ManageEngine
PAM360

Best Practices Guide

www.manageengine.com/pam360

ManageEngine PAM360

Table of Contents

Introduction to ManageEngine PAM360 6

Target Audience for this Guide 7

1. Recommended System Configuration 8

2. Deployment Best Practices 9

2.1 Choosing the Deployment Platform

2.2 Choosing the Backend Database

2.3 Securing the Installation Master Key

2.4 Securing the Database Configuration

3. Server and Environment Hardening 15

3.1 Server Hardening

3.2 Configuring a Dedicated Service Account

3.3 Binding IP Address for Web Server

3.4 Securing Access using IP Restrictions

4. User Onboarding and Management Best Practices 19

4.1 Leverage Directory Integration for User Provisioning

4.2 Leverage Directory Authentication

4.3 Enforce Two-Factor Authentication

4.4 Assign User Roles Based on User Responsibilities

4.5 Organize Users into User Groups

4.6 Delete Default Accounts

4.7 Restrict Access to PAM360 Native Tools

5. Privileged Resource Management 24

5.1 Onboarding Resources

5.2 Configure Resource Types

5.3 Remove Unwanted Privileged Accounts

5.4 Randomize Passwords after Resource Discovery

5.5 Organize Resources into Resource Groups

5.6 Nested Resource Groups

5.7 Additional Fields

6. Granular Access Control and Password Sharing 27

6.1 Password Sharing

6.2 Group-Based Sharing

6.3 Access Control Workflow

6.4 Just-In-Time Privilege Elevation

6.6 Enforce Users to Provide a Reason while Accessing Passwords

6.7 Integrate PAM360 with Enterprise Ticketing Systems

7. Password Policies 33

7.1 Configure Unique Password Policies for Critical Resource Groups

7.2 Configure Account-Level Password Policies

7.3 Define Password Age when Creating Policies

8. Password Resets and SSH Key Rotation 35

8.1 Perform Periodic Password Randomization and Key Rotation

8.2 Choose the Appropriate Password Reset Mode

8.3 Restart Services After Password Resets

9. Secure Remote Access 38

9.1 Enable Automatic Logon Without Revealing Passwords

9.2 Configure Session Gateway Settings

9.3 Configure Advanced Connection Settings

9.4 Discover and Configure RemoteApp for Windows Servers

10. Privileged Access to Third Parties 41

10.1 Manage Third-Party Access to Corporate Systems

11. Data Center Remote Access 43

11.1 Avoid Sharing Jump Server Credentials

11.2 Export Passwords for Offline Access

12. Session Management and Monitoring 44

12.1 Monitor Critical Sessions in Real Time

12.2 Record Privileged Sessions

12.3 Regularly Purge Recorded Sessions

13. SSL/TLS Certificate Management 47

13.1 Discover and Import Certificates

13.2 Follow Secure Certificate Request and Acquisition Practices

13.3 Ensure the Latest Certificate Version is Deployed

13.4 Integrate with Public Certificate Authorities (CA)

13.5 ServiceDesk Plus CMDB Integration

13.6 Perform SSL Vulnerability Scanning

14. Auditing and Reporting 50

14.1 Conduct Regular Internal Audits

14.2 Configure Alerts for Critical Events

14.3 Use Daily Digest Emails to Reduce Notification Volume

14.4 Customize Email Templates

14.5 Integrate with SIEM and Management Systems

14.6 Schedule Periodic Report Generation

14.7 Purge Audit Records Periodically

15. External Integrations 54

15.1 Advanced Analytics

15.2 Vulnerability Scanners

15.3 Integration with SIEM Tools

15.4 Plugins for CI/CD Platforms

15.5 Robotic Process Automation (RPA)

15.6 Integration with ADSSP

16. High Availability and Disaster Recovery 60

16.1 Configure an Appropriate High Availability Model

16.2 Configure Database Backup for Disaster Recovery

17. Periodic Maintenance 63

18. Emergency and Offline Access 65

19. Administrator Offboarding 67

20. Security Best Practices 68

21. Privacy Settings 69

Introduction to ManageEngine PAM360

ManageEngine PAM360 is a privileged access management suite that enables organizations to protect against data breaches and cyber attacks by securing privileged access to resources and associated accounts across the organization.. PAM360 regulates and monitors access to sensitive data stored within critical systems. It encrypts and stores privileged accounts in a secure vault, protecting sensitive information from unauthorized access and other security threats. PAM360 enforces secure password policies, provides role-based access to resources, and offers efficient user and resource management. It also seamlessly integrates with a wide range of external IT solutions, including ITSM and SIEM systems, enabling organizations to automate workflows, streamline privileged access processes, and centralize security monitoring. Its comprehensive reporting, auditing, and integration capabilities further strengthen security and help organizations meet regulatory compliance requirements.

Target Audience for this Guide

With the growing cyber threats and stricter regulatory mandates, adopting privileged access management best practices is essential to protect critical systems, reduce security risks, and maintain regulatory compliance. This guide is designed for IT administrators, security professionals, system architects, and compliance officers responsible for managing, securing, and governing privileged access across their organizations.

This guide provides comprehensive best practice recommendations for planning, deploying, configuring, and managing ManageEngine PAM360 across diverse enterprise environments. It covers key aspects of privileged access management, including user and resource onboarding, authentication, password management, access control, privileged session management, auditing, reporting, integrations, and business continuity. The recommendations presented in this guide help organizations strengthen their security posture, improve operational efficiency, and maximize the value of their PAM360 deployment while aligning with organizational security policies and compliance requirements.

1. Recommended System Configuration

The following recommended system configurations provide a baseline for deploying PAM360 based on the size of your organization and the number of privileged accounts to be managed. As the number of privileged accounts increases, resource requirements may also increase depending on factors such as the number of users, concurrent sessions, and the volume of activities and data processed by PAM360. Use the recommendations below as a guideline when planning your PAM360 deployment.

Organization	Processor	RAM	Hard Disk
Small & Medium Businesses (<5,000 Privileged Accounts)	4 Cores or More	16 GB or More	Application: > 4 GB Database: > 10 GB
Mid-Market Businesses (<20,000 Privileged Accounts)	8 Cores or More	16 GB or More	Application: > 4 GB Database: > 10 GB
Enterprises (<50,000 Privileged Accounts)	16 Cores or More	24 GB or More	Application: > 5 GB Database: > 50 GB
Large Enterprises (>50,000 Privileged Accounts)	24 Cores or More	32 GB or More	Application: > 8 GB Database: > 100 GB

Additional Detail: We recommend you install PAM360 on a dedicated, hardened, high-end server for superior performance and security.

2. Deployment Best Practices

This section outlines the recommended best practices for deploying ManageEngine PAM360 in production environments. It covers key deployment considerations, including selecting the appropriate deployment platform and backend database, securing the installation master key, and protecting database configuration information. Following these recommendations helps establish a secure and reliable foundation for your PAM360 deployment.

2.1 Choosing the Deployment Platform

ManageEngine PAM360 supports deployment on both Windows and Linux operating systems. While both platforms provide the same core privileged access management capabilities, a Windows-based deployment is recommended for organizations that extensively manage Windows infrastructure or rely on Active Directory for identity management. Deploying PAM360 on a Windows server offers the following advantages:

- **Native Active Directory Integration:** PAM360 can directly integrate with Active Directory to import users and groups. It also supports NTLM-based Single Sign-On (SSO), allowing domain users who have already authenticated to their Windows systems to seamlessly access PAM360 without authenticating again. In Linux deployments, Active Directory authentication is available through LDAP-based integration.
- **Agentless Password Management for Windows Resources:** When PAM360 is deployed on a Windows server with direct connectivity to the target systems, it can rotate passwords of the Windows resources without requiring additional agents. If PAM360 is deployed on a Linux server, a PAM360 agent should be installed on the Windows resources and domain controllers to execute password resets for Windows domain, local, and service accounts.
- **Extended Windows Account Management:** Deploying PAM360 on a Windows server facilitates password management for Windows-specific components, including

Windows service accounts, scheduled tasks, IIS Web.Config files, and IIS application pool accounts, providing broader management capabilities for Windows environments.

Organizations managing predominantly Linux-based environments should deploy PAM360 on Linux servers. However, administrators should evaluate the operational requirements of their infrastructure and choose the deployment platform that minimizes administrative effort while maximizing native integration capabilities.

2.2 Choosing the Backend Database

ManageEngine PAM360 supports both PostgreSQL and Microsoft SQL Server (MS SQL) as backend databases. By default, PAM360 is bundled with a PostgreSQL database, making it an ideal choice for small and medium-sized organizations. For enterprise and large enterprise deployments that require greater scalability, high availability, clustering, and advanced disaster recovery capabilities, Microsoft SQL Server is the recommended backend database. When deploying PAM360 with Microsoft SQL Server, consider the following best practices:

- **Use a Dedicated SQL Server Instance -** Deploy PAM360 on a dedicated MS SQL Server instance to avoid resource contention, configuration conflicts, and operational disruptions with other applications. Since PAM360 communicates with MS SQL Server only over a secure SSL connection, ensure that a valid SSL certificate is configured for PAM360 before establishing the database connection.
- **Secure the Database Encryption Key -** After configuring MS SQL Server as the back-end database, PAM360 automatically generates an encryption key for database-level encryption. Store this key in a secure location separate from the database server to protect it from unauthorized access and accidental loss. The encryption key is required when configuring high availability, migrating the database, or performing disaster recovery operations. Losing the key may require reconfiguring the MS SQL database and can result in permanent data loss.
- **Use Windows Authentication -** Configure the database connection using Windows

Authentication instead of a local SQL Server account. We recommend using the same domain service account to run SQL Server, SQL Server Agent service, and the PAM360 database connection to simplify administration and strengthen security.

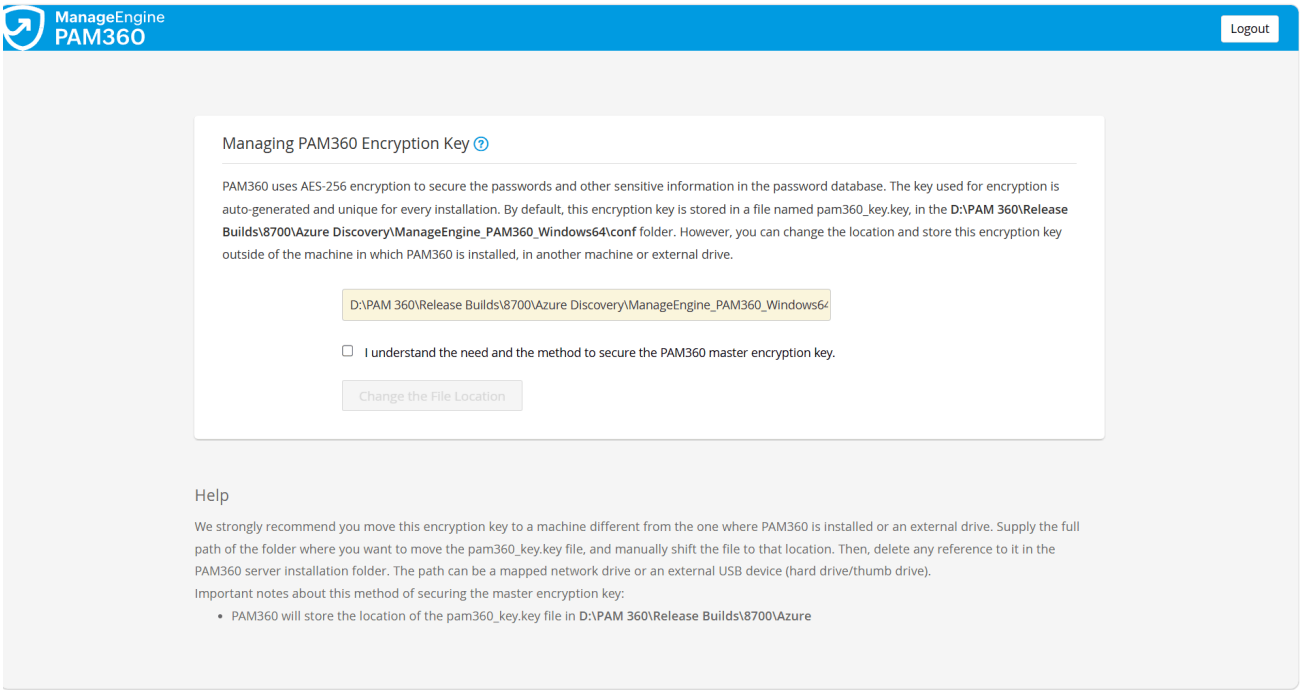
- **Enforce Encrypted Database Communication -** Enable the **Force Encryption** option on the MS SQL Server instance to ensure that all communication between PAM360 and the database is encrypted. Clients that do not support encrypted connections should not be permitted to connect.
- **Restrict Network Access -** Enable only the TCP/IP protocol on the SQL Server instance and disable unused protocols to reduce the attack surface. Configure firewall rules to allow access only through the required SQL Server ports from authorized systems.
- **Harden the SQL Server -** Hide this SQL Server instance to prevent it from being enumerated by other tools and restrict database access exclusively to the PAM360 service account and authorized database administrators, following the principle of least privilege.

2.3 Securing the Installation Master Key

ManageEngine PAM360 uses **AES-256 encryption** to protect privileged passwords and other sensitive information stored in its database. During installation, PAM360 automatically generates a unique master encryption key for each deployment and stores it in the **pam360_key.key** file under the **<PAM360-Installation-Directory>/conf** directory.
It is strongly recommended that the master encryption key not be stored on the same server as the PAM360 installation or its database backups. Storing the encryption key alongside the encrypted data increases the risk of unauthorized access if the server is compromised. Instead, move the **pam360_key.key** file to a secure external location, such as a dedicated server, network drive, or encrypted external storage device, and restrict access to the PAM360 service account and authorized administrators.

During the initial login after setup, you will be prompted to relocate the encryption key. Move the **pam360_key.key** file to the desired location, update the new folder location, and click

the **Change the File Location** button. PAM360 will record the location of the pam360_key.key in a configuration file named **manage_key.conf**, located in the **<PAM360-Installation-Directory>/conf** folder. Ensure the file or the key value is not stored anywhere within the PAM360 installation folder.



You can also directly edit this file to change the key file location. If you want to move the key file to a new location after the initial setup, move the encryption key to the new location, update the **manage_key.conf** file with the new location of the **pam360_key.key** file and remove any remaining copies. Ensure that the specified location remains continuously accessible to the PAM360 server, as the application requires access to the master key during startup and for cryptographic operations such as database backup and recovery.

Since the master encryption key is required for database restoration, migration, and high-availability configurations, it should be included in the organization's backup and disaster recovery strategy. Losing this key may prevent PAM360 from accessing encrypted data and can result in permanent data loss.

2.4 Securing the Database Configuration

In addition to the master encryption key, PAM360 secures database communication using a

separate database key unique to each installation. By default, this key and the database connection parameters, including database credentials and connection setting parameters, are stored in the **database_params.conf** file within the PAM360 installation directory.

Although the database is configured not to accept any remote connections, it is recommended that the **database_params.conf** file be moved to a secure location outside the PAM360 installation directory. This helps protect sensitive database configuration information from unauthorized access and prevents critical configuration files from residing alongside the application binaries. Access to this file should be restricted to the PAM360 service account and authorized administrators by applying the principle of least privilege.
After moving the file to a secure external location, update the new file location in the **wrapper.conf** file (Windows) or **wrapper_lin.conf** file (Linux). The wrapper file is located within the **<PAM360-Intsallation-Directory/Conf>** folder. Ensure that the configured path remains continuously accessible to the PAM360 server, as the application requires access to this file during startup. An incorrect or inaccessible path will prevent the PAM360 service from starting.

Follow these steps to relocate the database_params.conf file:

1. Stop the PAM360 service.
2. Move the **database_params.conf** file from the PAM360 installation directory to a secure external location.
3. On Windows, open the **wrapper.conf** file. On Linux, open the **wrapper_lin.conf** file. The files are located in the **<PAM360-Installation-Directory/Conf>** folder.
4. Locate the following entry: **wrapper.java.additional.9=-Ddatabaseparams.file**.
5. Replace the default path **./../conf/database_params.conf** with the new location of the **database_params.conf** file. For example: **wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\Ddrive\sharedfiles\database_params.conf**
6. Save the configuration file.
7. Start the PAM360 service and verify that the application starts successfully.

As part of the organization's disaster recovery strategy, include the **database_params.conf**

file in secure backup procedures. Since it contains the information required to establish database connectivity, protecting and retaining this file is essential for successful recovery and migration operations.

While updating the path, locate the line **wrapper.java.additional.9=-Ddatabaseparams.file** in the **wrapper.conf** file (Windows) or the **wrapper_lin.conf** file (Linux). By default, the path is configured as:**./../conf/database_params.conf**. After relocating the **database_params.conf** file to a secure location, update this entry to reference the new file location. For example: **wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\Ddrive\sharedfiles\database_params.conf**.
Restart the PAM360 service after updating the configuration for the changes to take effect.

3. Server and Environment Hardening

This section highlights the recommended best practices for securing the server and network where ManageEngine PAM360 is deployed. It covers server hardening, service account configuration, web server network settings, and IP-based access restrictions to help strengthen the security of your PAM360 deployment.

3.1 Server Hardening

Since all application binaries, configuration files, encryption keys, logs, and supporting components reside within the **<PAM360-Installation-Directory>** on the PAM360 server, it should be treated as a critical infrastructure asset and hardened accordingly. Administrators should implement operating system and network-level security controls to minimize the attack surface and restrict unauthorized access. Some of the basic recommendations include:

- **Restrict Interactive Access** - Disable remote access to this server for all regular domain users using domain group policies. Limit administrative access to authorized personnel and grant write permissions to the PAM360 installation directory only to designated administrators.
- **Secure Network Communication** - Set up inbound and outbound connection firewalls to protect against incoming and outgoing traffic. Configure which ports should be opened to execute various password management operations such as remote password resets and restrict unnecessary network access.

3.2 Configuring a Dedicated Service Account

Create a dedicated domain service account exclusively for PAM360 and use it consistently across the deployment. Configure the PAM360 Windows service to run under this service account instead of the default local system account. The same service account can also be used for Active Directory integration, including user and resource discovery, simplifying

administration while following the principle of least privilege.

Assign only the permissions required for PAM360 to perform its operations, and avoid using shared or highly privileged administrative accounts as the service account.

To configure a service account to run PAM360, go to the services console (“services.msc”) on the server where PAM360 is deployed and navigate to the properties of PAM360. Change the configured local system account to the dedicated service account created for PAM360.

3.3 Binding IP Address for Web Server

By default, the PAM360 web server listens on all available IP addresses on the host server. Thus, PAM360 will be reachable on any or all IP addresses on the configured port. Therefore, it is recommended to bind the web server to a dedicated IP address to limit network exposure and prevent unintended access. Follow the steps below to bind a single IP address for PAM360:

1. Stop the PAM360 service.
2. Open the **server.xml** file present in the **<PAM360-Installation-Directory>\conf** folder and locate the following entry:

   <Connector SSLEnabled=”true” URIEncoding=”UTF-8” acceptCount=”100” ciphers=”TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256” clientAuth=”false” debug=”0” disableUploadTimeout=”true” enableLookups=”false” keystoreFile=”conf/server. keystore” keystorePass=”passtrix” maxHttpHeaderSize=”32768” maxSpareThreads=”75” maxThreads=”150” minSpareThreads=”25” port=”8282” scheme=”https” secure=”true” server=”PAM360” sslProtocol=”TLS” truststoreFile=”jre/lib/security/cacerts” truststorePass=”changeit” truststoreType=”JKS” useBodyEncodingForURI=”true”/>

3. In the above line, next to the value port=”8282”, add the following entry: **address=”<IP-Address>”**. Here, replace <IP-Address> with the actual IP address of the server that PAM360 should use for incoming connections.
4. Restart the PAM360 service after updating the configuration for the changes to take

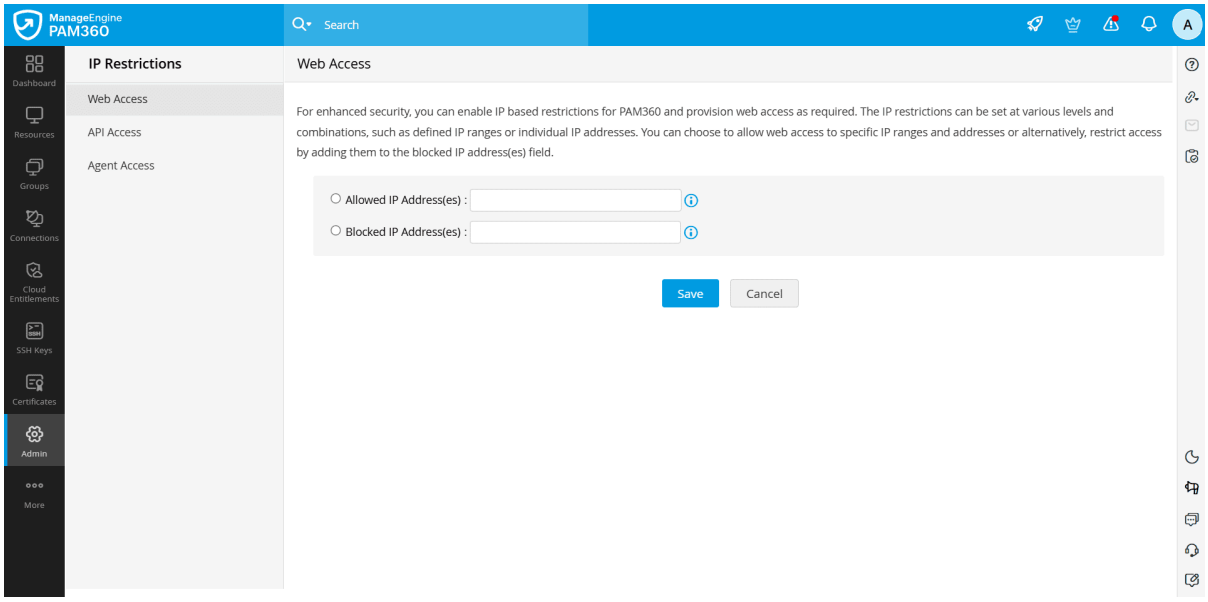
effect.

3.4 Securing Access using IP Restrictions

By default, PAM360 can be accessed from any client system that has network connectivity to the server. It is recommended to restrict access to the PAM360 web interface by allowing connections only from trusted client systems, such as administrator workstations, jump servers, or secure management networks. Limiting access to known client systems significantly reduces the attack surface and minimizes the risk of unauthorized access attempts. PAM360 allows you to restrict web, API, and agent access by IP address.

To configure IP restrictions, navigate to **Admin** >> **Server Hardening** >> **IP Restrictions** >> **Web Access**. On the **IP Restrictions** page, you can configure IP restrictions in two ways:

1. **Allowed IP Addresses** - Specify the IP addresses or IP address ranges that can access the PAM360 web server.
2. **Blocked IP Addresses** - Specify the IP addresses or IP address ranges that are blocked from accessing the PAM360 web server.



You can repeat the above process for API and agent access as well. We recommend specifying the required IP or IP address ranges to explicitly permit access only from authorized sources, as it provides stronger protection than blocking known addresses.

Review and update the configured IP restrictions periodically to ensure they remain aligned with changes to the organization's network infrastructure.

4. User Onboarding and Management Best Practices

This section outlines the recommended best practices for onboarding users and managing user access in ManageEngine PAM360. It covers user provisioning, authentication, role assignment, user grouping, and endpoint access controls to help organizations establish a secure and well-governed privileged access environment.

4.1 Leverage Directory Integration for User Provisioning

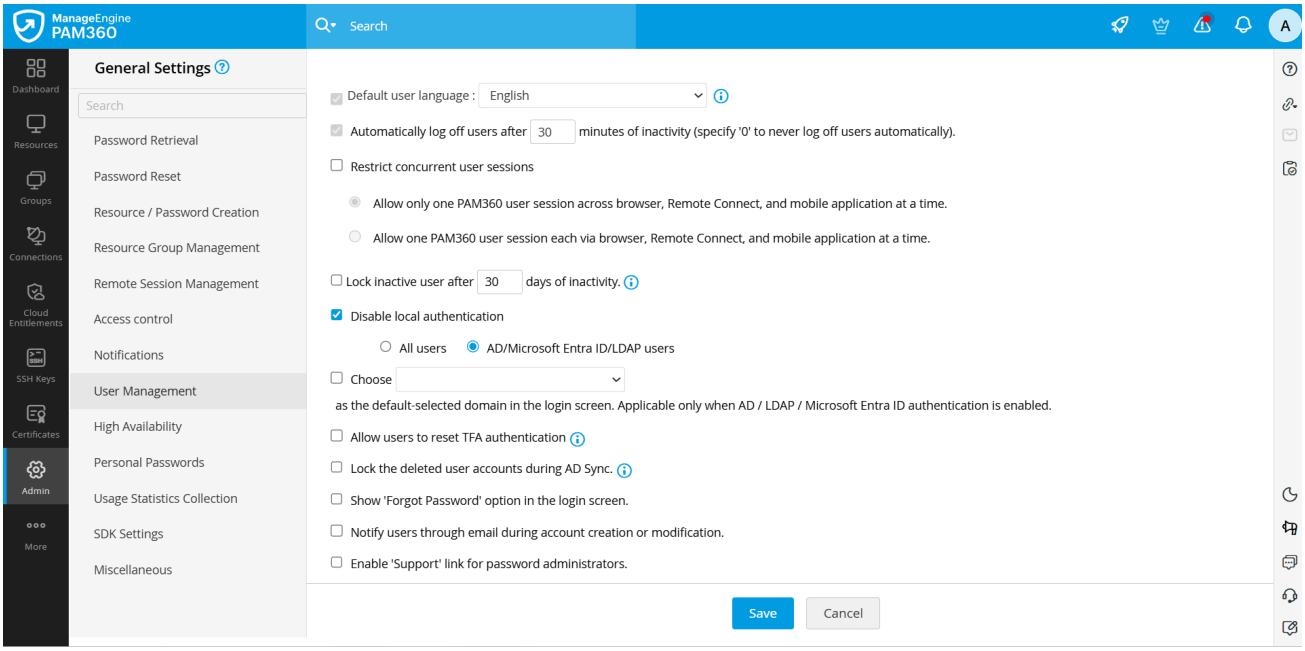
Integrating PAM360 with an enterprise directory service, such as Active Directory, LDAP, or Microsoft Entra ID, simplifies user management and strengthens authentication security. Directory integration enables centralized user provisioning, eliminating the need to manage user identities separately within PAM360. With the integration, you can import users, groups, or organizational units directly from the directory services and assign appropriate PAM360 roles based on their responsibilities. You can also enable periodic synchronization to ensure that user additions, deletions, and organizational changes are automatically reflected in PAM360, helping maintain an accurate and up-to-date user inventory. When users are permanently deleted from Active Directory, PAM360 disables and locks these accounts, sends an email and an alert notification, allowing you to either delete or unlock them.

4.2 Leverage Directory Authentication

After integrating PAM360 with a directory service, it is recommended to use the directory's authentication mechanism to authenticate users with their Active Directory, LDAP, or Microsoft Entra ID credentials. This centralizes identity management, simplifies password administration, and enables organizations to enforce their existing authentication policies through the enterprise directory. Users can access PAM360 via the directory's authentication mechanism, including supported Single Sign-On (SSO) capabilities, without maintaining separate local account passwords. Since users are authenticated directly against the configured directory, their directory login passwords are not stored locally in

PAM360.

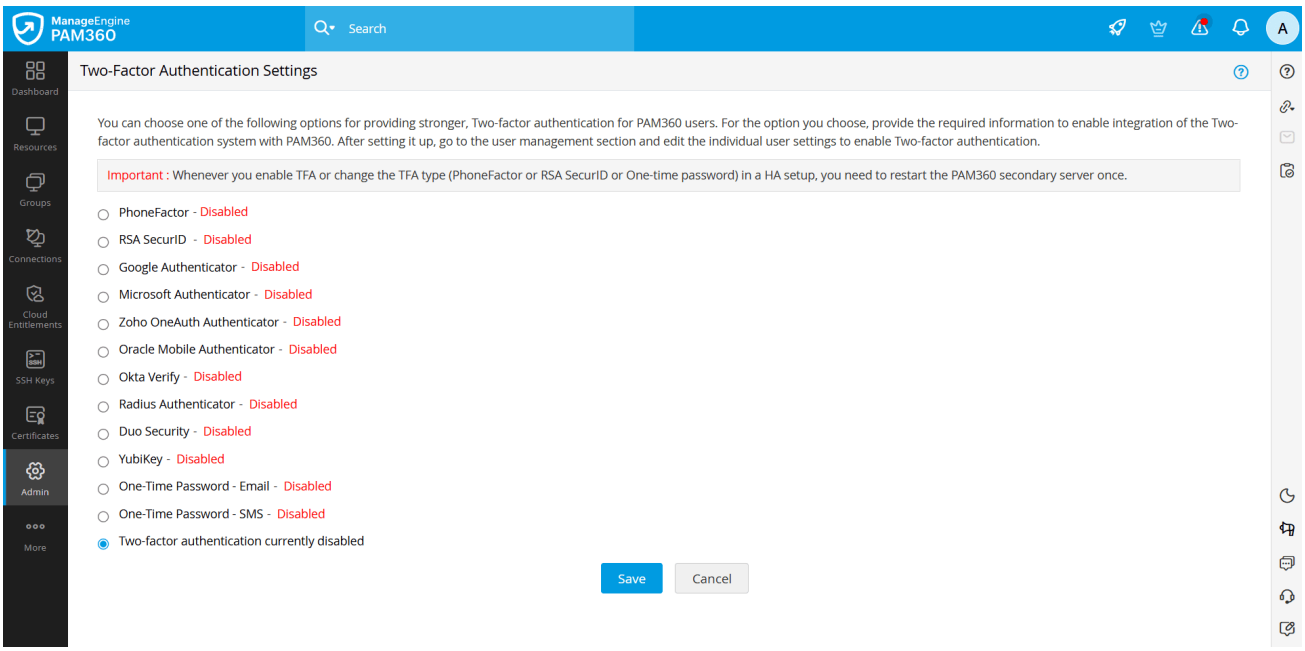
After enabling AD/LDAP/Entra ID authentication, it is recommended to disable local authentication. To disable local authentication, navigate to **Admin** >> **Customization** >> **General Settings** >> **User Management**, select **Disable local authentication**, and configure the other setting as required. However, if a local PAM360 account is configured as a break-glass account, local authentication cannot be disabled. In such cases, disable the **Show 'Forgot Password' option in the login screen** option to prevent users from utilizing local authentication while retaining access to the break-glass account.



4.3 Enforce Two-Factor Authentication

Enable two-factor authentication (TFA) for all PAM360 users to provide an additional layer of protection beyond passwords. Requiring users to verify their identity through an additional layer of authentication significantly reduces the risk of unauthorized access due to compromised credentials. PAM360 supports multiple authentication mechanisms for TFA, including Azure MFA, Duo Security, RSA SecurID, Google Authenticator, RADIUS-compliant solutions, email-based one-time passwords, SMS-based one-time passwords, and Zoho OneAuth. Select the authentication mechanism that best aligns with your

organization's identity and security infrastructure.



4.4 Assign User Roles Based on User Responsibilities

While onboarding users, assign roles based on their job responsibilities in accordance with the principle of least privilege, ensuring they receive only the permissions required to perform their assigned responsibilities. Limit administrator privileges to personnel responsible for product administration, and avoid assigning elevated permissions unnecessarily. Where appropriate, create custom roles aligning with organizational responsibilities instead of granting broader access through predefined administrative roles. Explore this **link** to learn more about user roles in PAM360 and the detailed steps to create a custom user role.

The Super Administrator role in PAM360 provides unrestricted access to all privileged resources managed within the product. Since this role has unrestricted access to all privileged resources, it should be reserved exclusively for emergency or break-glass scenarios. As a best practice, create only one Super Administrator account and assign it to a highly trusted administrator. Once the role has been established, prevent additional Super Administrator accounts from being created unless explicitly required. Explore this **link** to

learn about the Super Administrators in PAM360.

To restrict the creation of additional Super Administrator accounts, navigate to **Admin** >> **Authentication** >> **Super Administrators**, and then enable the **Deny Creation of Super Admins by Admins** option.

4.5 Organize Users into User Groups

Organize users into logical groups based on their job functions, departments, or operational responsibilities. User groups simplify resource sharing, access control, approval workflows, and administrative management. Organizations with Active Directory or LDAP integrations can import existing directory groups and use the same hierarchical structure in PAM360.

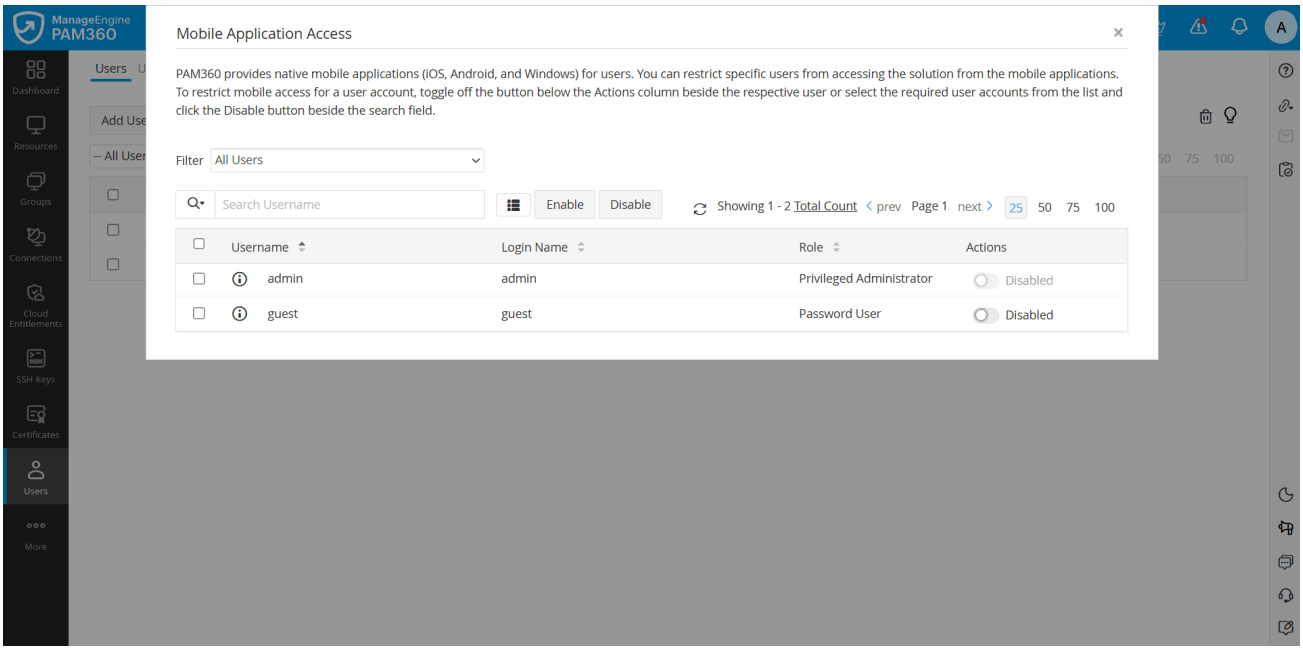
4.6 Delete Default Accounts

After creating one or more administrator accounts, remove or disable the default admin and guest accounts to reduce unnecessary attack vectors and eliminate the use of shared default credentials.

4.7 Restrict Access to PAM360 Native Tools

By default, users can access PAM360 through the web interface, mobile applications, browser extensions, and remote connect application. Organizations with strict endpoint security requirements should restrict access to mobile applications and browser extensions unless explicitly required.

Enable mobile application, browser extension, and remote connect access only for users whose responsibilities require them, such as administrators working remotely or personnel who frequently access web-based applications. Periodically review these permissions to ensure they remain aligned with operational requirements.



To modify mobile application, browser extension, and remote connect access, navigate to the **Users** tab, click the **More Actions** button in the top pane, select **Configure** from the displayed options, and select **Mobile Application Access**, **Browser Extension Access**, or **Remote Connect Access** based on your requirement. In the window that appears, you can use the toggle button under the **Actions** column next to the desired user to modify their access.

5. Privileged Resource Management

This section outlines the recommended best practices for onboarding and organizing resources in PAM360. It covers resource discovery and import methods, resource type classification, removal of unnecessary privileged accounts, password randomization, resource grouping, and the use of additional fields to simplify resource management and retrieval.

5.1 Onboarding Resources

The first step in managing the privileged passwords in your environment via PAM360 is onboarding resources and their associated accounts. PAM360 supports resource onboarding through various methods. The most convenient method is Privileged Resource Discovery, in which PAM360 automatically discovers the privileged resources within the organization based on the specified parameters. This method allows you to identify and onboard privileged resources across the environment. Manual addition and importing resources from CSV/TSV files can be used when resources should be added individually or when credentials and resource information are being migrated from an existing password management solution or stored in spreadsheets.

5.2 Configure Resource Types

When adding resources manually or through CSV/TSV import, ensure that each resource is assigned the appropriate resource type. Resource types determine how PAM360 communicates with the target resource and are required for operations such as password verification and resets. Resources without a specified type are categorized as Unknown, which can prevent password management operations from functioning correctly. PAM360 provides a range of predefined resource types. You can view the list of supported resource types under **Admin >> Resource Management >> Resource Types**.

5.3 Remove Unwanted Privileged Accounts

Resource discovery automatically enumerates the accounts associated with discovered resources. Some of these accounts may be unnecessary, unauthorized, or orphaned accounts. For example, discovering a Windows resource may also enumerate guest accounts without any admin privileges. These accounts are not required to be managed via PAM360. From a security perspective, unauthorized accounts should be identified and deleted to avoid any unforeseen vulnerabilities. Review the accounts identified during discovery and delete any unauthorized accounts from both PAM360 and target systems. Maintaining only the privileged accounts that are required for business and administrative operations reduces the attack surface and minimizes unnecessary privileged access.

5.4 Randomize Passwords after Resource Discovery

After onboarding the resources and associated accounts, it is essential to randomize the passwords of the discovered accounts to prevent continued direct access to passwords that are known or stored by users before PAM360 was deployed. Existing credentials could have been stored in spreadsheets, text files, or other media, allowing users to access resources directly outside PAM360. Randomizing the passwords ensures that previously known credentials can no longer be used for direct access and replaces weak or reused passwords with strong, unique credentials managed by PAM360.

- To discover accounts of a specific resource, select the desired resources on the Resources tab, then select **Discover Accounts** from the top pane.
- To randomize passwords for discovered accounts, navigate to the Resources tab, select the desired resources, click the **Resource Actions** button in the top pane, then select **Configure** >> **Remote Password Reset** from the displayed options.

5.5 Organize Resources into Resource Groups

Use resource groups to organize resources and simplify the administration of privileged accounts. Several advanced password management operations, including on-demand password rotation, automated password delegation, and scheduled password rotation, can be performed at the resource group level. Where possible, use criteria-based resource

groups to organize resources based on the defined criteria. PAM360 automatically identifies resources that meet the specified criteria and adds them to the corresponding group, eliminating the need to associate all required resources to the resource group. Any resources discovered or onboarded to PAM360 that match the resource group criteria will be automatically added to the respective resource groups.

5.6 Nested Resource Groups

Use nested resource groups to establish a logical hierarchy that makes it easier for users to locate and manage resources, particularly in environments with numerous resources. Organize the password explorer tree according to your organization's departments or teams, and place the corresponding resource groups under the appropriate organizational nodes. For a consistent navigation experience across the organization, enable the password explorer tree view setting to display a uniform tree for everyone. Consider renaming the top-level Resource Groups node to the organization's name and creating subordinate nodes for departments or teams.

To allow administrators to manage the resource groups password explorer tree, navigate to **Admin >> Customization >> General Settings >> Password Retrieval** and enable the **Allow administrators to manage nested groups via Password Explorer** option. Once enabled, resource groups managed by all administrators will be displayed in the Password Explorer tree. However, users will only see the resources they own or those shared with them.

5.7 Additional Fields

Use additional fields to capture organization-specific information during resource onboarding. Additional fields can be used to record attributes not available in the default resource properties, enabling administrators and users to identify and locate resources more efficiently. Additional fields can also be used when creating criteria-based resource groups, searching for specific resources or passwords, and sharing resources, making them useful for both resource organization and access management.

6. Granular Access Control and Password Sharing

This section outlines the recommended best practices for securely sharing privileged credentials and controlling access to resources in PAM360. It covers granular sharing privileges, group-based sharing, access control workflows, just-in-time privilege elevation, and integration with enterprise ticketing systems.

6.1 Password Sharing

When sharing resources, assign the minimum level of access required for users or user groups to perform their responsibilities. PAM360 provides the following sharing privileges:

- **RemoteApp Only:** Allows users to access the configured application associated with the resources.
- **View Passwords:** Allows users to retrieve and view shared passwords.
- **Modify Passwords:** Allows users to access and modify the shared passwords.
- **Full Access:** Provides complete management access to the shared resource or resource group, including the ability to share the resource, resource group, or account passwords.

As a best practice, provide **View Passwords** permissions wherever they are sufficient for the user's operational requirements. Exercise caution when assigning **Full Access**, as users with this privilege have extensive control over the shared resource or password and can modify, delete, and re-share it with other users. PAM360 also supports sharing resources without exposing passwords in plain text when auto-logon is configured for the resource. This allows authorized users to initiate remote sessions to the resource without viewing the credentials.

6.2 Group-Based Sharing

Where possible, share resource groups with user groups instead of sharing individual resources or passwords with individual users. Group-based sharing simplifies access

management, supports bulk operations, and reduces the administrative effort required to maintain permissions as users and resources change.

- For example, create a criteria-based resource group with Windows resource type as the matching criteria, which will add all Windows resources in your environment to the dynamic group. As new Windows resources are added, they are automatically included in the criteria-based resource group.
- Similarly, create a user group for Windows administrators and share the resource group containing Windows resources to this user group. If you have integrated AD/LDAP, you can import the user group directly and enable auto-synchronization of the user database.

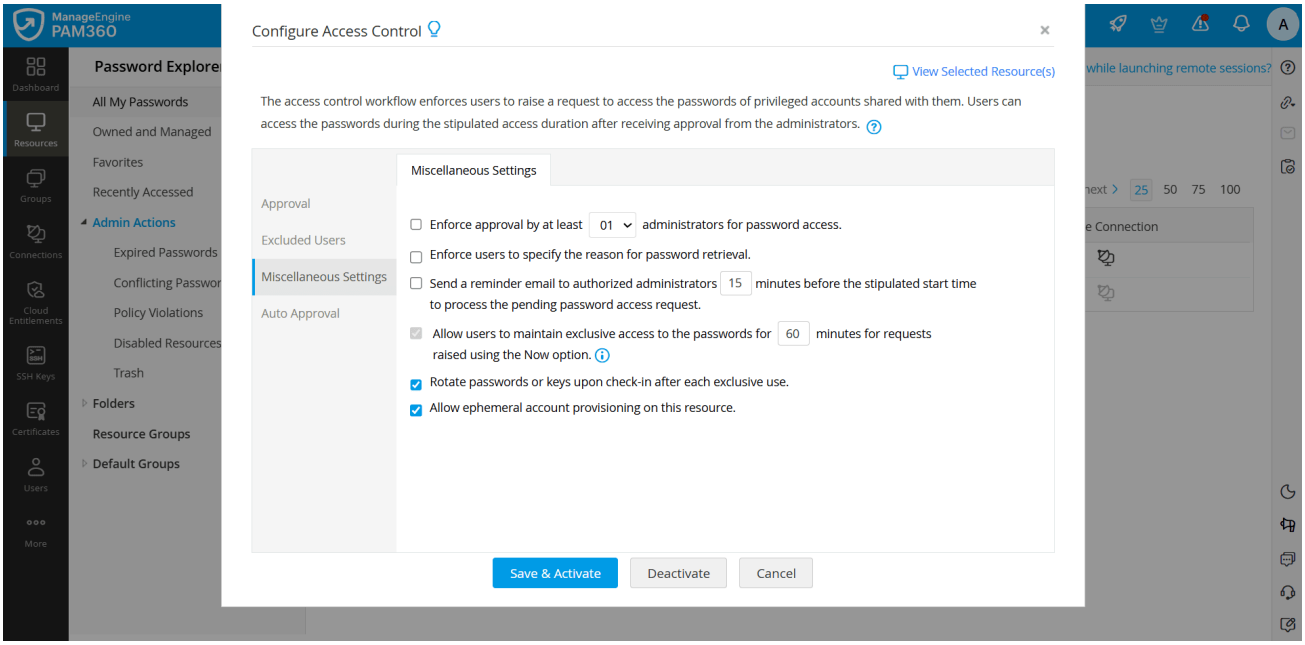
Whenever a new Windows administrator joins the organization, their AD account will automatically be added to PAM360's Windows administrator user group. The new user will subsequently gain access to the Windows resource group, inheriting the group's permissions to manage Windows machines. This approach provides a scalable access model in which resource and user group membership can be maintained independently while permissions remain consistent.

6.3 Access Control Workflow

The access control workflow in PAM360 is a request-release mechanism in which users should raise a request to gain access to passwords, which should be approved by administrators, allowing them to access the target machines. Configure access control workflows for critical resources to prevent users from directly accessing privileged passwords without prior approval.

Configure access restrictions such as time-limited access to further limit exposure of critical credentials. For highly sensitive resources, enable dual approval so that two or more authorized administrators should approve an access request before users can access the credentials. Dual approval is particularly useful when responsibility for a critical administrative credential is shared between multiple teams or departments.

To configure access control for a resource, navigate to the **Resources** tab, click on the Resource Actions icon under the Actions column beside the desired resource, and select **Configure** >> **Access Control** from the displayed options. Alternatively, you can select the desired resources, click the **Resource Actions** icon in the top pane, and select **Configure** >> **Access Control** from the displayed options. Explore this **link** for more information about the access control workflow in PAM360.



6.4 Just-In-Time Privilege Elevation

The Just-in-Time (JIT) privilege elevation feature in PAM360 provides temporary elevated privileges to local and domain user accounts on Windows resources when administrative access is required only for a specific task or period. This enables administrators to grant elevated privileges only when required and automatically remove them after the specified period, reducing the risks associated with permanently privileged accounts.

For example, a local Windows account such as 'dbuser' that normally operates without administrative privileges can be temporarily elevated to the privilege level of an administrator or another designated privileged user for the required duration. Similarly, domain users can be granted temporary elevated privileges through the appropriate Active Directory security groups. This enables administrators to assign users with elevated

privileges to perform privileged tasks without standing privileges or sharing administrative credentials.

Where feasible, use Ephemeral Account Provisioning in PAM360 to implement Zero Standing Privileges (ZSP) and minimize the exposure of persistent privileged accounts. PAM360 can dynamically create a temporary privileged account on the target resource when access is approved and automatically remove the account after the session ends or access is checked back in. This provides users with time-bound, on-demand access while adhering to the Principle of Least Privilege (PoLP), reducing the risk of credential misuse and lateral movement. Ensure that ephemeral access is configured only for appropriate resources, with the required remote login credentials and local privilege groups, and integrated with access control workflows so that privileged access remains controlled and fully auditable. Explore this **link** for the detailed steps to configure ephemeral account provisioning in PAM360.

6.5 Ephemeral Account Provisioning

Leverage Ephemeral Account Provisioning in PAM360 to implement Zero Standing Privileges (ZSP) and minimize the exposure of persistent privileged accounts. PAM360 dynamically creates a temporary privileged account on the target resource when accessing the target resource, and automatically removes the account after the password is checked back in. This provides users with time-bound, on-demand access while adhering to the principle of least privilege, reducing the risk of credential misuse. Ensure ephemeral access is configured only for appropriate resources, with the required remote login credentials so that privileged access remains controlled and fully auditable. Explore this **link** for the detailed steps to configure ephemeral account provisioning in PAM360.

6.6 Enforce Users to Provide a Reason while Accessing Passwords

PAM360 records password-related activities in its audit trails, including details such as the timestamp and IP address associated with the activity. As an additional accountability measure, PAM360 allows administrators to mandate users to provide a reason whenever

they retrieve a password. The reasons provided by users are also recorded in the Audits tab along with other information about password activity, providing additional context for access reviews and forensic investigations. From a security perspective, this requirement should be enforced to ensure that the business justification for password retrieval is consistently captured.

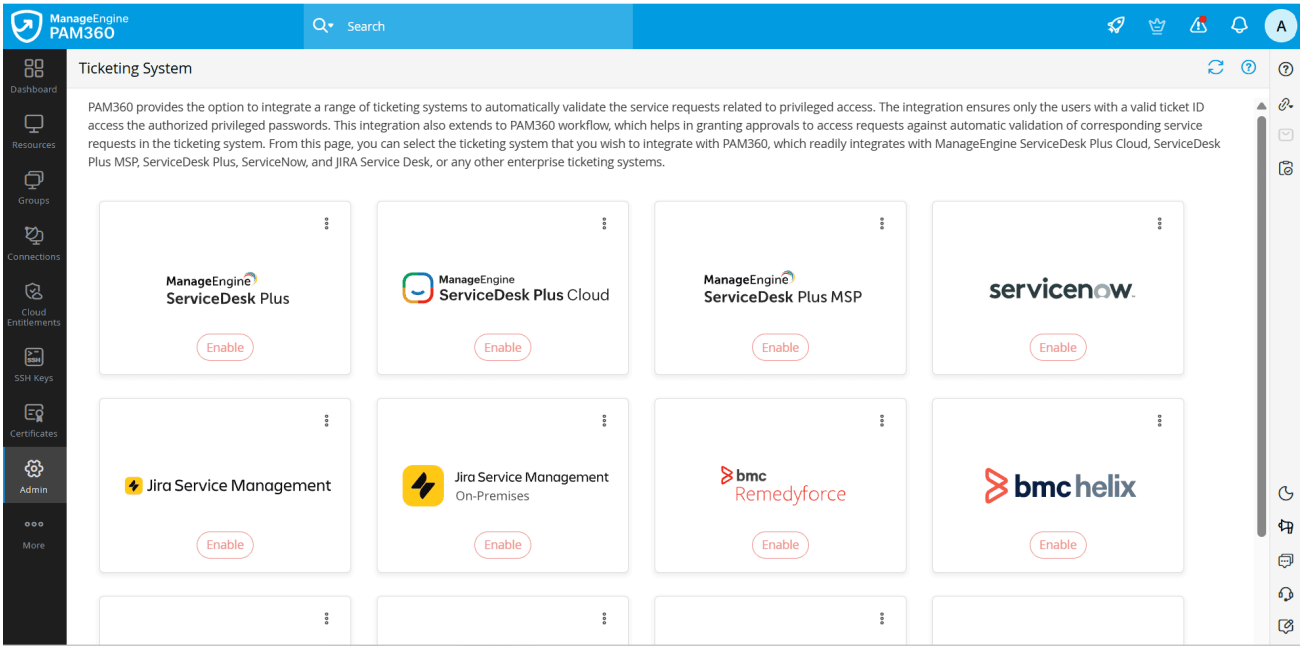
To mandate users to provide a reason while retrieving a password, navigate to **Admin** >> **Customization** >> **General Settings** >> **Password Retrieval**, and enable the **Enforce users to provide a reason for password retrieval** option.

6.7 Integrate PAM360 with Enterprise Ticketing Systems

PAM360 seamlessly integrates with a range of ticketing systems to automatically validate service requests related to privileged access. The integration ensures that users get authorized privileged access only with only with a valid ticket ID. PAM360 can validate the service requests and provide privileged access to the password associated with the ticket ID. To enable a stronger retrieval workflow for your critical resource passwords, we suggest you integrate PAM360 with your enterprise ticketing system. PAM360 supports integration with multiple ticketing systems, including:

- **ManageEngine ServiceDesk Plus**
- **ManageEngine ServiceDesk Plus Cloud**
- **ManageEngine ServiceDesk Plus MSP**
- **ServiceNow**
- **Jira Service Management On-Premises**
- **Jira Service Management Cloud**
- **BMC Helix Remedyforce**
- **BMC Helix ITSM**
- **TOPdesk**
- **GLPI**
- **Salesforce Service Cloud**

Explore the provided links for more information about the ticketing system integrations.



To configure the ticketing system integration, navigate to **Admin >> Integration >> Ticketing System Integration**.

7. Password Policies

This section outlines the recommended best practices for configuring password policies in PAM360. It covers defining separate policies for critical resource groups and sensitive accounts, and setting password age requirements to ensure privileged passwords are regularly changed.

7.1 Configure Unique Password Policies for Critical Resource Groups

Password policies help define password strength by mandating password requirements such as character complexity. PAM360 allows you to configure different password policies for different resource groups. For highly sensitive resources, organize them into a dedicated resource group and associate a separate password policy with stricter requirements. This allows you to apply stronger password controls to critical resources without imposing the same requirements across the entire environment.

To associate a password policy with a resource group, navigate to the **Groups** tab, select the desired resource group, click on the **Bulk Configuration** option in the top pane, and select **Associate Password Policy** from the displayed options.

7.2 Configure Account-Level Password Policies

A resource may contain one or more administrative accounts along with other standard accounts. To provide stronger protection for privileged accounts on critical resources, configure a separate password policy at the account level. This allows you to apply stricter password requirements specifically to sensitive accounts without affecting other accounts associated with the resource.

To associate a password policy at the account level,

- Navigate to the **Resources** tab and click on the desired resource.
- In the **Account Details** window, click the **Account Actions** icon beside the desired

resource and select **Edit Account** from the displayed options.

- In the **Edit Account** window that appears, select the desired policy from the Password Policy drop-down menu.

7.3 Define Password Age when Creating Policies

When configuring a password policy, always specify a maximum password age to ensure passwords are automatically reset when they reach the defined age. If no maximum password age is specified, the passwords will not expire. Configuring a defined password age helps ensure that privileged passwords are periodically changed and reduces the risk associated with long-lived credentials.

8. Password Resets and SSH Key Rotation

This section outlines the recommended best practices for periodically resetting privileged passwords and rotating SSH keys. It covers scheduled password randomization, selecting the appropriate password reset mode based on the target environment, and restarting dependent services after password resets to ensure continued operation.

8.1 Perform Periodic Password Randomization and Key Rotation

Secure management of privileged accounts requires strong, unique passwords that are periodically reset. Configure scheduled password resets for resource groups in PAM360 to ensure that privileged passwords are regularly randomized. A 90-day password reset interval is a commonly used timeframe in IT compliance requirements such as PCI DSS. In addition to scheduled password resets, configure passwords to be automatically reset in the following situations:

- After a user completes their password access and checks the password back in.
- When sharing permissions are revoked for users with whom the password was previously shared.
- When the password reaches the maximum age defined in the associated password policy.

For SSH keys, configure regular key rotation every 30–45 days and perform bulk key rotation immediately after onboarding users.

8.2 Choose the Appropriate Password Reset Method

PAM360 supports remote password reset in three different ways: agentless, agent-based, and through Application Gateways. Choose the password reset method based on whether the PAM360 server has direct connectivity to the target resources.

- **Agentless Mode** - Use agentless password reset when the PAM360 server can directly connect to the target resource. In this method, PAM360 connects to the

target system and changes the password. The required administrative credentials should be available in PAM360 to perform the password rotation. When PAM360 is installed on Linux, two accounts are required: one with root privileges and another normal user account for remote login.

- **Agent-Based Mode** - Use the agent-based password reset method for resource-specific requirements when the target resource does not reside in the same network as the PAM360 server. In this mode, an agent is deployed on the remote host to execute the password reset operation. Communication between the agent and the PAM360 application server is one-way and occurs via a secure HTTPS connection, eliminating the need to open inbound firewall ports. Use agent-based mode in the following scenarios:
    - Administrative credentials for the resource are not available in PAM360.
    - Required services are not running on the target resource, such as Telnet or SSH on Linux systems or RPC on Windows systems.
    - PAM360 is installed on Linux, and password changes need to be performed on Windows resources.
    - Resources are distributed across two environments, such as environments A and B, with a firewall between them. In this scenario, PAM360 can be installed in environment A and use agentless mode for resources in that environment, while agents can be installed on resources in environment B for password resets. This allows passwords in both environments to be managed without introducing additional firewall port exceptions.
- **Application Gateway** - Prefer Application Gateway when the target resources do not reside in the same network as the PAM360 server and multiple resources within these remote or segmented networks should be managed. The Application Gateway is installed on a machine that can communicate with both the PAM360 server and the target resources. Password verification and reset operations initiated from PAM360 are routed through the Application Gateway to the associated resources. A single Application Gateway can manage multiple associated resources within a

network segment. Therefore, prefer an Application Gateway over installing agents individually on every resource when:

- Multiple resources are located within the same DMZ, secure subnet, branch network, or isolated environment.
- A common machine within the network can connect to the resources that must be managed.
- The required resource types and password management operations are supported through the Application Gateway.

Where direct connectivity is available, agentless mode is the preferred and more convenient method for performing password resets.

8.3 Restart Services After Password Resets

PAM360 can periodically reset the passwords of Windows domain accounts used to run services, scheduled tasks, and IIS application pools and update the new passwords across the dependent services and application pools. To ensure that services, scheduled tasks, and application pools continue to function with the updated credentials, enable the option to automatically restart the associated services after a password reset while configuring the remote password reset for domain accounts.

9. Secure Remote Access

This section outlines the recommended best practices for securing remote access to privileged systems through PAM360.

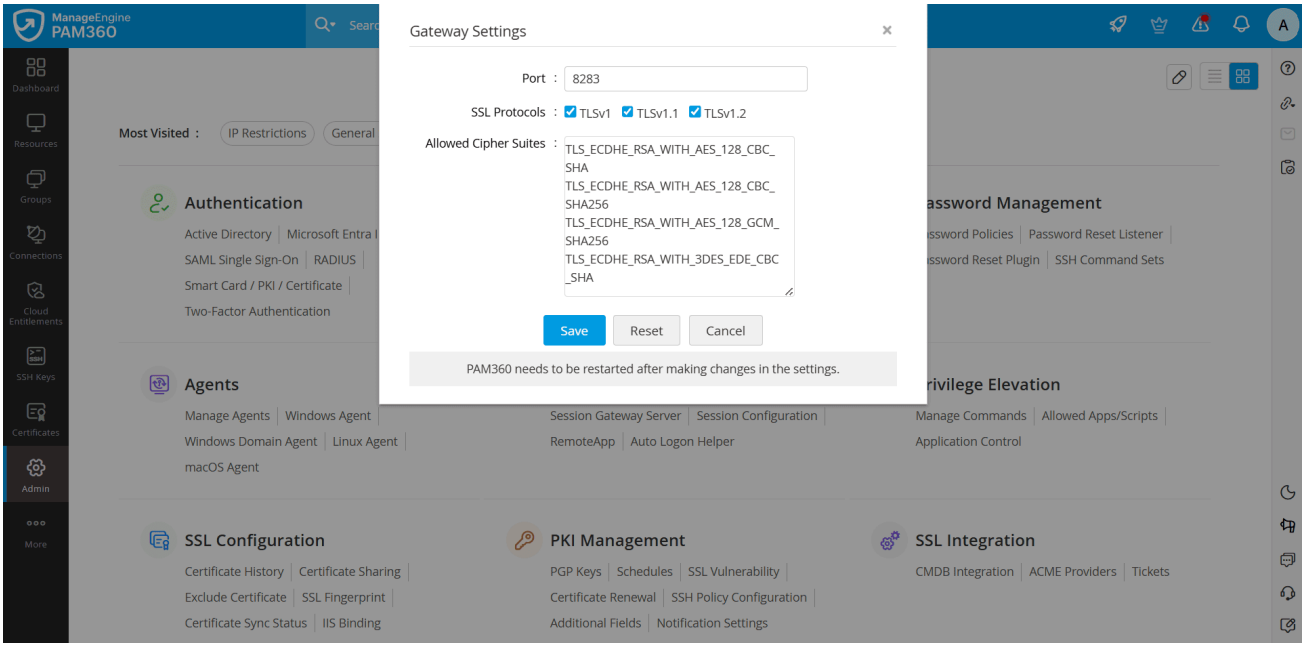
9.1 Enable Automatic Logon Without Revealing Passwords

After configuring the auto-logon helper for remote connections, PAM360 allows users to connect to remote systems with a single click without requiring them to enter passwords manually. To ensure password security and minimize unnecessary exposure of privileged credentials, prevent users from retrieving these passwords in plain text when the auto-logon helper is configured and password visibility is not required.

You can prevent users from retrieving passwords in plain text by enabling the **Mask passwords for selected user roles** option under **Admin >> Customization >> General Settings >> Password Retrieval**, where you can mask passwords for all user roles, non-administrator roles, or custom user roles in your environment.

9.2 Configure Session Gateway Settings

PAM360 provides configurable session gateway settings to secure and manage remote connections. Administrators can customize gateway settings such as the cipher suites used for SSL communication, the gateway port, and SSL protocols used for remote connections. Configure these settings according to the organization's security and remote access requirements.



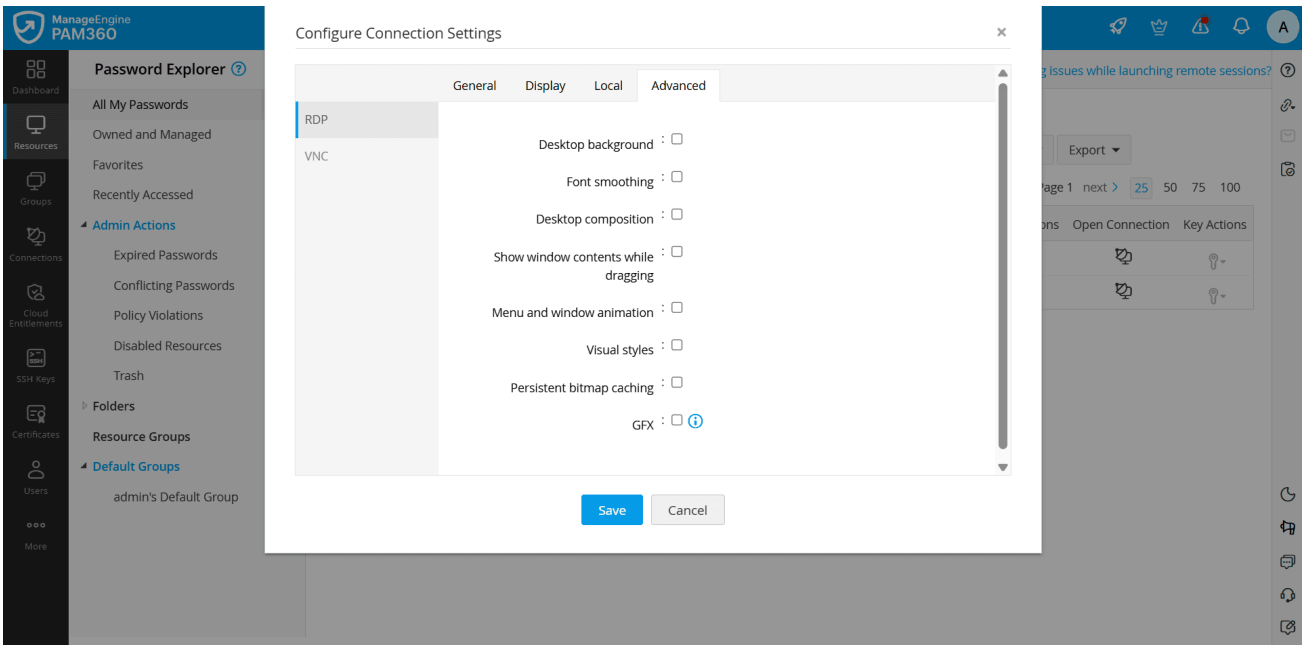
To configure gateway settings, navigate to **Admin >> Privileged Session >> Session Gateway Server**. For additional customization options and technical details, refer to the **gateway.conf** file located in **<PAM360_installation_directory>\conf** folder.

9.3 Configure Advanced Connection Settings

PAM360 provides advanced connection settings that can be customized to improve the speed and performance of remote connections. These settings are available for RDP, SSH, and VNC connections and provide centralized configuration for remote sessions. Changes made to these settings are also applied locally on the remote system. Available settings include keyboard layout, desktop background, mapped drives, and remote audio support.

To configure these settings, navigate to the **Resources** tab, switch to the **Passwords** pane, and click the **Account Actions** icon next to the required account and select **Connection Settings** from the displayed options. Alternatively, you can also select the desired accounts, click the **Account Actions** button in the top pane, and select **Connection Settings** from the displayed options. In the **Configure Connection Settings** window, you can manage the connection settings for RDP, SSH, and VNC sessions. The available settings will depend on the selected resource type. Click here to learn in detail about the advanced connection

settings in PAM360.



9.4 Discover and Configure RemoteApp for Windows Servers

RemoteApp allows users to access specific applications configured on Windows servers without providing access to the entire remote desktop. Configure RemoteApp for Windows resources where users require access to specific applications rather than unrestricted access to the remote system.

PAM360 allows you to either automatically discover RemoteApps configured on Windows target systems or manually add them to PAM360. Restricting users to specific RemoteApps helps reduce the scope of privileged remote sessions by limiting their access to the application required for their tasks.

For example, if **SQL Studio** is configured as a RemoteApp and assigned to a user, launching the session opens SQL Studio directly. The user cannot access the taskbar, navigate to other areas of the remote desktop, or perform operations outside the configured application.

To avail this feature, the respective RemoteApps required RemoteApps should be installed and configured on the target Windows servers before they can be used with PAM360.

10. Privileged Access to Third Parties

This section outlines best practices for managing privileged access to third parties such as contractors, consultants, and vendors. It covers temporary and least-privilege access, secure remote access through PAM360.

10.1 Manage Third-Party Access to Corporate Systems

Third parties such as contractors, consultants, and vendors may require access to corporate IT resources to fulfill contractual obligations and other business requirements. When granting privileged access to third-party vendors, grant only the minimum privileges required and restrict access to a defined period according to the duration of the business requirement. Consider the following best practices when providing privileged access to third parties:

- **Manage third-party vendors as PAM360 users:** Add third-party users to PAM360 and require them to establish remote sessions to target systems through PAM360. This allows their privileged access to be centrally managed and monitored.
- **Prevent plain-text password exposure:** After configuring the auto-logon helper for a resource, allow third parties to access the target system without revealing the underlying credentials in plain text.
- **Provision ephemeral accounts**: Configure ephemeral account provisioning to grant privileged access to third-party users through temporary accounts. This allows users to request temporary, time-bound privileged accounts for just-in-time access instead of relying on persistent privileged accounts. This helps eliminate standing privileges and reduces the risk associated with compromised or forgotten privileged accounts.
- **Enforce access control workflows:** Configure access control workflows for resources to be accessed by third-party users to enforce time-limited password access and automatically reset passwords after the approved usage period.
- **Configure session recording** - Ensure privileged session recording is configured in your environment, allowing administrators and auditors to review privileged sessions

periodically and maintain a complete record of all operations performed by users on privileged resources.

- **Monitor privileged sessions:** Regularly shadow third-party sessions and review privileged session recordings to identify suspicious or malicious activity and take immediate remediation measures when required.
- **Reset passwords after contract termination:** When a vendor or contractor's engagement ends, immediately reset the passwords of all resources accessed by third-party users to prevent continued access using previously authorized credentials.

11. Data Center Remote Access

This section outlines recommended best practices for securely accessing remote resources through landing servers, eliminating the need to share jump server credentials, and securely exporting passwords for environments where PAM360 cannot be accessed due to the lack of internet connectivity.

11.1 Avoid Sharing Jump Server Credentials

Accessing resources in remote data centers often requires users to connect through multiple jump servers because direct access to the target systems is restricted. This can require users to authenticate manually at each stage using separate jump server credentials. Sharing these credentials among users is not a secure practice, as it makes it difficult to control and trace individual access.

Instead, use the landing server configuration in PAM360 and require users to access data center resources through PAM360. This provides secure, one-click access to the target resources while eliminating the need for users to authenticate at each jump server manually. It also centralizes the management of jump server credentials within PAM360.

11.2 Export Passwords for Offline Access

If a data center environment does not permit internet connectivity, users in that environment may not be able to access PAM360 to retrieve the required passwords. In such scenarios, export the required passwords beforehand as an encrypted HTML file and securely make the file available for offline access.

To export the passwords of privileged resources and associated accounts, navigate to the **Resources** tab, select the desired resources, click the **Resource Actions** button in the top pane, and select **Export Passwords** from the displayed options.

12. Session Management and Monitoring

This section outlines the recommended best practices for monitoring, recording, and managing privileged sessions in PAM360. It covers real-time session monitoring, session recording, and the periodic purging of recorded sessions to support privileged access oversight, security investigations, and efficient storage management.

12.1 Monitor Critical Sessions in Real Time

Use the session shadowing feature to establish dual controls over critical privileged sessions and monitor user activity in real time. Administrators can join active sessions to observe user activity without interrupting the end user's session. This capability is particularly useful for providing remote assistance, troubleshooting, and monitoring to protect against potentially malicious activity.

Session collaboration also allows multiple users to work together within the same RDP or SSH session by sharing control of the mouse cursor. If suspicious activity is detected, administrators can terminate the session immediately to prevent further misuse of privileged access.

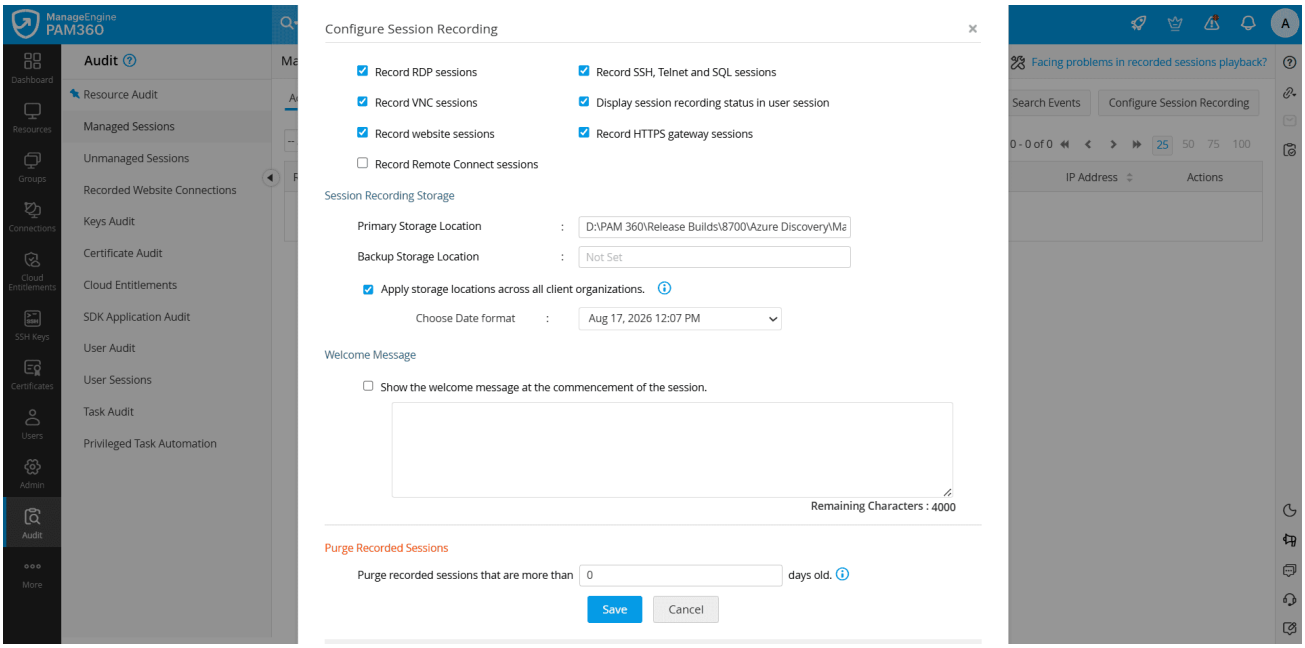
To monitor active sessions, navigate to **Audit >> Active Privileged Sessions** and click **Join** beside the required session. To terminate a session, click **Terminate** beside the required session.

12.2 Record Privileged Sessions

Enable session recording for privileged sessions to maintain a detailed record of user activity for auditing, investigation, and compliance purposes. PAM360 supports session recording for RDP, VNC, SSH, Telnet, and SQL sessions launched through the application. Configure appropriate external storage and backup locations for session recordings to suit your organization's storage, retention, and security requirements. Administrators and Auditors can review recordings from the **Audits** tab along with relevant information such as the resource to which the session was launched, account name, user who initiated the

session, session launch time, session duration, etc.

To configure session recording, navigate to **Audit** >> **Managed Sessions/Unmanaged Sessions** and click the **Configure Session Recording** button in the top pane. On the **Configure Session Recording** page that appears, you can enable session recording for all session types, configure session recording storage, and specify a welcome message to be displayed to users.



12.3 Regularly Purge Recorded Sessions

Regularly review and purge session recordings that are no longer required to free up storage space. This is particularly important in large environments where a high volume of RDP, VNC, SSH, Telnet, and SQL sessions may be recorded. Define a retention period based on your organization's security, operational, and compliance requirements, and delete recordings older than the configured retention period. Recordings can also be stored on a local drive and moved to another location when required.

For selective cleanup, individual session recordings or chat histories can be deleted from the **Audit** tab. To maintain accountability and prevent unauthorized deletion of session recordings, PAM360 requires approval from at least two administrators before a session

recording or chat session can be deleted.

To delete a specific recording or chat history, navigate to **Audit >> Managed/Unmanaged Sessions** and click the **Delete** icon beside the required session.

12.4 Configure Session Events Monitoring

Configure Session Events Monitoring to maintain comprehensive visibility into privileged user activity and system events on Windows systems, including activity performed during privileged sessions launched via PAM360 or those launched directly outside PAM360. Set up the PAM360 agent with System Events Logging and Keystroke Logging on critical Windows resources to capture session logon and logoff events, program execution, active window changes, commands, and user keystrokes. This provides a detailed, timestamped audit trail that supports security monitoring, compliance, and forensic investigations. Where appropriate, use the event filters and global Search functions on the Audits tab to focus on relevant activities and investigate suspicious or unauthorized actions. Explore this **link** for more information about session events monitoring in PAM360.

13. SSL/TLS Certificate Management

This section outlines the recommended best practices for discovering, acquiring, deploying, and managing SSL/TLS certificates in PAM360. It covers certificate discovery and import; certificate requests and acquisition; deployment; integration with certificate authorities and the ServiceDesk Plus CMDB; and SSL vulnerability scanning.

13.1 Discover and Import Certificates

Use PAM360's certificate discovery feature to identify and import certificates associated with user accounts in Active Directory, certificates stored in the Microsoft Certificate Store, and certificates issued by public and private certificate authorities. To maintain an up-to-date certificate inventory, configure scheduled certificate discovery tasks to periodically discover and import certificates from the required resources into PAM360.

13.2 Follow Secure Certificate Request and Acquisition Practices

You can seamlessly create self-signed certificates from PAM360. However, use self-signed certificates only within internal networks where the required trust relationships are established. For stronger cryptographic security, replace SHA-1 certificates with SHA-2 certificates wherever applicable.

For public-facing websites, always obtain SSL certificates from trusted third-party certificate authorities. When acquiring a certificate from a trusted CA, attach the certificate when closing the certificate request in PAM360 to ensure it can be centrally managed. Organize acquired certificates into logical groups to simplify certificate management and enable bulk operations.

13.3 Ensure the Latest Certificate Version is Deployed

Always ensure that the latest version of a certificate is active on the servers where it is deployed. When multiple versions of the same certificate are managed in PAM360, verify

that the correct and latest version is deployed to the corresponding endpoint servers. Use bulk deployment when the same SSL certificate needs to be deployed across multiple servers.

13.4 Integrate with Public Certificate Authorities (CA)

Use PAM360's integration with public certificate authorities to manage the certificate lifecycle centrally, including requesting, acquiring, deploying, renewing, and tracking certificates. Certificate requests can be initiated from the PAM360 web interface using the built-in CSR generation tool. Follow these best practices when managing certificates through certificate authority integrations:

- Immediately revoke a certificate if its private key is compromised and submit a new certificate request using a new private key.
- Generate a new private key whenever a certificate is renewed.
- Configure agent mapping to facilitate timely certificate renewal through automated domain validation.

13.5 ServiceDesk Plus CMDB Integration

Integrate PAM360 with ManageEngine ServiceDesk Plus CMDB to export SSL certificate details from the PAM360 repository to the CMDB. This allows administrators to centrally monitor certificate usage, expiry, and other certificate-related information from the ServiceDesk Plus interface.

13.6 Perform SSL Vulnerability Scanning

Perform SSL vulnerability scanning to identify vulnerabilities in certificates managed via PAM360 and check certificate revocation status through CRL and OCSP. When a certificate or its associated server configuration is identified as vulnerable, take the necessary remedial measures, such as replacing the certificate or updating the server configuration. Disable the SSL 3.0 protocol across endpoints within your network to prevent forced

fallback to SSL 3.0 and reduce exposure to vulnerabilities such as POODLE. Configure periodic vulnerability scans where required and enable email notifications to keep administrators informed about the scan results.

14. Auditing and Reporting

This section outlines the recommended best practices for auditing privileged activities, monitoring important events, generating reports, and managing audit data in PAM360. It covers regular internal audits, activity alerts, consolidated notifications, customized email templates, SIEM integration, scheduled reports, and audit record retention.

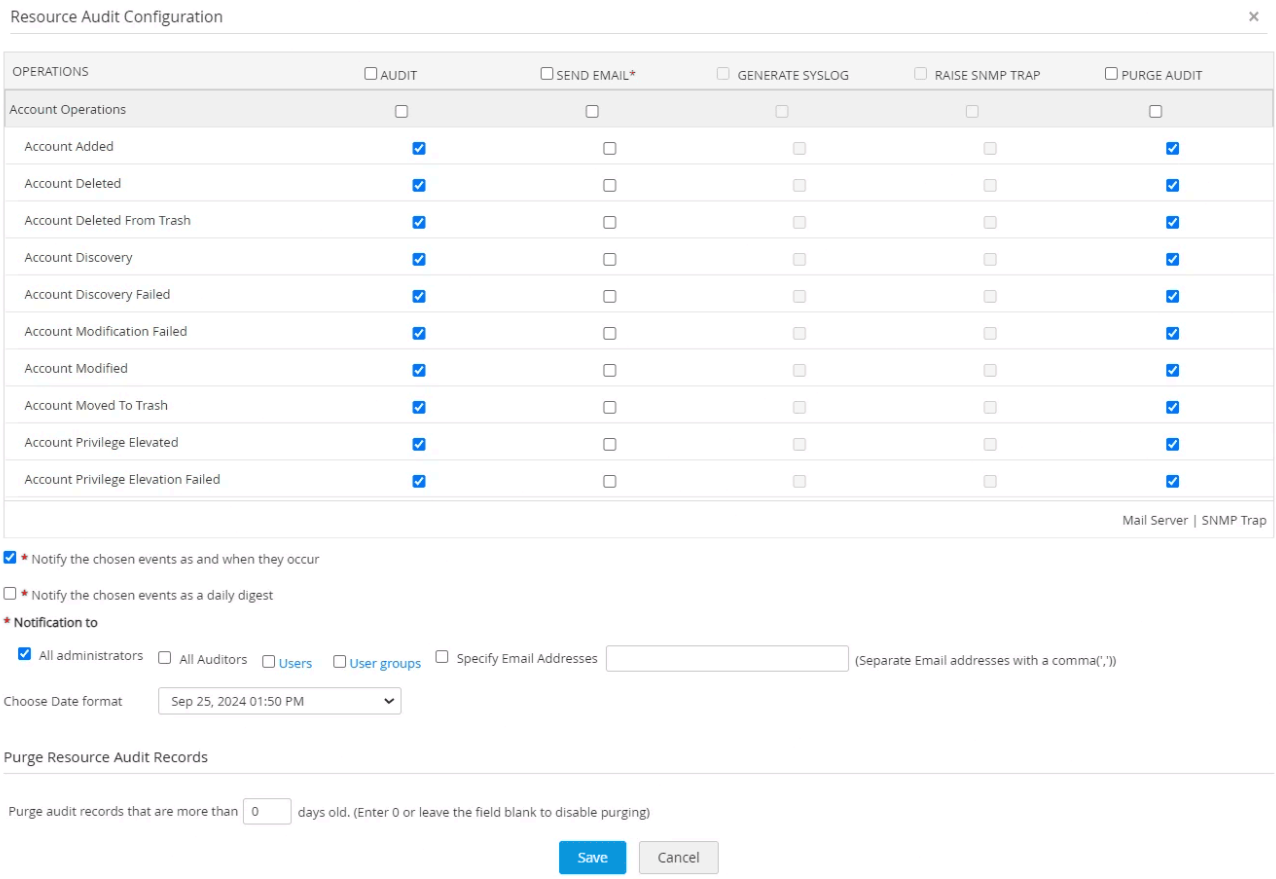
14.1 Conduct Regular Internal Audits

As PAM360 manages sensitive privileged access information, it maintains a complete record of all user activities within the application to ensure comprehensive tracking. All user actions and resource events are recorded as audit entries, along with the corresponding timestamps and IP addresses from which users accessed the application. Review audit records regularly for more information about privileged access to identify and eliminate any gaps in privileged access.

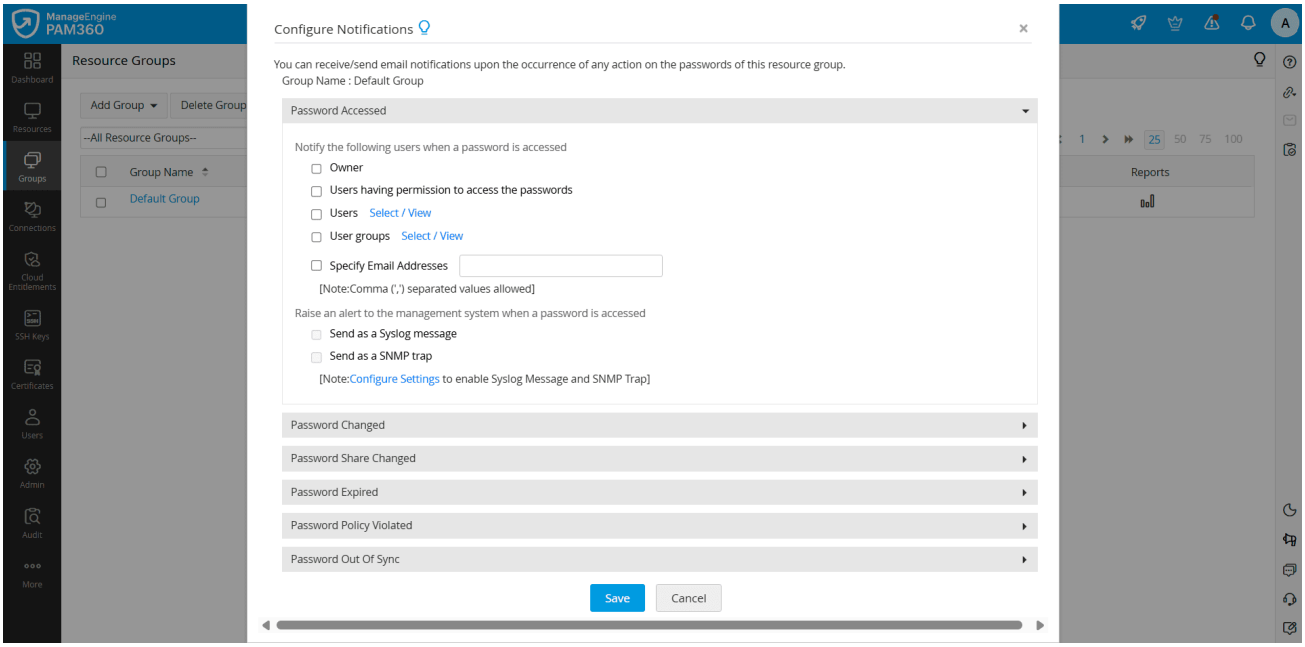
14.2 Configure Alerts for Critical Events

PAM360 provides flexible options for selective auditing. Configure email notifications for important privileged access activities to keep administrators informed of significant changes and user operations. You can configure notifications to alert designated recipients when specific events occur, enabling improved monitoring and tighter control over privileged access activities. Recommended events include activities such as new user additions, password deletions, and password sharing.

Operational-level audits can be configured from the **Resource Audit**, **User Audit**, and **Task Audit** pages. To configure the resource audit, navigate to **Audit** >> **Resource Audit**, click the **Audit Actions** button in the top pane, and select **Configure Resource Audit** from the displayed options. In the **Resource Audit Configuration** page, you can select the desired events to generate audit trails, send email notifications, generate syslog messages, raise SNMP traps, and purge audit trails. Similarly, alerts for user and task audit events can be configured from the respective pages.



To configure alerts for password-related events, go to the **Groups** tab, click the **Actions** icon next to the desired resource group, and select **Configure Notifications** from the displayed options. In the **Configure Notifications** window, you can configure notification alerts, generate syslog messages, and raise SNMP traps for various password-related events.



14.3 Use Daily Digest Emails to Reduce Notification Volume

When alerts are configured for a large number of resources and activities, frequent notifications can result in excessive email traffic. If real-time notifications are not required for every event, configure daily digest emails to receive a consolidated summary of notifications at the end of each day.

14.4 Customize Email Templates

Customize PAM360's default email notification templates to align with your organization's requirements. This allows administrators to provide relevant information and maintain consistency across notifications. Email templates can be configured under **Admin >> Customization >> Email Templates**.

14.5 Integrate with SIEM and Management Systems

If your organization uses an external SIEM tool, you can integrate this SIEM tool with PAM360 to feed syslog messages to the tool whenever privileged activities occur within PAM360. This integration provides a holistic view of privileged access with overall network

activity from a central location, facilitating security monitoring.

14.6 Schedule Periodic Report Generation

Use PAM360's scheduled report generation feature to periodically generate reports providing detailed insights into privileged access instead of manually generating recurring reports. Schedule the reports required for monitoring password inventory, password expiration status, user access frequency, user activity, and other operational information. Scheduled reports are automatically generated at the configured intervals and sent to the registered email address.

14.7 Purge Audit Records Periodically

Audit records can grow rapidly as PAM360 captures privileged operations and user activities. If audit records older than a defined retention period are no longer required, configure periodic purging to manage storage efficiently.

To automatically purge audit records that are older than a specified number of days, navigate to **Audit** >> **Resource Audit**, click the **Audit Actions** button in the top pane, and select **Configure Resource Audit** from the displayed options. In the **Resource Audit Configuration** page, specify the required retention period in the checkbox provided under the Purge Audit Records section. For example, entering 90 will delete audit records that are older than 90 days. By default, the purge option is disabled and the number of days is set to zero.

15. External Integrations

This section outlines the recommended practices for extending PAM360's privileged access management capabilities through external integrations with analytics platforms, vulnerability scanners, SIEM solutions, CI/CD platforms, RPA tools, and other enterprise products. These integrations help organizations centralize privileged access information, automate security workflows, and improve visibility across their IT environment.

15.1 Advanced Analytics

PAM360 integrates with analytics platforms to analyze privileged activities and identify potentially suspicious behavior. Through Advanced Analytics, you can:

- Detect unusual user behavior and identify potential security threats.
- Analyze historical audit logs to identify anomalous activities.
- Identify the sources of anomalies using the Zia analytics assistant.
- Combine data from multiple sources and PAM360 modules to gain consolidated insights and improve visibility.
- Email, export, publish, and share key findings through secure sharing options.

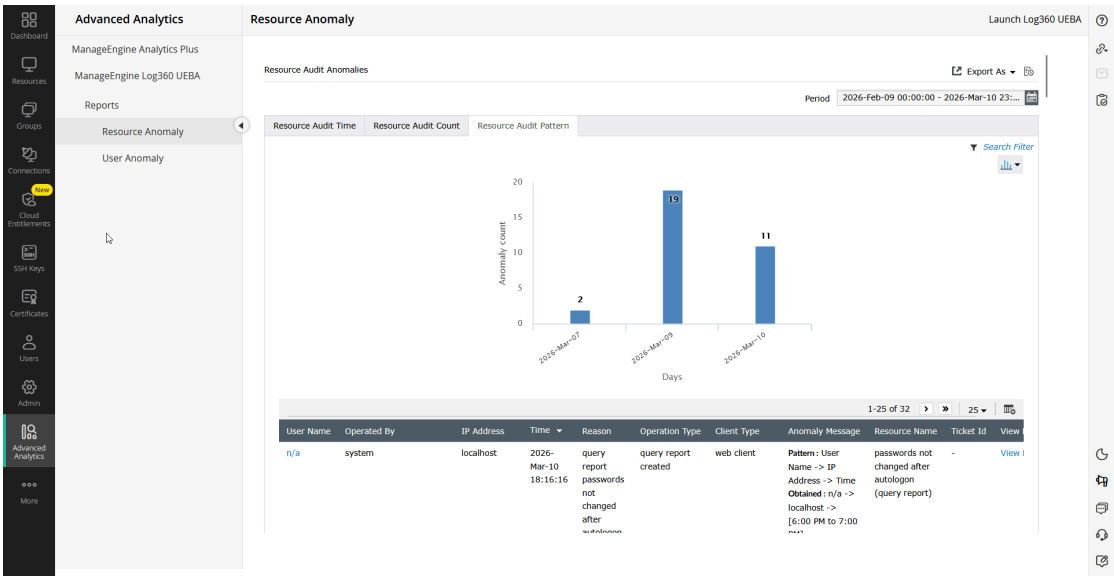
PAM360 supports integration with ManageEngine Analytics Plus and ManageEngine Log360 UEBA. These integrations provide deeper visibility into privileged activities through dashboards and behavioral analysis, helping you identify anomalous activities, monitor risk patterns, and receive notifications when configured thresholds are exceeded.

1. **Analytics Plus Integration:** Navigate to **Advanced Analytics** >> **ManageEngine Analytics Plus** to view dashboards based on the data imported from PAM360 into Analytics Plus. The following dashboards provide insights into different aspects of privileged activity:

    - **User Activity Dashboard:** Provides information about user activity in PAM360, including the number of users who accessed a particular resource or account during a specified period, the most active user, the number of users added

during the selected period, and the user with the highest level of access.

- **Operations Overview:** Provides an overview of resource and password-related operations, including the number of resources and accounts, the most active user, the most-used resource, and the percentage of password accesses.
- **Access Control Dashboard:** Provides information on resource access, including the user with access to the highest number of accounts, the most widely shared account, the total number of password requests, and the number of requests revoked during the selected period.
- **Anomaly Detection:** Provides information about anomalous activities during the selected period, including the number of operations performed outside business hours, the most frequent operation performed outside business hours, the number of user sessions conducted outside business hours, the account accessed most frequently outside business hours, the user with the highest number of authentication failures, and the user with the highest number of unauthorized access attempts.



2. **Log360 UEBA integration:** Log360 UEBA segregates resource and user audit trails from PAM360 and establishes user behavior patterns based on the time at which activities occur and their frequency. Using score-based risk assessment, Log360 UEBA identifies activities that deviate from established behavior patterns as

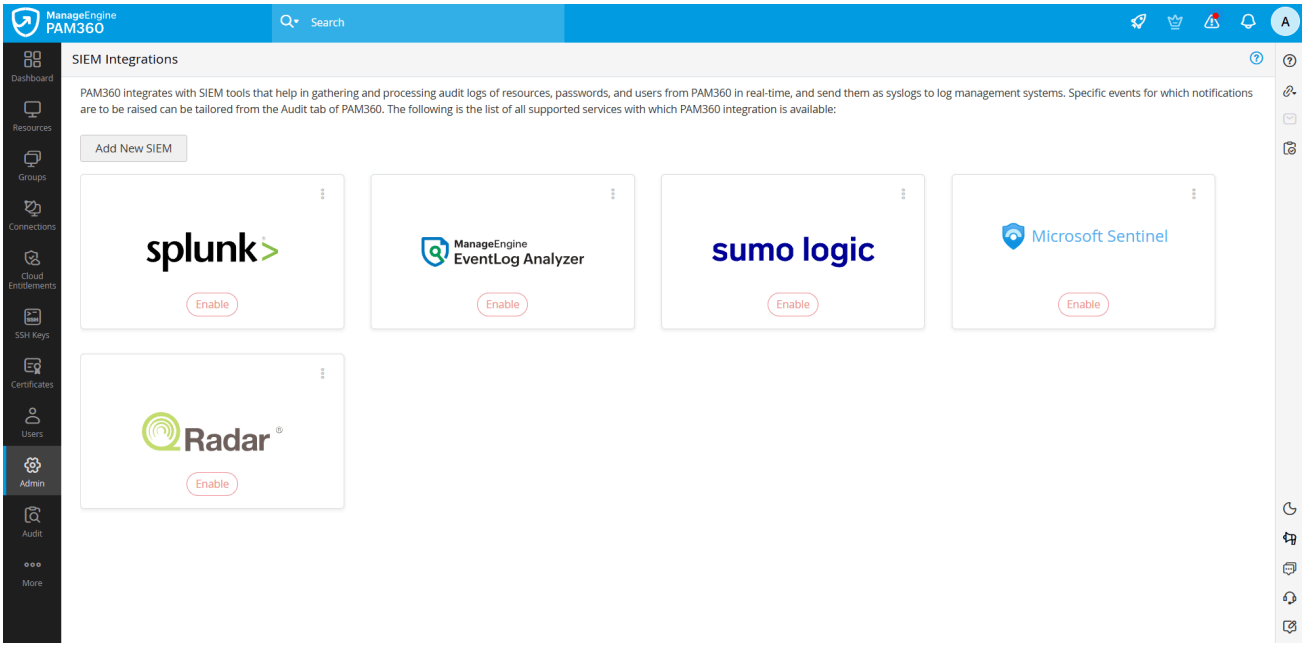
anomalies. Anomaly reports can be visualized using bar graphs and pie charts, scheduled for generation, and exported in CSV, PDF, XLS, and HTML formats.

15.2 Vulnerability Scanners

ManageEngine PAM360 integrates with Rapid7 InsightVM, a vulnerability management solution that scans endpoints across the network and identifies systems that may pose security risks. We recommend leveraging this integration to securely manage and centrally control the privileged credentials required to perform vulnerability scans. Through the PAM360–InsightVM integration, you can securely store and manage required credentials in PAM360 and provide InsightVM access to them directly from the PAM360 interface, reducing the need to expose or manually distribute privileged credentials.

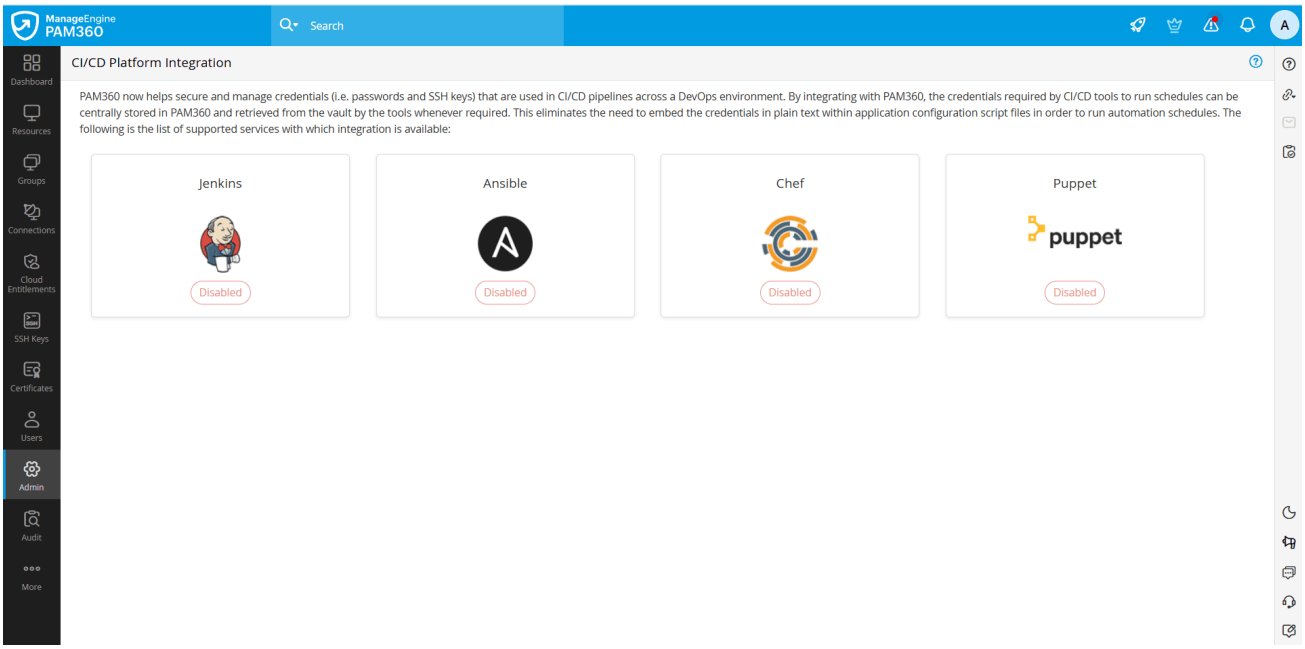
15.3 Integration with SIEM Tools

Integrate PAM360 with SIEM and external log management systems to collect and process audit information about resources, passwords, users, and scheduled tasks in real time. PAM360 supports integrations with SIEM tools such as Splunk, ManageEngine EventLog Analyzer, Sumo Logic, and other syslog collectors. Use these integrations to gain deeper visibility into privileged access activities and correlate them with broader network activity from a centralized security monitoring platform.



15.4 Plugins for CI/CD Platforms

CI/CD pipelines often require privileged passwords, API keys, and access tokens to communicate with systems and services. Often, these credentials are stored in plain text within scripts or pipeline configurations. Storing privileged credentials in plain text can lead to critical security issues. To mitigate such risks, PAM360 seamlessly integrates with CI/CD plugins such as Jenkins, Ansible, Chef, and Puppet, which helps eliminate embedded credentials in the DevOps pipeline. Integrate PAM360 with the CI/CD platforms to securely retrieve required credentials from the PAM360 vault when the tasks are executed. This approach eliminates embedded credentials from DevOps workflows while ensuring that the required credentials remain centrally managed and protected.



15.5 Robotic Process Automation (RPA)

PAM360 integrates with Robotic Process Automation (RPA) tools to automate routine password-related tasks and securely provide privileged credentials to automated workflows when required. This reduces manual intervention and eliminates the need for administrators to retrieve and handle passwords during recurring operational activities.

- **Automation Anywhere:** Integrate PAM360 with Automation Anywhere to securely retrieve passwords from the PAM360 vault using the resource and account details specified in the automation workflow. The retrieved passwords can be used by other automation tools to perform tasks that require privileged access. For example, in an automated remote login workflow, Automation Anywhere can retrieve the required password securely from PAM360 and use it to authenticate to the target device, eliminating the need for administrators to retrieve or handle the credential manually.
- **Cortex XSOAR:** Integrate PAM360 with Cortex XSOAR by Palo Alto Networks to incorporate privileged credential operations into automated security workflows. Cortex XSOAR supports standardized responses through case management, automation, real-time collaboration, and threat intelligence management. This integration is useful for automating credential-related operations as part of security

workflows and reducing manual intervention across the incident life cycle.

15.6 Integration with ADSSP

Integrate PAM360 with ManageEngine ADSelfService Plus (ADSSP) to automatically synchronize the password of the Active Directory account configured in ADSSP. ADSSP uses an Active Directory account with the required privileges to perform operations such as password resets and account unlocks on behalf of domain users. Whenever the password of this Active Directory account is reset in PAM360, the updated password is automatically synchronized with ADSSP. This eliminates the need to manually update the configured password after every password change, prevents authentication failures caused by outdated credentials, and ensures uninterrupted self-service password management operations.

15.7 Integration with AI Platforms

PAM360 offers AI-driven capabilities that help administrators quickly analyze key activity patterns and identify potential risks associated with privileged access. Integrate PAM360 with the supported AI platforms to generate intelligent insights that reduce manual effort and support informed decision-making. Enable AI-powered capabilities based on your requirements, and review the data shared with the configured AI platform before enabling features such as session summaries, which may include system events, user inputs, outputs, keystrokes, and other user activity. Treat AI-generated summaries and policy recommendations as decision-support inputs and validate them before taking access or privilege-related actions. Explore this **link** for more information about the required roles and permissions, supported capabilities, and the integration steps.

16. High Availability and Disaster Recovery

Continuous access to privileged resources is essential for maintaining business continuity and minimizing operational disruptions. Since PAM360 acts as the centralized repository for privileged credentials and access management, server failures, infrastructure outages, or database issues can directly impact administrative operations across the organization. Implementing an appropriate High Availability (HA) and Disaster Recovery (DR) strategy helps organizations minimize downtime, maintain access to privileged resources during failures, and recover critical data in the event of unforeseen incidents.

PAM360 provides multiple High Availability models for both PostgreSQL and Microsoft SQL Server deployments, along with built-in database backup capabilities for Disaster Recovery. Organizations should evaluate their infrastructure, scale, backend database, and business continuity requirements to implement the most appropriate high availability and disaster recovery strategy. Explore this link for the detailed information about the available high availability models in PAM360.

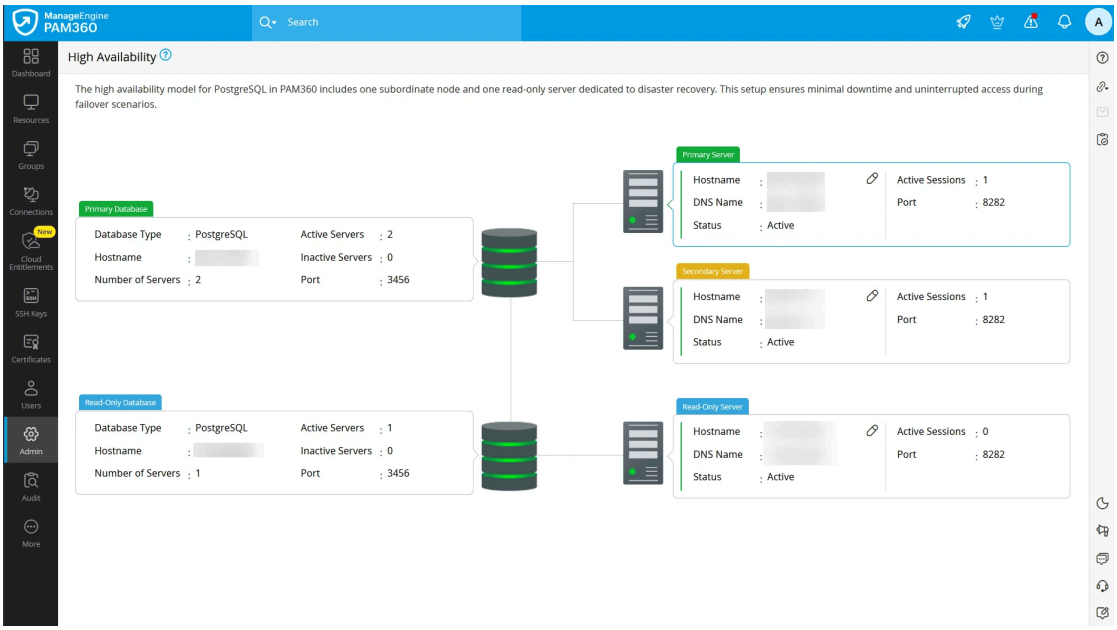
16.1 Configure an Appropriate High Availability Model

PAM360 provides multiple High Availability (HA) models to address different organizational requirements, deployment architectures, and backend databases. Select the model that best aligns with your organization's infrastructure, scalability, and business continuity requirements.

1. **Failover Service Model:** Available for MS SQL deployments, this model uses redundant PAM360 server instances connected to a common MS SQL cluster. During a primary server failure, operations are automatically transferred to the standby server with minimal downtime.
2. **Read-Only Server Model:** Available for PostgreSQL deployments, this model uses one or more read-only servers that continuously synchronize with the primary server using PostgreSQL streaming replication. During planned maintenance or primary server failures, a read-only server can be promoted to the primary server. Multiple

read-only servers can be deployed across different locations.

3. **Application Scaling Model:** Distributes application workloads across one main node and multiple sub-nodes connected to a common database cluster, improving scalability, performance, and availability for large deployments.
4. **Secondary Server Architecture Model:** Provides redundancy by deploying a secondary PAM360 server alongside the primary server. The implementation differs based on the configured backend database:
    - **PostgreSQL** - Primary and secondary servers share a common PostgreSQL database, with an optional Read-Only server maintaining a real-time replica. The recommended deployment comprises a Primary Server, Secondary Server, and Read-Only Server.



    - **Microsoft SQL -** Primary and secondary servers maintain separate database instances synchronized through SQL Server replication. During failover, the secondary server provides read/write access (except password resets) until the primary server is restored.

Select the High Availability model that best aligns with your organization's size, infrastructure, configured backend database, and business continuity requirements. To maximize resilience, deploy secondary or read-only servers across separate network

segments wherever possible. For geographically distributed organizations, deploy the primary server at the headquarters and the secondary or read-only server at another office to minimize the impact of localized infrastructure failures.

After configuring High Availability, continuously monitor the health of the primary, secondary, and read-only servers and their associated databases. PAM360's built-in High Availability monitoring capabilities provide configurable notifications and display the status of the servers, PostgreSQL replication, and associated databases, enabling administrators to detect availability issues, database failures, and replication problems before they affect privileged access operations.

To configure and monitor High Availability, navigate to **Admin >> Business Continuity**.

16.2 Configure Database Backup for Disaster Recovery

The data stored in the PAM360 database is critical to the organization's privileged access infrastructure. To minimize the risk of data loss due to hardware failures, software issues, or other unforeseen events, implement an appropriate disaster recovery strategy.
PAM360 supports both live database backups and scheduled automated backups. Select the backup method that best aligns with your organization's recovery objectives and operational requirements. Store backup files in a secure remote location separate from the PAM360 server to ensure they remain available during disaster recovery operations.

17. Periodic Maintenance

Regular maintenance is essential to keep the PAM360 deployment secure, stable, and fully supported. Keeping the product and its associated components up to date, planning maintenance activities appropriately, and staying informed about security advisories help ensure optimal performance while minimizing operational disruptions. Follow these maintenance best practices:

- **Keep PAM360 updated** - Regularly review and apply the latest PAM360 upgrade packs to benefit from new features, security enhancements, bug fixes, and updates to bundled components such as Apache Tomcat, PostgreSQL, and the Java Runtime Environment (JRE).
- **Plan maintenance activities appropriately** - Schedule upgrades during planned maintenance windows, preferably outside business hours, since applying upgrade packs requires temporarily stopping the PAM360 service. If High Availability is configured, review and follow any required post-upgrade High Availability reconfiguration. When maintenance is performed during business hours, notify users in advance using the message board.
- **Keep client applications updated** - Encourage users to periodically update PAM360 mobile applications, browser extensions, and other client applications to maintain compatibility with the PAM360 server and benefit from the latest security enhancements and bug fixes.
- **Review security advisories** - Monitor the security advisories sent to the registered email address and promptly implement the recommended remediation measures whenever security vulnerabilities are disclosed.
- **Validate server migrations before decommissioning the existing installation** - When moving PAM360 to another server, verify that the new installation is fully operational before removing the existing deployment. Retaining the original installation until the migration is validated provides a reliable fallback in the event of migration failures, data corruption, or other unforeseen issues.

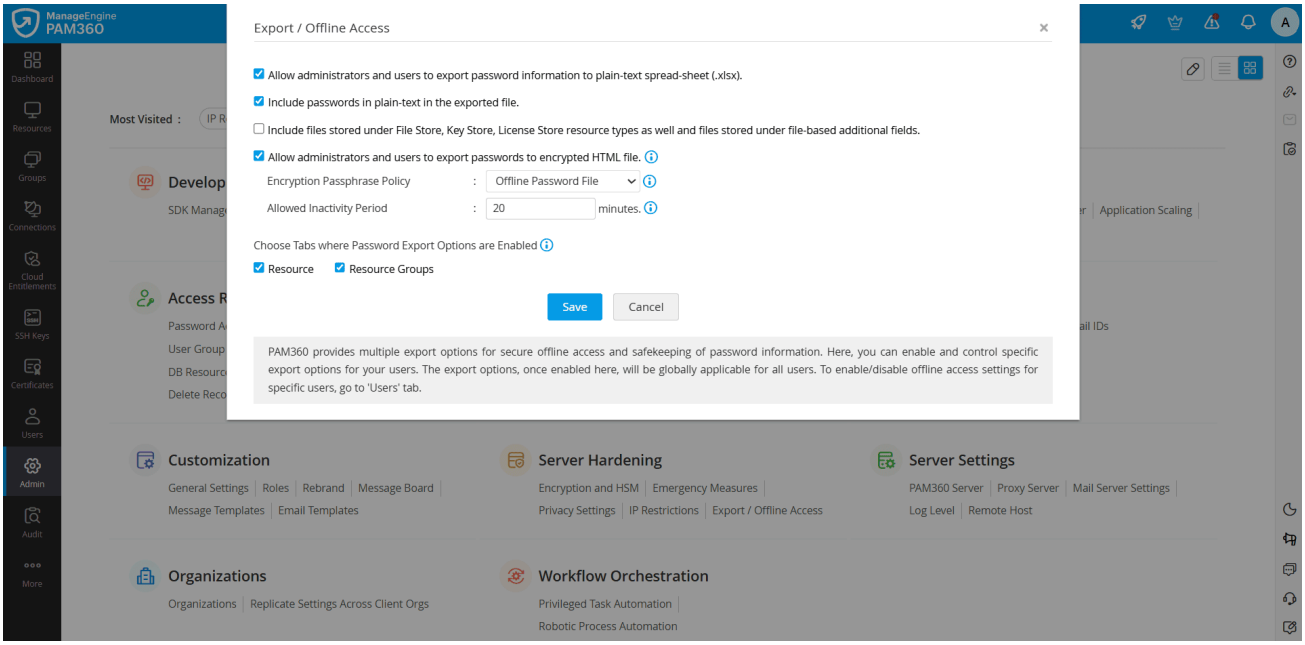
To send a message to all users via the message board, navigate to **Admin >> Customization >> Message Board.**

18. Emergency and Offline Access

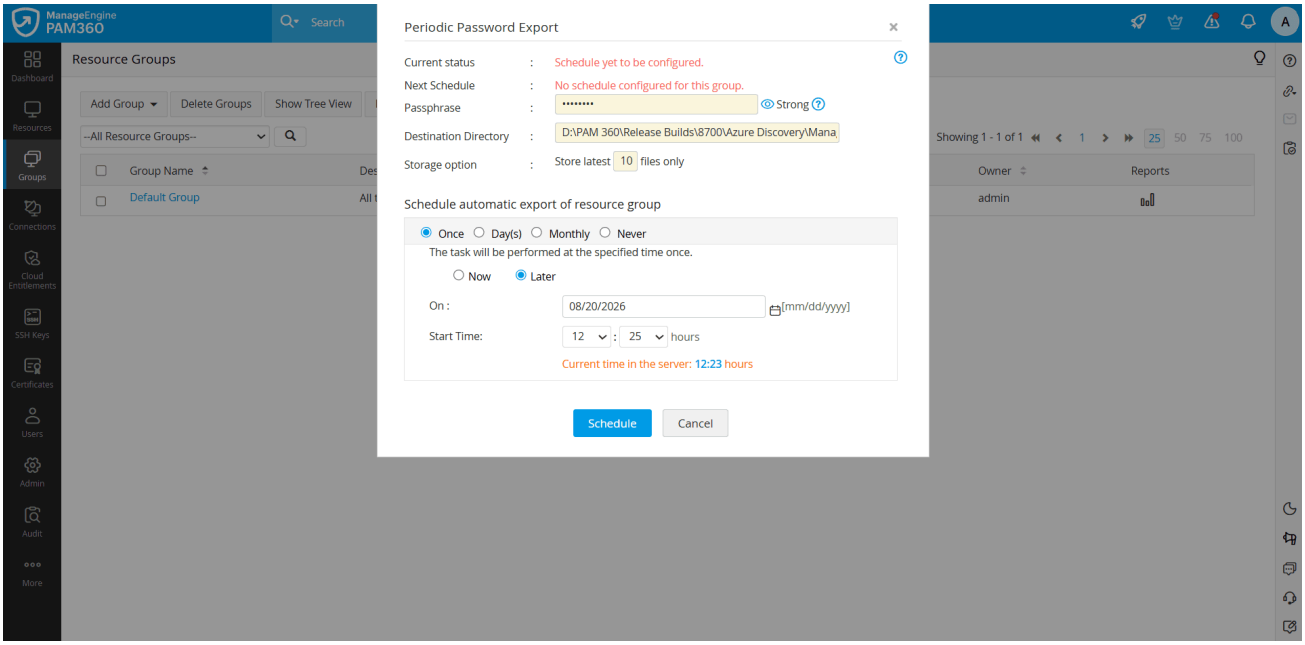
Ensure that authorized administrators can access PAM360 and retrieve critical credentials even when normal authentication or network connectivity is unavailable. Maintain a controlled emergency account for directory service outages and use secure offline password exports when PAM360 cannot be accessed from restricted environments.

- **Maintain a local emergency account:** Retain a local PAM360 account for emergency or break-glass access if Active Directory becomes unavailable and directory-authenticated users cannot log in. Keep this account tightly controlled and use it only when required.
- **Use encrypted offline password exports:** For controlled environments such as data centers where internet connectivity is unavailable, periodically export required passwords as encrypted HTML files and store them in a secure location. Protect the files with a 16-digit passphrase and configure automatic logout for the offline file to limit exposure. Offline exports can be generated on demand or scheduled for resource groups on a daily, weekly, or monthly basis.

To update the offline access settings navigate to **Admin >> Server Hardening >> Export / Offline Access**.



To configure periodic password exports, navigate to the **Groups** tab, click the Actions button next to the desired resource group, and select **Periodic Password Export** from the displayed options.



19. Administrator Offboarding

When an administrator leaves the organization, their privileged access and responsibilities should be promptly reviewed and transferred to prevent unauthorized access and ensure that critical PAM360 operations continue without disruption.

- **Prepare an Exit Report** - Review the departing administrator's privilege level and generate a user-specific report listing the passwords they could access. Use this report to identify resources that require ownership transfer and password rotation.
- **Transfer Resource Ownership:** Transfer ownership of all resources created or owned by the departing administrator to another authorized administrator before removing their PAM360 account.
- **Transfer Approver Privileges:** If the administrator is an approver for access control requests, transfer their approver privileges to another authorized administrator.
- **Reset Associated Passwords:** Immediately reset the passwords of resources owned by the departing administrator after transferring ownership to another administrator. This helps prevent continued access using credentials that may have been known to the departing administrator.

To transfer the user's entire accountabilities, including resource ownership and approver privileges, navigate to the **Users** tab and click the **User Actions** icon beside the respective user whose resources and responsibilities need to be transferred, and click **Transfer User Accountabilities** from the displayed options.

20. Security Best Practices

Protect PAM360 communications, user sessions, exported credentials, and application interfaces by enforcing secure communication, limiting session exposure, preventing malicious input, and restricting access to trusted systems.

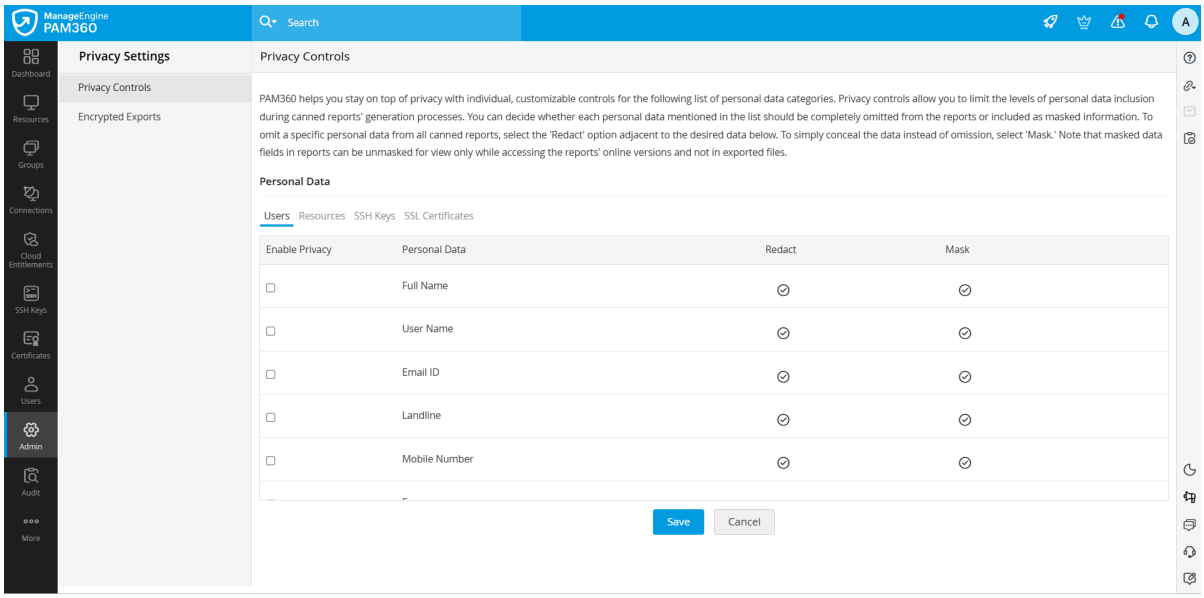
- **Use SSL Communications:** Always use SSL-secured communication for sensitive operations, including password resets and resource addition or import.
- **Prevent Malicious Script Execution:** Keep PAM360's protection against harmful scripts and HTML-based inputs enabled. By default, PAM360 identifies and blocks harmful scripts. Scripts that contain harmful HTML tags will also be blocked from execution. If a legitimate script requires this protection to be temporarily disabled, re-enable it immediately after completing the task.
- **Configure Inactivity Timeout:** Reduce the risk of unattended web sessions by configuring the inactivity timeout to 15 minutes or less, rather than relying on the default 30-minute timeout. Configure this under **Admin >> Customization >> General Settings >> User Management**.
- **Configure Browser Extension Auto-Logout:** Configure browser extension sessions to automatically log out after 15–30 minutes of inactivity. Logout periods can be configured under **Settings** in the browser extension.
- **Restrict Password Exports:** Allow users to export passwords only as encrypted HTML files wherever possible. If CSV exports are permitted, disable the option to export passwords in plain text under **Admin >> Server Hardening >> Export / Offline Access**.
- **Restrict Access by IP Address:** Use IP-based restrictions to limit access to PAM360 from authorized systems and networks. Restrictions can be applied to web access, API calls, mobile applications, browser extensions, and agent communication, using individual IP addresses or defined IP ranges.

To configure IP-based restrictions, navigate to **Admin >> Server Hardening >> IP Restrictions**, and select **Web Access**, **API Access**, or **Agent Access** as required.

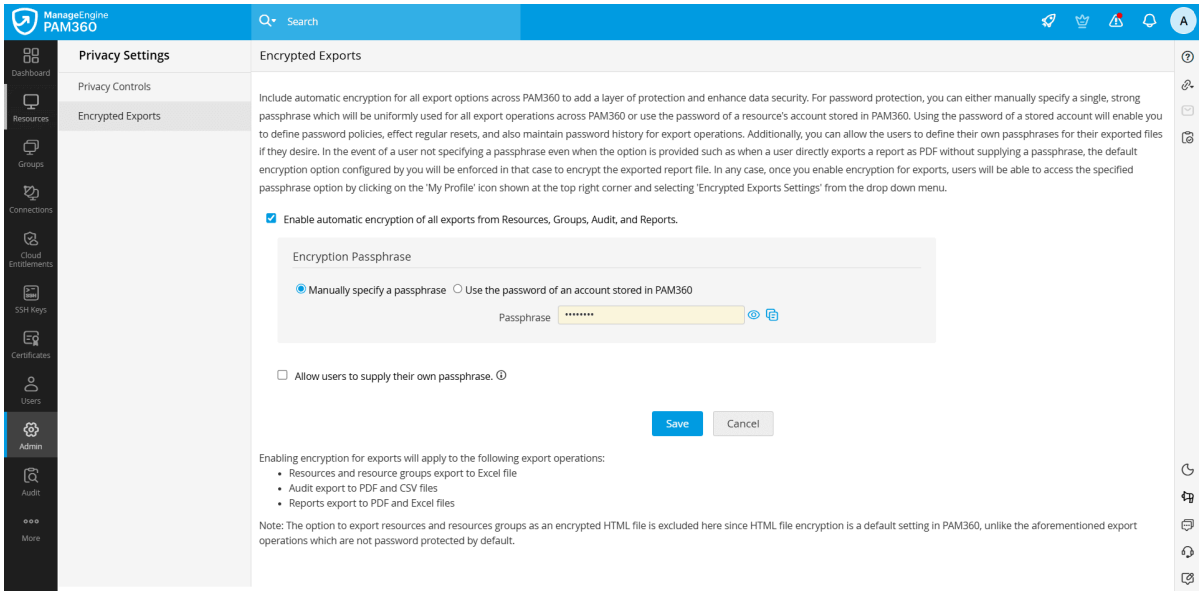
21. Privacy Settings

Protect personal and sensitive information contained in PAM360 reports and exported files by applying appropriate privacy and encryption controls.

- **Apply Privacy Controls to Reports:** Configure PAM360 to mask or remove personal data from canned reports based on your organization's privacy requirements. Highly confidential information should be masked or excluded wherever it is not required in the report. Configure these settings under **Admin >> Server Hardening >> Privacy Settings >> Privacy Controls**.



- **Encrypt Exported Files:** Enable encryption for PAM360 exports to provide an additional layer of protection for exported data. You can configure a global passphrase for all exports or allow users to define individual passphrases. The configured passphrase is required to access the exported file. Configure this under **Admin >> Server Hardening >> Privacy Settings >> Encrypted Exports**.


ManageEngine
PAM360
Search
A
Dashboard
Resources
Groups
Connections
Cloud Entitlements
SSH Keys
Certificates
Users
Admin
Audit
More
Privacy Settings
Privacy Controls
Encrypted Exports
Encrypted Exports
Include automatic encryption for all export options across PAM360 to add a layer of protection and enhance data security. For password protection, you can either manually specify a single, strong passphrase which will be uniformly used for all export operations across PAM360 or use the password of a resource's account stored in PAM360. 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. Additionally, you can allow the users to define their own passphrases for their exported files if they desire. In the event of a user not specifying a passphrase even when the option is provided such as when a user directly exports a report as PDF without supplying a passphrase, the default encryption option configured by you will be enforced in that case to encrypt the exported report file. In any case, once you enable encryption for exports, users will be able to access the specified passphrase option by clicking on the 'My Profile' icon shown at the top right corner and selecting 'Encrypted Exports Settings' from the drop down menu.
Enable automatic encryption of all exports from Resources, Groups, Audit, and Reports.
Encryption Passphrase
Manually specify a passphrase
Use the password of an account stored in PAM360
Passphrase
Allow users to supply their own passphrase.
Save
Cancel
Enabling encryption for exports will apply to the following export operations:
Resources and resource groups export to Excel file
Audit export to PDF and CSV files
Reports export to PDF and Excel files
Note: 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.

Sustaining a Secure and Resilient PAM360 Environment

Implementing these best practices helps organizations establish a secure and resilient PAM360 setup. Review the access control configurations, resource sharing, audit data, business continuity measures, and external integrations regularly to ensure they continue to meet changing security, operational, and compliance requirements. By consistently applying least-privilege access, secure credential management, and continuous monitoring, organizations can strengthen privileged access protection and maximize the security value of their PAM360 deployment.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360