ManageEngine
AD360

AD360

Quick start guide

www.manageengine.com/active-directory-360/

Index

Overview

AD360 is an integrated solution that helps organizations simplify IAM and IT compliance challenges in Windows Active Directory, Microsoft 365, Exchange Servers, and cloud applications. AD360 provides all the features that you need to easily manage, audit, secure, and report on your entire Windows-based IT infrastructure and cloud applications.

There are seven different components that you can integrate with AD360, each of which provides a unique set of features. You can choose the components you want based on your business requirements and integrate them with AD360. Refer here for the list of components that you can integrate with AD360.

This document explains how to successfully deploy and configure the important settings of AD360 and its components.

Deployment

System requirements

Hardware		Recommended
Processor		3GHz or faster
Screen resolution		1,024x768 pixels or higher
RAM	AD360	4GB **Note:** Based on the components that you integrate with AD360, you will have to allocate additional RAM for the product to run at optimal efficiency. Please check the following rows for the additional RAM required by each individual component. If you plan on integrating more than two components with AD360, we recommend you install no more than two components on a single machine.
	ADManager Plus	6GB (8GB if it is a virtual machine)
	ADAudit Plus	16GB

	ADSelfService Plus	16GB
	Exchange Reporter Plus	16GB
	M365 Manager Plus	16GB
	RecoveryManager Plus	16GB
	SharePoint Manager Plus	8GB (16GB if it is a virtual machine)
Disk space	AD360	10GB minimum **Note:** Based on the components that you integrate with AD360, you will have to ensure additional disk space. Please refer to the following rows for the recommended disk space required by each component.
	ADManager Plus	50GB **Note:** Based on the number of scheduled reports and automations running in parallel, additional disk space might be necessary.
	ADAudit Plus	100GB **Note:** Based on the number of users and audit events captured, additional disk space might be necessary.
	ADSelfService Plus	200GB (SSD preferred)
	Exchange Reporter Plus	200GB (SSD preferred) **Note:** Based on your organization's size, mailbox size, traffic volume, and Outlook Web Access logins, additional disk space might be necessary.
	M365 Manager Plus	500GB (SSD preferred) **Note:** Based on your tenant size, mailbox size, and traffic volume, additional disk space might be necessary.

	RecoveryManager Plus	**Active Directory and Entra ID backups:** This requirement varies based on the number of AD objects, Entra ID objects, the size of your Domain Controller, and the retention period set for your backups. RecoveryManager Plus typically compresses backups to a third of their original size. It has a best case compression ratio of 2:1 for Domain Controller backups. **Microsoft 365, Google Workspace, Exchange, and Zoho WorkDrive backups:** This requirement varies based on the number of backed-up Exchange (on-premises and online) mailboxes, the size of your SharePoint Online and OneDrive for Business sites, and Zoho WorkDrive files, and the retention period that you set for your backups. If the total size of these is 1TB, make sure that you have 1TB of free disk space to store the full backup and all subsequent incremental backups.
	SharePoint Manager Plus	50GB

***Note:**

RAM and disk space requirements could vary based on the components you've integrated with AD360.

Supported platforms

ManageEngine AD360 supports the following Microsoft Windows operating system versions:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 11
- Windows 10
- Windows 8
- Windows 7

Supported browsers

AD360 requires one of the following browsers to be installed in the system:

- Microsoft Edge (all versions)
- Mozilla Firefox 4 and above
- Google Chrome 10 and above

Supported databases

AD360 supports the following databases:

- PostgreSQL (the default database bundled with the product)
- Microsoft SQL Server

For a detailed list of requirements, please refer to our system and port requirements guide.

Installation

ManageEngine AD360 can be installed on any machine in the domain that satisfies the recommended system requirements.
You can install AD360 as:

- An application
- A Windows service

Note:
Ensure that you have the necessary privileges and rights to install and run the product. If you are using Windows Vista or an older operating system, disable User Account Control and then proceed with the installation. For more information, click here.

Installing AD360 as an application

1. By default, AD360 will be installed as an application.
2. Click here to download the executable file from the website.
3. Double-click the ManageEngine_AD360.exe download file to start the installation.
4. Follow the instructions on the install shield wizard to complete the installation of AD360.

You can choose from three modes of installation: **Standard, Minimal**, and **Custom.**

- **Standard installation:** Downloads and installs all the components along with AD360. This installation mode is highly recommended, as it installs AD360 along with all the components necessary for comprehensive identity management and ensures IT security and compliance.

- **Minimal installation:** Installs AD360 alone. You can opt for this installation mode if you are already running the components you need. To integrate the components with AD360, follow the steps listed here.

- **Custom installation:** You can use this installation mode to pick and install only the components you want along with AD360.

The application's web console can be launched by double-clicking the AD360' shortcut icon on the desktop. When opened as an application, AD360 runs with the privileges of the user who installed the application.

Installing AD360 as a Windows service

To install AD360 as a service:

1. Install **AD360** as an application.
2. Go to **Start Menu > All Programs.**
3. Select **AD360** and click **Install AD360 as Service.**

Alternatively, you can also install AD360 as a service from the notification tray.

1. Install **AD360** as an application.
2. Click the **Notification icon** [🔔] at the top-right corner of the screen.
3. Select the **AD360 is not installed as a service** alert, and the click **Install**. This will initiate AD360 service installation in the background.

Once the AD360 service is installed, you can start the product as a Windows service. When started as a service, AD360 runs with the privileges of the system account or the service account (if configured).

Uninstalling AD360

To uninstall AD360, select **Start Menu > All Programs > AD360 > Uninstall AD360.**

Working with AD360

Starting AD360

AD360 can be started either using the system account (when run as service) or user account (when run as an application). Starting AD360 will also start the integrated components automatically.
On starting AD360, the client is automatically launched in the default browser.

Launching the AD360 client

To launch the AD360 client:

1. Open any of the supported web browsers and type **http://<hostname>:8082** in the address bar where *<hostname>* refers to the DNS name of the machine in which AD360 is installed.
2. Specify the user name and password as admin (for first time users) in the respective fields and click Login. You can change this default password by navigating to **Admin > General Settings > Personalize > Change Password.**

Stopping AD360

To stop AD360, select **Start > Programs > AD360 > Stop AD360.**
You can enable the single shutdown option so that all the individual components will also be shut down when AD360 is stopped. To enable this setting:

- Navigate to **Admin > General Settings > Product Settings.**
- Under the General section, select **Enable Single Shutdown.**

Integrating the components

AD360 contains seven components, each providing a rich but unique set of features. These components are:

1. ADManager Plus: Provides management, reporting, automation, delegation, and workflow capabilities for Active Directory, Microsoft 365, Exchange, and Google Workspace.
2. ADAudit Plus: Performs real-time change auditing, alerting, and compliance management for Active Directory, Azure Active Directory, and file servers.
3. ADSelfService Plus: Provides MFA, password self-service, and single sign-on capabilities.
4. Exchange Reporter Plus: Provides reporting, auditing, and monitoring capabilities for Exchange Servers and Exchange Online along with reporting capabilities for Skype for Business Server.
5. M365 Manager Plus: Provides management, reporting, automation, delegation, auditing, and alerting capabilities for Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services.
6. RecoveryManager Plus: Takes care of backup and recovery of Active Directory, Azure Active Directory, Exchange Online, SharePoint Online, OneDrive for Business, Google Workspace, on-premises Exchange, and Zoho WorkDrive.
7. SharePoint Manager Plus: Helps you manage, audit, and report on both on-premises and Microsoft 365 SharePoint environments.

To effectively tackle all your Identity management and IT security challenges, these seven components have to be integrated with AD360. To integrate these components, follow the steps given below.

Note:

If you've chosen the standard installation method, the components will be automatically installed and integrated with AD360. For other modes of installation, please follow the below steps to download, install, and integrate the components.

Step 1: Download and install the components

Note:

If you already have the components installed and running, please update the components to their latest build and proceed with Step 2.

1. Download the components either from the link available under the dashboard of each component or from the AD360 website.
2. Install the components one-by-one by double-clicking the downloaded EXE files and following the instructions of the install shield wizard.
3. Once the installation is complete, start the components by double-clicking the desktop shortcut icons of the respective components.

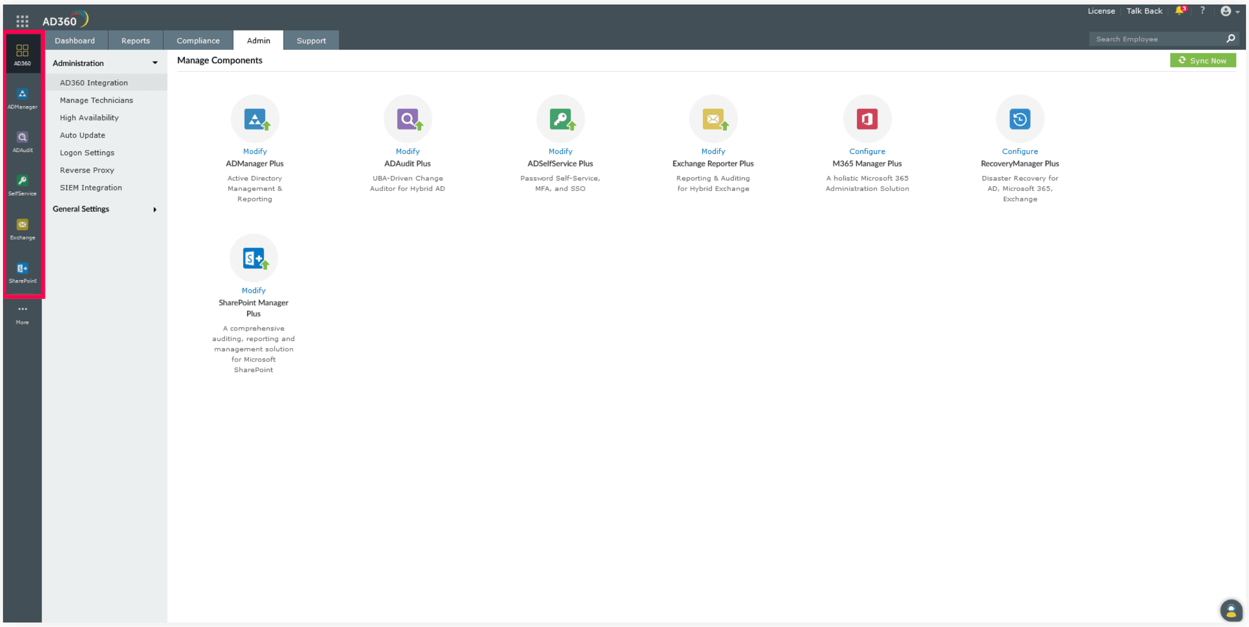
Step 2: Integrate the components

Note:
Make sure that all the components that are to be integrated with AD360 are running before proceeding with the steps given below.

1. Go to **Admin** > **Administration** > **AD360 Integration.** From this page, you can integrate the components you need.
2. Click on any tab (say ADManager Plus).
3. Enter the **Server Name** or **IP** and **Port Number** of the server in which that particular component is running.
4. Select the connection **Protocol** from the drop-down menu.
5. Click **Integrate Now.**
6. Repeat steps 3-5 for the remaining components under the respective tabs.

Accessing the individual components

Once you're logged in to AD360, you will be presented with the dashboards of the individual components you've integrated.
You can access the individual components using the applications panel on the left-hand side of the screen.



Setting up individual components

Synchronizing settings between the components

The domain settings, component integration, mail server, proxy server, and other similar configurations will be automatically synchronized across each component. This saves a lot of time as you don't have to configure the same settings across all the integrated components. Any changes you make in one of the components will be automatically reflected in the other components, too.

To synchronize the settings between AD360 and the individual components:

1. Navigate to **Admin > Administration > AD360 Integration.**
2. Click **Sync Now.**

Domain settings

A domain can be added only in the individual components and the details added in one component will be synchronized with all other connected components. Also, if there is a change in the administrator credentials that was used in configuring a domain with a component, simply update the change in one component and it will be synchronized across all the other components.

Integration settings

The different components of AD360 communicate with each other for various purposes like single sign-on, domain configuration updates, etc. Any change to the hostname and port number of a component must be reflected in the other components' settings to facilitate uninterrupted communication. But with the AD360, there is no need to make the changes in all the components manually. Simply update these changes in the AD360 integration settings page and the changes will be automatically synchronized across all the components.

Privileges required

Refer to this guide for more information on the permissions and privileges required by AD360 and the individual components.

ADManager Plus

Domain configuration

During start-up, ADManager Plus adds all the domains that could be discovered. If you wish to manually add more domains or modify the added domains, follow the steps below.

To add more domains:

1. Click the **Domain Settings** link from the top-right corner of the client.
2. The domains that are already added are listed here. Click **Add new domain.**
3. Specify the **Domain Name.**
4. Click on the **Discover** link to locate the domain controllers from the DNS and add them automatically. You can also add all the domain controllers manually. The domain controller that appears first in the list is considered as the primary domain controller. Use the up and down arrows to reorder the domain controllers.
5. Specify the authentication details of a user with administrator privileges. You can also refer to this guide to learn about the granular permissions needed.
6. Click **Add** to add the domain.

You can perform the following actions from the *Add Domain Details* section:

1. **Changing the default domain:** The domain that is first discovered is considered as default domain. The default domain is shown in bold letters. Delegating security roles can only be done to the security principals of the default domain. If you wish to change the default domain, click the ▦ icon in the Actions column to make it default.
2. **Modifying a domain:** To modify the domain details, click the ✎ icon, change the required values, and click **Save.**
3. **Deleting a domain:** To delete a domain, click the 🗑 icon.
4. **Refreshing the domain details:** To synchronize the object details with Active Directory, click the ⟳ icon.

Microsoft 365 tenant configuration

1. Click the **Admin** tab.
2. Under System Settings, select **Microsoft 365/Google Workspace.**

   Note: Ensure that the MSOnline PowerShell module for Azure Active Directory is installed on the same machine where ADManager Plus is installed. Click here for help regarding installation of the Azure AD module.
3. Click the **Microsoft 365** tab.
4. Enter the **User Name** and **Password** of the Microsoft 365 Global Administrator account or an account that has the appropriate privileges to create new accounts.
5. Select the **domains** for which the Microsoft 365 option should be provided.
6. Click **Save.**

Google Workspace domain configuration

1. Click the **Admin** tab.
2. Under System Settings, select **Microsoft 365/Google Workspace.**
3. Click the **Google Workspace** tab.
4. Enter the **User Name** of the Google Workspace administrative account and the **Service Account Email.**
5. Add the relevant **P12 Key File Path**. Click here for the steps to create a service account email and the P12 file, and also to grant domain-wide authority to the new service account.
6. Select the **domains** for which the Google Workspace option should be provided.
7. Click **Save.**

ADAudit Plus

Domain configuration

Please follow the domain configuration steps listed under ADManager Plus to add a domain in ADAudit Plus.

ADSelfService Plus

Domain configuration

Please follow the domain configuration steps listed under ADManager Plus to add a domain in ADSelfService Plus.

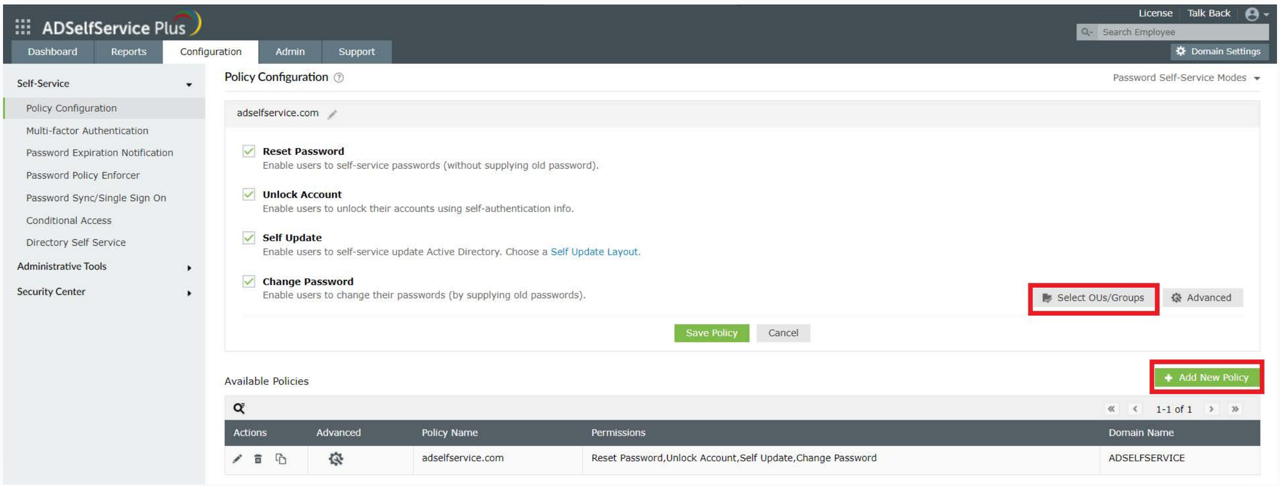
Policy configuration

ADSelfService Plus offers a multitude of self-service features to domain users, including:

- Self-service password reset
- Self-service account unlock
- Directory self-update
- Password change from a web-based portal

As an administrator, you can decide whether users of a domain or selected OUs can avail themselves of any or all of these functions. In other words, you set a self-service policy for the users and define what features they can use in ADSelfService Plus.

From the **Policy Configuration** section, you can define, edit, or delete policies.
By default, when ADSelfService Plus discovers DCs of a domain, it sets a policy for the entire domain. When you log in for the first time as an administrator, this default policy will be shown to you. By default, every self-service feature is selected in the default policy.



Policy Configuration

adselfservice.com

☑ **Reset Password**
Enable users to self-service passwords (without supplying old password).

☑ **Unlock Account**
Enable users to unlock their accounts using self-authentication info.

☑ **Self Update**
Enable users to self-service update Active Directory. Choose a Self Update Layout.

☑ **Change Password**
Enable users to change their passwords (by supplying old passwords).

Actions	Advanced	Policy Name	Permissions	Domain Name
		adselfservice.com	Reset Password,Unlock Account,Self Update,Change Password	ADSELFSERVICE

If it fits your requirement, you can retain it; otherwise, you can edit this default policy by following the steps listed below.

1. Click on the **Configuration** tab.
2. Enter a **Policy Name** in the text box provided.
3. Select the self-service features that you wish to enable for the users.
4. Click **Select OUs/Groups** and select the OUs and groups that you want to be governed by this policy.
5. Click **OK** and then **Save.**

This will allow users in the selected OUs to enjoy the self-service features that are selected in the policy.

Note:

ADSelfService Plus allows you to define any number of self-service policies in a given domain. If more than one policy is applied to an OU or group, then the policy with the highest priority will take effect.

Exchange Reporter Plus

Organization configuration

To gather data from your Exchange Organization you will need to add that Exchange Organization to Exchange Reporter Plus.

If you provide the appropriate credentials during installation, the Exchange Organization will be added automatically to Exchange Reporter Plus. You can also manually add a new Exchange Organization and modify, delete, or choose an existing Exchange Organization as the default from the **Organization Settings** option.

Configuring Exchange Server in Exchange Reporter Plus

1. Click the **Org/Tenant Settings** button at the top-right corner of the screen.
2. Under the **Exchange Server** tab, click **Add New Organization.**
3. Enter the name of the **Global Catalog Server.**

   Note:

   If the Exchange Server is within your forest, the Exchange Organization will be added automatically.
4. Enter the **User Name** and **Password** of a user account that has appropriate privileges.
5. Click **Save.**

Configuring the Exchange Online tenant in Exchange Reporter Plus

1. Click the **Org/Tenant Settings** button at the top-right corner of the screen.
2. Under the *Exchange Online* tab, click **Add New Tenant.**
3. Enter the **Account Nam**e and **Password** of a user account that has appropriate privileges.
4. Click **Save.**

Configuring Skype for Business Server in Exchange Reporter Plust

1. Click the **Org/Tenant Settings** button at the top-right corner of the screen.
2. Under the Skype Server tab, click **Add New Forest.**
3. Enter the name of the **Global Catalog Server.**

   Note:

   If the Skype for Business Server is within your forest, the Global Catalog Server name will be updated automatically.
5. Enter the **User Name** and **Password** of a user account that has appropriate privileges.
6. Click **Save.**

Making an Exchange Organization, Tenant, or Skype Server the default

Any Exchange Organization can be set as the default by clicking on the ☰✓ icon next to the corresponding Exchange Organization. The same applies for a Microsoft 365 tenant and Skype for Business Server.

By design, the product dashboard shows reports, home graphs, and schedule creation options for the server or tenant selected as the default.

M365 Manager Plus

Configuring Microsoft 365 tenants

1. Click the **Tenant Settings** option found in the top-right corner.
2. Click the **Add New Tenant** button in the top-right corner of the *M365 Tenant Settings* page.
3. Enter the **Account Name** of the Microsoft 365 tenant.
4. In the Password field, enter the **password** of the Microsoft 365 tenant. If you are adding an MFA-enabled Microsoft 365 or federated account, generate the app password in the *Microsoft 365 portal*, and enter it in the *Password* field.

   Note:

   We recommend using a Microsoft 365 service account to configure Microsoft 365 tenants in M365 Manager Plus. The service account must have the **Global Admin** role or should have the appropriate privileges.
5. Click **Save** to add the tenant.

   Note:

   If you are using an MFA-enabled account, federated account, or 32-bit version of M365 Manager Plus, please contact support@m365managerplus.com to set up the Azure Active Directory module to collect data.

Modifying an existing Microsoft 365 tenant

You can edit or delete the details of any existing Microsoft 365 tenant.
To edit an existing tenant, click the ✎ icon located in the **Actions** column of the desired tenant.
To delete a Microsoft 365 tenant, click the 🗑 icon located in the **Actions** column of the desired tenant.

Making an existing Microsoft 365 tenant the default tenant

1. If a specific Microsoft 365 tenant is set as the default, then it will be the default tenant across all the tabs of the product.
2. To make an Microsoft 365 tenant the default tenant, click the ☑ icon located in the Actions column of the desired tenant.

Permissions required

While configuring Microsoft 365 tenants, use the credentials of an administrator who is a member of the Microsoft 365 global admin role.

RecoveryManager Plus

Domain configuration

1. Click the **Account Configuration** button located at the top-right corner of the screen.
2. Select the **On-premises AD** tab.
3. Click the **Add New Domain** option located at the top-right corner of the screen.
4. Enter the name of the domain.
5. Click the **Discover DCs** link to automatically detect the domain controllers in the specified domain. You can also add the domain controller manually by clicking **Add** and providing the name of the DC.
6. If you want the product to automatically connect to the secondary DC and start gathering changes from the AD database if the primary DC fails, select the **Enable auto-switch on DC failure** option.

   Note:

   This option is not recommended if your AD environment has more than 5,000 user objects. RecoveryManager Plus incrementally backs up changes made to objects and their attributes using DirSync. After each backup, the product stores a cookie that identifies the directory state at the time of the previous DirSync search in the domain controller. When the domain controller is changed, the cookies used to identify changes will not be available in the secondary domain controller. This means all objects from the domain will be identified and checked with backed-up data for any changes and the process will take as much time as a full backup to complete.
7. Enter the **Username** and **Password** of a domain administrator.
8. Click **Add** to add the domain details in the product.

Microsoft 365 tenant configuration

1. Click the **Account Configuration** button located at the top-right corner of the screen.
2. Select the **Office 365 Tenant** tab.
3. Enter the **Account Name** and **Password** of the Microsoft 365 tenant. Use the credentials of an administrator with the global admin role. The account name should be entered in the *account@company.onmicrosoft.com* format.
4. You can also use a service account that is a member of the Microsoft 365 global admin role to configure your tenant with RecoveryManager Plus.

   Note:

   If multi-factor authentication is enabled for the account used, provide the **app password** in the Password field.
5. If you use Modern Authentication in your Microsoft 365 environment and Legacy Authentication is disabled, you'll need the client ID and client secret to configure your Microsoft 365 account. To get your client ID and client secret, follow these steps.

Note:

If you want to back up your Azure AD using RecoveryManager Plus, select **Modern Authentication** and provide the **client ID** and **secret.**

6. Choose the Microsoft 365 environment in which the tenant was created from the drop-down box.
7. Click **Save** to add the tenant.

Google Workspace domain configuration

1. Click the Account Configuration button located at the top-right corner of the screen.
2. Select the Google Workspace tab.
3. Select the type of account that you wish to add to RecoveryManager Plus.
   a. Personal account: Selecting this option will allow you to add a personal Google account to RecoveryManager Plus.
   b. Workspace account: Selecting this option will allow you to add a Google Workspace account to RecoveryManager Plus. Once added, you can configure a backup schedule for all users in the workspace.

a. Adding a personal Google account
   i. Enter the email address of the user.
   ii. In the *Credentials JSON* field, click the **Browse** button and select the appropriate **file.** Learn how to create a Credentials JSON.
   iii. Click **Configure** to add the user account to RecoveryManager Plus.
   iv. In the page that appears, allow RecoveryManager Plus to access the following information and click **Allow.**
      1. Read, compose, send, and permanently delete all your email from Gmail.
      2. See, edit, create, and delete all of your Google Drive files.
      3. See, edit, download, and permanently delete your contacts.
      4. See, edit, share, and permanently delete all the calendars you can access using Google Calendar.

b. Adding a Workspace account
   i. Enter the email address of the administrator.
   ii. Provide the **Service Account ID.**
   iii. In the *Service Key* field, click the **Browse** button and select the appropriate file. Learn how to create a service account and to generate the service key.
   iv. Click **Configure** to add the Workspace to RecoveryManager Plus.

Exchange Server organization configuration

1. Click the **Account Configuration** button located at the top-right corner of the screen.
2. Select the **On-premises Exchange** tab.
3. Select the **Server Type** from the available options: Global Catalog and Exchange Server.
4. Provide the **Server Name**.
5. Enter the **User Name** and **Password** of a user who is a member of the **Organization Management role group.** The user name should be entered in the *Domain\username* format.
6. If your server is an Exchange Server, you'll have the option to **Enable SSL.**
7. The user account used to configure the Exchange organization must have appropriate impersonation rights to back up and restore Exchange mailboxes. Select **Grant Impersonation** to provide the account with this privilege.

   Note:

   If this option is not selected, you can only back up and restore the mailbox of the user whose email address has been used to configure the Exchange organization.
8. Click **Save.**

SharePoint Manager Plus

SharePoint on-premises farm server configuration

Note:

Ensure you satisfy the prerequisites before adding your farm server to SharePoint Manager Plus.

1. Navigate to **Admin** tab **> Configuration > Farm Server.**
2. Click on the **Add server** button located in the top-right corner of the screen.
3. In the New Farm Details dialog box, provide the **Fully Qualified Domain Name** of the server to be added. (Preferably any one of the WFE servers or the server machine where Central web administration is available)
4. Specify the farm admin credential to add the farm server.

Microsoft 365 tenant configuration

1. Navigate to **Admin** tab **> Configuration > Farm Server.**
2. Click on the **Add server** button located in the top-right corner of the screen.
3. In the **New Farm Details** dialog box, click on the **Add Office 365** link.
4. Select the authentication type from the available choices:

a. Default: Use this method if conditional access is not enabled for the Office 365 administrator account
b. Azure Application: Use this method if MFA or conditional access is enabled for the Office 365 administrator account.

a. Default authentication:

i. Provide the **Admin Tenant URL**. To find your admin tenant URL, follow the steps listed here.
ii. Specify the credentials of an Office 365 administrator. If MFA is enabled for the administrator account, follow the steps listed here to generate an app password.

b. Azure Application:

i. Follow the steps listed here to create an Azure application manually.
ii. Specify the credentials of an Office 365 administrator.
iii. Provide the **Application ID, Secret key,** complete location of the generated **PFX certificate file,** and **certificate password** to configure the tenant.

High availability

High availability refers to a system or component that aims to ensure an agreed level of operational performance for a higher-than-normal period. AD360 helps administrators maintain high availability even in the case of failure of the primary server.
For more instructions on enabling high availability, refer this guide.

Reverse proxy

You can make AD360 act as a reverse proxy server for the products that you've integrated with it. AD360 lets you enable a context-based reverse proxy, a port-based reverse proxy, or both.
For more information, refer this guide.

Enabling SSL

Navigate to **Admin → General Settings → SSL Certification Tool.**
If you don't have a SSL certificate, select the Generate Certificate option and follow the steps here.
If you already have a SSL certificate, select the Apply Certificate option and follow the steps here.

Apply Certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

- In the *Apply Certificate* to drop-down, select the component for which you want to apply the SSL certificate.
- Choose an Upload Option based on the certificate file type.
  - **ZIP upload:**
    1. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.
    2. If your CA has sent you individual certificate files—user, intermediary, and root certificates, then you can put all these certificate files in a ZIP file and upload it.

  - **Individual Certificates:**
    1. If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.
    2. If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.

  - **Certificate Content:**
    1. If your CA has sent just the certificate content, then choose Certificate Content option, and paste the entire content.

- If the certificate file requires a password, then enter it in the *Certificate* Password field. Or, if the certificate contains a password-protected private key, enter the password in the Private Key Passphrase field.

Note: Only Triple DES encrypted private keys are currently supported.

- Click **Apply.**
- Finally, restart AD360 and its components.

Generate Certificate

- In the **Common Name field**, enter the name of the server.
  Example: For the URL **https://servername:9251**, the common name is **servername.**
- In the *Organizational Unit* field, enter the department's name which you want to be displayed in the certificate.
- In the *Organization* field, enter the legal name of your organization.
- In the *City* field, enter the name of the city as provided in your organization's registered address.
- In the *State/Province* field, enter the name of the state or province as provided in your organization's registered address.

- In the *Country Code* field, enter the two letter code of the country where your organization is located.
- In the *Password* field, enter a password that consists of at least 6 characters to secure the keystore.
- In the *Validity (In Days)* field, specify the number of days for which the SSL certificate will be considered valid.

Note: When no value is entered, the certificate will be considered to be valid for 90 days.

- In the *Public Key Length (In Bits)* field, specify the size of the public key.

Note: The default value is 2048 bits and its value can only be incremented in multiples of 64.

- After all values have been entered, you can select either of these two options:
    - **Generate CSR**

      This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.

      1. Click **Download CSR** or manually get it by going to the **<Install_dir>\Certificates** folder.
      2. Once you have received the certificate files from your CA, follow the steps listed under Apply Certificate to apply the SSL certificate.

    - **Apply Self-signed Certificate**

      This option allows you to create a self-signed certificate and apply it instantly in the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning telling them that the website is not trusted, which may cause concern.

      If you want to go ahead and apply the self-signed certificate, follow the steps given below:

      1. Click **Apply Self-Signed Certificate.**
      2. You'll be taken directly to step 3.
      3. Here, **select the components** in which you want to apply the self-signed certificate from *Apply certificate* to drop-down box.
      4. Once you get the message that SSL certificate has been successfully applied, **restart the components** for the changes to take effect.

Database migration

For AD360

In AD360, you can change the built-in database server (PostgreSQL) to MS SQL Server or another instance of a PostgreSQL server.

Supported database migrations

- PostgreSQL server to MS SQL Server or another instance of PostgreSQL server.
- MS SQL Server to PostgreSQL server or another instance of MS SQL Server.

Supported database versions

- PostgreSQL: 9.2 to 9.5
- MS SQL: 2005 and above

  Note: Take a backup of the database before you proceed.

Prerequisites

For MS SQL database

- Copy the **bcp.exe** and **bcp.rll** files from the directory in which the SQL Server is installed and paste them in the AD360 bin folder (<AD360_installed_directory/bin).
  - Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\bcp.exe.
  - Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\Resources\1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\Resources\1033\bcp.rll\
- For migration to MS SQL, please install the corresponding SQL Native Client in the AD360 machine as per the MS SQL Server version.

MS SQL Server version	Native client
2005	Download
2008	Download
2008 R2	Download
2012	Download
2014	Download
2016	Download
2017	Download
2019	Download

- If a firewall is enabled in the MS SQL Server machine, the TCP and UDP ports must be opened.

For External pgSQL database

- In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for **wal_level** entry. Uncomment the entry and change its value to **archive.**
- Copy all the files in the *<postgresql_installdir>/lib and <postgresql_installdir>/bin* folders, and paste them in the *<product_home>/pgsql/lib and <product_home>/pgsql/bin* folders respectively. <product_home> refers to the home directory of AD360 or the integrated products for which you're configuring the auto backup scheduler.
- Restart the external PostgreSQL server.
- Repeat the above steps whenever you update the PostgreSQL server.

Steps to migrate a database

1. Log in to **AD360** as an administrator.
2. Navigate to **Admin > General Settings > Database Settings > Database Configuration.**
3. Select **AD360** under Component Name.
4. From the *Select Database Server* menu, select the **database server** that you want to change to.
5. If you select PostgreSQL server, then:
    a. In the *DB Server Name/IP* and *Port* fields, enter the **host name** or **IP address** and the **port number** of the PostgreSQL database server.
    b. Enter the **Username** and **Password** of a user who has permission to create a new database.
6. If you select MS SQL Server, then:
    a. In the DB Server Name/IP and Port fields, enter the **host name** or **IP address** and the **port number** of the MS SQL database server.
    b. In the *DB Server Instance* field, select the **SQL Server instance** you want to use.
    c. For *Authentication*, you can either use Windows credentials or a SQL Server user account.
    d. If you want to use a SQL Server user account, select **SQL Authentication** and enter the **Username** and **Password.**
    e. If you want to use **Windows Authentication**, select Windows Authentication, and enter the **username** and **password** of a Windows domain user account. To autofill the username and password of the user currently logged in to the machine, check the **box** next to *Use Default Windows Authentication.*

    Note:

    - The user account used must have permission to create a database in the selected MS SQL Server.
    - The bcp.exe and bcp.rll files must be manually moved to the AD360 bin folder as mentioned in the Prerequisites section.
7. Check the **box** next to *Migrate Existing Data* to copy the data from your old database to the new database.

    Important: Leave this box unchecked only if you want to change the database of a fresh installation of AD360 or its components.
8. Click **Configure.**

Auto backup

AD360 can automatically back up its database and the databases used in the integrated components at regular intervals according to the schedule you choose. Using this option, you can back up the built-in PostgreSQL DB or external PostgreSQL and MS SQL databases configured in the product.

Supported DB versions for auto backup:

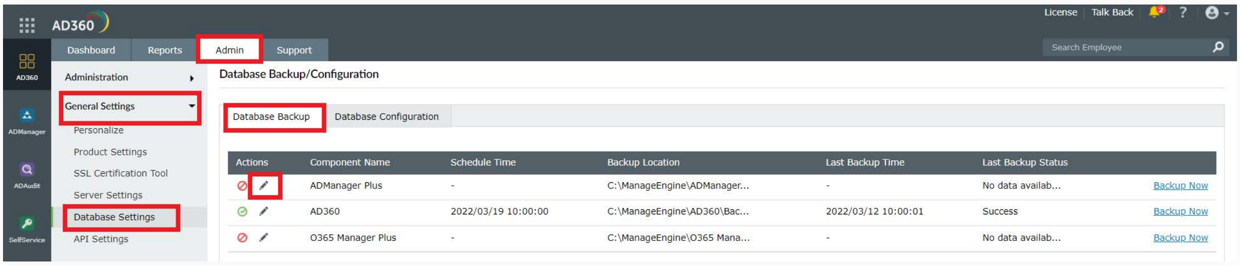
- PostgreSQL: Version 9.2 to 9.5
- MS SQL: Version 2008 and above

Prerequisite for backing up external PostgreSQL

- In the machine where PostgreSQL is installed, go to **<postgresql_installdir>/data** and open the **posgresql.conf** file. Search for **wal_level** entry. Uncomment the entry and change its value to **archive.**
- Copy all the files in the *<postgresql_installdir>/lib* and *<postgresql_installdir>/bin* folders and paste them in the *<product_home>/pgsql/lib* and *<product_home>/pgsql/bin* folders respectively. Here, <product_home> refers to the home directory of AD360 or the integrated products for which you're configuring the auto backup scheduler.
- Restart the external **PostgreSQL server.**
- Repeat the above steps whenever you update the PostgreSQL server.

Steps to schedule database backup

1. Navigate to **Admin > General Settings > Database Settings > Database Backup.**
2. Choose AD360 or an integrated product for which you want to schedule auto backup, and click the ✎ icon.



Database Backup/Configuration

Actions	Component Name	Schedule Time	Backup Location	Last Backup Time	Last Backup Status	
⊘ ✎	ADManager Plus	-	C:\ManageEngine\ADManager...	-	No data availab...	Backup Now
✓ ✎	AD360	2022/03/19 10:00:00	C:\ManageEngine\AD360\Bac...	2022/03/12 10:00:01	Success	Backup Now
⊘ ✎	O365 Manager Plus	-	C:\ManageEngine\O365 Mana...	-	No data availab...	Backup Now

3. Select whether you want to schedule the backup daily, weekly, or monthly and at what time from the *Backup Frequency* drop-down.
4. Enter the **number** of incremental backups to take for every full backup in the *Full Backup after __ incremental backups* box. Enter **0** if you want to take only full backups.

5. Enter the **Backup Storage Path.**
   a. You can either choose a local folder or shared folder to store the backups.
   b. If the shared folder you've chosen needs permission to store the backups, then check the **box** next to *Authentication Required,* and enter the **necessary credentials.**

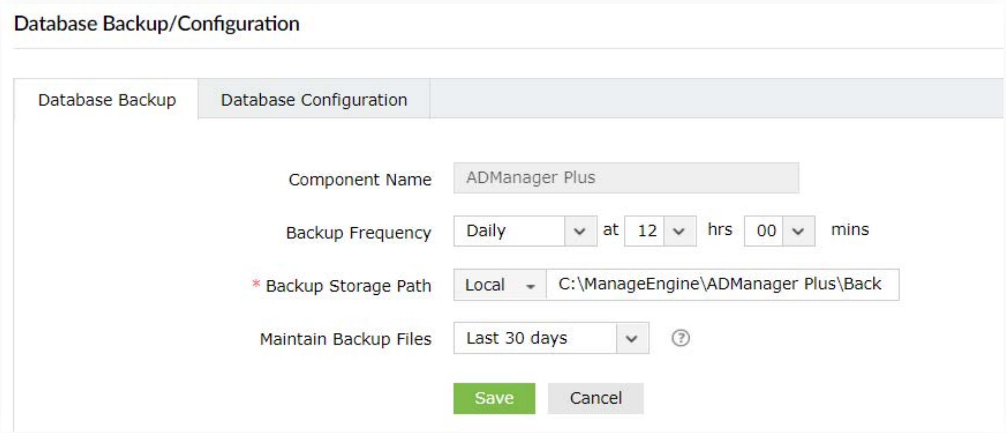
   Note 1:

   If the shared folder is located in a workgroup computer, then create a new domain account in AD. This new account should have the same username and password as that of a local account in the workgroup computer. Use the credentials of this new account for authentication.

   Note 2:

   If the specified path is wrong or unreachable, the backup will be stored in the default backup folder (<Installation_Folder\Backup>).

6. Set a **retention period** for the backup files from the *Maintain Backup Files* drop-down.



Database Backup/Configuration

Component Name: ADManager Plus

Backup Frequency: Daily at 12 hrs 00 mins

* Backup Storage Path: Local C:\ManageEngine\ADManager Plus\Back

Maintain Backup Files: Last 30 days

7. Click **Save.**

Other settings

1. To disable auto backup for AD360 or a particular integrated product, click the 🗑 icon located in the Actions column of the auto backup configuration table.
2. To get the status of the latest backup, click the ⟳ icon.
3. To edit the backup schedule for a particular component, click the ✎ icon located in the Actions column of the component.
4. Use the **Backup Now** option to initiate a backup instantly.
5. Click the 🗒 icon in the status column to view all available backups.

Restoring backups from an old version of MS SQL Server to a new MS SQL Server

If you've installed a new version of MS SQL Server and want to configure it in AD360 or in its integrated components in place of the old MS SQL Server, you can use the backup you've taken using AD360. Just note that, besides the backup you've taken using AD360, you need to copy the files in <MS_SQL_Old_Version>/Backup to <MS_SQL_New_Version>/backup.

Troubleshooting tips

If you get an error while backing up the database, please check whether:

- The database server is running.
- There is sufficient space in the backup storage location.

Auto update

Enable this to automatically update AD360.

1. Navigate to **Admin > Administration > Auto Update.**
2. To enable auto update for a particular component, click the ⊘ icon located in the *Actions* column of the particular component.
3. To disable auto update for a particular component, click the ✓ icon located in the *Actions* column of the particular component.
4. To edit the update scheduler for a particular component, click the ✎ icon located in the *Actions* column of the component.
5. In the *Check for Update* option, select whether you want to check for updates daily, weekly or monthly.
6. Selecting the **Automatically Download and update AD360** option will download and install any available updates automatically.
7. You can also choose to receive notifications about available updates by selecting these options under *Notify* me.
    a. **When updates are available:** Notifications will be sent when updates are available.
    b. **After installing the update:** Notifications will be sent after the updates are downloaded and installed.
8. Click **Save.**
9. Furthermore, you can use the **Update History** link to view all the installed updates.

Alternatively, you can configure the auto-update settings by following the steps listed below:

1. Navigate to the **Support** tab.
2. Check the **Check for updates** box at the top-right corner of the page.
3. Click the **Settings** link in the pop-up that appears, then click the **Auto Update** tab.
4. Check the **box** next to *Enable Auto Update* to enable auto update.
5. In the *Check for Update* option, select whether you want to check for updates daily, weekly or monthly.
6. Selecting the **Automatically Download and update AD360** option will download and install any available updates automatically.
7. You can also choose to receive notifications about available updates by selecting the options under Notify me.
    a. **When updates are available:** Notifications will be sent when updates are available.
    b. **After installing the update:** Notifications will be sent after the updates are downloaded and installed.
8. Click **Save.**

Mail server and proxy settings

Under Server Settings, you can configure the proxy settings in case you are using a proxy server and configure the mail server to send notifications from the product. The following settings can be found here:

- Mail Settings
- Proxy Settings

Mail Settings

- Navigate to **Admin > General Settings > Server Settings.**
- Under the *Mail Settings* tab, the settings are divided into two sections:
  - Configure Mail Server
  - Notification Settings

Configure Mail Server

1. Enter the **Server Name** or **IP** and **Port Number** of your **Mail Server** in the respective fields.
2. In the *From Address* field, enter the **email address** that will be used to send out notifications and alerts from AD360.
3. In the *Admin Mail Address* field, enter your **email** if you wish to receive notifications for the emails sent from AD360.
4. Select the **Connection Security** type. You can choose either **SSL, TLS**, or None.
5. If authentication is required for accessing the mail server, select Authentication and enter the **username** and **password** necessary to access the mail server.
6. Click **Save Settings.**

Notification Settings

To notify the admin when the license is about to expire, check the **box** next to the *Enable License/AMS Expiry Notification* field.

1. To notify the admin when the application shuts down unexpectedly, check the box next to the *Enable Downtime Notification* field.
2. Click **Save Settings.**

Proxy Settings

1. Navigate to **Admin > General Settings > Server Settings.**
2. Click the **Proxy Settings** tab.
3. Select the **Enable Proxy Server** option.
4. Enter the **Server Name or IP** and **Port Number** of the proxy server in the respective fields.
5. Enter the **username** and **password** for accessing the proxy server.
6. Click **Save.**

Alternatively, you can change the proxy settings by following the steps listed below.

1. Navigate to the **Support** tab.
2. Click **Check for updates** at the top-right corner of the page.
3. Click on **Settings** and select the **Enable Proxy Server** check box.
4. Enter the **Server Name** or **IP** and **Port Number** of the proxy server in the respective fields.
5. Enter the **username** and **password** for accessing the proxy server.
6. Click **Save Settings.**

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

Support

To get a personalized demo of AD360:

Click here to request a demo

To get a customized quote for AD360:

Click here to get a quote

For more details or speak to someone:

✉ ad360-support@manageengine.com ☎ +1.844.245.1108 (toll-free)