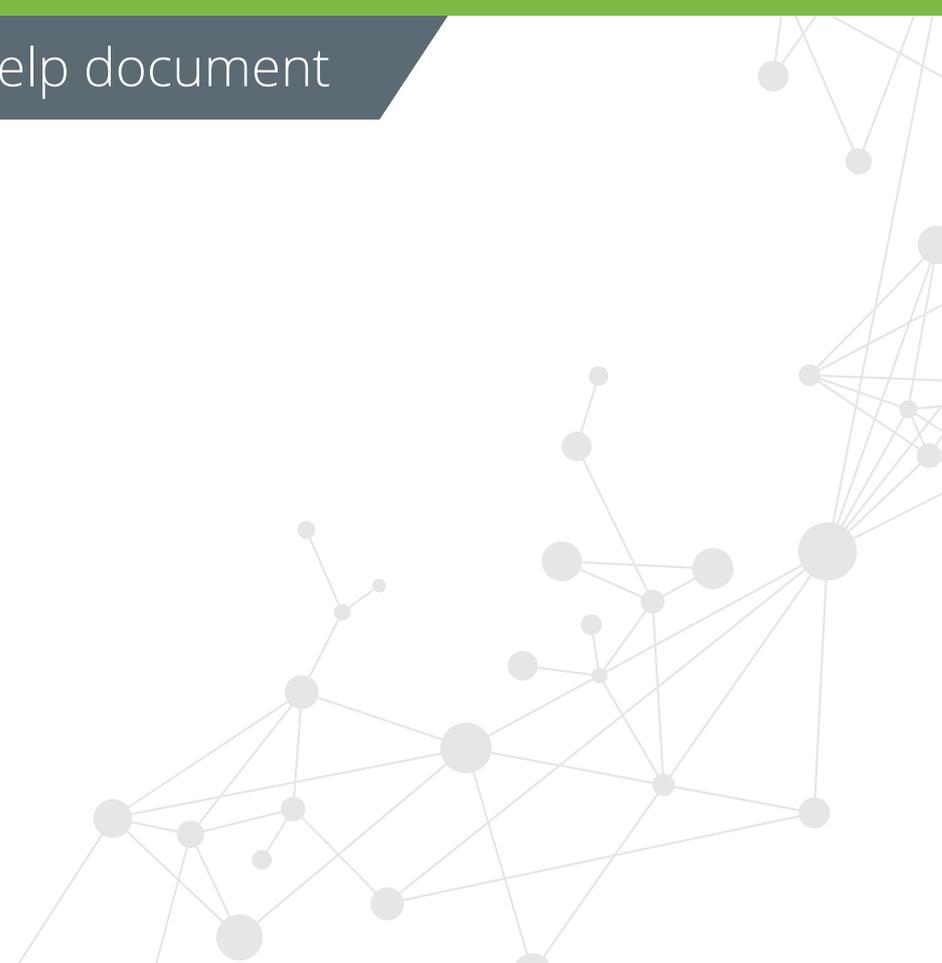




ManageEngine
AD360

Welcome to **AD360**

Help document



Overview



Integrated Solution for IAM

Unify AD Management, AD Auditing, Password & IT Self-Service, and Exchange Reporting to make your organization's Active Directory and Exchange environment easily manageable.



Streamline IAM Operations

Automate crucial AD tasks such as user account provisioning / de-provisioning with a workflow to ensure that crucial data does not land into wrong hands.



Secure AD Audit & IT Compliance

Audit crucial changes made to AD objects and determine if the changes made are in conformance with the IT regulatory compliance such as SOX, HIPAA, PCI, etc.



Ensure a secure self-service

Ensure self-service for password reset and account unlock in the Winlogon (CTRL+Alt+DEL) screen to dramatically reduce the help desk tickets.



Control workflow automation

Customizable review-approve framework to help you keep control over automation for crucial tasks.



Monitor the Exchange Traffic

Monitor complete Exchange traffic data like OWA usage, email traffic, mailbox size and permissions and export reports to any of the formats like xls, csv, html and pdf.

Table of Contents

Getting Started	1
System Requirements	1
Installation	1
Deployment Scenarios	2
Working with AD360	3
Licensing	4
Migrating PGSQL to MSSQL	4
Dashboard View	9
Admin	11
Administration Settings	11
AD360 Integration	11
High Availability	13
Auto Backup/Update	15
Logon Settings	16
General Settings	19
Personalize	19
Product settings	20
Server settings	21
Send Support Info	23
Knowledge Base	25
How do I reset the password of the admin account?	25
How do I change the password of the admin account?	25
How do I install AD360 as a Windows service?	25
How to I manually backup and restore the database in AD360?	26
How do I move AD360 to a new server?	26
How do I change the port number of AD360?	27
Troubleshooting Tips	28
SSL Troubleshooting Tips	31
FAQ	33

Getting Started

System Requirements

Hardware (Recommended)

- Processor : P4 - 2.0 GHz or better
- RAM : 4 GB
- Disk Space : 40 GB

Supported Platforms

- 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 & above)

Supported Browsers

- Internet Explorer 9.0 and above
- Firefox 4 and above
- Chrome 10 and above

Installing and Uninstalling

Installing AD360

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.**

Once the **AD360 Service** is installed, you can start the product as **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.**

Deployment Scenarios

Enable SSL for Secure Communication over the Internet:

You will need to enable SSL for enhanced security and secure communication by AD360 over the Internet. To enable SSL on AD360, kindly follow the steps given below:

- Logon to the AD360 by providing proper admin credentials.
- Go to **Admin ---> General Settings ---> Product settings.**
- In the **Connection Type section**, choose the radio button corresponding to **HTTPS** and enter the **Port Number** you want to use.
- Click **Save** and restart AD360.

This will enable SSL, and a secure communication by AD360 Plus over the internet is possible.

Working with AD360

This section discusses the following topics:

- Starting AD360
- Accessing AD360 client
- Stopping AD360

Starting AD360:

To start AD360, double-click the AD360 shortcut icon placed in the desktop. It can also be started from the Start Menu as shown below:

- Go to **Start** ---> **All Programs** ---> **AD360** ---> **Start AD360**

This will open AD360 client in your default web browser.

Running AD360 as a Service:

If you have installed AD360 as a service, you can start AD360 as a service as shown below:

- Go to **Start** ---> **Control Panel** ---> **Services** ---> **start ManageEgnine AD360 service.**

[Click here](#) to learn how to install AD360 as a service.

Starting the Components:

If all the components are installed on the same machine as AD360, then starting AD360 will automatically start the components as well. But if the components are installed on different machines, then you have to manually start the components before starting AD360.

- To manually start the components, just **double-click the components' shortcut icons** placed on the desktop or go to **Start** ---> **All Programs** ---> **<Component>** ---> **Start** ---> **<Component>**.

When you enter the user credentials and log in to any one of the component, you will be automatically logged in to the other components as well. There is no need for you to enter the log in details in each and every component

Accessing AD360 Client:

To launch the AD360 client, 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 running and 8082 is the default port number of AD360. Specify the username and password as admin (for first time login) in the respective fields and click Login.

If you have changed the password, you should use the new password to login.

Stopping AD360:

- To stop AD360 go to **Start Menu** ---> **All Programs** ---> **AD360** ---> **Stop AD360**.

Licensing

AD360 is available as a free download with full access to all product functions and technical support for a 60 day trial period. Once the 60 day trial expires, you have to apply the AD360 Professional or Standard Edition license to continue enjoying the full benefits of the product. [Click here](#) to identify which edition of AD360 suits you best.

After installing AD360, buy and apply the appropriate license using the **License** link available in the top right corner of the AD360 Web portal.

Note: You can choose to buy license for all the components or only the components that you want based on your requirement. Only the selected components' features will be available in AD360. Visit our [online store](#) to buy the components.

For purchasing the license or any queries, please contact sales@manageengine.com The license file will be sent through e-mail.

To apply the license:

- Click the **License** available in the top right corner of the AD360 client. This opens the **License details** of the product.
- Select the **License.xml** file received from ZOHOO Corp using the **Browse** button.
- Click **Apply** to apply the license.

Migrating the PostgreSQL Data to MS SQL Server

In a simple three stage process, migrate the PostgreSQL data and run the AD360 Server with MS SQL Server.

- Backing up PostgreSQL Data
- Configuring MS SQL Server
- Migrating PostgreSQL Data to MS SQL Server

Backing up PostgreSQL Data

- Stop the AD360 Server/Service.
- Invoke the `<AD360 Home>\bin\backupDB.bat` in command prompt to backup the data available in PostgreSQL database. By default, the backup file will be stored under `<AD360 Home>\Backup\AD360_Backup<Backup_time>` directory.

Configuring MS SQL Server

Common Settings to be performed in MS SQL Server

- Open **SQL Server Configuration Manager**.
- Goto **SQL Server Services** and ensure the service **SQL Server Browse'** is running.
- Goto **SQL Server Network Configuration** ---> **Protocols for SQLEXPRESS** (the given instance while configuring the MS SQL) ---> **Enable TCP/IP**. Then restart the **SQL Server (SQLEXPRESS - the given instance) Service**.
- Set the following configuration for the **SQL Server Configuration Manager**:
 - **SQL Server Network Configuration** ---> **Protocols for <instances>** ---> **Enable everything**.
 - **SQL Native Client Configuration** ---> **Client Protocols** ---> **Enable all**.

Providing credentials to other users in the domain

- Go to **SQL Server Management Studio**.
- Expand the following **<MACHINE_NAME>\SQLEXPRESS** ---> **Security** ---> **Logins**.
- Check whether the user provided in the **AD360 Service** is already in the list.

If not, right click the **Logins**, **New Login** and provide a corresponding user name. The New user must have the **sysadmin server level role** and **database level role of db_owner**.

Follow the steps to provide the sysadmin role permission:

Right click the user, click 'Properties'

Go to 'Server Roles' ---> Check **sysadmin** and click 'OK'

Note:

Details about user roles: Refer the documents in the following links:

For Server Level Roles: <http://msdn.microsoft.com/en-us/library/ms188659.aspx>

For Database Level Roles: <http://msdn.microsoft.com/en-us/library/ms189121.aspx>

Server Role of the user should be 'sysadmin' and Database Role of the user should be 'db_owner'.

The members of **sysadmin server role** can perform any activity in **SQL Server** and have completes control over all database functions.

The members of **db_owner database role** can perform any activity in the database.

MS SQL Server in local computer

Copy the following files to **<AD360 Home>\bin** folder.

- **bcp.exe**- **<MSSQL Installation Dir>\Tools\Binn\bcp.exe**
- **bcp.rll**- **<MSSQL Installation Dir>\Tools\Binn\Resources\1033\bcp.rll**

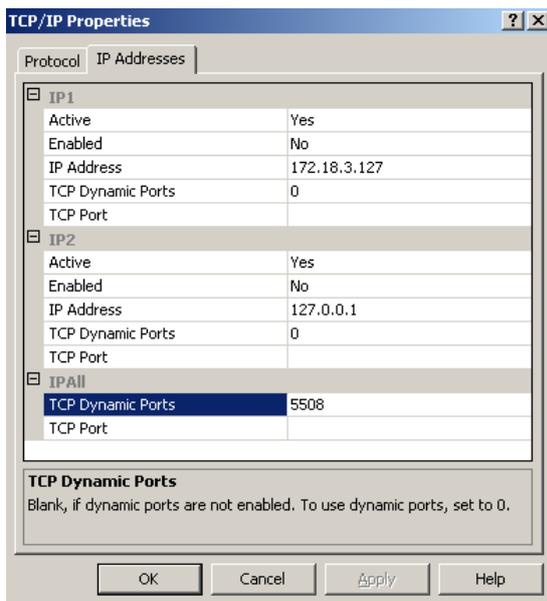
Windows Firewall Settings

If the Firewall is enabled in MS SQL Server machine, the TCP and UDP Ports need to be opened.

UDP Port is normally 1434.

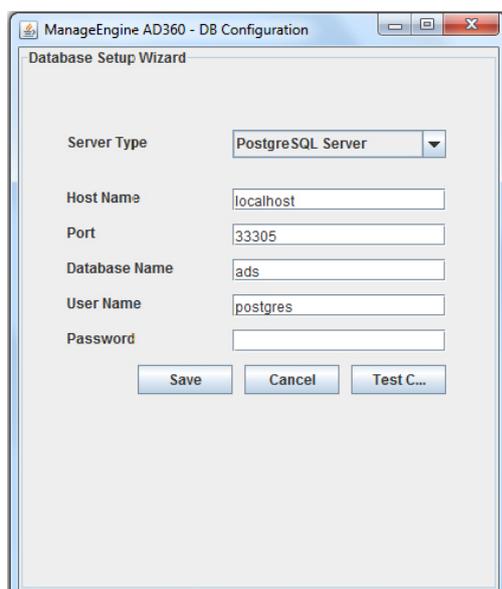
To check TCP Port settings, open SQL Configuration Manager:

- SQL Server Network Configuration ---> Protocols for <instances>
- Right click TCP/IP ---> Properties ---> Goto IP Addresses Tab and scroll until TCP Dynamic Ports and enter the current value in your Firewall.



Invoke the <AD360 Home>\bin\ChangeDB.bat in command prompt to configure the MS SQL SERVER credentials like ServerName, Port, UserName and Password.

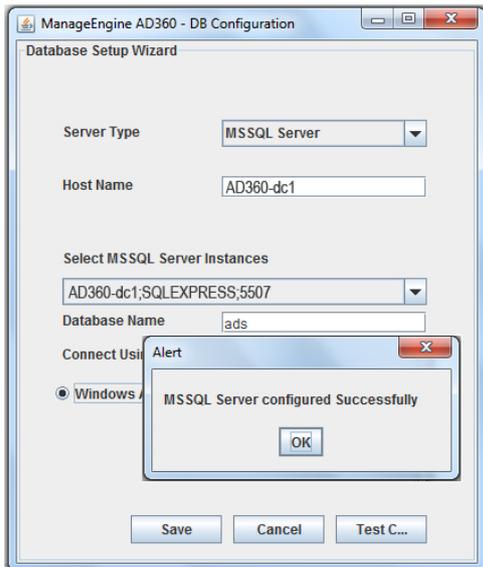
- Database Setup Wizard pops-up.



In the wizard screen, select Server Type as MSSQL Server. Available SQL Server Instances are listed in a combo box. Enter the Host Name and Named instance of the SQL Server from the instances.

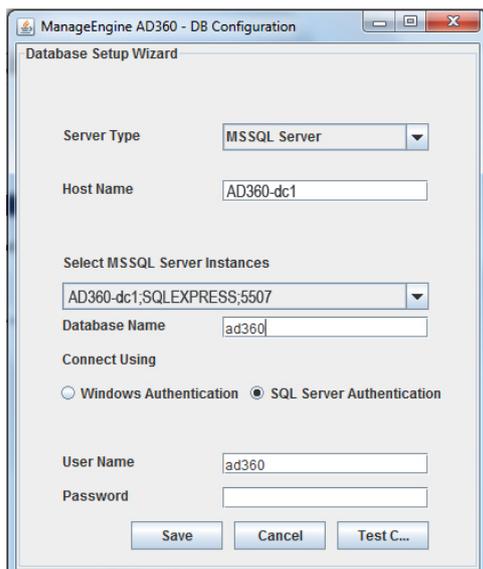
- Select the authentication type using the "Connect Using:" options.
- The options are:
 - Windows Authentication

For Windows Authentication, the credentials of the Domain user are automatically taken



- SQL Server Authentication

For MS SQL Server Authentication, enter the User Name and Password.



- Click Test Connection to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.
- Click Save button to save the MS SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.

Migrating PostgreSQL Data to MS SQL

- Invoke the <AD360 Home>\bin\run.bat to start the AD360 server in the command prompt.
- After the server is started completely, stop the server by terminating the run.bat in the command prompt or invoke the <AD360 Home>\bin\shutdown.bat
- Invoke the <AD360 Home>\bin\restoreDB.bat zipfilename and wait till the database is completely restored. Note: Executing the restoreDB.bat will delete the existing data, if any.
- Start the AD360 Server/Service to work with the MS SQL SERVER as the database.

Dashboard

Important: To be able to view the dashboard of AD360, you have to ensure that the different components of AD360 are setup and that the domain and network settings of each component are configured appropriately. Here's a [checklist](#) of settings to look over to get an unbridled view of the dashboard.

Dashboard is the home page for AD360. It provides a quick snapshot of all essential aspects of the four components in a polished graphical display. The graphical representation helps you to grasp the most important information quickly from the home page itself and take necessary actions with the help of the product. Besides displaying vital information, you can also access important features of different components from the links provided in the right hand side of the dashboard.

Under Dashboard, each of the four components of AD360 has a separate dashboard view. The following information are shown under each tab:

ADManager Plus

The dashboard of 'AD Management' component displays vital information about domain users, machines, and other AD objects like groups and OUs.

The following reports are viewable under this tab:

- User Reports
- System Reports
- Other Reports

ADSelfService Plus

The dashboard of 'Password Self-Service' component provides a comprehensive view of user password and account status, enrollment data, and users' actions inside the Password Self-Service component.

The following reports are viewable under this tab:

- User Reports
- Enrollment Reports
- Audit Reports

ExchangeReporter Plus

An essential snapshot of all the important details of your Exchange environment is captured under the dashboard of 'Exchange Auditing' component.

The following reports are viewable under this tab:

- Server Storage Usage
- Mailbox Size
- Organization Traffic Summary
- Top Server Traffic

To Switch Between Dashboard View of Different Domains:

The dashboard can show the above information for only one domain at a time. To change the dashboard view to display the information of another domain,

Please do the following:

- Go to Dashboard (home page of AD360).
- In the top right corner of Dashboard, you can find a drop down menu 'Select Domain to View'.
- Choose the domain of your choice from the drop down menu to view all the essential information pertaining to that domain.

Admin

The admin tab in AD360 allows you to configure the below settings:

- Administration Settings
- General Settings

Administration Settings

AD360 Integration

- AD Management
- AD Auditing
- Password Self-Service
- Exchange Auditing

To get a complete solution for all your Active Directory challenges and management problems, these four components have to be integrated into AD360. Follow the steps shown below:

Step 1: Download and Install the Components

Note: If you already have the components installed and running, you can skip this step and proceed with Step 2 (Integrate the components)

- 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.

Step2: Integrate the Components

Note: Make sure that all the components are set up and 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 four 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.

Switch between different components of AD360:

Once all the components are integrated, you can switch between each component to access the full feature set that each component offers. You can easily switch between the four components by using the Jump to link provided at the top right corner of the AD360 Web Client. Simply place your mouse pointer over the 'Jump to' link and select the component.

Data Synchronization Across Components

Once the different components of AD360 are integrated, the data related to domain settings, component integration, etc., will be automatically synchronized across each component. This saves a lot of time for the administrators, as they no longer have to configure the same settings across all the four components. Any changes they make in any one of the components will be reflected in the other components also. The data relating to the following configuration settings will be automatically synchronized across all the components of AD360:

Domain Settings:

If you want to add a Domain to all the components in AD360, simply add the domain to any one of the component and it will be automatically added to all the other 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.

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 are 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 runs 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.

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.x.x, then the primary server, standby server and the virtual IP should also lie in the IP range 172.21.x.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.

- Navigate to **Admin** ---> **Administration** ---> **High Availability**.
- Select the component for which you want to configure high availability settings.
- Please check the check box **Enable High Availability** to proceed with configuring the settings.

The screenshot displays the 'High Availability' configuration page in the ManageEngine AD360 interface. The page is divided into a sidebar and a main content area. The sidebar contains navigation links for Administration, General Settings, and Logon Settings. The main content area is titled 'High Availability' and features a form for configuring a High Availability Architecture. The form includes a checkbox for 'Enable High Availability', fields for 'Primary Server URL', 'Standby Server Name/IP', 'Admin Username', 'Password', 'Virtual IP Address', and 'Virtual Host Name'. A diagram on the right illustrates the High Availability Architecture, showing a Web Interface connected to a Primary Server and a Standby Server, which are part of an Application Cluster connected to a Database Server.

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.
- Click **Save**.

Auto Backup/Update

Auto Backup

- 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 backup 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

- 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.

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**.

Logon Settings

Selecting the option Enable Single Sign-on with Active Directory will allow users, who are already authenticated with their Windows domain to automatically log in to AD360.

To enable single sign-on for multiple components and domains, follow the steps listed below:

- Navigate to **Admin** ---> **Administration** ---> **Logon Settings**.
- Mark the check-box **Enable Single-Sign On with Active Directory**.
- Select the components that you wish to enable single sign-on from the **Select Components** drop-down box.

Note: The component will only be displayed if the component supports single sign-on.

- Select the domains that you wish to enable single-sign on from the **Select Domains** drop-down box.
- Click **Save Settings**.

To modify existing single sign-on settings,

- Navigate to **Admin** ---> **Administration** ---> **Logon Settings**.
- Click the  icon in the status column against the domain that you wish to modify the settings.
- Enter the **Computer Name** and **Password** in the respective fields.
- Click on the **Create this computer account in the domain** check-box to create a computer with the entered credentials if it is already not present in the domain.
- Click **Advanced**. If the **DNS Servers** and **DNS Site** are not filled automatically after entering the computer name and password, enter them manually.
- Click **Save**.

To identify the DNS Server IP address:

- Open Command Prompt from a machine belonging to the domain that you have selected
- Type `ipconfig /all` and press enter
- Use the first IP address displayed under DNS Server

To identify the DNS Site:

- Open Active Directory Sites and Services in Active Directory
- Expand the Sites and identify the Site in which the Domain Controller configured under the selected domain appear
- Use the Site name for DNS Site

See the images below for reference.

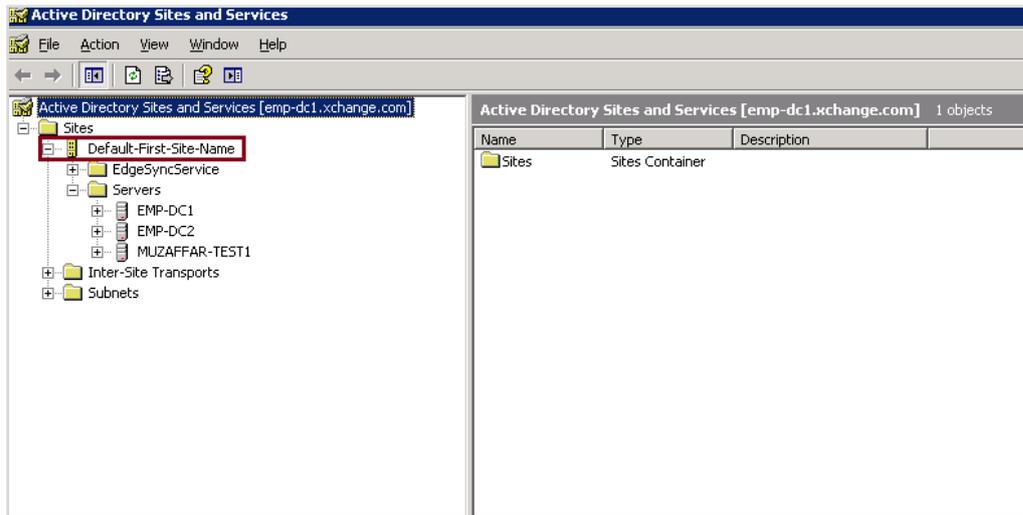
```

c:\ C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\administrator.XCHANGE>ipconfig /all
Windows IP Configuration

Host Name . . . . . : emp-ex03
Primary Dns Suffix . . . . . : xchange.com
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : xchange.com
                                     csez.zohocorpin.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . : 
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-4C-B9-C7
Dhcp Enabled. . . . . : No
IP Address. . . . . : 172.18.3.140
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.18.0.1
DNS Servers . . . . . : 172.18.3.138
  
```



Troubleshooting steps for SSO:

Trusted sites are the sites with which NTLM authentication can occur seamlessly. If SSO has failed, then the most probable cause is that the AD360 URL isn't a part of your browser's trusted sites. Kindly add the AD360 URL in the trusted sites list.

Follow the steps given below:

- Internet Explorer
- Chrome
- Firefox

Note:

1. It is recommended that you close all browser sessions after adding the URL to the trusted sites list for the changes to take effect.
2. Google Chrome and Internet Explorer use the same internet settings. Changing the settings either in Internet Explorer or in Chrome will enable NTLM SSO in both browsers. It is again recommended to close both the browser sessions for the changes to be enabled.

Internet Explorer

1. Open Internet Explorer and click the **Tools** button.
2. Click **Internet options**.
3. In the Internet options dialog box that opens, click the Security tab, and then click a security zone (Local intranet, Trusted sites, or Restricted sites).
4. Click **Sites**.
5. If you are using IE 11, click on the advanced button and add the AD360 site in the list of intranet site.
6. If you are using versions lower than IE 11, add the AD360 site in the list of intranet sites.

7. Click **Close**, and then click **OK**.
8. Close all browser sessions and reopen your browser.

Chrome

1. Open Chrome and click the **Customize and control Google Chrome** icon (3 horizontal lines icon on the far right of the Address bar).
2. Click **Settings**, scroll to the bottom and click the **Show advanced settings** link.
3. Under the **Network** section click **Change proxy settings**.
4. In the Internet Properties dialog box that opens, navigate to the **Security tab** --> Local Intranet, and then click **Sites**.
5. Click **Advanced** and add the URL of AD360 in the list of intranet site.
6. Click **Close**, and then **OK**.
7. Close all browser sessions and reopen your browser.

Chrome

1. Open Firefox web browser and type **about:config** in the address bar.
2. Click **I'll be careful, I promise** in the warning window.
3. In the **Search** field, type: **network.automatic-ntlm-auth.trusted-uris**.
4. Double-click the "network.automatic-ntlm-auth.trusted-uris" preference and type the URL of AD360 in the prompt box. If there are sites already listed, type a comma and then the URL of AD360. Click **OK** to save the changes.
5. Close all browser sessions and reopen your browser.

General Settings

The general settings for AD360 include:

- Personalize
- Product settings
- Server settings

Personalize

AD360 provides administrators the ability to configure the product based on personal preferences and requirements. You can change the password to your account from this section.

You can also modify the date and time format and the time zone.

The following settings are present under Personalize:

- Personalize
- Change Password

Personalize

- Navigate to **Admin** ---> **General Settings** ---> **Personalize**.
- Under Personalize tab, there are two sections:
 - Date & Time Settings
 - General Settings

Date & Time Settings

- Choose the **Language** that you prefer from the drop-down menu of the **Language** field.
- Choose the **Time Zone** and **Date/Time** Format from the drop-down menus of the respective fields.

General Settings

- To **change the logo** of the product, click on **Choose File** button adjacent to the **Change Logo** field.
- In the **Change Browser Title** field, you can edit the **Browser Title** of the product.
- Change the **Browser Favicon** by clicking on the **Choose File** button adjacent to the **Change Browser Favicon** field.
- You can also **hide the 'Forgot Password?' link** in the login page by selecting the **Hide 'Forgot Password?' link in login page** check-box.
- Click **Save Settings**.

Change Password

To change the default AD360 admin account password, follow the steps given below:

- Navigate to **Admin** ---> **General Settings** ---> **Personalize** ---> **Change Password**.
- Under **Change Password** tab, enter the password of the AD360 admin account in the **Old Password** field.
- Now, enter the **new password** and re-enter the same to **confirm your new password** in the respective fields.
- Click on **Change Password** button.

Product Settings

You can change the following settings of AD360 from this tab.

- **Connection Type**
- **General**

Connection Type

- Choose your connection type. You can choose to use either http or https.
- Specify the **Port Number** of your choice after choosing they type of connection.
- Default ports - HTTP : 8082, HTTPS : 8445.
- To enable LDAP SSL, mark the check-box against the **Enable LDAP SSL** field.
- Click **Save** to store the configured settings.

General

- Select the **Session Expiry Time** - time for which the user session would last - from the drop-down box.
- Select the level of logs that is to be collected by the product. The default working mode for Office365 Manager Plus is **Normal** with minimal set of debugging information. Select **Debug** to collect detailed log reports.
- Enable or disable collection of anonymous **Usage Statistics Gathering** to send to us.
- Click **Save** to store the configured settings.

Server 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.

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**.

Send Support Info

AD360 Support

In-order to analyze issues or other challenges faced by evaluators / customers, AD360 product team might request for product logs (Support Information). This will provide the team a clear understanding on the problem / challenge reported.

The creation of the support information can be done either automatically or manually.

Under Dashboard, each of the four components of AD360 has a separate dashboard view. The following information are shown under each tab:

How to automatically create and send information:

- Click on Support Tab ---> Support Info ---> Create System logs: Auto
- This will automatically create a support info file. Note: The time taken for creating the support info file can vary from a few seconds to minutes depending on the logs that have been created by the product over time.
- Once the support info files are ready, save the file locally by clicking on the link provided
- Attach the saved zip file and mail it to ad360-support@manageengine.com
- Alternatively if the file size is large you can upload the saved file to our server by following the below steps.
- Type : <http://bonitas.zohocorp.com/upload/index.jsp> on a web browser
- Select "AD360" from the Product drop down menu
- Provide your Email address
- Add a comment
- Attach the saved support info file from the stored location
- Click on Upload

How to manually create and send Information:

- Go to AD360 installation folder
- Open the bin folder
- Double click on "compressLogFiles.bat" file.
- Go back to the installation folder and open logs\archive folder to find a zip file named in the format: "ssmmHHddMMyyyy".
- Attach the zip file and mail it to ad360-support@manageengine.com
- Alternatively if the file size is large you can upload the saved file to our server by following the below steps.
- Type : <http://bonitas.zohocorp.com/upload/index.jsp> on a web browser
- Select "AD360" from the Product drop down menu
- Provide your Email address
- Add a comment
- Attach the saved support info file from the stored location
- Click on Upload

Knowledge Base

Reset Admin Password

How do I reset the password of the admin account?

To reset your admin password,

- Navigate to <Installation_Dir>\bin folder. By default, the path is C:\ManageEngine\AD360\bin.
- Find and run the resetADSPassword.bat file.
- Your password will now be reset to the default password admin.

Change Admin Password

How do I change the password of the admin account?

To change the password of your admin account,

- Click the  icon located at the top right corner of AD360 window and click Change Password.
- In the change password page, enter the old password. Then, enter the new password and confirm it by keying in the new password in the 'confirm password' field.
- Click **Change Password**.

Alternatively, you can also:

- Click the Admin tab.
- Navigate to **Administration --> Logon Settings --> Change Password**.
- Enter the old and new passwords. Confirm the new password by keying in the new password in the 'confirm password' field.
- Click **Change Password**.

Install AD360 as a Windows service

How do I install AD360 as a Windows service?

After installing AD360, follow these steps to install the product as a service:

- Navigate to **Start menu ---> All Programs**.
- Select **AD360**.
- Click on **NT Service folder**.
- Click on **Install AD360 as a Service**.
- When AD360 is installed as a service, it runs with the privileges of the system account.

Manually Backup and Restore Database

How to manually backup and restore the database in AD360?

To backup the AD360 database,

- Start Command Prompt as an administrator (right-click command prompt and select 'Run as Administrator')
- Navigate to <Installation_Dir>\bin folder by using the cd command. By default, the path to installation directory is C:\ManageEngine\AD360.
- Now, execute the command backupDB.bat to backup the database.
- A folder named Backup will be created at AD360 installation directory (By default: C:\ManageEngine\AD360) and it will contain the DB backup in compressed file format.

To restore a AD360 database,

- Start Command Prompt as an administrator (right-click command prompt and select 'Run as Administrator')
- Navigate to <Installation_Dir>\bin folder by using the cd command. By default, the path to installation directory is C:\ManageEngine\AD360.
- Now, execute the command **restoreDB.bat** to restore the database.
restoreDB.bat compressed_file_name.zip

Migrate Server

How do I move AD360 to a new server?

To move AD360 to a new server. follow the steps listed below.

Note: Please upgrade AD360 to the latest build using the Service Pack before migration. And, do not uninstall AD360 from the old machine until the new installation works fine.

- Navigate to <install_dir>/conf (By default: C:\ManageEngine\AD360\conf)
- Open **database_params.conf** file in a text editor and identify the database that is being used by AD360 in your environment.
- If the database is MySQL or MS SQL, then contact AD360 support for further guidance.
- If the database is PostgreSQL, then continue with the following steps.
- Stop AD360(Start ---> All Programs ---> AD360 ---> Stop AD360 if it running as an application, or Start ---> Run ---> services.msc ---> Stop the 'ManageEngine AD360' if it is running as a service.)
- Open command prompt as administrator.
- Navigate to <Installation directory>\bin
- Run **backupDB.bat** file to back up the database of your current installation. This will create a folder named **Backup** in the installation folder. By default, C:\Program Files\ManageEngine\AD360. This folder will contain the database in compressed file format.

- Backup patch files, if you have any. Take a copy of the Patch folder present in AD360 installation directory (By default: C:\ManageEngine\AD360)
- Stop AD360(Start ---> All Programs ---> AD360 ---> Stop AD360 if it running as an application, or Start ---> Run ---> services.msc ---> Stop the 'ManageEngine AD360' if it is running as a service.)
- Open command prompt as administrator.
- Navigate to <Installation directory>\bin
- Run **backupDB.bat** file to back up the database of your current installation. This will create a folder named **Backup** in the installation folder. By default, C:\Program Files\ManageEngine\AD360. This folder will contain the database in compressed file format.
- Backup patch files, if you have any. Take a copy of the Patch folder present in AD360 installation directory (By default: C:\ManageEngine\AD360)Download and install the build of the same number on the new server.
- Stop AD360 after installation on the new server.
- Paste the Patch folder under the AD360 installation directory (By default: C:\ManageEngine\AD360)
- Copy and paste the compressed database backup file created from the old installation in the following location on the new server: <Installation directory>\AD360\bin (By default: C:\ManageEngine\AD360\bin)
- In the new server, open the command prompt as an administrator.
- Navigate to <Installation_Dir>bin.
- Execute the 'restoreDB.bat' file from the command prompt using the compressed DB file. For example: restoreDB.bat compressed_file_name.zip
- Start AD360. (Start ---> All Programs ---> AD360 ---> Start AD360)

Change Port

How do I change the port number of AD360?

To change the port number in AD360,

- Click **Admin** tab.
- Navigate to **General Settings** ---> **Product Settings**.
- If you wish to use **HTTP**, select the **HTTP** field under **Connection Type**, enter the new port number.
- If you wish to enable the secure socket layer, select **HTTPS** and enter the appropriate port number.
- Click **Save**.
- Restart AD360 for the changes to take effect.

Troubleshooting Tips

- **Installing AD360**
 - Access Denied
- **AD360 Integration**
 - When I try to integrate a component, I get this error **Server is down. Make sure the component's server is up and running.**
 - When I try to integrate a component, I get this error **Incompatible component. Please check whether the component's version is compatible with AD360.**
 - Super Admin credential is required for components installed on a remote host.
 - Incorrect Server Details
 - Please try after updating the component settings in AD360.
 - Communication Failure
 - Invalid Component Details
 - Invalid Server URL
- **Dashboard**
 - **Unable to view one or more of the components' dashboard.**
- **Product Settings**
 - Please enter a HTTP port number that is not used by other applications.

Access Denied

If the operating system that you use is Windows Vista or later, ensure that User Account Control is disabled. Enabling UAC will allow just the administrator to install the software.

To disable UAC, follow the steps given below:

Select Control Panel ---> User Account

- **For Windows 7 and Windows 2008 R2,**
 - Click 'User Account Control' Settings link.
 - This will open the User Account Control Settings dialog showing the control level.
 - Drag the control level to 'Never Notify' and click OK
- **For Windows Vista and Windows 2008**
 - Click 'Turn User Account Settings On or Off' link.
 - Uncheck the 'Use User Account Control (UAC) to protect your computer' option and click OK.

When I try to integrate a component, I get this error Server is down. Make sure the component's server is up and running.

This error occurs when the component you are trying to integrate is not running.

Make sure that you have installed the component that you are trying to integrate with AD360 and that the component is running.

If not go to Start ---> All Programs ---> Click XYZ ---> Click Start XYZ. Here XYZ is the component's name.

When I try to integrate a component, I get this error Incompatible component. Please check whether the component's version is compatible with AD360.

This error occurs when the version of a component that you are trying to integrate is lower/higher than the version supported by the version of your AD360.

Update the component or AD360 to the latest version.

Super Admin credential is required for components installed on a remote host.

When you try to integrate a component that has been installed on a remote host, you will need the credentials of the super administrator of the installed component.

Please enter the credentials of the super admin to proceed with the integration.

Incorrect Server Details

The server details that you have entered belongs to a different component. Ensure that the values you have entered belongs to the selected component and try again.

Please try after updating the component settings in AD360.

To rectify this issue, follow the steps listed below:

- Navigate to **Admin --> Administration --> AD360 Integration**. You will be presented with four tabs each representing a component of AD360.
- Click on the component that has to be fixed.
- 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 **Update Settings**.

Please try after updating the component settings in AD360.

To rectify this issue, follow the steps listed below:

- Navigate to **Admin --> Administration --> AD360 Integration**. You will be presented with four tabs each representing a component of AD360.
- Click on the component that has to be fixed.
- 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 **Update Settings**.

Communication Failure

Ensure that the product has a valid SSL certificate and that SSL 3.0 is disabled.

If the problem still persists, contact ad360-support@manageengine.com

Invalid Component Details

This error occurs when you have two or more instances of the same component installed in your environment, and you try to integrate the second component with AD360.

To integrate the second component, follow the steps listed below:

- Navigate to **Admin --> Administration --> AD360 Integration**.
- Select the component that you wish to integrate with AD360.
- To add the new component, remove the existing component from AD360 by clicking on **Remove** and then click **OK**.
- Now, enter the **Server Name** and **Port Number** of the component to be added and click **Integrate Now**.

The component will now be integrated with AD360.

Invalid Server URL

Check the server URL that you have entered.

- Enter the **Server Name or IP** and **Port Number** of the server from which that particular component is running in the respective text boxes.
- Select the **Connection Protocol** from the drop down menu.
- Click **Integrate Now**.

Unable to view one or more of the components' dashboard.

Following are the list of situations that may hinder the dashboard view of the components:

- **Component Setup:** To view the dashboard of AD360, you must first download and install its components. Only when a component is installed and integrated with AD360, you can view its dashboard. If you have already installed the component, make sure that any change made to the hostname and port number of a component is reflected under the AD360 integration tab in Administration settings of AD360. [Click here to learn more about installing and integrating the components with AD360.](#)
- **Domain Selection:** It is possible to configure different domains with different components. As you switch between the dashboard views of different components, make sure that the domain that you have configured with that component is selected. Also, make sure that you have logged in with the appropriate credentials to view the dashboard of the domain you have selected.

Please enter a HTTP port number that is not used by other applications.

Description:

This error may occur when you are trying to enable HTTPS. When you try to enable HTTPS, AD360 will automatically assign a port number for HTTP based on the HTTPS port number you've chosen. And if that new HTTP port number is used by some other application, then this error occurs.

Solution:

- Once you get the error, select **HTTP**.
- Change the port number to something that is not in use by another application.
- Now, select **HTTPS**.
- Click **Save**.

SSL Troubleshooting Tips

This section will help you to troubleshoot any SSL server certificate related issues that you might encounter in the product.

Error Messages:

- [Blocked Content](#)
- [Certificate Name mismatch](#)
- [Hostname mismatch](#)
- [Invalid Certificate](#)

Blocked Content

Description:

This problem arises when AD360 is configured to use HTTPS under connection settings and integrated component is configured to use HTTP. As a result, you will not be able to access the component from the apps pane.

Resolution:

If AD360 is configured with HTTPS, then you must configure the integrated components to use HTTPS (SSL) to successfully access the components from the apps pane.

Certificate Name mismatch

Description:

This error occurs when the common name of the SSL Certificate doesn't exactly match the hostname of the server in which the component is installed.

Resolution:

Please get a new SSL certificate for the current hostname of the server in which the component is installed.

Hostname mismatch

Description:

This error occurs when the component's SSL certificate is issued for a hostname that is different from the AD360's hostname. For example, AD360 could be installed on a parent domain and the component could be running on a child domain.

Resolution:

In this scenario, you can configure a valid SSL wildcard certificate and apply it to both the component and AD360.

Invalid Certificate

Description:

This error occurs when the SSL certificate you have configured with the component is invalid. A certificate can become invalid if it has expired or other reasons.

Resolution:

Please configure the component to use a valid SSL certificate.

FAQ

- General
- License
- Advanced

General

1. What is AD360?

ManageEngine AD360 is a 100% web-based product that provides a complete solution to all your Windows Active Directory challenges and management problems. With AD360 you can perform the following tasks:

- Active Directory Management
- Active Directory Auditing
- Password Self-Service for end-users
- Exchange Analysis and Reports

2. What operating systems are supported by AD360?

AD360 support the following Windows operating systems:

- 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 & above)

3. AD360 runs in a web browser. Does that mean I can access it from anywhere?

Yes, you can connect to the AD360 from any machine on the network through a Web browser.

4. Do I need any prerequisite software to be installed before using AD360?

No, AD360 do not require any prerequisite software to be installed. You need to have only the four components of AD360 installed and running to enjoy all the benefits of the product.

5. Can AD360 work if DCOM is disabled on remote systems?

Yes, AD360 does not use the DCOM service to perform the tasks.

License

1. What are the different editions of AD360?

AD360 is available as a free download with a 60 day trial period. Once the trial expires, you have to purchase and apply the Professional or Standard Edition license. [Click here](#) to identify which edition of AD360 suits you best

2. How can I upgrade to a higher edition?

From any edition, you can upgrade to the required higher edition by obtaining the appropriate license from ZOHO Corp.

Advanced

1. How do I move AD360 to a different machine? (Migration)

Please follow the steps given below:

Note: Steps 5 and 7 are applicable only if the existing build is migrated from the older version build.

- Stop AD360 which is running currently.
- Go to the <installation directory> \ bin \
- Run the file "backupDB.bat". This will create a backup of the existing database files in zip format under <installation directory> \ backup \.
- Take this zip file (<existing_db_zip_name>) and copy it to the new server.
- Take a copy of "specs.xml" present under <installation directory> \ Patch \ and copy it to the new server
- Install the same version of AD360 (the version you have in the existing server) in the new server
- Ensure that the application has started and then stop AD360.
- Create a folder named "patch" under installation directory and copy the "specs.xml" under this folder
- Go to the <installation directory> \ bin \. Open a command prompt.
- Type - restoreDB.bat <existing_db_zip_name> and enter. This will restore the previous settings.
- After the restore process is completed, start AD360.

Note: Ensure that you retain the existing installation of AD360 until the new installation of AD360 is working as intended.

Contact Us

SALES ENQUIRIES:

Toll Free : +1 844 245 1101

SUPPORT ENQUIRIES:

Toll Free : +1-888-720-9500

OFFICES

USA - California

Zoho Corporation
4141 Hacienda Drive
Pleasanton,
California 94588, USA

INDIA - Chennai

Zoho Corporation Pvt. Ltd.,
Estancia IT Park,
Plot No. 140 & 151, GST Road,
Vallancherry Village,
Chengalpattu Taluk,
Kanchipuram District 603 202, INDIA
Ph : 044 - 67447070 / 71817070
Fax : 044 67447172

Sales

To purchase ManageEngine Office365 Manager Plus from any part of the world, you can fill out the [Sales Request Form](#). Our sales executive will contact you shortly. You can also send us an email at sales@manageengine.com.

Technical Support

One of the value propositions of ZOHO Corp. to its customers is excellent support. During the evaluation phase the support program is extended to you free of charge.

Please send your technical queries to ad360-support@manageengine.com

Alternatively, from within the product, select the Support tab. It has the following options that will allow you to reach us:

- Request Support - Submit your technical queries online.
- Need Features - Request for new features in AD360.
- User Forums - Participate in a discussion with other AD360 users.
- Live Chat - Get instant response to your queries.
- Contact Us - Speak to our technical team using the toll free number (+1-888-720-9500)