ManageEngine

AD360

Quick Start Guide

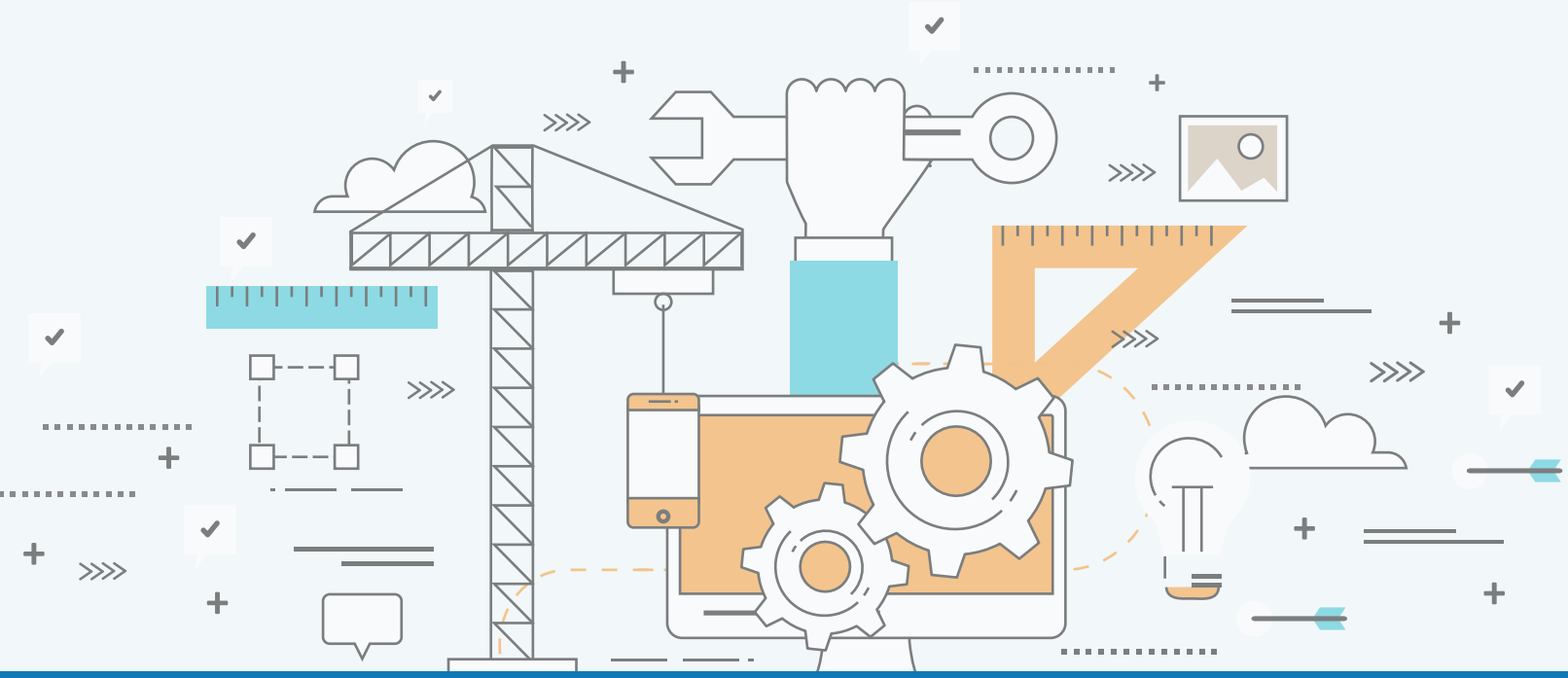


Table of Contents

Overview

AD360 is an integrated solution that helps organizations simplify IAM and IT compliance challenges they face with Windows Active Directory, Exchange Servers, and cloud applications. The four products that come integrated in AD360—ADManager Plus, ADAudit Plus, ADSelfService Plus, and Exchange Reporter Plus—provide all the features that you need to easily manage, audit, secure, and get reports on your entire Windows-based IT infrastructure and cloud applications.

This document explains how to successfully deploy and configure the basic settings of AD360.

Deployment

System Requirements

Hardware	Recommended
Processor	CPU: P4 - 2.0 GHz
RAM	4 GB
Disk Space	40 GB

Supported Platforms

ManageEngine AD360 supports the following Microsoft Windows operating system versions:

- Windows Server 2012 R2
- Windows Server 2012

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP SP3

Supported Browsers

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

- 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

Installation

ManageEngine AD360 can be installed on any machine in the domain provided that they meet 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. For more information click here.

Install AD360 as an Application

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

You can choose from three install types: Standard, Minimal and Custom.

- **Standard Installation:** Downloads and installs all the components along with AD360. This installation type is highly recommended, as it installs AD360 along with all the components necessary for a comprehensive Active Directory and Exchange management.
- **Minimal Installation:** Installs AD360 alone. You can use this installation type if you are already running the components you need.

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

The application can be launched on a web browser by double-clicking the 'AD360' shortcut icon present on the desktop. When opened as an application, AD360 runs with the privileges of the user who has logged on to the computer.

Install 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.
- Click **Install** against the AD360 not installed as a service alert to initiate the 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.

To Uninstall AD360

To uninstall AD360, **Select Start Menu → All Programs → AD360 → Uninstall AD360.**

Working with AD360

Starting AD360

AD360 can be started either in the system account (when run as service) or in user account (when run as an application). Starting AD360 will also start the individual components automatically.

When AD360 is installed as a Service

Option to install AD360 as a service is available in the installation wizard.

- To start AD360 using the **system account**, select **Start** > **Programs** > **AD360 > Start AD360.**
- To start AD360 using a **user account**, double-click the AD360 desktop icon.

When AD360 is not installed as a service

In this case, AD360 can only be started in the **user account**. To start the product, select **Start > Programs > AD360 > Start AD360.**

On starting AD360, the client is automatically launched in the default browser.

When AD360 is started in Windows XP/Windows Server 2003 machines with firewall enabled, Windows may pop up security alerts asking whether to block or unblock the following program as shown in the images below:

You should **Unblock** this program to start AD360.

Fig: Java Alert

Launching AD360 client

To launch the AD360 client,

1. Open a 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 the default password by going 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. To enable it, go to **Admin > General Settings > Product Settings**. Under the **General** section, select **Enable Single Shutdown**.

Integrating the components

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

- ADManager Plus – includes management, reporting, automation, delegation, and workflow features for Active Directory, Exchange, Office 365 and G Suite.
- ADAudit Plus – includes real-time auditing, alerting, and compliance for Active Directory and file servers.
- ADSelfService Plus – includes password self-service and single sign-on for Active Directory and cloud applications
- Exchange Reporter Plus – includes reporting, auditing, and monitoring of Exchange Servers.
- O365 Manager Plus – includes management, reporting, auditing, and alerting of all Office 365 services.

To get a complete solution for all your Active Directory challenges, these five components have to be integrated with AD360. Follow the steps shown below:

Step 1: Download and Install the Components

Note: If you've chosen the Standard Installation mode or already have the components installed and running, you can skip this step 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 install shield wizard.

- Once the installation is complete, start the different components by double-clicking on the desktop shortcut icons of the respective components.

Step 2: Integrate the Components

Note: Make sure that all the components are running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the AD360 version you are currently running.

- 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 from 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 from the same tab of AD360 using the Apps Panel.

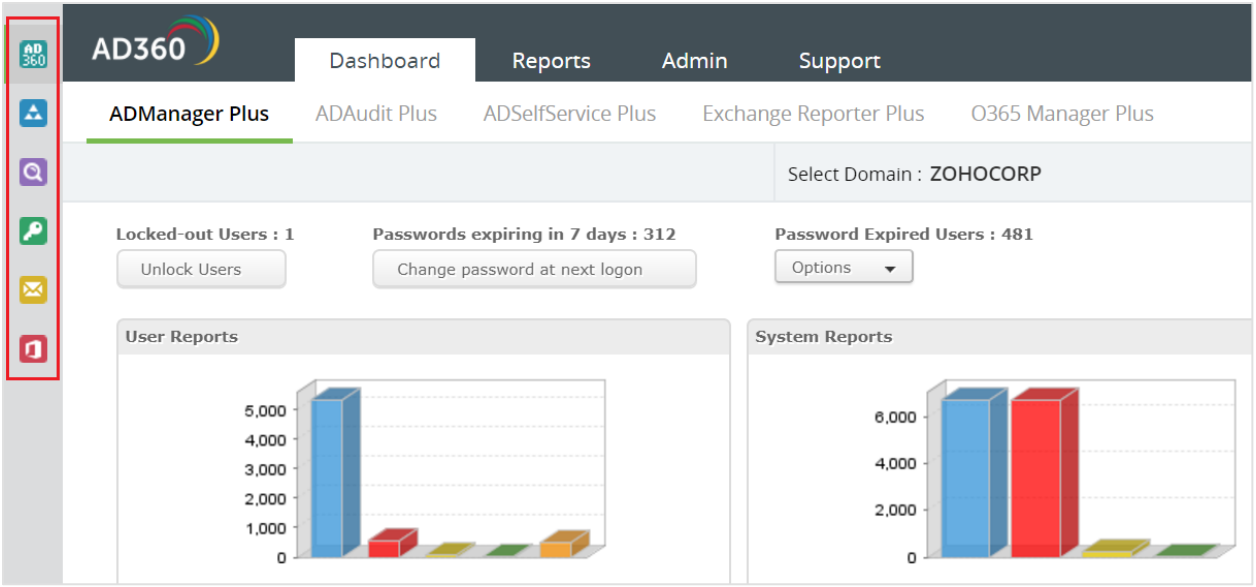


Fig 2: Apps panel

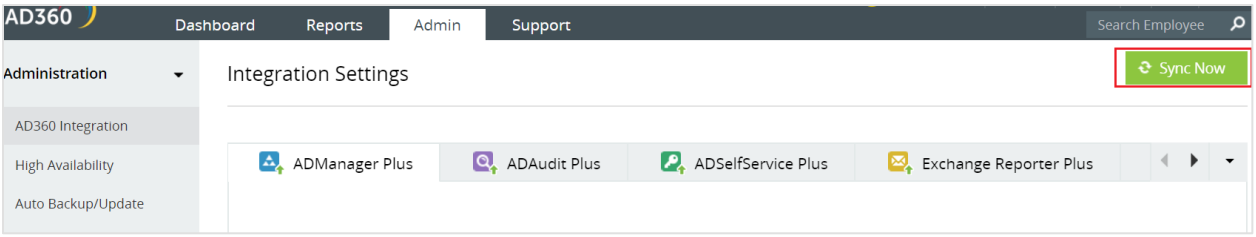
Setting up individual components

Synchronizing settings between the components

Data related to domain settings, component integration, mail server, proxy server, etc., will be automatically synchronized across each component. This saves a lot of time as you no longer have to configure the same settings across all the five components. Any changes you make in any one of the components will be automatically reflected in the other components also. The data relating to the following configuration settings will be automatically synchronized across all the components of AD360.

To synchronize 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 synced 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 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 settings, etc. Any changes to the hostname and port number of a component must be reflected in the other components for smooth running of all the components. But with AD360, there is no need for you, the administrator, to manually make the changes in all the components. Simply update these changes in the AD360 Integration settings page and the changes will be automatically synchronized across all the components.

ADManager Plus

Domain Configuration

During startup, ADManager Plus adds all the domains that could be discovered. If you wish to add more domains or modify the added domains, you can do it from here.

To add more domains, follow the steps below:

1. Click the **Domain Settings** link from the client to open the Domain Settings page.
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 **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 move the added domain controllers in the order of priority.
5. Specify the authentication details of the user as which the domain controller will be contacted.
6. Click **ADD** to add the domain.

You can perform the following actions from here:

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 from 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.

Permissions Required

- While adding new domains, the username and password provided will be used for management and generating reports.
- The user account used to configure domain settings must have the privileges to perform a management operation. Read only privilege is sufficient to generate and view reports.
- The first domain controller in the list will be contacted first for all operations. If it turns unsuccessful, then the next domain controller in the list will be contacted.

ADAudit Plus

Domain Configuration

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

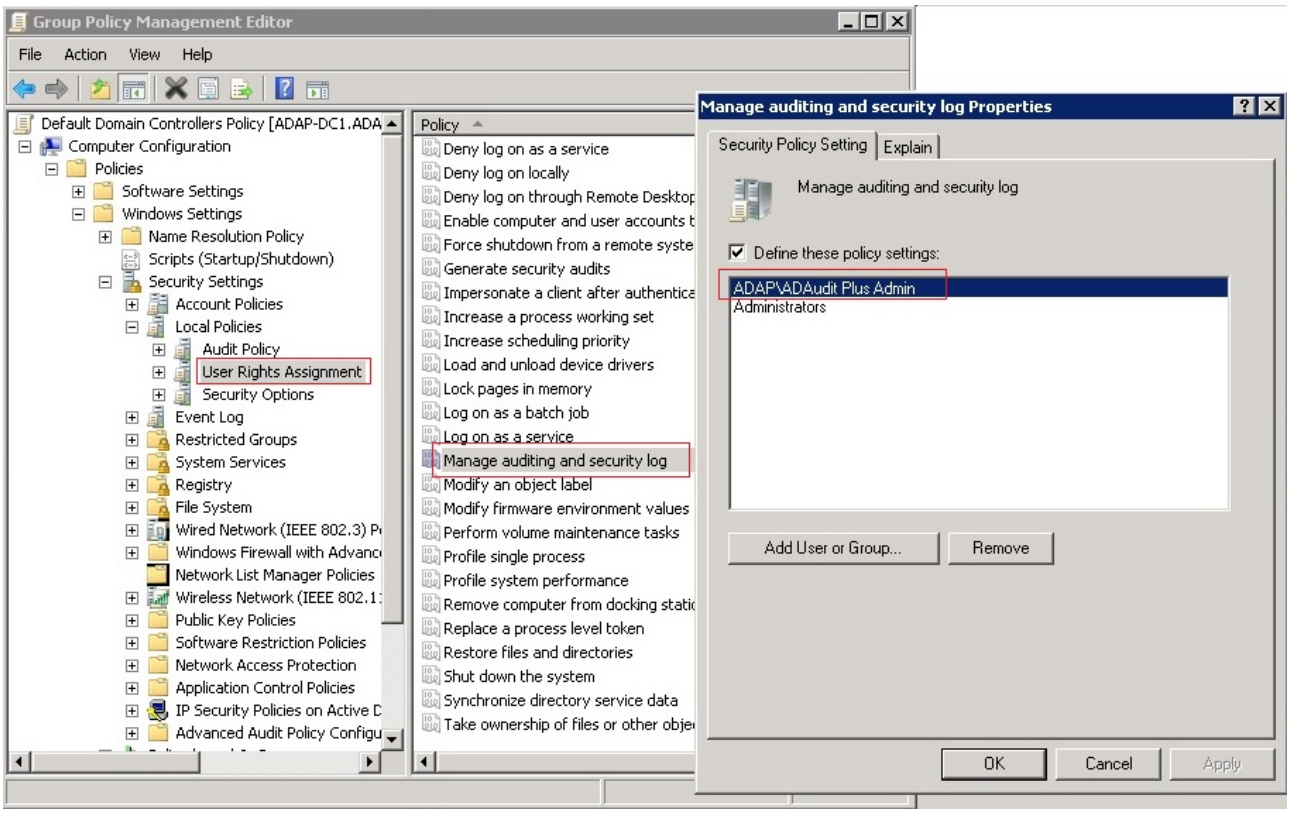
Required Privileges and Permissions

Create a 'user' account in your Active Directory and configure ADAudit Plus Service/Domain Settings page with this 'user' account for data collection, processing and report generation.

ADAudit Plus instantly starts to audit, when provided with a **'Domain Admin'** account. When users' do not want to provide a 'Domain Admin' account, follow the below steps to manually configure the successful working of ADAudit Plus.

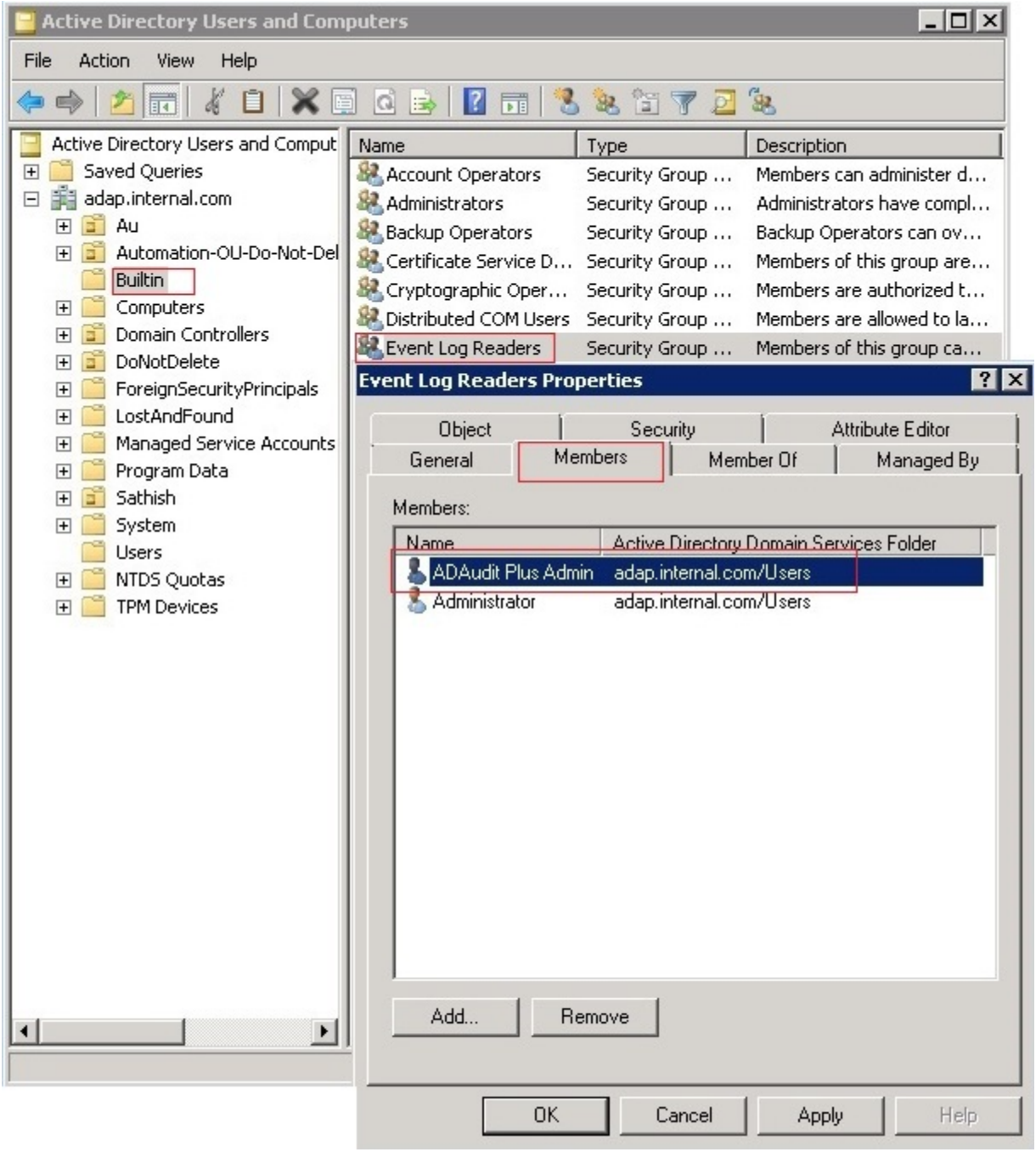
Manage Auditing and Security Log Privilege

Add the user in 'Manage auditing and security log' policy; this is present in Computer Configuration I Windows Settings I Security Settings I Local Policies I User Rights Assignment - Use a GPO and push this setting to **all audited Servers.**



Member of Event Log Readers

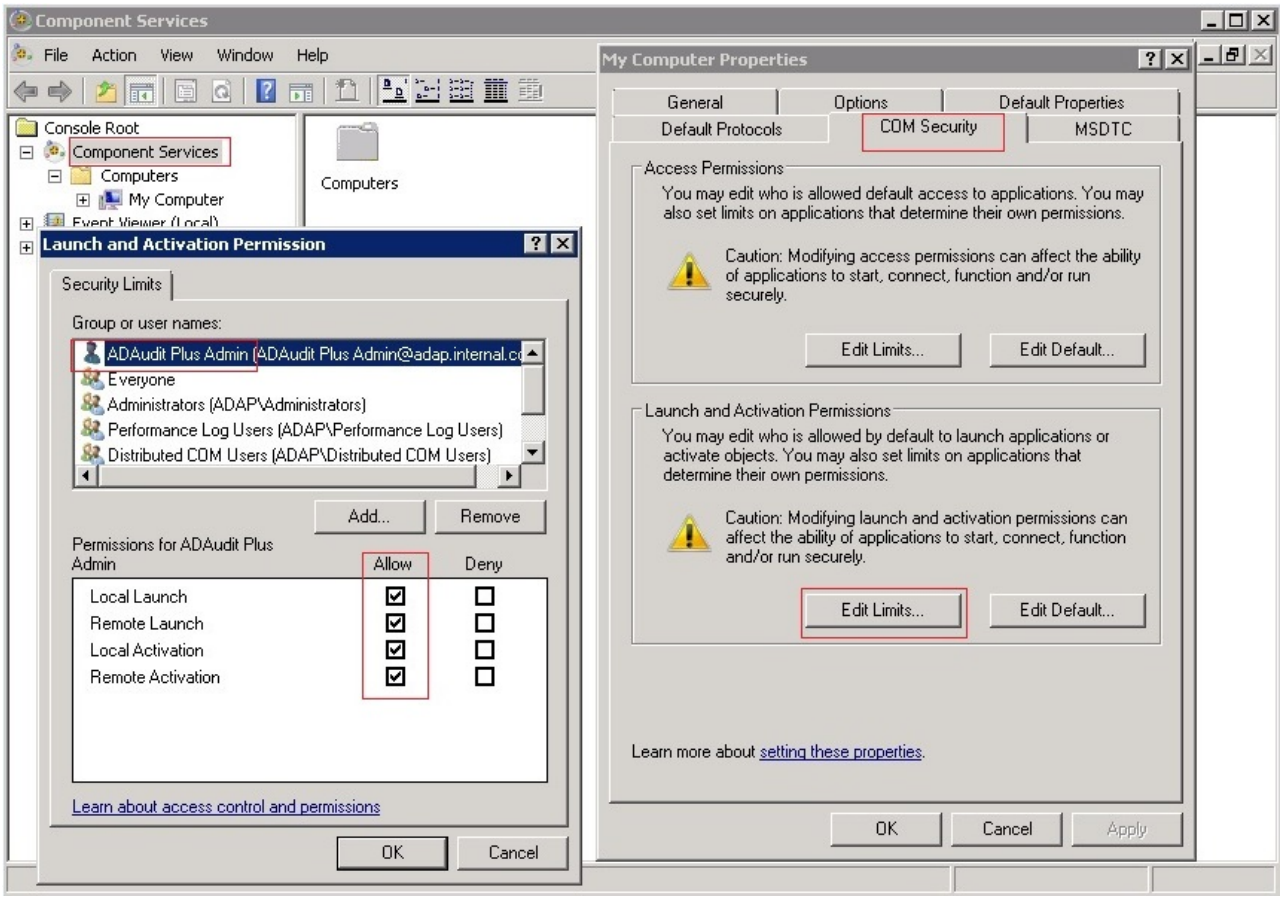
- **For Domain Controllers above 2003:** Open Active Directory Users and Computers I Built-in Container I Add user as a member of 'Event Log Readers' group.



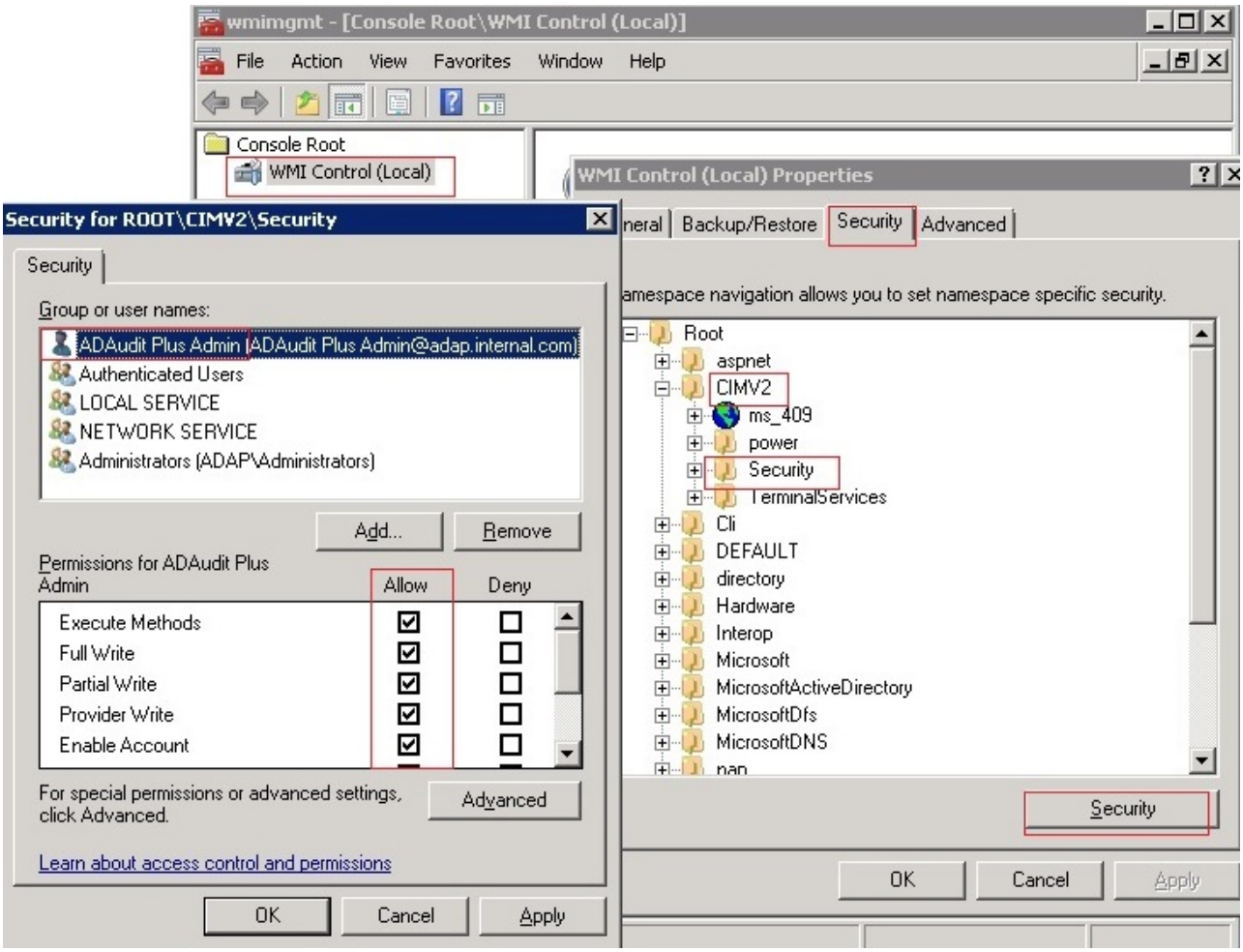
DCOM & WMI Permission

The 'user' must have the DCOM & WMI permission in the **Primary Domain Controller** of the domain.

- **DCOM Permission:** Component Services I Computers I My Computer I Right Click and go to Properties I COM Security I Edit Limits of 'Launch and Activation Permissions I In Security Limits, Add the 'user' with Allow for all permissions. .

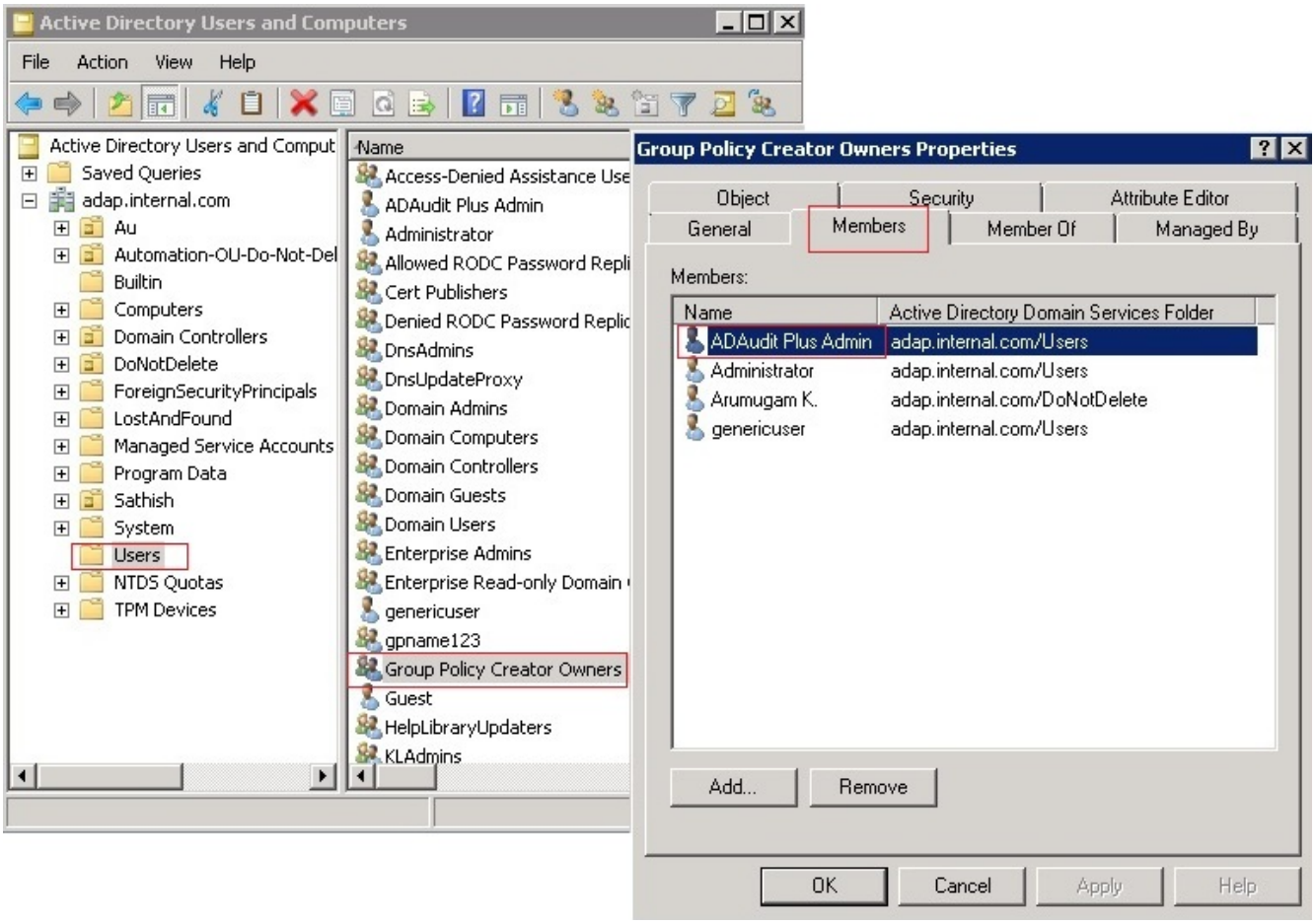


- **WMI Permission:** Go to Start I Run 'wmimgmt.msc' I Security Tab I CIMV2 I Security I Add the 'user' with Allow for all permissions.



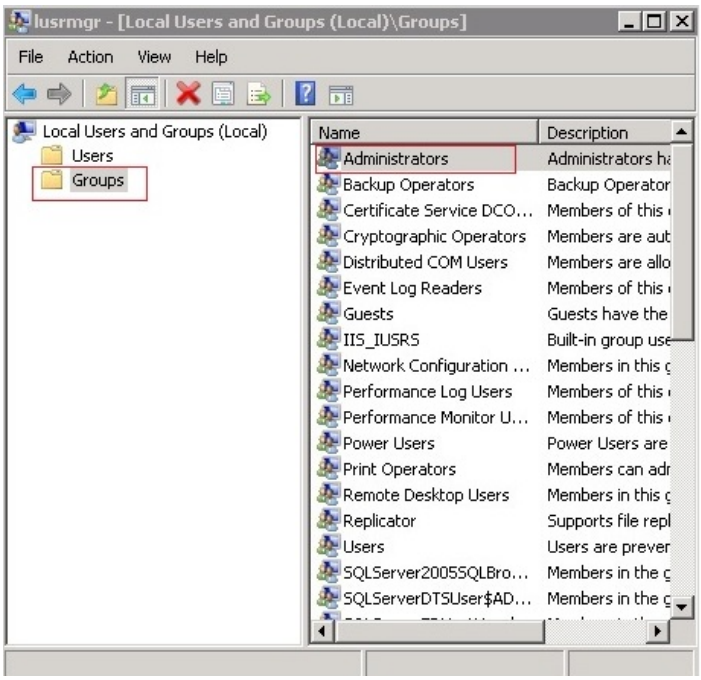
Member of Group Policy Creator Owners

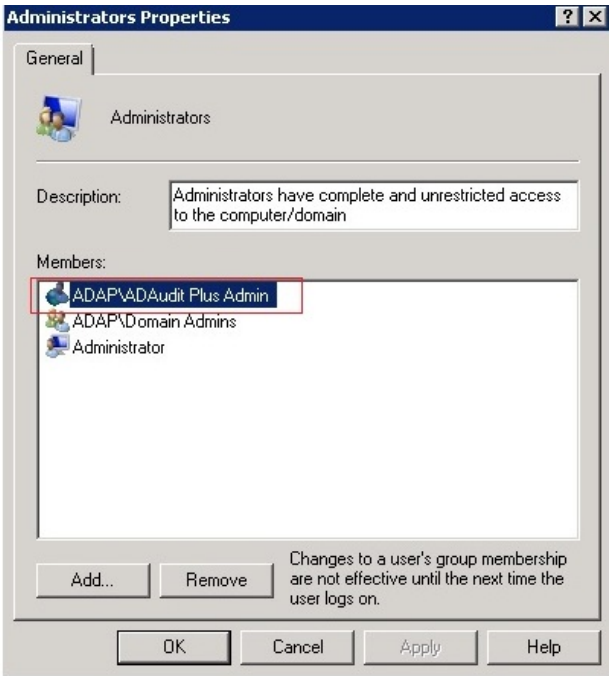
Open Active Directory Users and Computers I Users Container I Add user as a member of 'Group Policy Creator Owners' group



Member of Local Administrators Group

Open Local Users and Groups I Groups I Add user as a member of 'Local Administrators' group **(On Every Monitored File Servers for File Server Auditing).**





ADSelfService Plus

Domain Configuration

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

Permissions required

The account used to configure domain settings must have domain admin privileges for all self-service features to work properly. If giving domain admin credential is not an option, then you can give appropriate permissions required to perform specific self-service tasks. For the exact permission list, please contact support@adselfserviceplus.com.

Policy Configuration

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

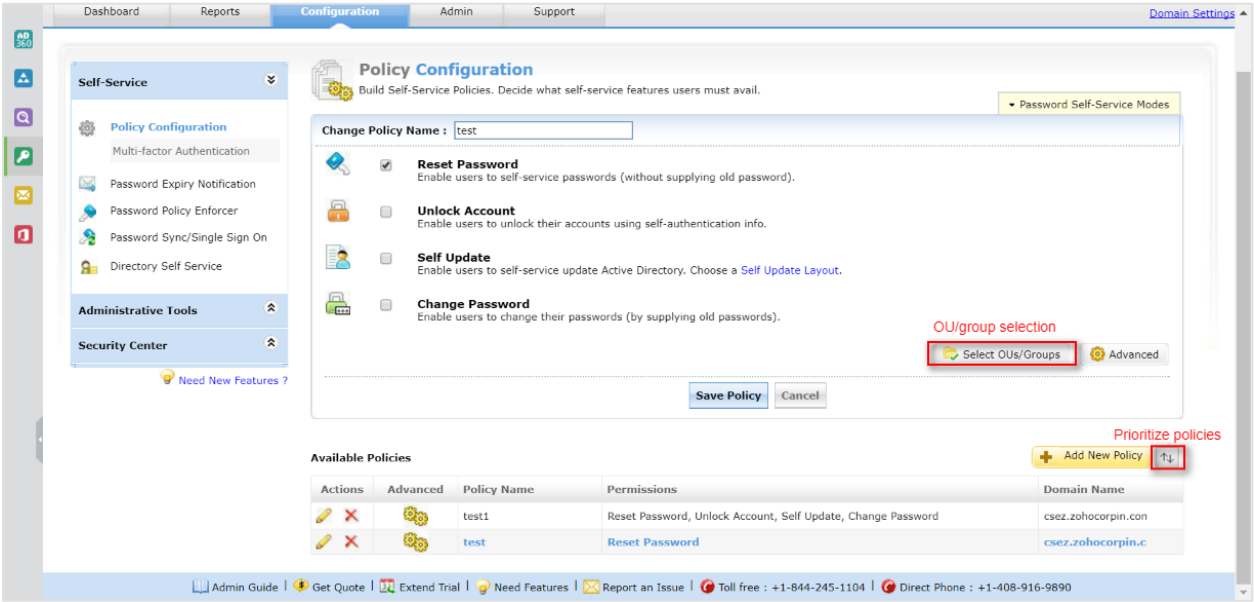
- Self-Reset Passwords
- Self-Unlock Accounts
- Update Personal Info / Self Update of AD Accounts

- Change Passwords

As an administrator, you can decide whether users of a domain or selected organizations unit(s) (OU) will avail themselves of any or all of these functions. In other words, you set a "self-service policy" for the users and define the extent they can use ADSelfService Plus.

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

By default, ADSelfService Plus sets a policy for the entire domain, when it discovers DCs of a domain. Thus 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. If it fits your requirement, you can retain it; else, you can edit it.



- Click on the "Configuration" Tab.
- Enter a Policy Name in the Text box provided.
- Provide a check against one or all self-service features that you wish to delegate to users.
- Click on "Select OUs" button.

- This will "Pop-up" the list of all OUs in the configured Domains in a "Tree View" or "List View".
- Select "Domain" from the dropdown this will list OUs in the selected Domain.
- Provide a check against one or all OUs to select OUs for policy application.
- Click on "OK" button.
- Click on "Save" button this will save the configured settings.

This will allow users in the selected OUs to enjoy the Self Service features that are checked 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 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. Click on the "Organization Settings" link under the "Admin" Tab
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 on "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.]

Modifying an Exchange Organization

To modify an Exchange Organization:

1. Click on the "Organization Settings" link under the "Admin" Tab
2. Click on the icon against the Exchange Organization that is to be modified.
3. Modify the required fields.
4. Click on "Update"

Deleting an Exchange Organization

To delete an Exchange Organization:

1. Click on the "Organization Settings" link under the "Admin" Tab
2. Click on icon against the Exchange Organization to be deleted.

Making an Exchange Organization as Default

Any Exchange Organizations can be made as default by clicking on the icon against the corresponding Exchange Organization.

By design, the product shows reports, home graphs and schedule creation options for the Exchange Organization selected as default.

Permissions required

1. The ERP Admin Account must be a member of the following groups.

- For Exchange 2010, 2013, and 2016: Organization Management group and Domain Admin.
- For Exchange 2007 and 2003: Exchange View only Administrator group and Domain Admin.

2. Transport queues role should be assigned to the user or the Organization Management group in order to run Email Monitoring Reports.
   - To assign this role to the user:
     - New-ManagementRoleAssignment -Name TransportRoleAssignment -User 'DOMAIN\userName' -Role 'Transport Queues'
   - To assign this role to Organization Management group:
     - New-ManagementRoleAssignment -Name TransportRoleAssignment -SecurityGroup 'Organization Management' -Role 'Transport Queues'

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 Ofice365 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:

Making an Office 365 tenant the default tenant will make the particular tenant default across all tabs 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.

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 for a server in case of failure of the primary server.

AD360 achieves this by employing a high availability architecture which designates a backup server to act as a shield 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 till the time the primary server is down.

- Whenever the primary server encounters unplanned downtime, the standby server becomes operational and takes control of components.

Prerequisites

Before enabling this setting, make sure that the following conditions are satisfied.

1. Make sure that the version of the MS SQL server used is higher than 2005.
2. Make sure that both instance of the product:
   - Are installed and running as a service.
   - Have the same build architecture (32-bit or 64-bit), version and build number.
   - Are connected to the same domain, and network. If your IP range is 172.21.9.x, then the primary server, standby server and the virtual IP should also lie in the IP range 172.21.9.x.

High Availability can be disabled only from the standby server. Please shutdown the component in the primary server and start it from the standby server.

Configuration

Follow the below steps to enable this setting.

1. Navigate to **Admin > Administration > High Availability**.

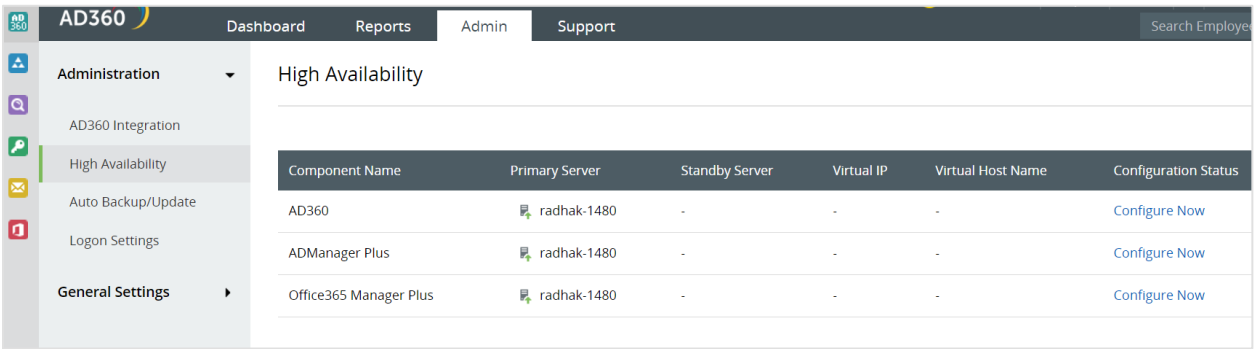


Fig 3: High availability settings

2. Select the component for which you want to configure high availability settings.
3. Enter the appropriate values for the subsequent fields to enable this setting.

- **Primary Server:** This text box will contain the URL of the primary server on which the selected component is installed.
- **Secondary Server:** Enter the details of the secondary server which will take over during downtimes of the primary server.
  - **Standby Server Name/IP:** Enter the URL of the secondary server that you want to take over during downtimes of the primary server.
  - **Admin Username/Password:** Enter the super admin credentials of the component in standby server.

Note: Super administrators are users who have been provided with the full control over the entire application.

- **Virtual IP:** Enter a single IP with which to access both the primary and standby servers. When the product is accessed using this IP, the data is routed directly through the server that is active at that particular time.
  - **Virtual IP Address:** A virtual IP address is an unused static IP address. Open cmd and try pinging an IP. If it throws the error "Request timed out", the IP is unused and can be used as the virtual IP. Enter the virtual IP to access both primary and standby servers.
  - **Virtual Host Name:** A virtual host name is the alias given to the virtual IP. This can be set from the DNS server. Enter the virtual host name to access both primary and standby servers.

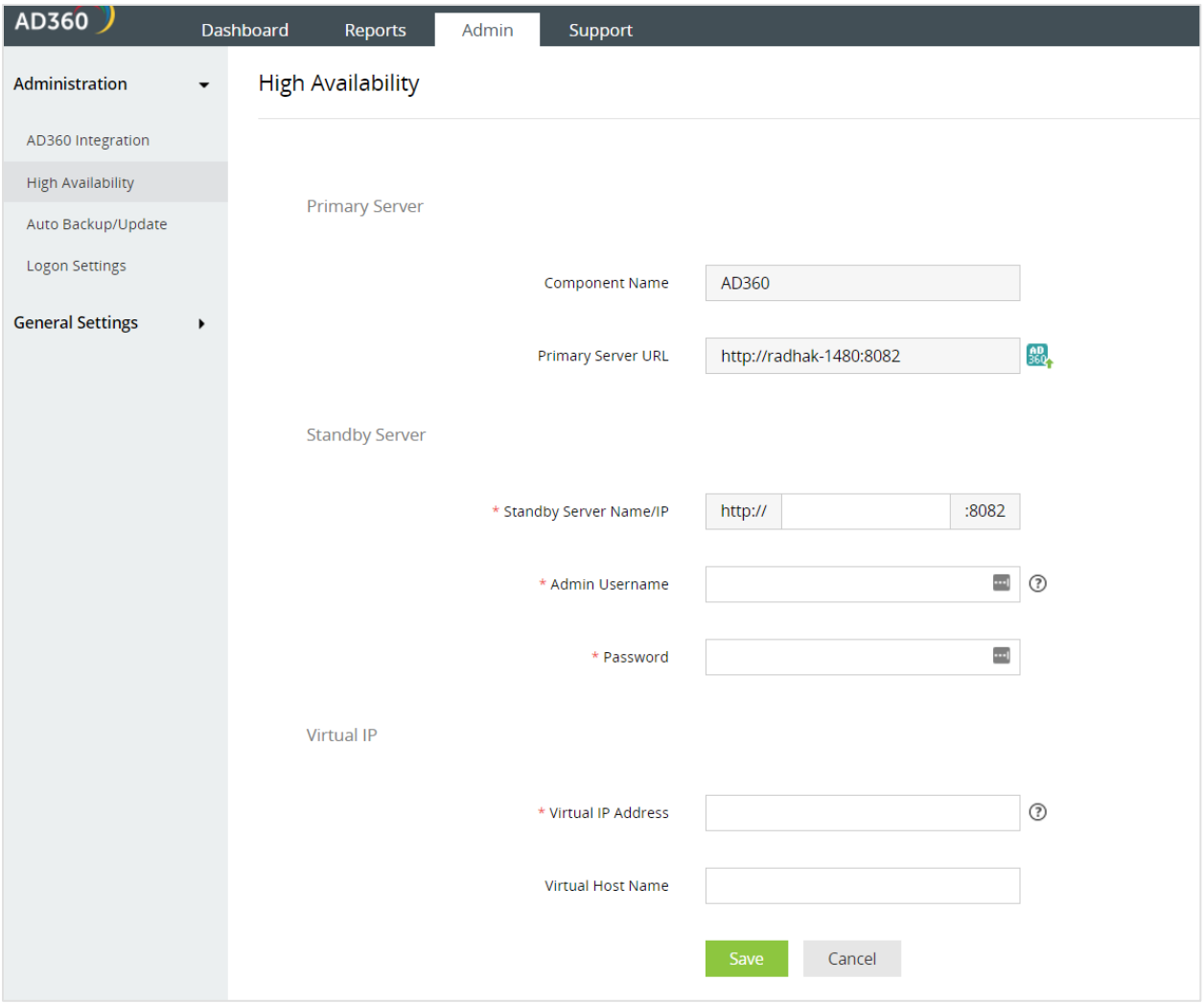


Fig 4: High availability configuration

4. Click **Save**.

Enabling SSL

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

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

Database Migration

- Run **<AD360 home>\bin\ChangeDB.bat** as an administrator from a command prompt.
- In the wizard that pops up, select the products for database migration. Make sure those products are up and running.
- Select the **Server Type** (database) to which you want to migrate to.
- Enter all the other required configuration details.
- Select **Migrate Existing Data** if you want to migrate all the existing data. Otherwise, a new database with default values will be created.
- Click **Change** for the changes to take effect.

Auto Backup and Auto Update

Auto Backup

This allows you to centrally configure automatic database back settings for AD360 and its individual components (only ADManager Plus and O365 Manager Plus are supported).

- Navigate to **Admin** → **Administration** → **Auto Backup/Update** → **Auto Backup**.
- To **enable** auto backup for a particular component, click on the icon located in the action column of the particular component.
- To **disable** auto backup for a particular component, click on the icon located in the action column of the particular component.
- 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.
- In the **Schedule Backup** option, select whether you want to back up the component daily, weekly or monthly.
- In the **Backup Storage Path field**, enter the path to the location where you want to store the backups.
- In the **Maintain Backup Files** field, select the number of days till which the backups have to be retained.
- Click **Save Settings** to schedule backup.
- Click **Backup Now** to initiate a backup instantly.
- Furthermore, you can use the **Recent Backups** icon in the status column to view all available backups.

Auto Update

Enable this to automatically download and update AD360.

- Navigate to **Admin** → **Administration** → **Auto Backup/Update** → **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.

Mail Server and Proxy Settings

Under server settings, you can configure the mail server for sending notifications, alerts, etc., 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 expiry, 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**.

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.