ManageEngine
ADManager Plus

Solution Architecture

www.admanagerplus.com

Table of Contents

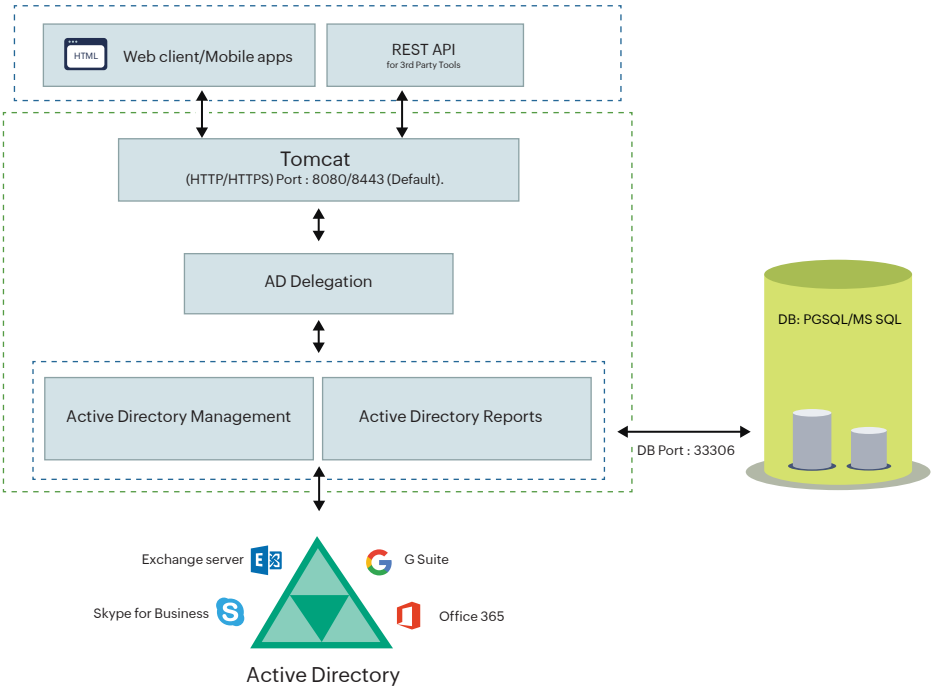
ManageEngine ADManager Plus MSP

ADManager Plus is a unified Windows Active Directory (AD), Microsoft 365, and Exchange management and reporting solution that helps AD administrators and help desk technicians in their day-to-day activities. With ADManager Plus, you can:

- Simplify several routine AD tasks such as user provisioning, cleaning up dormant accounts, managing NTFS permissions, and more.
- Streamline user management across Microsoft 365, Google Workspace and Exchange platforms from a single place.
- Get more than 200 pre-packaged reports, with built-in management actions.
- Create a customizable workflow structure that helps maintain records of tasks and AD data for retrieval at anytime, thus assisting you to meet certain IT compliance requirements.
- Automate routine AD tasks such as user provisioning, de-provisioning, and more.
- Back up AD objects fully and incrementally, and recover them in the blink of an eye.

1. ADManager Plus architecture

ADManager Plus follows the client-server model and comes with a built-in PostgreSQL as its database.



Client

ADManager Plus can be accessed from a web browser by entering the IP address or computer name and port number of the server as the URL.

Eg: admp-client:<portnumber> (or) 193.45.23.4:<portnumber>

It can also be accessed from a mobile device using the ADManager Plus Android or iOS application. You can log in to ADManager Plus MSP using ADManager Plus authentication, domain credentials, single sign-on (SSO), smart card authentication, and more.

Server

You can deploy ADManager Plus in any Windows machine in your domain. Once the product is installed, it automatically discovers the AD domains in your network. You can also manually configure new domains.

Database

By default, ADManager Plus comes bundled with a PostgreSQL database, but can also be migrated to an external MS SQL database. On the first of every month, the database is backed up automatically to avoid data loss due to untoward incidents. All management and reporting actions performed using ADManager Plus is recorded as audit reports and are stored in the product's database. By default, these audit reports are archived and you can customize the storage location and retention period for these audit reports.

ADManager Plus' technology stack:

- Client-side of the application is developed using HTML, CSS, JavaScript, jQuery plugin, Ember framework, and Jakarta Server Pages (JSP, formerly JavaServer Pages).
- Server-side framework is developed using Java, Native C, and C#.
- ADManager Plus uses Java Database Connectivity (JDBC) to connect to databases.
- ADManager Plus allows web browsers and servers to communicate using the HTTP/HTTPS and LDAP protocol.

Product ports

Port Number	Protocol	Purpose
8080/8443 (8080 is the default port and can be changed to HTTPS in the Admin tab)	HTTP/HTTPS	Necessary to connect to Apache Tomcat web server
33306	TCP	To connect to the bundled database

System Ports

Allow outbound connections to ports on the source server (ADManager Plus Server) and inbound connections to ports on the target servers (DCs, etc.).

Port Number	Protocol	Source	Destination	Port Type	Service	Purpose
389/639	TCP and UDP	ADManager Plus Server	Domain Controllers	Static	LDAP	Used to connect to AD
135	TCP	ADManager Plus Server	Domain Controllers	Static	RPC	Used to establish data exchange
445	TCP and UDP	ADManager Plus Server	Domain Controllers	Static	SMB	Used to get access to shared file systems
88	TCP	ADManager Plus Server	Domain Controllers	Static	Kerberos	Used to authenticate domain access requests
139	TCP	ADManager Plus Server	Domain Controllers	Static	NetBIOS session	Used in network communication
3268/ 3269	TCP	ADManager Plus Server	Domain Controllers	Static	Global Catalog	Used to perform search operations in the Global Catalog
25	SMTP	ADManager Plus Server	SMTP Server	Static	SMTP	Used to send emails
80	HTTP	ADManager Plus Server	SMTP Server	Static	Exchange	Used to connect to Exchange Servers
80, 443	HTTP/ HTTPS	ADManager Plus Server	Microsoft 365/ Google Workspace server	Static	Microsoft 365 and Google Workspace	Used to communicate with Microsoft 365 and Google Workspace platforms
49152 65535	TCP	ADManager Plus Server	RPC randomly allocated high TCP ports	Dynamic	RPC	Used to establish data exchange

2. ADManager Plus login process

The technician or administrator must log in to the application to perform management actions, generate reports, and delegate tasks.

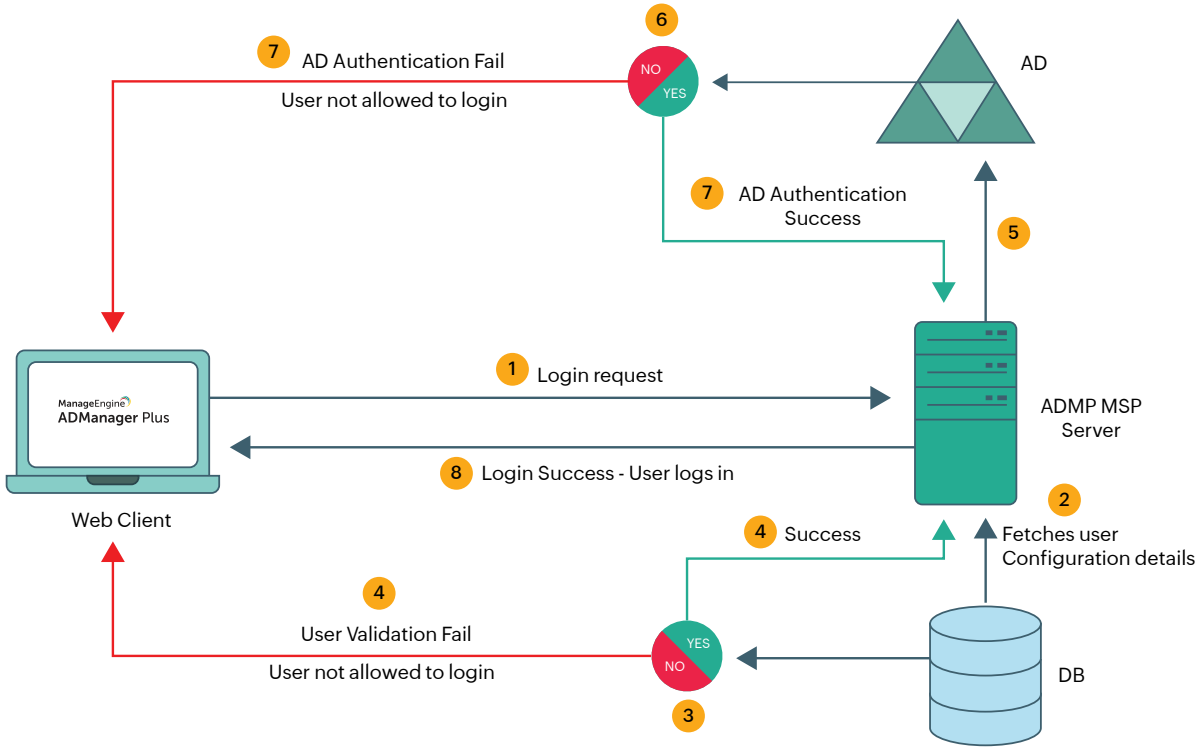
ADManager Plus comes with three built-in technician accounts:

- Admin
- Help desk
- HR Associate

Apart from these, you can configure any number of AD user accounts as technicians. Except the default admin role, the other roles can be modified or removed. Using ADManager Plus, you can delegate the help desk roles to users and groups. Delegating a role to a group would result in all the group members having permission to perform the tasks defined in that role. Technicians can be delegated roles in the tool without elevating their rights in the AD.

When technicians enter their username and password, the tool:

1. Performs AD authentication for the help desk technicians configured in the product and database authentication for the built-in technicians.
2. Validates account details with respect to ADManager Plus configuration for technicians.
3. Performs authorization.



2.1 Authentication

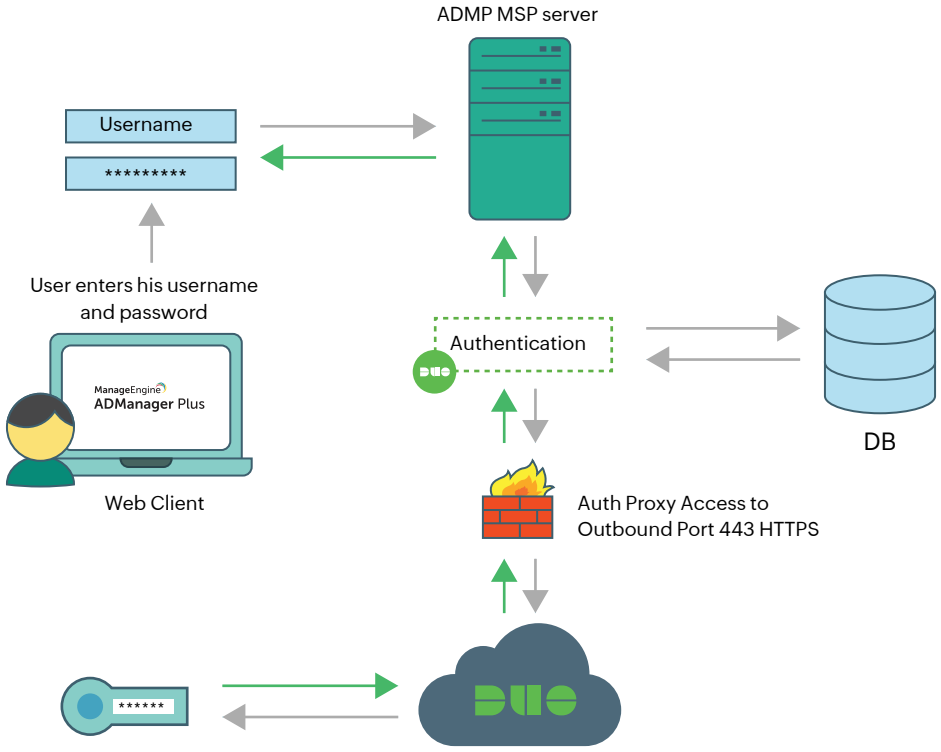
Users can log in to ADManager Plus using domain authentication, Two-Factor Authentication (2FA), and SSO authentication services.

During domain authentication, ADManager Plus will perform LDAP* binding with the configured DC using ADsOpenObject API. It will then validate the password with the domain controller and check if the given account is expired, locked-out, or disabled in AD, or if its password has expired. If any of the above cases are true, the binding will fail and the tool will not allow the user to log in.

2FA

ADManager Plus offers 2FA through authentication services such as Duo Security, Google Authenticator, SMS verification, Microsoft Authenticator, RSA SecurID, and One Time Password (OTP) via email. When a user tries to log in to ADManager Plus, they are first authenticated using their username and password. If it is successful, they are directed to the configured authentication service (Duo, Microsoft Authenticator, SecurID, or RSA) or asked to enter an additional piece of authentication information such as OTP. If the second step is also successful, the user is allowed to log in to ADManager Plus MSP

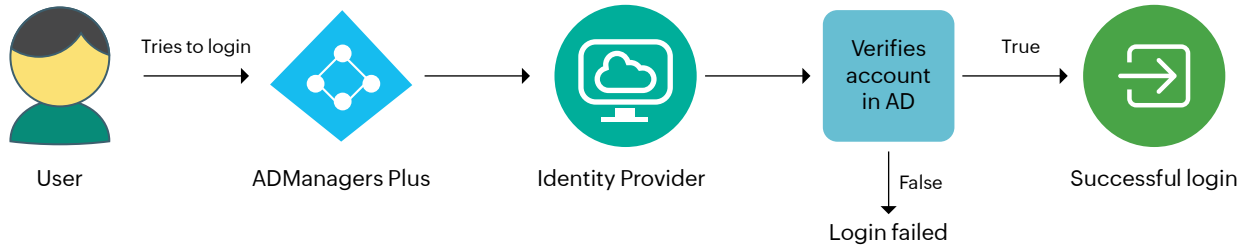
Duo Security: Once the user enters the credentials, the tool authenticates it with AD. On successful authentication, username and application key will be sent to Duo Security for verification. Upon successful verification, the user will be logged into to ADManager Plus. The Duo Security secret key is stored in the database using AES-CBC encryption with PKCS5 padding.



RSA SecurID: For RSA authentication, ADManager Plus does not store any key information, as the configuration file (sdconf.rec within AMConfig.zip) received from RSA server stores the configuration details. Users can use the security codes generated by the RSA SecurID mobile app, hardware tokens, or tokens received in their mail or mobile to log in to ADManager Plus.

SSO

You can set up SSO to access ADManager Plus through NTLM or SAML authentication.



2.2 ADManager Plus technician validation

When a user account is configured as a technician, information such as technician name, AD account status, roles, licenses, and privileges is stored in the product database. Once AD authentication succeeds, the user account information will be validated with this configuration. If there is no configuration** available, users will not be allowed to log in.

2.3. Authorization

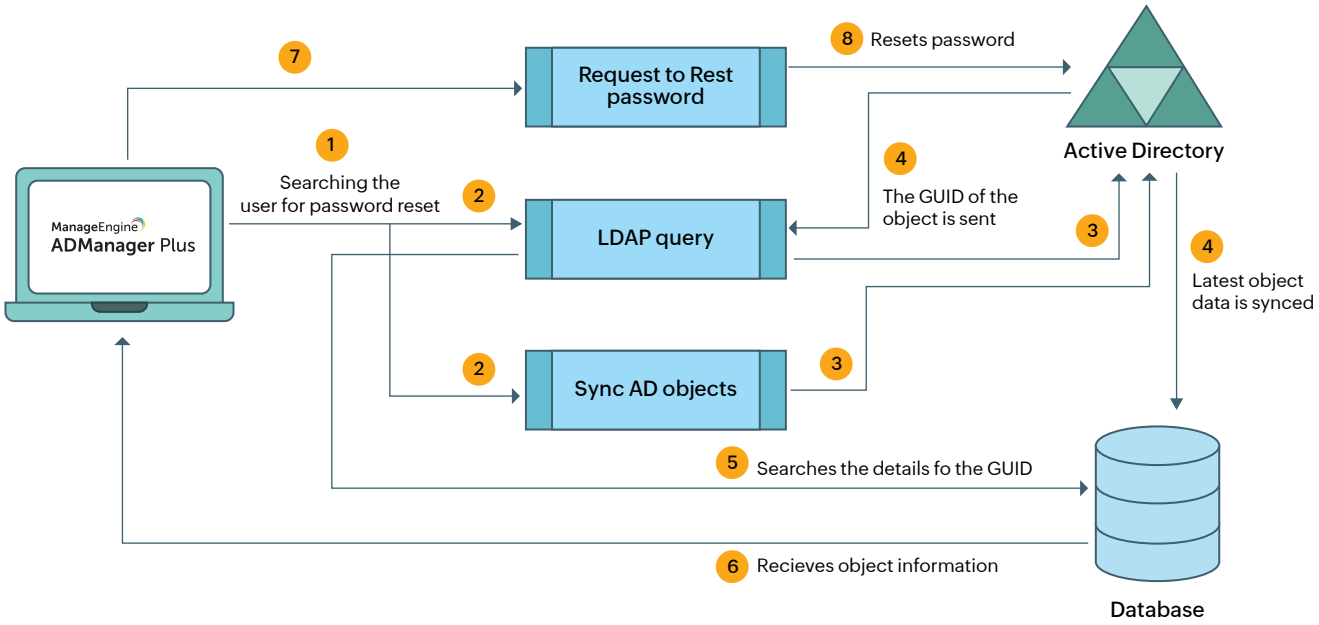
In this step, the tool will fetch the delegated roles and domains from configuration details stored in the database and assign them to the technician, and a session will be created for the technician in the browser.

*Only for AD users. The built-in technicians will be authenticated using the database. LDAPS can be configured in connection settings of ADManager Plus.
**For group-based delegation, user configuration happens during the login process.

3. ADManager Plus modules

3.1 AD management

When an AD management action is initiated, ADManager Plus MSP will use an LDAP query to identify the desired AD objects, perform the necessary action in AD using Windows APIs, and store the resulting data in the database. It will then retrieve the data from the database and display it on the console.



APIs used:

ADsOpenObject

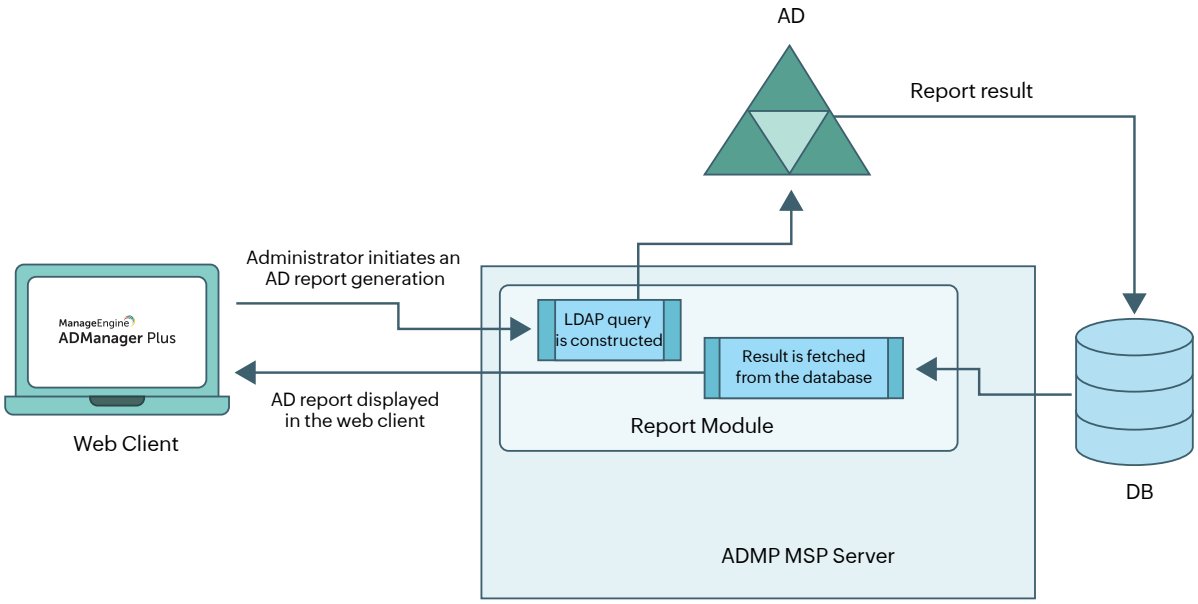
SetObjectAttributes

SetPassword

CreateDSObject

3.2 AD reporting

ADManager Plus report library contains more than 200 out-of-the-box reports that provide information on users' real last logon times, inactive AD users, group members (including nested group members), NTFS permissions, and more. These reports can be exported in PDF, Excel (XLSX), CSV, CSVDE and HTML formats.



When a user initiates a report generation action, the web client will send the input to the server via HTTP/HTTPS. Based on this input, the server will construct an LDAP query. The LDAP query is executed in AD, and the results will be stored in database and displayed on the ADManager Plus MSP console. The tool uses IDirectorySearch (API) for retrieving reports.

APIs used:

IDirectorySearch::ExecuteSearch

IDirectorySearch::GetColumn

3.3 ADManager Plus delegation

Roles in ADManager Plus:

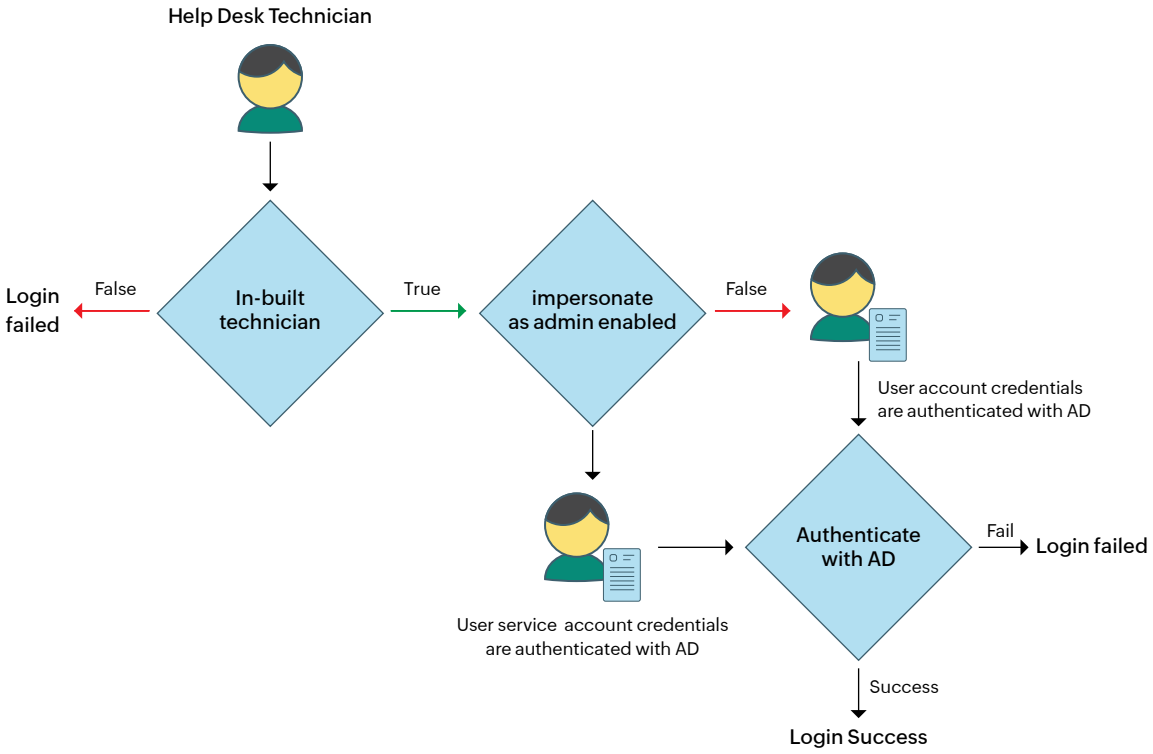
ADManager Plus offers predefined help desk roles that can be assigned to help desk technicians. These roles can be deleted or modified based on your needs. However, the Super Admin role, which contains all the privileges, cannot be deleted or modified. You can also create customized roles and assign them to the desired users to empower them to perform AD tasks within the specified administrative boundaries. Every time a role is created, the tool creates a Role ID and every management or reporting action that is defined in the role is assigned an ActionID. The Role IDs and ActionIDs are stored in the product's back end database. Every role that has been created, modified, or deleted is recorded and can be viewed in the Admin Audit Report.

Delegation to help desk technicians:

ADManager Plus empowers help desk technicians to perform tedious and routine AD tasks that don't require the dependency of administrators, thereby reducing their workload. You can create a single technician or multiple technicians in one go. Each technician has a unique login ID, to which the delegated domain will be mapped. Every technician should be configured to at least one role. Besides delegating AD management and reporting, you can also delegate Microsoft 365 and Google Workspace management and reporting tasks.

Service account:

Upon logging in to ADManager Plus, you can add AD domains in the Domain Settings section. You can either use an account that belongs to the Domain Admins group (recommended) or a service account that has been assigned all the sufficient privileges required by ADManager Plus. The credential you provide while configuring the AD domain in the Domain Settings section is stored in the database.



Impersonate as admin:

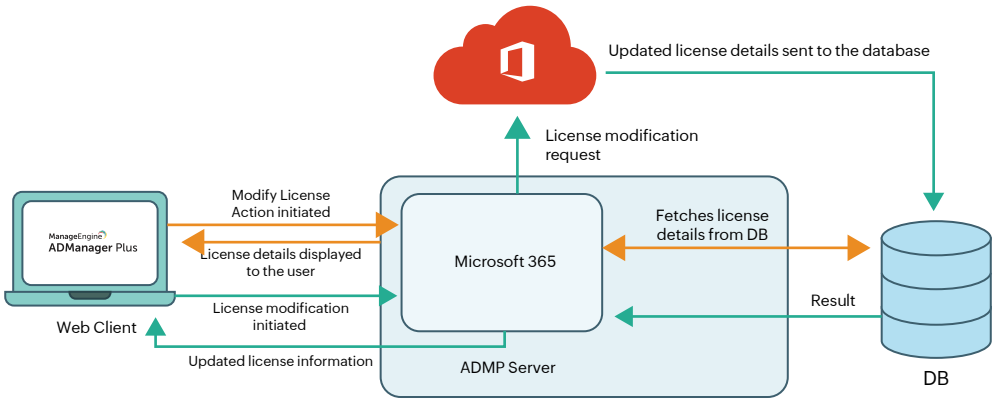
When a technician does not have the necessary permissions in AD to carry out the delegated tasks, the option Impersonate as Admin can be enabled. When enabled, the technician will be able to perform the delegated tasks with the privileges of the user account that has been configured in the Domain Settings or with the user account that has been configured to run ADManager Plus. The actions performed by technicians using this option would be logged in the DC as if it was performed by the user account specified in Domain Settings. However, a complete audit trail of the actions done by any user account using ADManager Plus can be obtained from the Admin Audit report.

Authorization:

ADManager Plus verifies authorization for the actions, domains, OUs, groups and file servers delegated to the technician before sending data to domain controllers. The tool displays only the authorized actions while carrying out management tasks based on the roles assigned to the technician.

3.4 Microsoft 365 management and reporting

ADManager Plus requires MS Online or Azure AD PowerShell, along with a stable internet connection for managing Microsoft 365 accounts.



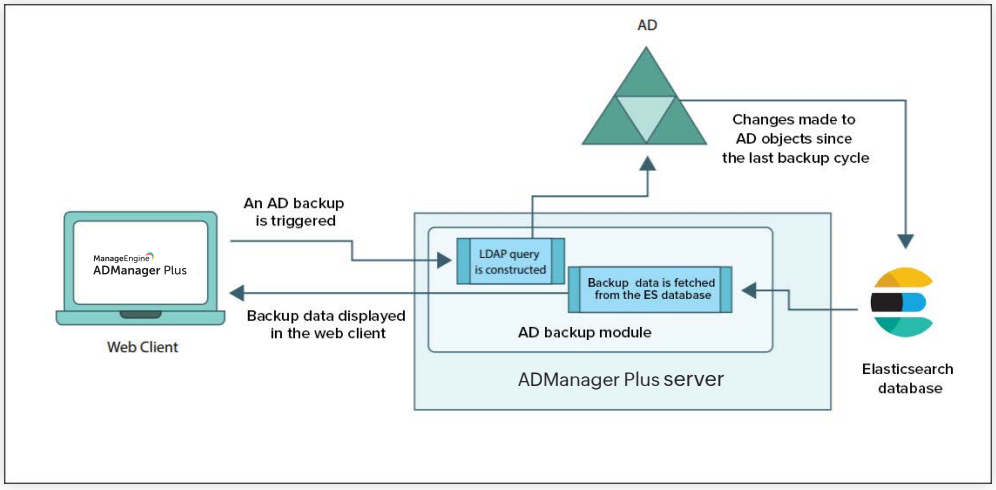
For instance, if the administrator chooses to remove a license assigned to a specific Microsoft 365 user using ADManager Plus, the tool will retrieve the account and license information from the product database and call the configured REST API or construct a suitable PowerShell script. Once the script is executed, the corresponding Microsoft 365 license will be removed for that user and the updated license information of the user will be stored in the database and displayed on the console.

3.5 Backup and recovery

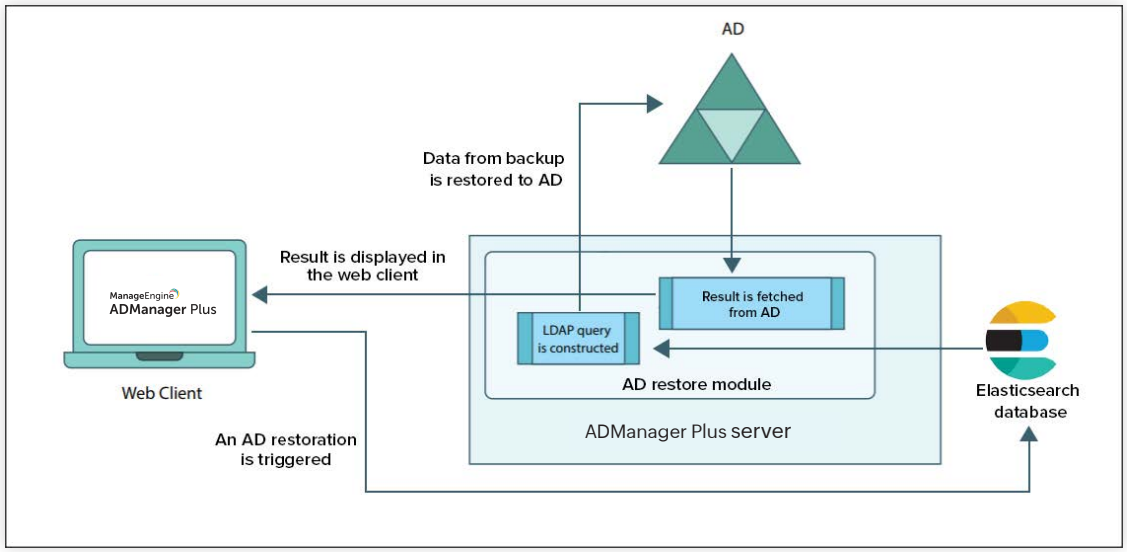
3.5.1 AD backup and recovery

ADManager Plus allows you to backup and recover deleted AD objects.

AD backup: With the AD backup feature in ADManager Plus, you can take full backups or incremental backups and save up space and time. Upon initiating an AD backup in ADManager Plus, an LDAP query will be constructed. The LDAP query is executed in AD, and all the changes made to AD objects since the last backup cycle are identified. These values are then stored in the Elasticsearch database. The tool will then display the list of all backed up objects.

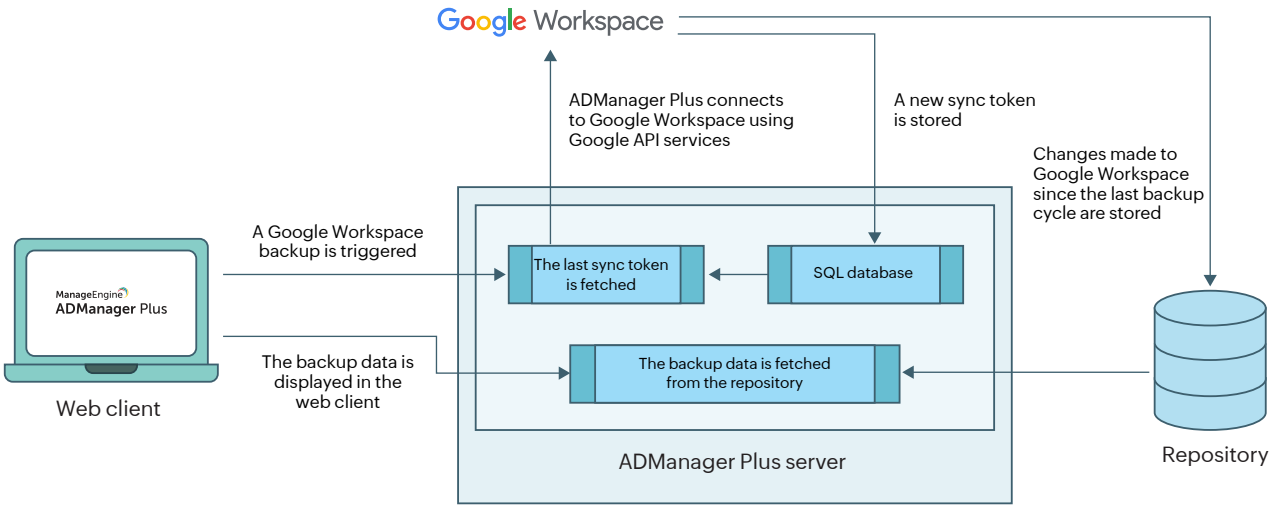


AD Recovery: When any recovery action is triggered by the administrator, an LDAP query is generated and the ADManager Plus server fetches the data to be restored from the Elasticsearch database. This value is then restored to AD, and the result is displayed in the GUI.

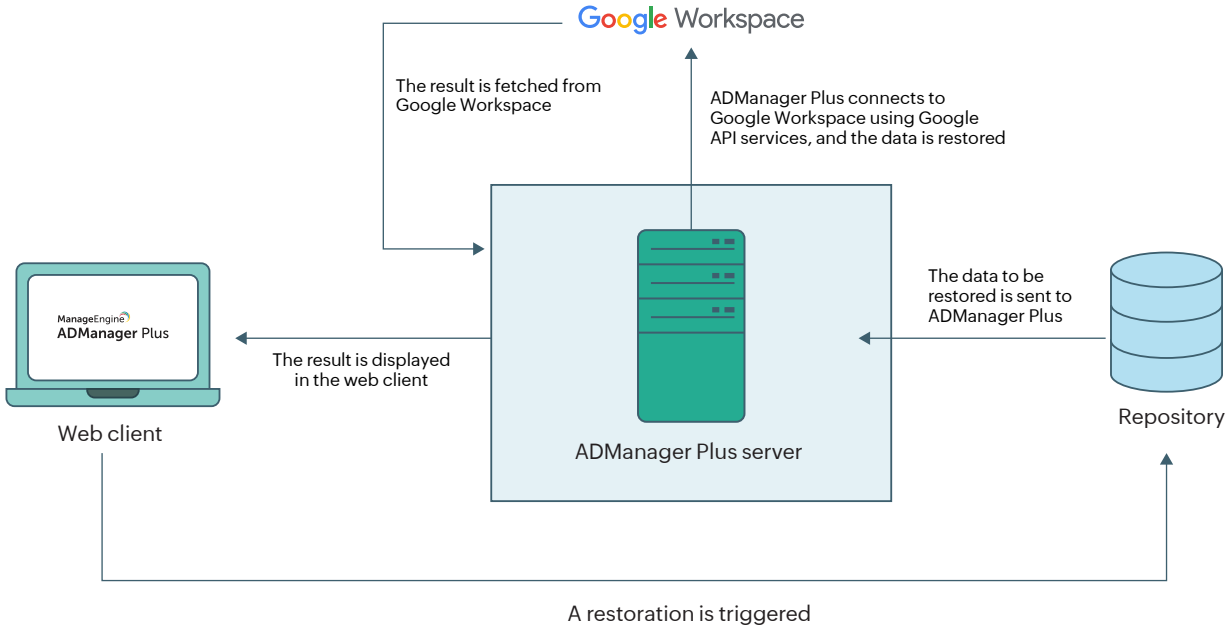


3.5.2 Google Workspace backup and recovery

Google Workspace backup: When a backup is initiated for Google Workspace, the web client sends the request to ADManager Plus' server via HTTPS, which is handled by Google API services. ADManager Plus fetches the sync token from the previous backup to identify the data modified since the last backup cycle. All changes made are backed up and stored in the backup repository. A new sync token is generated and stored in the SQL database to be used for the next backup cycle. The backup stored in the repository is fetched and displayed in the web client.



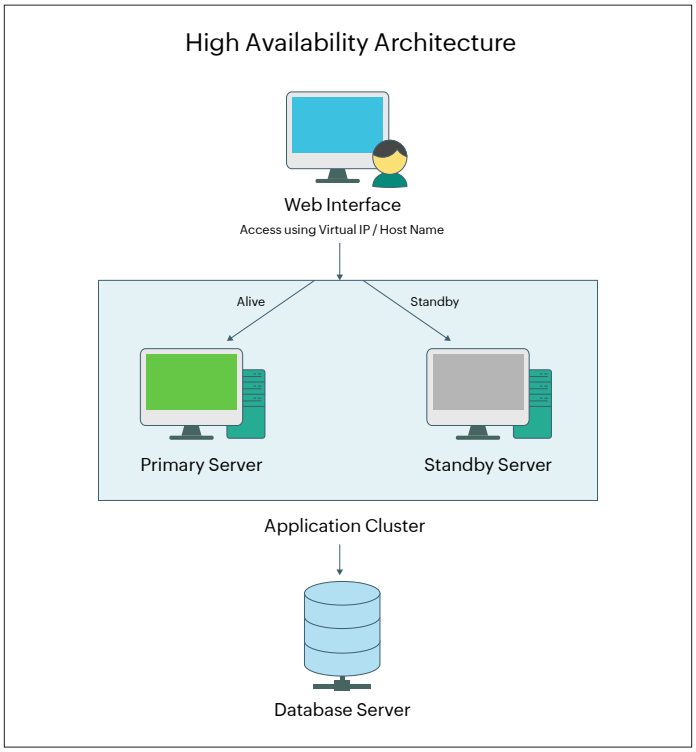
Google Workspace recovery: When any recovery action is triggered by the administrator, ADManager Plus fetches the data to be restored (the objectID, userID, and binary file information) from the repository. ADManager Plus uses the binary file information to restore the data. ADManager Plus connects to Google Workspace through Google API services, and the objectID and userID information is used to perform the restoration. The result is displayed on the product dashboard and the restore history page.



4. High availability

If ADManager Plus is installed as a service, you can configure the tool to automatically start as soon as the server starts. Web service availability can be ensured by enabling the high availability option. ADManager Plus achieves this by employing a high availability architecture that designates a server to act as a standby to the primary server.

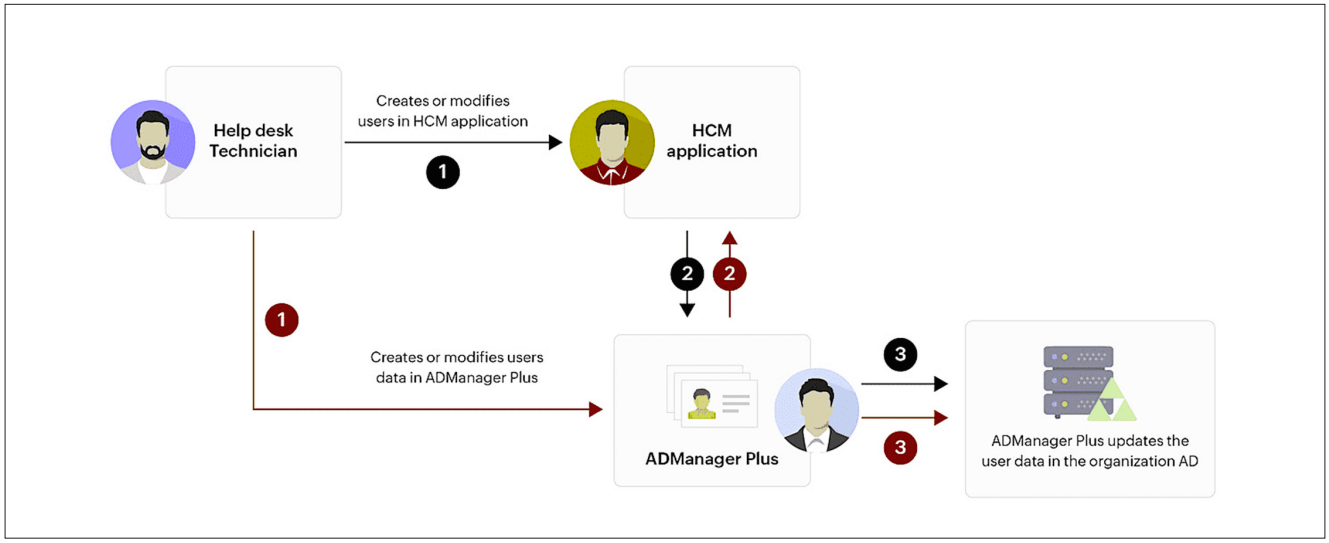
- The same database is used for both the servers, and at any given time, a single server will cater to user requests and the other will be inactive.
- Whenever the primary server runs encounters unplanned downtime, the standby server becomes operational and takes control of components.



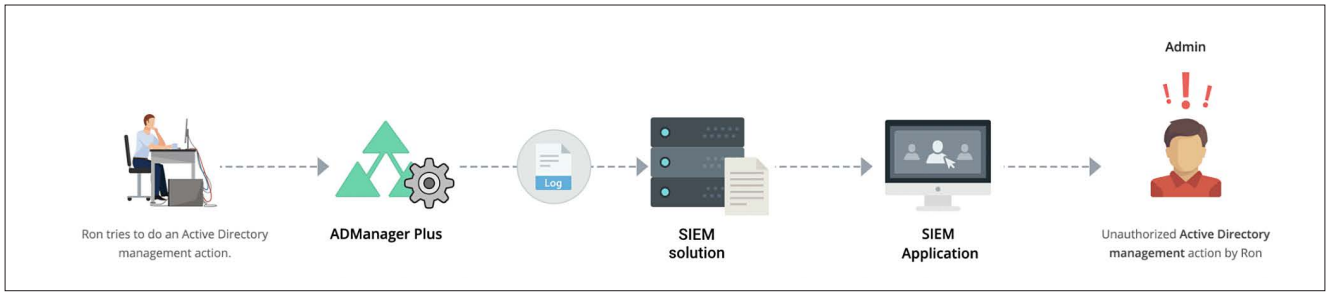
5. Integration

5.1 Integration with HCM applications

ADManager Plus can be integrated with HCM applications to retrieve user data and automate AD tasks using templates and policies. This eliminates the need for manual updates by HR admins and allows for scheduled user provisioning. The integration process is simplified with preconfigured settings for a wide range of applications.

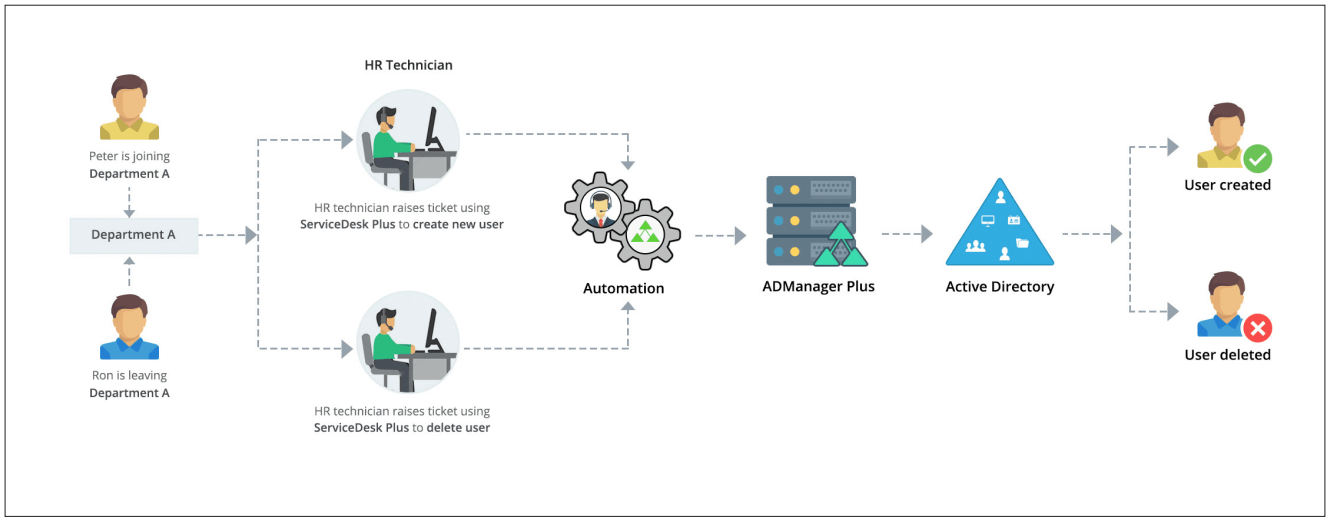


5.2 Integration with SIEM applications



Integration with SIEM solutions make it easy to analyze the audit trail of AD management actions executed using ADManager Plus. Detected activities performed through ADManager Plus are logged and sent to the SIEM system post action. SIEM systems generate alerts based on predefined rules or thresholds, and notifications are sent to administrators. Organizations can utilize this to analyze logs and detect anomalies, threats, and vulnerabilities.

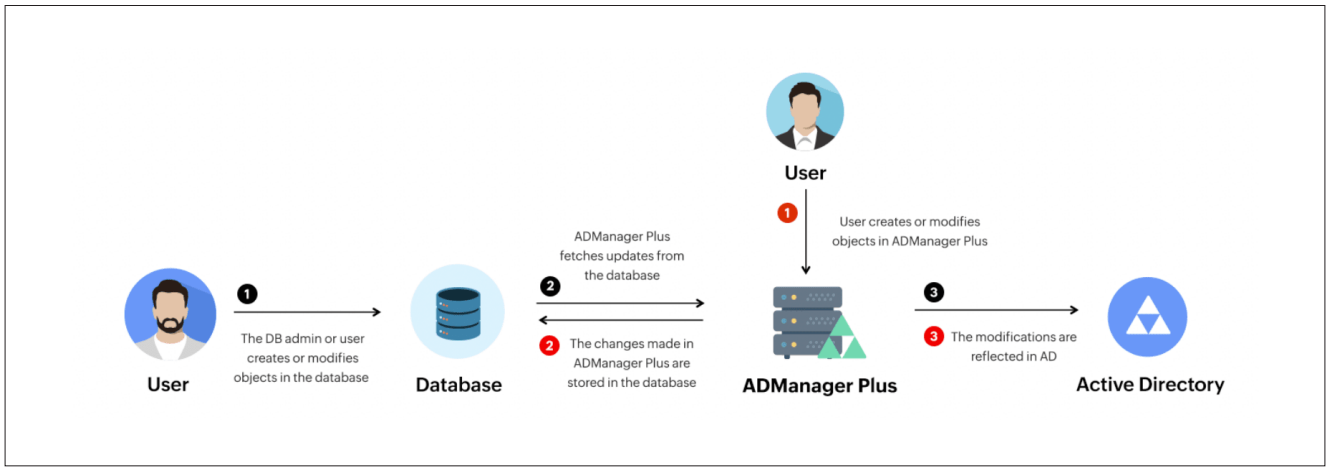
5.3 Integration with ITSM and help desk applications



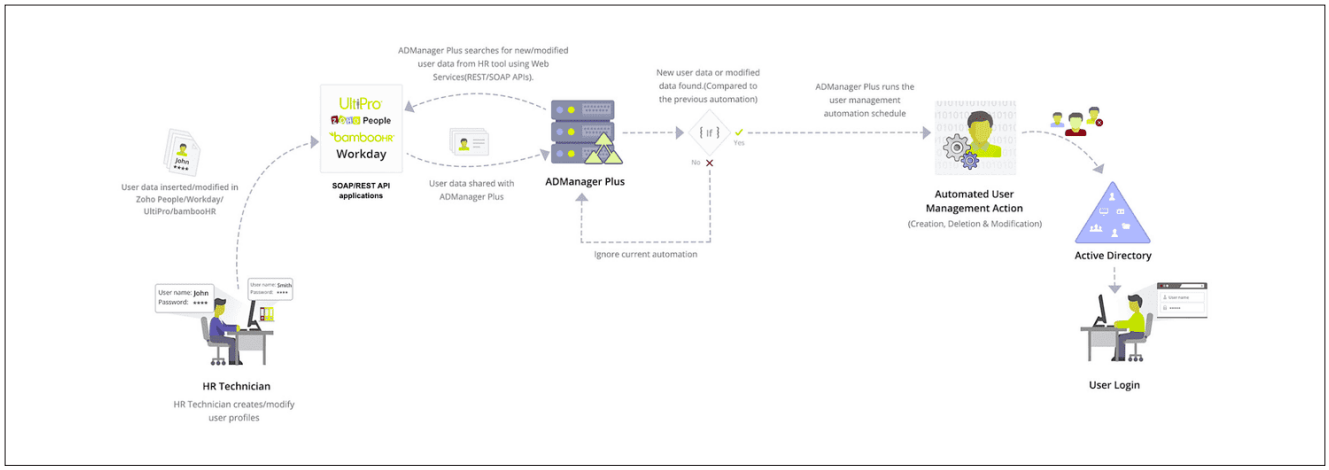
Integrating ADManager Plus with ITSM applications streamlines identity management requests. Automations can be set up to regularly retrieve tickets generated in ITSM applications and initiate actions such as user provisioning or adjusting permissions that will be updated in AD. Post update, closing the ticket can also be automated. This process aligns user management processes with overall IT service delivery, promoting a cohesive and well-coordinated approach within the organization.

5.4 Integration with databases

ADManager Plus simplifies AD account management for IT administrators and HR managers by seamlessly integrating with Microsoft SQL and Oracle databases. This integration enables effortless user provisioning, management, and deprovisioning, eliminating the need for manual intervention. ADManager Plus extracts relevant user data from the integrated databases. Extracted data is synchronized with AD, and the processed data is also updated in the database to ensure consistency between the database records and user accounts in AD



5.5 Integration with any enterprise application using APIs



ADManager Plus integrates with various applications, like UKG Pro, ServiceDesk Plus, and Salesforce, to automate user management. The process begins with ADManager Plus searching for new or modified user data from the external applications using web services (REST or SOAP APIs). The new or modified data is then compared to the previous version. Following this, ADManager Plus runs the user management automation schedule, leading to automated user management actions involving the creation, deletion, and modification of user data in AD.

6. Rest APIs

ADManager Plus offers REST APIs to enable integration with other applications like help desk tools. These APIs allow you to access ADManager Plus from other applications and perform necessary AD user account management functions. Click here to know more.

7. Mobile applications

ADManager Plus can be accessed from anywhere at anytime using its iOS and Android applications. A wide range of AD management and reporting actions are accomplished with the help of APIs.

8. Security measures against vulnerabilities

ADManager Plus takes stringent security measures during different phases of the development cycle to mitigate security vulnerabilities. These measures are overseen by a security team exclusively meant to diagnose and handle potential vulnerabilities in the product.

Our in-house security tool is one such measure to help identify and mitigate potential security vulnerabilities in a product executable. It works by applying a set of rules and provides security reports listing all the rules that were violated in the product executable. Additionally, an internal and external bug bounty program has been put in place to report on the vulnerabilities in our suite of products.

9. Confidentiality

ADManager Plus application has implemented the following measures to uphold the confidentiality of user data:

- ADManager Plus' database is password protected by default.
- Database backup passwords are generated at the time of backup and can be configured in Privacy Settings (Admin -> General Settings -> Security and Privacy -> Privacy Settings) in the tool.
- Exported reports can be protected by password.
- Only authorized users can carry out operations in ADManager Plus.

- No user details are exposed without authorization.
- Object name (Name of the object on which the action was carried out)
- Object domain (Domain name of the object)
- Status (Result of the task)
- Additional details such as attribute values and request details

10. Integrity

ADManager Plus report data is fetched from Active Directory directly. To maintain the integrity of the report data, the AD sync occurs every 10 minutes. The intuitive dashboard is updated on a daily basis. The report data in ADManager Plus will have the same information as in the domain controllers. The tool will also check values of non-replicated attributes such as lastlogonTime on each DC to find the most recent one before displaying it.

11. Accountability

Audit logs maintain the details of all AD Management activities like password reset, user deletion, creation/modification of user accounts, etc., performed using ADManager Plus. Besides these, audit reports list the actions performed by help desk technicians. It provides details, such as what action was performed on which object and the time at which it was performed.

List of entities stored in the database while ADManager Plus syncs with Active Directory are as follows:

- User attributes
- Group attributes
- Computer attributes
- Contact attributes
- OU attributes

Information stored in ADManager Plus database which will be displayed in audit reports are:

- Name of the technician who performed the task
- Action name (Example: Unlock Users)
- Action category (Example: User Modification)
- Module used (Module used to perform the task, example: Automation)

- Action time
- Object name (Name of the object on which the action was carried out)
- Object domain (Domain name of the object)
- Status (Result of the task)
- Additional details such as attribute values and request details.

ADManager Plus is a unified solution for all your AD, Exchange, Skype for Business, Google Workspace, and Microsoft 365 management needs. It simplifies several routine tasks such as provisioning users, cleaning up dormant accounts, managing NTFS and share permissions, and more. ADManager Plus also offers more than 200 prepackaged reports, including reports on inactive or locked-out AD user accounts, Microsoft 365 licenses, and users' last logon times. Perform management actions right from these reports. Build a custom workflow structure that will assist you in ticketing and compliance, automate routine AD tasks such as user provisioning and de-provisioning, and more.
Download a free trial today to explore all these features.

Related resources:

- Permissions required for the AD account configured in ADManager Plus
- System requirements
- Steps to install ADManager Plus