ManageEngine
ADManager Plus

Solution Architecture

www.admanagerplus.com

Table of Contents

ManageEngine ADManager Plus

ManageEngine ADManager Plus is an identity governance and administration (IGA) solution with powerful hybrid Active Directory (AD) management and reporting capabilities that helps you streamline identity management across enterprise applications. With an intuitive, easy-to-use interface, ADManager Plus handles complex tasks like user provisioning and deprovisioning, running access certification campaigns, orchestrating identity management activities, automating routine AD operations, implementing approval-based workflows, integrating with third-party applications, performing non-invasive delegation, and protecting data on your enterprise platforms with regular backups.

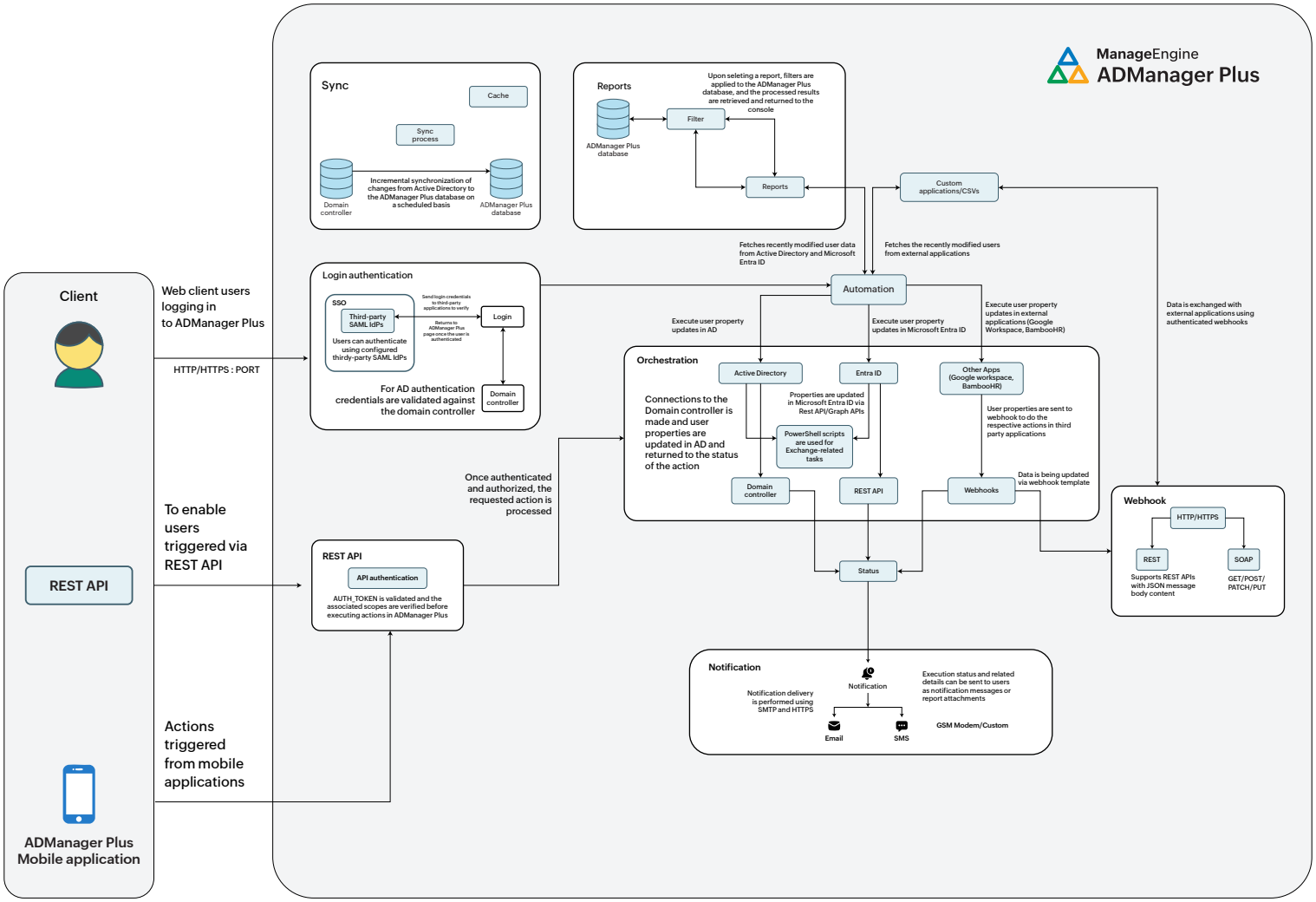
ADManager Plus provides a comprehensive collection of AD reports, including those crucial for fulfilling compliance requirements. It enables the management and reporting of Exchange Server, Microsoft 365, Google Workspace, and AD environments from a unified interface.

- Quickly view the status of key AD objects with an intuitive, customizable dashboard.
- Get one-step, multi-platform user provisioning for AD, Microsoft 365, Exchange, and more.
- Perform on-the-fly management tasks from over 200 built-in reports.
- Use risk status insights to assess potential risks within your AD and Microsoft Entra ID environment.
- Visualize potential attack paths in your AD environment to identify vulnerable privileged groups and reduce security risks.
- Review object access rights and permissions with periodic audit campaigns.
- Orchestrate and execute life cycle management task sequences across various integrated applications.
- Get script-free automation of critical and repetitive tasks.
- Monitor and streamline the execution of various AD tasks with multi-level, approval-based workflows.
- Assign AD tasks to help desk technicians with granular, non-invasive delegation.
- Back up and restore AD, Microsoft Entra ID, and Google Workspace objects.

1. ADManager Plus architecture

ManageEngine ADManager Plus is an identity governance and administration (IGA) solution with powerful hybrid Active Directory (AD) management and reporting capabilities that helps you streamline identity management across enterprise applications. With an intuitive, easy-to-use interface, ADManager Plus handles complex tasks like user provisioning and deprovisioning, running access certification campaigns, orchestrating identity management activities, automating routine AD operations, implementing approval-based workflows, integrating with third-party applications, performing non-invasive delegation, and protecting data on your enterprise platforms with regular backups.

ADManager Plus provides a comprehensive collection of AD reports, including those crucial for fulfilling compliance requirements. It enables the management and reporting of Exchange Server, Microsoft 365, Google Workspace, and AD environments from a unified interface.



1.1 How ADManager Plus works

User access and authentication

- Web client users log into ADManager Plus through HTTPS.
- Supports multiple authentication methods including third-party SSO providers using SAML, as well as traditional AD authentication.
- Domain controllers can be integrated for user verification.

Core operations

- Users perform AD management tasks through the product interface.
- Sync process automatically updates changes from AD to the ADManager Plus database.
- Custom workflows can be established for user life cycle management.

Reporting and analytics

- When users request reports, the system filters data from the ADManager Plus database.
- Reports can be customized and generated based on user needs.
- Fetches, for example, recently modified users from both Microsoft Entra ID and external applications.

Automation and integration

- Includes automation features for user provisioning and management.
- Connects to various external systems like Microsoft Entra ID, LDAP/LDAPS, and webhooks.
- Triggers actions from mobile applications via REST API.

Notifications

- Sends notifications through email and SMS.
- Supports workflow automation using SMTP for email delivery.

External connectivity

- REST API enables integration with other applications.
- Pulls data from external sources using webhooks.
- Supports Graph API for Microsoft 365 integration.
- The overall flow ensures that management tasks are centralized, automated, and accessible through multiple channels while maintaining security and audit trails.

1.2 Architectural components

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

Server

You can deploy ADManager Plus on 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 is bundled with a PostgreSQL database, with the option to migrate to an external Microsoft SQL Server database. The database is automatically backed up on the first day of every month to protect against data loss resulting from system failures, accidental deletions, or infrastructure issues. 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.

1.3 ADManager Plus' technology stack

- The client-side of the application is developed using HTML, CSS, JavaScript, jQuery plugins, and the Ember.js framework.
- The server-side framework is developed using Java, Native C, and C#, with Jakarta Server Pages (JSP) used for server-side rendering where applicable.
- ADManager Plus uses Java Database Connectivity (JDBC) to connect to databases.
- ADManager Plus allows web browsers and servers to communicate using HTTP/HTTPS and LDAP/LDAPS protocols, respectively, along with other required Windows protocols.

Ports for ADManager Plus core functionality

These ports are used for internal communication within the ADManager Plus application or for accessing its web console.

Port number	Protocol	Purpose	Notes
8080	HTTP	Default web access to ADManager Plus console.	Customizable during installation.
8443	HTTPS	Secure web access to ADManager Plus console.	Recommended for secure connections.
33306	TCP	Connection to the product's database.	Default for bundled PostgreSQL.
9280	HTTP	Connection to the Elasticsearch database.	Used for search functionality.
9380	TCP	Inter-node communication in a cluster.	Only required in a clustered deployment.

Ports for communication with managed systems

These ports facilitate communication from the ADManager Plus server to your domain controllers, Exchange servers, Microsoft 365, Google Workspace, and other managed systems. All connections listed here are outbound from the ADManager Plus server and inbound to the managed systems.

Port Number	Protocol	Source	Destination	Port Type	Service	Purpose
389/636	TCP and UDP	ADManager Plus Server	Domain Controllers	Static	LDAP	To connect to AD.
135	TCP	ADManager Plus Server	Domain Controllers	Static	RPC	For data exchange.
445	TCP	ADManager Plus Server	Domain Controllers	Static	SMB	To get access to shared file systems.
88	TCP	ADManager Plus Server	Domain Controllers	Static	Kerberos	For authentication when accessing a domain resource.

3268/ 3269	TCP	ADManager Plus Server	Domain Controllers	Static	Global Catalog	Necessary for performing search operations in the Global Catalog.
25	SMTP	ADManager Plus Server	SMTP server	Static	SMTP	To send emails.
80	HTTP	ADManager Plus Server	Exchange server	Static	Exchange	For connecting to Exchange servers.
80, 443	HTTP/ HTTPS	ADManager Plus Server	Microsoft 365 or Google Workspace servers	Static	Microsoft 365 and Google Workspace	Required for communicating 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.
464	TCP and UDP	ADManager Plus Server	RPC randomly allocated high TCP ports	Dynamic	Kerberos	To change or set user passwords.
5985/ 5986	TCP	ADManager Plus Server	RPC randomly allocated high TCP ports	Dynamic	PowerShell remoting	For executing reports and management actions that involve running commands on domain controllers.

For detailed firewall and network requirements for Microsoft 365 and Google Workspace platforms, see System Requirements.

2. ADManager Plus login process

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

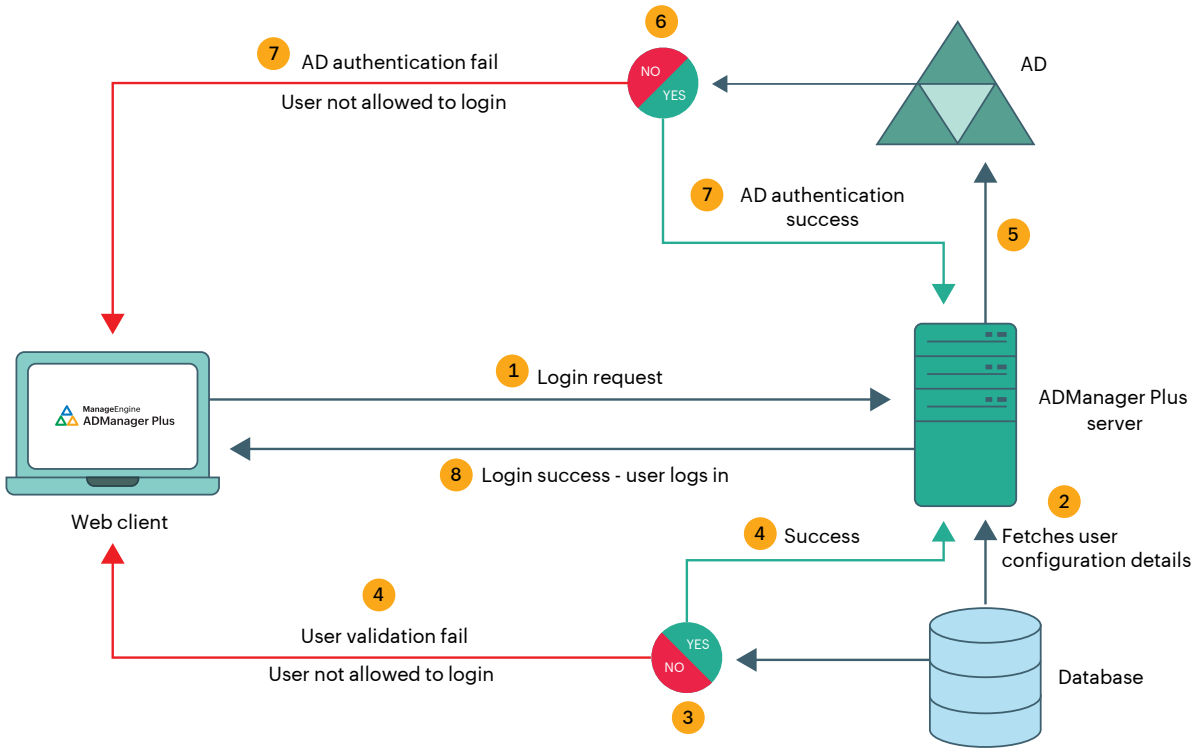
ADManager Plus comes with three built-in technician accounts:

- 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

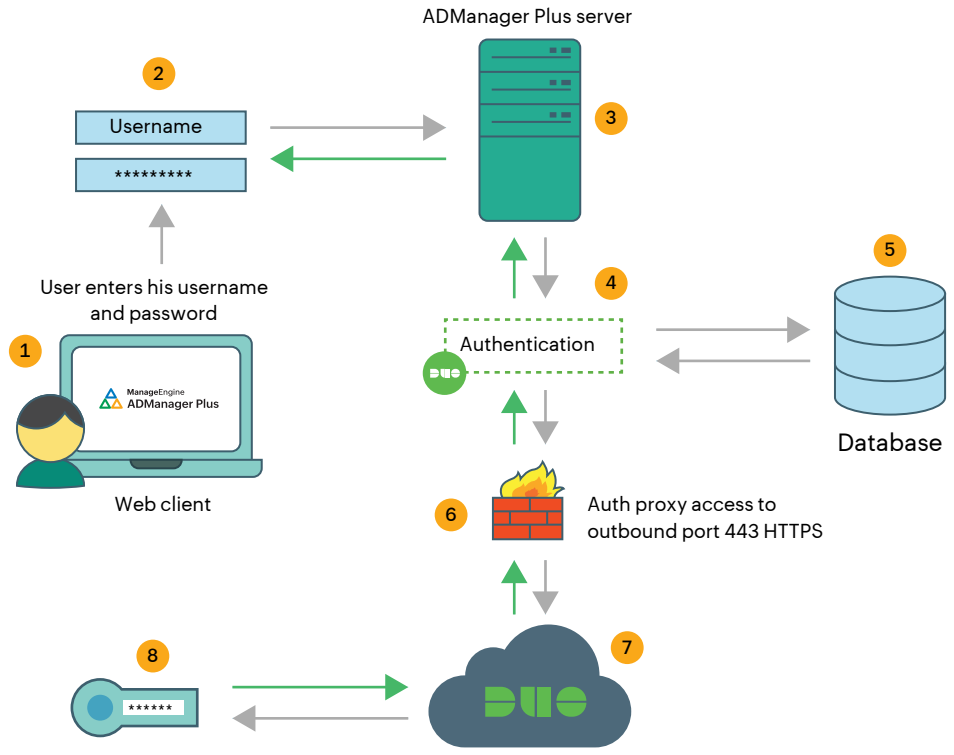
Users can log in to ADManager Plus using domain authentication, Two-Factor Authentication (2FA), and SSO authentication services.

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.

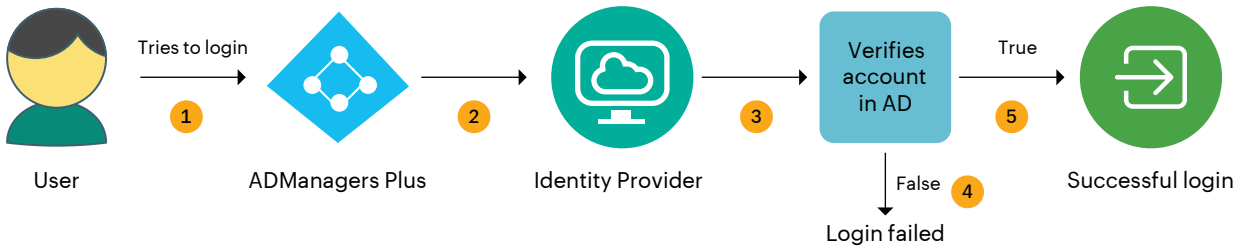
Duo Security: Once the user enters the credentials, the tool authenticates it with AD. On successful authentication, username and application key will be sent to Duo Security for verification. Upon successful verification, the user will be logged into to ADManager Plus. The Duo Security secret key is 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.

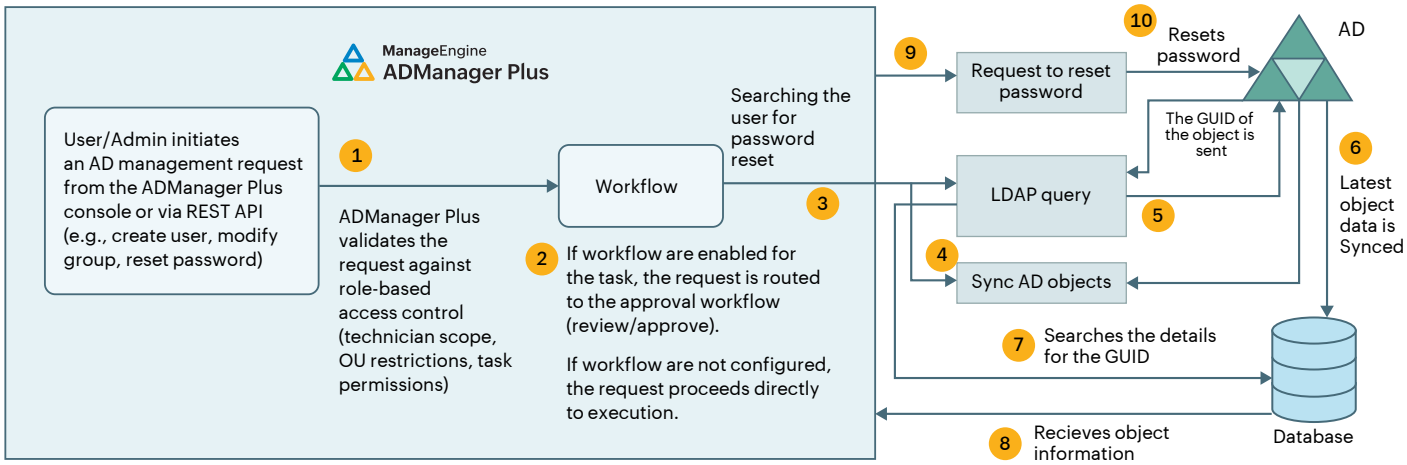
3. ADManager Plus modules

3.1 Management and workflow

ADManager Plus follows a centralized management architecture where all identity management actions are initiated through the web or API layer and processed by the server-side execution engine. Each request is validated against role-based access controls and, if configured, optionally routed through approval workflows before execution. The execution engine retrieves the required object state from the ADManager Plus database, invokes the appropriate directory or cloud connector, and performs the requested operation. Execution results, including success or failure status and attribute changes, are persisted in the database and reflected in the management console, reports, and audit logs.

AD:

For on-premises AD management, ADManager Plus uses LDAP queries to identify directory objects and executes changes using native Windows APIs and PowerShell where required. Operations such as user provisioning, group modification, and access updates are performed directly against domain controllers, with results synchronized back to the product database.



APIs used:

ADsOpenObject

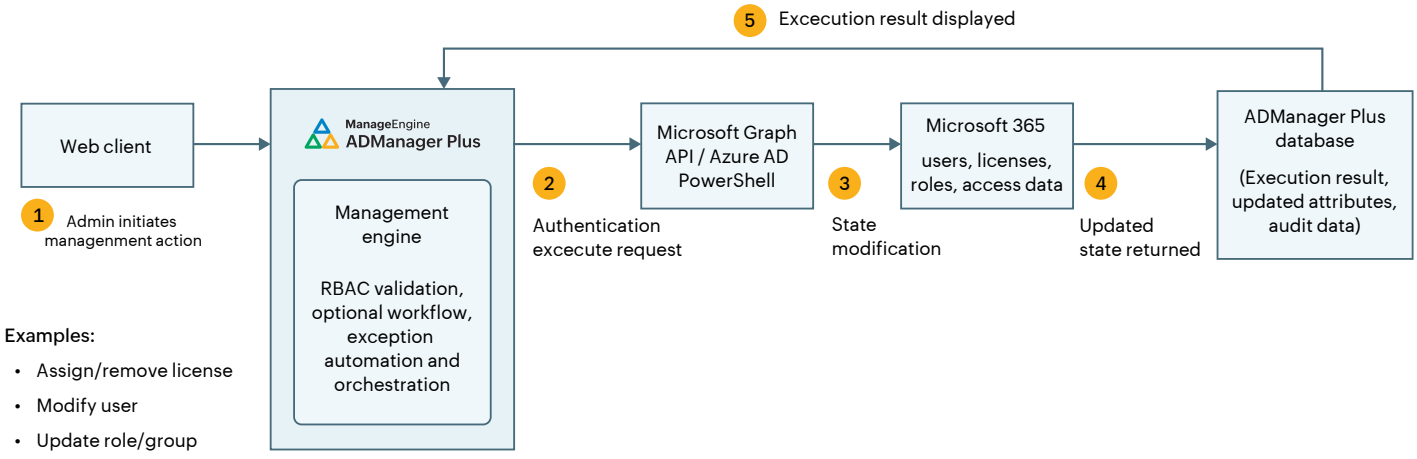
SetObjectAttributes

SetPassword

CreateDSObject

Microsoft 365:

For Microsoft 365, ADManager Plus executes management actions using REST-based integrations such as Microsoft Graph APIs and, where applicable Microsoft Entra PowerShell. For example, license management operations retrieve user and license details from the database and invoke the appropriate API or PowerShell command. Updated cloud identity state is then stored and displayed in the console.



Google Workspace:

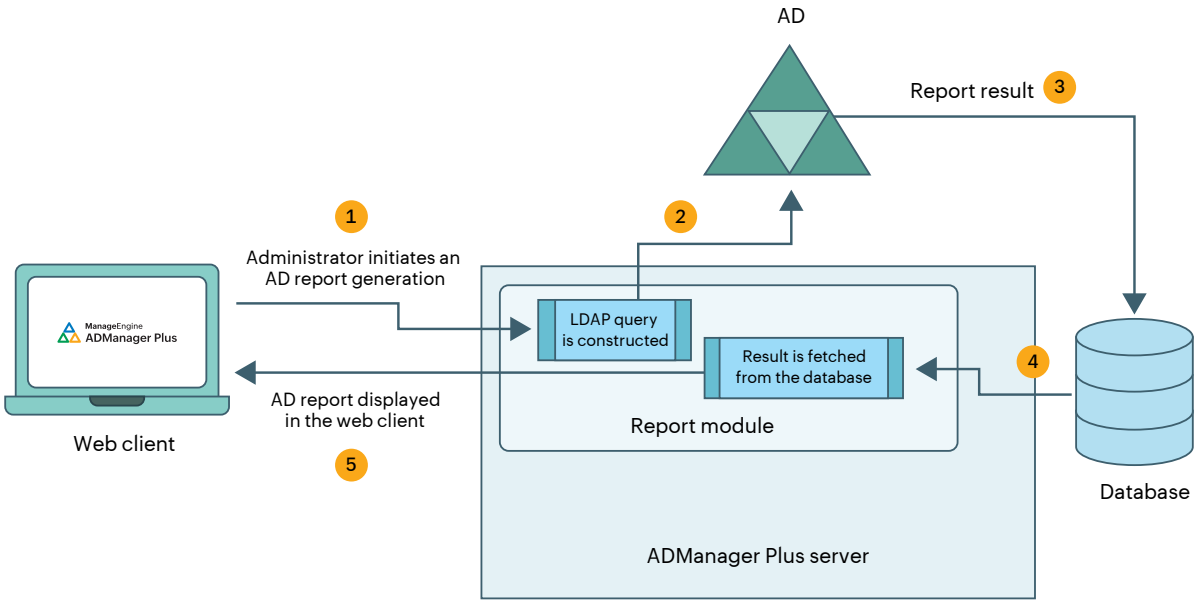
For Google Workspace environments, management operations are performed using Google Workspace Admin APIs over secure HTTPS connections. User actions are executed via API calls, with the resulting state captured in the ADManager Plus database to maintain auditability and reporting consistency.

3.2 Reporting

ADManager Plus implements a unified reporting architecture where report requests are submitted from the web client to the server over HTTP/HTTPS. Based on the report type, the reporting engine dynamically constructs directory queries or API calls, retrieves identity and access data from the target systems, and normalizes the results into the product database. This stored data enables historical analysis, compliance reporting, risk assessment, risk exposure management, and access certification workflows. Reports are rendered through the console and can be exported in multiple formats for audit and compliance use.

AD:

AD reports are generated using LDAP queries and native directory APIs such as IDirectorySearch to retrieve user activity, group memberships, permissions, and access-related attributes.



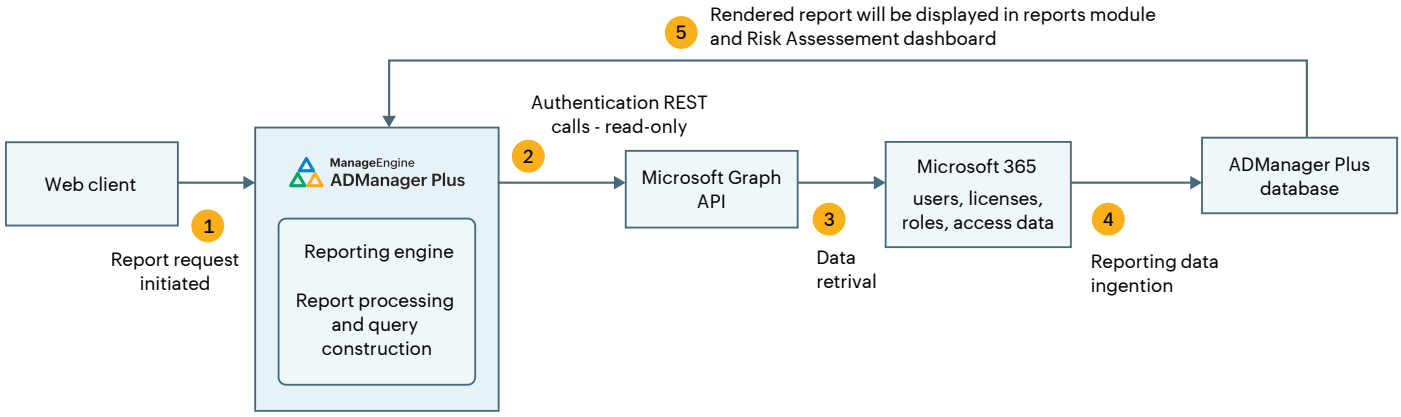
APIs used:

IDirectorySearch::ExecuteSearch

IDirectorySearch::GetColum

Microsoft 365:

Microsoft 365 reports use REST-based integrations, including Microsoft Graph APIs, to collect data on users, licenses, roles, and access configurations for cloud governance and certification use cases.



Google Workspace:

Google Workspace reports are generated using Google Workspace Admin APIs to retrieve Google Workspace users, active user, and suspended users data over secure HTTPS connections.

3.3 ADManager Plus delegation

Roles in ADManager Plus:

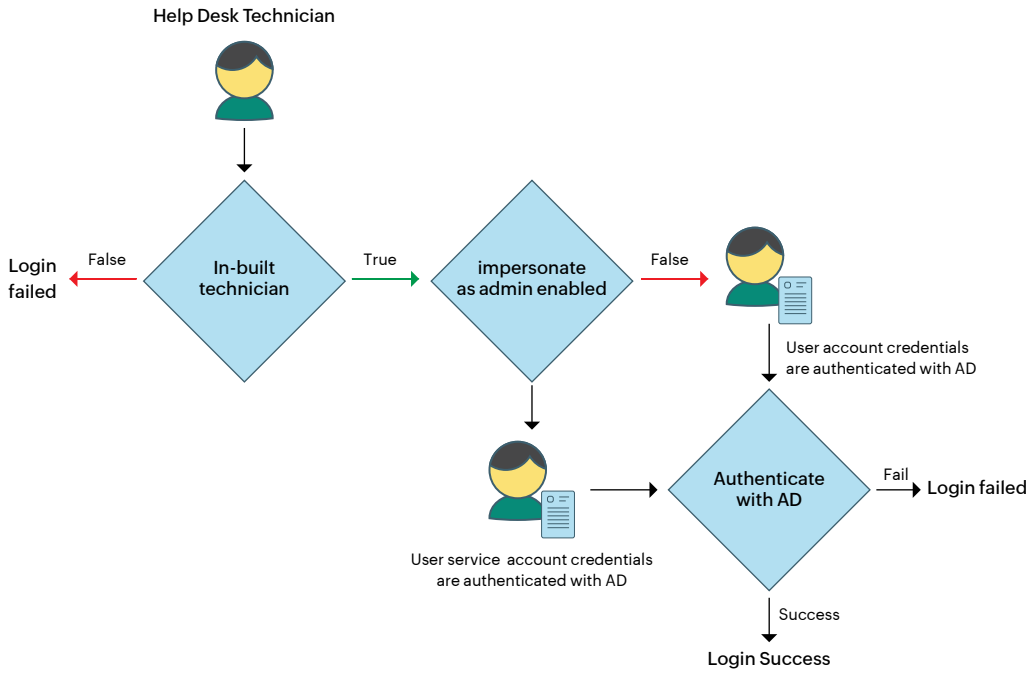
ADManager Plus offers predefined help desk roles that can be assigned to help desk technicians. These roles can be deleted or modified based on your needs. However, the Super Admin role, which contains all the privileges, cannot be deleted or modified. You can also create customized roles and assign 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 Directory/Application 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 Directory/Application 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 Directory/Application Settings section 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 Directory/Application Settings section. 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.

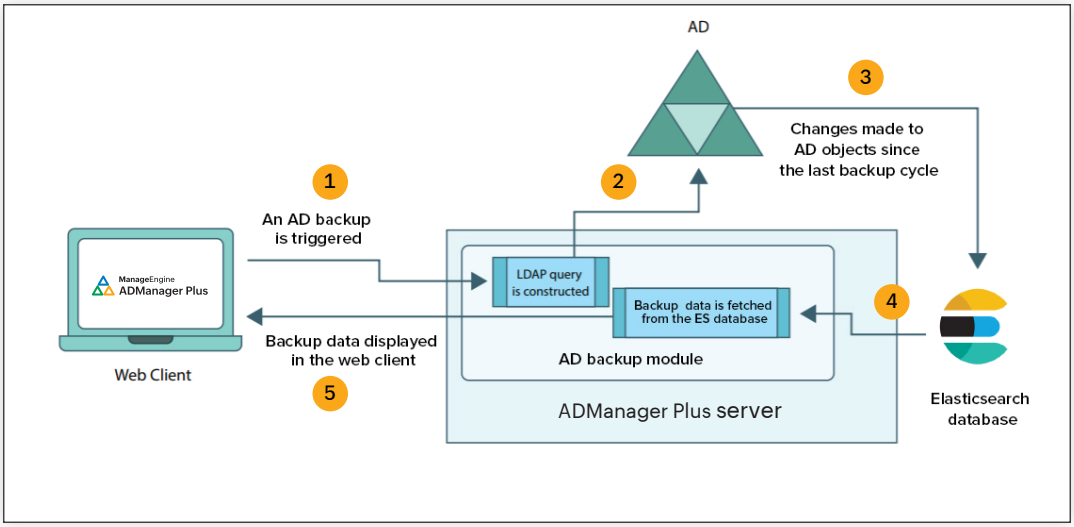
3.4 Backup and recovery

3.4.1 AD backup and recovery

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

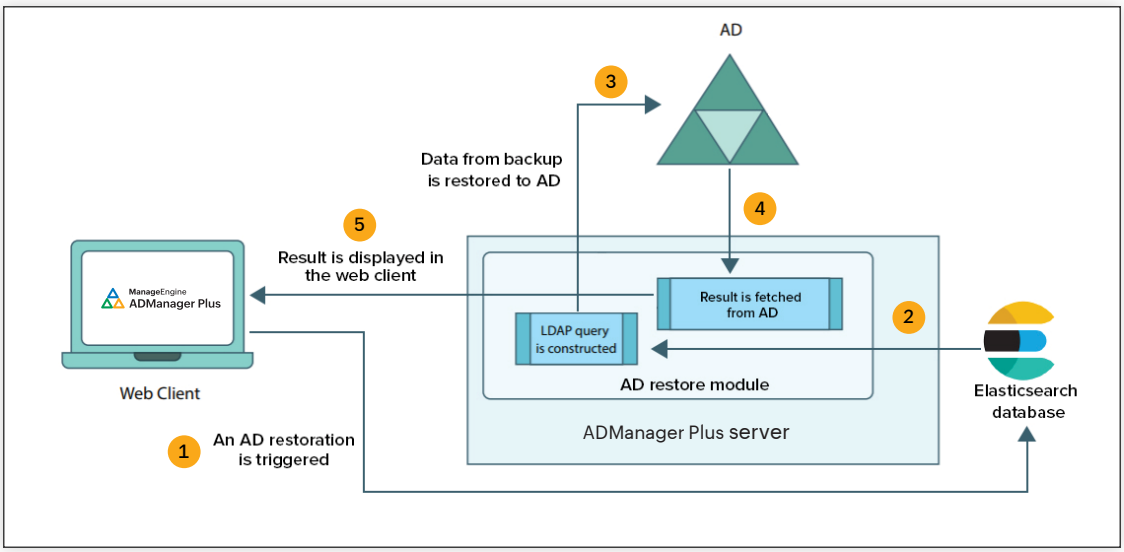
AD backup:

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:

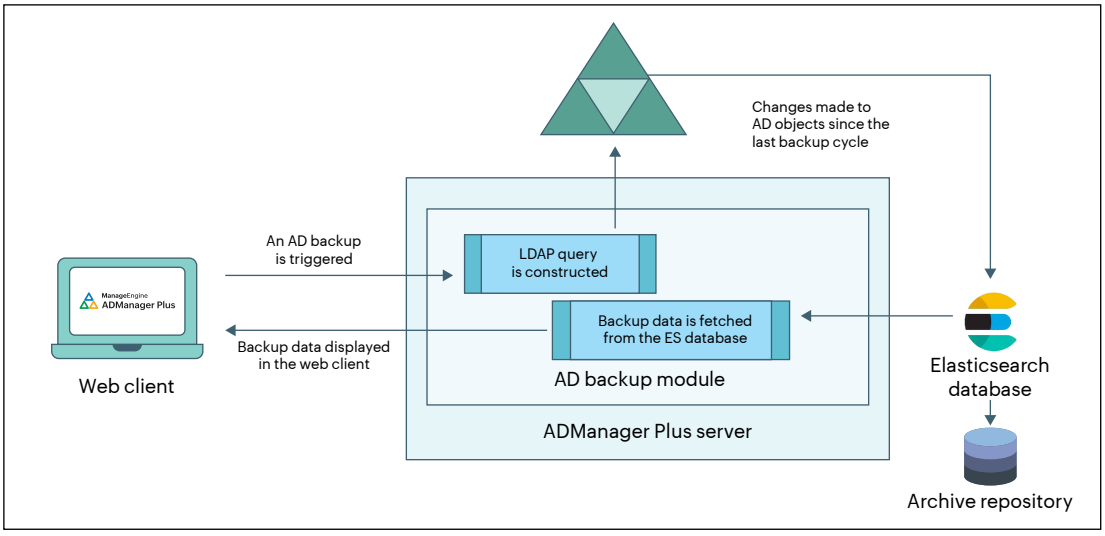
When any recovery action is triggered by the administrator, an LDAP query is generated and the ADManager Plus server fetches the data to be restored from the Elasticsearch database. This value is then restored to AD, and the result is displayed in the GUI.



3.4.2 Microsoft Entra ID backup and recovery

Microsoft Entra ID backup:

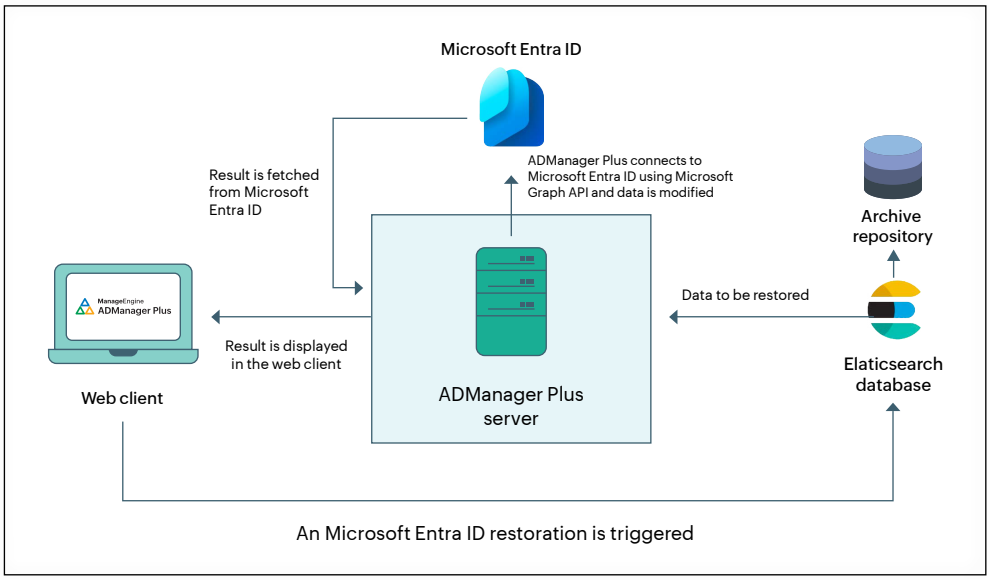
ADManager Plus backs up all Microsoft Entra ID objects in your tenant, including users, groups, applications, service principals, and directory roles. When a Microsoft Entra ID backup is triggered, the web client sends the input to the server via HTTP/HTTPS. The delta token from the previous backup is fetched from the SQL database. ADManager Plus then connects to Microsoft Entra ID through the Microsoft Graph API and fetches the data modified since the last backup cycle. All changes made to Microsoft Entra ID objects since the last delta token are backed up and stored in the backup repository. A new delta 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.



Storing all backed up data in Elasticsearch is not always ideal since it might cause performance issues. ADManager Plus offers the flexibility to store older backed up data in an archive repository, and re-index it as needed for restoration. Archived backups can be stored in local, shared, and NAS repositories. After a backup is completed, ADManager Plus identifies backups that have exceeded the index period, de-indexes them, and moves them to the archive repository. The data remains in the archive repository until it surpasses the archive retention period, at which point it is permanently deleted.

Microsoft Entra ID recovery:

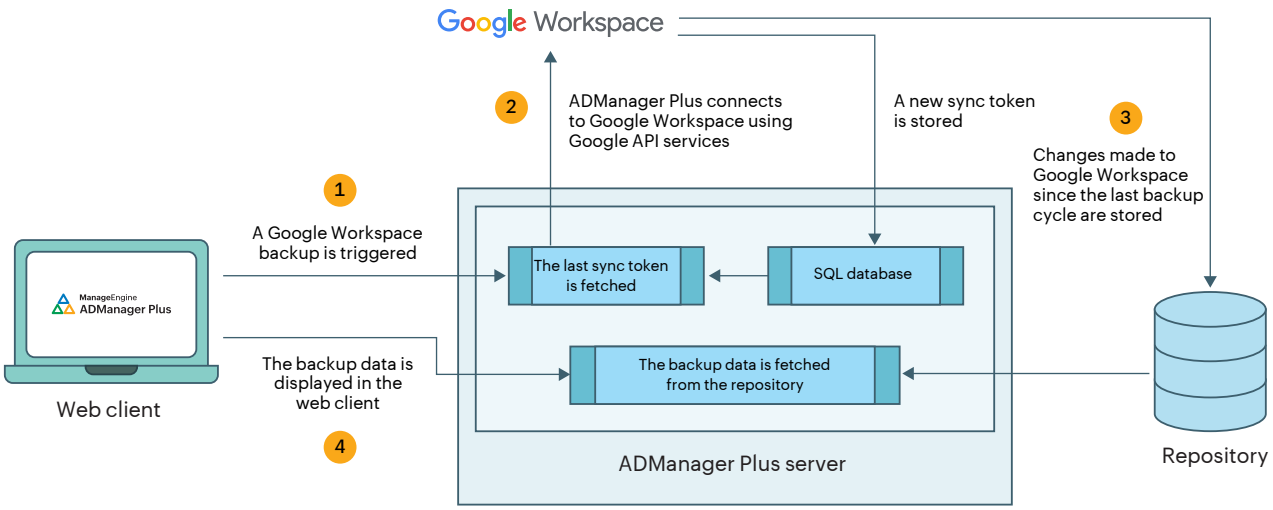
When a recovery action is initiated, the administrator first begins by searching the Elasticsearch database for the data to be restored. If the data is not found, it must be retrieved from the archive repository and re-indexed to the Elasticsearch database for restoration. When the data is found in the Elasticsearch database, ADManager Plus then connects to Microsoft Entra ID through the Microsoft Graph API, and the values are restored to Microsoft Entra ID. The result is then displayed in the UI.



3.4.3 Google Workspace backup and recovery

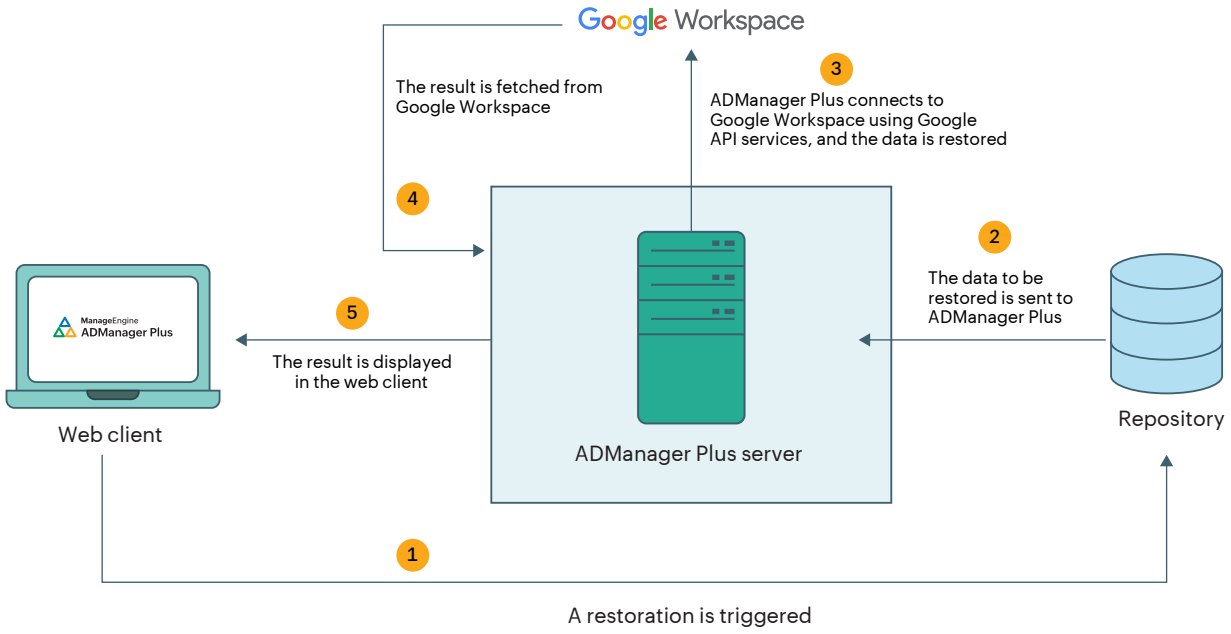
Google Workspace backup:

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:

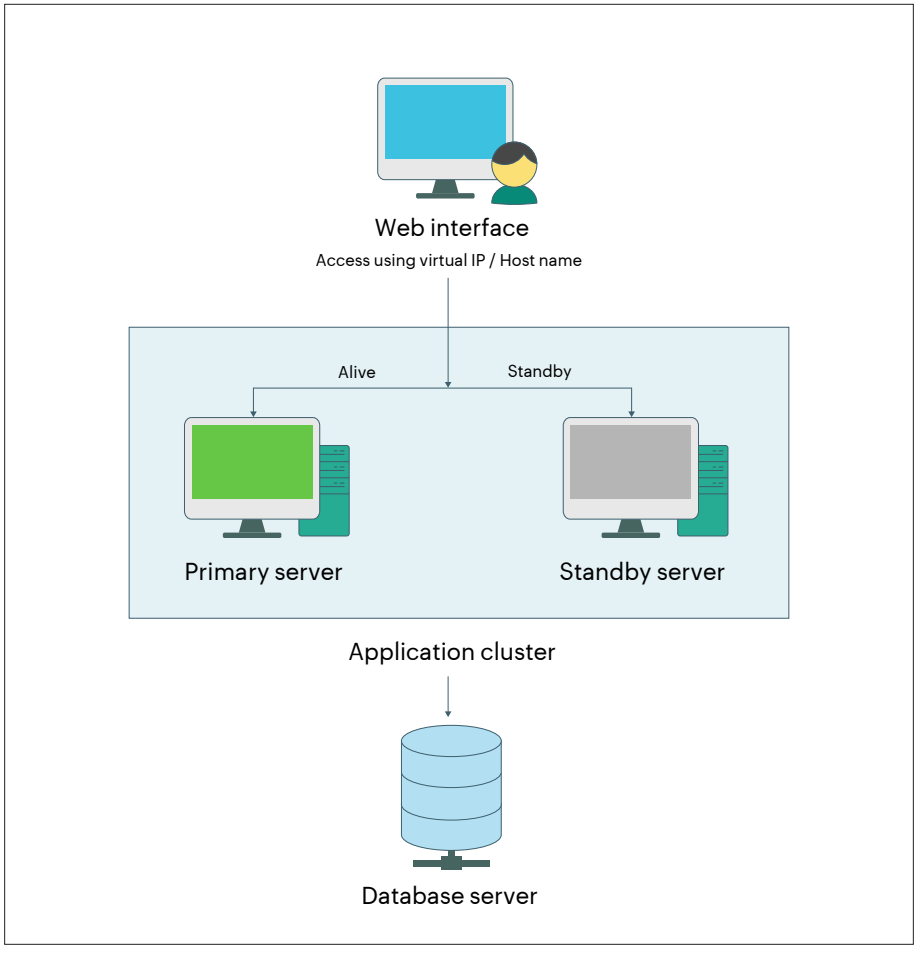
When any recovery action is triggered by the administrator, ADManager Plus fetches the data to be restored (the objectID, userID, and binary file information) from the repository. ADManager Plus uses the binary file information to restore the data. ADManager Plus connects to Google Workspace through 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.

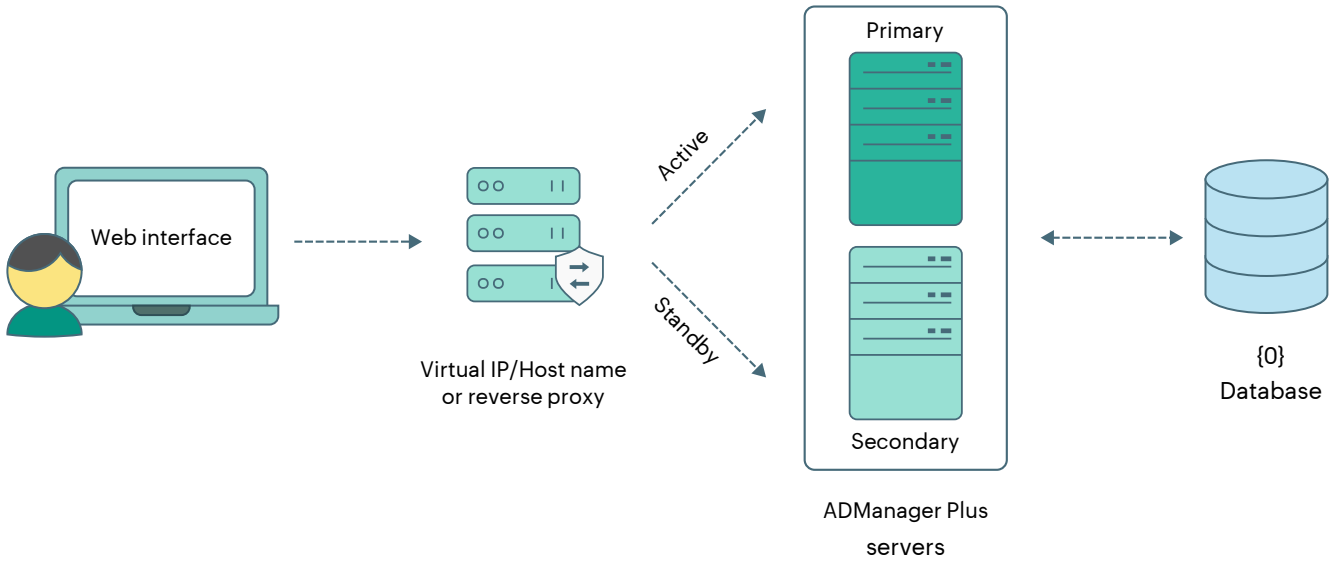
- The same database is used for both the servers, and at any given time, a single server will cater to user requests and the other will be inactive.
- Whenever the primary server runs encounters unplanned downtime, the standby server becomes operational and takes control of components.



5. Load balancing

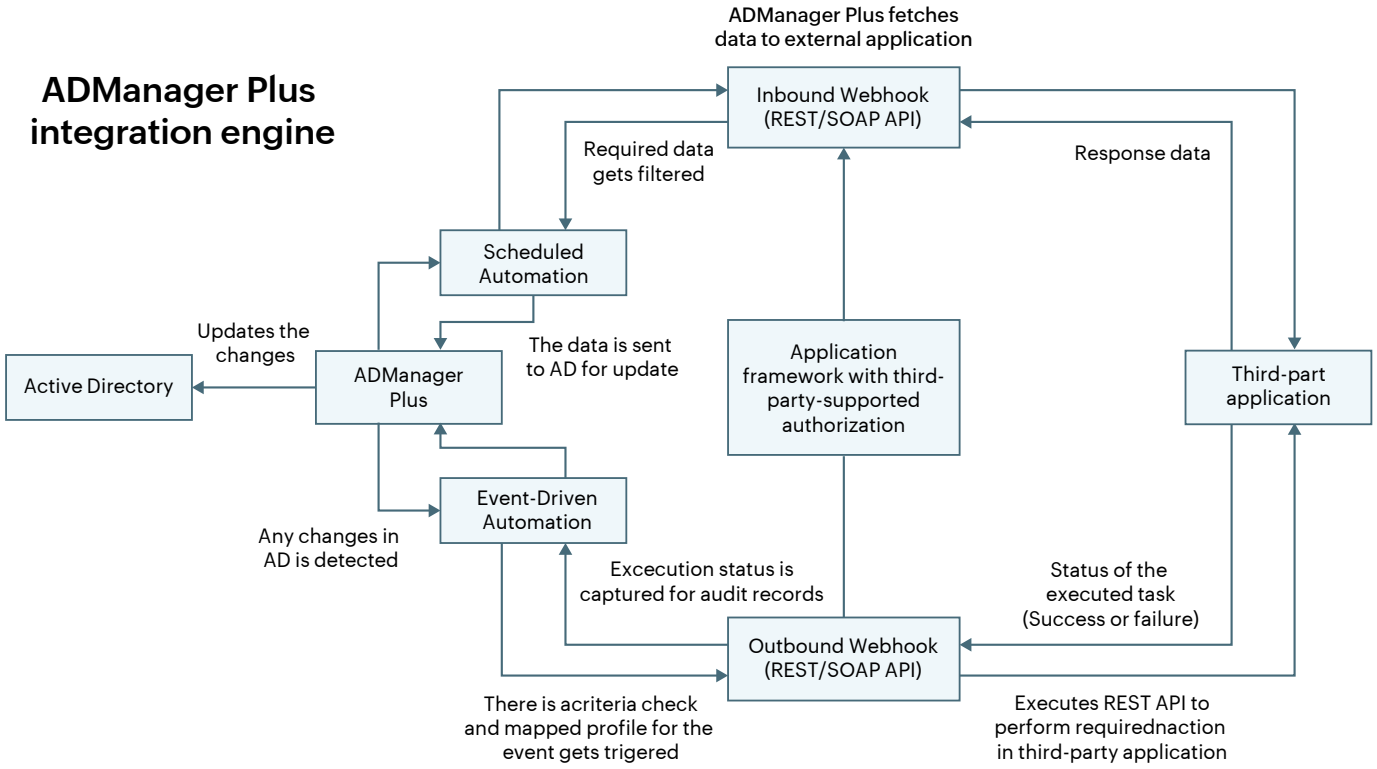
ADManager Plus supports built-in, application-layer load balancing for enterprise deployments, enabling horizontal scaling and high availability. In a load-balanced setup, a designated primary node hosts the load balancing service and exposes a virtual access endpoint (virtual hostname or IP). All UI, REST API, and automation requests are received at this endpoint and routed to active nodes based on node health and availability. Each node processes requests independently while sharing a common backend database, ensuring consistency of configuration, execution state, reporting data, and audit logs across the cluster.

The load balancing mechanism is integrated with ADManager Plus failover logic. If the primary node hosting the load balancer becomes unavailable, request routing automatically shifts to the next available secondary node, which can be promoted to assume the primary role. Scheduler execution and workflow orchestration are owned by a single active node at any time and coordinated through the shared database to prevent duplicate job execution during failover. This design ensures continuous service availability, controlled execution, and seamless client access without requiring changes to the access endpoint.



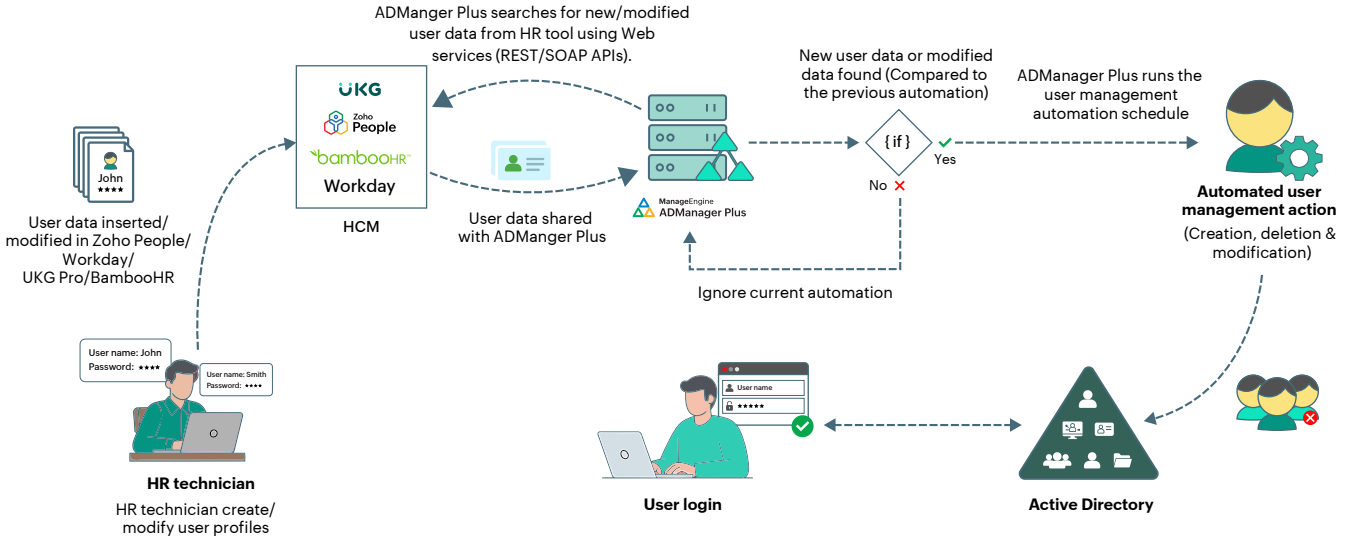
6. Integrations

The ADManager Plus integration engine supports both scheduled and event-driven automation to orchestrate identity operations between AD and external applications. Scheduled automations authenticate to external systems using secure credentials such as OAuth tokens, API keys, or service accounts and exchange filtered identity data through authenticated inbound webhooks over REST or SOAP APIs, after which validated updates are executed in AD using delegated directory credentials. Event-driven automations continuously monitor AD for changes, perform criteria checks and profile mappings, and invoke authenticated outbound webhooks through an application framework that enforces third-party authorization. All external API calls, directory operations, and execution responses are authenticated, authorization-checked, and the resulting success or failure status is captured and stored for audit, compliance, and traceability.



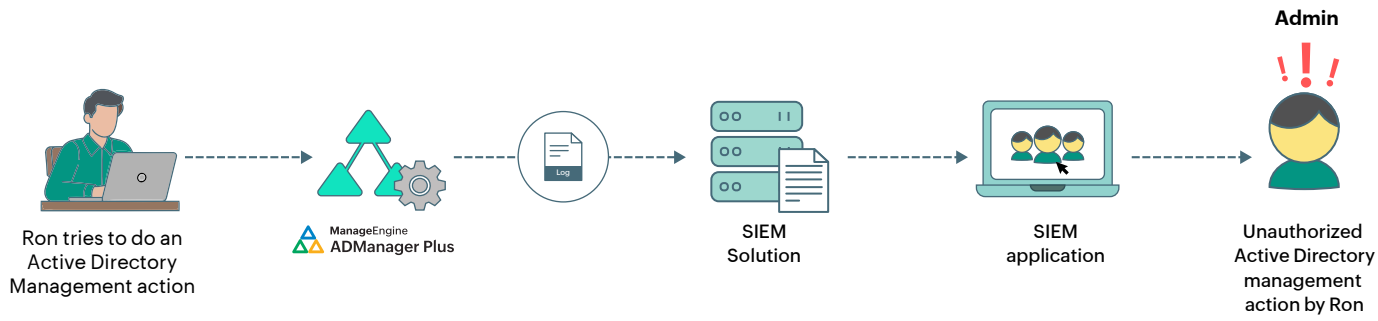
6.1 Integration with HCM applications

ADManager Plus integrates with HCM applications using secure API-based connectors that authenticate using supported mechanisms such as API keys, OAuth tokens, or service accounts, depending on the HCM platform. Retrieved identity data is validated and mapped to predefined templates and policies within ADManager Plus. Synchronization jobs can be triggered on a schedule or on demand and may optionally pass through approval workflows before execution. All authentication events, data transformations, and execution outcomes are recorded in the product database to ensure traceability and audit compliance.



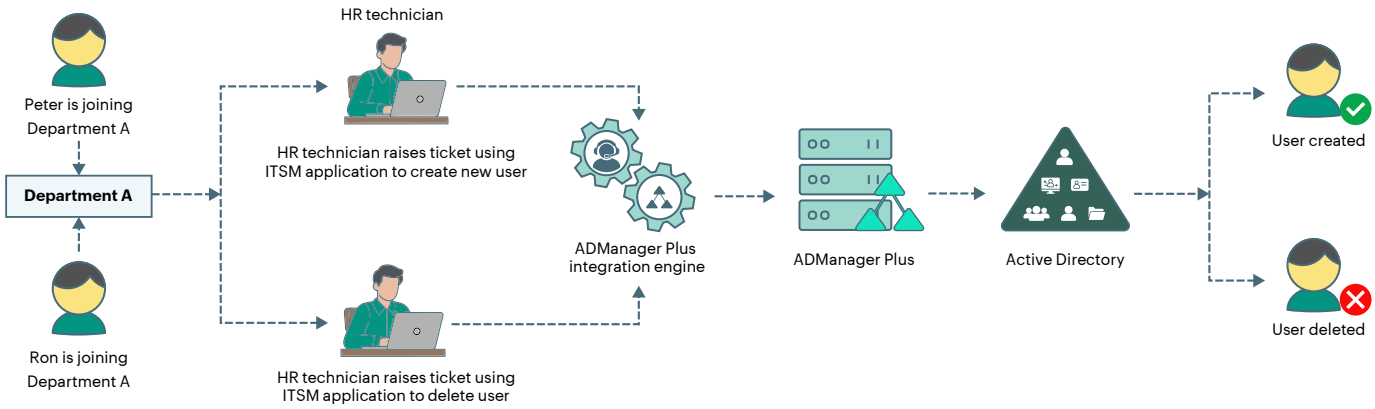
6.2 Integration with SIEM applications

ADManager Plus integrates with SIEM platforms by securely exporting audit logs and management activity events generated during directory and cloud operations. Log transmission is authenticated using supported mechanisms such as token-based authentication or secure log forwarding channels. Events are transmitted post-execution, ensuring only completed actions are reported. SIEM systems apply correlation rules and thresholds on the received data to detect anomalies, security incidents, and policy violations, enabling centralized monitoring and incident response.



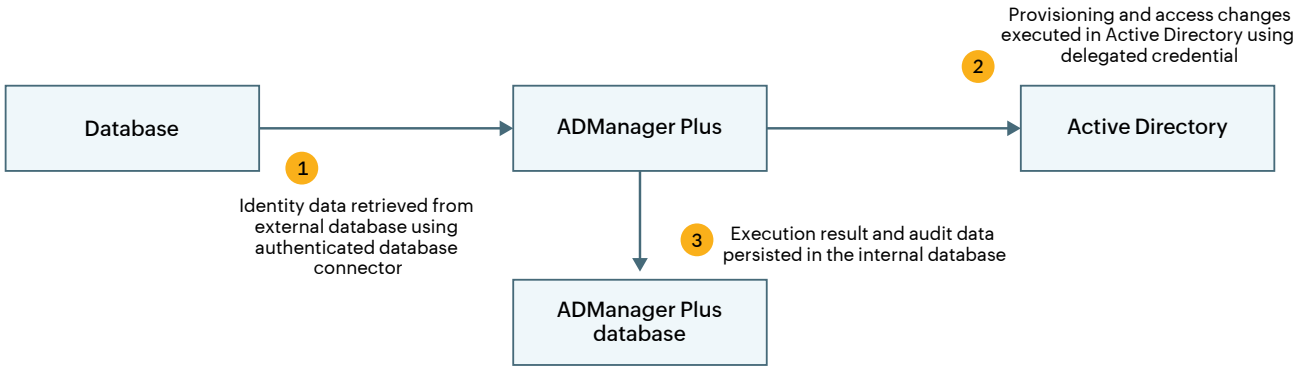
6.3 Integration with ITSM and help desk applications

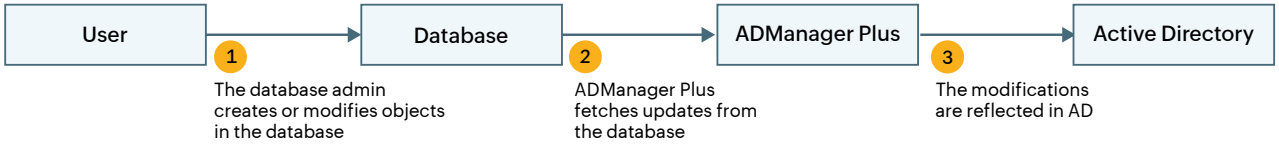
ADManager Plus integrates with ITSM and help desk systems using REST APIs secured by API keys, OAuth tokens, or service credentials. The system periodically retrieves identity-related tickets through authenticated API calls and validates requested actions against role-based access controls and optional workflows. Upon execution, ADManager Plus updates the ticket status with execution results and can optionally automate ticket closure. All authentication checks, authorization decisions, and execution responses are logged to maintain consistency and accountability between ITSM and identity platforms.



6.4 Integration with databases

ADManager Plus integrates with relational databases such as Microsoft SQL Server and Oracle using authenticated database connections based on service accounts or database credentials. Identity data is extracted through scheduled or on-demand queries, transformed according to configured mappings, and synchronized with AD and other managed systems. Updated identity state information can be written back to the database using the same authenticated connection, ensuring data consistency while maintaining auditability of access and changes.





7. 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.

8. 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.

9. 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.

10. 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

11. 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.

12. 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.

Related resources:

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