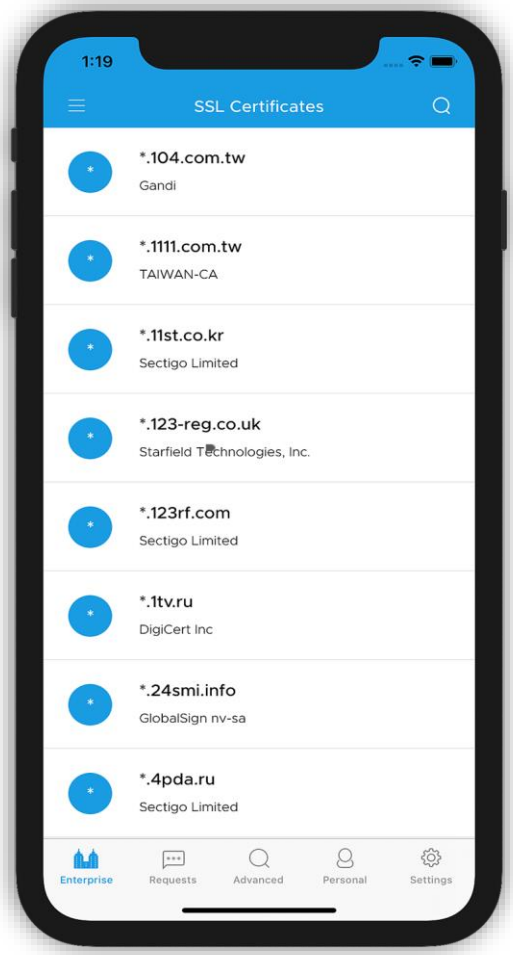
Tap the SSH Keys option from the Enterprise menu to view all the SSH keys that you are managing in the PAM360 repository. Tap any SSH key to view key details such as Key Type, Key Length, the key's Fingerprint, Username of the user who created the key, and Age of the key.





vii. SSL Certificates

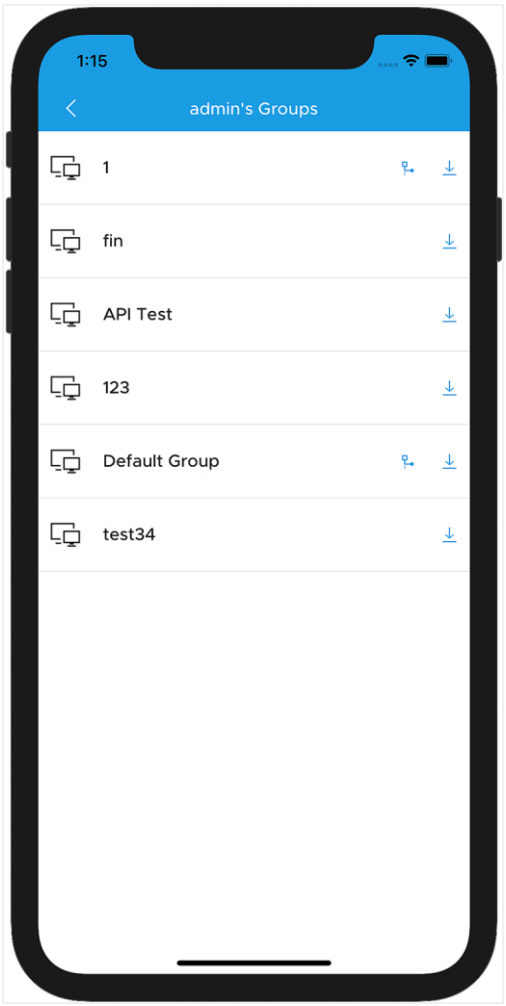
Tap the Certificates option from the Enterprise menu to view all the SSL certificates that you are managing in the PAM360 repository. Tap any SSL certificate from the list to view the following certificate details: Common Name, Port, Validity period, SAN, Issuer, Signature Algorithm, Finger Print, Serial Number, Key Algorithm, Key Size, Issuer.

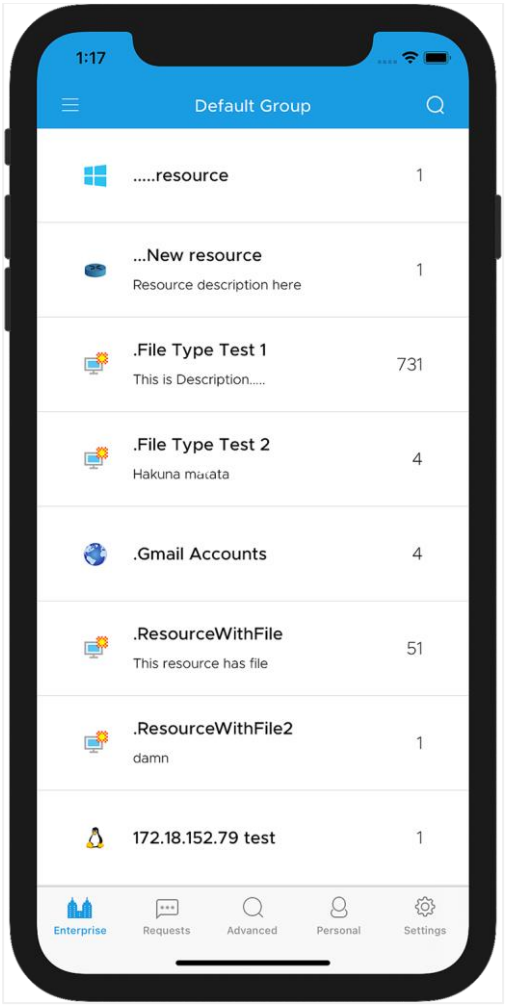


viii. Resource Groups

Administrators can create resource groups to combine similar resources for easier management. The grouping can be done either by specifying individual resources (Static group) or by specifying a set of criteria (Dynamic group). In the case of a dynamic or a criteria-based group, whenever a newly added resource matches the criteria of an existing group, PAM360 automatically adds the resource to this group. You can share the resource groups with other users or user groups. Users to whom the groups are shared can see the passwords of only the resources that are part of the shared group at that time.

Tap the Resource Groups option from the Enterprise Filter menu to view all the resource groups that are owned or managed by you. If a resource group has a subgroup, it will be indicated by a connection icon; to view the subgroups, simply tap the icon. If you wish to view the resources within a resource group, tap the name of the required resource group. Similarly, tap a resource name within the resource group to view the accounts that belong to the selected resource, and the account name to view the account details.



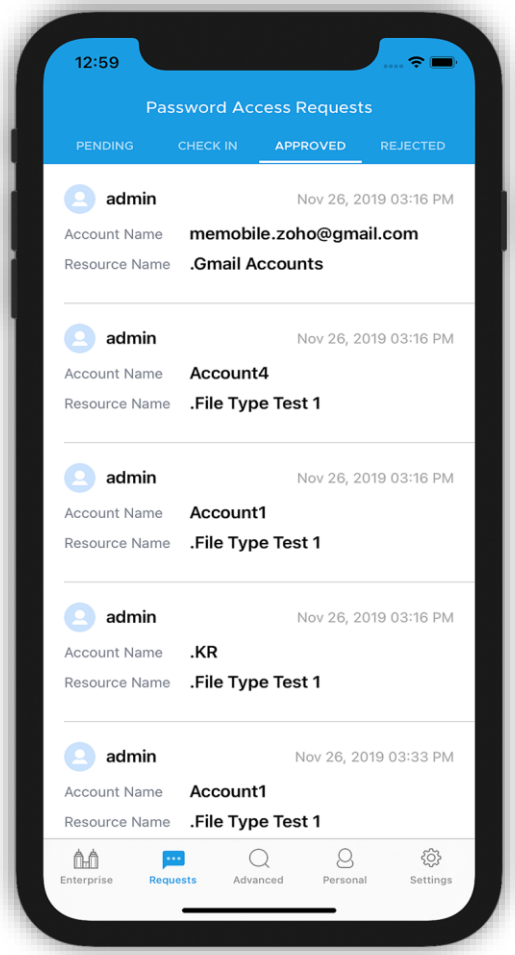


4.2 Requests

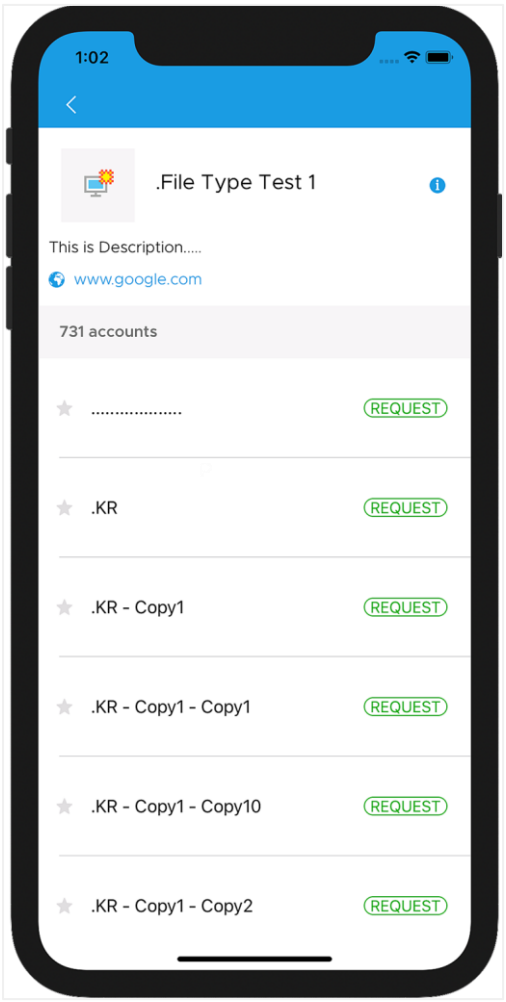
PAM360 provides an access control mechanism that allows administrators to grant password access to users for a specific period. Admins can start granting exclusive privileges once a password is ready to share, and only one user is allowed to use a particular password at a single point in time. Through PAM360's iOS application, administrators can view the list of pending password access requests from other users and act upon them.

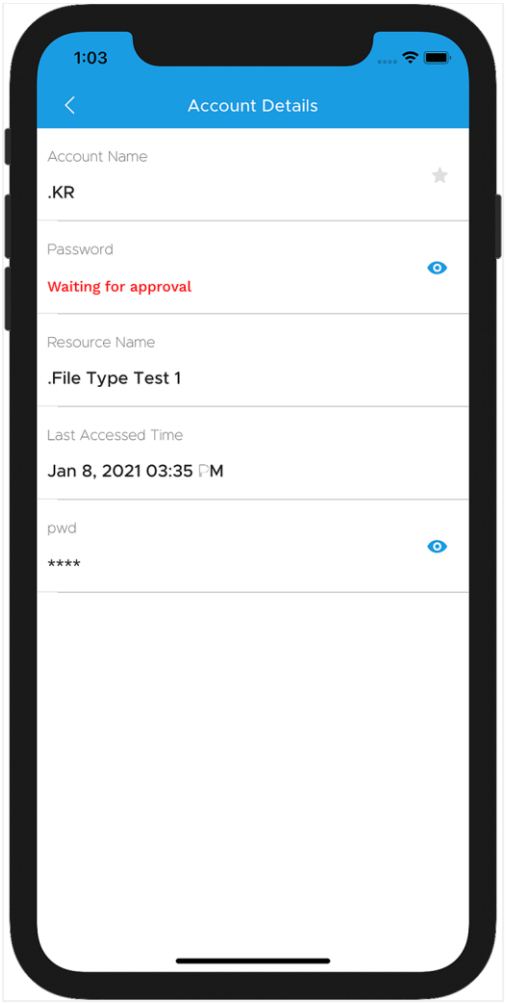
As an administrator, the **Password Access Requests** tab offers two sections:

1. **Pending** - to view the list of password access requests.
2. **Check-In** - to view the passwords that are currently in use and yet to be checked in.
3. **Approved** - to view the password requests that are approved by the administrators. This option includes details about the resource such as the resource name, account name, and date & time.
4. **Rejected** - to view the password requests that are rejected by the administrators. This option includes details about the resource such as the resource name, account name, and date & time.

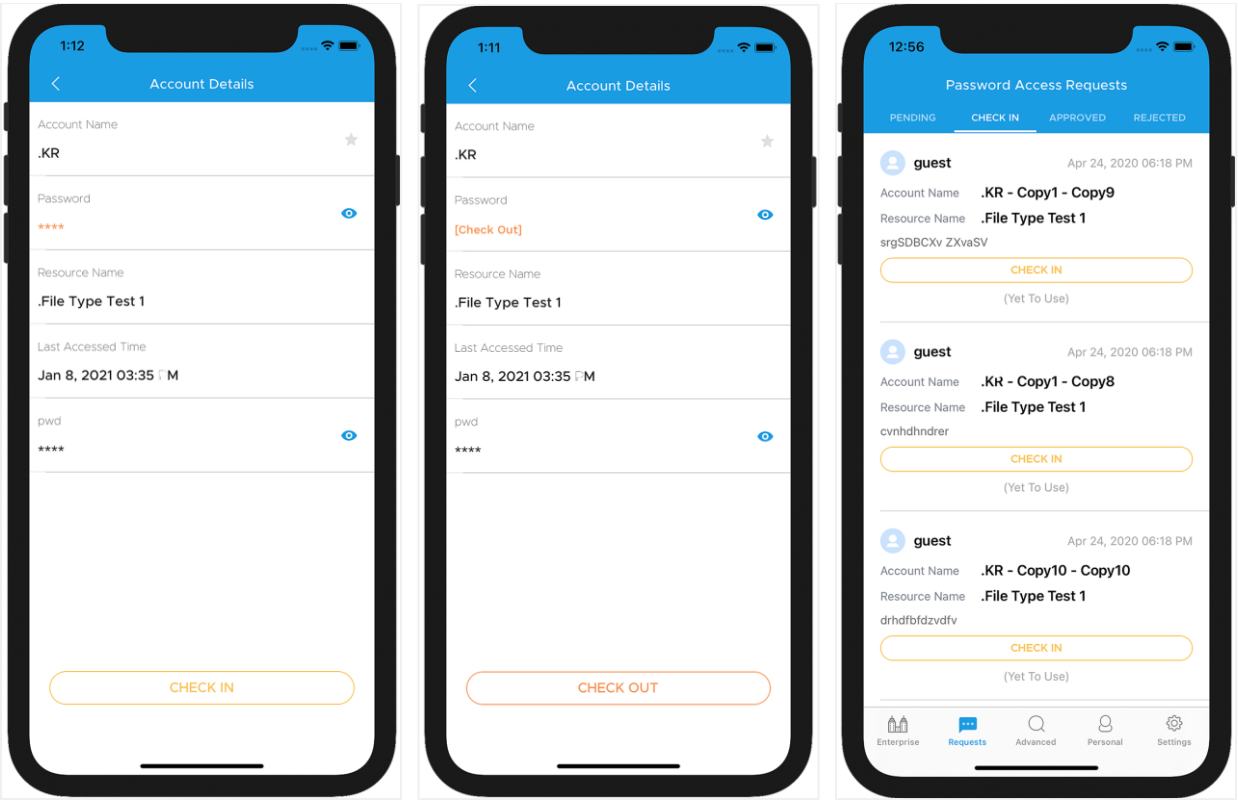


To send a password access request, tap an account, and tap the **Request** option in the account details section. Once your request has gone through, the status will change to **Waiting for Approval**.





Once an admin has approved your password request, you will be notified of the same, and the password will be available for **Check Out**. Once you check out the password for use, the status changes to **In Use**. Other users can see this status change in both the **Check-In** tab and the **Account Details** section of the particular account. To give up access to the password, tap the **Check-In** option. Now, the password is checked back into the PAM360 vault.

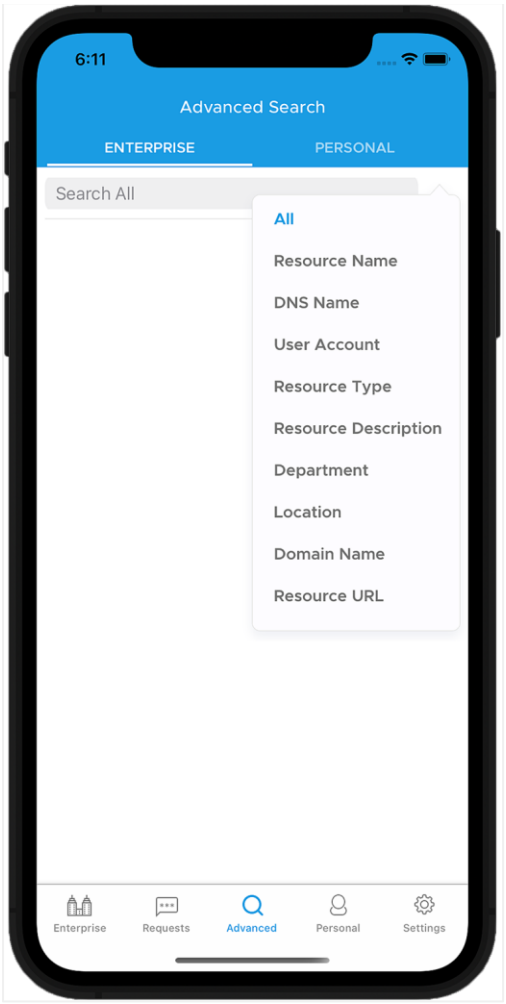


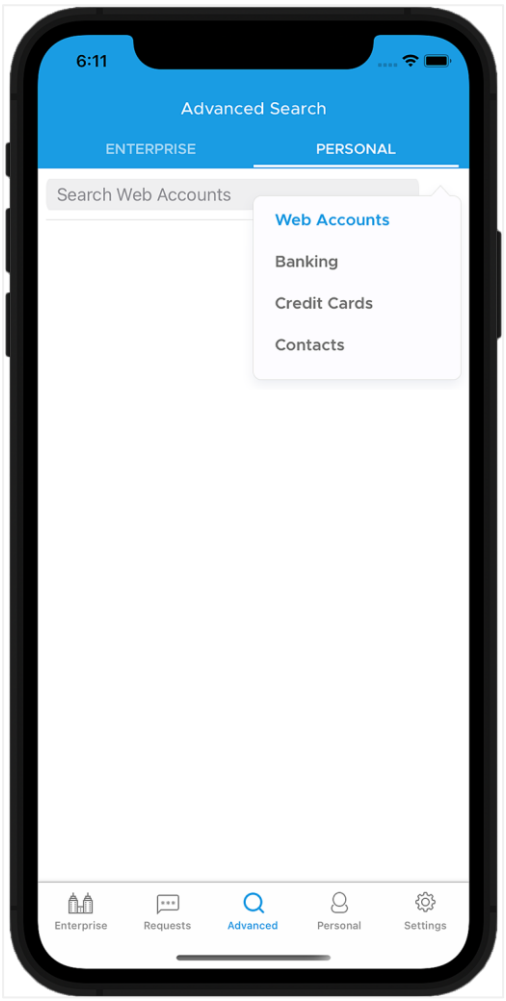
Once you check in the password and give up your access, you must go through the request-release workflow once again, if you should need access to it again. PAM360's iOS application also supports ticketing desk integration. Through the integration, PAM360 will prompt users to provide a ticket ID along with their request. Then, PAM360 will validate whether the ticket ID entered by the user exists in the ticketing system or not and only then grant access to the user to view the password.

4.3 Advanced

Advanced Search in PAM360's iOS application is a handy feature that can help you find any particular user or resource instantly. Tap **Advanced** from the navigation menu to either enter a keyword like **Name, Department, Location**, or use one of the many search filters available to tailor your search better. The Advanced Search section offers two separate tabs: Enterprise and Personal. In the Enterprise section, you can use search filters to tailor your search. The available search filters are **Resource Name, DNS Name, User Account, Resource Type, Resource Description, Department, Location, Domain Name**, and **Resource URL**. In the **Personal** section, the available search filters are **Web Accounts, Banking, Credit Cards,** and **Contacts**. In addition to these default search filters, if you have created any additional fields in PAM360's desktop installation, those custom column names will also appear as filters in the Advanced Search page. For example, the tab in PAM360 comes with an option to add **Tags** for the information you store. Use these tags as the keywords to search for data in the **Personal** section of the

Advanced Search page.





4.4 Personal

Apart from storing enterprise passwords, PAM360's iOS application allows you to store personal passwords in the PAM360 repository. The application provides four default categories: **Web Accounts, Banking, Credit Cards,** and **Contacts.** Among these categories, you can save your utmost personal data such as your personal email account information, credit card numbers, and other banking data, contact addresses, and phone numbers.

In addition to the default categories, add any number of additional custom fields to your **Personal** tab from the desktop application to store other information. For instance, if you wish to store details about the properties that you own, then add a custom category named **Properties**.

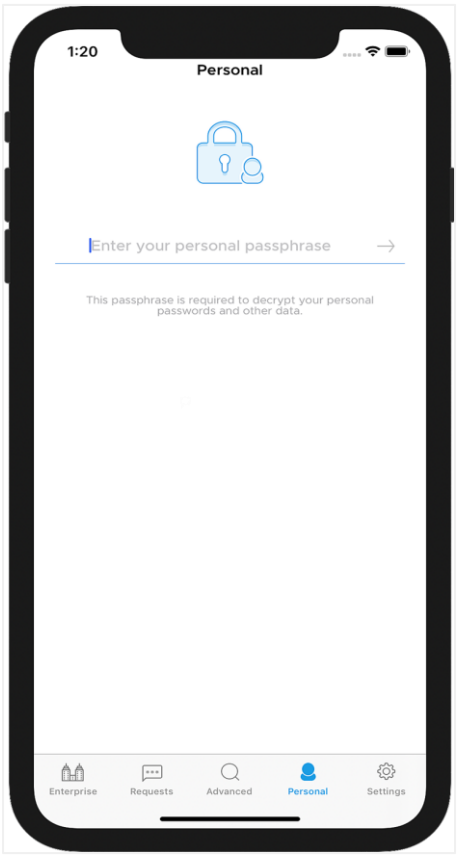
The application stores your personal data in a private repository that only you can access through the **Personal** tab. All information stored here is encrypted independently and hidden from all other users, including the administrator. While adding account details to the **Personal**

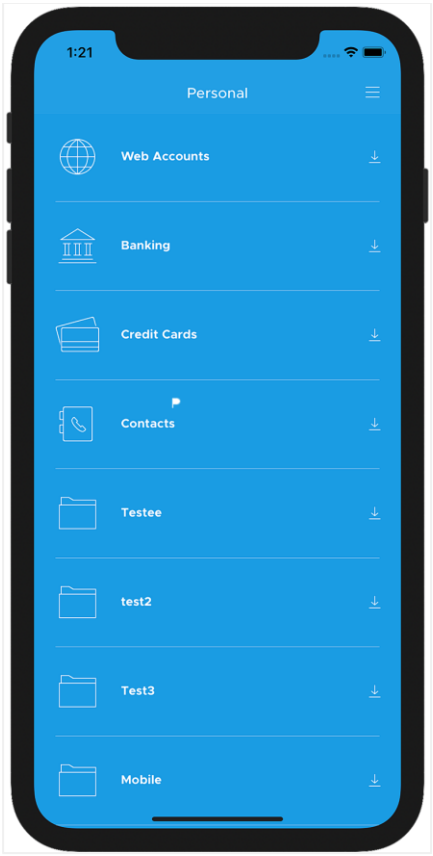
tab, there is an option to add **Tags**. Under this attribute, add keywords that can be used to search for the account under a particular category. Tap the Search icon and enter a keyword that was previously added as a tag to locate the account you are looking for.

4.4.1 Setting up a Personal Passphrase

To use the Personal tab in the application, you must set up a valid passphrase in PAM360's desktop installation and activate your Personal repository; do ensure the passphrase you provide matches the complexity rules enforced by your organization, if any. Once you set up your passphrase, you must enter it every time you need access to your personal passwords. Tap the refresh icon available at the top in case there is a change in the status of the personal passphrase. For example, if you try to login to your personal repository before setting up a passphrase, the application will not let you in. Once you create a passphrase in the desktop application, you can hit refresh in this page and login with your newly created passphrase right away, without moving out of the Personal tab.

> **Note:** Please note that if you forget or misplace the passphrase used for your Personal repository, you cannot reset the passphrase or retrieve your personal data without it.





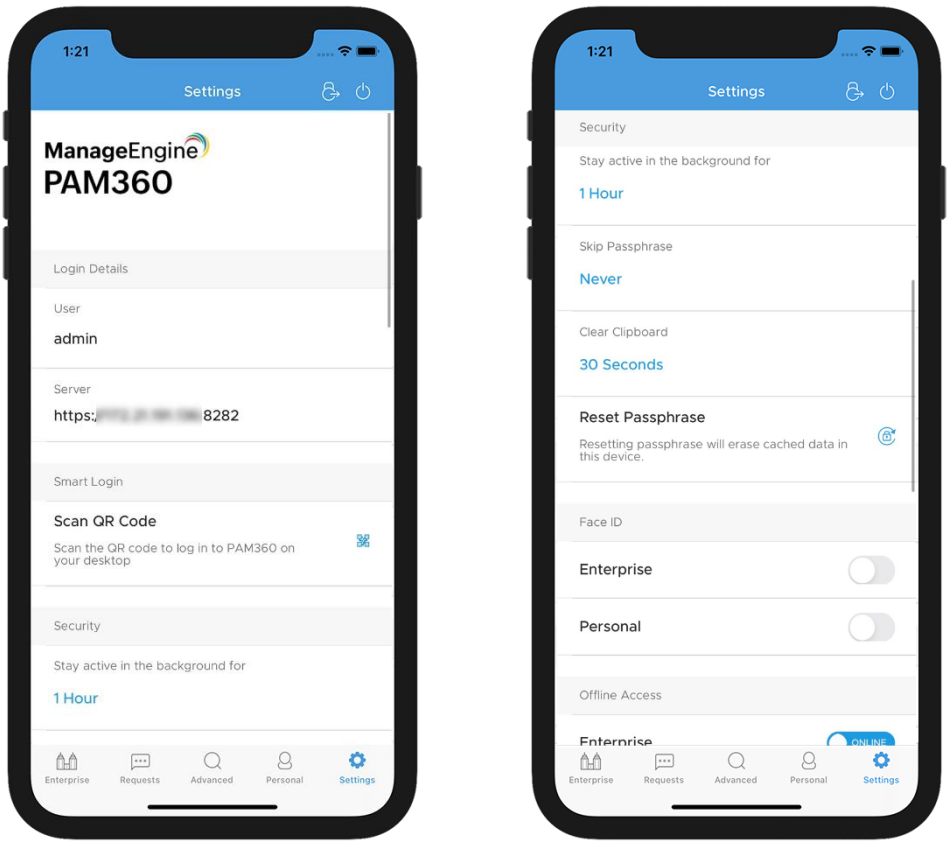
Alternatively, PAM360's iOS application provides the option to login to the **Personal** tab using your mobile device's Touch ID. Click here to learn how to enable Touch ID for the Personal tab.

4.4.2 Exiting the Personal Tab

To exit the **Personal** tab, tap the lock icon at the top right corner. You will return to the **All My Passwords** section and the **Personal** tab will be locked. To enter the Personal tab again, you must supply the passphrase again.

4.5 Settings

The Settings menu offers a comprehensive collection of options that are split categorically for ease of use. Use this menu to customize various security options, view login details, privacy policy of the iOS application, and more.



4.5.1 Login

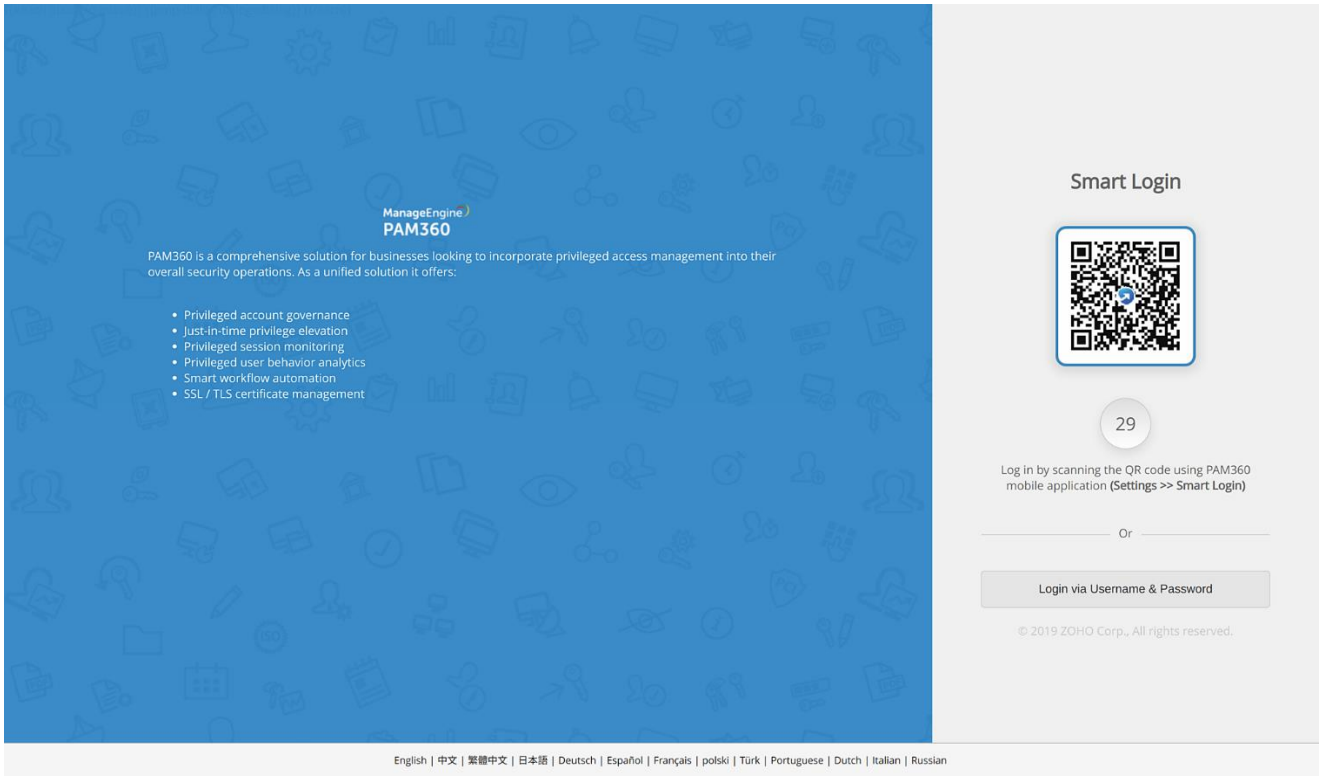
The **Login** section displays the **Username** and **Server** address to which PAM360 is currently connected. If the High Availability feature is turned on in your environment, then the iOS application will also display the secondary server details on the **Settings** page. If the primary server is down, you can connect it to the secondary server for uninterrupted service.

4.5.2 Smart Login

The **Smart Login** feature enables seamless access to the PAM360 web interface by simply scanning the QR code presented on the PAM360 webpage. This direct login approach streamlines the process, providing password less authentication and substantially minimizing the effort required for web login, all while maintaining robust security measures.

1. Head to the PAM360 login webpage and select the **Smart Sign-In** option.

2. Using the QR scanner available in the **Smart Login** section, scan the QR code displayed on the PAM360 web interface.



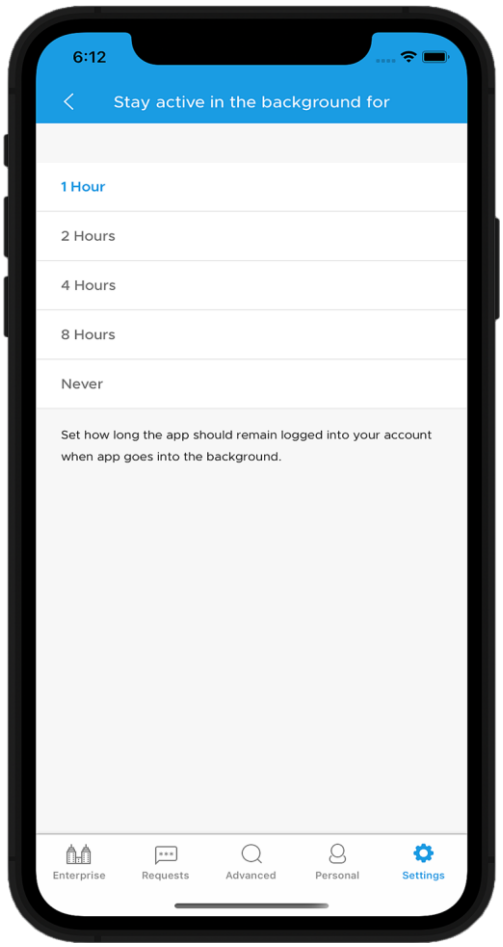
3. By doing so, you will be logged in to your PAM360 account.

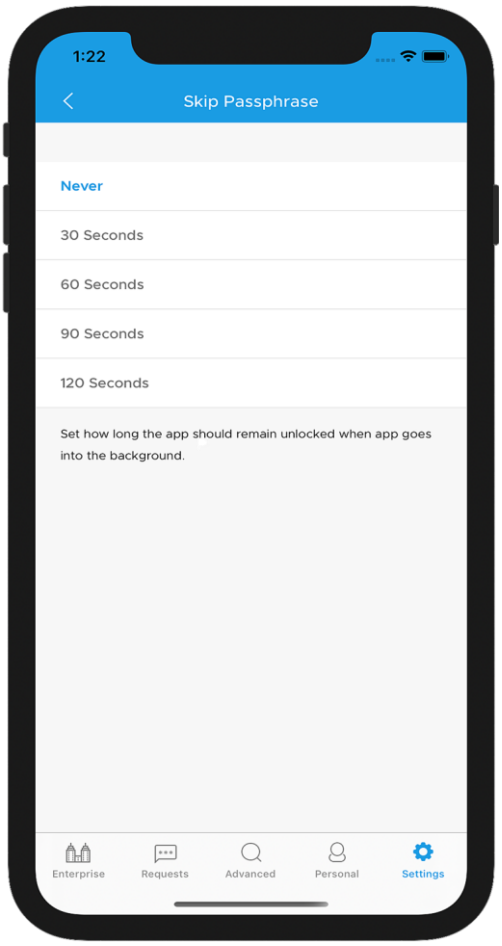
4.5.2 Security

The **Security** section has the following options:

i. Stay active in the background for

Set the duration for how long the application should remain logged in to your account when the application goes into the background. You can choose any one duration ranging from **1 to 8** hours. This option will allow you to stay logged into PAM360 when you need to switch between PAM360 and other applications multiple times. Alternatively, tap **Never** to log out as soon as the application goes into the background.



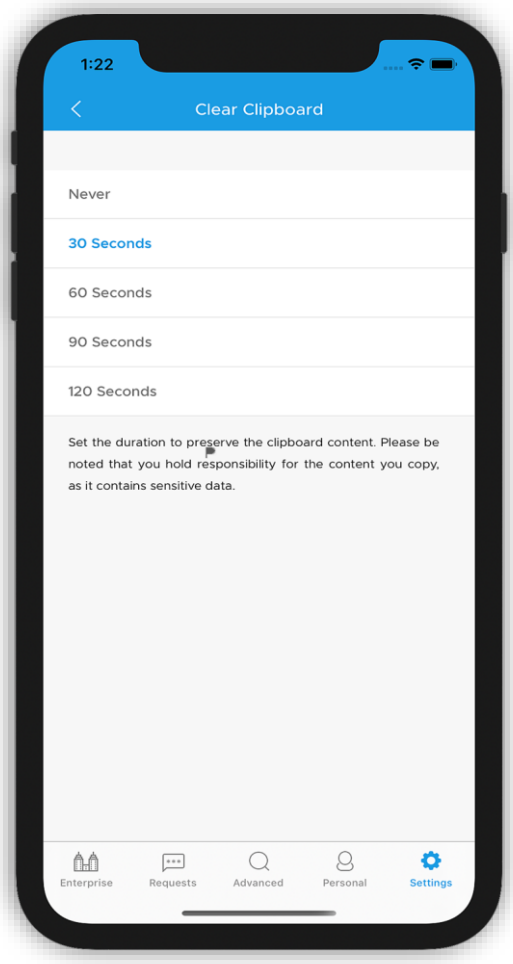


ii. Skip passphrase

If you leave the application, however briefly, without logging out, it will prompt you to enter your passphrase again to get back in. Set a duration for the application to not prompt for the passphrase while running in the background. You can choose any one duration ranging from **30 to 120 seconds**. Alternatively, tap **Never** to always prompt for a passphrase during login.

iii. Clear Clipboard

PAM360's iOS application can preserve any data you copy from within the application for a specified duration. To copy any password, tap the copy icon that is present beside the password. Tap the **Clear Clipboard** option to set a duration to preserve content you have copied to the clipboard. You can choose any one duration ranging from **30 to 120 seconds**. Alternatively, tap **Never** to never save any copied content in the clipboard.



iv. **Reset Passphrase**

Tap this option to erase all cached data saved in this device. Once reset, all offline passwords will be inaccessible and you will have to set up a new passphrase to reinstate access.

4.5.3 Touch ID

Use the toggle buttons to enable **Touch ID** support to access your Enterprise and Personal passwords. Enabling Touch ID will allow you to access your passwords without having to enter your passphrase every time. However, please note that, if you enable this option, your login credentials will be stored in your device's keychain.

4.5.4 Offline Access

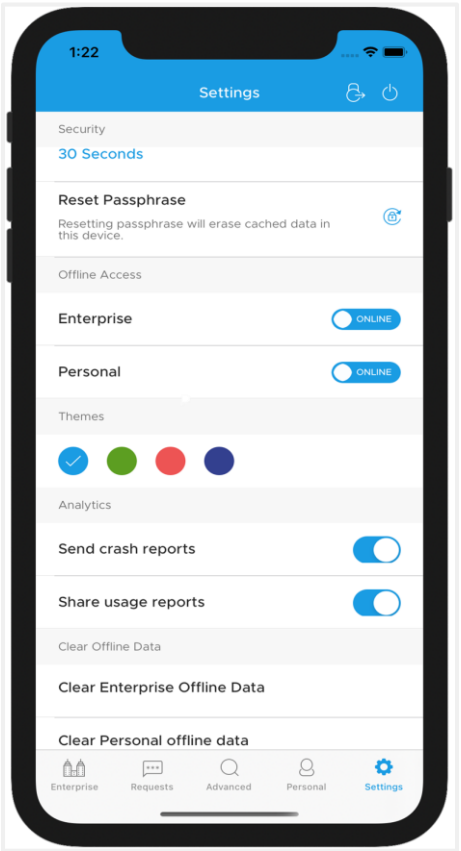
The toggle buttons beside **Enterprise** and **Personal** indicate whether the PAM360 application is currently in online or offline mode. PAM360's iOS application offers a secure offline mode that allows you to access passwords even when you do not have access to the internet. To access passwords in the offline mode, download the required passwords first; only the passwords which are downloaded before going offline would be available for access in the offline mode. Apart from downloading individual passwords, the application allows you to download a

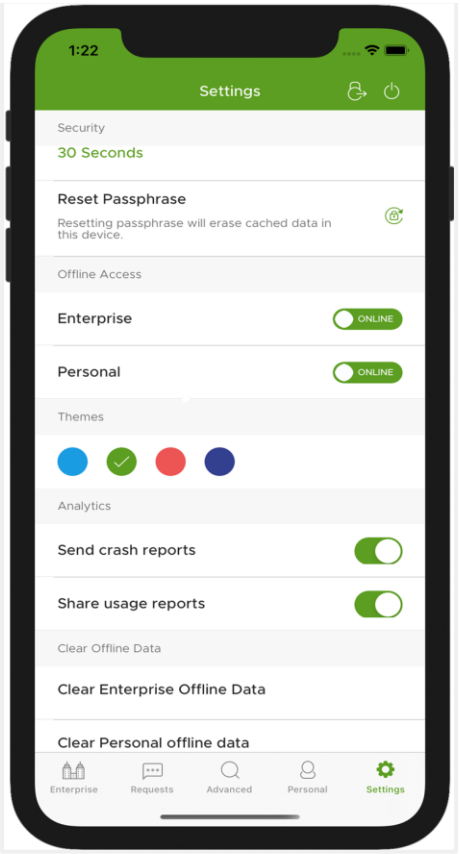
group of passwords from the **Enterprise** menu, such as the **Favorites, Recents, Windows RDP Passwords,** and **SSH Passwords.** Additionally, you can download resource groups and personal passwords. To download passwords for offline access, go to the Enterprise menu, and click the downward arrow beside the required list of passwords.

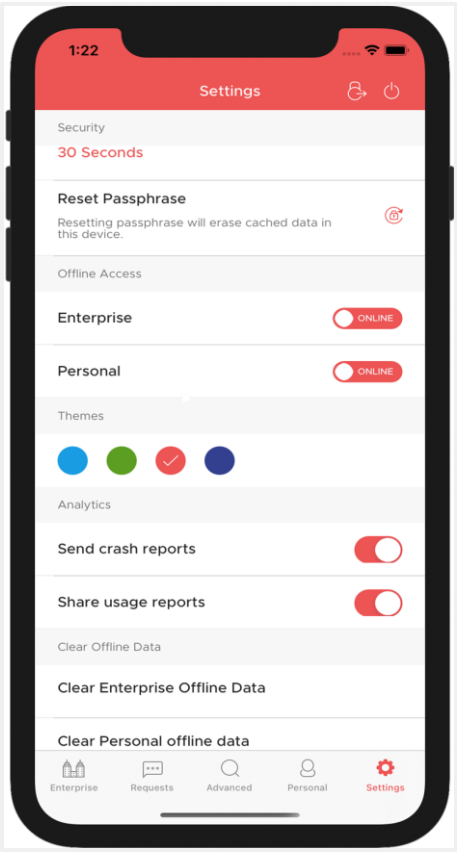
> **Note: Offline** mode will work only if the **Allow password caching for offline access via mobile** option is enabled in **General Settings**.

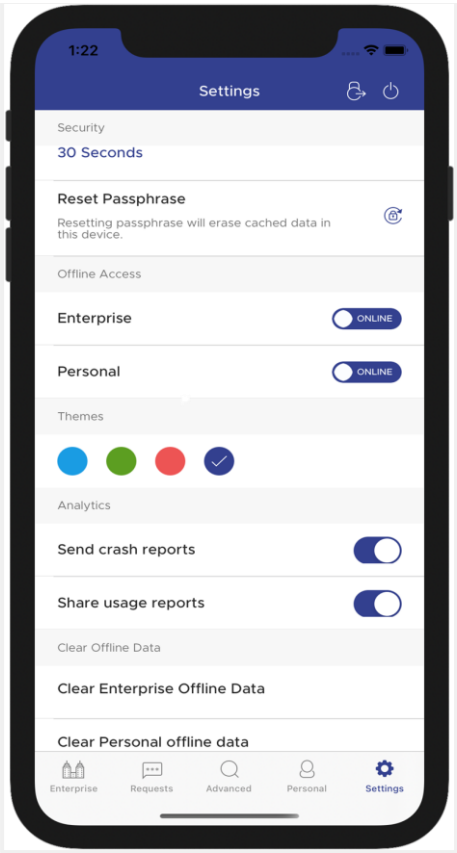
4.5.5 Themes

Using this option, change the background color of your application. As of now, there are four colors to choose from: Blue, Green, Red, and Dark Blue.



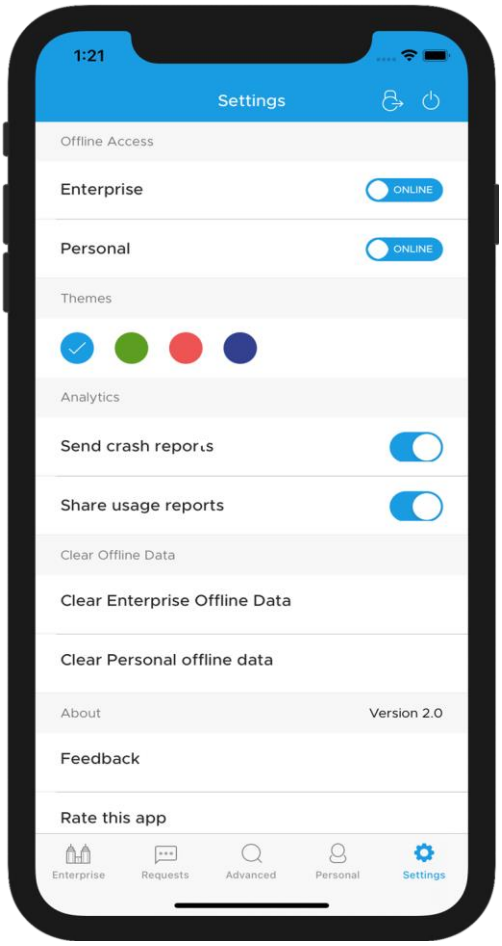






4.5.6 Analytics

Apart from the above options, you can choose to share **Usage Statistics** or **Crash Reports** to ManageEngine by using toggle buttons under Analytics. Usage statistics data gives an insight into usability data such as what features of the application you use more, how frequently, etc. This type of data is used as research to learn user behavior, gather pain points, if any, and enhance the application's performance and user experience based on the data. Crash reports are detailed system logs that capture the state of the application when the crash happens. Collecting and analyzing this data will help us learn what caused the application to crash and rectify it in the next version.



4.5.7 Clear Offline Data

Under this, you will find two options:

Clear Enterprise Offline Data - Tap this option to clear all offline cache. This action will delete all your enterprise passwords that are saved offline.

Clear Personal Offline Data - Tap this option to clear all personal offline cache. This action will delete all your personal passwords that are saved offline.

4.5.8 About

Feedback - This option allows you to leave feedback regarding the functionality of the application anonymously.

Rate This App - This option redirects you to the App Store where you can leave a rating for the application.

Take a Tour - This option offers you a brief and concise tour of the main functionalities of the application.

In addition to the above, you can read PAM360's **Privacy Policy** and **Acknowledgments** in this section.

5. Uninstalling the Mobile Application

To uninstall the mobile application, follow the below steps:

1. Locate the ManageEngine PAM360 application on your device, long press the icon, and click **Uninstall**.
2. Tap **Ok** in the confirmation pop-up.

Now, the PAM360 mobile application is successfully uninstalled. Once you uninstall the application, all PAM360-related data is removed from the device.

Technical Support	
If you face any issue with the mobile application, get in touch with our technical support team. **Toll free number**: +1-888-720-9500 **Email ID**: pam360-support@manageengine.com	
Download PAM360 iPhone app Available on the App Store	Download PAM360 Android app ANDROID APP ON Google play

Chrome Browser Extension

To make password management and auto-logon activities seamless, PAM360 provides the option to securely synchronize your privileged accounts and passwords across browsers through native browser extensions.

The extensions help you perform privileged access management operations such as sending and approving password requests, auto-filling passwords to websites, web applications, and also set up an Auto Logon gateway to launch RDP and SSH sessions. The extensions allow you to view all the passwords, resource groups, favorites, recently used resources and also enable you to search for resources.

The browser extensions, once deployed, allow you to directly perform most of the privileged access management activities, with PAM360 running in the background.

Apart from the Chrome browser extension, the other available extensions are:

- Firefox
- Edge

This document explains you in detail about the Chrome browser extension. Below is a detailed explanation of the steps to install the extension, the settings required, and how it helps in managing the privileged resources:

1. Benefits
2. Steps to Install the Extension
3. Supported Operations
4. Settings

1. Benefits

The Chrome browser extension provides certain advantages such as:

1. Automatic login to websites and applications from the browser without the need to access the PAM360 web interface.
2. Exclusive icons for auto-logon and copy username/password to simplify operations.
3. **Resource Description** icon () to display more information about a resource. Click the resource name to list all the associated accounts.
4. Central Search bar to search for resources based on the criteria, such as resource name, DNS name, etc., specified at the time of resource creation.

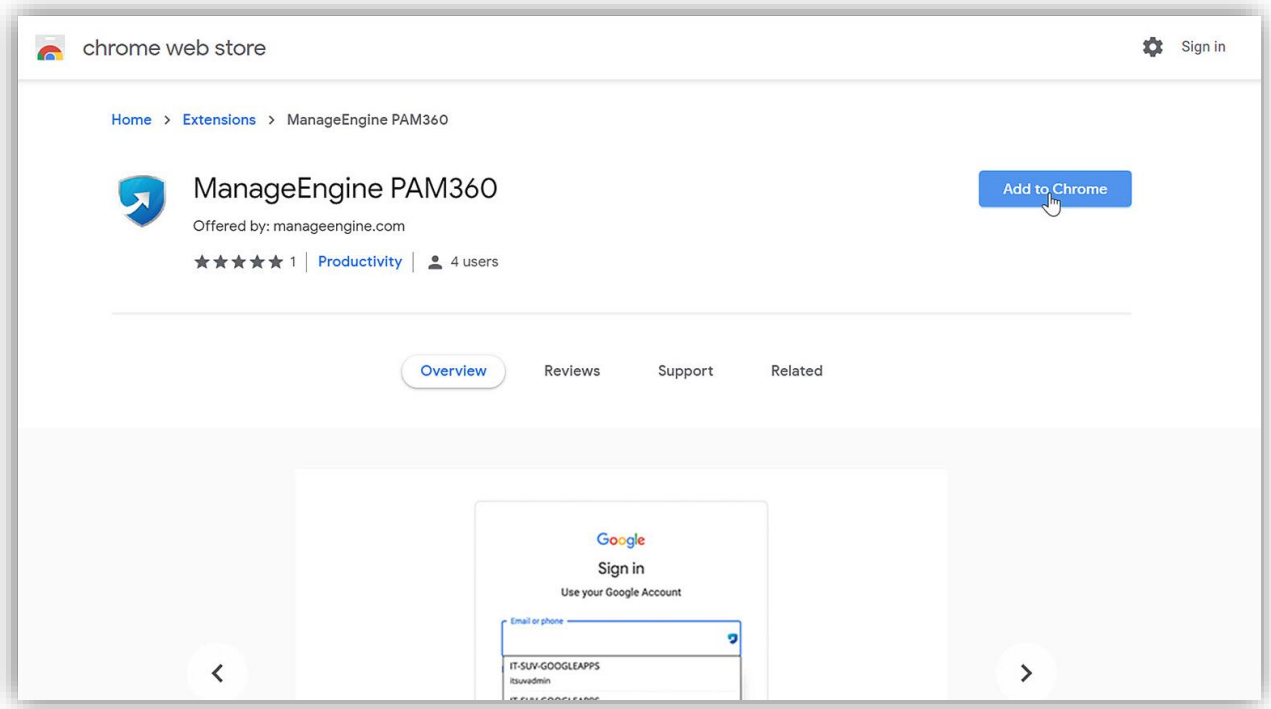
2. Steps to Install the Extension

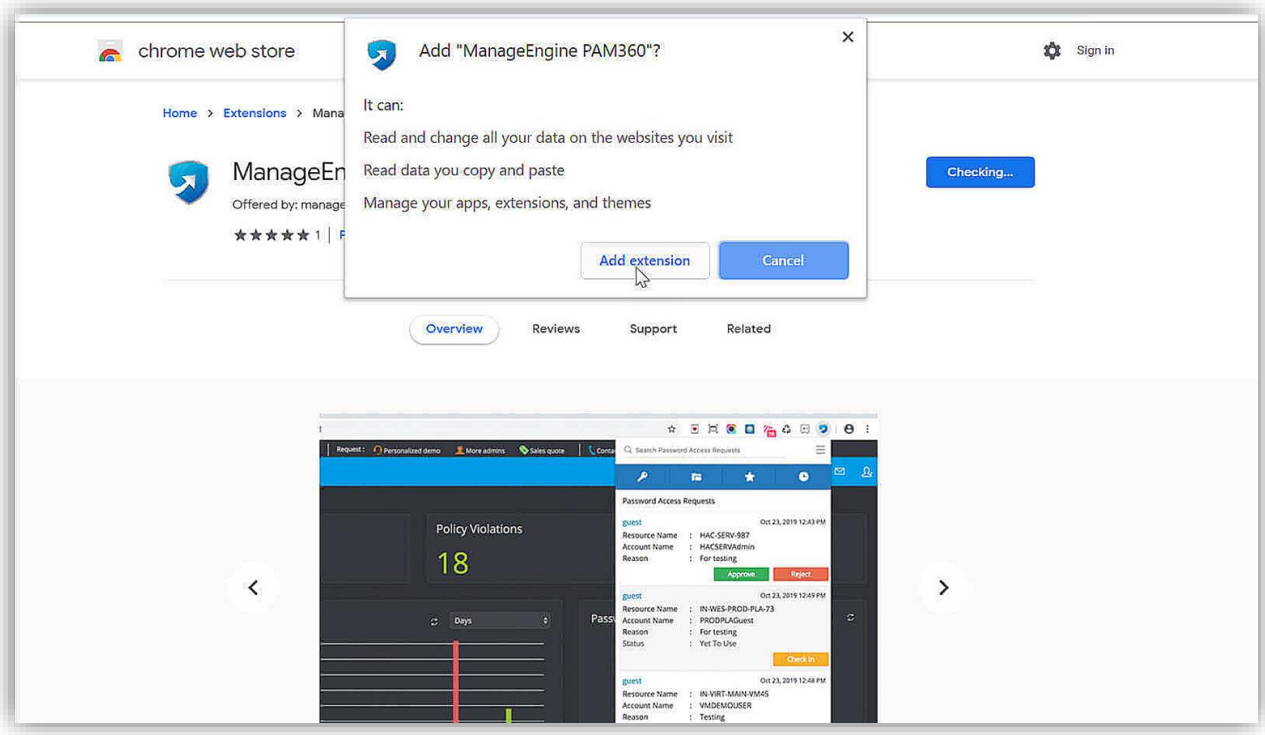
1. There are two ways to download the browser extension for Chrome:

   i. Go to PAM360 download page. Scroll down and click the **Chrome** icon under **Browser Extensions.** It will redirect you to the **Chrome web store.**

   ii. Directly access the Chrome web store link from Chrome browser.

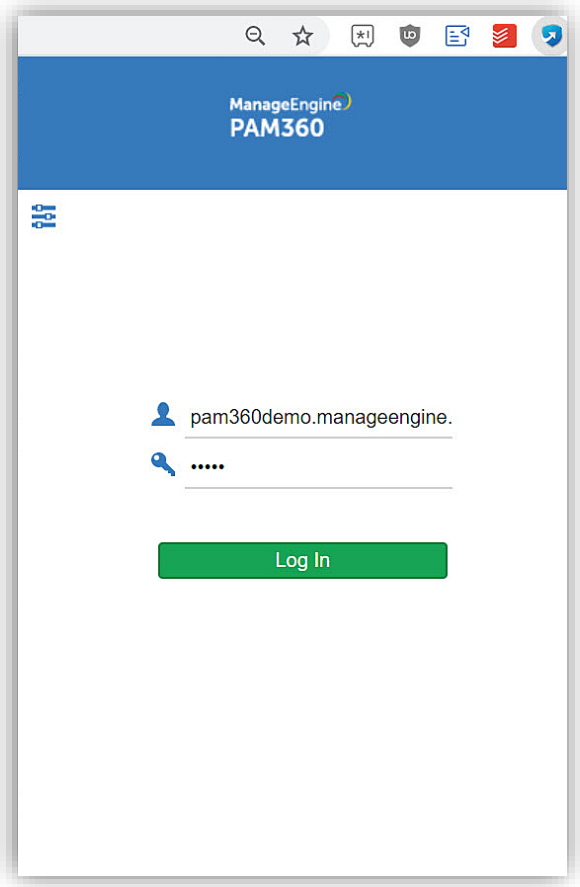
2. Click the **Add to Chrome** button and click **Add Extension** in the confirmation pop-up that appears.

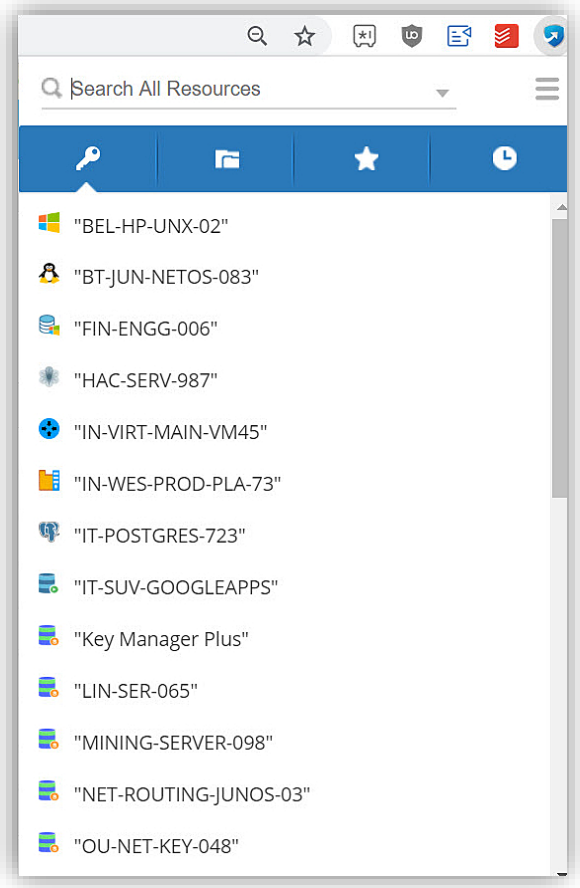


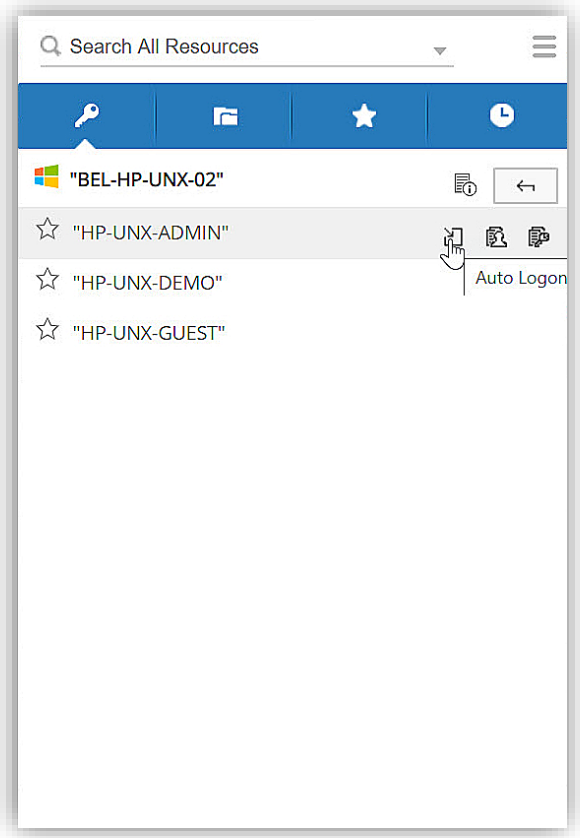


3. After installation, PAM360 icon will appear in the address bar of the browser. Click the icon and enter the **Host** where PAM360 is running and specify the connection **Port**.
4. Enter your login credentials. The browser extension supports all types of login (**Local/AD/LDAP/RADIUS)** and authentication mechanisms as available in the web interface.

Now, the PAM360 extension is added to Chrome successfully.


ManageEngine
PAM360
pam360demo.manageengine.
Log In


Search All Resources
"BEL-HP-UNX-02"
"BT-JUN-NETOS-083"
"FIN-ENGG-006"
"HAC-SERV-987"
"IN-VIRT-MAIN-VM45"
"IN-WES-PROD-PLA-73"
"IT-POSTGRES-723"
"IT-SUV-GOOGLEAPPS"
"Key Manager Plus"
"LIN-SER-065"
"MINING-SERVER-098"
"NET-ROUTING-JUNOS-03"
"OU-NET-KEY-048"



3. Supported Operations

3.1 View Passwords

To view the list of all passwords, click the **All Passwords** tab in the browser extension. To view passwords specific to a resource group, click the **Resource Groups** tab. Here, the browser extension will maintain the same tree structure of resource groups and corresponding accounts as shown in the PAM360 web interface. You can view the password of any account associated with that particular resource group from the **Resource Groups** tab.

3.2 Search All Resources

Search for resources directly from the search bar in the browser extension based on any criteria such as resource name, user name, DNS name, user account, resource type, resource description, department, location, domain name, all resources or additional custom fields.

3.3 Automatic Launch of RDP and SSH Sessions

Click the auto logon icon to launch a direct connection to websites or Windows/Linux resources.

- For Linux resources, choose either **SSH** or **Telnet**.
- For Windows resources, choose either **Windows Remote Desktop** or **RDP Console Session**.
- For websites, the URL will open directly.

3.4 Username and Password Autofill on a Website or Application

To autofill credentials on a website/application, the credentials must already be stored in PAM360. When you attempt to login to a website, click the PAM360 extension icon that appears beside the credentials field and choose an account. The corresponding username and password will be auto-filled after which you can manually hit enter and login to the website.

> **Important Note:**
>
> PAM360 Browser extensions are designed to securely retrieve the stored credentials from the PAM360 vault and auto-fill the form in target webpages/websites. This feature allows users to automatically log into websites and web applications without entering the credentials manually.
>
> Please note that this feature is primarily for convenience and is not a fool-proof system as the credentials are submitted in the client-side browser. Therefore, make sure if you have enforced the necessary security measures in the client-side browser and the user systems.

3.5 Favorites

This option provides quick access to the list of all your frequently used passwords that you marked as favorites in PAM360. This helps you locate resources and corresponding passwords easily. To mark any password as a favorite in the **All Passwords,** click the star icon beside it.

3.6 Recently Used

Click the **Recently Used** tab in the browser extension to find the list of all recently accessed passwords.

3.7 Copy Username or Password

Click the Copy Username or Password options to copy the credentials to the clipboard for pasting them elsewhere as required.

3.8 File Download

You can download the digital files, certificates and documents stored under a FileStore

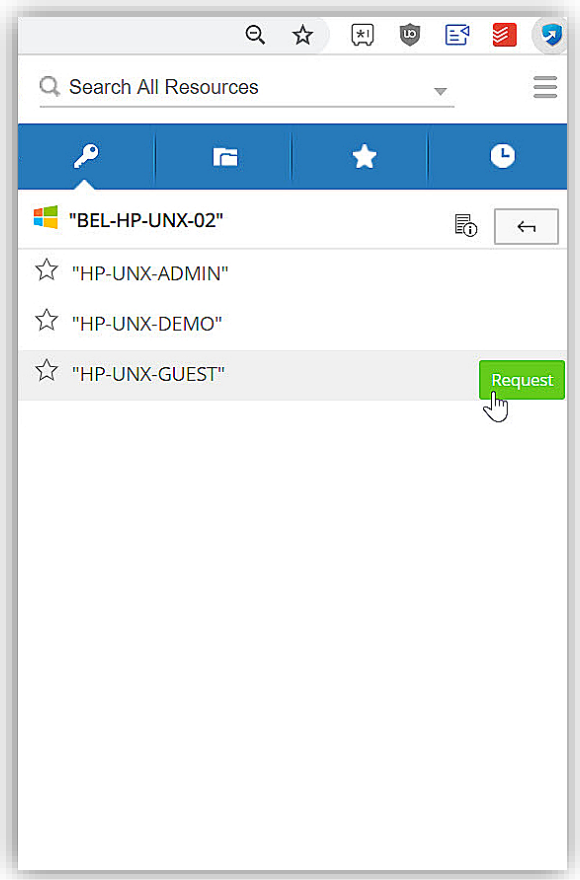
resource type, directly from the extension.

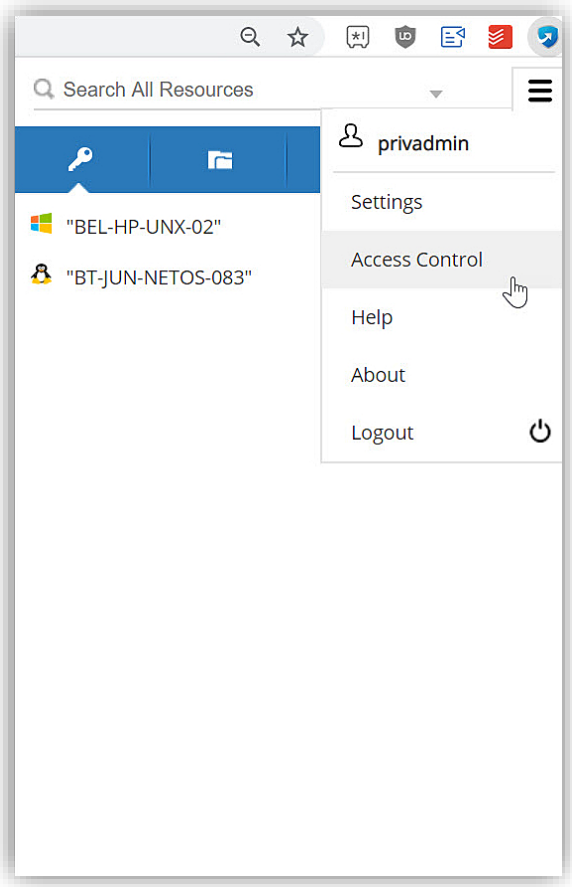
3.9 Password Access Request/Release

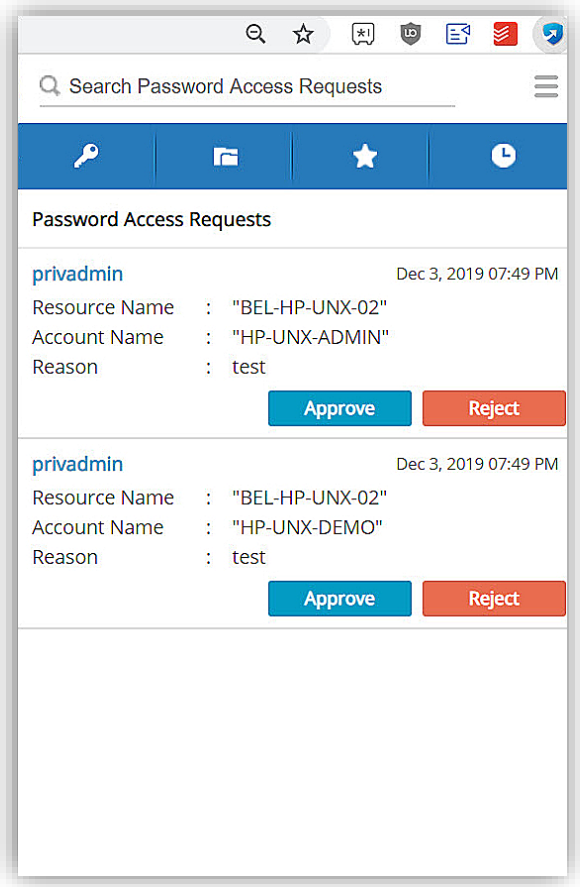
If you have configured password access control workflow in your web interface, the same will be applied to the browser extension. The administrators can either approve or reject password requests from the browser extension menu. Once a password request is approved, you can perform password check-in and check-out operations also from the extension.

Notes:

- If you have enabled Ticketing System Integration or the reason for retrieving the passwords setting in your PAM360 web interface, the browser extension will also prompt you to enter the ticket id or reason for access whenever you try to retrieve the password.
- The access control mechanism in the browser extension works the same way as in the web interface.




Search All Resources
privadmin
Settings
Access Control
Help
About
Logout
"BEL-HP-UNX-02"
"BT-JUN-NETOS-083"



4. Settings

4.1 Clear Clipboard

Specify a time period in seconds to choose how long the copied data should remain in the clipboard. Enter '0' as the value to never clear the clipboard.

4.2 Automatically Logout After

Specify a time period in minutes to choose how long the session should remain logged in. Enter '0' as the value to never logout of a session in the browser extension. The automatic logout time specified for the web interface and the extension are independent of each other. However, you can apply the same automatic logout time given for the web interface to the browser extension as well. Follow the below steps to do so:

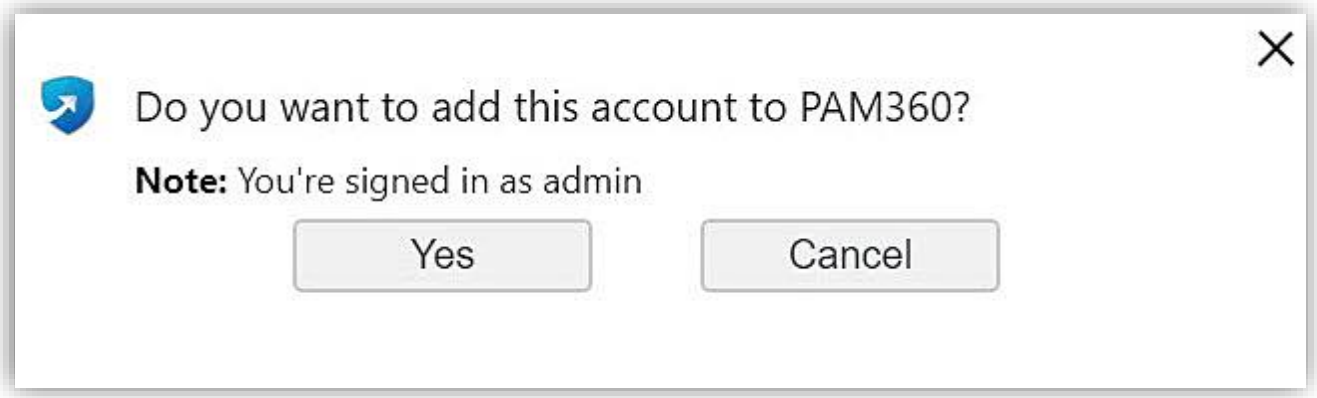
1. Go to PAM360's web interface. Navigate to **Admin >> Settings >> General Settings** and click **User Management** from the left pane.
2. Specify a value for automatic logout in the option **Automatically log off users for X minutes** and select the checkbox **Enforce this as a maximum time limit also for users logged in through browser extension.**

4.3 Prevent Browser from Prompting to Save Passwords

Select this option to prevent the browser from prompting to save passwords during any login. Once you select the option, click **Allow** in the pop-up that opens to confirm your permission to prevent the browser from prompting further.

4.4 Prevent Extension from Prompting to Add Accounts

Select this option to prevent the browser extension from prompting to save passwords during any login. However, if this option is unchecked, PAM360 will prompt to add your account when you try to login to a website. The account details will be saved as an enterprise account in PAM360 web interface.

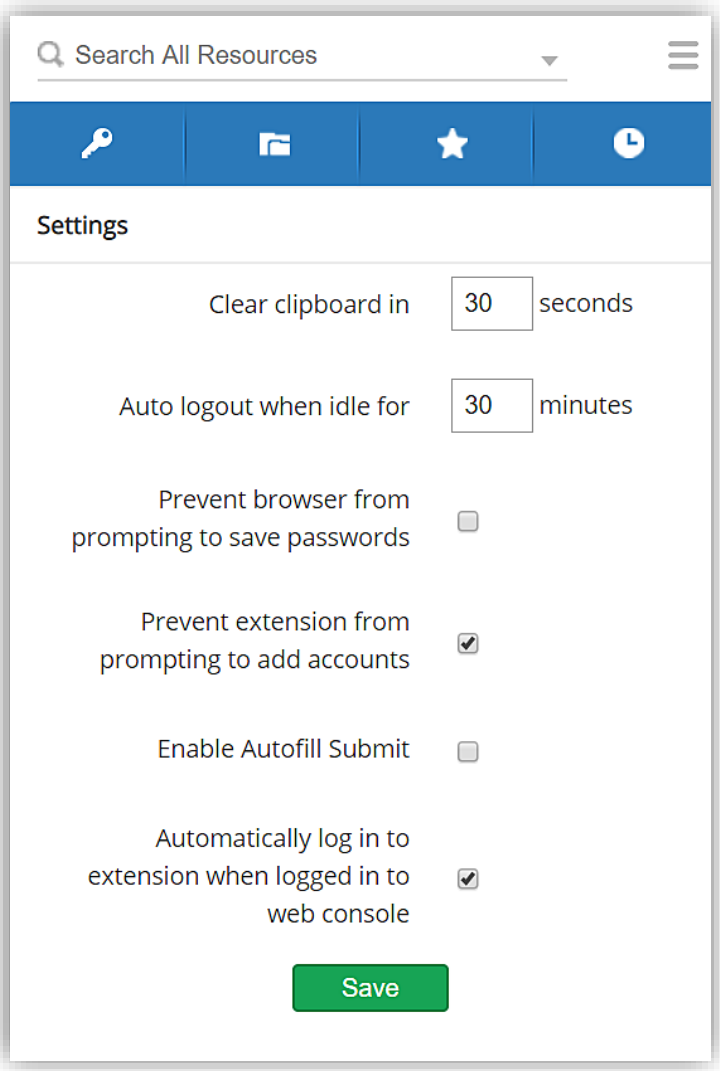


4.5 Enable Autofill Submit

Select this option to enable the browser extension to auto-fill the credentials and submit them during login.

4.6 Automatically Log in to Extension When Logged in to Web Interface

Select this option to enable concurrent login to the browser extension when you are logged into the PAM360 web interface.


Search All Resources
Settings
Clear clipboard in
30
seconds
Auto logout when idle for
30
minutes
Prevent browser from prompting to save passwords
Prevent extension from prompting to add accounts
Enable Autofill Submit
Automatically log in to extension when logged in to web console
Save

Firefox Browser Extension

To make password management and auto-logon activities seamless, PAM360 provides the option to securely synchronize your privileged accounts and passwords across browsers through native browser extensions.

The extensions help you perform privileged access management operations such as sending and approving password requests, auto-filling passwords to websites, web applications, and also set up an Auto Logon gateway to launch RDP and SSH sessions. The extensions allow you to view all the passwords, resource groups, favorites, recently used resources and also enable you to search for resources.

The browser extensions, once deployed, allow you to directly perform most of the privileged access management activities, with PAM360 running in the background.

Apart from the Firefox browser extension, the other available extensions are:

- Chrome
- Edge

This document explains you in detail about the Firefox browser extension. Below is a detailed explanation of the steps to install the extension, the settings required, and how it helps in managing the privileged resources:

1. Benefits
2. Steps to Install the Extension
3. Supported Operations
4. Settings

1. Benefits

The Firefox browser extension provides certain advantages such as:

1. Automatic login to websites and applications from the browser without the need to access the PAM360 web interface.
2. Exclusive icons for auto-logon and copy username/password to simplify operations.
3. **Resource Description** icon ( ) to display more information about a resource. Click the resource name to list all the associated accounts.
4. Central Search bar to search for resources based on the criteria, such as resource name, DNS name, etc., specified at the time of resource creation.

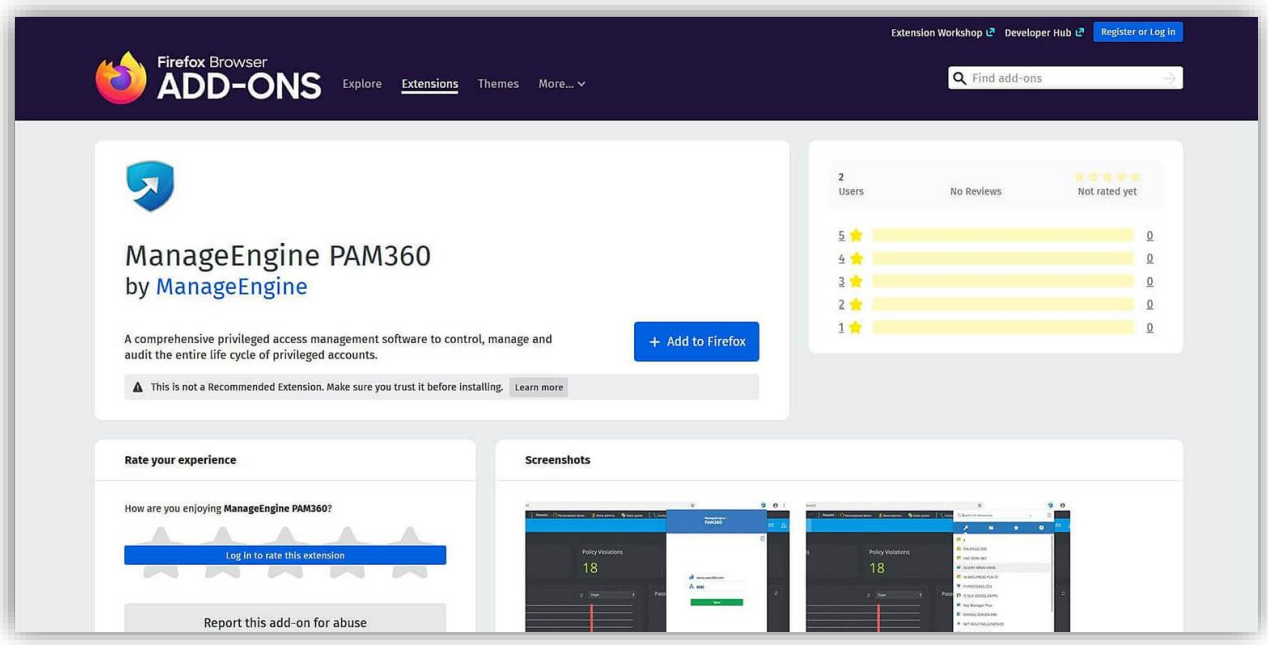
2. Steps to Install the Extension

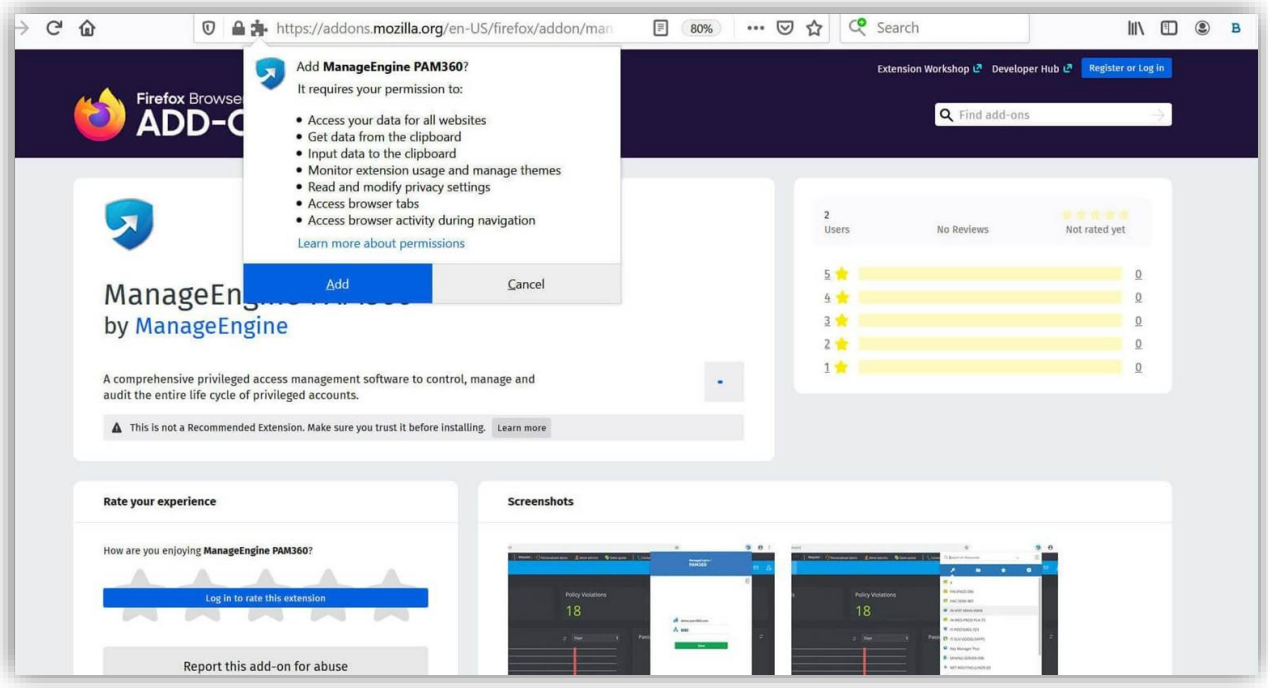
1. There are two ways to download the browser extension for Firefox:

   i. Go to PAM360's download page. Scroll down and click the **Firefox** icon under **Browser Extensions.** It will redirect you to the **Firefox Add-ons page.**

   ii. Go to the Firefox add-ons page from Firefox browser.

2. Click the **Add to Firefox** button and click **Add** in the confirmation pop-up that appears.



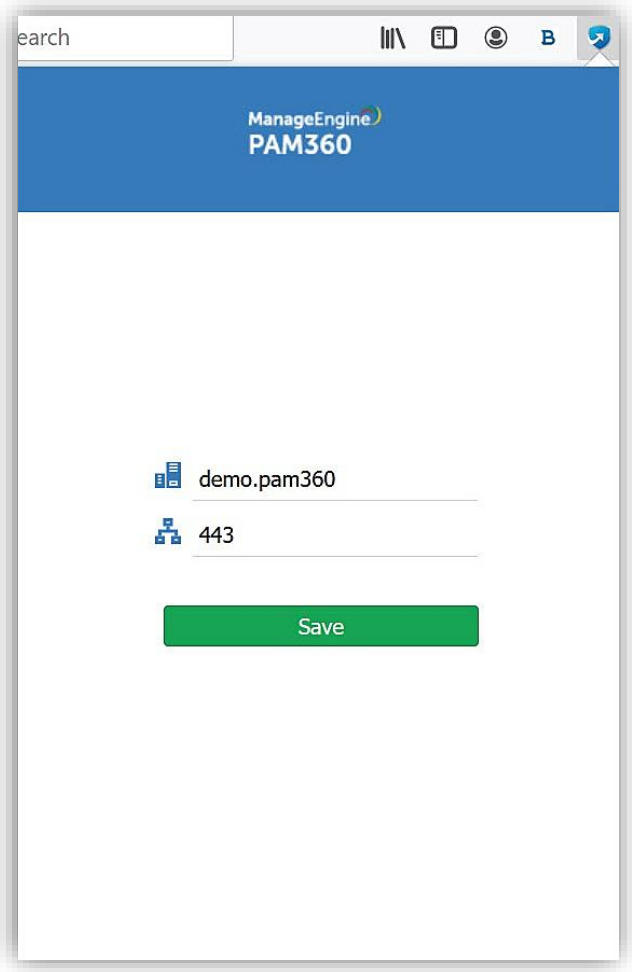


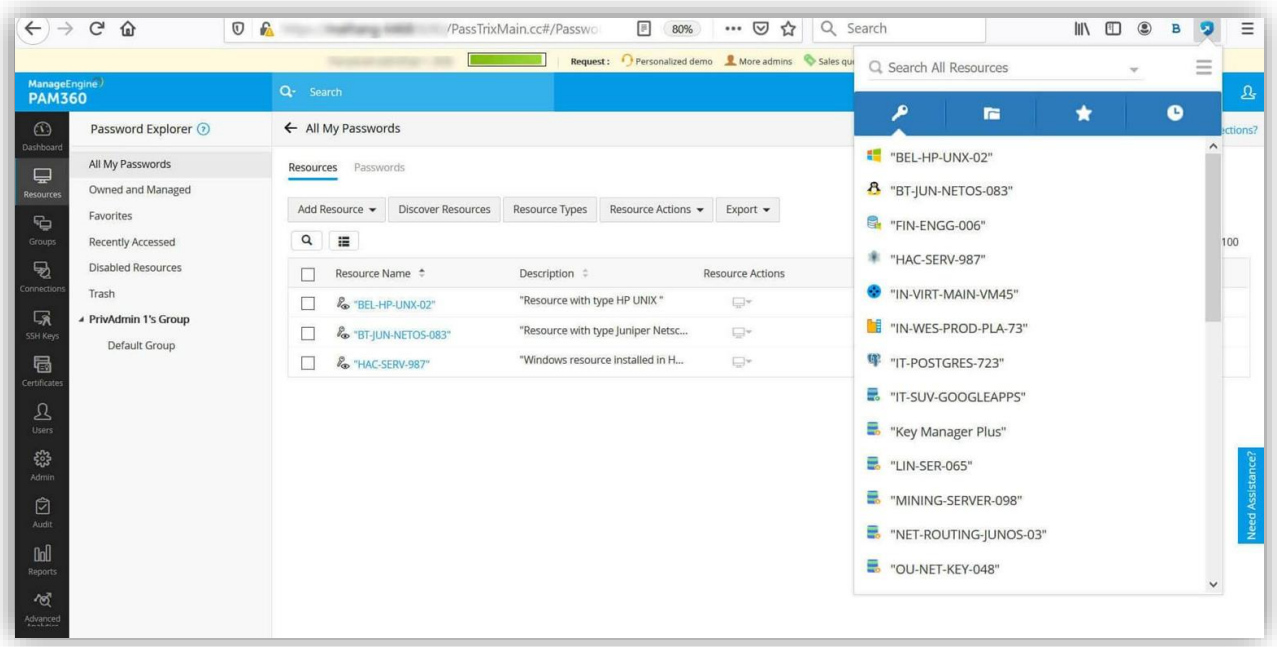
3. After installation, PAM360 icon will appear in the address bar of the browser. Click the

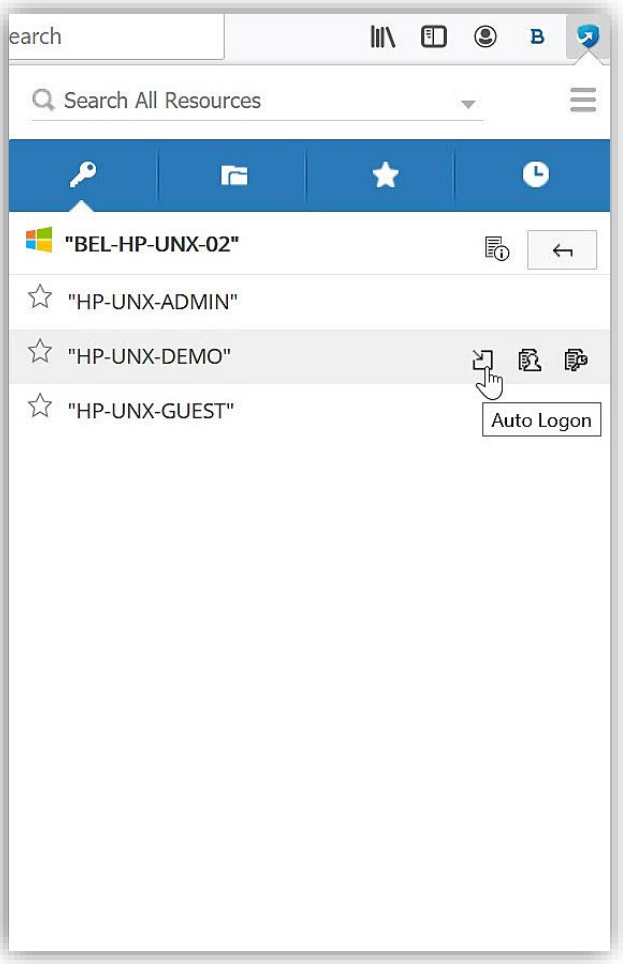
icon and enter the **Host** where PAM360 is running and specify the connection **Port**.

4. Enter your login credentials. The browser extension supports all types of login (**Local/AD/LDAP/RADIUS)** and authentication mechanisms as available in the web interface.

Now, the browser extension is ready to use.







3. Supported Operations

3.1 View Passwords

To view the list of all passwords, click the **All Passwords** tab in the browser extension. To view passwords specific to a resource group, click the **Resource Groups** tab. Here, the browser extension will maintain the same tree structure of resource groups and corresponding accounts as shown in the PAM360 web interface. You can view the password of any account associated with that particular resource group from the **Resource Groups** tab.

3.2 Search All Resources

Search for resources directly from the search bar in the browser extension based on any criteria such as resource name, user name, DNS name, user account, resource type, resource description, department, location, domain name, all resources or additional custom fields.

3.3 Automatic Launch of RDP and SSH Sessions

Click the auto logon icon to launch a direct connection to websites or Windows/Linux resources.

- For Linux resources, choose either **SSH** or **Telnet**.
- For Windows resources, choose either **Windows Remote Desktop** or **RDP Console Session**.
- For websites, the URL will open directly.

3.4 Username and Password Autofill on a Website or Application

To autofill credentials on a website/application, the credentials must already be stored in PAM360. When you attempt to login to a website, click the PAM360 extension icon that appears beside the credentials field and choose an account. The corresponding username and password will be auto-filled after which you can manually hit enter and login to the website.

Important Note:

PAM360 Browser extensions are designed to securely retrieve the stored credentials from the PAM360 vault and auto-fill the form in target webpages/websites. This feature allows users to automatically log into websites and web applications without entering the credentials manually.

Please note that this feature is primarily for convenience and is not a fool-proof system as the credentials are submitted in the client-side browser. Therefore, make sure if you have enforced the necessary security measures in the client-side browser and the user systems.

3.5 Favorites

This option provides quick access to the list of all your frequently used passwords that you marked as favorites in PAM360. This helps you locate resources and corresponding passwords easily. To mark any password as a favorite in the **All Passwords,** click the star icon beside it.

3.6 Recently Used

Click the **Recently Used** tab in the browser extension to find the list of all recently accessed passwords.

3.7 Copy Username or Password

Click the Copy Username or Password options to copy the credentials to the clipboard for pasting them elsewhere as required.

3.8 File Download

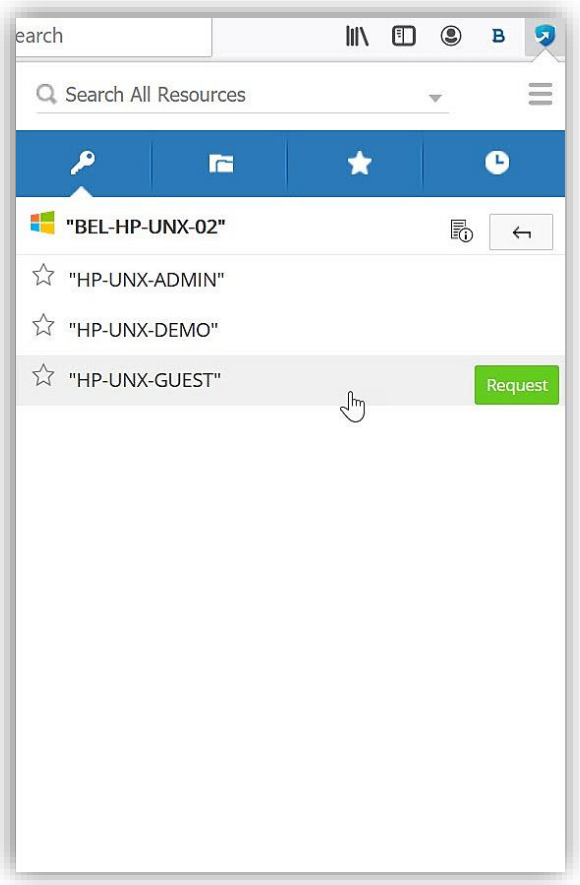
You can download the digital files, certificates and documents stored under a FileStore resource type, directly from the extension.

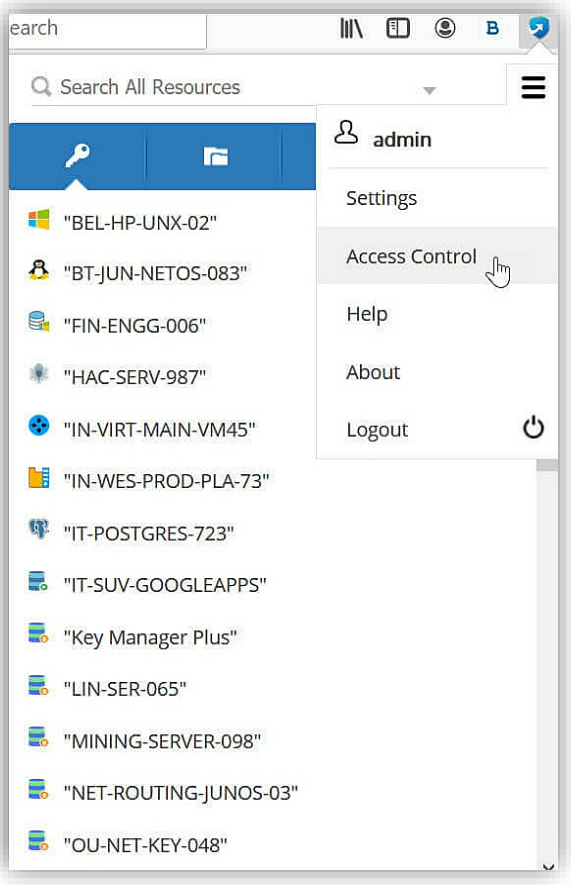
3.9 Password Access Request/Release

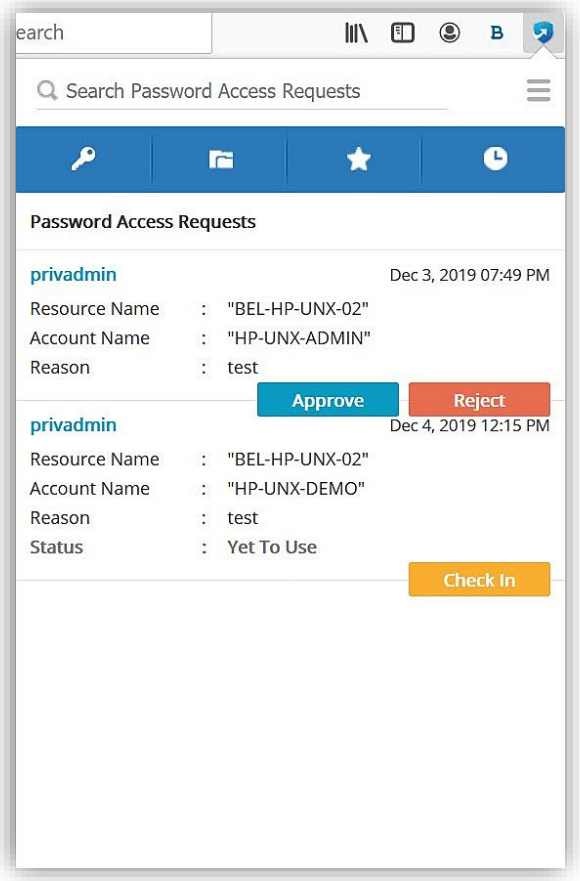
If you have configured password access control workflow in your web interface, the same will be applied to the browser extension. The administrators can either approve or reject password requests from the browser extension menu. Once a password request is approved, you can perform password check-in and check-out operations also from the extension.

Notes:

- If you have enabled Ticketing System Integration or the reason for retrieving the passwords setting in your PAM360 web interface, the browser extension will also prompt you to enter the ticket id or reason for access whenever you try to retrieve the password.
- The access control mechanism in the browser extension works the same way as in the web interface.


earch
Search All Resources
"BEL-HP-UNX-02"
"HP-UNX-ADMIN"
"HP-UNX-DEMO"
"HP-UNX-GUEST"
Request


earch
Search All Resources
admin
Settings
Access Control
Help
About
Logout
"BEL-HP-UNX-02"
"BT-JUN-NETOS-083"
"FIN-ENGG-006"
"HAC-SERV-987"
"IN-VIRT-MAIN-VM45"
"IN-WES-PROD-PLA-73"
"IT-POSTGRES-723"
"IT-SUV-GOOGLEAPPS"
"Key Manager Plus"
"LIN-SER-065"
"MINING-SERVER-098"
"NET-ROUTING-JUNOS-03"
"OU-NET-KEY-048"


earch
Search Password Access Requests
Password Access Requests
privadmin
Dec 3, 2019 07:49 PM
Resource Name : "BEL-HP-UNX-02"
Account Name : "HP-UNX-ADMIN"
Reason : test
Approve
Reject
privadmin
Dec 4, 2019 12:15 PM
Resource Name : "BEL-HP-UNX-02"
Account Name : "HP-UNX-DEMO"
Reason : test
Status : Yet To Use
Check In

4. Settings

4.1 Clear Clipboard

Specify a time period in seconds to choose how long the copied data should remain in the clipboard. Enter '0' as the value to never clear the clipboard.

4.2 Automatically Logout After

Specify a time period in minutes to choose how long the session should remain logged in. Enter '0' as the value to never logout of a session in the browser extension. The automatic logout time specified for the web interface and the extension are independent of each other. However, you can apply the same automatic logout time given for the web interface to the browser extension as well. Follow the below steps to do so:

1. Go to PAM360's web interface. Navigate to **Admin >> Settings >> General Settings** and click **User Management** from the left pane.
2. Specify a value for automatic logout in the option **Automatically log off users for X minutes** and select the checkbox **Enforce this as a maximum time limit also for users logged in through browser extension.**

4.3 Prevent Browser from Prompting to Save Passwords

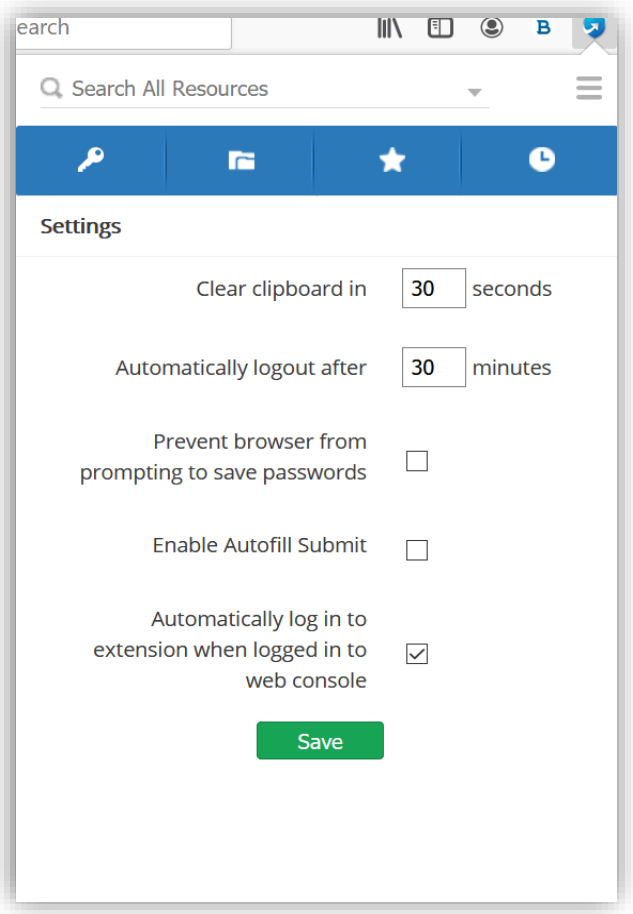
Select this option to prevent the browser from prompting to save passwords during any login. Once you select the option, click **Allow** in the pop-up that opens to confirm your permission to prevent the browser from prompting further.

4.4 Enable Autofill Submit

Select this option to enable the browser extension to auto-fill the credentials and submit them during login.

4.5 Automatically Log in to Extension When Logged in to Web Interface

Select this option to enable concurrent login to the browser extension when you are logged into the PAM360 web interface.


earch
Search All Resources
Settings
Clear clipboard in
30
seconds
Automatically logout after
30
minutes
Prevent browser from prompting to save passwords
Enable Autofill Submit
Automatically log in to extension when logged in to web console
Save

Edge Browser Extension

To make password management and auto-logon activities seamless, PAM360 provides the option to securely synchronize your privileged accounts and passwords across browsers through native browser extensions.

The extensions help you perform privileged access management operations such as sending and approving password requests, auto-filling passwords to websites, web applications, and also set up an Auto Logon gateway to launch RDP and SSH sessions. The extensions allow you to view all the passwords, resource groups, favorites, recently used resources and also enable you to search for resources.

The browser extensions, once deployed, allow you to directly perform most of the privileged access management activities, with PAM360 running in the background.

Apart from the Edge browser extension, the other available extensions are:

- Chrome
- Firefox

This document explains you in detail about the Edge browser extension. Below is a detailed explanation of the steps to install the extension, the settings required, and how it helps in managing the privileged resources:

1. **Benefits**
2. **Steps to Install the Extension**
3. **Supported Operations**
4. **Settings**

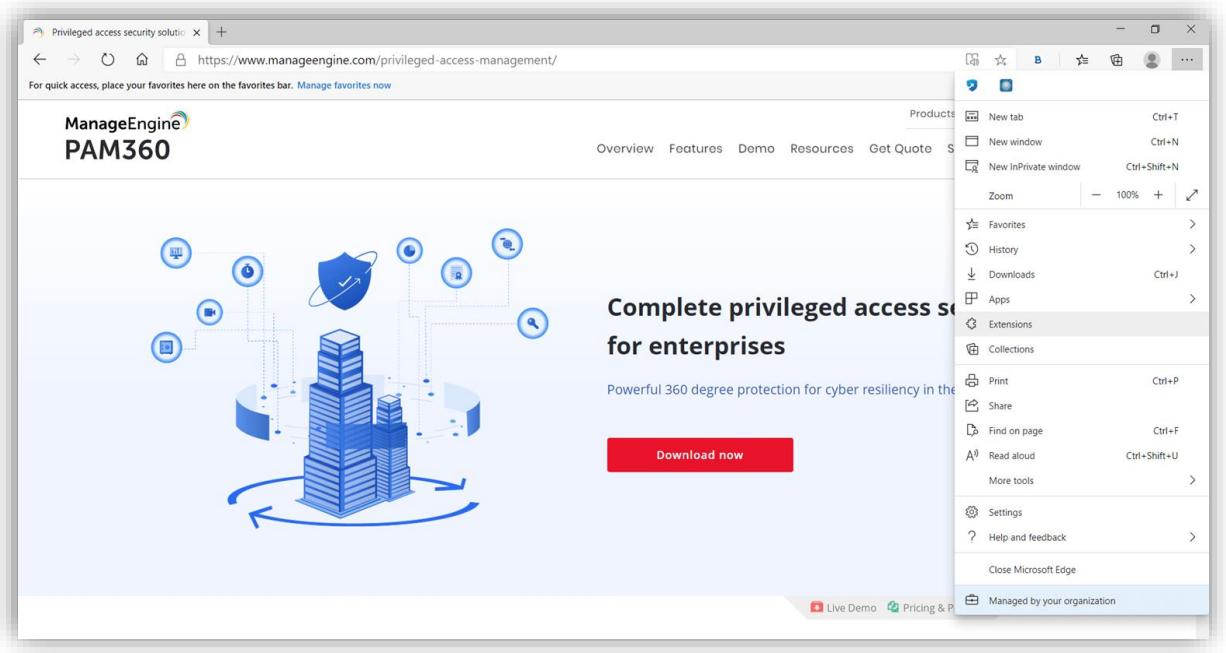
1. Benefits

The Edge browser extension provides certain advantages such as:

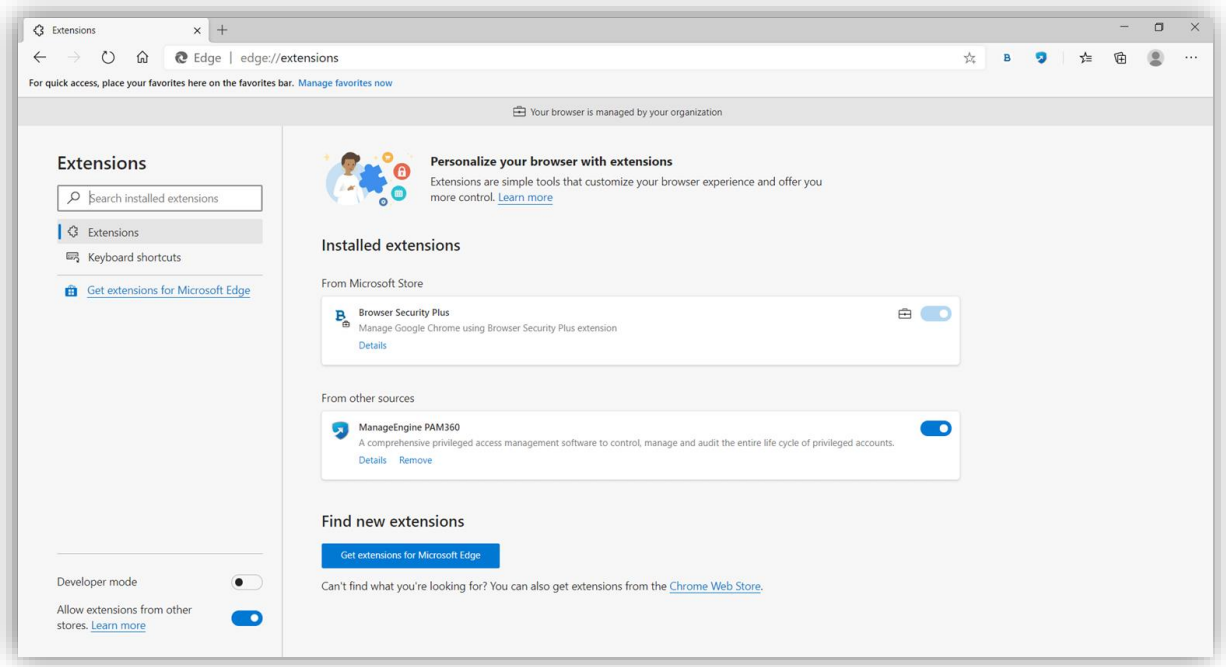
1. Automatic login to websites and applications from the browser without the need to access the PAM360 web interface.
2. Exclusive icons for auto-logon and copy username/password to simplify operations.
3. **Resource Description** icon ()to display more information about a resource. Click the resource name to list all the associated accounts.
4. Central Search bar to search for resources based on the criteria, such as resource name, DNS name, etc., specified at the time of resource creation.

2. Steps to Install the Extension

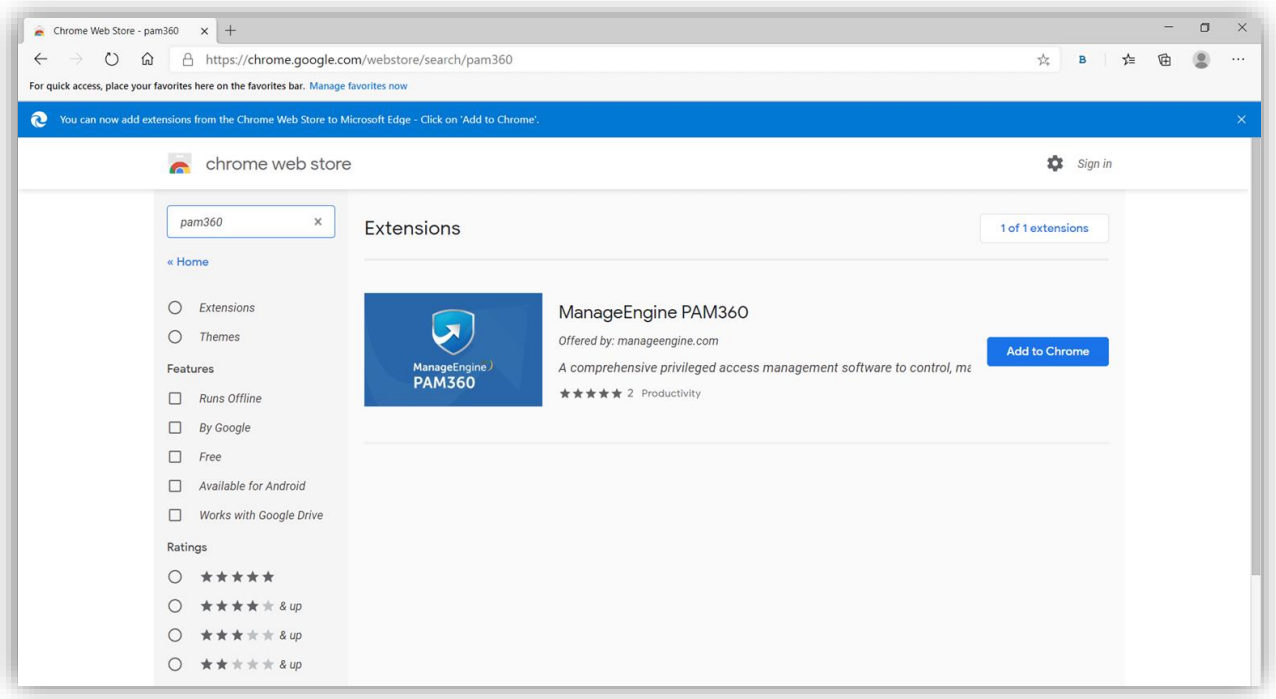
1. Open **Microsoft Edge** browser and click **Settings and more** icon or press **Alt+F.**
2. Click **Extensions** from the right pane that appears.



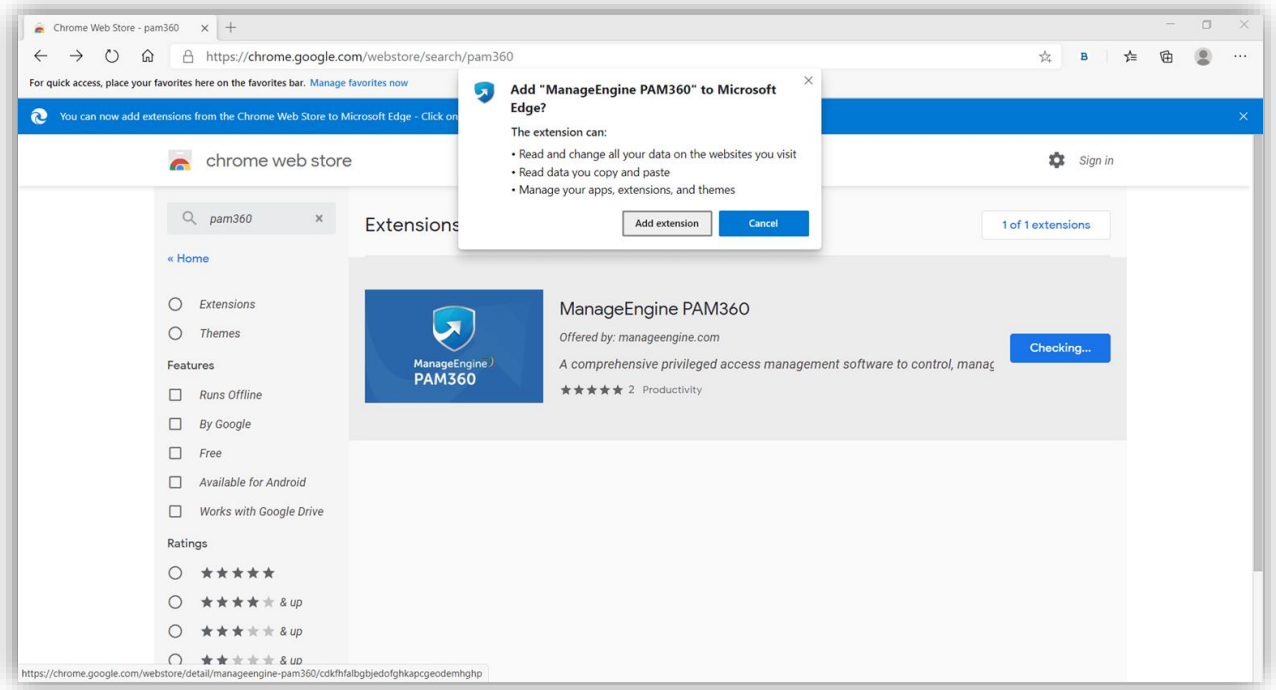
3. Enable **Allow Extensions from other stores** and click **Allow** in the pop-up that appears.



4. Go to the Chrome Web Store and search for PAM360.

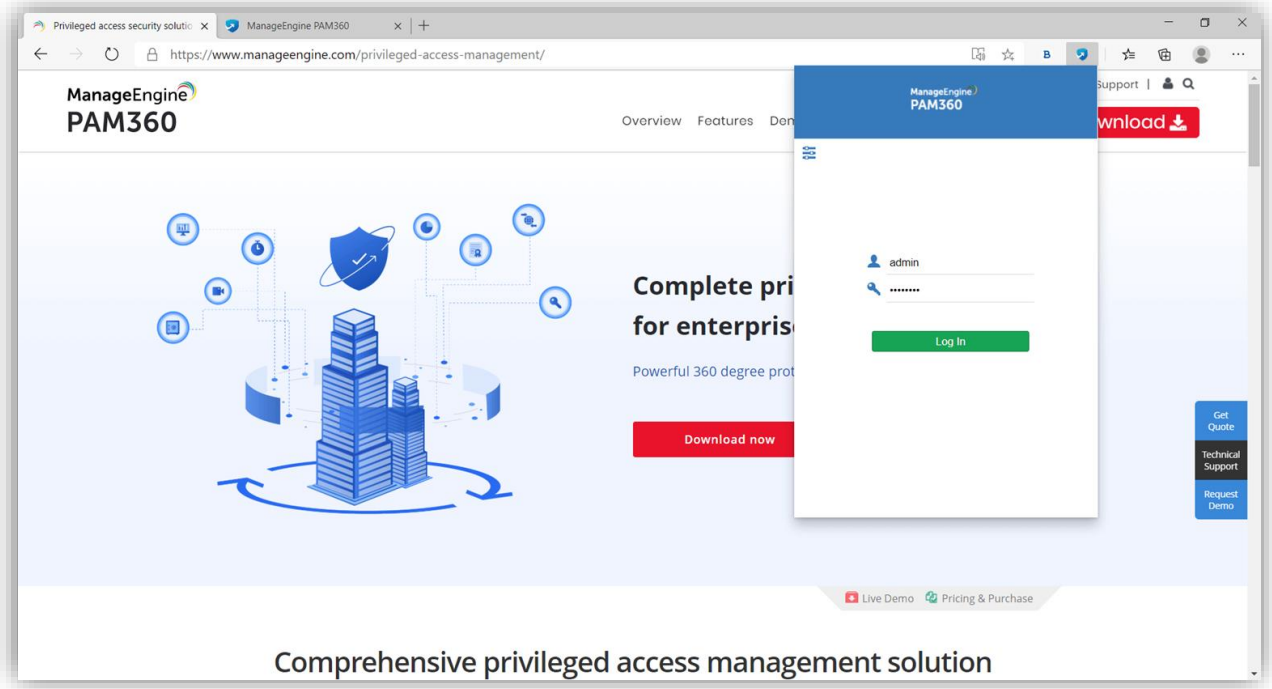


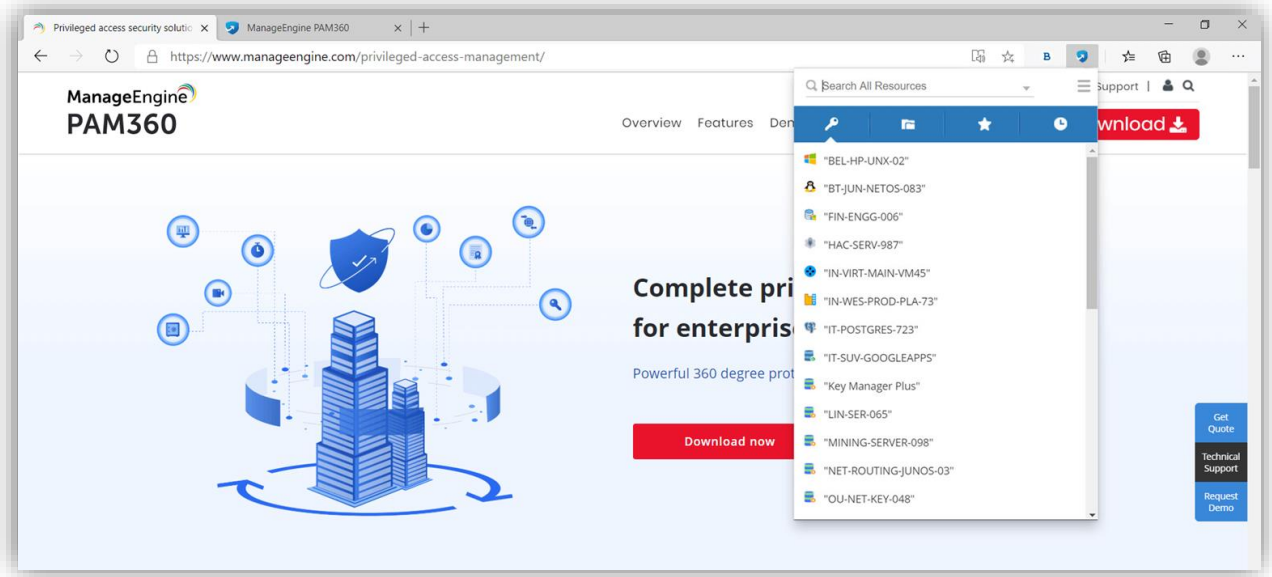
5. Click **Add to Chrome** and click **Add extension** in the pop-up that appears.

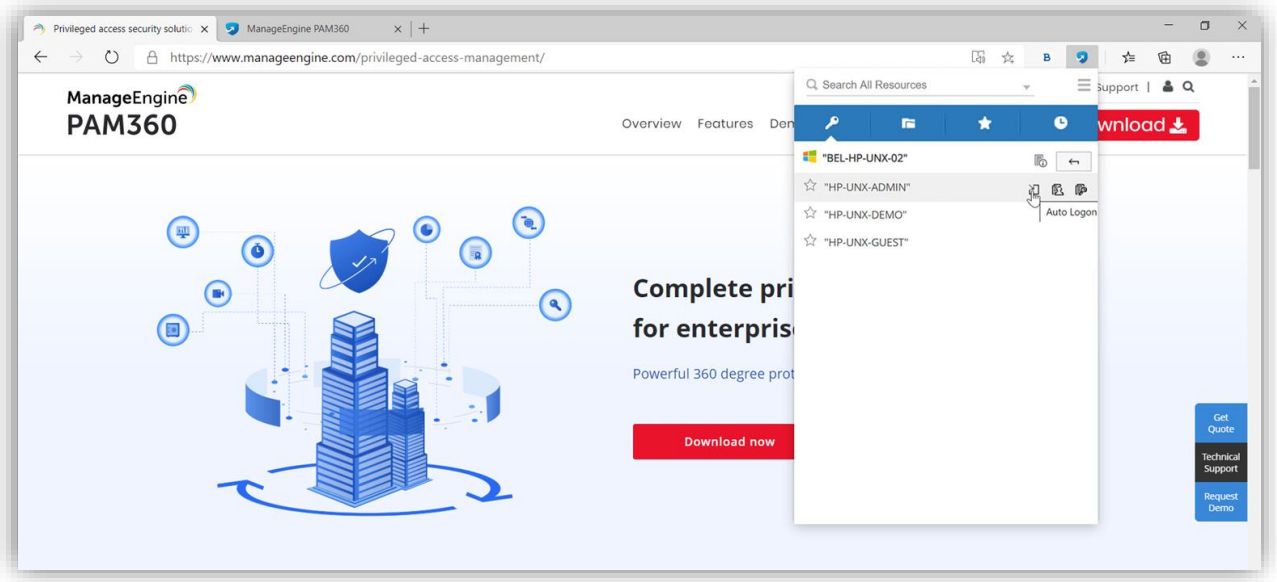


6. After installation, PAM360 icon will appear in the address bar of the browser.
7. Click the icon and enter the **Host** where PAM360 is running and specify the connection **Port**.
8. Enter your login credentials. The browser extension supports all types of login (**Local/AD/LDAP/RADIUS**) and authentication mechanisms as available in the web

interface.


ManageEngine
PAM360
Overview
Features
admin
Log In
Download now
Live Demo
Pricing & Purchase
Comprehensive privileged access management solution


ManageEngine
PAM360
Overview
Features
Search All Resources
"BEL-HP-UNX-02"
"BT-JUN-NETOS-083"
"FIN-ENGG-006"
"HAC-SERV-987"
"IN-VIRT-MAIN-VM45"
"IN-WES-PROD-PLA-73"
"IT-POSTGRES-723"
"IT-SUV-GOOGLEAPPS"
"Key Manager Plus"
"LIN-SER-065"
"MINING-SERVER-098"
"NET-ROUTING-JUNOS-03"
"OU-NET-KEY-048"
Download now



Now, the PAM360 extension is added to Microsoft Edge successfully.

3. Supported Operations

3.1 View Passwords

To view the list of all passwords, click the **All Passwords** tab in the browser extension. To view passwords specific to a resource group, click the **Resource Groups** tab. Here, the browser extension will maintain the same tree structure of resource groups and corresponding accounts as shown in the PAM360 web interface. You can view the password of any account associated with that particular resource group from the **Resource Groups** tab.

3.2 Search All Resources

Search for resources directly from the search bar in the browser extension based on any criteria such as resource name, user name, DNS name, user account, resource type, resource description, department, location, domain name, all resources or additional custom fields.

3.3 Automatic Launch of RDP and SSH Sessions

Click the auto logon icon to launch a direct connection to websites or Windows/Linux resources.

- For Linux resources, choose either **SSH** or **Telnet**.
- For Windows resources, choose either **Windows Remote Desktop** or **RDP Console Session**.
- For websites, the URL will open directly.

3.4 Username and Password Autofill on a Website or Application

To autofill credentials on a website/application, the credentials must already be stored in PAM360. When you attempt to login to a website, click the PAM360 extension icon that appears beside the credentials field and choose an account. The corresponding username and password will be auto-filled after which you can manually hit enter and login to the website.

Important Note:

PAM360 Browser extensions are designed to securely retrieve the stored credentials from the PAM360 vault and auto-fill the form in target webpages/websites. This feature allows users to automatically log into websites and web applications without entering the credentials manually.

Please note that this feature is primarily for convenience and is not a fool-proof system as the credentials are submitted in the client-side browser. Therefore, make sure if you have enforced the necessary security measures in the client-side browser and the user systems.

3.5 Favorites

This option provides quick access to the list of all your frequently used passwords that you marked as favorites in PAM360. This helps you locate resources and corresponding passwords easily. To mark any password as a favorite in the **All Passwords,** click the star icon beside it.

3.6 Recently Used

Click the **Recently Used** tab in the browser extension to find the list of all recently accessed passwords.

3.7 Copy Username or Password

Click the Copy Username or Password options to copy the credentials to the clipboard for pasting them elsewhere as required.

3.8 File Download

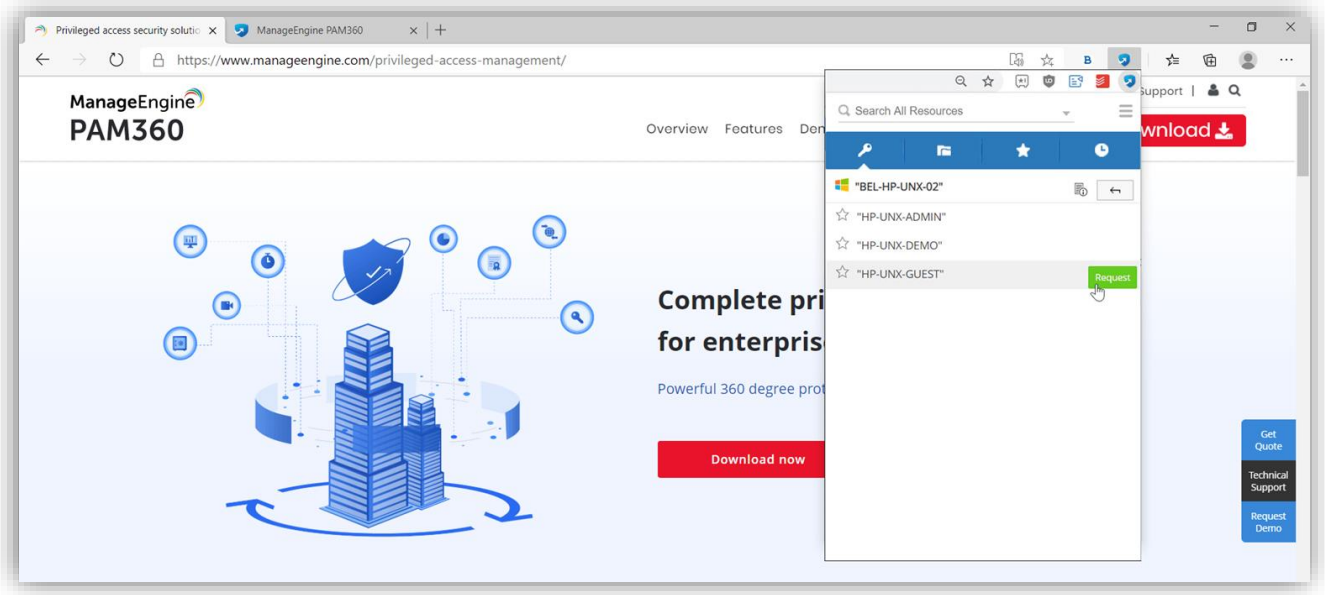
You can download the digital files, certificates and documents stored under a FileStore resource type, directly from the extension.

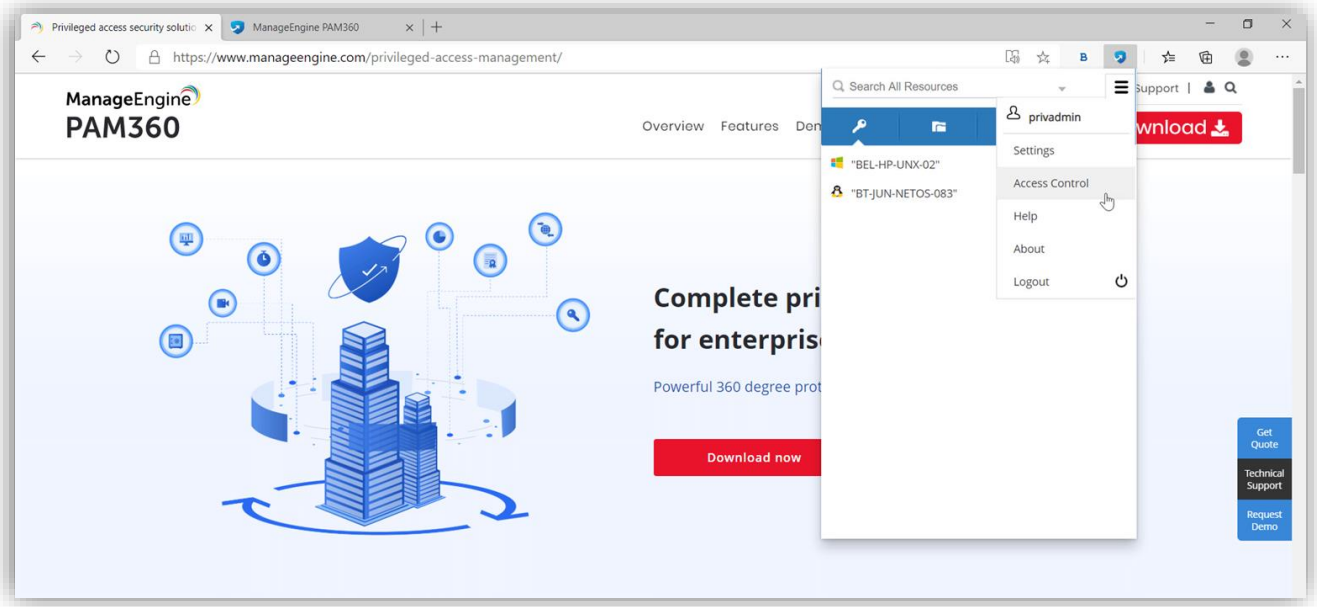
3.9 Password Access Request/Release

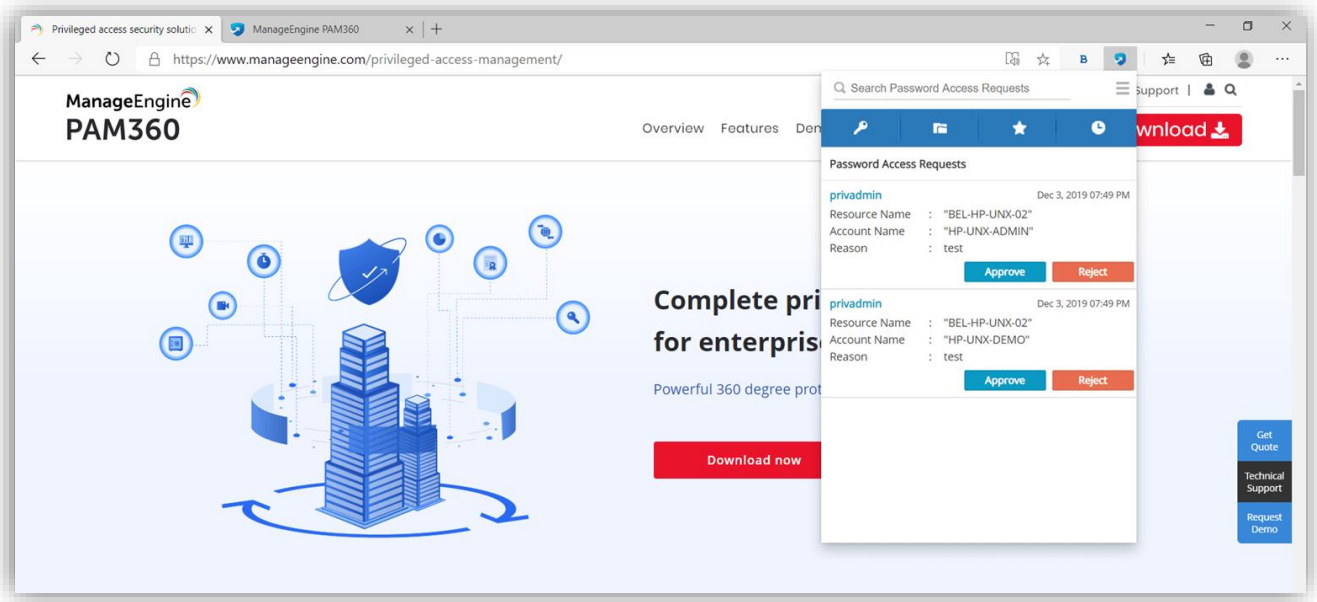
If you have configured password access control workflow in your web interface, the same will be applied to the browser extension. The administrators can either approve or reject password requests from the browser extension menu. Once a password request is approved, you can perform password check-in and check-out operations also from the extension.

Notes:

- If you have enabled Ticketing System Integration or the reason for retrieving the passwords setting in your PAM360 web interface, the browser extension will also prompt you to enter the ticket id or reason for access whenever you try to retrieve the password.
- The access control mechanism in the browser extension works the same way as in the web interface.







4. Settings

4.1 Clear Clipboard

Specify a time period in seconds to choose how long the copied data should remain in the clipboard. Enter '0' as the value to never clear the clipboard.

4.2 Automatically Logout After

Specify a time period in minutes to choose how long the session should remain logged in. Enter '0' as the value to never logout of a session in the browser extension. The automatic logout time specified for the web interface and the extension are independent of each other.

However, you can apply the same automatic logout time given for the web interface to the browser extension as well. Follow the below steps to do so:

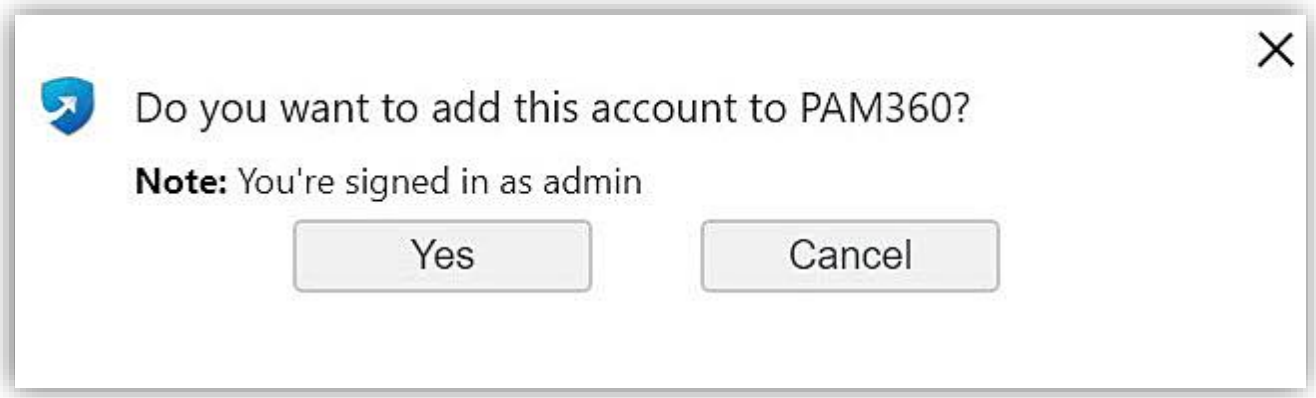
1. Go to PAM360's web interface. Navigate to **Admin >> Settings >> General Settings** and click **User Management** from the left pane.
2. Specify a value for automatic logout in the option **Automatically log off users for X minutes** and select the checkbox **Enforce this as a maximum time limit also for users logged in through browser extension.**

4.3 Prevent Browser from Prompting to Save Passwords

Select this option to prevent the browser from prompting to save passwords during any login. Once you select the option, click **Allow** in the pop-up that opens to confirm your permission to prevent the browser from prompting further.

4.4 Prevent Extension from Prompting to Add Accounts

Select this option to prevent the browser extension from prompting to save passwords during any login. However, if this option is unchecked, PAM360 will prompt to add your account when you try to login to a website. The account details will be saved as an enterprise account in PAM360 web interface.

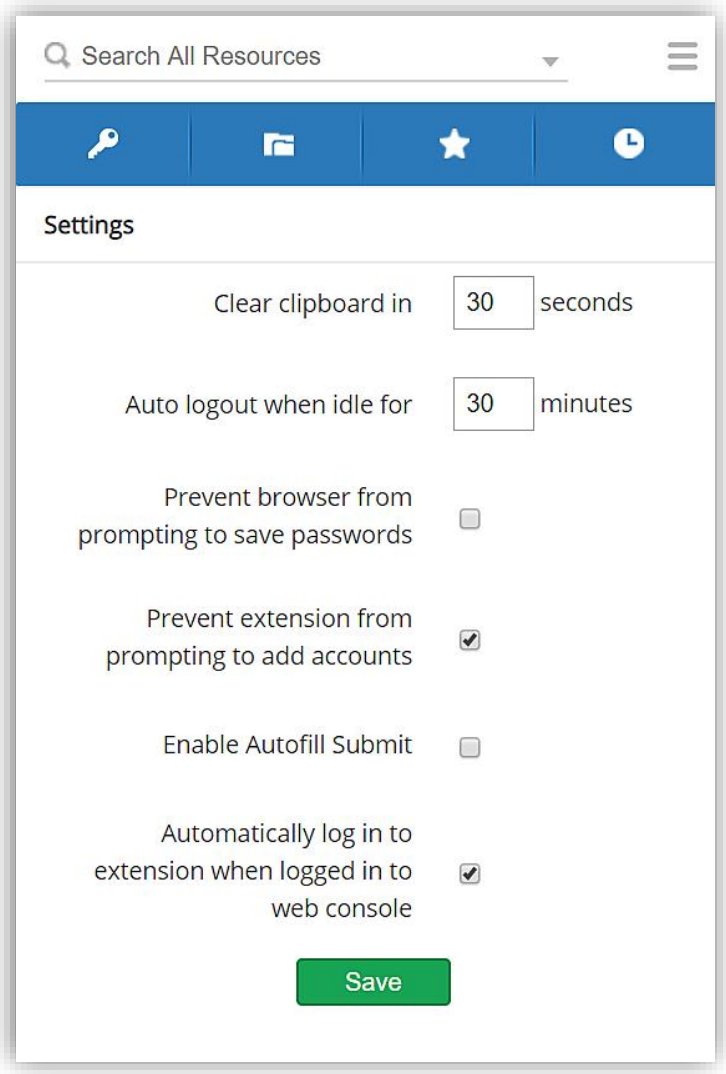


4.5 Enable Autofill Submit

Select this option to enable the browser extension to auto-fill the credentials and submit them during login.

4.6 Automatically Log in to Extension When Logged in to Web Interface

Select this option to enable concurrent login to the browser extension when you are logged into the PAM360 web interface.


Search All Resources
Settings
Clear clipboard in
30
seconds
Auto logout when idle for
30
minutes
Prevent browser from prompting to save passwords
Prevent extension from prompting to add accounts
Enable Autofill Submit
Automatically log in to extension when logged in to web console
Save

PAM360 User Account Settings

A PAM360 user granted web access can customize their user account by accessing the My Profile icon located at the top right corner of the PAM360 webpage.

1. Clear Clipboard

By selecting this action from the drop-down list under the My Profile icon, all passwords, account/resource details, sample codes, or any other copied information from the sessions will be removed from the clipboard.

2. Change Password

To modify your local authentication password, click on **Change Password**. In the ensuing pop-up window, enter all the required information and click **Save**.
Please note that if your IT administrator has implemented a password policy for your organization, the new password must comply with these guidelines. You can access information about the password policy set by your IT administrator by clicking on the information icon. The **Generate Password** option can be used to create a password that aligns with your organization's policies.
Always remember your new password, as it will not be sent via email. If you have forgotten your password, use the **Forgot password link** on the PAM360 login page to initiate the reset process. If this link is unavailable, please contact your administrator.

3. User Settings

> **Note:** This setting will only be visible to users who are provided with REST and Application Access in PAM360 from build following 6700.

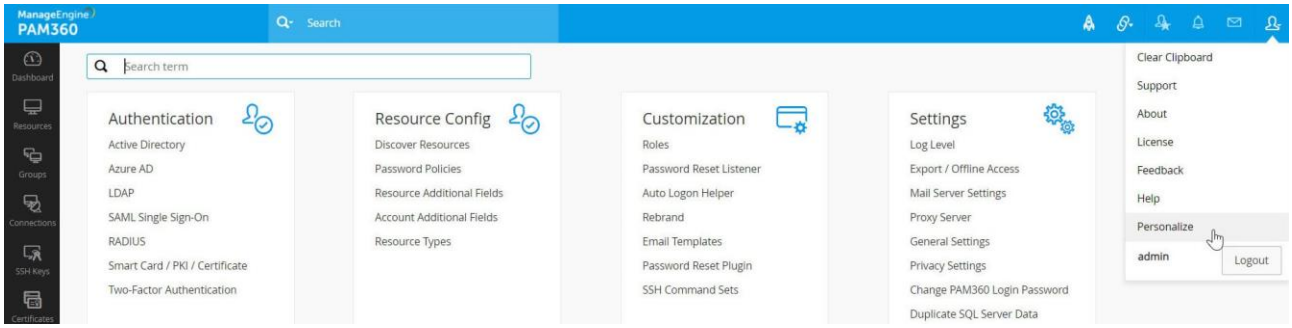
Click on the **User Settings** option; a dialogue box will open and list the REST and Application access of your user account within PAM360. You can disable the REST API/SDK Access and re-enable it when required, and also regenerate the user Authentication Token if you feel suspicious about the existing token.

4. Personalize

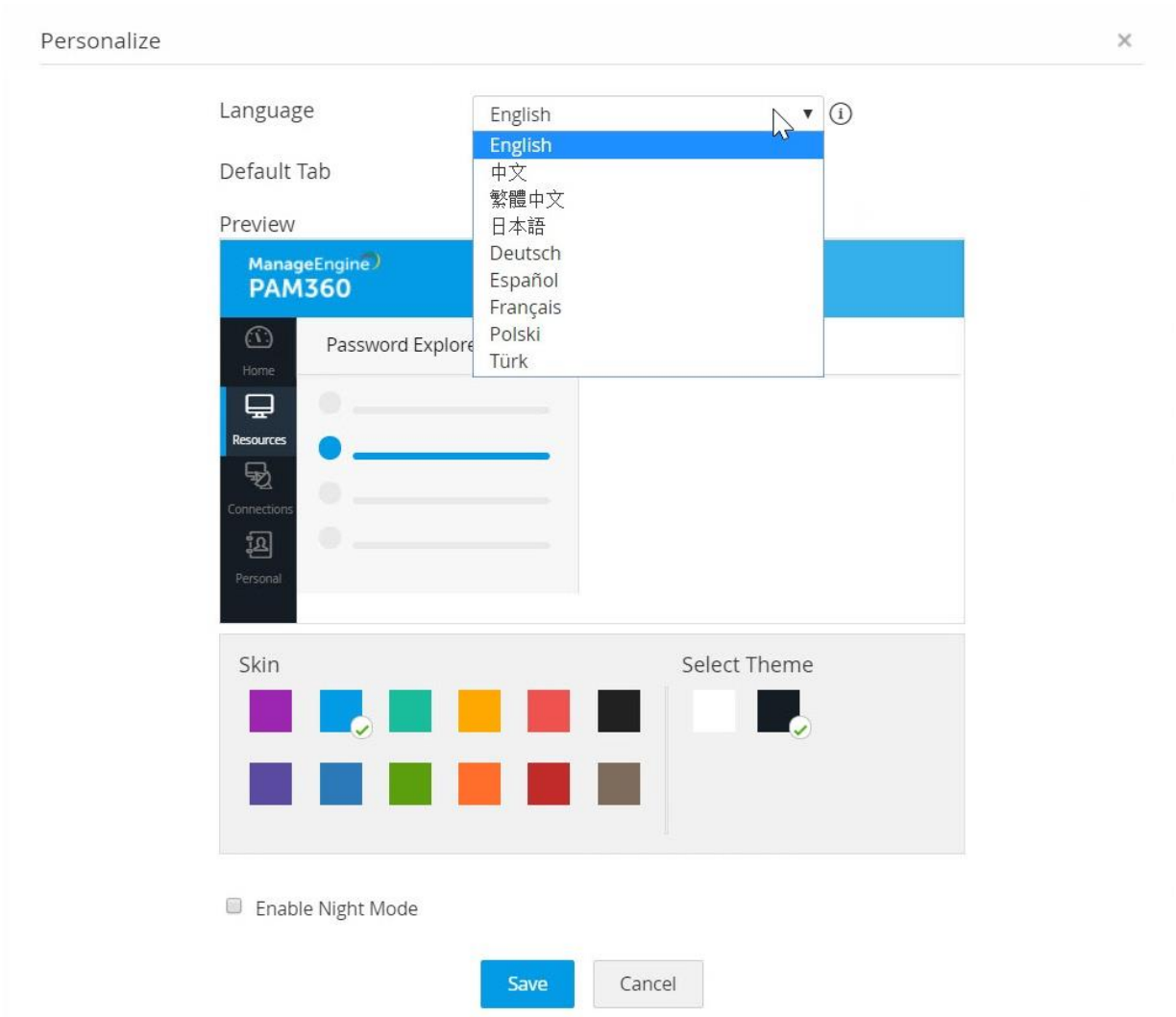
PAM360 allows its users to personalize display settings for their PAM360 account. Users can choose a convenient language from a list of options, enable night mode, and also choose a theme and background color for their account.

To personalize PAM360,

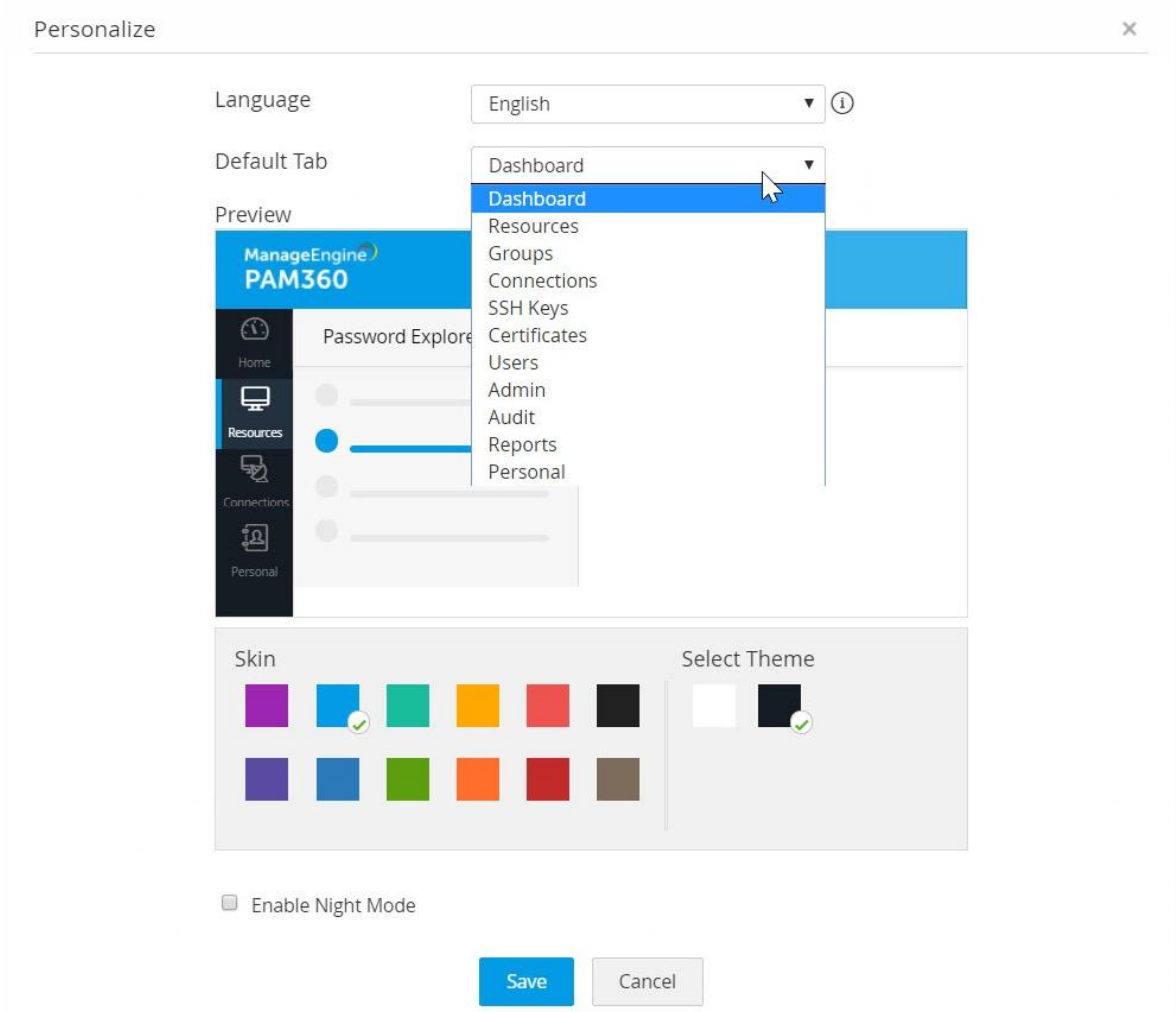
1. Click the **My Profile** icon on the top-right corner and click **Personalize** from the drop-down menu.



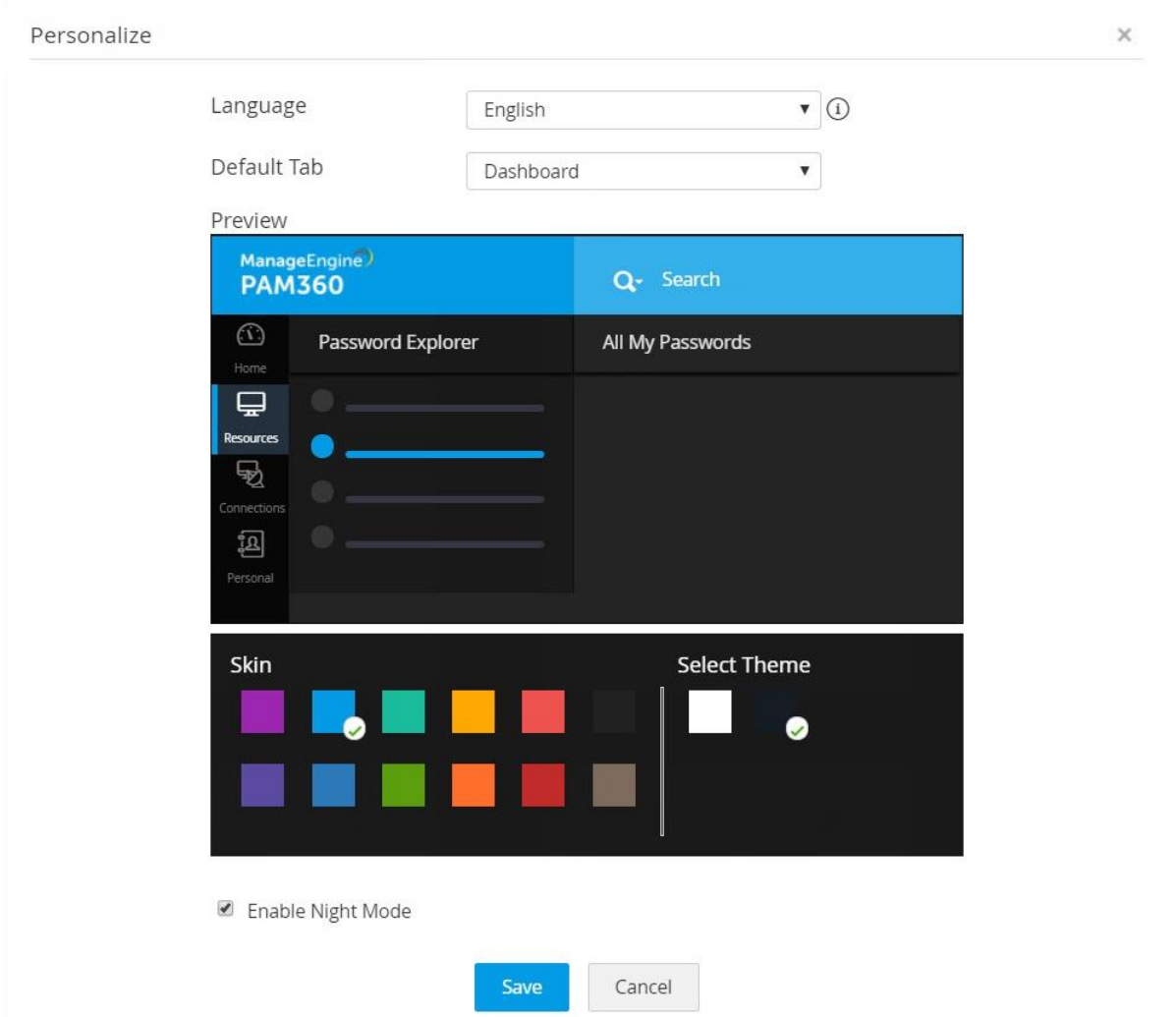
2. In the **Personalize** window that appears:
   i. From the **Language** drop-down menu, choose any language, and the changes will be reflected on the web interface.



ii. The **Default Tab** drop-down allows you to choose a particular tab to be loaded every time the website is being launched.



iii. Choose a background color from the list of **Skins** available.



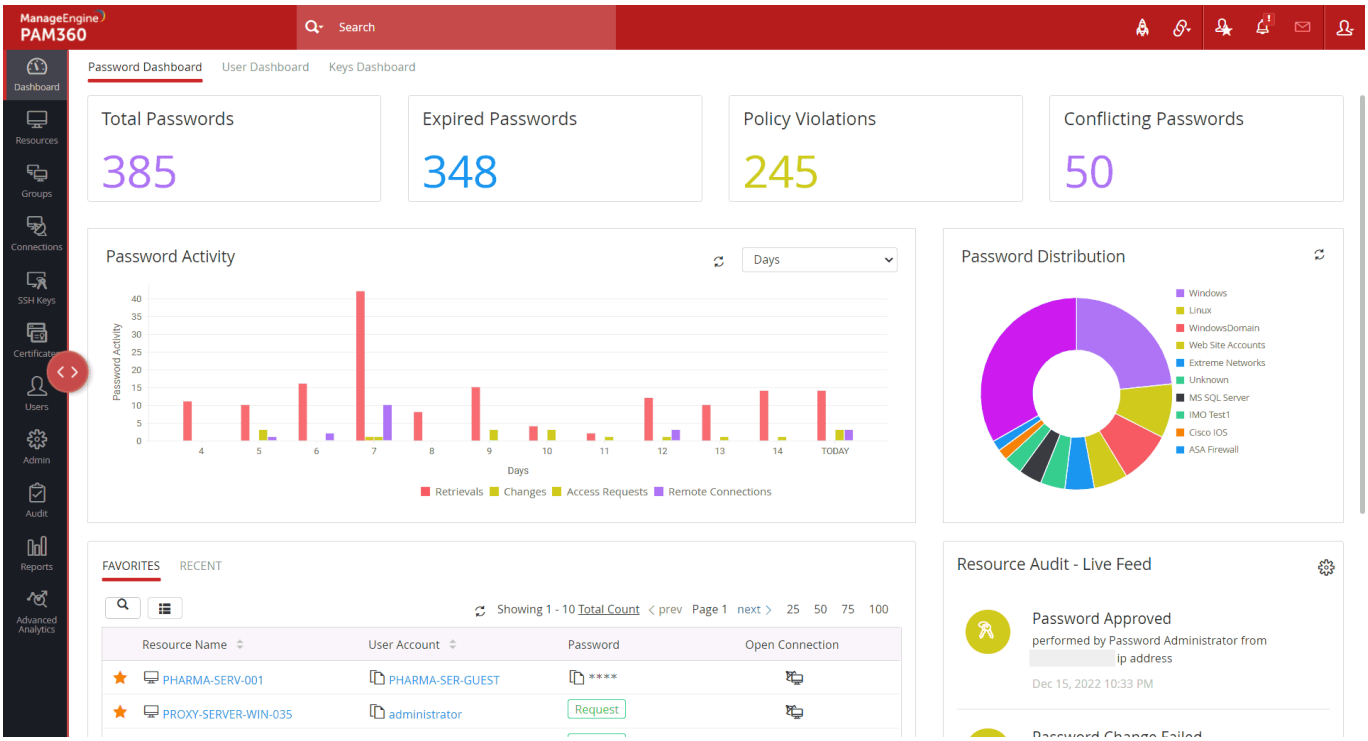
iv. Choose between **Light and Dark themes** to be applied throughout the interface.

v. Enable the night mode if required, by selecting **Enable Night Mode**.

vi. A preview of all the changes made will be available under **Preview**.

vii. Click **Save** to apply the changes.

Now, the PAM360 will apply the changes and will look based on your selection.



The remaining **Browser Extension, Remote Connect,** and **Mobile Application** will lead you to the respective web pages from where they can be utilized and used.

Further, using the **Logout** option will log you out from the PAM360 interface.

PAM360 - Frequently Asked Questions

1. General

1. Do I need to install any prerequisite software before using PAM360?
2. What are the operating systems supported by PAM360?
3. Can others see the resources added by me?
4. Can I add my own attributes to PAM360 resources?
5. What happens if a user leaves the organization without sharing their sensitive passwords with anyone?
6. How to add a new Active Directory (AD) domain in PAM360?
7. How to remove an AD domain from PAM360?
8. How to fix the errors “The list of Groups is too large to display” and "The list of OUs is too large to display" while importing from AD?
9. How can I edit the properties of an existing scheduled task, such as changing the time or the frequency?
10. Can an AD sync job be set to occur multiple times a day, such as once every 4 hours?
11. How to fix the “PAM360 detected harmful content in the data entered by the user and aborted the operation" error occurred while importing resources through a csv/tsv file?
12. How do I troubleshoot if importing users/resources from AD fails?
13. Can I run custom queries to generate results for integration with other reporting systems?
14. Does domain SSO work across firewalls/VPNs?
15. Can I rebrand PAM360 with my own logo and organizational information?
16. Does PAM360 record Password viewing attempts and retrievals by users?
17. Why does the size of PostgreSQL wal_archive file increase at a rapid pace?
18. Does PAM360 support High Availability?
19. What are the various syslog formats followed by PAM360?
20. Does PAM360 alter the number of Windows CAL licenses?
21. How do I run the PAM360 service using a group Managed Service Account (gMSA)?
22. How do I fix the PostgreSQL server start-up failure?
23. How to handle the following exceptions that occur while upgrading PAM360 version?
24. How to perform version upgrade using the CLI mode?

25. Logs, Reports, and CAPTCHA are unreadable after a version upgrade. How to fix this issue?
26. Do you recommend Antivirus exclusion during the installation of PAM360?
27. How to utilize multiple ManageEngine application services simultaneously without limitations?
28. How many client organizations does the PAM360 support?

2. Web Interface and Authentication

1. Can I change the default port 8282 where PAM360 is listening?
2. How do I change the PAM360 web portal access URL?
3. PAM360 is a web-based application that can be accessed via a web browser. Does that mean I can access it from anywhere?
4. Can I change the IP address in which PAM360 application is binding when I have multiple NIC cards and IP's available in the server?
5. What if my users are not notified of their PAM360 accounts?
6. What are the authentication schemes available in PAM360?
7. What are the user roles available in PAM360? What are their access levels?
8. What if I forget my PAM360 login password?
9. Why do I sometimes see a security warning while accessing the PAM360 console via the browser?

3. Security

1. How secure are my passwords in PAM360?
2. How secure are Application-to-Application and Application-to-Database password management done through Password Management APIs?
3. Can we install our own SSL certificates?
4. How to generate signed SSL certificates? [OR] How to make the PAM360 server trusted by web browsers and users?
5. Can we create server certificates with SubjectAlternativeName (SAN)?

4. Password Synchronization

1. Can I change resource passwords from the PAM360 console?
2. When do I use the agent and agent-less modes for password synchronization?
3. Can I enable agent less password reset if I add my own resource type for other distributions of Linux/other versions of Windows?

4. Is there a way to carry out remote password synchronization for custom resource types that do not come out of the box in PAM360?
5. How do I troubleshoot when password synchronization does not happen?
6. How do I reset domain passwords when Windows domain password reset fails with an error message: "The authentication mechanism is unknown"?
7. What are the prerequisites for enabling Windows service account reset?
8. Does domain SSO work across firewalls / VPNs?

5. Backup and Disaster Recovery

1. Can I move PAM360 from one server to another?
2. Can I setup disaster recovery for the PAM360 database?
3. Where does the backup data get stored? Is it encrypted?

6. Licensing

1. What is the Licensing Policy for PAM360?
2. Can I buy a permanent license for PAM360? What are the options available?
3. How can I apply my license file?
4. I want to have a High Availability setup with multiple servers. Will a single license suffice for this?
5. Can PAM360 support more than 1000 administrators?
6. Can I extend my evaluation to include more administrator users or for more number of days?

7. SSH Key Management

1. Are there any differences in the way SSH user accounts and SSH service accounts are managed using PAM360?
2. Is there any way to view SSH keys that were not rotated?
3. Does PAM360 support management of digital keys other than SSH keys and SSL certificates?

8. SSL Certificate Management

1. Is there any certificate type that PAM360 is incompatible with?
2. Is it possible to automatically identify and update the latest version of certificates in PAM360' certificate repository?

3. Does the Linux version of PAM360 support certificate discovery from Active Directory and MS Certificate Store?
4. Is it possible to track the expiry of certificates with the same common name in PAM360' certificate repository?
5. How do I import private key for a certificate?
6. How do I deploy a certificate to Certificate Store and map it to the application that uses the certificate?
7. Does PAM360 support subnet based certificate discovery?
8. Does PAM360 support automatic scheduling for certificate discovery from MS Certificate Store?
9. Are certificate related alert emails generated for all versions of a certificate (the ones that show in "certificate history" also) or only for those certificates listed in PAM360' certificate repository?
10. Are certificates issued by the company's internal Certification Authority (CA) counted for licensing?
11. How do I import a root certificate into PAM360?

9. Policy-Based Access Privilege - Zero Trust Approach

1. What are the agent types concerning the Zero Trust approach?
2. How does the agent work for user devices and resources?
3. Will the device installed with the PAM360 agent of usage type 'User Device' be added as a resource in PAM360?
4. Can I use the policy-based access privilege feature in an agentless mode?
5. How to fetch the default system data from a user device/resource?
6. How do you decide a weightage of a parameter for the trust score validation?
7. How does the user trust score and the resource trust score calculated?
8. What is the purpose of an access policy?
9. How many access policies can a user and a resource be associated with?
10. When does a conflict happen in policy-based access privilege?
11. If there are multiple access policies associated with a resource via various static groups, what will be the intended active access policy of a resource?

12. How to resolve a conflict between the access policies of a resource?

13. How does the precedence of the actions work in the access policy conditions?

14. Where can I see the user trust score?

15. Where can I see the resource trust score?

16. What are the possible reasons for the session termination?

1. General

1. Do I need to install any prerequisite software before using PAM360?

Apart from the standard system requirements (both hardware and software), the following elements are essential for the proper functioning of the PAM360 server.

These are especially required if you are planning to make use of PAM360's account discovery and password reset provisions.

- An external mail server (SMTP server) for the functioning of PAM360 server and to send various notifications to users.
- A service account [OR] a gMSA that has either domain admin rights or local admin rights in the PAM360 server and in the target systems that you would like to manage.
- Visual C++ Redistributable for Visual Studio 2015 and above (for PAM360's Account Discovery and Password Reset features.)
- Microsoft .NET framework 4.5.2 or above must be installed in the server where PAM360 is installed.

To check if these software requirements are configured:

- Go to Support » Software Requirements and click Check Configuration.

In the pop-up box that opens, the configuration status will be displayed.

2. What are the operating systems supported by PAM360?

PAM360 supports the following flavors of Windows and Linux operating systems:

Windows	Linux
Windows Server 2019	Ubuntu 9.x and above

Windows Server 2016	CentOS 4.4 and above
Windows Server 2012 R2	Red Hat Linux 9.0
Windows Server 2012	Red Hat Enterprise Linux 7.x
Windows 10	Red Hat Enterprise Linux 6.x
Windows 8	Red Hat Enterprise Linux 5.x

3. Can others see the resources added by me?

Except for super administrators (if configured in your PAM360 set up), no one including admin users, will be able to see the resources added by you. However, if you share your resources with other administrators, they will be able to see them.

4. Can I add my own attributes to PAM360 resources?

Yes, you can extend the attributes of the PAM360 resource and user account to include details that are specific to your needs. Refer to the help section Adding Resources Manually for more details.

5. What happens if a user leaves the organization without sharing their sensitive passwords with anyone?

If an administrative user leaves the organization, they can transfer the resources they own to other administrators. By doing so, they'll have no access to those resources themselves, unless they transfer the resources to themselves. Refer to the help section Transferring Ownership of Resources/Resource Groups for more details.

6. How to add a new Active Directory (AD) domain in PAM360?

Administrators can add new domains for both resource discovery and user discovery operations. Follow the below steps for resource discovery:

1. Go to the Resource tab and click Discover Resources.
2. Here you can click New Domain beside the Enter Domain Name field and add a new domain name.

Refer to the help section Steps to Discover Resources for detailed instructions.

To add a new domain for user discovery:

1. Go to the Admin tab and click Authentication >> Active Directory.
2. Here you can click New Domain beside the Enter Domain Name field and add a new domain name.

Refer to the help section Importing Users for detailed instructions.

7. How to remove a domain from PAM360?

To remove a domain from PAM360, you first need to remove the users that belong to this domain. Once the users are removed, follow the below steps to remove the domain information:

1. Go to the Admin tab and click Authentication >> Active Directory.
2. Here, click the View Synchronization Schedules option.
3. Delete the required domain from the Domains pane on the left.

8. How to fix the errors “The list of Groups is too large to display” and "The list of OUs is too large to display" while importing from AD?

To fix these errors, you need to increase the number of OUs and groups allowed during the AD import. Follow the below steps:

a. Stop the PAM360 service.
b. Take a backup of the system_properties.conf file present inside \conf directory.
c. Now, open the system_properties.conf in the Word Pad with admin permission and edit the following values:
    i. Search for domain.ou.limit=2500 and change the value to 25000.
    ii. Search for domain.group.limit=2500 and change the value to 25000.
d. Save the file and restart the PAM360 service.

9. How can I edit the properties of an existing scheduled task, such as changing the time or the frequency?

You can modify the time interval for AD synchronization by following the below steps. To create a new task or edit the existing scheduled tasks, follow the below steps:

a. Log in as an administrator and go to the **Groups** tab.

b. Click the Actions icon available beside the resource group and select **Periodic Account Discovery** from the drop down.

c. In the pop-up that comes up, schedule or modify the time interval for AD synchronization.

> **Note:** Only the owner of the scheduled task can edit or modify the existing schedules by navigating to **Admin >> Manage >> Scheduled tasks.**

10. Can an AD sync job be set to occur multiple times a day, such as once every 4 hours?

Configuring a schedule to run every 4 hours must be done when you import the OU/Group from AD.

To import, go to **Resources >> Discover Resources >> Import**. Here, specify the synchronization interval as per your requirement and import.

11. How to fix the “PAM360 detected harmful content in the data entered by the user and aborted the operation" error occurred while importing resources through a csv/tsv file?

As a security measure, PAM360 to restricts certain characters such HTML tags (< , >), "URL: HTTPS://" or "URL: HTTP://", security mark (?), end line and multiple spaces in the notes or any other field in PAM360 to avoid causing security violations in the product.

If any of these characters are used in any other fields except the password field, then it causes a violation and the import fails.

To avoid this, verify your CSV/TSV file to ensure these characters are removed for a successful import.

> **Note:** It is advisable to ensure that the resource & account descriptions do not exceed the max limit of 2000 characters.

12. How do I troubleshoot if importing users/resources from AD fails?

Verify the following:

- Check if the user credentials are correct.
- If you are trying with an admin user and it fails, try entering the credentials of a non-admin user. This is just to verify if connection could be established properly.

If the above verifications fail, please contact pam360-support@manageengine.com.

13. Can I run custom queries to generate results for integration with other reporting systems?

Yes, you can. Please contact our support with your specific request and we will help you with the relevant SQL query to generate XML output.

14. Does domain SSO work across firewalls / VPNs?

The domain Single Sign On (Windows-integrated authentication) is achieved in the Windows environment by setting non-standard parameters in the HTTP header, which are usually stripped off by devices like firewalls / VPNs. PAM360 is designed for use within the network. So, if you have users connecting from outside the network, you cannot have SSO enabled.

15. Can I rebrand PAM360 with my own logo and organizational information?

Yes. PAM360 provides you with the following options for customization and rebranding:

- Using your own logo for web interface the mobile app. (Recommended image size is 210*50 pixels)
- Setting a login page description for the product.
- Changing the default color of the user interface.
- Displaying a banner with customized legal content.
- Customizing a privacy policy content and display an acceptance button for the same.

To carry out the above functionalities:

a. Navigate to **Admin >> Customization >> Rebrand**.

b. Under the **Logo and Theme** section, set up a customized logo and a login page description, and change the default skin tone.

c. Under **Login Page Text**, add policies and/or legal conditions to be displayed in the login page.

Note that at any point, this configuration can be disabled. Refer to the help section **Rebranding PAM360** to know more.

16. Does PAM360 record Password viewing attempts and retrievals by users?

Yes, PAM360 records all operations that can be possibly performed by a user- including password viewing and copying operations. From audit trails, you can get a comprehensive list of all the actions and attempts by the users with password retrieval. Refer to the help section Audit and Notification to know more.

17. Why does the size of PostgreSQL wal_archive file increase at a rapid pace?

This issue occurs when the backup location specified in PAM360 is no longer accessible to save the backup file. In simple terms, whenever the PostgreSQL database backup fails, wal_archive folder size will start increasing.

Solution:

- Check if there is enough disk space available on the PAM360 drive.
- If not, remove the logs directory and a few files present inside directory.
- You need to have only one or two backups to be present here.
- Login to PAM360 and navigate to Admin >> Configuration >> Database Backup.
- Click on the 'Backup Now' button.

This will trigger an instant backup and automatically purge the wal_archive directory.

18. Does PAM360 support High Availability?

Yes, refer to the help section High Availability for more details.

19. What are the various Syslog formats followed by PAM360?

The following are three different types of syslog formats that PAM360 uses to send syslog messages to your syslog collector host:

i. **Resource Audit**

```
operatedName+":"+operatedIp operationType operatedDate statusMess
resourceName+":"+accName+":"+reason
```

ii. **User Audit**

operatedName+":"+operatedIp operationType operatedDate statusMess auditUserName+":"+reason

iii. Key Audits

SSL: <190> Parent_Domain: manageengine.com Included_Domain: kmp.com Days_to_Expire: 100 Expire_Date: 5.08.2020
SSH: <190> Key_Name:172.21.147.130_test123_id Days_Exceeded:0 Modified_On:2016-02-16 17:41:24.008

20. Does PAM360 alter the number of Windows CAL licenses?

Generally, RDP sessions are invoked from the PAM360 server and relayed to the end user's browser through a third-party component called Spark Gateway. This component comes bundled with PAM360 and does not have any relation to Windows CAL licenses. Hence, PAM360 does not affect the number of Windows CAL licenses in any way. Users need to purchase as many CAL licenses, as suggested by Microsoft.

21. How do I run the PAM360 service using a group Managed Service Account (gMSA)?

To know in detail about running the PAM360 service using a group Managed Service Account, refer to the help section Installing PAM360.

22. How do I fix the PostgreSQL server start-up failure?

Error Scenarios:

- **During Upgrade:**

  'Trying to start PostgreSQL server failed' error in the command prompt after choosing the PPM file.

- **While setting up HA:**

  'Trying to start PostgreSQL server failed' error in the command prompt after executing the HASetup.bat command.

- **During Service Start up:**

i. PAM360 service start failure after the upgrade.

ii. PAM360 service start failure after updating the PAM360 service account in Services console.

For the above two cases, do the following:

Open the **<PAM360-HOME>\logs\wrapper** file with notepad/Notepad++ and move to the very bottom of the file (i.e. most recent time frame) and check if we get the 'Trying to start PostgreSQL server failed' error.

Possible Causes:

The following causes are explained with respect to the above error scenarios:

The 'Trying to start PostgreSQL server failed' error occurs when,

1. PAM360 is unable to access few sub-folders inside PAM360 (i.e appropriate permission not given).
2. The PostgreSQL DB fails to start because of a background process that was not terminated properly.

The instant DB port might be occupied by a different process.

Solution:

The solution given below applies to all the above error scenarios. To fix this issue, follow the below steps to provide permission,

1. Start the Task Manager and kill all Postgres process (make sure **"show process from all users"** is selected - For PAM360).
2. Update the PAM360 service with a privileged account in the services console.
3. Open command prompt using administrator and execute the below query:
   i. **icacls "installation path" /q /c /t /grant Users:F**
      - **installation path** - Provide the Manage_Engine folder location.
      - **Users** - Provide the PAM360 service account in the following format: **<DomainName\user name> or <username@domainname>**.
      - **Example: icacls "C:\ProgramFiles\ManageEngine\PAM360" /q /c /t /grant ManageEngine\svcpam360:F**

   ii. If the key is placed outside the PAM360 folder, kindly provide permission for the key's locations using icacls command.

   iii. In the same way, provide full control permission for **<PAM360>\pgsql\data** folder.

   iv. Check the **<PAM360_Installation_Directory>/pgsql/data** folder and ensure if it has inherited that permission.
4. Navigate to **<PAM360_Installation_Directory>/pgsql/data** and open **pg_hba.conf** and

search **NULL**. If you find any, remove the entire line that contains NULL.

5. Rename the logs folder present inside the **<PAM360_Installation_Directory>** as **logs.old** and create a new folder as logs.
6. Rename the Patch folder present inside the **<PAM360_Installation_Directory>** as **Patch.old** and create a new folder as Patch.
7. Navigate to **<PAM360_Installation_Directory>/bin** directory and look for files named **.lock** or **lockfile**. If present, move both these files to any other directory.
8. Go to **<PAM360_Installation_Directory>/pgsql/data** directory and look for files named **recovery.conf** and **postmaster.pid**. If present, move this file to any other directory.
9. Now, try to apply the PPM or configure HA or try starting the service.

If the issue still persists, zip and send us the logs from the **<PAM360_HOME>** and also the **<PAM360-HOME>\pgsql\data\pg_log** folder along with the above screen shots to pam360-support@manageengine.com.

23. How to handle the following exceptions that occur while upgrading PAM360 version?

Exception #1: Caused by: java.lang.OutOfMemoryError: GC overhead limit exceeded

1. Stop the PAM360 service.
2. Take a backup of the <PAM360_Installation_Directory> or a VM snapshot.
3. Navigate to <PAM360 installation directory>\bin and open the file **UpdateManager.bat** (UpdateManager.sh for Linux)
4. Open this file using any editor and search for the entry: $JAVA -Xmx100m $JAVA_OPTS -Dtier-type=BE -Djava.library.path=./lib/native -Dtier-id=BE1 -cp $CLASSPATH com.adventnet.tools.update.installer.UpdateManager -u conf $*
5. Change the value to $JAVA -Xmx2048m $JAVA_OPTS -Dtier-type=BE -Djava.library.path=./lib/native -Dtier-id=BE1 -cp $CLASSPATH com.adventnet.tools.update.installer.UpdateManager -u conf $*
6. Save the file. Start the PAM360 service and try the upgrade once again.

If the issue still persists, please send your logs to pam360-support@manageengine.com for further investigation.

Exception #2: Trying to start the PostgreSQL server failed

1. Stop PAM360 service.
2. Kill any Postgres or PAM360.exe process using task manager.
3. Exit the PAM360 tray icon.
4. Run PAM360 service account using a privileged account. And give this account <PAM360_Installation_Directory> full and manage folder permission.

5. Open command prompt using the privileged account.
6. Proceed with the upgrade.

24. How to perform version upgrade using the CLI mode?

Windows

1. Stop the PAM360 service.
2. Open command prompt with administrator privileges.
3. Navigate to <PAM360_Installation_Directory> /bin and execute - UpdateManager.bat -u conf -c -option i Mention the .ppm file location in the next line.
4. Enter to proceed with the upgrade.

Linux

1. Stop the PAM360 service.
2. Open command prompt with administrator privileges.
3. Navigate to /bin and execute - UpdateManager.sh -u conf -c -option i -ppmPath
    - Eg: UpdateManager.sh -u conf -c -option i -ppmPath c:\pam360.ppm.
4. Enter to proceed with the upgrade.

Click here for detailed upgrade pack instructions.

25. Logs, Reports, and CAPTCHA are unreadable after a version upgrade. How to fix this issue?

Check for the following:

i. Open logs and check if you could find the following error:
javax.servlet.ServletException: javax.servlet.ServletException: java.lang.Error: Probable fatal error:No fonts found.

ii. Check if you have installed dejavu fonts.

Use the following commands to install the dejavu fonts.

i. **For RHEL / Centos:**

sudo yum install fontconfig dejavu-sans-fonts dejavu-serif-fonts

ii. **Ubuntu / Debian:**

sudo apt install fonts-dejavu fontconfig

iii. **SLES:**

sudo zypper install dejavu-fonts fontconfig

Now, you have successfully installed the dejavu font in your machine.

After installing, follow the below steps:

1. Navigate to <PAM360 Installation Directory>/conf folder.
2. Open wrapper_lin.conf file and add following property:
   wrapper.java.additional.27=-Dsun.java2d.fontpath=<Font Dir Path>

   [or]

3. Copy all the ttf files and paste it under <PAM360 Installation Directory>/jre/lib/fonts folder.
4. Restart the PAM360 service.

26. Do you recommend Antivirus exclusion during the installation of PAM360?

Yes, we do recommend the exclusion of the 'ManageEngine/PAM360' directory from Antivirus, Endpoint Detection and Response (EDR) and Extended detection and response (XDR) scanning during the product installation - the installation wizard will prompt you to do so. The essential components that make the product operative are available inside this directory, which includes different scripts that are used for initiating remote connections and in performing maintenance operations. If this directory is not excluded, there will be slowness in the product as the Antivirus scanning will scan each script file during scheduled operations in PAM360. Also, features such as remote password reset may not function properly.

27. How to utilize multiple ManageEngine application services simultaneously without limitations?

Presently, both ManageEngine PAM360 and other ManageEngine products utilize some common cookie names (JSESSIONID and JSESSIONIDSSO), which can hinder concurrent sessions of the ManageEngine application services. To enable multiple sessions with similar cookies in PAM360, follow these steps to identify and customize the PAM360 cookie settings:

1. Navigate to <PAM360_Installation_Directory>/conf.
2. Open the system_properties.conf file with the administrator privilege, add the following at the end of the line and save.

```
org.apache.catalina.authenticator.Constants.SSO_SESSION_COOKIE_NAME=PAMJSESSIONIDSSO

org.apache.catalina.SESSION_COOKIE_NAME=PAMSESSIONID
```

3. Now, open the web.xml file with the administrator privilege, look out for the <session-config> section, and update it as follows:

```
<session-config>
<session-timeout>450</session-timeout>
<cookie-config>
<name>PAMSESSIONID</name>
</cookie-config>
</session-config>
```

4. Now, restart the PAM360 service and proceed.

28. How many client organizations does the PAM360 support?

As of now, PAM360 is equipped to support up to 900 client organizations.

2. Web Interface and Authentication

1. Can I change the default port 8282 where PAM360 is listening?

Yes, you can change the default port as explained below:

1. Login to PAM360 as an **Administrator**. Navigate to **Admin >> Configuration >> PAM360 Server**.
2. Enter the required port beside the **Server Port** field, and click **Save**.
3. Restart PAM360 for this configuration to take effect.

2. How do I change the PAM360 web portal access URL?

1. Login as an administrator. Navigate to **Admin >> Settings** and click **Mail Server Settings**.
2. Fill in the required URL in the **Access URL** field and save the settings.

This will serve as your custom web URL for PAM360 from now on.

3. PAM360 is a web-based application that can be accessed via a web browser. Does that mean I can access it from anywhere?

PAM360 is an on-premise tool installed in a physical server or virtual machines (VM). You can access PAM360's web interface from any machine on the network connected to the same LAN network using the web browsers.

4. Can I change the IP address in which PAM360 application is binding when I have multiple NIC cards and IP's available in the server?

PAM360 comes bundled with a tailored version of TomCat webserver which allows users to access the webpage and also the JVM which performs the product operations. You can use the below steps to configure the Bind IP address for both these components.

Steps for changing webserver bind IP

1. Stop the PAM360 service.
2. Navigate to **<PAM360 installation folder>/conf** directory and take a backup of the file named **server.xml**.
3. Open Wordpad as an administrator and open **server.xml** under **<PAM360 installation folder>/conf** directory.
    i. Look for the **port="8282"** and add the entry **address="<IP addresses of the application server>"** next to it.
    ii. Save the file.
4. Start the PAM360 service. This time the Tomcat webserver will start using the bind IP that you have specified.

Steps for changing JVM bind IP

1. Stop the PAM360 service.
2. Navigate to **<PAM360 installation folder>/conf** directory and take a backup of the file named **wrapper.conf**.
3. Open Wordpad as an administrator and open **wrapper.conf** under **<PAM360 installation**

folder>/conf directory.

i. Look for the word **wrapper.app.parameter.1** and add the following line below **wrapper.app.parameter.1**.

- **wrapper.app.parameter.2=-Dspecific.bind.address=<IP addresses of the application server>**

ii. Save the file.

4. Now, rename **<PAM360 installation folder>/logs** folder to **logs_older** and start the PAM360 service.
5. Connect to the login page and try using the product features such as Password reset. The source IP for these operations will be the IP Address that you have configured.

5. What if my users are not notified of their PAM360 accounts?

In general, users are notified of their PAM360 accounts only through emails. If a user does not get the notification emails, verify:

- if you have configured the mail server settings properly, with the details of the SMTP server in your environment.
- if you have provided valid credentials as a part of mail server settings, as some mail servers require the same for mails to be received.
- if the '**Sender E-Mail ID**' is properly configured, as some mail servers reject emails sent without the From address or mails originating from unknown domains.

6. What are the authentication schemes available in PAM360?

You can use one of the following three authentication mechanisms out of PAM360:

- **Active Directory:** When enabled, the authentication request is forwarded to the configured domain controller and based on the result, the user is allowed or denied access into PAM360. The user name, password and the domain are supplied in the PAM360 login screen. This scheme works only for users whose details have been imported previously from AD, and is available only when the PAM360 server is installed on a Windows system.
- **LDAP Directory:** When enabled, the authentication request is forwarded to the configured LDAP directory server and based on the result, the user is allowed or denied access into PAM360. The username, password and the option to use LDAP authentication are supplied in the PAM360 login screen. This scheme works only for users whose details have been imported previously from the LDAP directory.

- **PAM360 Local Authentication:** The authentication is done locally by the PAM360 server. Irrespective of AD or LDAP authentication being enabled, this scheme is always available for the users to choose in the login page. This scheme has a separate password for users and the AD or LDAP passwords are never stored in the PAM360 database. However, for security reasons, we recommend that you disable the local authentication for users after enabling AD/LDAP authentication.
- **Azure AD:** Once you integrate PAM360 with Azure Active Directory (Azure AD) in your environment, you can allow users to use their Azure AD credentials to log in to PAM360 in both Windows and Linux platforms. To use this authentication, PAM360 should first be added as a native client application in your Azure AD portal.
- **Smartcard Authentication:** Enabling this feature will mandate users to possess a smartcard, and also know their Personal Identification Number (PIN). Note that smartcard authentication will bypass other first factor authentication methods like AD, LDAP or Local Authentication.
- **RADIUS Authentication:** You can integrate PAM360 with RADIUS server in your environment and use RADIUS authentication to replace the local authentication provided by PAM360. The users who will be accessing PAM360 using their RADIUS server credentials will have to be added as users in PAM360 first. When you do so, you need to ensure that the "username" in PAM360 is the same as the username used for accessing the RADIUS server.
- **SAML SSO:** PAM360 acts as the Service Provider (SP) and it integrates with Identity Providers (IdP) using SAML 2.0. The integration basically involves supplying details about SP to IdP and vice-versa. Once you integrate PAM360 with an IdP, the users have to just login to the IdP and then, they can automatically login to PAM360 from the respective IdP's GUI without having to provide the credentials again. PAM360 supports integration with Okta, AD FS, and Azure AD SSO.

Note:

For SAML SSO authentication, the **Assertion Consumer URL** is the hostname of the server, by default. To update the Assertion URL, follow the below steps:

1. Go to **Admin >> Settings >> Mail Server Settings**.
2. Under **Access URL**, update the required URL and click **Save**.

Now, the **Assertion Consumer URL** under **Service Provider Details** will be updated.

7. What are the user roles available in PAM360? What are their access levels?

PAM360 comes with five pre-defined roles:

- Privileged Administrator
- Administrators
- Password Administrator
- Password Auditor
- Password User

Apart from these default roles, any administrator can be promoted as a Super Administrator with the privilege to view and manage all the resources. Refer to the help section **Managing User Roles and Permissions** for details on the access levels of the default roles.

8. What if I forget my PAM360 login password?

> **Note: Show 'Forgot Password' option in the login screen** should be enabled under **Admin >> General Settings >> User Management.**

If you were already given a valid PAM360 account for Local Authentication,

1. Click the **Forgot Password?** link available in the login page to reset your password.
2. In the pop-up that appears,
    i. Enter the **Username** and the corresponding **Email Id**.
    ii. Click **Reset** to send a password reset link to the configure Email.
3. Open your email and find the email containing the password reset link and click on the link.
4. Now, PAM360 will send a **One Time Password** (OTP) to the configured email.
5. Use this **One Time Password** along with the **Username** and choose **Local Authentication** in the Domain name drop down menu to login.
6. PAM360 will prompt you to reset your password. Mention the One Time Password under **Old Password** and enter the **New Password.**
7. Click **Save.**

You have successfully reset your PAM360 password.

9. Why do I sometimes see a security warning while accessing the PAM360

console via the browser?

The PAM360 web console always uses the HTTPS protocol to communicate with the PAM360 server. The PAM360 server comes with a default self-signed SSL certificate, which the standard web browsers will not recognize, thereby issuing a warning. You can ignore this warning while you're testing or evaluating the product. However, if you're rolling it out in production, we recommend that you install an SSL certificate bought from an authorized Certificate Authority (CA) that is recognized by all standard web browsers.

3. Security

1. How secure are my passwords in PAM360?

Ensuring secure storage of passwords and offering solid defense against intrusion are the top priorities of PAM360. The following measures ensure high level security for your passwords:

- Passwords are encrypted using Advanced Encryption Standard (AES), and stored in the database. AES is currently the strongest encryption algorithm known, and has been adopted as an encryption standard by the U.S. Government.
- The database which stores all the passwords accepts connections only from the host that it is running on, and is not visible externally.
- Role-based, fine-grained user access control mechanism ensures that users can view and access passwords only based on the permissions granted to them.
- All transactions between the PAM360 console and the server take place through HTTPS.
- PAM360's in-built password generator helps you generate strong passwords.

2. How secure are Application-to-Application and Application-to-Database password management done through Password Management APIs?

PAM360 offers RESTful APIs and SSH-based CLI APIs that can be used for Application-to-Application/Database password management. The applications connect and interact with PAM360 through HTTPS. An application's identity is verified first by verifying the validity of its SSL certificate, and then by verifying the source IP/hostname in which it resides. Each application/database must be registered as an API User in PAM360. During this registration, the hostname/IP of the application server has to be supplied and a unique authentication token that uses the REST API will be generated. This token needs to be sent along with the API requests for authentication. In addition to these security checks, each application/database can only access the information that are explicitly delegated to them by an administrative user. Refer to the help section Sharing Individual Resources to know more about sharing/delegating passwords.

3. Can we install our own SSL certificates?

Yes, you can install your own SSL certificates. Follow the steps below:

1. Navigate to **Admin >> Configuration >> PAM360 Server**.
2. Choose the Keystore Type as **JKS, PKCS12** or **PKCS11** whichever you chose while generating the CSR.
3. Browse and upload the **Keystore File**.
4. Enter the same **Keystore Password**, you entered while generating the CSR.
5. Modify the **Server Port**, if required.
6. Hit **Save**. Restart the PAM360 service once, for the certificate change to take effect.

4. How to generate signed SSL certificates?
[OR]
How to make the PAM360 server trusted by web browsers and users?

PAM360 runs as a HTTPS service. It requires a valid CA-signed SSL certificate with the principal name as the name of the host on which it runs. By default, on first time startup, it creates a self-signed certificate, which will not be trusted by the user browsers. Thus, while connecting to PAM360, you need to manually verify the certificate information and the host name of PAM360 server carefully and should force the browser to accept the certificate.

To make the PAM360 server trusted by web browsers and users:

- Obtain a new signed certificate from a CA for the PAM360 host. **[OR]**
- Configure an existing certificate obtained from a CA with wild-card principal support for the PAM360 host.

There are different ways to generate the signed SSL certificates:

1. By using the **"Certificate Management"** module of PAM360.
2. By using the OpenSSL or Keytool (bundled with Java) to create your certificates, get them signed by a CA and use them with PAM360.
3. By installing a wild card certificate.

You can decide the mode of generating the signed SSL certificates based on what your security administrators recommend. The detailed steps for using each of the above methods are provided under the links below.

Note: If you already have a certificate signed by a CA, then we recommend using OpenSSL to create the keystore and configure it in PAM360 (steps 4 and 5 in the instructions below).

1. Generating Signed SSL certificates using the Certificate Management module of PAM360
2. Generating Signed SSL certificates using OpenSSL
3. Generating Signed SSL certificates using Keytool
4. Generating Signed SSL certificates by installing a wild card certificate

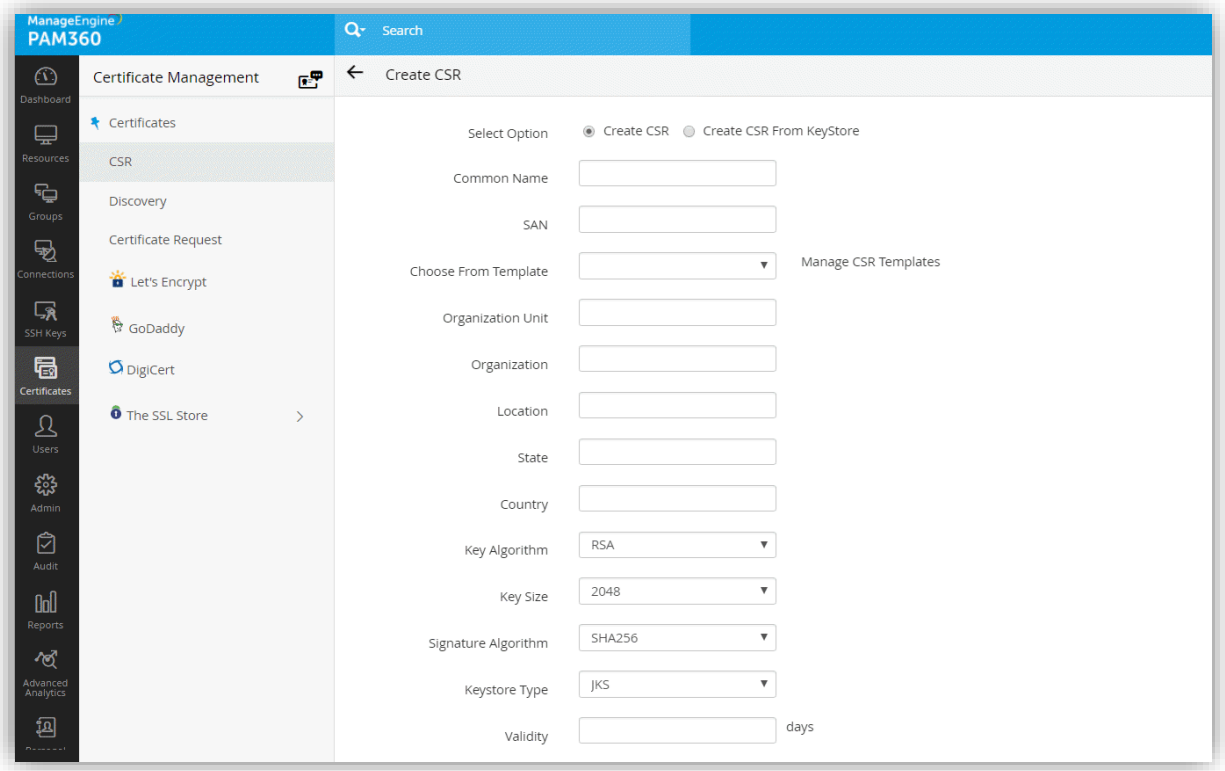
1. Generating Signed SSL certificates using the Certificate Management module of PAM360

You can generate signed SSL certificates through the Certificate Management module of PAM360 and also apply the certificate changes (Certificate Keystore) directly from the PAM360 console. This involves three processes:

1.1 Generating a Certificate Signing Request (CSR):

To request and acquire certificates from a Local CA through PAM360, you need to first generate a Certificate Signing Request (CSR). Here are the steps for the same:

1. Navigate to the **Certificates >> Create CSR**.
2. Click the **Create** button. The Create CSR page is displayed.
3. Select either of the options **Create CSR** or **Create CSR From KeyStore**, based on whether you want to create a new CSR or create a CSR from an already existing private key, respectively.
    i. If you have selected **Create CSR**, fill in the details, such as **Common Name, SAN, Organization Unit, Organization Location, State, Country, Key Algorithm and Key Size**. Select the **Key Algorithm** and **Keystore Type**. Enter the **Validity** and **Store Password**.



ii. If you have selected **Create CSR From KeyStore**, browse and attach the required private key file along with the Private Key Password.

4. Click the **Create** button. You will be redirected to a window where the CSR content is displayed. You can copy the CSR content or export it to a mailbox.
   - **Email** - Select this option to send the certificate file via email to the specified mail id.
   - **Export CSR / Private Key** - Select this option to export the CSR or the corresponding private key alone based on your requirement.
5. View the saved CSRs under **"Certificates >> Create CSR"**.

Note: The 'show passphrase' eye icon corresponding to each CSR allows the administrators to view the KeyStore passwords of the CSR files.

1.2 Signing the Certificate:

PAM360 provides the option to sign and issue certificates to all clients in your network either from your Microsoft Certificate Authority or using a custom root CA certificate that is trusted within your environment.

Note: Remember, you should have generated a valid Certificate Signing Request (CSR) before getting your certificate signed from the local CA. Refer to the above section 1.1 for generating a CSR.

Follow the below steps to sign the certificate:

1. Navigate to **"Certificates >> Create CSR"**.
2. Select the required CSR from the table and click **Sign** from the top menu.
3. In the pop-up window displayed, provide the name of the server that runs the internal certificate authority, CA Name and choose the certificate template based on your requirement. Click **Sign Certificate**. The CSR is signed now and the issued certificate can be viewed under **"Certificates >> Certificates"**.

1.3 Applying the Certificate Keystore for PAM360 web server:

To apply the certificate Keystore, first you need to create it.

1. Navigate to **"Certificates >> Certificates"**. Click the signed certificate link under the heading Common Name. In the certificate details page displayed, click the **Export** icon present at the top right corner of the screen. The certificate file will be downloaded to your local machine.
2. Now, navigate to **"Certificates >> Create CSR"**.
3. Click the **Import Certificate** icon corresponding to the CSR of the signed certificate. Browse and choose the certificate file downloaded in your local machine and click **Import**. Now, the certificate will be bonded with the private key to form a Keystore.
4. Now navigate back to **"Certificates >> Certificates"** and click the certificate link under the heading Common Name. In the certificate details page displayed, scroll down and click the **Export** link. This will download the certificate Keystore to your local machine.
5. The final step is to navigate to **"Admin >> Configuration >> PAM360 Server"** and do the following:
    i. Choose the Keystore Type as **JKS, PKCS12 or PKCS11**, whichever you chose while generating the CSR.
    ii. Browse and upload the **Keystore File**.
    iii. Enter the same **Keystore Password**, you entered while generating the CSR.
    iv. Modify the **Server Port**, if required.
    v. Hit **Save**. Restart the PAM360 service once, for the certificate change to take effect.

2. Generating Signed SSL certificates using OpenSSL

OpenSSL mostly comes bundled with the Linux distributions. If you are using the Windows server and do not have OpenSSL installed, download it from http://www.slproweb.com/products/Win32OpenSSL.html. Make sure the 'bin' folder under the OpenSSL installation is included in the 'PATH' environment variable.

2.1 Create the public-private key pair that will be used for the SSL handshake

1. Open the command prompt.
2. Execute **'openssl genrsa -des3 -out <privatekey_filename>.key 1024'**

   <privatekey_filename> is the filename you specify to store the private key.
3. You will be prompted to enter a pass-phrase for the private key. Enter **'passtrix'** or a pass-phrase of your choice. (Though it is not documented, Tomcat has issues with passwords containing special characters, so use a password that has only alpha characters)
4. A file will be created in the name **<privatekey_filename>.key** in the same folder.

2.2 Create a Certificate Signing Request (CSR) for submission to a certificate authority to create a signed certificate with the public key generated in the previous step

1. Execute **'openssl req -new -key <privatekey_filename>.key -out <certreq_filename>.csr'**
   - **<privatekey_filename>.key** is the one used in the previous step.
   - **<certreq_filename>.csr** is the filename you specify to carry the certificate creation request to the CA (certificate authority).
2. You will be prompted to enter a series of values that are part of the distinguished name (DN) of the server hosting PAM360.
3. Enter values as required. Importantly, for the **'Common Name'** supply the **fully qualified name of the server hosting PAM360** (with which it will be accessed through the browsers).
4. A file will be created in the name **<certreq_filename>.csr** in the same folder.

2.3 Submit the CSR to a Certificate Authority (CA) to obtain a CA signed certificate

Some of the prominent CAs are Verisign, Thawte, RapidSSL. Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA. This process usually takes a few days time and you will be returned your signed SSL certificate and the CA's root certificate as .cer files. Save them both in the same working folder where files from steps 1 and 2 are stored

2.4 Import the CA-signed certificate to a keystore

1. Open command prompt and navigate to the same working folder.

2. Execute **'openssl pkcs12 -export -in <cert_file>.cer -inkey <privatekey_filename>.key -out <keystore_filename>.p12 -name PAM360 -CAfile <root_cert_file>.cer -caname PAM360 -chain'**

   where,

   - **cert_file.cer** is the signed SSL certificate with the .cer extension.
   - **privatekey_filename.key** is the private key file with a .key extension.
   - **keystore_filename.p12** name is the keystore that will be generated with a .p12 extension.
   - **root_cert_file.cer** is the CA's root certificate with a .cer extension.
3. When prompted for a password, enter the same password, you used in **step 1** for the private key. This requirement is due to an inherent limitation in tomcat, which requires the two passwords to match.
4. Now, a keystore file in the name **<keystore_filename>.p12** will be generated in the same folder.

2.5 Configure the PAM360 server to use the keystore with your SSL certificate

This is the final step in generating Signed SSL certificates using OpenSSL.

1. Copy the **<keystore_filename>.p12** generated in step 4 to the **<PAM360_Install_Folder>\conf** folder.
2. Open command prompt and navigate to the **<PAM360_Install_Folder>\conf** folder.
3. Open the file **server.xml** and do the following changes:
   - Search for the entry **'keystoreFile'**, which will have the default value set to **'conf/server.keystore'**. Change the value to **'conf/<keystore_filename>.p12'**.
   - Starting from version 9700, the keystore password is encrypted and cannot be updated directly in the server.xml file.In order to manually update the keystore password in the .xml file, disable the encryption first, by changing the value**'keystorePassEncrypted=true'** to **'keystorePassEncrypted=false'**.
4. Now, set the value of **'keystorePass'** to **"passtrix"** or the password you specified in the previous step while creating the keystore.
5. Add a new entry **keystoreType= PKCS12** or **PKCS11** next to the keystorePass entry.
6. Save the **server.xml** file.
7. Restart the PAM360 server and connect through the web browser. If you are able to view the PAM360 login console without any warning from the browser, you have successfully installed your SSL certificate in PAM360.

3. Generating Signed SSL certificates using Keytool

3.1 Create the public-private key pair that will be used for the SSL handshake

1. Go to the **<PAM360_Home>/jre/bin** folder.
2. Execute the command:

   For Windows:

   .\keytool -genkey -alias PAM360 -keyalg RSA -sigalg SHA256withRSA -keypass <privatekey_password> -storepass <keystore_password> -validity <no_of days> -keysize 2048 -keystore <keystore_filename>

   For Linux:

   ./keytool -genkey -alias PAM360 -keyalg RSA -sigalg SHA256withRSA -keypass <privatekey_password> -storepass <keystore_password> -validity <no_of days> -keysize 2048 -keystore <keystore_filename>

   where,

   <keystore_password> is the password to access the keystore, <privatekey_password> is the password to protect your private key. Note that due to an inherent limitation in tomcat, **these two passwords have to be the same.** (Though it is not documented, Tomcat has issues with passwords containing special characters, so use a password that has only alpha characters) **<no_of_days>** is the validity of the key pair in number of days, from the day it was created
3. The above command will prompt you to enter details about you and your organization.
   - For the **'first and the last name'**, enter the **FQDN** of the server where PAM360 is running.
   - For other fields, enter the relevant details.
4. A keystore file will be created in the name **<keystore_filename>** in the same folder, with the generated key pair.

3.2 Create a Certificate Signing Request (CSR) for submission to a certificate authority to create a signed certificate with the public key generated in the previous step

1. Go to the **<PAM360_Home>/jre/bin** folder.
2. Execute the command: **"keytool -certreq -keyalg RSA -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -file <csr_filename> -keystore <keystore_filename> -ext san=dns:<hostname.domain.com>,dns:<hostname>,dns:<alias.domain.com>"**.

> **Note**: The **<csr_filename>** that you choose should have the .csr extension.

3. A CSR file in the name **<csr_filename>** will be created in the same folder.

3.3 Submit the CSR to a Certificate Authority (CA) to obtain a signed certificate

Some of the prominent CAs are Verisign, Thawte, RapidSSL. Check their documentation / website for details on submitting the CSRs. Please note that this is a paid service. This process usually takes a few days of time. You will receive your signed SSL certificate and the CA's certificate as .cer files. Save both the files in the **<PAM360_Home>/jre/bin** folder.

3.4 Import the CA-signed certificate to the PAM360 server

1. Go to the **<PAM360_Home>/jre/bin** folder using command prompt.
2. If you have a single file as the certificate bundle(p7b), then run the below command:

   "keytool -import -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -keystore <keystore_filename> -trustcacerts -file <your_ssl_bundle.p7b>"

   where,

   - **<boundlessness>** is the certificate bundle obtained from the CA, a .p7b file saved in the previous step. The **<privatekey_password>,<keystore_password>** and **<keystore_filename>** are the ones used in the previous steps.
   - If you have 3 files, the root, the intermediate and the actual certificates in .cer format, then you need to import each one of them using the below commands.
     - **"keytool -import -alias root -keypass <privatekey_password> -storepass <keystore_password> -keystore <keystore_filename> -trustcacerts -file <rooter>"**
     - **"keytool -import -alias inter -keypass <privatekey_password> -storepass <keystore_password> -keystore <keystore_filename> -trustcacerts -file <inter.cer>"**
     - **"keytool -import -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -keystore <keystore_filename> -trustcacerts -file <your_ssl_cert.cer>"**
3. Now, copy the **<keystore_filename>** to the **<PAM360_Home>/conf** folder.

3.5 Configure the PAM360 server to use the keystore with your SSL certificate

This is the final step in generating Signed SSL certificates using Keytool.

1. Go to the **<PAM360_Home>/conf** folder.
2. Open the file **server.xml**.

3. Search for the entry **'keystoreFile'**, which will have the default value set to **"conf/server.keystore"**. Change the value to **"conf/<keystore_filename>"**, where **<keystore_filename>** is the one used in the previous steps.
4. Starting from **version 9700**, the keystore password is encrypted and cannot be updated directly in the server.xml file. In order to manually update the keystore password in the.xml file, disable the encryption first, by changing the value **'keystorePassEncrypted=true' to 'keystorePassEncrypted=false**.

> **Note:** This step is applicable only if you're using the **version 9700 or above.**

5. Set the value of **'keystorePass'** to **"passtrix"** or the password you specified in the previous step while creating the keystore.
6. Restart the PAM360 server and connect through the web browser. If you are able to view the PAM360 login console without any warning from the browser, you have successfully installed your SSL certificate in PAM360.

> **Note:** Tomcat, by default, accepts only the JKS (Java Key Store) and PKCS #12 format keystores. In case, the keystore is of PKCS #12 format, include the following option in the **server.xml** file along with the keystore name, keystoreType="PKCS12? This notifies tomcat that the format is PKCS12. Restart the server after this change.

4. Generating Signed SSL certificates by installing an existing wild card supported SSL certificate:

1. Go to the **<PAM360_Home>/conf** folder.
2. Open the file **server.xml.**
3. Search for the entry **'keystoreFile'**, which will have the default value set to **"conf/server.keystore"**. Change the value to **"conf/<keystore_filename>"** where **<keystore_filename>** belongs to the existing wild-card certificate.
4. Also search for the entry **'keystorePass'** (found next to the keystoreFile), which will have the default value set to **"passtrix"**. Change the value to **"<keystore_password>"**, where **<keystore_password>** protects the existing wild-card certificate keystore.
5. Restart the PAM360 server and connect through the web browser console. If you are able to view the PAM360 login console without any warning from the browser, you have successfully installed your SSL certificate in PAM360.

Note: Please refer your CA's documentation for more details and troubleshooting.

5. Can we create server certificates with SubjectAlternativeName (SAN)?

Yes, you can create a certificate using SAN with an alias name and apply it in PAM360. Follow the below steps:

1. Creating a CSR using PAM360's SSL certificate management module, and submitting it to any CA for signing

1.1 Create a Certificate Signing Request (CSR)

1. Login to PAM360 as an administrator.
2. Navigate to **Certificates >> Create CSR**.
3. Click on the **'Create'** button.
4. Here, provide a **name** for your certificate.
5. The Subject Alternative Name (SAN) will be auto-filled when you click on it after providing the common name. You can include additional SANs in the text field.
6. Provide the other details including your **organization details, location, validity, and a password**.
7. Click on **'Create'**.
8. Once done, you will find the option to export the certificate and the private key, or send the CSR to an email address that you specify.

1.2 Submit the CSR to a Certificate Authority (CA) to obtain a CA signed certificate

After creating the CSR, the next step is get the CSR verified and signed by a CA. There are two options to do this:

1. You can export the CSR file and manually send it to a third party CA to get it signed.
2. You sign and issue certificates to all clients in your network either from your Microsoft Certificate Authority or using a custom root CA certificate that is trusted within your environment. To do this, navigate to Certificates >> Create CSR, select a certificate, and click on 'Sign'. Refer to the help section Certificate Signing for more details on certificate signing.

Once signed, you can view the certificate under 'Certificates'.

1.3 Import the CA-signed certificate to the PAM360 server

To import the certificates in your network:

1. Navigate to the **Certificates**.
2. Click on **'Add'**.
3. Choose the required option:
   i. **File Based Certificate"** Browse and import the required certificate file directly from your system.
   ii. **Content Based Certificate"** Copy the content of the required certificate file and paste it in the text box.
   iii. **Keystore Based"** Import all individual certificates available in keystore simultaneously. Upload the required keystore file and enter its corresponding password (if any).
4. Click on the **'Add'** button.

2. Creating a certificate with SAN using Microsoft internal CA

Make sure you follow the below mentioned steps to create server certificate with SubjectAlternativeName using Microsoft Internal CA. Also, in Additional Attributes, specify the 'san:dns=<The URL which you use to access PAM360>', and then try creating the certificate.

1. Connect to the server where Microsoft Certificate Service is running.
2. Open a command prompt and execute certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
3. Then, restart Microsoft Certificate Service(certsvc).
   Create the private key using the below command,"./keytool -genkey -alias PAM360 -keyalg RSA -keypass <privatekey_password> -storepass <keystore_password> -validity <no_of days> -sigalg SHA256withRSA -keysize 2048 -keystore <keystore_filename>"
4. Here, when it prompts for first and last name, specify the name which you use to access PAM360.
5. Create the Certificate Signing Request(CSR) using the below command: 'keytool -certreq -keyalg RSA -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -file <csr_filename> -keystore PAM360.keystore'
   i. Submit CSR request to Microsoft Internal CA:
   ii. Open IE and go to your CA's certificate request page.
   iii. Request advanced certificate.
   iv. Submit a certificate request.
   v. Copy and paste content of <csr_filename>.cer file.
   vi. Certificate template should be Web Server.

vii. In "Additional Attributes", enter 'san:dns=passwordmanager&dns=passwordmanager.tcu.ad.local' and click on 'Submit'.

viii. Download the certificate chain in base64 format as PAM360cert.p7b.

6. Import the downloaded 'PAM360cert.p7b' file into the PAM360.keystore "keytool -import -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -keystore PAM360.keystore -trustcacerts -file PAM360cert.p7b"

Notes:

1. If you receive the error message "Failed to establish chain from reply" with the above command, it means the root and intermediate certs of your CA are not available in the trusted store of the PAM360. So, before importing the actual certificate, you have to import the root certificate with a different alias and then import the actual certificate. Also, if you have multiple root certificates, then you have to import them one by one with the different alias names.

   For example,

   ./keytool -import -alias root1 -keypass Password123 -storepass Password123 -keystore PAM360.keystore -trustcacerts -file root1.cer
   ./keytool -import -alias root2 -keypass Password123 -storepass Password123 -keystore PAM360.keystore -trustcacerts -file root2.cer

   Based on the number of root or intermediate root certificates, you have to execute the above command with different alias names and then continue with the actual certificate.

2. The actual certificate should be in .cer or .crt format.

7. Applying the certificate keystore in PAM360.

   i. Login to PAM360 as an administrator.

   ii. Navigate to Admin >> Configuration >> PAM360 Server.

   iii. Choose PKCS12 or PKCS11 as the Keystore Type.

   iv. Click on 'Browse' and select your PFX/P12 file.

v. Provide the correct keystore password and save the configuration.

vi. Restart PAM360 service to bring the certificate change into effect.

3. Creating certificate with SAN signed by third party vendor like GoDaddy, Verisign, Commodo, etc.

Make sure you follow the below mentioned steps to get SAN certificate signed from the third party vendors.

1. Create the private key using the below command,

   './keytool -genkey -alias PAM360 -keyalg RSA -keypass <privatekey_password> -storepass <keystore_password> -validity <no_of days> -sigalg SHA256withRSA -keysize 2048 -keystore <keystore_filename>"'

   Here, when it prompts for first and last name, specify the name which you use to access PAM360.

2. Create the Certificate Signing Request(CSR) using the below command:

   'keytool -certreq -keyalg RSA -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -file <csr_filename> -keystore PAM360.keystore'

3. Submit CSR request to third party signing tool and ensure to get the certificate signed using SAN name. Download the certificate chain in base64 format as PAM360cert.p7b
4. Import the downloaded 'PAM360cert.p7b' file into the PAM360.keystore keytool -import -alias PAM360 -keypass <privatekey_password> -storepass <keystore_password> -keystore PAM360.keystore -trustcacerts -file PAM360cert.p7b

Note: If you receive the error message "Failed to establish chain from reply" with the above command. Then, the root and intermediate certs of your CA are not available in the trusted store of the PAM360. So, before importing the actual certificate, you have to import the root certificate with a different alias and then the actual certificate. Also, if you have multiple root certificates, then you have to import them one by one with different alias names.

For example,

./keytool -import -alias root1 -keypass Password123 -storepass Password123 -keystore PAM360.keystore -trustcacerts -file root1.cer
./keytool -import -alias root2 -keypass Password123 -storepass Password123 -keystore PAM360.keystore -trustcacerts -file root2.cer

Based on the number of root or intermediate root certificates, you have to execute the above command with different alias names and then continue with the actual certificate.

5. Applying the certificate keystore in PAM360.
   i. Login to PAM360 as an administrator.
   ii. Navigate to **Admin >> Configuration >> PAM360 Server**.
   iii. Choose **PKCS12** or **PKCS11** as the Keystore Type.
   iv. Click on **Browse** and select your PFX/P12 file.
   v. Provide the correct keystore password and save the configuration.
   vi. Restart PAM360 service to bring the certificate change into effect.

4. Password Synchronization

1. Can I change resource passwords from the PAM360 console?

Yes. PAM360 can remotely reset the passwords of various end points. PAM360 supports both agent-based and agent-less modes of changing passwords. Refer to the help section Remote Password Reset for more information.

2. When do I use the agent and agent-less modes for password synchronization?

Let us first look at the requisites for both the modes:

The agent mode requires the agent to be installed as a service in each end point and run with administrative privileges to perform password reset operations. The agent uses one-way communication using outbound traffic to reach the PAM360 server.

For the agent less mode, you must supply administrative credentials to perform the password changes. For Linux, you must specify two accounts- one with root privileges and the other with normal user privileges that can be used to login remotely. Telnet or SSH service must be running on the resources. For Windows domain, you must supply the domain administrator's credentials. For Windows and Windows Domain, PAM360 uses remote calls, so relevant ports must be open on the resource.

Based on this, you can choose which mode you want for your environment, indicated by the following tips:

Choose the agent mode when:

- You do not have administrative credentials stored for a particular resource in PAM360,
- You do not have the required services running on the resource (Telnet / SSH for Linux, RPC for Windows),
- You run PAM360 in Linux and want to make password changes to a Windows resource.

Choose agent less mode in all other cases as it is a more convenient and reliable way of doing password changes.

3. Can I enable agent less password reset if I add my own resource type for other distributions of Linux / other versions of Windows?

Yes, you can. As long as your resource type label contains the string 'Linux' or 'Windows', you can still configure agent less password reset for those resources.

Example of valid resource type labels to enable password reset:

Debian Linux, Linux - Cent OS, SuSE Linux, Windows XP Workstation, Windows 2003 Server

4. Is there a way to carry out remote password synchronization for custom resource types that do not come out of the box in PAM360?

PAM360 supports remote password reset for custom resource types through SSH command sets, password reset plugins, and password reset listeners.

- **SSH Command Sets:** For SSH-based devices, you can build command-based executables directly from PAM360 using a set of default or customized SSH commands. These command sets can then be associated with the respective SSH

device accounts that do not come out of the box with PAM360 to perform their password resets without the need for a CLI.

- **Password Reset Plugin:** You can build your own implementation class and run it via PAM360 to enforce automatic password resets of custom resource types. With the plugin, you can also leverage access control for legacy accounts and automatically reset passwords instantly upon usage. This way, the passwords of these accounts will serve as one-time passwords that are reset after every use via the associated plugin.
- **Password Reset Listeners:** Listeners are custom scripts or executables that can be invoked for local password changes, as well as to reset the passwords of custom resource types for which remote password reset is not supported out-of-the-box by PAM360. You can configure listener scripts individually for each resource type including the custom ones.

5. How do I troubleshoot when password reset does not happen?

In the agent mode:

- Check if the agent is running by looking at the Windows active process list for the entry 'PAM360Agent.exe' or the presence of a process named 'PAM360Agent' in Linux.
- Check if the account in which the agent is installed has sufficient privileges to make password changes.

In the agent less mode:

- Check if the right set of administrative credentials have been provided and the remote synchronization option is enabled.
- Check if the necessary services are running on the resource (Telnet / SSH for Linux, RPC for Windows).
- Check if the resource is reachable from the PAM360 server using the DNS name provided.

6. How do I reset domain passwords when Windows domain password reset fails with an error message: "The authentication mechanism is unknown"?

This happens when PAM360 is run as a Windows service and the 'Log on as" property of the service is set to the local system account. Change it to any domain user account to be able to reset domain passwords. Follow the instructions below to effect that setting:

1. Go to the Windows Services Applet (from **Control Panel >> Administrative Tools >> Services**).
2. Select the 'ManageEngine PAM360' service, right-click >> choose 'Properties'.

3. Click the 'Log On' tab and choose 'This Account' radio button and provide the username and password of any domain user - in the format <domainname>\<username>.
4. Save the configuration and restart the server.

7. What are the prerequisites for enabling Windows Service Account Reset?

Before enabling windows service account reset, ensure if the following services are enabled in the servers where the dependent services are running:

- Windows RPC service should have been enabled.
- Windows Management Instrumentation (WMI) service should have been enabled.

8. Does domain SSO work across firewalls / VPNs?

The domain Single Sign On (windows integrated authentication) is achieved in the Windows environment by setting non-standard parameters in the HTTP header, which are usually stripped off by devices like firewalls / VPNs. PAM360 is designed for use within the network. So, if you have users connecting from outside the network, you cannot have SSO this enabled.

5. Backup and Disaster Recovery

1. Can I move PAM360 from one server to another?

Yes. you can migrate PAM360 to another server by following the below steps:

1. Stop PAM360 service, exit tray icon.
2. Make sure that the Postgres process is not running in Task Manager.
3. Copy and move entire PAM360 directory to the new server.
4. Open command prompt with admin rights and navigate to <PAM360 HOME>\bin directory. Execute the command PAM360.bat install. (This will install PAM360 service.)
5. Move the encryption key(PAM360_key.key) to the new server and specify the correct location of it in PAM360/conf/manage_key.conf file. Refer to the help section Managing PAM360 Encryption Key for more information about the encryption key.
6. Go to services console, provide a service account and start PAM360 service.
7. If you want the tray icon, go to the <PAM360 HOME>, right click on PAM360.exe and select "Run as Administrator".
8. Now you should be able to access the PAM360 web page using the new server name in the URL.

2. Can I setup disaster recovery for the PAM360 database?

Yes, you can. PAM360 can periodically backup the entire contents of the database, which can be configured through the PAM360 console. Refer to the help section Database Backup (PostgreSQL) for more details.

3. Where does the backup data get stored? Is it encrypted?

All sensitive data in the backup file are encrypted using the **7-Zip** utility, which has options to encrypt and compress data by the **AES256** algorithm. The encrypted data is stored under the **'<PAM360_Install_Directory/backUp>'** directory as a .zip file. We recommend you to store the backup in secure, secondary storage for disaster recovery.

6. Licensing

1. What is the Licensing Policy for PAM360?

There are three license types:

1. **Evaluation download / Trial Version** - You can straightaway download and install this trial version. It is fully functional, capable of supporting a maximum of 5 administrators and you can evaluate all the features for 30 days.
2. **Free Edition** - Licensed software that allows you to have **1 administrator** and manage up to **10 resources**. Valid forever.
3. **Registered Version** - You get the Enterprise edition, and Licensing is based on the Number of Administrators. This is useful if you require more enterprise-class features such as auto discovery of privileged accounts, integration with ticketing systems and SIEM solutions, jump server configuration, application-to-application password management, out-of-the-box compliance reports, SQL server / cluster as backend database, etc.

Note: PAM360 comes with five user roles - Administrator, Password Administrator, Privileged Administrator, Password Auditor and Password User. The term 'administrator' denotes Administrators, Password Administrators and Privileged Administrators. So, licensing restricts the number of administrators as a whole, which includes Administrators, Password Administrators and Privileged Administrators. There is no restriction on the number of Password Users and Password Auditors. To get more details on the five user roles, refer to the help section Managing User Roles and Permissions for more information.

2. Can I buy a permanent license for PAM360? What are the options available?

Though PAM360 follows an annual subscription model for pricing, we also provide perpetual licensing option. The perpetual license will cost three times the annual subscription price, with 20% AMS from the second year. Contact sales@manageengine.com for more details.

3. How can I apply my license file?

1. Login as an administrator in the PAM360 web interface. Click the 'My Account' icon at the top right corner and select License from the drop down.
2. Browse to add the license file and click on Upgrade. Your new license file is added.
3. Now, restart the PAM360 service for the license to take effect. You can check to see if the license is applied and other details under the same section.

4. I want to have a High Availability setup with multiple servers. Will a single license suffice for this?

Yes, if you buy a single license, you are entitled to have the High Availability setup. You can apply the same license on the Primary as well as the Secondary servers. Follow the below steps:

1. Stop the PAM360 service in the Primary server.
2. Login PAM360 using the Secondary server URL as an **Administrator**.
3. Tap **License** under the **User** menu, at the top right corner of the console.
4. Update the same license file which you applied for the Primary server.

5. Can PAM360 support more than 1000 administrators?

Yes, very much. If you want a license with more than 1000 administrator users, please contact sales@manageengine.com for more details.

6. Can I extend my evaluation to include more administrator users or for more number of days?

Yes. Fill in the required details in the website and we will send you the license keys.

7. SSH Key Management

1. Are there any differences in the way SSH user accounts and SSH service accounts are managed using PAM360?

No, PAM360 adopts the same approach for managing SSH user accounts and SSH service accounts. The only difference is that during resource discovery, if service / root account credentials are provided to establish connection with the resource, you acquire extended privileges to import and manage keys from all user accounts in the resource.

Whereas, when connection to the resource is established using user account credentials, you get key management privileges only for SSH keys present in that particular account.

2. Is there any way to view SSH keys that were not rotated?

Yes. We have a dashboard that displays the number of keys that were not rotated for the predefined time period as specified in the notification policy.

3. Does PAM360 support management of digital keys other than SSH keys and SSL certificates?

PAM360 houses a key vault called "Key Store" which facilitates the storage and management of any type of digital key. However, the option to discover and import is limited to SSH keys and SSL certificates only, and isn't available for other types of digital keys.

8. SSL Certificate Management

1. Is there any certificate type that PAM360 is incompatible with?

No. PAM360 supports all X.509 certificate types.

2. Is it possible to automatically identify and update the latest version of certificates in PAM360' certificate repository?

Yes. You can create scheduled tasks to perform automatic certificate discovery through which you can import and replace old certificates from target systems with their updated versions in PAM360' certificate repository. Refer to the help section Managing SSH/SSL Schedules for a detailed explanation on creating schedules.

3. Does the Linux version of PAM360 support certificate discovery from Active Directory and MS Certificate Store?

No, it doesn't. The AD User Certificate and MS Certificate Store tabs appear only in the Windows version of PAM360.

4. Is it possible to track the expiry of certificates with the same common name in PAM360' certificate repository?

PAM360 differentiates certificates by their common names and records certificates with same common names as a single entry in its certificate repository. We've designed it this way because PAM360 licensing is based on the number of certificates and we don't want customers to spend many license keys for the same certificate.

However, if there's a need to manage both the certificates separately, you can do so by listing them as separate entries in PAM360' certificate repository. Once listed, the newly added certificate will be counted for licensing.

To add a certificate with the same common name as a separate entry in certificate repository,

1. Navigate to the **Certificates** tab and click **Certificates**, and click the **Certificate History** icon beside the certificate.
2. Click the **'Certificate Settings'** icon beside the required version of the certificate and click on **'Manage Certificate'**.
3. The selected version is listed as a separate certificate in the certificate repository.
4. In case you want to manage only one version of the certificate, click **'Certificate Settings'** icon beside the required version and choose 'Set as current certificate' option.

5. How do I import private key for a certificate?

Follow the steps below to import a certificate's private key into PAM360.

1. Navigate to the **Certificates** tab and click **Certificates**.
2. Select the certificate for which you need to import the private key.
3. Click the **Import Keys** option from the **More** drop down menu at the top.

Browse for the file that contains the private key, enter the keystore password, and click on 'Import'. The private key will be imported and attached to the selected certificate.

6. How do I deploy a certificate to Certificate Store and map it to the application that uses the certificate?

PAM360 facilitates certificate deployment through which you can deploy certificates from its repository to target server's Microsoft Certificate Store.

Refer to the help section Deploying SSL Certificates to Target Web Servers for step-by-step explanation on certificate deployment.

To map the certificate to its corresponding application, you've to manually restart the server on which the application is running for the change to take effect.

7. Does PAM360 support subnet based certificate discovery?

No. PAM360 currently doesn't support subnet based SSL certificate discovery.

8. Does PAM360 support automatic scheduling for certificate discovery from MS Certificate Store?

No. Currently, PAM360 doesn't support automatic scheduling for certificate discovery from MS Certificate Store.

9. Are certificate related alert emails generated for all versions of a certificate (the ones that show in "Certificate History" also) or only for those certificates listed in PAM360's certificate repository?

Email notifications are generated ONLY for certificates listed in PAM360's certificate repository and NOT for different versions of a certificate displayed in "Certificate History" section.

10. Are the certificates issued by the company's internal Certification Authority (CA) counted for licensing?

Yes. All types of SSL certificates, SSH keys and any other digital key being managed using PAM360 are taken into account for licensing. There's a dashboard widget "License Details" that provides insights on the type and number of digital identities being managed using PAM360 that will be taken into account for licensing.

11. How do I import a root certificate into PAM360?

To import a root certificate, open the Command Prompt and navigate to the **<pam360_server_home>\bin** directory and execute the following command:

For Windows:

importCert.bat <Absolute Path of certificate>

For Linux:

importCert.sh <Absolute Path of certificate>

9. Policy-Based Access Privilege - Zero Trust Approach

1. What are the agent types concerning the Zero Trust approach?

Two agent types are relevant to the zero trust approach: "User Device" and "Resource". These agents are installed on user devices and resources, respectively, and their operation depends on the type of parameters being fetched for the trust score calculation.

2. How does the agent work for user devices and resources?

The agent works by fetching the data from the user device/resource, such as firewall status, antivirus status, open ports, processes/services running, application/packages installed, etc., that can be used to calculate the trust score for the user/resource. This score is then used to determine whether the user/resource meets the required criteria for privileged access and account governance.

3. Will the device installed with the PAM360 agent of usage type 'user device' be added as a resource in PAM360?

No, the user device installed with a PAM360 agent of usage type '**User Device**' will not be added as a resource in PAM360. The devices installed with the agent of usage type 'Resources', will only be added as a resource in PAM360.

4. Can I use the policy-based access privilege feature in an agentless mode?

Yes, you can use the policy-based access privilege feature in an agentless mode with only the authentication parameters defined for the users.

5. How to fetch the default system data from a user device/resource?

By default, all the devices/resources in an organization will be configured with a set of open ports, browser plugins/add-ons, applications/packages, and processes and services. To find out the respective details from a device/resource in an organization for configuring the relevant score parameter, do the steps that follow:

1. Download this zip file and extract it to any of the desired devices.
2. Open the respective folder **Windows** or **Linux** based on your Operating System (OS) where you have extracted the zip.
3. Execute the bash/ sh/ bat/ ps1 file '**fetch_configuration_details**' with the run as administrator privilege.
4. Upon execution, an output file with the name '**query_result.txt**' is generated in the same folder location.
5. Open the **query_result.txt** file to check for the default device data or system properties for defining the respective score parameter. Use the search option to search the value of the respective parameter with the relevant below ids:
    i. Antivirus_status
    ii. Application_and_packages
    iii. Chrome_extensions
    iv. Disk_encryption_status
    v. Firefox_addons
    vi. Firewall_status
    vii. OS_version
    viii. Open_ports
    ix. Process_and_services
    x. Secure_boot_status

6. How do you decide a weightage value for a parameter for the trust score validation?

The weightage values for each parameter in the trust score validation are defined on a scale of 0-10 according to the organization's priority. Depending on your importance over each parameter, you can fix a weightage value. For example, if you need to monitor the invalid sign-

in attempts strictly and do not have any importance over the OS version, you can give a weightage of 10 to the invalid sign-in attempts and a value of around 2-5 for the OS version.

7. How does the user trust score and the resource trust score calculated?

The user trust score is calculated based on the user's authentication and user device state, whereas the resource trust score is determined based on the resource state, both using their respective parameter configuration and weightage defined by the administrator.

8. What is the purpose of an access policy?

An access policy plays a crucial role in automatically granting/restricting access privileges to resources based on criteria such as user trust score, resource trust score, password policy, and access control defined by the administrator.

9. How many access policies can a user and a resource be associated with?

A user can be associated with one or more access policies through various conditions for multiple resources. A resource can be associated with multiple access policies via different static resource groups. However, only one access policy that was recently associated will be active for the resource.

10. When does a conflict happen in policy-based access privilege?

Conflict occurs in policy-based access privilege when a resource is associated with multiple access policies via different static resource groups.

11. If there are multiple access policies associated with a resource via various static groups, what will be the intended active access policy of a resource?

In this scenario, the most recently associated access policy with the resource via a static resource group is intended to be the active access policy for that resource.

12. How to resolve a conflict between the access policies of a resource?

1. Navigate to the **Groups** tab.
2. Click on the **Actions** icon beside the respective static resource group.
3. Select the option **Edit Group Attributes**.

4. In the pop-up that appears, select the respective access policy in the **Access Policy** field that is to be associated with the resource group.
5. Click **Save** to apply the changes.

13. How does the precedence of the actions work in the access policy conditions?

If you have an access policy with multiple conditions that have varying criteria and actions for the same user, the privileged access calculation for that access policy will always consider the action from the condition that has the higher precedence value. **E.g.**, Deny/terminate, Exclude User Group.

14. Where can I see the user trust score?

The **Users** tab will display the trust scores of each user in PAM360. The users with the password user, password auditor, connection user, or password administrator roles will not be able to view the user trust scores or receive notifications about them. Only those with the privileged administrator, administrator, and custom user roles will be able to view the trust scores of all the users in the **Users** tab.

15. Where can I see the resource trust score?

The **Resources** tab displays resource trust scores next to their respective resources. Only users who own or manage a resource can see its trust score. However, super administrators in PAM360 can view the trust scores for all resources.

16. What are the possible reasons for the session termination?

While using a session, either the user trust score or the resource trust score may decrease if the user or resource violates the predefined parameters set by the administrators. If your session is terminated, you can reach out to your administrator to obtain more information regarding the reason for the termination.

PAM360 MSP Edition - Getting Started

ManageEngine PAM360 is also available in MSP edition, which has been specially designed taking into consideration the requirements of the Managed Service Providers. If you are an MSP wishing to manage the administrative passwords of your clients separately from a single management console or offer password management services to them, you can leverage the MSP edition.

Passwords can be securely shared between MSP administrators and their respective customers, making sure that users only get access to the passwords they own or ones that are shared with them. The solution offers the flexibility to entrust the control of the password vault to the MSP administrator, the end user or both, as desired.

The MSP edition also follows the basic password entitlement model of PAM360 which means, at any time, one will be able to view only the passwords that are owned and shared. As MSP admin, while you will be able to view the names of the organizations you manage, you will be able to view the data pertaining to all your customers only if you add their resources or if they share the resources with you. Your customers will be able to view the data belonging to their organization only.

This document walks you through the following topics:

1. Prerequisites
2. Installation Steps
3. Silent Install
    3.1 In Windows
    3.2 In Linux
4. Adding Users
5. Adding Organizations
    5.1 Adding Client Organizations
    5.2 Adding Organizations Manually
    5.3 Importing Organizations from CSV
    5.4 Replicating Settings Across Client Orgs
6. Granting Privilege to Manage Organizations
7. MSPOrg
    7.1 Frequently Asked Questions

1. Prerequisites

1. For testing the MSP edition, you need to deploy a separate machine. If you try to install the MSP edition in the same machine where PAM360 is running, it will uninstall the

existing PAM360 instance.

2. Download and install the **ManageEngine_PAM360_MSP.exe**

2. Installation Steps

Refer to the help section Installing PAM360 for the detailed step-by-step procedure.

3. Silent Install

A silent install is used to install an application without the need to interact with the UI. This type of installation is helpful for applications with limited installation steps. Before commencing the silent install, certain parameters such as Name, EmailId, Path, etc., are automatically set or manually entered. Execute the commands as instructed below to install the application automatically.

3.1 Steps to Silent Install PAM360 in Windows Server

3.1.1 Primary Server

1. Download the file ManageEngine_PAM360_MSP_64bit.exe.
2. Download the installation file WindowsPrimaryMSP.iss.
3. Open **WindowsPrimaryMSP.iss** file in Notepad and edit **Name, MailId, Phone, Company, Country**, and save.
4. Move **WindowsPrimaryMSP.iss** file to **C:\Windows**.
5. Open Command Prompt as an administrator and navigate to the **ManageEngine_PAM360_MSP_64bit.exe** file location.
6. Execute the command:

   ManageEngine_PAM360_MSP_64bit.exe -a -s -f1"C:\Windows\WindowsPrimaryMSP.iss" -f2"C:\Windows\WindowsPrimaryMSP.log"

PAM360 will get installed, and the service will start automatically.

3.1.2 Secondary Server

1. Download the file ManageEngine_PAM360_MSP_64bit.exe.
2. Download the installation file WindowsSecondaryMSP.iss.
3. Move **WindowsSecondaryMSP.iss** file to **C:\Windows**.
4. Open Command Prompt as administrator and navigate to the **ManageEngine_PAM360_MSP_64bit.exe** file location.

5. Execute the command:

   ManageEngine_PAM360_MSP_64bit.exe -a -s -f1"C:\Windows\WindowsSecondaryMSP.iss" -f2"C:\Windows\WindowsSecondaryMSP.log

PAM360 will get installed, and the service will start automatically.

3.1.3 Steps to Uninstall PAM360 in Windows Server

1. Download the uninstallation file WindowsUninstallMSP.iss.
2. Move **WindowsUninstallMSP.iss** file to **C:\Windows\.**
3. Open Command Prompt as administrator and navigate to the **ManageEngine_PAM360_MSP_64bit.exe** file location.
4. Execute the command:

   ManageEngine_PAM360_MSP_64bit.exe -a -s -f1"C:\Windows\WindowsUninstallMSP.iss" -f2"C:\Windows\WindowsUninstallMSP.log"

PAM360 will get uninstalled.

3.2 Steps to Silent Install PAM360 in Linux Server

3.2.1 Primary Server

1. Download the file ManageEngine_PAM360_MSP_64bit.bin for Linux.
2. Download the installation file LinuxPrimaryMSP.txt.
3. Open **LinuxPrimaryMSP.txt** in notepad.
4. Mention the user installation directory's path (**USER_INSTALL_DIR**) and file overwrite's (**-fileOverwrite_**) path.
5. Save and move **LinuxPrimaryMSP.txt** to home directory.
6. Open the Console and navigate to **ManageEngine_PAM360_MSP_64bit.bin** file location
7. Execute the command:

   chmod a+x ManageEngine_PAM360_MSP_64bit.bin

8. Execute the command:

   ./ManageEngine_PAM360_MSP_64bit.bin -i silent -f /home/LinuxPrimaryMSP.txt

PAM360 will get installed.

3.2.2 Secondary Server

1. Download the file ManageEngine_PAM360_MSP_64bit.bin for Linux.
2. Download the installation file LinuxSecondaryMSP.txt.
3. Open **LinuxSecondaryMSP.txt** in notepad.
4. Mention the user installation directory's path (**USER_INSTALL_DIR**) and file overwrite's (**-fileOverwrite_**) path.
5. Save and move **LinuxSecondaryMSP.txt** to home directory.
6. Open the console and navigate to**ManageEngine_PAM360_MSP_64bit.bin** file location
7. Execute the command:

   chmod a+x ManageEngine_PAM360_MSP_64bit.bin

8. Execute the command:

   ./ManageEngine_PAM360_MSP_64bit.bin -i silent -f /home/LinuxSecondaryMSP.txt

Now, the PAM360 will get installed.

4. Adding Users (MSP org)

The MSP administration process starts with user management. The first step is to add users to your MSP organization. You should designate one administrator as Account Manager™ for each of your clients. Refer to the help section Adding Users Manually to proceed with adding users.

5. Adding Organizations

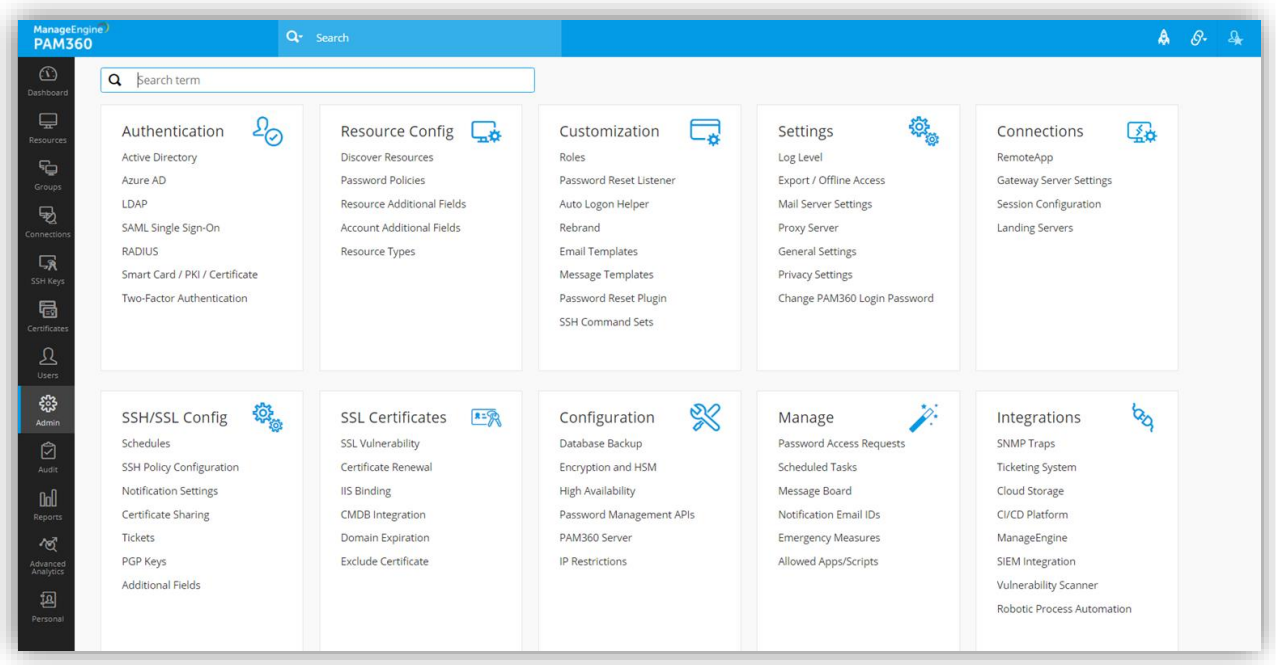
5.1 Adding Client Organizations

After adding users, you need to add your client organizations. Navigate to **Admin >> Organizations** section and you will find an icon named **Organizations**. The organizations to be managed by the MSP should be registered with PAM360 here.

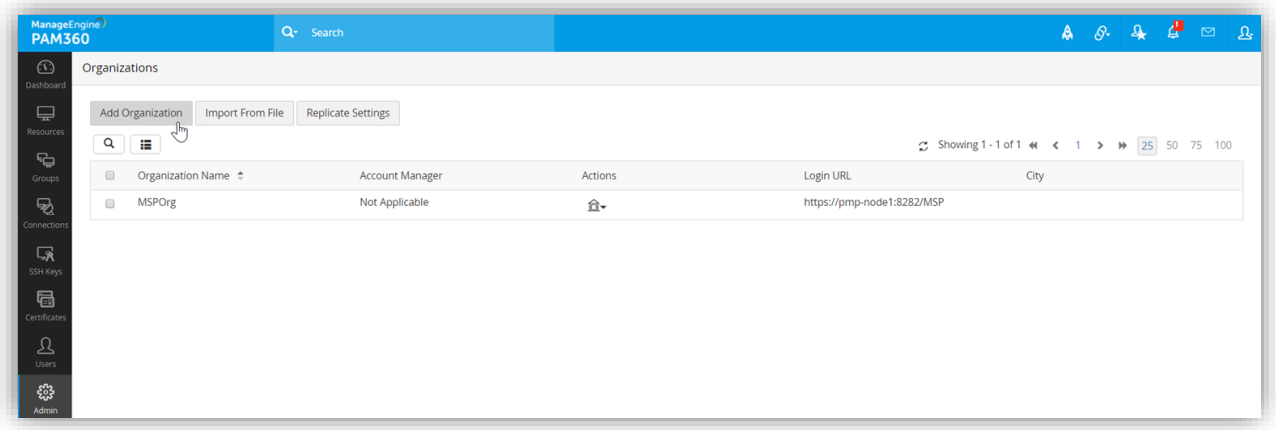
You can manually add the client organizations one-by-one or import all the organizations in bulk from a CSV file.

5.2 Adding Organizations Manually

1. Navigate to **Admin >> Organizations.**



2. Click **Add Organization**.

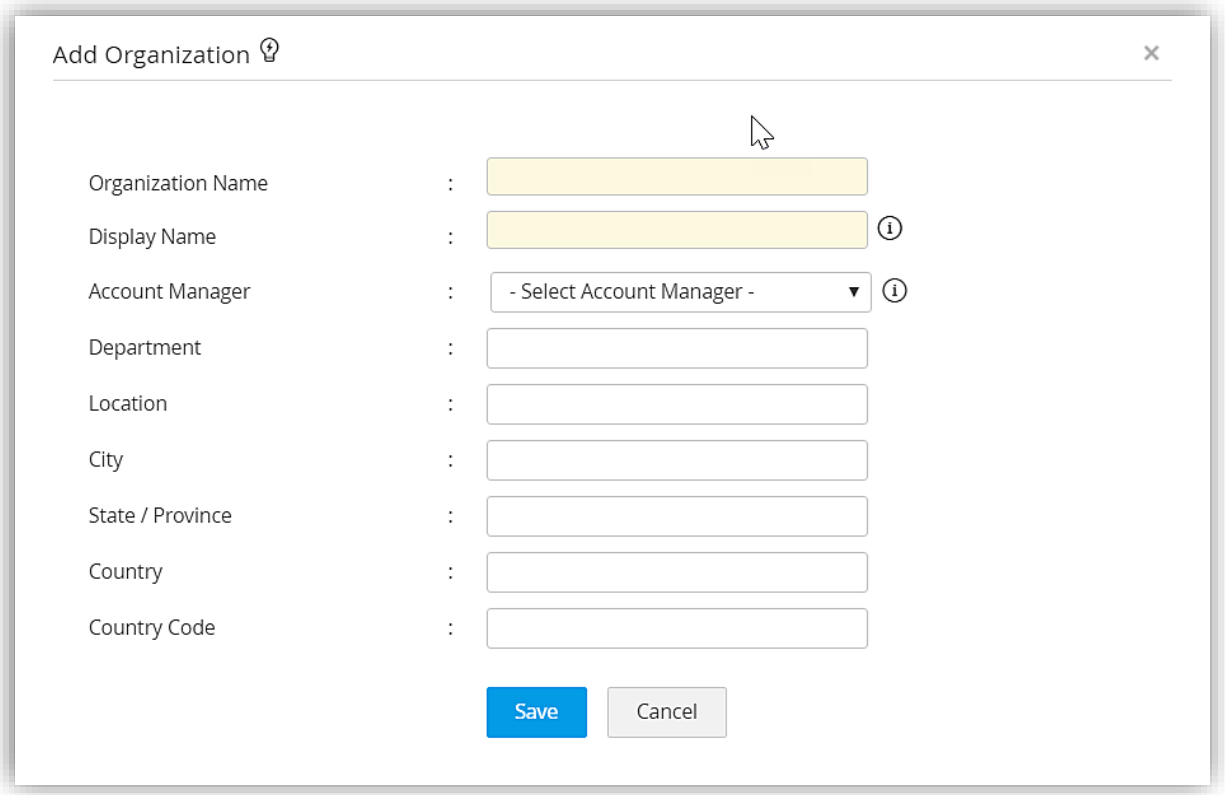


3. In the pop-up form that opens,
   i. Specify a name for the organization being added.
   ii. **Display Name:** The name with which you wish to identify the organization being added.
      - Only alphanumeric characters without empty spaces are allowed here.
      - The name should be a single word.
      - The name that you enter here will appear in the drop-down at the top right hand side of PAM360 GUI.
      - In addition, the display name will appear in PAM360 login URL.

(For example, if you assign **xyz** as the display name, the login URL for the organization will be **https://:/xyz**).

iii. **Account Manager:** You can designate any administrator at your end (MSP) as the Account Manager for the organization being added. As the name indicates, the account manager will be the point of contact for the organization being managed and will have privileges to add and manage resources on behalf of the organization. The Account Manager with the role Admin in PAM360 will be able to manage the users of the organization too. You can designate only one account manager per organization being managed. The same administrator can be made the account manager for multiple client organizations.

iv. Fill-in other details like **Department**, **Location** etc. as required and click **Save**.

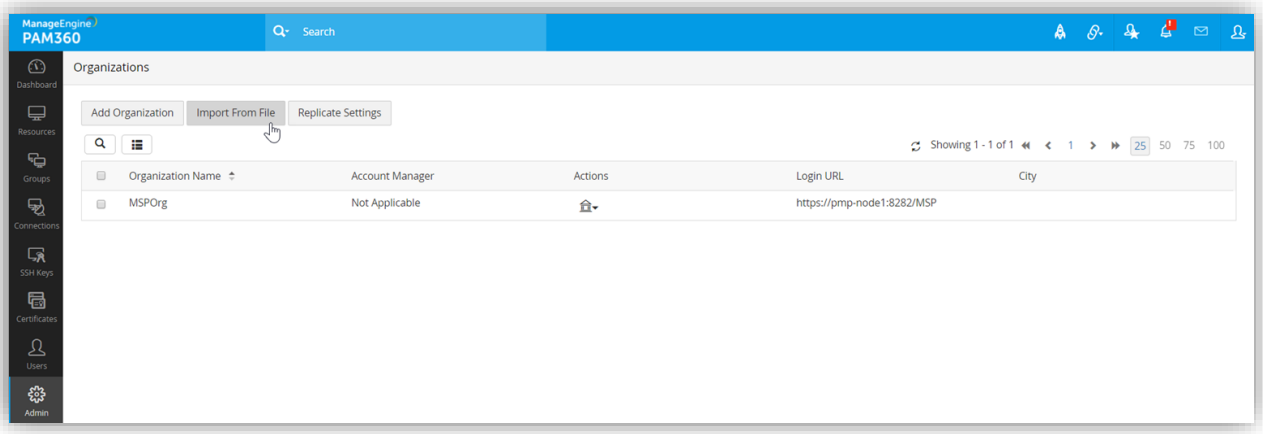


5.3 Importing Organizations from CSV

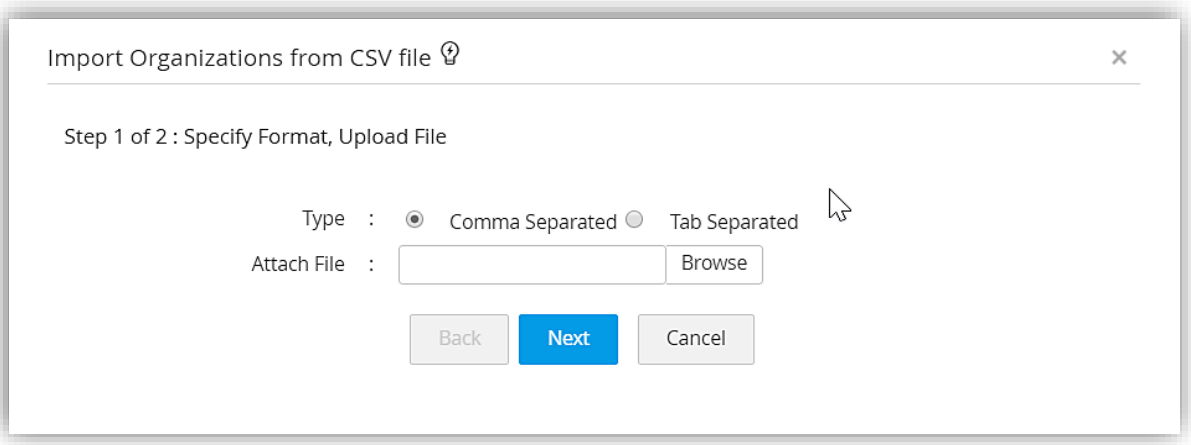
You can import multiple organizations from a CSV file using the import wizard. The CSV should have entries regarding organization name, display name and other details in comma separated form. The entry for each organization should be in a new line. All the lines in the CSV file should be consistent and have the same number of fields. CSV files having extensions .txt and .csv are allowed.

To import organizations,

1. Navigate to **Admin >> Organizations >> Import Organization.**



2. In the pop-up form that opens,
    i. Choose the file format.
    ii. Browse and select the CSV file containing the organizations.
    iii. Click **Next.**



    iv. In the pop-up form that opens, you can choose which fields in the CSV file maps to the corresponding attribute of the Organization.
    v. Click **Finish.**

The result of every line imported will be logged as an audit record.

5.4 Replicating Settings Across Client Orgs

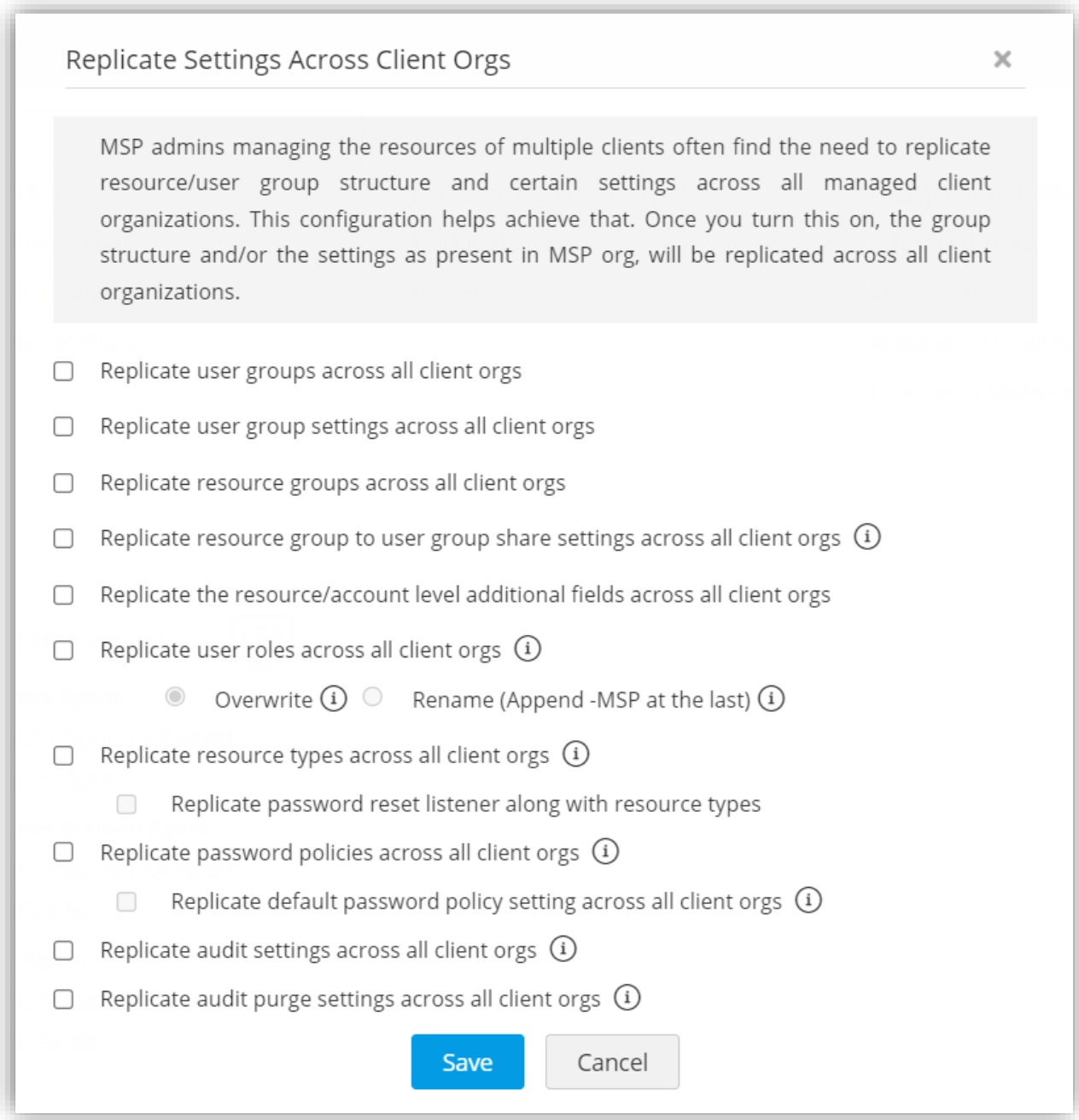
PAM360 allows MSP admins to replicate resource/user group structure and the settings across all managed client organizations.

To set this up, follow the steps:

1. Navigate to **Admin >> Organizations >> Replicate Settings Across Client Orgs.**
2. Select the required options using the checkboxes.
3. Click **Save** to save changes.

Listed below are some group structure and/or settings that can be applied to all client orgs as they are present in the MSP org.

i. User groups across all client orgs.
ii. User group settings across all client orgs.
iii. Resource groups across all client orgs.
iv. Resource group to user group share settings across all client orgs.
v. Replicate the resource/account level additional fields across all client orgs.
vi. User roles across all client orgs Overwrite/Rename (Append - MSP at the last).
vii. Resource types across all client orgs.
viii. Password policies across all client orgs.
ix. Audit operation type settings across all client orgs.
x. Audit purge settings across all client orgs.



6. Granting Privilege to Manage Organization Access

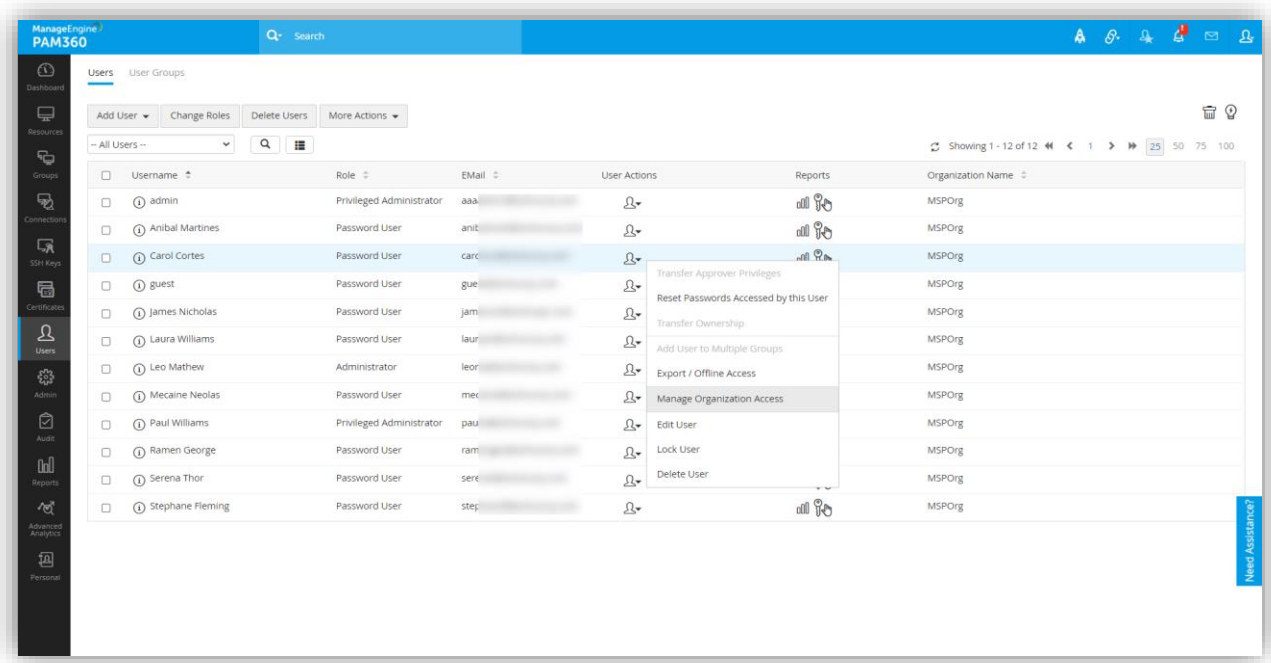
In addition to designating an administrator as **Account Manager**, you can grant access privileges to the client organization to any other member of your MSP organization. An administrator with this permission will be granted admin privileges within the client organization. Similarly, if permission is granted to a password administrator or a password user, they will have their respective privileges.

PAM360 requires approval before managing a client organization to ensure greater security. An administrator at the MSP can initiate organization access for a client organization, but they need to be approved by some other administrator at the MSP. It is not possible to approve the request by the one who initiates it or the one for whom it is being initiated. This is to ensure that no administrator can acquire manage permission for themselves or grant that privilege to anyone else without the approval of another administrator. This essentially means that the MSP organization should have a minimum of three administrators to carry out this process.

For example, assume the scenario when **Admin A** wants to provide access to **Admin B** for organization **ABC**. In this case, both **Admin A (the proposer)** and **Admin B (the admin designate)** cannot approve the access permission. Another admin, say **Admin C**, will have to approve the client organization request.

To mange client organizations at user/user group level, do the steps that follow:

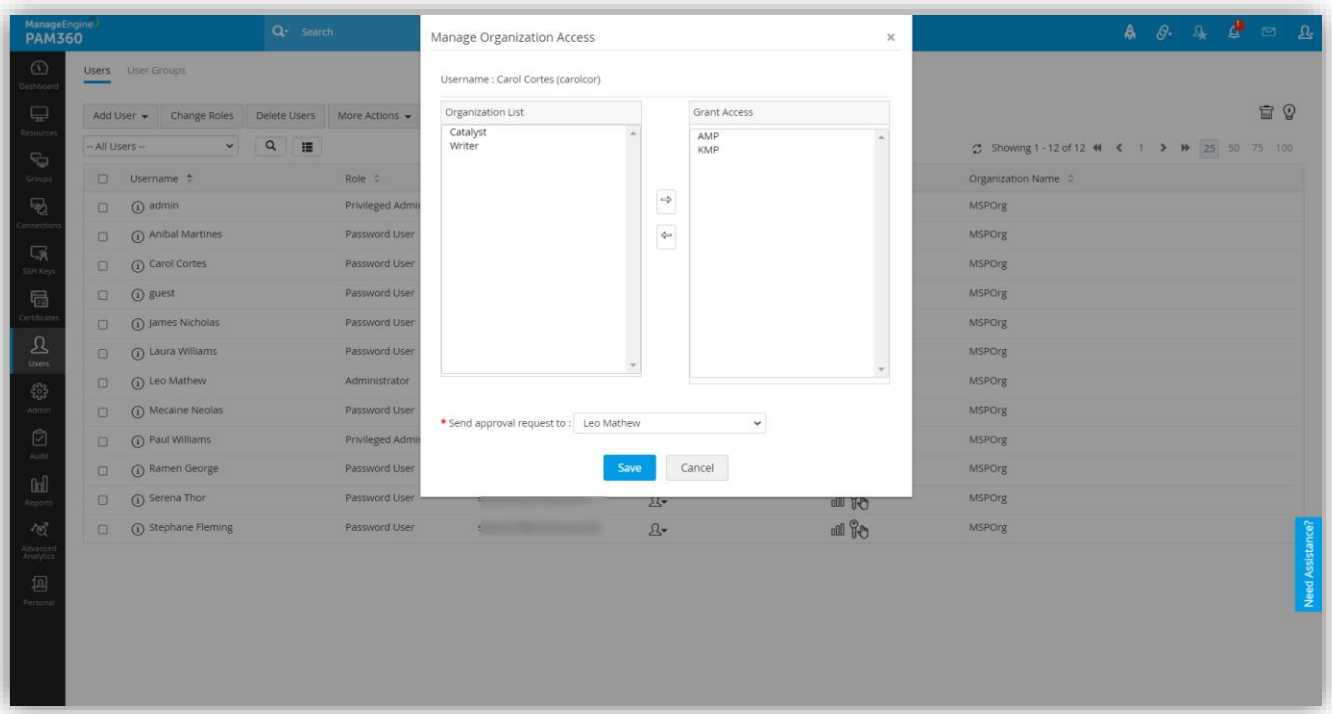
1. Log in to your MSP account and navigate to the **Users/User Groups** tab.
2. Click the **User Actions/ Actions** icon against the desired user and select **Manage Organization Access** from the dropdown.



3. In the pop-up form that opens,

i. Select the required client organizations from the **Organization List** and move it to **Grant Access** column using the arrows.

ii. Select the name of the approver and click **Save.**

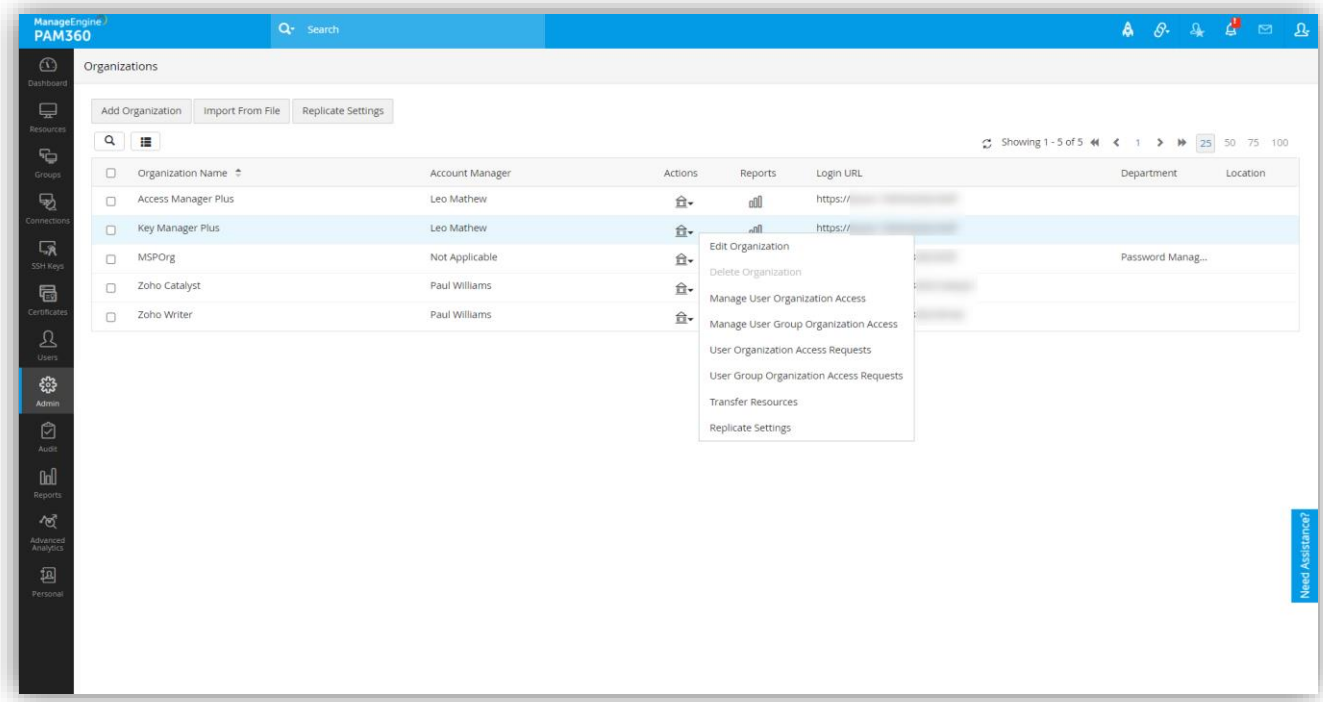


4. The user will gain access to the organization once it is approved by the respective administrator. Alternatively, you can also grant access from the **Organizations** page by clicking the **Actions** icon against the desired organization and selecting **Manage Organization** Access from the dropdown.

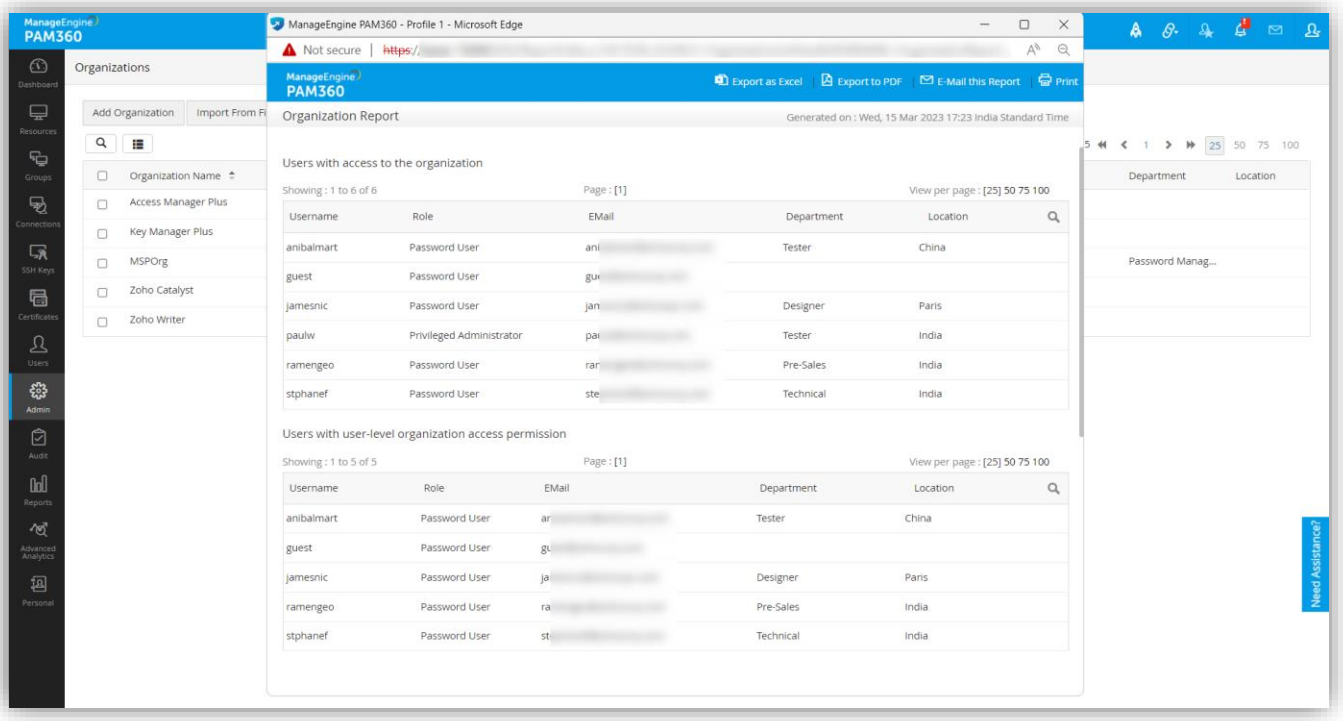
Once the administrator approves the request, the user/user group will get access to the client organization.

You can also perform the following operations from the **Organization** page by clicking the **Actions** icon beside the desired organization:

- Manage user organization access
- Manage user group organization access
- Grant permission to the user organization access requests
- Grant permission to the user groups organization access requests



You can also generate report for a client organization to know more about the users and user groups managed in it. To do this, navigate to **Admin >> Organizations >> Organizations** and click the report icon beside the desired client organization. In the window that opens, you will get the list of users and user groups managed at different levels.



7. MSPOrg (The default org)

By default, one organization named MSPOrg will be available. This default org is basically your organization (MSP's organization). The passwords that you add here will pertain to your own organization and not that of your clients.

7.1 Frequently Asked Questions

7.1.1 How to Manage Password for Client Organizations?

Once the organization is added, you will see the list of organizations being managed by you (i.e for which you have manage permission or for which you are the account manager) on the top band of the PAM360 GUI.

Select the required organization and proceed with resource addition. You can then share the passwords with your clients. On the other hand, if you are providing Password Management Service, you will ask your client to add passwords themselves.

7.1.2 How to access any specific client org?

You can access your MSP org as usual by accessing the URL *https://<PAM360-Host-Name>:8282/*. You can select the required client organization from the top band of the PAM360 GUI.

7.1.3 How do your clients access PAM360?

After creating an organization, you clients can connect to their organization and view/manage passwords by typing the URL as explained below:

https://<Host Name:<port>/<Name of the org>

For instance, assume that the name of the organization of your client is abc and PAM360 is running on the host pam360host, then the URL to connect to an organization will be: *https://pam360host:8282/abc*.

For information on how to perform various password management features, refer to the respective sections of the help documentation.

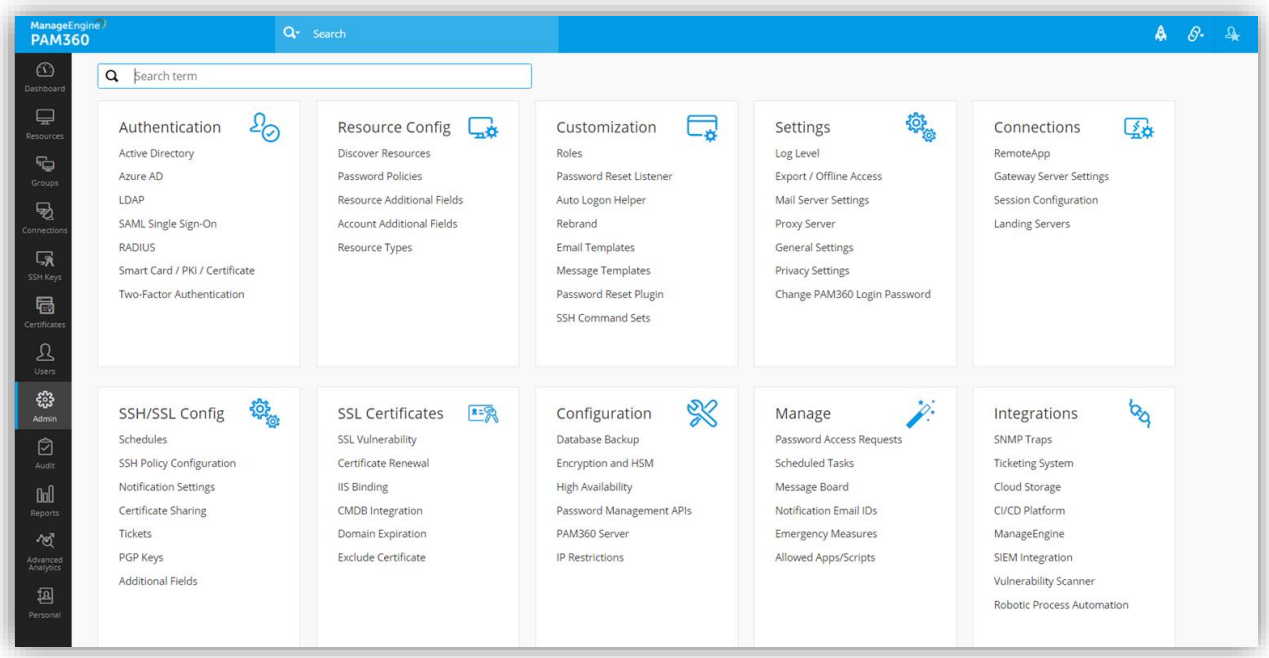
7.1.4 How to delete a client organization?

You can be eligible to delete a client organization in PAM360 only if you are an MSPOrg administrator. Additionally, you should also have any of the following privileges:

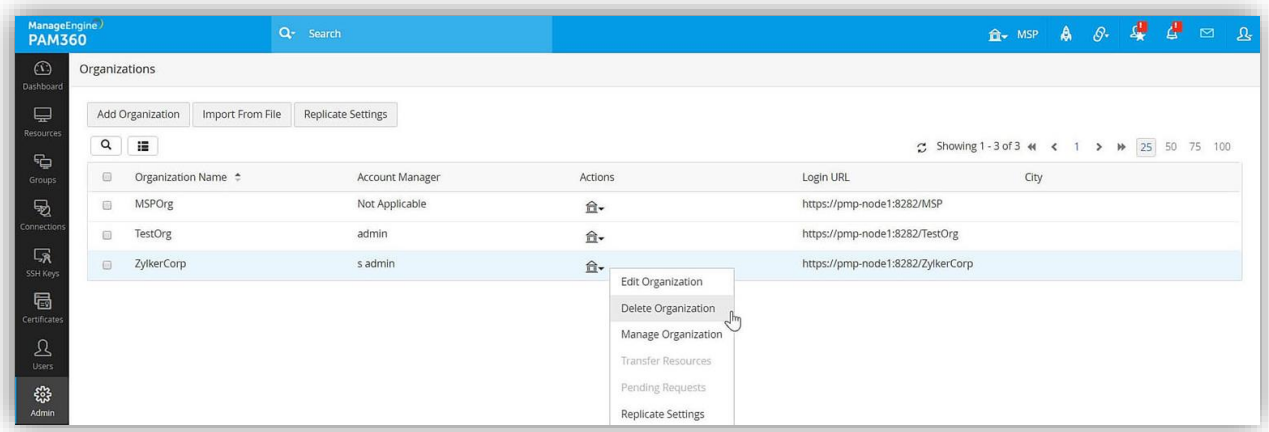
1. Be the Account Manager of the client organization you want to delete.
2. Hold **Manage Organization** permission for the client organization you want to delete.

To delete an organization,

1. Navigate to **Admin >> Organizations.**



2. Locate the client organization that you want to delete, click on **Actions** icons beside it, and select **Delete Organization** from the drop down menu.



3. Click **Ok** to confirm deletion. Note that deleting a client organization will also delete all resources and users added under it.