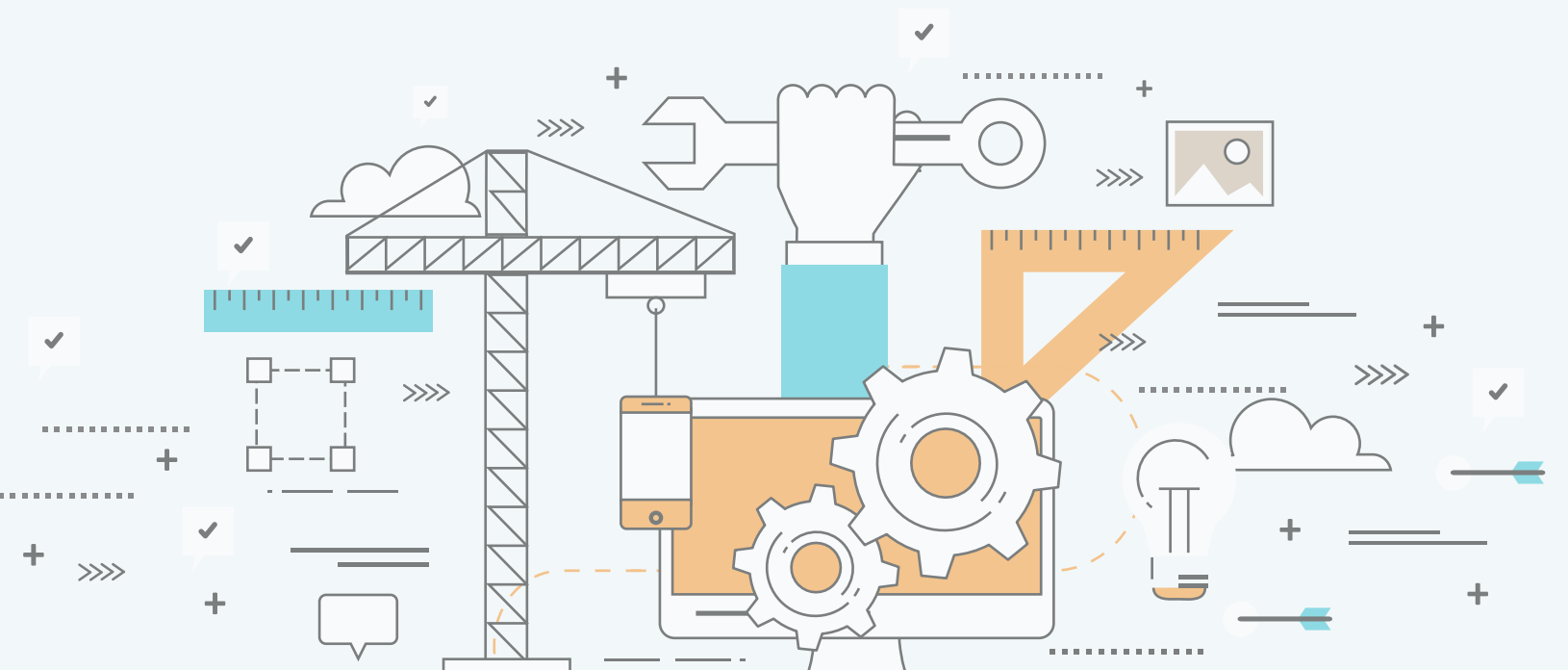


# Quick Start Guide



## Table of Contents

<b>Overview</b> .....	<b>3</b>
<b>Deployment</b> .....	<b>3</b>
System Requirements.....	3
Installation.....	5
Working with AD360.....	7
<b>Integrating the components</b> .....	<b>8</b>
<b>Accessing the individual components</b> .....	<b>10</b>
<b>Setting up individual components</b> .....	<b>10</b>
Synchronizing settings between the components.....	10
ADManager Plus.....	12
ADAudit Plus.....	13
ADSelfService Plus.....	13
Exchange Reporter Plus.....	15
O365 Manager Plus.....	16
RecoveryManager Plus.....	17
<b>Other Settings</b> .....	<b>18</b>
High Availability.....	18
Reverse Proxy.....	18
Enabling SSL.....	18
Database Migration.....	18
Auto Backup.....	22
Auto Update.....	25
Mail Server and Proxy Settings.....	26
<b>Support</b> .....	<b>28</b>

## Overview

AD360 is an integrated solution that helps organizations simplify IAM and IT compliance challenges they face in Windows Active Directory, 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 six different components that you can integrate with AD360, with each providing a unique set of features. You can choose the components you want based on your business requirements and integrated 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	P4 - 2.0 GHz
RAM	4 GB*
Disk Space	40 GB*

\*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:

<ul style="list-style-type: none"> <li>• Windows Server 2016</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008</li> <li>• Windows Server 2003 R2</li> <li>• Windows Server 2003</li> </ul>	<ul style="list-style-type: none"> <li>• Windows 10</li> <li>• Windows 8</li> <li>• Windows 7</li> <li>• Windows Vista</li> <li>• Windows XP SP3</li> </ul>
--	---

## Supported Browsers

One of the following browsers is required to access the AD360 web client:

- Internet Explorer 9 and above
- Firefox 4 and above
- Chrome 10 and above

## Supported Databases

ManageEngine AD360 supports the following databases:

- PostgreSQL (default database bundled with AD360)
- MS SQL

For a detailed list of requirements, please refer 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 necessary privileges and rights to install and run the product. If you are using Windows Vista or later operating systems, disable User Account Control and then proceed with the installation. For more information [click here](#).

### Installing AD360 as an Application

- By Default, AD360 will be installed as an application.
- Click [here](#) to download the executable file from the website.
- Double-click the downloaded file **ManageEngine\_AD360.exe** to start the installation.
- 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 ensuring 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, refer the steps [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 run AD360 as a service, you have to install AD360 as a Service. Follow the steps given below:

- Install AD360 as an application.
- Go to Start Menu → All Programs.
- Select AD360 and click Install AD360 as Service.

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

- Install AD360 as an application.
- Click the notification icon [  ] at the top-right corner of the screen.
- 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 AD360 client

To launch the AD360 client,

1. Open any of the supported web browser and type **http://hostname:8082** in the address bar. Here, the hostname refers to the DNS name of the machine where 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 **single shutdown** so that all the individual components will also be shutdown when AD360 is stopped. To enable this, go to **Admin > General Settings > Product Settings**. Under the **General** section, select **Enable Single Shutdown**.

## Integrating the components

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

- ADManager Plus – provides management, reporting, automation, delegation, and workflow capabilities for Active Directory, Exchange, Office 365 and G Suite.
- ADAudit Plus – performs real-time change auditing, alerting, and compliance management for Active Directory, Azure Active Directory, and file servers.
- ADSelfService Plus – provides password self-service and single sign-on for Active Directory and cloud applications
- Exchange Reporter Plus – provides reporting, auditing, and monitoring capabilities for Exchange Servers, Exchange Online, and reporting capabilities for Skype for Business Servers.
- O365 Manager Plus – provides management, reporting, auditing, and alerting capabilities for Office 365.
- RecoveryManager Plus – takes care of Active Directory, Exchange Server, and Exchange Online backup and recovery.

To get a complete solution for all your Active Directory challenges, these six components have to be integrated with AD360. To integrate the components, follow the steps given below:

**Note:** If you've chosen the standard installation method, the components would 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](#).



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

## Step 2: Integrate the Components

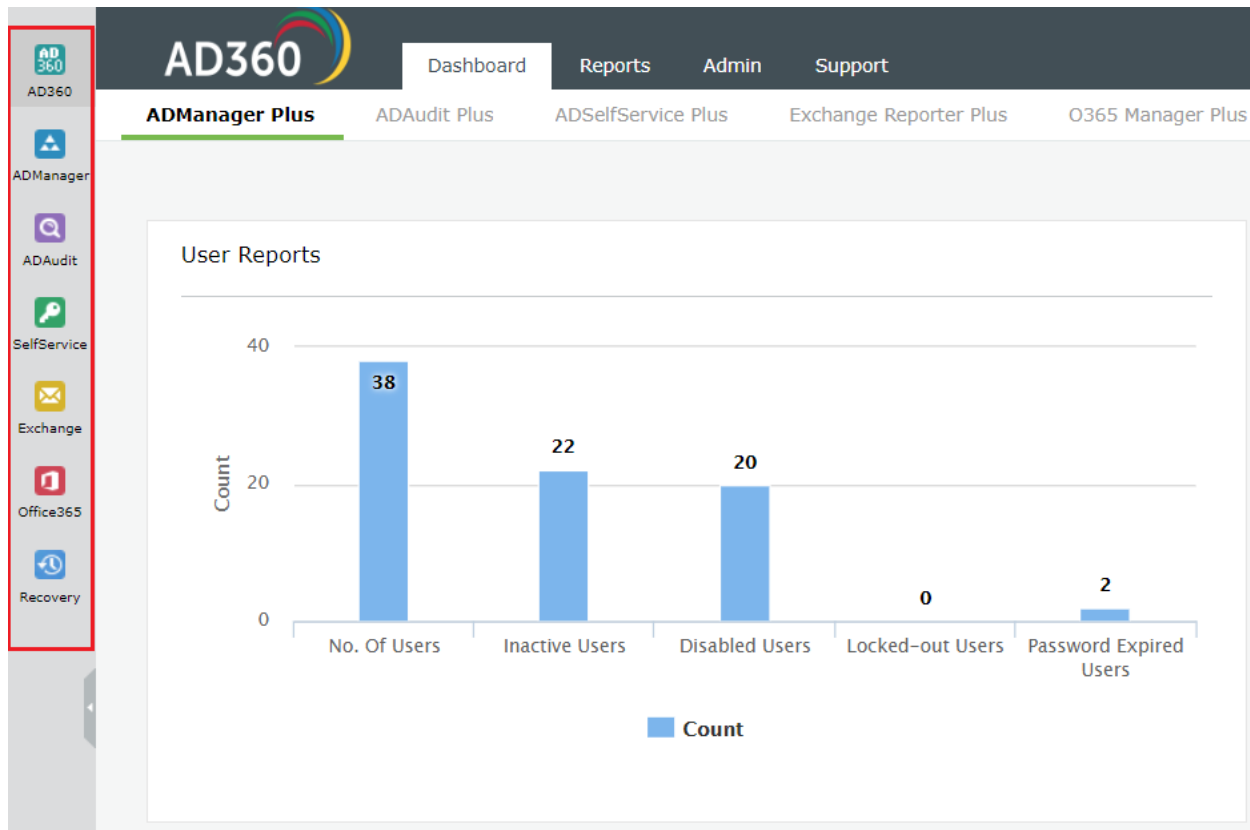
**Note:** Make sure that all the components that are to be integrated with AD360, are running before proceeding with the steps given below.

- Go to **Admin > Administration > AD360 Integration**. You will be presented with five tabs each representing a component of AD360.
- Click on **any one of the tab (say ADManager Plus)**.
- Enter the **Server Name or IP** and **Port Number** of the server in which that particular component is running.
- Select the connection **Protocol** from the drop down menu.
- Click **Integrate Now**.
- Repeat the above 3 steps for other components as well 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 Apps Panel.



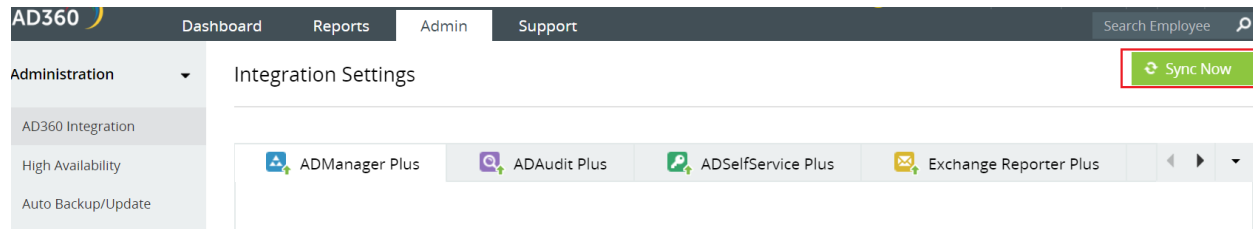
## Setting up individual components

### 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 any one of the components will be automatically reflected in the other components also.

To synchronize the settings between AD360 and the individual components:

- Go to **Admin > Administration > AD360 Integration**.
- 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 credential that was used in configuring a domain with a component, simply update the change in any one of the components 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, updating domain configurations, 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 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 this guide](#) for more information on the permissions and privileges required by AD360 and the individual components.

## ADManager Plus





### Domain Configuration

During startup, 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 client.
2. The domains that are already added are listed here. Click the **Add new domain** link to open the **Add Domain Details** dialog.
3. Specify the Domain Name.
4. Click on the **Discover** link to locate the domain controllers from the DNS and add. Else, 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 this guide](#) to know the granular permissions needed by ADManager Plus.
6. Click **ADD** to add the domain.

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

1. **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 action column to make it default.
2. **Modifying Domain:** To modify the domain details, click the  icon and change the required values and save.
3. **Deleting a Domain:** To delete a domain, click the  icon.
4. **Refreshing the Domain Details:** To synchronize the object details with the Active Directory, click the  icon.

## ADAudit Plus

### Domain Configuration

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

## ADSelfService Plus

### Domain Configuration

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

### Policy Configuration

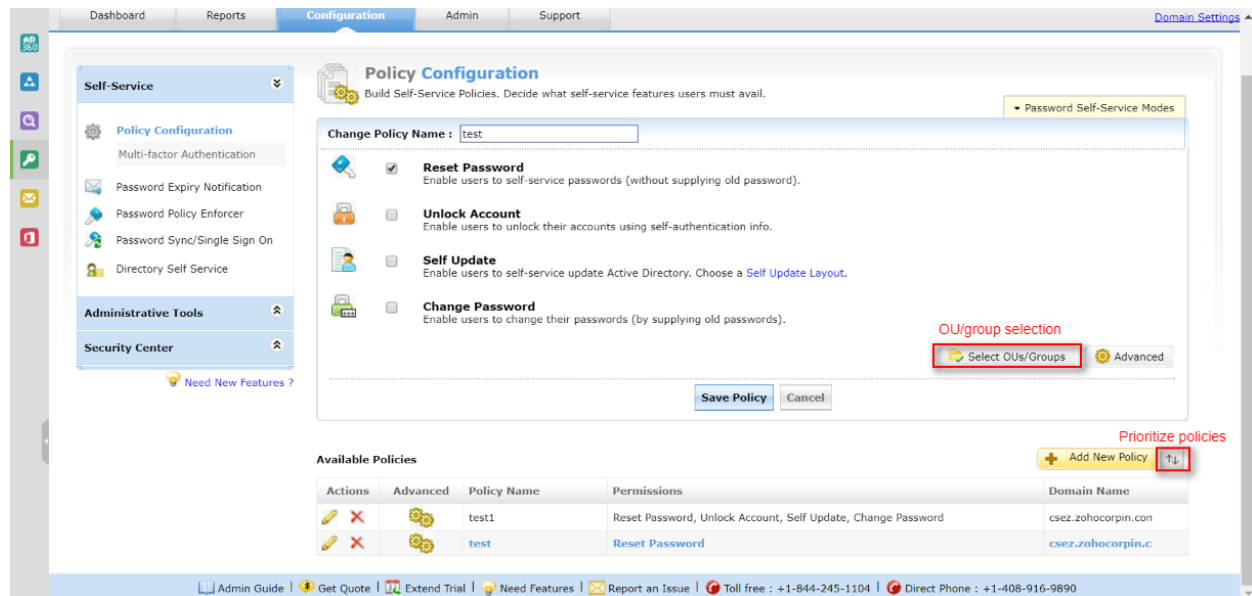
ADSelfService Plus offers a multitude of self-service features such as the below, to domain users.

- Self-service password reset
- Self-service account unlock
- Directory self-update
- Password change from 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.

The Policy Configuration section provides all the functionalities for you to define/edit/delete policies.

By default, when ADSelfService Plus discovers DCs of a domain, it sets a policy for the entire domain. Therefore when you log in for the first time (as an administrator), this default policy will be shown to you. Conventionally, every self-service feature is selected in the default policy. If it fits your requirement, you can retain it; else, you can edit this default policy.



- Click on the **Configuration** Tab.
- Enter a **Policy Name** in the Text box provided.
- Select the self-service features that you wish to delegate to users.
- Click **Select OUs/Groups** button.
- Select the OUs and groups that you want to be governed by this policy.
- 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 settings

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

If you give appropriate credentials during installation, the Exchange Organization will be added automatically. You can also manually add a new Exchange organization and delete, modify or make an existing Exchange Organization as default from the "Organization Settings" option.

### Adding a new Exchange Organization

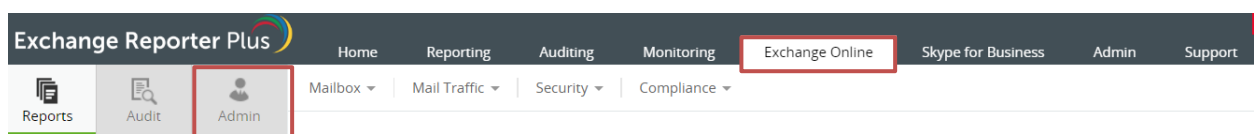
To add a new Exchange Organization:

1. Go to **Admin > Scheduling > Organization Settings**.
2. Click on **Add New Organization** under Configurations.
3. Enter the **Global Catalog Server** name. [If your Exchange Server is within your forest, Global Catalog Server name will be updated automatically.]
4. Provide **Credentials** and click **Add** to add a New Exchange Organization.

[The credentials provided here will be used for a seamless data extraction from the Exchange Servers. Ensure proper credentials are provided. Check the complete list of [privileges required for various data gatherings](#).]

### Adding an Office 365 Tenant

1. Go to **Exchange Online > Admin**.




2. Click **Add New Tenant**.

3. Enter the **Account Name** and **Password** of an Exchange Online admin.
4. Click **Save**.

## Adding a Skype for Business Server

1. Go to **Skype for Business** tab. In the left pane, click **Skype Settings > Add New Forest**.
2. Enter the **Global Catalog Server** name and the credentials of an admin account.
3. Click **Save**.

## Making an Exchange Organization, Tenant, or Skype Server as Default

Any Exchange Organization can be set as default  by clicking on the  icon against the corresponding Exchange Organization. The same applies for an Office 365 tenant and Skype for Business Server.

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

## O365 Manager Plus


### Office 365 Tenant Settings

- Go to **Admin > Administration > O365 Tenant Settings**.
- To add a new Office 365 tenant, click the **Add New Tenant** button in the top-right corner of the O365 Tenant Settings page.
- Enter the **Account Name** and the **Password** of the Office 365 tenant.
- Use the credentials of an administrator who is a member of the Office 365 Global admin role. The account name should be entered in the format "account@company.onmicrosoft.com".
- Click **Save** to add the tenant.

### Modify an existing Office365 tenant:

You can edit the details of any existing Office 365 tenant or delete an Office 365 tenant.



- To edit an existing tenant, click on the  icon located in the action column of the desired tenant.
- To delete an Office 365 tenant, click on the  icon located in the action column of the desired tenant.

### **Make any existing Office 365 tenant the default tenant:**

If you make an Office 365 tenant as the default tenant, then that particular tenant will be selected by default across all the tabs (dashboard, reports, audit, management, etc.) in the product.

- To make an Office 365 tenant the default tenant, click the icon located in the action column of the desired tenant.

### **Permissions Required**

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

### **RecoveryManager Plus**

#### **Adding an Active Directory domain for backup**

1. Go to **Active Directory > Settings > Domain Settings**.
2. Click **Add New Domain**.
3. Enter the domain details and administrator credentials.
4. Click **Save**.

#### **Adding an Office 365 tenant or Exchange organization for backup**

1. Go to **Exchange > Configuration**.
2. Click **Add New Tenant**.
3. Choose whether you want to configure backup for on-premises Exchange or Exchange Online from the **Exchange Type** drop down.
4. Enter the credentials of an admin account.
5. If you'd chosen Exchange Online, choose the **Azure environment** in which the tenant was created.
6. Click **Save**.

## Other Settings

### High Availability

High availability refers to a system or component which aims to ensure an agreed level of operational performance for a higher than normal period. AD360 helps administrators to maintain high availability even in the case of failure of the primary server.

[Refer this guide](#) for instructions on enabling high availability.

### Reverse Proxy

You can make AD360 to 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

You can enable SSL for AD360 by going to **Admin > General Settings > Product Settings**.

For individual components, go to the Admin tab of the respective components and enable SSL.

### 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.

#### Important points to remember

- 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

- Copy the **bcp.exe** and **bcp.rll** files from the SQL Server's installed directory and paste them in the AD360 bin folder (<AD360\_installed\_directory/bin).

**Note:** Instead of manually copying the files, you can also do this while configuring database migration [directly from the user interface](#).

- 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 MS SQL migrations, 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	<a href="#">Download</a>
2008	<a href="#">Download</a>
2008 R2	<a href="#">Download</a>
2012	<a href="#">Download</a>
2014	<a href="#">Download</a>
2016	<a href="#">Download</a>
2017	<a href="#">Download</a>

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

### Steps to migrate 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:
  - In the **DB Server Name/IP and Port** field, enter the host name or IP address and the port number of the PostgreSQL database server.
  - Enter the **Username** and **Password** of a user who has permission to create a new database.
6. If you select **MS SQL Server**, then:

- In the **DB Server Name/IP and Port** field, enter the host name or IP address and the port number of the MS SQL database server.
- In the **DB Server Instance** field, select the SQL Server instance you want to use.
- If you have already moved the bcp.exe and bcp.rll files, the same will be visible in the **Select bcp.exe File** and **Select bcp.rll File** fields. If not, click Browse and select the bcp.exe and bcp.rll files from SQL Server installed directory.
- For Authentication, you can either use Windows credentials or a SQL Server user account.
- If you want to use a SQL Server user account, then select SQL Authentication and enter the Username and Password.
- 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 into the machine check the box against **Use Default Windows Authentication**.

**Note:** The user account used must have permission to create a database in the selected MS SQL Server.

7. Check the box against **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 **Save**.

## Auto Backup

AD360 can automatically back up its database and the databases used in the integrated components at regular intervals, as scheduled by you. 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

1. In the machine where PostgreSQL is installed, go to **<postgresql\_installdir>/data** and open the **postgresql.conf** file. Search for **wal\_level** entry. Uncomment the entry and change its value to **archive**.
2. Copy all the files in **<postgresql\_installdir>/lib** and **<postgresql\_installdir>/bin** folders and paste them in **<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.
3. **Restart** the external PostgreSQL server.
4. Repeat the steps 1 to 3 from above 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 edit  icon.

Actions	Component Name	Schedule Time	Backup Location	Last Backup Time	Last Backup Status
<input checked="" type="checkbox"/>	AD360	2019/01/05 02:00:00	D:\AD360_4215_RELEASE_BRANCHDec_26_2018_4\AD360\Backup	-	No data available <a href="#">Backup Now</a>
<input type="checkbox"/>	ADManager Plus	-	-	-	Component temporarily unavailable <a href="#">Backup Now</a>
<input type="checkbox"/>	O365 Manager Plus	2019/01/03 05:30:00	D:\O365_4221_ADS_BACKUP_BRANCHDec_26_2018\O365 Manager Plus\Backup	2019/01/02 11:11:24	Success <a href="#">Backup Now</a>

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**.

- o. You can either choose a local folder or shared folder to store the backups.
- o. If the shared folder you've chosen needs permission to store the backups, then put a check against the **Authentication Required** box, 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

Database Backup
Database Configuration

Component Name

Backup Frequency Weekly ▼ on Saturday ▼ at 02 ▼ hrs 00 ▼ mins

\* Full Backup after  incremental backups. ?

\* Backup Storage Path Local ▼




Maintain Backup Files Retain all ▼ ?

Save
Cancel

ⓘ By default, incremental backups are taken during auto-backups.

7. Click **Save**.

### Other settings

- 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.
- To get the status of the latest backup, click the  icon.
- To edit the backup schedule for a particular component, click on the  icon located in the action column of the component.
- Use the **Backup Now** option to initiate a backup instantly.
- Use the **Recent Backups** icon in the status column to view all available backups.

### Restoring backup from an old version of MS SQL server to 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 do so by using 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.

- Navigate to Admin → Administration → Auto Update.
- To **enable** auto update for a particular component, click on the  icon located in the action column of the particular component.
- To **disable** auto update for a particular component, click on the  icon located in the action column of the particular component.
- To edit the update scheduler for a particular component, click on the  icon located in the action column of the component.
- In Check for Update option, select whether you want to check for updates daily, weekly or monthly.
- Selecting the option Automatically Download and update AD360 will download and install any available updates automatically.
- You can also choose to receive notification about available updates by selecting the options under Notify me.
  - When updates are available: Notifications will be sent when updates are available.
  - After installing the update: Notifications will be sent after the updates are downloaded and installed.
- Click Save.

- Furthermore, you can use the Update History link to view all the installed updates.

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

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

## Mail Server and Proxy Settings

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

- Mail Settings
- Proxy Settings

## Mail Settings

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

## Configure Mail Server

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

## Notification Settings

- To notify the admin when the license is about to expire, check the box against the Enable License/AMS Expiry Notification field.
- To notify the admin when the application shuts down unexpectedly, check the box against the Enable Downtime Notification field.
- Click Save Settings

## Proxy Settings

- Navigate to Admin → General Settings → Server Settings.
- Click on the Proxy Settings tab.
- Select Enable Proxy Server option.
- Enter the Server Name or IP and Port Number of the proxy server in the respective fields.
- Enter the username and password credentials for accessing the proxy server.
- Click Save Settings.

Alternatively, you can also change the Proxy settings by following the steps listed below:

- Navigate to **Support** tab.
- Click on **Check for updates** box at the top right corner of the page.
- Click **Settings** link in the pop-up that appears, then click on **Proxy Settings** tab.
- Select Enable Proxy Server option.
- Enter the Server Name or IP and Port Number of the proxy server in the respective fields.
- Enter the username and password credentials for accessing the proxy server.
- Click Save Settings.

## Support

### Toll Free Number

+1-844-245-1108

### Contact Us

US: +1-408-916-9393

### Support email

[ad360-support@manageengine.com](mailto:ad360-support@manageengine.com)

### About AD360

AD360 is an integrated solution that takes care of identity and access management, IT compliance, and security of your Active Directory, Exchange, and cloud applications. It supports user life cycle management, multi-platform user provisioning, single sign-on for cloud applications, password self-service, real-time auditing, monitoring, and alerting, and pre-packaged compliance reports. AD360 also allows you to automate or delegate common administrative tasks to help desk technicians while still retaining control through approval workflows.