

# User Guide



ManageEngine  
**ADManager**<sup>plus</sup>

## Table Of Contents

<b>WELCOME TO MANAGEENGINE ADMANAGER PLUS .....</b>	<b>5</b>
Release Notes .....	7
Contacting ZOHO Corp. ....	8
<b>TECHNOLOGY OVERVIEW.....</b>	<b>10</b>
Active Directory Overview.....	11
Active Directory Terminologies .....	13
<b>GETTING STARTED .....</b>	<b>14</b>
System Requirements .....	15
Installing ADManager Plus .....	16
ADManager Plus Deployment Scenarios .....	18
Working with ADManager Plus .....	21
Installing Service Packs.....	23
Uninstalling Service Packs .....	24
Licensing ADManager Plus .....	25
Dashboard View .....	26
Configuring Domains .....	27
<b>CSV IMPORT .....</b>	<b>28</b>
Users Creation in Active Directory by Import CSV .....	29
Modify Active Directory Users Properties/ Attributes by Import CSV.....	31
Create Contacts in Active Directory .....	33
Modify Contacts in Active Directory Using CSV .....	34
Delete Contacts .....	35
Create Group in Active Directory Using CSV .....	36
Modify Group in Active Directory .....	37
<b>ACTIVE DIRECTORY MANAGEMENT .....</b>	<b>38</b>
Active Directory User Management .....	39
Create Users.....	40
Creating a Single User .....	41
Creating Bulk Users .....	43
Users Creation in Active Directory by Import CSV .....	45
Active Directory Additional Attributes .....	47

Modify Users .....	48
Modify Active Directory Users Properties/Attributes by Import CSV .....	49
Active Directory Single User Modification.....	51
Bulk User Modifications .....	52
Modifying General User Attributes .....	53
Resetting Password .....	54
Modifying Naming Attributes .....	55
Modifying Security Attributes .....	56
Modifying Organization Attributes .....	57
Modifying Profile Attributes.....	58
Modifying Contact Attributes .....	59
Modifying Group Attributes .....	60
Move Users to a Different Container .....	61
Modify Logon Workstation .....	62
Modifying Inheritable Permissions.....	63
Move Home Folders .....	64
Modify Custom Attributes .....	65
Delete users .....	66
Dial-in or VPN properties.....	67
Modifying Terminal Services .....	68
Modifying Terminal Services Attributes .....	68
Modifying User Profiles .....	69
Modifying Environmental Variables .....	70
Modifying Session Attributes .....	71
Modifying Remote Control Attributes.....	72
Creating User Templates .....	73
Searching Users, Groups, and Computers.....	77
Active Directory Computer Management.....	78
Enable-Disable Computers .....	79
Modifying General Attributes .....	80
Modifying Group Attributes .....	81
Move Computers.....	82
Active Directory Group Management.....	83
Active Directory Group Management.....	83
Single Group Management.....	84
Bulk Group Management.....	85
CSV Based Group Management .....	87

Active Directory Contact Management .....	88
Create Contacts in Active Directory.....	89
Bulk Contacts Modification .....	90
Address/Organization Attributes.....	91
Naming Attributes.....	92
Contact Attributes.....	93
Modify Contacts in Active Directory Using CSV .....	94
Delete Contacts.....	95
Active Directory Exchange Management.....	96
Modifying Delivery Restrictions.....	97
Modifying SMTP Address .....	98
Modifying Delivery Options .....	100
Modifying Storage Limits.....	101
Modifying Naming Attributes.....	102
Modifying Exchange Features .....	103
Creating Mailbox to Users .....	104
Exchange Off-line Address Book.....	105
<b>ACTIVE DIRECTORY REPORTS.....</b>	<b>106</b>
Active Directory User Reports .....	107
Active Directory Contacts Reports.....	115
Active Directory Password Reports .....	116
Active Directory Group Reports .....	118
Active Directory Computer Reports .....	121
<b>ACTIVE DIRECTORY EXCHANGE REPORTS .....</b>	<b>124</b>
Active Directory Terminal Services Reports .....	130
Active Directory GPO Reports .....	131
Active Directory OU Reports.....	134
<b>ACTIVE DIRECTORY NTFS REPORTS .....</b>	<b>136</b>
Active Directory Security Reports .....	138
Active Directory Policy Reports .....	140
Scheduling Reports .....	141
Audit Logs.....	144
Help Desk Delegation Overview .....	145
Help Desk delegation.....	146
Help Desk Reset Password Console.....	151

<b>ACTIVE DIRECTORY DELEGATION.....</b>	<b>152</b>
Creating Security Roles .....	153
Viewing Security Roles .....	154
Modifying Security Roles .....	155
Applying Security Roles.....	156
Built-in Security Roles.....	157
<b>ADMIN SETTINGS.....</b>	<b>158</b>
Customizing Naming Format .....	159
Titles & Departments .....	160
Offices & Companies .....	161
Customizing Password Settings .....	162
Customizing LDAP Attributes .....	163
Customizing Delete Policy .....	164
AD Search Settings .....	165
Connection Settings.....	166
Server Settings .....	167
Configure Mail Server .....	168
Personalize Settings .....	169
ServiceDesk Settings.....	170
<b>WEB BASED PEOPLE SEARCH.....</b>	<b>171</b>
<b>SEARCHING SECURITY PERMISSIONS.....</b>	<b>172</b>
<b>ACTIVE DIRECTORY EXPLORER .....</b>	<b>173</b>
<b>TROUBLESHOOTING TIPS.....</b>	<b>174</b>
<b>FAQ.....</b>	<b>180</b>
<b>KNOWN ISSUES AND LIMITATIONS.....</b>	<b>185</b>
<b>ADMP - ADSSP INTEGRATION.....</b>	<b>186</b>

# Welcome To ManageEngine ADManager Plus

---

Managing the Active Directory is an open challenge that every IT administrator faces in his day-to-day activities. Manually configuring the users and security permissions is extremely time consuming, tiresome, and error prone, particularly in large, complex windows networks. Moreover, it is essential to have an in-depth knowledge about the Active Directory to accomplish these tasks.

ManageEngine ADManager Plus offers a 100% web-based solution to meet your Active Directory management requirements. It allows you to create or modify multiple users in the Active Directory by hiding the complexities of the native Active Directory features. With its role-based security model, you can efficiently manage the security permissions with ease. The comprehensive reports provide you a quick insight in to the Active Directory objects.

The powerful search facility allows you to determine the permissions granted for a specific Active Directory object. The search can be made on a specific AD object, for a specific user and based on the permissions the user has. This lets you to perform an audit for the defined security permissions for a specific AD object or for a specific user.

The Active Directory Explorer lets you browse through the Active directory for any of the domains. You can view the properties and security permissions of the various AD objects of that domain.

The following sections will help you to get familiar with the product:

- [Technology Overview](#): Provides a brief introduction to Windows Active Directory.
- [Getting Started](#): Provides you the details of system requirements, product installation and start up.
- [Configuring Domains](#): Helps you in configuring your domains to manage using ADManager Plus
- [Personalizing the Client](#): Helps you to set your preferences like changing password, themes, etc.
- [Active Directory User Management](#): Explains the various ways to create user accounts in the Active Directory using ADManager Plus.
- [Active Directory Reports](#): Helps you to view the reports of the Active Directory infrastructure components.
- [Active Directory Delegation](#): Explains the creation and delegation of security roles to grant/revoke permissions to the security principals.
- [Help Desk Delegation](#): Allows delegation of administrative tasks to non-administrative users in a secured way with a defined scope.
- [Self Service Portal](#): Helps users update their contact information.

- [Searching Security Permissions](#): Enables searching ACEs to determine the permissions of the security principals.
- [Active Directory Explorer](#): Enables you to view the Active Directory in the Windows explorer format.
- [Troubleshooting Tips](#): Helps you to troubleshoot the problems with the product.
- [FAQ](#): Provides a set of frequently asked questions to clarify your product related queries.
- [Known Issues and Limitations](#): Provides the limitations and the known issues of ADManager Plus.

# Release Notes

---

The key features of this release comprise the following:

## 1. User Management

- Create Users in different OUs using CSV Import
- Modify SMTP Address for Users

## 2. Contact Management

- Delete Contacts

## 3. Reports

- Users not in a Group
- Members of Domain Users Group Only
- Users with Change Password at Next Logon
- IMAP4 Enabled Users
- POP3 Enabled Users
- OMA Disabled Users
- Customize column settings for Scheduled Reports
- Shares in the Servers
- Permissions for Folders
- Folders accessible by Accounts
- AD Objects accessible by Accounts
- Subnets accessible by Accounts
- Servers accessible by Accounts
- Subnet Permissions
- Server Permissions

## 4. HelpDesk Delegation

- Restrict Reports viewable by HelpDesk
- Multiple roles can be Delegated to a Single Technician

## 5. Admin Settings

- Disable Forgot Password Link on Logon Page
- Create Customized "Offices/Companies" for your Organization

## 6. General

- Windows Server 2008 Support



## Contacting ZOHO Corp.

---

- [ZOHO Corp.](#)
  - [Sales](#)
  - [Technical Support](#)
- 

### ZOHO Corp.

<b>Web site</b>	<a href="http://www.zohocorp.com">www.zohocorp.com</a>
<b>ZOHO Corp. Headquarters</b>	ZOHO Corp., Inc. 4141, Hacienda Drive Pleasanton, CA 94588 USA Phone: +1-925-924-9500 Fax : +1-925-924-9600 E-mail: <a href="mailto:info@zohocorp.com">info@zohocorp.com</a>
<b>ZOHO Development Centre</b>	ZOHO Corporation Private Limited DLF IT Park, Block 7, Ground floor, No. 1/124, Shivaji Garden, Nandambakkam Post, Mount PH Road, Ramapuram, Chennai 600 089, INDIA  Email: <a href="mailto:sales@manageengine.com">sales@manageengine.com</a>

### Sales

To purchase ManageEngine ADManager Plus from any part of the world, you can fill out the Sales Request [Form](#). A sales person will contact you shortly. You can also send us an e-mail at [sales@manageengine.com](mailto:sales@manageengine.com).

You can also call the ZOHO Corp at the following numbers: Phone: +1-925-924-9500  
 Fax: +1-925-924-9600 and request for Sales

### 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 [support@admanagerplus.com](mailto:support@admanagerplus.com)

Following is the support format to be enclosed, while sending support mails:

- Edition ( Free or Professional Edition) of the product
- Operating System version, such as Win 2000, 2003, etc.
- Browser version, such as Netscape 7.0, IE 5.5, etc.
- Details of the problem
- Steps to reproduce the problem.

Alternatively, select the **Support** tab from the client window. 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 ADManager Plus.
- User Forums - Participate in a discussion with other ADManager Plus users.
- Contact Us - Speak to our technical team using the toll free number (1-888-720-9500)

## Technology Overview

---

To get started with ManageEngine ADManager Plus it is essential to be familiar with basics of Windows Active Directory and Group Policy. Read the following sections for more details. If you are familiar with the basics, you can skip this section.

- [Active Directory Overview](#)
- [Active Directory Terminologies](#)

## Active Directory Overview

---

The Windows Active Directory is a hierarchical framework of objects. This provides information of the various Active Directory objects, such as resources, services, user accounts, groups, and so on, and sets the access permission and security on these objects. The structure of the Active Directory network components are:

- **Domains:** A group of computers that share a common directory database.
- **Domain Trees:** One or more domains that share a contiguous namespace.
- **Domain Forests:** One or more domain trees that share common directory information.
- **Organization Units:** A container or a subgroup of domains that is used to organize the objects within a domain into a logical administrative group.
- **Objects:** The objects represent single entities, such as computers, resources, users, applications, and so on, with their attributes.

### Active Directory Groups

Groups are the Active Directory objects that can contain the users, computers, and other groups (nested groups). There are two types of groups, namely, Security Groups and Distribution Groups. While a security group is used to group users, computers, and other groups to assign permissions to resources, the distribution group is used only to create e-mail distribution lists. The scope of the group can be Local, Domain Local, Global, or Universal.

- **Local Groups:** Its scope is limited only to the machine on which it exists. It can be used to grant permissions to access the machine resources.
- **Domain Local Groups:** It has domain-wide scope, meaning, it can grant resource permissions on any of the windows machines in that domain.
- **Global Groups:** It also has domain-wide scope, but, can be granted permissions in any domain.
- **Universal Groups:** This group can be granted permissions in any domain, including domains in other forests (based on trust relationship).

### Active Directory Users

A User, in order to logon to a computer or a domain, requires an user account in the Active Directory, which establishes an identity for him/her. Based on this identity, the operating system authenticates the user and grant access to the domain resources. There are two pre-defined user accounts, administrator and guest, that are used to logon initially to make the necessary configurations.

### Active Directory Computers

Similar to user accounts, the computer accounts are used to provide necessary authorization to the computers for using the network and domain resources.

### Managing Security Permissions

The basic security permissions supported by Windows, such as Read, Write, and Full Control, are available to each and every objects on the Active Directory. Apart from these standard permissions, AD also provides some special permissions based on the

object class, such as List contents, Delete Tree, List Object, Write Self, Control Access, Create Child, Delete Child, Read Property, Write Property, and so on.

These permissions have to be assigned to the users or groups to restrict or grant access to the Active Directory objects. Each assignment of permissions to users or groups is referred to as Access Control Entry (ACE).

## **Inherited Permissions**

Permissions set on a container (or a parent object) can be applied to its child objects as well. This is referred to as inherited permissions. The Active Directory security model allows you to define explicit permissions or propagate permissions to its child objects. For example, you specify the following conditions for propagation:

- This object only
- This object and all child objects
- Computer objects
- Group objects
- Organizational unit objects
- User objects

Containers can be any Active Directory components like Domain, Organizational Units and only objects within those containers can inherit permissions from the parent.

Some commonly used [Active Directory terminologies](#) are discussed in the next topic.

## Active Directory Terminologies

---

Some of the commonly used Active Directory terminologies and their definitions are given below:

**Discretionary Access Control Lists (DACLS)** - The part of the security descriptor of the Active Directory object that grants or denies access to the object. Only the owner of the object can change the permissions in the DACL.

**System Access Control Lists (SACLs)** - The part of the security descriptor of the Active Directory objects that specify the events, such as file access, system shutdowns, and so on, that have to be audited on a per-user or per-group basis.

**Access Control Entries (ACEs)** - An entry in the object's access control lists that determines security principles and the permissions associated with it.

**Security Identifiers (SIDs)** - A unique number associated with each User account, Group, and Computer account. The Windows internal processes refer to these SIDs rather than the account or group names to uniquely identify these objects.

**Security Descriptors** - The data structure associated with the Active Directory object that specifies the permissions granted or denied to the users and groups (DACL) and the owner of the object. It also specifies the events that have to be audited (SACL).

**Security Principals** - Active Directory objects, such as Users, Groups, and Computers, that have an Security ID associated with it is referred to as Security Principals.

## Getting Started

---

The following sections describes how to get started with ADManager Plus.

- [System Requirements](#)
- [Installing ADManager Plus](#)
- [Working with ADManager Plus](#)
- [Installing Service Packs](#)
- [Uninstalling Service Packs](#)
- [Licensing ADManager Plus](#)

## System Requirements

- 
- [Hardware Requirements](#)
  - [Software Requirements](#)
- 

### Hardware Requirements

Hardware	Recommended
Processor	P4 - 1.0 GHz
RAM	512 MB
Disk Space	200 MB

### Software Requirements

#### Supported Platforms

ManageEngine ADManager Plus supports the following Microsoft Windows operating system versions:

- Windows 2000.
- Windows XP.
- Windows 2003.
- Windows Vista.

#### Supported Browsers

ManageEngine ADManager Plus requires one of the following browsers to be installed in the system for working with the client.

- Internet Explorer 5.5 and above
- Netscape 7.0 and above
- Mozilla 1.5 and above
- Firefox 1.5 and above

Preferred screen resolution 1024 x 768 pixels or higher.



# Installing ADManager Plus

- [Installing ADManager Plus](#)
- [Uninstalling ADManager Plus](#)

## Installing ADManager Plus

ADManager Plus is distributed in the EXE format. ADManager Plus can be installed in any machine in the domain with the specified [system requirements](#). You can install ADManager Plus as:

- [An Application](#)
- [A Windows Service](#)

### Installing ADManager Plus as an Application

By Default ADManager Plus will be installed as an application, run the self-extracting EXE and follow the instructions.

When ADManager Plus is installed as an Application, starting ADManager Plus runs with the privileges of the user who has logged on to the system.

### ADManager Plus as a Windows Service

To run ADManager Plus as a service. Do the following steps after installing.

1. Go to Start Menu
2. All Programs
3. Select ADManager Plus
4. Select NT Service
5. Select Install ADMP Service

When ADManager Plus is installed as a service, starting ADManager Plus runs with the privileges of the system account.



**Note:** Ensure that you have necessary privileges to install and run the product:

1. For using the AD Reports module, ordinary user privilege is sufficient.
2. For performing the AD Management operations, such as create, modify users, etc., administrator privilege or a user with necessary privilege to perform these tasks is required.
3. You can modify the [Domain Settings](#) and change the user credentials that ADManager Plus has to use. This credential will be used irrespective of whether it is installed as a service or an application.
4. If you are using Vista ensure that 'user account control' is disabled. Because enabling 'user account control' will allow only administrator to install the software.



## Uninstalling ADManager Plus

To uninstall ADManager Plus , select **Start --> Programs --> ADManager Plus --> Uninstall ADManager Plus**.

## ADManager Plus Deployment Scenarios

---

- [Enable SSL for Secure Communication over the Internet](#)
  - [Configuring ADManager Plus to Securely Function in a De-militarized Zone \(DMZ\)](#)
  - [Open -up selective Firewall Ports to facilitate access over the Internet](#)
  - [Protocols and Ports Used](#)
- 

### Enable SSL for Secure Communication over the Internet:

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

- Logon to the "ADManager Plus Admin Login" by providing proper admin credentials.
- Click on the "Admin" tab ==> "Connection".
- Put a tick on the box provided near "Enable SSL Port [https]"
- Click on the "Save" to save the settings and restart ADManager Plus.

This will enable SSL and a secure communication by ADManager Plus over the internet is possible. A valid SSL certificate is to be applied for enabling SSL.

### Configuring ADManager Plus to Securely Function in a De-militarized Zone (DMZ)

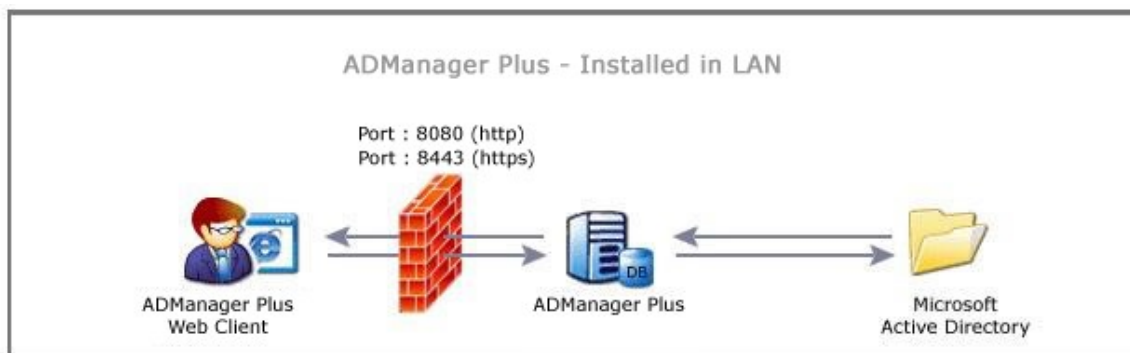
For ADManager Plus to be installed in the DMZ (Demilitarized Zone), Port "389" (to communicate with the LDAP Protocol) and Port "135" (to communicate with RPC) are to be opened up in the Firewall along with other dynamic ports.

Section: "Find all Dynamic Ports" highlights the steps for identifying dynamic ports that needs to be opened up in the firewall. We strongly recommend you to run ADManager Plus application in Secure Socket Layer (SSL) mode for a DMZ Server Installation. Check the above section on how to [enable SSL](#).

### Open -up selective Firewall Ports to facilitate access over the Internet :

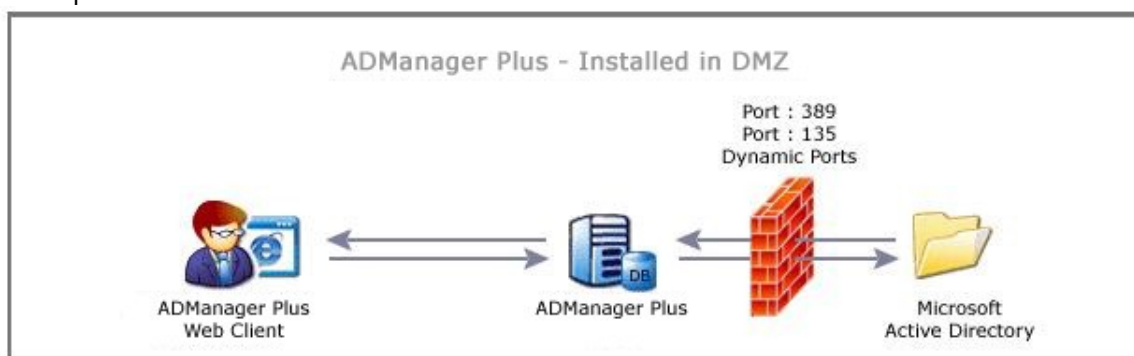
(i) When ADManager Plus is installed on your local area network with the url accessible across internet :

- Open the port on which ADManager Plus is running. By default ADManager Plus runs on port 8080 and it is configurable.



(ii) When ADManager Plus is installed in the DMZ, open the following ports in the Firewall:

- Port "389" to communicate with the LDAP Protocol.
- Port "135" to communicate with RPC.
- Refer section: "[Find Dynamic Ports](#)" for other dynamic ports that needs to be opened in the Firewall. These will be used for communication between AD and ADManager Plus.



## Protocols and Ports Used

ADManager Plus uses Windows ADSI (Active Directory Service Interfaces) to interact with the Active Directory, which in turn uses LDAP (for querying and modifying directory services running over TCP/IP) Protocol on Port 389.

Right now, ADManager Plus communicates with the Active Directory using normal LDAP connection. And we have planned to use secured LDAP connections.

## Finding / Identifying Dynamic Ports:

ADManager Plus uses several other ports which are dynamic. It is required by an administrator to identify all available dynamic ports and open them up in the Firewall. In-order to open-up dynamic firewall ports one can follow the below steps.

Step 1: Open a command prompt in the Domain Controller.

Step 2: Type the following command and execute it in the command prompt.

```
portqry -n "<Your_Domain_Controller_Name>" -e 135 -l resultPorts.txt
```

In case you use different port for RPC, use the Port Number in which your RPC is running by replacing 135 in the above command.

Step 3: After executing the above command, open the "resultPorts.txt" from where the command is executed.

Step 4: Find for all the "\_tcp" in the "resultPorts.txt" (Ex :  
ncacn\_ip\_tcp:100.190.1.2[1142])

Step 5 : The value in the Square Brackets[ ] are the ports which needs to be opened. Make a note of these ports. (Ex: in the above result, 1142 is the port that needs to be opened).

Step 6: Continue with the search until the file ends and open all the identified ports.

## Working with ADManager Plus

---

- [Starting ADManager Plus](#)
  - [Launching ADManager Plus Client](#)
  - [Stopping ADManager Plus](#)
- 

### Starting ADManager Plus

ADManager Plus can be started either in the system account (when run as service) or in user account (when run as application).

#### When ADManager Plus is installed as a Service

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

To start ADManager Plus in the **system account**, select **Start --> Programs --> ADManager Plus--> Start ADManager Plus**

To start ADManager Plus in the **user account**, double-click the ADManager Plus desktop icon.

#### When ADManager Plus is not installed as a Service

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

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

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

1. mysqld-nt - Database server
2. Java(TM) 2 Platform Standard Edition binary - Java.

You should **Unblock** these programs to start ADManager Plus.



Fig: MySQL Alert



Fig: Java Alert

## Launching ADManager Plus Client

To launch the ADManager Plus client,

1. open a Web browser and type **http://hostname:8080** in the address bar. Here the hostname refers to the DNS name of the machine where ADManager Plus is running.
2. Specify the user name and password as **admin** (for first time users) in the respective fields and click **Login**. If you have [changed the password](#), you should use the changed password to login.

## Stopping ADManager Plus

To stop ADManager Plus, select **Start --> Programs --> ADManager Plus--> Stop ADManager Plus**

## Installing Service Packs

---

ZOHO Corp. periodically provides Service Packs which provide new features (requested by the customers), fixes for certain bugs and document updates in the form of HTML files. Service Packs can be downloaded from the Web site, and updated into ManageEngine ADManager Plus using the Update Manager tool.



**Note:** Ensure that no application is running when applying the Service Pack. This prevents any files used by the application from being over-written. For example if the ADManager Plus is running, stop the server and then install the service pack.

The steps to apply a Service Pack are as follows:

1. Start Update manager by executing the script **UpdateManager.bat** file located in *<ADManager Plus Home>/bin* directory.
2. Click **Browse** and select the Service Pack file (.ppm) to be installed. Click **Install** to install the Service Pack.
3. You can go through the Readme file of the Service Pack by clicking the **Readme** button.



**Note:** On clicking **Install**, the tool checks whether there is enough space for the installation of the service pack. If there is no enough space, the tool informs you about the lack of space. You must clear the space and then proceed with the installation.



## Uninstalling Service Packs

---

You have the option of reverting the changes incorporated by the installation of a Service Pack. You can revert to the previous version of the Service Pack or to the base version of the application. Before you start the un-installation process, make sure no application is running.

The steps to revert to a previous version are as follows.

1. Start Update manager by executing the script **UpdateManager.bat** file located in *<ADManager Plus Home>/bin* directory.
2. Select the service pack, which needs to be uninstalled, from the Installed Service Pack list. Click **Uninstall** to proceed with the uninstallation.
3. The list of dependent service packs if any will be shown for your confirmation before proceeding with the process.
4. Click **Finish** to proceed.

The specified Service Pack will be uninstalled from the application. You can now continue with the screen (like uninstalling another Service Pack) or quit the tool by clicking **Exit**.

## Licensing ADManager Plus

---

ADManager Plus is available in three editions - **Free**, **Standard** and **Professional** Editions

Download the product from the [Website](#).

The **Free Edition**, the **Standard Edition** and the **Professional Edition**, come packaged as a single download. During the evaluation phase, the **Standard** and **Professional Editions** are installed and can be evaluated for 30 days. After 30 days, it is automatically converted to the **Free Edition**, unless the **Standard/Professional Edition** license is purchased. [Learn more...](#)

For purchasing the license or any queries, please contact [sales@zohocorp.com](mailto:sales@zohocorp.com). The license file will be sent through e-mail.

To upgrade from a Trial Edition or Free Edition to Professional Edition

1. Click the **License** link available in the top right corner of the ADManager Plus client. This opens the License details of the product.
2. Click the **Upgrade Now** link and select the license file received from ZOHOCorp using the **Browse** button.
3. Click **Upgrade** button to upgrade from Trial or Free Edition to Professional Edition.

### Restrictions in Free Edition

The following are the restrictions in the **Free Edition**:

1. Only one domain can be managed.
2. Can be used to create/modify up to 100 users.
3. Can generate and view all the Active Directory reports for one domain.
4. Can create a maximum of 10 security roles, but, can delegate up to a maximum of 2 security roles twice each.

## Dashboard View

---

The **Home** tab projects a Dashboard View of the essential and top level information of domains. The Dashboard View projects the following:

- [Vital Help Desk Reports](#)
- [Canned Reports](#)

**Vital Help Desk Reports:** This section holds a concise list of the essential help desk related reports. The number of Password Expired Users and those whose password is likely to get expired within a week's time is also listed against appropriate headings. Password attributes of users can be modified using the Change password at Next Logon button.

**Canned Reports:** This section contains an auto-generated list of users listed under the most commonly used report types of the User, System and Other Reports categories. These reports get generated everyday at a scheduled time of the day. You can also get an updated list of users with the relevant numbers based on the options you select. The **Update Dashboard** option allows you to synchronize the Active Directory and **ADManager Plus**. You can select the category of reports from the **Update details of** dialog. Meanwhile, if you want to know the latest details of only specific reports, use the **Update** option adjacent to the report name.

## Configuring Domains

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.







**Note:** The procedure to add domains like Child Domains, Domains from same and different forests are the same.

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.

**Note:** While adding new domains, the user name and password provided will be used for management and report purpose in the product.

If the user entered in the domain settings should have the privilege to perform a management operation. Read only privilege is sufficient for a users to view reports. the first domain controller will be contacted first if it turns unsuccessful then the next domain controller in the order will be contacted.

## CSV Import

---

Now you can create and modify users, groups, contacts using CSV import.

- [Create users using CSV](#)
- [Modify users using CSV](#)
- [Create groups using CSV](#)
- [Modify groups using CSV](#)
- [Create contacts using CSV](#)
- [Modify contacts using CSV](#)

## Users Creation in Active Directory by Import CSV



**Note:** The following information conveys the mandatory and useful guide lines for successful creation on users by importing from CSV [List of LDAP attributes supported](#). [Sample CSV file](#).

### Bulk user creation by CSV

To create a user, any one of the following naming attributes is mandatory and enough: **givenName** or **cn** or **name** or **samAccountName**.

**To mention the user's OU in the CSV :** In case you want to create users under different OUs, mention the user's **givenName**, followed by the **OUName** in the CSV file. Example: John, "OU=FinanceOU, DC=abc, DC=com"

In case you want to create a user in a child OU, here's a sample of the values that need to be supplied in the CSV file. Example: John, "OU=PayrollOU, OU=FinanceOU, DC=abc, DC=com". In this example, PayrollOU is the child OU and FinanceOU is the parent OU.

**To have Useraccountcontrol attribute in CSV :** Useraccountcontrol should contain the flag value of the user account properties. Example: A flag value 512 indicates that the account is general; and value 514 indicates that the account is disabled. For detailed information, click <http://support.microsoft.com/kb/305144>

While specifying the password you will be prompted to choose one of the two options:

1. Selecting the option User must change password at next logon will assign a value 0; to pwdLastSet
2. Unselecting the option, User must change password at next logon will assign a value -1 to pwdLastSet

**To have memberOf attribute in CSV :** A user can be a member of more than one group, to support multiple values Distinguished Name (DN) of the groups should be separated by semicolon (;).

**Example:** "CN=Group1,CN=Users,DC=domain,DC=com;CN=Group2,CN=Users,DC=domain,DC=com"

**To have primaryGroupID attribute in CSV** For a user in multiple groups only one group is considered as primary; to specify that RID should be assigned.

**AccountExpires:** While specifying the account details, you will be prompted to choose one of the two options:

1. Selecting the option Account Never Expires will assign a value 0 to Accountexpires.
2. To have a expiry date set a date specify the file time. Other values should be in the FileTime format(Contains a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).)

**To have userWorkstations attribute in CSV** To restrict users to specific computers the Netbios names of computers separated by (,) should be entered and all values should be in

**To have 'Country' attribute in CSV**

1. The three values c, co, countryCode are mandatory.
2. c - 2 letter country code (eg. US for United states).
3. co - Country Name(Full Country Name).
4. countryCode - 3 digit country code(eg. 840 for United States).

**To have manager attribute in CSV:** CSV should contain the DN of the manager.

**To have MailBox Enabled Users attribute in CSV:** CSV should have

1. Minimum Attributes Needed - mailNickname, homeMDB, msExchHomeServerName.
2. homeMDB - should contain the DN of the mail box store.
3. msExchHomeServerName - value of mail server in legacyExchangeDN Format.

**To have Mail Enabled Users attribute in CSV:** CSV should have

1. Minimum Attributes Needed - mailNickname, targetAddress, msExchAdminGroup
2. targetAddress - value should be something like(SMTP:user@yahoo.com)
3. msExchAdminGroup- value of exchange Admin Group in legacyExchangeDN Format.

**To have attributes** Home Folders and Profile Path, TS Home Folder, ProfilePath in CSV

1. The values can be an absolute path of the folder
2. May contain variables like %userName%, %givenName% etc..

**To have Additional email address**

1. The user should have the attribute '**proxyAddresses**' set to a value.  
**Example** - "smtp:user@mail1.com;smtp:user@mail2.com"

**To have Additional Attributes**

- Select the '**Additional Attributes**' tab to add custom attributes. Enter the exact Attribute name and value.  
**Example:** If you wish to have Employee Id Number in user attributes, then enter 'Employee Id Number' as the Attribute name and enter the value. This will add that attribute in to the user account properties and the information can be obtained from Reports.

**User creation by Template**

1. A user can be created by selecting the predefined templates available in the option "selected Template"
2. By selecting a template, all the properties of the template will be applied to the users being created.
3. By clicking in 'change' you can change the template from mail enabled users to mailbox enabled users etc.
4. A set of users with common properties can be created by using the specific template. [Creating user template](#)

**Example:** If your intention is to create user accounts with mailbox for permanent employees, you can select the template 'MailBox Enabled Users' and start creating accounts. All the users created eventually will bare the same properties.



**Note:** First create a csv with all the updated information and then start the process.

## Modify Active Directory Users Properties/ Attributes by Import CSV

ADManager Plus provides the ability to modify the users by just importing from a CSV file. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Modify users** link under CSV import.
3. Import the CSV file and click OK. [Sample CSV file](#).
4. This will list all users and their attributes.
5. Click update to update the information in Active directory.

### Know these Tabs:

**Change Headers:** Clicking on this will allow you to change the attributes (eg.given name to sn); then save.

### Update in AD:

A pop-up displays all the LDAP Attributes provided in your CSV. You can specifically select the attributes to be modified on the active directory by placing a checkmark against the attributes on display and clicking on "OK" button.


By further clicking on the "**Show search**" link the display screen expands to provide a Match Criteria for users in AD in-order to be updated.

### Match Criteria for users in AD:

Using this option users can be matched uniquely in AD by selecting one or more LDAP attributes, placing a check mark against them, which helps in identifying specific users to be modified.

Eg:-

Take for example you have two users with the name "John Smith" in your office and you want to update one of them. This option helps to identify him uniquely by providing one or more LDAP attributes which are specific to that user.

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. First create a CSV with all the updated information and then start the process.</li> <li>2. It is recommended to give a unique value attribute like samaccountname, distinguishedname, userprincipalname to the users</li> <li>3. If Multiple users match the same criteria then the users names will be appended by numbers starting from the number specifies the users with same name but distinguishes them by number.</li> <li>4. The modifications done on UserAccountControl attributes using CSV will not be replaced but appended.</li> </ol>
---	--





An example entry to modify the "department" and "telephone number" for group of users is given below:

<pre>givenName,samAccountName,department,telephoneNumber Mathewiles,Mathewiles,Transportation,01455 882107 <b>EmmanuelSam,EmmanuelSam,Transportation,01455 882108</b> Strongosky,Strongosky,Transportation,01455 882109</pre>
---



## Create Contacts in Active Directory

---

You can create contacts for external users. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Create contacts** link under CSV import.
3. Import the CSV file and click OK.
4. Once you see the list imported click Next.
5. Select the container from the list provided.
6. click on 'Create contacts'
7. This will list all users and their contacts.

An example entry to create contacts is below.

```
name,givenName,displayName,description,mail,co,department
John,Mathew,John Mathew,description,Martyn@domain.com,Cananda,Sales
smith,adam,adam,description,smith@domain.com,Cananda,Marketing
john,paul,johnpaul,description,john@domain.com,Cananda,Accounts
philip,kotler,philipkotler,description,philip@domain.com,Cananda,Analyst
pralad,kakkar,praladkakkar,description,pralad@domain.com,Cananda,sales
```

[Sample CSV File](#)

## Modify Contacts in Active Directory Using CSV

---

You can modify Active Directory Contacts attributes using CSV import. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Select **Contact Management** link on the left pane and open the Contact Management page.
3. Select the **Modify Contacts** link under **CSV Import**.
4. Click the **Import** button. **Browse** the CSV file to be imported and click **OK**.
5. Select the contacts for which the details need to be updated in the **CSV Import** page,
6. Click the **Update in AD** button.
7. Select the attributes to be modified in the **Select Attributes** dialog.
8. Click **OK**.

The Contacts' attributes will now hold the values as mentioned in the CSV file that was imported.

**Note:**

The **Match criteria for Contacts in AD: Show**, allows you to specify the LDAP names that should uniquely identify the contacts.

## Delete Contacts

---

Obsolete or unwanted contacts and their accounts can be deleted using this option. To perform the deletion follow the below steps:

- Select the AD Mgmt tab.
- Click the **Delete contacts** link available under General Attributes. This opens the **Delete Contact Accounts from Active Directory** dialog.
- Select the domain and search the contacts. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
- You can import the list of contacts to be modified from CSV format or select the user from 'show All contacts' list or Type a contact name.
- From the listed contacts, select the contacts to be deleted.
- Click on Apply to confirm the deletion.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Create Group in Active Directory Using CSV

---

ADManager Plus provides the ability to create groups by just importing from a CSV file. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Create Group** link under CSV import.
3. Fill all the details; to add members import the users from CSV file or select them and click OK.
4. You can also create an Exchange email address to groups. Check in the box adjacent to '**Create an Exchange E-Mail Address**' and enter the details and save.
5. This will create a mail enabled group.
6. Click save to update the information in Active directory.



**Note:** First create a CSV file containing the group members list and then start the process.

## Modify Group in Active Directory

---

ADManager Plus provides the ability to modify the members of groups by just importing from a CSV file. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Modify Group** link under CSV import.
3. This option allows you to change or modify the members only. you cannot change the scope of the group here.
4. Select the domain and the group to be modified.
5. Import the members list from a CSV file or select the members. You can also delete the existing members from the group.
6. Click save to update the information in Active directory.

## Active Directory Management

---

ADManager Plus is in-built with powerful Management tools that encompasses all the areas of Active Directory. You can manage mass users, computers, groups, contacts and exchange from one point in a simple way.

This section guides you in managing Active Directory using ADManager Plus. Follow the links to learn more:

- [Active Directory User Management](#)
- [Active Directory Computer Management](#)
- [Active Directory Group Management](#)
- [Active Directory Contact Management](#)
- [Active Directory Exchange Management](#)



**Caution:** Perform the above steps in a test or pre-production environment prior to rolling out to production departments.

## Active Directory User Management

---

ManageEngine ADManager Plus enables you to create or modify multiple user accounts to your windows domain with ease. You have the flexibility to copy the user properties from another user and/or create multiple user templates to match your requirements. You can then change the personal details either manually or by importing them.

ADManager Plus supports modifying common administrative tasks such as resetting password, disabling user accounts, moving users to a different container, and so on. It also supports modifying exchange and terminal service attributes such as, delivery restrictions, creating mailbox, modifying user profiles, environment variables, and so on.

This section guides you in managing users using ADManager Plus. Follow the links to learn more:

- [Create users](#)
- [Modify Users](#)
- [Create User Template](#)
- [Search Users, Groups and Computers](#)



# Create Users

## Active Directory Create Users

---

ManageEngine ADManager Plus enables you to create multiple user accounts to your windows domain with ease. You have the flexibility to create single users, multiple users either manually or by CSV import.

This section guides you in Creating users using ADManager Plus. Follow the links to learn more:

- [Creating a Single User](#)
- [Creating Bulk Users](#)
- [Creating Users Using CSV](#)
- [Additional Attributes](#)

## Creating a Single User

---

To create an user account,

1. Click **AD Mgmt** tab
2. Click 'Create Single User' link under 'Create Users'. This opens the Create Single User screen.
3. Specify the values for User Profile attributes.
4. Select a valid container. You can change the existing container by clicking on 'change'.
5. You can also create a new container by selecting the tab 'Create New OU' which you find after attempting to 'change' the container. Select the location to create the and name it.
6. Select the **Account Details** tab and specify the account properties.  
There are different options available for password settings. You can choose any one from 'Randomly generate password', 'Type a password' etc. You can even customize the password settings to your organizational objectives, **Link** click here for password customization.  
**Member of:** All the groups cannot be set as primary group to users for security reasons. So before applying primary group for users check the authorization. Only Security Global and Security Universal Groups can be set as Primary Group.
7. Select the **Contact Details** tab to specify the contact information about the user.
8. Select the **Exchange Server** tab to create a external mail enabled user or mailbox enabled user or with no mail. Specify the exchange attributes only if the mailbox is enabled.  
External Mail enabled users don't have mail box in the exchange server but mailbox enable users do.  
Choose Mail server and mailbox store while creating mailbox enabled user choose Admin groups and give Target SMTP address  
(Example: "smtp:user@mail1.com; smtp:user@mail2.com") while creating external mail enabled users.
9. Select the **Terminal Services** and specify the terminal services attributes.
10. Select the '**Additional Attributes**' link to add custom attributes. Enter the exact Attribute name and value Ex: If you wish to have Employee Id Number in user attributes, then enter 'Employee Id Number' as the Attribute name and enter the value. This will add that attribute in to the user account properties and the information can be obtained from Reports.
11. After specifying the required details, click **Create User**.

### User creation by Template:

1. A user can be created by selecting the predefined templates available in the option "selected Template"
2. By selecting a template, all the properties of the template will be applied to the users being created.
3. By clicking in 'change' you can change the template from mail enabled users to mailbox enabled users etc.

4. A set of users with common properties can be created by using the specific template. **Link** to template creation

Ex: If your intention is to create user accounts with mailbox for permanent employees, you can select the template 'MailBox Enabled Users' and start creating accounts. All the users created eventually will bare the same properties. For details on the user attributes, refer to the Microsoft Documentation [here](#) and [here](#).

**Note:**




1. To create Mailbox Enabled Users in Exchange 2007, you would require the Exchange Management Console, failing which the legacy Mailbox will be created.
2. The mandatory parameters for creating a user are the First Name, the Logon Name, SAMaccount Name and the FullName. When the attribute is left blank, the user account will be created with the default values.
3. Changing domain in middle of things will reset all domain specific attributes.
4. OWA - 2 DC Replication. If Mailbox is created in one Domain controller, Out look Web Access contacts other Domain Controller to confirm the mapping, but do not authenticate.  
The Real Scenario for this is:
  1. A Domain May have more than one domain controllers.
  2. Users We will be created in the first available domain controller in ADManager Plus.
  3. The OWA authenticates a DC for login, if the DC is not the one in which user is created, it will not be recognised about this until it is replicated.

## Creating Bulk Users

ADManager Plus provides various options to create multiple user accounts in your Windows domain. Please follow the steps below to create multiple users simultaneously:

1. Click **AD Mgmt** tab
2. Click the **Create Bulk Users** link under **Create Users** to invoke the Create Bulk Users wizard.
3. Select the domain from the select domain combo box.
4. You have the following options to add users:
  1. Click **Add Users** button and specify the user attributes to add users manually. Continue adding more users by clicking the **Add More Users** button.
  2. Click **Import** button to import the user details from a [csv file](#).
  3. Select a previously created user template, and add the users by just specifying the name of all the users manually, while all the other attribute values are taken from the chosen template. You can also combine options two and three, in which case the values imported from the CSV file takes precedence.
5. After adding all the users, the next step is to select the container object where the user accounts have to be created. Click **Select Container** to proceed to the next step.
6. Select the container by browsing the Active Directory. By default, the User container of the selected domain is chosen. To choose a different container, click the **Change** link and select a different container. You can also create a new container by selecting the tab '**Create New OU**' which you find after attempting to 'change' the container. Select the location to create the and name it.
7. Click **Create Users** to create the defined uses in the selected container.

For details on the user attributes, refer to the Microsoft Documentation [here](#) and [here](#).

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. The exchange attributes need not be specified, if you do not wish to enable mailbox for the users.</li> <li>2. To create Mailbox Enabled Users in Exchange 2007, you would require the Exchange Management Console, failing which the legacy Mailbox will be created.</li> </ol>
---	--

[Click Here](#) to learn more about user creation using CSV

### Importing Data from CSV Files

ADManager Plus provides you the flexibility to import user details from a CSV file. The first line in the CSV file should contain the attribute names as defined in the Active Directory. The givenName attribute is a mandatory field in the CSV file. An example entry is given below:

```
givenName,sn,initials
John,Mathew,Martin
Peter,Jackson,Samuel
George,Simon,Jones
```

### Sample CSV file.


#### Hints:

1. While adding users who have same set of permissions, you can create a user template by specifying the required permissions and create a CSV file containing the names of the users, which can be imported while creating bulk users.
2. If you have to create users with different permissions, you can include the attributes that have different values for different users in the CSV file along with their names and can still have a base template for common attributes.




**Note:** When you use a combination of user template and CSV file, the attribute values specified in the CSV file takes precedence.

## Copying User Attributes

When you add a user by specifying the attributes or by importing the data from the CSV file, the added/imported user attributes gets listed in a tabular format. Clicking the  icon from a particular row makes a copy of that user from where you can click and modify the attributes.

If you wish to modify the user properties, click on the attribute value to change or click the  icon to open the user properties in the UI to edit.

To delete an added user, click the  icon.

## Users Creation in Active Directory by Import CSV



**Note:** The following information conveys the mandatory and useful guide lines for successful creation on users by importing from CSV. [List of LDAP attributes supported.](#) [Sample CSV file.](#)

### Bulk user creation by CSV

To create a user, any one of the following naming attributes is mandatory and enough: **givenName**.

**To have Useraccountcontrol attribute in CSV :** Useraccountcontrol should contain the flag value of the user account properties. Example: A flag value 512 indicates that the account is general; and value 514 indicates that the account is disabled.

For detailed information, click <http://support.microsoft.com/kb/305144>

While specifying the password you will be prompted to choose one of the two options:

1. Selecting the option User must change password at next logon will assign a value 0; to pwdLastSet
2. Unselecting the option, User must change password at next logon will assign a value -1 to pwdLastSet

**To have memberOf attribute in CSV :** A user can be a member of more than one group, to support multiple values Distinguished Name (DN) of the groups should be separated by semicolon (;).

**Example:** "CN=Group1,CN=Users,DC=domain,DC=com;CN=Group2,CN=Users,DC=domain,DC=com"

**To have primaryGroupID attribute in CSV** For a user in multiple groups only one group is considered as primary; to specify that RID should be assigned.

**AccountExpires:** While specifying the account details, you will be prompted to choose one of the two options:

1. Selecting the option Account Never Expires will assign a value 0 to Accountexpires.
2. To have a expiry date set a date specify the file time. Other values should be in the FileTime format(Contains a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).)

**To have userWorkstations attribute in CSV** To restrict users to specific computers the NetBIOS names of computers separated by (,) should be entered and all values should be in

### To have 'Country' attribute in CSV

1. The three values c, co, countryCode are mandatory.
2. c - 2 letter country code (eg. US for United states).
3. co - Country Name (Full Country Name).
4. countryCode - 3 digit country code (eg. 840 for United States).

**To have manager attribute in CSV:** CSV should contain the DN of the manager.

**To have Password attribute in CSV:** CSV should contain the header 'password'.

**To have MailBox Enabled Users attribute in CSV:** CSV should have

1. Minimum Attributes Needed - mailNickame, homeMDB, msExchHomeServerName.
2. homeMDB - should contain the DN of the mail box store.
3. msExchHomeServerName - value of mail server in legacyExchangeDN Format.

**To have Mail Enabled Users attribute in CSV:** CSV should have

1. Minimum Attributes Needed - mailNickname, targertAddress, msExchAdminGroup
2. targertAddress - value should be something like(SMTP:user@yahoo.com)
3. msExchAdminGroup- value of exchange Admin Group in legacy ExchangeDN Format.

**To have attributes** Home Folders and Profile Path, TS Home Folder, ProfilePath in CSV

1. The values can be an absolute path of the folder
2. May contain variables like %userName%, %givenName% etc..

**To have Additional email address**

1. The user should have the attribute '**proxyAddresses**' set to a value.  
**Example** - "smtp:user@mail1.com;smtp:user@mail2.com"

**To have Additional Attributes**

- Select the '**Custom Attributes**' tab to add additional attributes. Enter the exact Attribute name and value.  
**Example:** If you wish to have employeeID in user attributes, then enter 'employeeID' as the Attribute name and enter the value. This will add that attribute in to the user account properties and the information can be obtained from Reports.

**User creation by Template**

1. A user can be created by selecting the predefined templates available in the option "selected Template"
2. By selecting a template, all the properties of the template will be applied to the users being created.
3. By clicking in 'change' you can change the template from mail enabled users to mailbox enabled users etc.
4. A set of users with common properties can be created by using the specific template. [Creating user template](#)

**Example:** If your intention is to create user accounts with mailbox for permanent employees, you can select the template 'MailBox Enabled Users' and start creating accounts. All the users created eventually will bare the same properties.



**Note:** First create a CSV with all the updated information and then start the process.

## Active Directory Additional Attributes

---

ManageEngine ADManager Plus provides you the flexibility to add custom additional attributes. Apart from the existing Attributes in the Active Directory you can define and Add new attributes which your environment demands. Additional Attributes can be defined in Active Directory while Creating users. You can import these attributes through a CSV file.

The common additional attributes comprise the following:

- employeeID
- employeeType
- assistant
- Secretary
- carlicense

Native Active Directory supports creation of Custom Attributes in Exchange. The Custom Attributes are predefined by name and the value can be given by you.



# Modify Users

## Active Directory Modify Users

---

ManageEngine ADManager Plus enables you to create multiple user accounts to your windows domain with ease. You have the flexibility to create single users, multiple users either manually or by CSV import.

This section guides you in Creating users using ADManager Plus. Follow the links to learn more:

- [Modify Users Using CSV](#)
- [Modify Single User](#)
- [Bulk User Modification](#)

## Modify Active Directory Users Properties/Attributes by Import CSV

ADManager Plus provides the ability to modify the users by just importing from a CSV file. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Modify users** link under CSV import.
3. Import the CSV file and click OK.
4. This will list all users and their attributes.
5. Click update to update the information in Active directory.

### Know these Tabs:

**Change Headers:** Clicking on this will allow you to change the attributes (eg.given name to sn) and then save.

### Update in AD:

A pop-up displays all the LDAP Attributes provided in your CSV. You can specifically select the attributes to be modified on the active directory by placing a checkmark against the attributes on display and clicking on "OK" button.


By further clicking on the "**Show search**" link the display screen expands to provide a Match Criteria for users in AD in-order to be updated.

### Match Criteria for users in AD:

Using this option users can be matched uniquely in AD by selecting one or more LDAP attributes, placing a check mark against them, which helps in identifying specific users to be modified.

Eg:-

Take for example you have two users with the name "John Smith" in your office and you want to update one of them. This option helps to identify him uniquely by providing one or more LDAP attributes which are specific to that user.

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. First create a CSV with all the updated information and then start the process.</li> <li>2. It is recommended to give a unique value attribute like samaccountname, distinguishedname, userprincipalname to the users</li> <li>3. If Multiple users match the same criteria then the users names will be appended by numbers starting from the number specifies the users with same name but distinguishes them by number.</li> <li>4. The modifications done on UserAccountControl attributes using CSV will be appended.</li> </ol>
---	---

An example entry to modify the "department" and "telephone number" for group of users is given below:

```
givenName,samAccountName,department,telephoneNumber
MathewIles,MathewIles,Transportation,01455 882107
EmmanuelSam,EmmanuelSam,Transportation,01455 882108
Strongosky,Strongosky,Transportation,01455 882109
```

[Sample CSV file](#)

## Active Directory Single User Modification

---

ADManager Plus enables you to modify single user account to your windows domain with ease. The single user account modification is summarized in one page where in you can change all the user account properties and save them in Active Directory.

This section guides you in modifying single user using ADManager Plus. Follow the links to learn more:

1. Generate any user report (AD Reports-> User Reports).
2. Click on the user name which you desire to modify.
3. A new window that lists down all the user properties pops up.
4. Any property of the user can be modified by selecting the respective tab and changing the desired property.
5. Click 'Update User' to update the changes in Active Directory.

# Bulk User Modifications

## Active Directory Bulk Users Modification

---

ADManager Plus provides the ability to modify Mass users general and terminal service attributes.

The following sections will give a clear understanding of different operations.

- [Modifying General User Attributes](#)
- [Modifying Terminal Services](#)

## Modifying General User Attributes

---

This section guides you in modifying the general user attributes, such as naming attributes, moving users to a different container, adding/removing users from groups, and so on.

All the below functions support CSV file import: [Sample CSV file](#)

- [Resetting Password](#)
- [Modifying Naming Attributes](#)
- [Modifying Security Attributes \(Unlock Users\)](#)
- [Modifying Organization Attributes](#)
- [Modifying Profile Attributes](#)
- [Modifying Contact Attributes](#)
- [Modifying Group Attributes](#)
- [Move Users to a Different Container](#)
- [Modifying Logon Workstation](#)
- [Modifying Inheritable Permissions](#)
- [Move Home Folders](#)
- [Custom Attributes](#)
- [Delete Users](#)

For details on the user attributes, refer to the [Microsoft Documentation](#).

## Resetting Password

---

To reset the password for the user(s), follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Reset Password** link available under General Attributes. This opens the **Modify Password Attributes of the Users** dialog.
3. To reset the password, select the Reset Password check box and select any of the options for setting the password.
4. To change the password properties, select the options as required.
5. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
6. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
7. From the listed users, select the users to reset the password and click Apply.

To know about Customization of Passwords click [here](#)

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.


## Modifying Naming Attributes


---

The format for the users' Name, Display Name, Logon Name and SAM Account Name can be modified from here. To modify the naming attributes,

1. Select the AD Mgmt tab.
2. Click the **Naming Attributes** link available under General Attributes. This opens the **Modify Naming Attributes of the Users** dialog.
3. Select the name format from the given options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the naming attributes and click Apply.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. Changing the Name format will change the name of the existing user account with all the other properties unaltered.</li> <li>2. Changing the Logon name and SAM account name may cause duplication, if one by the same name exists.</li> </ol>
---	--




## Modifying Security Attributes

---

This feature enables you to unlock the accounts that were locked due to bad logon or due to account settings. To unlock the accounts:

1. Select the AD Mgmt tab.
2. Click the **Unlock Users** link available under General Attributes. This opens the **Modify Account Attributes of the Users** dialog.
3. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
4. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
5. From the listed users, select the users for changing the security attributes and click Apply.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

**Enable / Disable users:** In most of the reports you find an option to Enable / Disable users. This is an integration of User management into Reports.

This feature enables you to modify or manage the user accounts from reports itself.

To perform this:

1. Look out for the options Enable / Disable / More actions in the user reports generated.
2. Check in the boxes adjacent to the desired users to select them.
3. Now you can Enable / Disable or perform More actions by clicking on the appropriate tab.

## Modifying Organization Attributes

---

You can change the users' address and organization details, such as Title, Department, Manager, etc., from here. To modify the Windows user organization attributes,

1. Select the AD Mgmt tab.
2. Click the **Organization Attributes** link available under General Attributes. This opens the **Modify Address/Organization Attributes of the Users** dialog.
3. Select the option to change and specify the value in the text field.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the security attributes and click Apply.

The change summary and the status of the modification can be verified.


Roll over the mouse over the  icon to see the attributes in the windows native UI.


## Modifying Profile Attributes

The user profiles, such as Profile Path, Logon Script Path, and Users' home folder can be modified from here. To modify the Windows user profile attributes,

1. Select the AD Mgmt tab.
2. Click the **Profile Attributes** link available under General Attributes. This opens the **Modify Profile Attributes of the Users** dialog.
3. This feature allows You to modify logonscript, profile path and home folder of users. Select the option to change and specify the value in the text field.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the profile attributes and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. Profile Path need not be specified, if it is a local path.</li> <li>2. When you specify the Home Folder/Profile Path in a network share, it is advisable to provide permissions only to the specified users to avoid any misuse/discrepancies.</li> <li>3. Logon Script specified should be located in SYSVOL\&lt;domainName&gt;.com\scripts directory in the Domain Controller.</li> </ol>
---	---

## Modifying Contact Attributes


---

You can modify or update the contact information of different users using this option. To perform the operation,

Note: The common contact attributes like office address and office phone number can be modified and applied to all users.

1. Select the AD Mgmt tab.
2. Click the **Contact Attributes** link available under General Attributes. This opens the **Modify Contact Attributes of the Users** dialog.
3. Enter the information in the relevant boxes.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users to change the contact attributes and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modifying Group Attributes

---

You can add users to specific groups, remove from specific groups, and can set the primary group for users from here. To modify the Windows user group attributes,

1. Select the AD Mgmt tab.
2. Click the **Group Attributes** link available under General Attributes. This opens the **Modify Group Attributes of the Users** dialog.
3. Specify the required options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the group attributes and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Move Users to a Different Container

---

You can move users to a different container from here. To move the users,

1. Select the AD Mgmt tab.
2. Click the **Move Users** link available under General Attributes. This opens the **Move Users to another OU** dialog.
3. Select the container to which the users have to be moved.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users and click **Apply**.

The change summary and the status of the modification can be verified.

## Modify Logon Workstation

---

You can modify the logon workstation for users. To modify this,

1. Select the AD Mgmt tab.
2. Click the **Modify Logon Workstation** link available under General Attributes. This opens the **Modify user logon workstations** dialog.
3. Select the option '**Allow all computers**' to allow user to logon to all computers.
4. Select the option '**Allow selected computers**' to restrict users to selected computers.
5. You can manually add or remove computers or click on the icon to select.
6. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
7. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
8. From the listed users, select the users and click **Apply**.

The change summary and the status of the modification can be verified.


## Modifying Inheritable Permissions

---

You can modify the inheritable permissions of objects and users i.e. you can allow or restrict a object from gaining permissions from its parent object. To modify the Inheritable permissions:

1. Select the AD Mgmt tab.
2. Click the **Modify Inheritable permissions** link available under General Attributes. This opens the **Modify user Inheritable Permissions** dialog.
3. Select one option from YES or NO either to 'allow' or 'restrict' the inheritance from their parent object.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users to modify the permissions and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.




## Move Home Folders

---

You can move home folders from one server to other. To perform this operation:

1. Select the AD Mgmt tab.
2. Click the **Move Homefolders** link available under General Attributes. This opens the **Move Homefolders** dialog.
3. Specify any the following attributes as required:
  1. Select the destination folder and the destination path to move the home folder
  2. Enter the destination path to move the profile path.
  3. Note: should be on remote server eg: \\serverName\directoryName.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the security attributes and click Apply.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.


## Modify Custom Attributes

---

The format for the users' Name, Display Name, Logon Name and SAM Account Name can be modified from here. To modify the naming attributes,

1. Select the AD Mgmt tab.
2. Click the **custom Attributes** link available under General Attributes. This opens the **Modify custom Attributes of the Users** dialog.
3. Enter the LDAP name and value, then select the data type from the given options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
6. From the listed users, select the users for changing the custom attributes and click Apply.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.



**Note:**

1. Changing the Name format will change the name of the existing user account with all the other properties unaltered.
2. Changing the Logon name and SAM account name may cause duplication, if one by the same name exists.


## Delete users


---

Obsolete or unwanted users and their accounts can be deleted using this option. To perform the deletion follow the below steps:

- Select the AD Mgmt tab.
- Click the **Delete Users** link available under General Attributes. This opens the **Delete User Accounts from Active Directory** dialog.
- Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
- You can import the list of users to be modified from CSV format or select the user from 'show All Users' list or Type a user name.
- From the listed users, select the users to be deleted.
- Click the **Configure Delete Policy** link to specify other user related folders ( **Roaming profiles, Remote Home folders**, etc) that need to be removed during user deletion.
- Click on Apply to confirm the deletion.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. Changing the Name format will change the name of the existing user account with all the other properties unaltered.</li> <li>2. Changing the Logon name and SAM account name may cause duplication, if one by the same name exists.</li> </ol>
---	--

## Dial-in or VPN properties

---

ADManager Plus allows to modify the Dial-in or VPN properties for users. Follow the steps below to perform the task:

1. Click the **AD Mgmt** tab and select **User Management** option from the left pane.
2. Select the **Dial-in or VPN Properties** link under **Bulk User Modification**.
3. Select the required **Remote Access Permission**.
4. You can select either **Allow**, **Deny** or **Apply Remote Access Policy** option.
5. Select the **domain** and do a **name search** to specify the users list or simply perform a **CSV** import of users.

## Modifying Terminal Services

### Modifying Terminal Services Attributes

---

This section guides you in modifying the terminal services attributes, such as remote control attributes, session attributes and so on.

All the below functions support CSV file import: [Sample CSV file](#).

- [Modifying User Attributes](#)
- [Modifying Environmental Variables](#)
- [Modifying Session Attributes](#)
- [Modifying Remote Control Attributes](#)

For details on the user attributes, refer to the [Microsoft Documentation](#).

## Modifying User Profiles

---

You can modify the home folder and the profile path for the users logging from terminal services from here. To modify the terminal service user profiles:

1. Select the **AD Mgmt** tab.
2. Click the **Profiles** link available under Terminal Services. This opens the **Modify Terminal Service Profile Attributes of the users** dialog.
3. Specify the home folder and/or the profile path for the users.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the profile attributes and click **Apply**.

The change summary and the status of the modification can be verified.

**Note:**

1. Profile Path need not be specified, if it is a local path.
2. When you specify the home folder/Profile Path in a network share, it is advisable to provide permissions to the specified users to avoid any misuse/discrepancies.

## Modifying Environmental Variables

---

You can modify the program to be started and the start folder when the user logs on to terminal services. To modify the terminal service environment:

1. Select the **AD Mgmt** tab.
2. Click the **Environment** link available under Terminal Services. This opens the **Modify Terminal Service Environment of the users** dialog.
3. Specify the program to be started and the start folder.
4. You can select the **Client devices** attributes namely **Connect client drives at logon**, **Connect client printers at logon**, **Default to main client printer** as yes/no.
5. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
6. From the listed users, select the users for changing the terminal service environment and click **Apply**.

The change summary and the status of the modification can be verified.

## Modifying Session Attributes

---

You can modify the session attributes from here for the users logging from terminal services. To modify the terminal service session attributes:

1. Select the **AD Mgmt** tab.
2. Click the **Sessions** link available under Terminal Services. This opens the **Modify Terminal Session Attributes of the users** dialog.
3. Select the session attributes as required.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the terminal service session attributes and click **Apply**.

The change summary and the status of the modification can be verified.



## Modifying Remote Control Attributes

---

You can enable or disable remote control and various other options for users logging from terminal services from here. To modify the terminal service remote control attributes:

1. Select the **AD Mgmt** tab.
2. Click the **Remote Control** link available under Terminal Services. This opens the **Modify Terminal Remote Control Attributes of the users** dialog.
3. Specify the remote control attributes as required.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the terminal service remote control attributes and click **Apply**.

The change summary and the status of the modification can be verified.


## Creating User Templates

Templates play an important role in maintaining different permissions for different levels of users. You can create as many templates as required to suit your needs, which can then be used in creating user accounts by just specifying the user names. To create a user template follow the steps below:

1. Click the **AD Mgmt** tab.
2. Click the **Create User Template** link available under **Create Template**. This opens the Create Template dialog.
3. Specify a name and description for the template.
4. Specify the values for **User Profile** attributes. *Note:* Selecting the option "Automatically append numbers starting from 2, if there are any duplicate names" will enable to create duplicate names prefixed with numbers. Example: If you try to create a user named 'john' which already exists, ADManager Plus will duplicate the name with 'john2' and so on.
5. Select the **Account Details** tab and specify the account properties.
6. Select the **Contact Details** tab to specify the contact information about the user.
7. Select the **Exchange Server** tab to specify the exchange attributes
8. Select the **Terminal Services** and specify the terminal services attributes.
9. Select the **Custom Attributes** link tab and enable the Run Custom Script on the Successful User Creation checkbox, to invoke any customized script immediately after user creation.
10. After specifying all the attributes as required, click **Save Template**.

The templates thus created will be available in the [bulk user creation](#) wizard from where you can select to apply templates for the users.

For details on the user attributes, refer to the Microsoft Documentation [here](#) and [here](#).

	<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. To create Mailbox Enabled Users in Exchange 2007, you would require the Exchange Management Console, failing which the legacy Mailbox will be created.</li> <li>2. For attributes like Logon Name, Display Name, Email, etc., you can choose any of the formats listed in the combo box. The chosen format will be automatically applied when you add users based on this template.</li> <li>3. When specifying the Local Path for the Home Folder for the users, you can use any LDAP Attributes in the path, which will be replaced during user creation dynamically. For example, a path can be specified as C:\Documents and Settings\%LogonName%, where, %LogonName% will be replaced by the corresponding Logon Name of the user dynamically.</li> </ol>
---	--

|

## Viewing/Modifying User Templates

To view or to modify the user templates,

1. Click the **AD Mgmt** tab.
2. Click the **View User Template** link available under **Create Template**. This will list all the templates that were created.

Tip: You can **sort** the templates in ascending/descending order using the arrow icon near the **Template Name** heading.

3. Click on the last icon under Action heading, to set that particular template as the default template.
4. To modify the template click the template name or the icon to open the Modify User Template dialog.
5. Modify the attributes as required and click **Save Template**.



**Note:** The modification to the attributes will not modify the user attributes of the users created prior to modification of the template. This applies to the users created henceforth using this template.

**User Creation with Advanced Permissions:** While creating User template you can assign advanced permissions and share properties, and eventually all the users created with those template will bear those permissions.

You will find these advanced permissions available in the following places:

### Advanced features in User Creation:

#### For Profile path:

Profile path specifies a Uniform Naming Convention (UNC) name, such as \\Server\Prof\$\%username%, to be the network folder where the user's roaming profile is stored. This way, user's roaming profile is downloaded to whichever workstation he logs onto and it is uploaded back to the server when he logs off. The dollar sign (\$) in the Prof\$ sharename makes it invisible so that users don't browse it.

Configuring the property "Profile path":

1. "Profile path" attribute can be found in the "Account Details" tab of "Create Template" wizard.
2. While specifying profile path click on 'Permissions' adjacent to it, this will open a window for profile path settings.
3. check in the box to Create Profile Path Directory before user first login
4. you can add more permissions by selecting the tab 'Permissions' to Add More Permissions'.
5. This leads you to set of options where in you can allow a selected user or group or computer, to have permissions like full control, read attributes, delete etc, over folder and its descendants.
6. Click on Add.
7. Check in the Box below to Inherit from parent the permission entries that apply to child objects.



**Note:** You can also create profile path for Windows Vista users by suffixing it with '.V2'. Example: Let's say the normal profile path looks like 'C:\Documents and settings\Jim', the Vista profile path will look something like 'C:\Documents and settings\Jim.V2'.

### For Home folders:

Home folders and My Documents make it easier for an administrator to back up user files and manage user accounts by collecting the user's files in one location. If you assign a home folder to a user, you can store the user's data in a central location on a server, and make backup and recovery of data easier and more reliable. ADManager Plus has provided some special features that helps in quickly configuring these properties for the user.

Configuring the property "Home Folder":

1. "Home folder" attribute can be found in the "Account Details" tab of "Create Template" wizard.
2. Click "Connect" and specify a drive letter.
3. In the box nearby, type a path. This path can be any of the following types:
  1. Network path, for example: \\server\users\tester
  2. You can substitute *username* for the last subfolder in the path, for example: \\server\users\%username%
  3. Where *server* is the name of the file server housing the home folders, and where *users* is the shared folder.<>
  4. The "%username%" will automatically get expanded to the user's name.

ADManager Plus also automatically creates a share of the format "\\server\%username%" and allows you to set the desired permissions for this network folder by clicking on the **Permissions** link. Enable the check box provided across "Create a New Share" below the "home folder" in order to create a new share folder in the network.

### For Mailbox Rights:

Mailbox rights allows to set permissions on users access to mailboxes. In native active directory you can set mailbox rights only after creating users, but with ADManager Plus you can provide the mail box rights while creating users.

Perform the following steps:

1. Set Mailbox rights can be found in the 'Exchange server' tab of 'create template' (ADMgmt-->create user Template). This applies to mailbox enabled users.
2. Click on "set Mailbox rights"
3. View the available permissions and Click on "ADD More permissions" to provide more permissions.
4. Select the operation either 'Allow' or 'Delete', select the object, select the permissions from the available list, select the scope of the operation.
5. Click on 'Add', then you will find the added permission.
6. Click OK.

**Enable Live Communications/ Office Communication Server 2007 Support :**

Select the LCS/OCS server. Specify SIP-URI (Session in Protocol -URI) format

The SIP-URI format should be of a valid format. Example; **sip: user@domain.com**

Also provide

- **Federation Settings**
- **Archiving Settings**
- **Remote Control Settings**

for the users imported from the CSV file in the template by checking in the respective checkboxes provided across them.

Native Active Directory supports enabling Live Communication. ADManager Plus facilitates easily enable and configure of Live Communication settings with the help of templates and by avoiding command line tools.

## Searching Users, Groups, and Computers

---

ADManager Plus provides the ability to locate any object in the Active Directory with its powerful search capability. You can also search across domains and restrict your search to users, groups, or computers. To search the Active Directory objects, follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Search Users, Groups, and Computers** link under Search Users.
3. All the domains configured in the [Domain Settings](#) will be available here to select. Select the domains that have to be searched. To restrict the search to specific OU's in the domain Click the **Select OU** link and choose the OU's that have to be searched.
4. Select the objects that have to be searched for. For example, if you want to search only the users, clear the check box of Groups and Computers.
5. Specify the search criteria. you can include the common name (cn) and the description of the objects in the search criteria.
6. Click **Search**.

ADManager Plus searches the active directory based on the specified search criterion and displays the result in the bottom panel. The search results include the name of the object, the object class, the fully qualified domain name (FQDN), and the domain name of the object.

### Viewing All the Users

To view all the users of the domain, click the **View Users** link under the Search Users of the **AD Mgmt** tab. This will display all the users of the default domain. To view the users of a different domain, select the domain from the **Change Domain** combo box.

## Active Directory Computer Management

---

This Feature assists you to handle bulk / mass computer modification. The following operations are available under this feature.

- [Modify Group Attributes](#)
- [Modify General Attributes](#)
- [Enable/Disable Computers](#)
- [Move Computers](#)
- [Delete Computers](#)

## Enable-Disable Computers

---

You can Enable/Disable Computers using this option. To change the status of computers,

1. Select the AD Mgmt tab.
2. Click the Enable/Disable Computers link available under Bulk computer Modification. This opens the **Enable/Disable Computers** dialog.
3. Specify the required options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of computers to be modified from CSV format or select a computer from 'Show All Computers' list or Type a Computer Name.
6. From the listed computers, select the computers for changing the status and click **Apply**.

The change summary and the status of the modification can be verified.




## Modifying General Attributes

---

This feature allows you to set Description, Location and Managed By for computers. To modify the Windows computer general attributes,

1. Select the AD Mgmt tab.
2. Click the **General attributes** link available under Bulk computer modification. This opens the Modify Address/Organization Attributes of the Computers dialog.
3. Specify the required options.
4. Select the domain and search the computers. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of computers to be modified from CSV format or select a computer from 'Show All Computers' list or Type a Computer Name.
6. From the listed computers, select the computers for changing the general attributes and click **Apply**.

The change summary and the status of the modification can be verified.

Roll the mouse over the  icon to see the attributes in the windows native UI.


## Modifying Group Attributes

---

You can add users to specific groups, remove from specific groups, and can set the primary group for users from here. To modify the Windows user group attributes,

1. Select the AD Mgmt tab.
2. Click the **Group Attributes** link available under Bulk computer Modification. This opens the **Modify Group Attributes of computers** dialog.
3. Specify the required options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of computers to be modified from CSV format or select a computer from 'Show All Computers' list or Type a Computer Name.
6. From the listed computers, select the computers for changing the group attributes and click **Apply**.

The change summary and the status of the modification can be verified.

Roll the mouse over the  icon to see the attributes in the windows native UI.

## Move Computers

---

You can move computers from one Organizational unit to other.

1. Select the AD Mgmt tab.
2. Click the **Move computers** link available under Bulk computer Modification. This opens the **Move computers to another OU** dialog.
3. Specify the required options.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
5. You can import the list of computers to be modified from CSV format or select a computer from 'Show All Computers' list or Type a Computer Name.
6. From the listed computers, select the computers and the respective container to move and click **Apply**.

The change summary and the status of the modification can be verified.

# Active Directory Group Management

## Active Directory Groups Management

---

Using ADManager Plus, you can create and modify group(s) based on your requirements. The following set of functionalities can be performed to streamline this operation:

- [Single Group Management](#)
- [Bulk Group Management](#)
- [CSV Import](#)

# Single Group Management

---

ADManager Plus offers the flexibility to manage individual groups via its Single Group Management feature which allows you to perform the following operations:

- [Single Group Creation](#)
- [Single Group Modification](#)

## Single Group Creation

1. Select the **AD Mgmt** tab.
2. Click the **Create Single Group** link under **Group Management**. This opens the **Create Distribution List & Security Group** Dialog.
3. Select the domain and specify the Group name, Group scope and Group type in the General section.
4. Specify the Email, Description and Notes in the Description section.
5. Import the members list from a CSV file or select the members in the Members section.
6. Specify the Member Of and Managed By details using the appropriate links that appear next to these text boxes.
7. Specify the container in the Container text field. Use the Change link to modify container details.
8. Enable the checkbox below Container text field, to create an exchange email address.
9. Click on Create Group button to save the details and create the new group.

## Single Group Modification

1. Select the **AD Mgmt** tab.
2. Click the **Single Group Modification** link under **Group Management**. This opens the **Modify Distribution List & Security Group** Dialog.
3. Select the domain and the group (along with its Scope and Type) to be modified.
4. Click on the Get Existing Members link to view the users in that group. You can add or remove the members from here.
5. Import the members list from a CSV file or select the members. You can also **Remove** the existing members from the group.

**Note:** To view the existing members in the group, click on the **Get Existing Members** list.

6. Click on the **Advanced Settings** link to update the necessary attributes. Make the changes as needed.
7. Click on the **Update Group** button to save changes in the Active Directory.

# Bulk Group Management

---

ADManager Plus offers the flexibility to manage multiple groups via its Bulk Group Management feature which allows you to perform the following operations:

- [Delete Groups](#)
- [Modify Organization Attributes of Group](#)
- [Move Groups](#)
- [Modify Exchange Attributes of Group](#)

## Delete Groups

You can delete unwanted or obsolete group accounts from your Active Directory using the **Delete Groups** feature. Follow the steps given below to complete the process.

1. Select the **AD Mgmt** tab.
2. Click on the **Delete Groups** link under **Group Management**. This opens the Delete Group Accounts from Active Directory dialog.
3. Specify the Domain. Use the Add OUs link to select the OUs.
4. Import the group list from a CSV file or search the group accounts.
5. Click on Apply to update the information in Active directory.

## Modify Organization Attributes Of Group

You can change the group address and organization details, such as Title, Department, Manager, etc., from here. To modify the Windows group organization attributes,

1. Select the AD Mgmt tab.
2. Click the Organization Attributes link available under Group Management. This opens the Modify Organization Attributes of the Groups dialog.
3. Enable and Specify the email, description and notes in the Description section.
4. Specify the Member Of and Managed By fields using the add/edit and change options that are available.
5. Select the domain. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
6. You can import the list of groups to be modified via a CSV format file or search for a particular group name(s).
7. Select the groups and click on Apply button to save changes.

The change summary and the status of the modification can be verified.

## Move Groups

You can move groups to another OU using the Move Groups feature of ADManager Plus. Follow the steps given below to perform this operation:

1. Select the AD Mgmt tab.
2. Click the Move Groups link under Group Management. This opens the Move Groups to another OU dialog.
3. Select the container to which the Group(s) need to be moved.
4. Select the domain and search the groups. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.

5. You can import the list of groups to be modified in a CSV format or also search for specific group names.
6. Select the groups from the list and click Apply.

The change summary and the status of the modification can be verified.

### **Modify Exchange Attributes of Group**

1. Select the **AD Mgmt** tab.
2. Click the **Exchange Attributes** link under Group Management. This opens the Modify Exchange Attributes of the Groups dialog.
3. Specify the choices for update in the Delivery Restrictions section.
4. Select the domain and the group to be modified. You can restrict to specify OUs using the Add OUs link.
5. Import the groups list from a CSV file or specify desired groups using search option.
6. Select the groups and click on the Apply button to update information in the Active directory.

## CSV Based Group Management

---

ADManager Plus offers Bulk Group Management based on CSV File Imports. The following operations are possible via a CSV import.

- [Create Groups in Bulk](#)
- [Modify Groups using CSV](#)

### Create Groups in Bulk

1. Select the **AD Mgmt** tab.
2. Click the **Create Bulk Groups** link under CSV import. This opens the Create Group page.
3. Select the domain in which the new groups need to be added.
4. Import the groups list from a CSV file and click on Next.
5. Select the Group Type & Scope from the dialog and click OK.
6. Select the container. You can also create a new OU using the Create New OU link.
7. Click on Create Groups button to initiate creation of Groups in bulk.
8. The created groups and their status can be verified.

### Modify Groups using CSV

1. Select the **AD Mgmt** tab.
2. Click the **Modify Groups Using CSV** link under CSV import. This opens the Modify Groups using CSV dialog.
3. Select the domain containing the groups to be modified.
4. Import the group list from a CSV file using the Import button.
5. Select the Groups that need to be modified. You can also Modify Headers using Change Headers option.
6. Click Update in AD button.
7. Select the attributes from the Select Attributes Dialog. You could also make use of the Match criteria link.
8. Click OK to update the information in Active directory.

### Sample CSV:

sAMAccountName
Adam
John
Peter
Lisa
Freeman
Samuel



# Active Directory Contact Management

## Active Directory Contacts Management

---

ManageEngine ADManager Plus enables you to create Contacts to your windows domain with CSV Import at ease. You have the flexibility to import the contacts from CSV file.

This section guides you in managing Contacts using ADManager Plus. Follow the links to learn more:

- [Create Contacts](#)
- [Bulk Contact Modification](#)

## Create Contacts in Active Directory

---

You can create contacts for external users. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Click the **Create contacts** link under CSV import.
3. Import the CSV file and click OK.
4. Once you see the list imported click Next.
5. Select the container from the list provided.
6. click on 'Create contacts'
7. This will list all users and their contacts.

An example entry to create contacts is below.

```
name givenName displayName description mail co department
John Mathew John Mathew description Martyn@domain.com Cananda Sales
smith adam adam description smith@domain.com Cananda Marketing
john paul johnpaul description john@domain.com Cananda Accounts
philip kotler philipkotler description philip@domain.com Cananda
Analyst
pralad kakkar praladkakkar description pralad@domain.com Cananda
sales
```

[Sample CSV File](#)

# Bulk Contacts Modification

## Active Directory Bulk Contact Management

---

AD Manager Plus comes with the **Bulk Contact Modification** feature which simplifies the task of **updating** details for **multiple contacts**.

This section primarily deals with the following topics:

- [Address/Organization Attributes](#)
- [Contact Attributes](#)
- [Naming Attributes](#)
- [Modify Contacts Using CSV](#)

## Address/Organization Attributes

---

You can change the contacts' **address** and **organization** details, such as Title, Department, Manager, etc., from here. To modify the Windows Contact **Address/Organization** attributes,

1. Click the **Contact Management** link in the right pane of the **Home** page. This opens the **Contact Management** page.
2. Click the **Address/Organization Attributes** link under **Bulk Contact Management**.
3. The **Modify Address/Organization Attributes** of the **Contacts** page displays various fields like Title, Department, Company, Manager, Street, City, etc.,
4. Use the checkbox to **enable** the required text field. Enter the new values in the text field.
5. Select the domain and **search** for contacts. You can limit your search to specific OU's of the domain by clicking the **Select OU** link.
6. You can import a list of contacts to be modified from a **CSV** format file or select particular contact(s) using the **Enter name(s) to search** option.
7. From the listed contacts, select those for which the attributes need to be modified. Click the **APPLY** button.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Naming Attributes

---


You can change the contacts' **naming** details with the help of this feature. To modify the Windows Contact **Naming Attributes**,

1. Select the **AD Mgmt** tab.
2. Click the **Contact Management** link in the left pane to open the **Contact Management** page.
3. Click the **Naming Attributes** link under **Bulk Contact Management** to open **Modify Naming Attributes of the Contacts** page.
4. Select the **Display name** format from the list. Use **Create your own format** link to add a new format of your choice.
5. **Modify the Full name format** by selecting from the given format list.

**Caution:** Modifying the **Full Name Format** may cause changes to the existing account.

6. Select the **domain** and **search** for contacts. You can limit your search to specific OU's of the domain by clicking the **Select OU** link.
7. You can import a list of contacts to be modified from a **CSV** format file or select particular contact(s) using the **Enter name(s) to search** option.
8. From the listed contacts, select those for which the attributes need to be modified. Click the **APPLY** button.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.


## Contact Attributes

---

You can change the contacts' **contact** details, like phone numbers, email, etc., from here. To modify the Windows Contact **Contact attributes**,

1. Select the **AD Mgmt** tab.
2. Click the **Contact Management** link in the left pane to open the **Contact Management** page.
3. Click the **Contact Attributes** link under **Bulk Contact Management**.
4. The **Modify Contact Attributes of the Contacts** page displays various fields like Telephone number, E-mail, Web page, Description, Office, Mobile, etc.,
5. Use the checkbox to enable the required text field. Enter the new values in the text field.
6. Select the domain and **search** for contacts. You can limit your search to specific OU's of the domain by clicking the **Select OU** link.
7. You can import a list of contacts to be modified from a **CSV** format file or select particular contact(s) using the **Enter name(s) to search** option.
8. From the listed contacts, select those for which the attributes need to be modified. Click the **APPLY** button.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modify Contacts in Active Directory Using CSV

You can modify Active Directory Contacts attributes using CSV import. To perform this operation follow the steps below:

1. Select the **AD Mgmt** tab.
2. Select **Contact Management** link on the left pane and open the Contact Management page.
3. Select the **Modify Contacts** link under **CSV Import**.
4. Click the **Import** button. **Browse** the CSV file to be imported and click **OK**.
5. Select the contacts for which the details need to be updated in the **CSV Import** page,
6. Click the **Update in AD** button.
7. Select the attributes to be modified in the **Select Attributes** dialog.
8. Click **OK**.

The Contacts' attributes will now hold the values as mentioned in the CSV file that was imported.

**Note:**

The **Match criteria for Contacts in AD: Show**, allows you to specify the LDAP names that should uniquely identify the contacts.

## Delete Contacts

---

Obsolete or unwanted contacts and their accounts can be deleted using this option. To perform the deletion follow the below steps:

- Select the AD Mgmt tab.
- Click the **Delete contacts** link available under General Attributes. This opens the **Delete Contact Accounts from Active Directory** dialog.
- Select the domain and search the contacts. You can limit your search to specific OU's of the domain by clicking the Select OU link and selecting the OU's.
- You can import the list of contacts to be modified from CSV format or select the user from 'show All contacts' list or Type a contact name.
- From the listed contacts, select the contacts to be deleted.
- Click on Apply to confirm the deletion.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.



# Active Directory Exchange Management

## Modifying Exchange Attributes

---

This section guides you in modifying the Exchange Server attributes, such as creating Mailbox for users, specifying mail storage limits, setting message size, message restrictions, and so on.

All the below functions support CSV file import: [Sample CSV file](#)

- [Modifying Delivery Restrictions](#)
- [Modifying Delivery Options](#)
- [Modifying Storage Limits](#)
- [Modifying Naming Attributes](#)
- [Modifying Exchange Features](#)
- [Creating Mailbox to Users](#)
- [Modify Exchange Off-line Address Book](#)

For details on the user attributes, refer to the [Microsoft Documentation](#).


## Modifying Delivery Restrictions

---

You can modify the delivery restrictions for users, such as the size of the sending and receiving messages and the restrictions to accept messages on the Exchange Server. To modify the mail delivery restrictions,

1. Select the **AD Mgmt** tab.
2. Click the **Delivery Restrictions** link available under Exchange Attributes. This opens the **Modify Delivery Restrictions of the Users** dialog.
3. Specify the maximum size for sent and received messages and the restrictions on accepting messages.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the delivery restrictions and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modifying SMTP Address


---

You can modify the SMTP Address for Mailbox enabled/Mail enabled users, and add additional email addresses in the proxy address field.

### To modify the SMTP address for Mailbox Enabled Users,

1. Select the **AD Mgmt** tab.
2. Click the **Modify SMTP** link available under Exchange Attributes. This opens the **Modify Delivery Restrictions of the Users** dialog.
3. Select the user category - **Mailbox Enabled Users**, for which you want to set additional email address.
4. Specify the Proxy email address by clicking on the **Add** button. The **Add Email Address Format dialog box** will appear.
5. Specify the additional email address format in the corresponding text field. Ensure you specify **SMTP** in upper case for setting the email address as Primary. For the email address to be a secondary address, mention **smtp** in small case in the format.
6. Click on Add More Format link in the dialog to specify/remove additional email address format.
7. Click OK after specifying the required format.
8. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
9. From the listed users, select the users for changing the delivery restrictions and click **Apply**.

The change summary and the status of the modification can be verified.


Roll over the mouse over the  icon to see the attributes in the windows native UI.

### To modify the SMTP address for Mail Enabled Users,

1. Select the **AD Mgmt** tab.
2. Click the **Modify SMTP** link available under Exchange Attributes. This opens the **Modify Delivery Restrictions of the Users** dialog.
3. Select the user category - Mail Enabled Users, for which you want to set additional email address.
4. Specify the Target Address in the corresponding text field. This field will be hidden in the earlier case when Mailbox enabled users was selected.
5. Specify the Proxy email address by clicking on the **Add** button. The **Add Email Address Format dialog box** will appear.
6. Specify the additional email address format in the corresponding text field. Ensure you specify **SMTP** in upper case for setting the email address as Primary. For the email address to be a secondary address, mention **smtp** in small case in the format.
7. Click on Add More Format link in the dialog to specify/remove additional email address format.
8. Click OK after specifying the required format.

9. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
10. From the listed users, select the users for changing the delivery restrictions and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modifying Delivery Options

---

You can modify the delivery options for users, such as recipient limit, send on behalf, and forwarding options from here. To modify the mail delivery options,

1. Select the **AD Mgmt** tab.
2. Click the **Delivery Options** link available under Exchange Attributes. This opens the **Modify Delivery Options of the Users** dialog.
3. Specify the required options as below:
  1. **Send on behalf:** Select this option to grant permissions to users who can send mail on behalf of the mailbox owner. Add the users by clicking the Add icon.
  2. **Recipient Limits:** Select this option and specify the maximum recipients or choose the default limit.
  3. **Forwarding Address:** Select this option and specify the user to whom the mails have to be forwarded. You can also choose to deliver mails to both the forwarded user and the mailbox owner.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the delivery options and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.



**Note:** If you grant a user both "Send as" and "Send on behalf of" permissions, the "Send as" permission overrides the "Send on behalf of" permission.

## Modifying Storage Limits

---

You can modify the mailbox storage limits and the deleted mail retention policies from here. To modify the mail storage limits

1. Select the **AD Mgmt** tab.
2. Click the **Storage Limits** link available under Exchange Attributes. This opens the **Modify Storage Limits of the Users** dialog.
3. Specify the storage limit and/or the deleted mail retention period.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the storage limits and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modifying Naming Attributes

---

The format for the users' Mail Alias and Display Name can be modified from here. You can also select whether to hide the alias from the Exchange Server address list or not. To modify the exchange naming attributes,

1. Select the **AD Mgmt** tab.
2. Click the **Naming Attributes** link available under Exchange Attributes. This opens the **Modify Exchange Naming Attributes of the Users** dialog.
3. Select the alias and name format from the given options.
4. Select whether to hide the alias from the Exchange Server address list or not.
5. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
6. From the listed users, select the users for changing the exchange naming attributes and click **Apply**.

The change summary and the status of the modification can be verified.


Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Modifying Exchange Features

You can enable or disable the exchange server features, such as Outlook Mobile Access, Outlook Web Access, IMAP4 Protocol, and POP3 Protocol from here. To modify the exchange features,

1. Select the **AD Mgmt** tab.
2. Click the **Exchange Features** link available under Exchange Attributes. This opens the **Modify Exchange Services Attributes of the Users** dialog.
3. Enable or disable the required features.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the exchange features and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

### Exchange Server Features

ADManager Plus supports enabling/disabling the following features of the Exchange Server

- **Outlook Mobile Access:** Enabling Outlook Mobile Access makes the user to access their exchange information using a mobile device. The users can browse their mailbox with a cell phone or other wireless device.
- **Outlook Web Access:** Enabling Outlook Web Access makes the user to access their mails through a Web browser. This feature is enabled for each user by default.
- **IMAP4 Support:** Internet Message Access Protocol version 4 (IMAP4) is an Internet messaging protocol that enables a client to access e-mail on a server, rather than downloading it to the user's computer. IMAP4 enables users to access and manipulate messages stored within mailboxes. IMAP4 also allows users to access public folders or multiple e-mail folders, search through a mailbox, etc.
- **POP3 Support:** Post Office Protocol version 3 (POP3) is an Internet messaging protocol that enables a POP3 client to download e-mail from a server. This protocol works well for computers that are unable to maintain a continuous connection to a server. POP3 does not allow users to manipulate messages on the server. E-mail is simply downloaded to the client where messages are managed. POP3 provides access only to a user's Inbox; it does not support access to public folders.



## Creating Mailbox to Users

You can create mailbox in the Exchange Server for the existing windows users from here. To create a mailbox,

1. Select the **AD Mgmt** tab.
2. Click the **Create Mailbox** link available under Exchange Attributes. This opens the **Create Mailbox to the Users** dialog.
3. Choose the Alias name format, exchange server, and the mailbox store.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for creating a mailbox and click **Apply**.

The change summary and the status of the modification can be verified.

**Note:**

1. Creating a mailbox will not enable the mailbox instantly. Mailbox will be enabled upon receipt of a mail or it depends on the Recipient Update Service (RUS) of the Exchange Server.
2. To create Mailbox Enabled Users in Exchange 2007, you would require the Exchange Management Console, failing which the legacy Mailbox will be created.


## Exchange Off-line Address Book

---

You can modify the exchange off-line address book for user accounts. To perform this operation,

1. Select the **AD Mgmt** tab.
2. Click the **Exchange Off-line Address Book** link available under Exchange Attributes. This opens the **Modify exchange off-line address book for user accounts** dialog.
3. Select the Exchange Off-line Address Book.
4. Select the domain and search the users. You can limit your search to specific OU's of the domain by clicking the **Select OU** link and selecting the OU's.
5. From the listed users, select the users for changing the storage limits and click **Apply**.

The change summary and the status of the modification can be verified.

Roll over the mouse over the  icon to see the attributes in the windows native UI.

## Active Directory Reports

---

ADManager Plus gives you an insight into the Active Directory by providing reports on various Active Directory components. The reports can be accessed by selecting the AD Reports tab from the client window. The following reports about the Active Directory are shown:

- [Active Directory User Reports](#)
- [Active Directory Password Reports](#)
- [Active Directory Group Reports](#)
- [Active Directory Computer Reports](#)
- [Active Directory Exchange Reports](#)
- [Active Directory GPO Reports](#)
- [Active Directory OU Reports](#)
- [Active Directory NTFS Reports](#)
- [Active Directory Security Reports](#)
- [Active Directory Other Reports](#)

More granular reports are provided for each of the above.

All the reports can be exported to HTML, PDF, XLS, CSV and CSVDE formats.

### Report Features

- Can generate reports for multiple domains.
- Ability to generate reports for custom inputs for granularity.
- Customizable columns by using the Edit Column link available in all the reports.
- Columnar sorting of reports
- Ability to print the reports.
- Using this reports you can export Active Directory Bulk Users (Export All users report to desired format).

## Active Directory User Reports

---

- [General Reports](#)
  - [Account Status Reports](#)
  - [Logon Reports](#)
  - [Nested Reports](#)
- 

### General Reports

- [All Users](#)
- [Users with Empty Attributes](#)
- [Users without managers](#)
- [Manager based users](#)
- [Users in more than one Group](#)
- [Recently Deleted Users](#)
- [Recently Created Users](#)
- [Recently Modified Users](#)
- [Dial-in Allow Access](#)
- [Dial-in Deny Access](#)
- [Users with Logon Script](#)
- [Users without Logon Script](#)

### All Users

Provides the details of all the users of the selected domain(s). For the domains to be listed here, you should have added all the domains from the Domain Settings page.

**How it works:** The report is generated by querying the LDAP for all users with the attribute 'objectClass' set to 'user' i.e. 'objectClass=user'

To view the report, select the domain(s) and click Generate. You can select a specific OU in each domain to view users in it.

### Users with Empty Attributes

This reports enables the administrators to find the list of users who do not have any value specified for a particular attribute.

**How it works:** The report is generated by querying the LDAP for all users with the attributes

"(!physicalDeliveryOfficeName=\*)(!telephoneNumber=\*)(!streetAddress=\*)(!l=\*)(!postalCode=\*)(!homePhone=\*))". Apart from this ADMP can also choose other attributes.

To view the report, select the domain(s), attribute, and click Generate.

## Users without Managers

This report enables the administrators to find the list of users who do not have any managers assigned to them.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(!manager=\*)"

To view the report, select the domain(s) and click Generate.

## Manager based Users

Provides the list of users that directly report to the user (Manager). The users listed as report are those that have the manager property set to this user.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(manager=CN=Administrator,CN=Users,DC=sample,DC=testdomain,DC=com)"

To view the report, select the Domain, Manager, and click Generate.

## Users in more than one Group

Provides the details of the users belonging to more than one group. The Member Of column in the reports provides the group names where the user is a member.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(memberOf=\*))"

To view the report, select the domain(s) and click Generate.

## Recently Deleted Users

Provides the list of user accounts that have been deleted recently. By default, AD maintains the deleted list for a period of 60 days, which can be extended to a max. of 120 days. The deleted user accounts shown in the report pertains to the max. period set in the AD.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(!&(objectClass=contact))(isDeleted=TRUE)"

To view the report, select the domain(s) and click Generate.

## Recently Created Users

Provides the details of the user accounts created recently. This is determined based on the value contained in the CreateTimeStamp attribute.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(createTimeStamp>=20061221120116.0Z)"

To view the report, select the domain(s), specify the number of days, and click Generate.

## Recently Modified Users

Provides the details of the user accounts modified recently. This is determined based on the value contained in the ModifyTimeStamp attribute.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(modifyTimeStamp>=20061221120200.0Z)"

To view the report, select the domain(s), specify the number of days, and click Generate.

## Dial-in Allow Access

This report generates the list of users who have access to Dial-in.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(msNPAllowDialin=TRUE))"

To view the report, select the domain(s) and click Generate.

## Dial-in Deny Access

This report generates the list of users who don't have access to dial-in.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(!(msNPAllowDialin=FALSE)(!(msNPAllowDialin=\*)))))"

To view the report, select the domain(s) and click Generate.

## Users with logon script

Logon scripts are those which run automatically when machine is turned on. This report generates the list of users who have been furnished with logon scripts.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(scriptPath=\*))"

To view the report, select the domain(s) and click Generate.

## Users without logon script

Logon scripts are those which run automatically when users machine is turned on. This report generates the list of users who do not have logon scripts.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(!(scriptPath=\*)))"

To view the report, select the domain(s) and click Generate.

## Account Status Reports

- [Disabled Users](#)
- [Locked Out Users](#)
- [Account Expired Users](#)
- [Recently Account Expired Users](#)

- [Soon-to-expire User Accounts](#)
- [Account never Expiry Users](#)
- [Smart Card Enabled Users](#)
- [Users with Duplicate Attributes](#)

## Disabled Users

Provides the details of the user accounts that are disabled. User accounts can be disabled as a security measure to prevent a particular user from logging on, rather than deleting the user account.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(userAccountControl = ADS\_UF\_ACCOUNTDISABLE)"

This report is auto-generated everyday at 6.00 AM. To view the disabled user accounts of a different domain, select the domain(s) and click Generate.

## Locked Out Users

Provides the details of the user accounts that have been locked out. The user account will get locked on frequent bad login attempts. The Account Lock Out Policy specifies the allowed number of bad login attempts after which the account will be locked. The account will be automatically unlocked after sometime.

**How it works:** The report is generated by querying the LDAP for all users with attribute "lockoutTime".

This report is auto-generated everyday at 6.00 AM. To view the locked user accounts of a different domain, select the domain(s) and click Generate.

## Account Expired Users

Provides the details of the user accounts that have expired. The report is generated for the default domain.

**How it works:** The report is generated by querying the LDAP for all users with the attribute  
 "(! (accountExpires=0)) (! (accountExpires=never)) (accountExpires <= currentTime)"

To view the expired user accounts of a different domain, select the domain(s) and click Generate.

## Recently Account Expired Users

Provides the details of the user accounts whose password has expired in the specified number of days.

**How it works:** The report is generated by querying the LDAP for all users with the attribute  
 "(! (accountExpires=0)) (! (accountExpires=never)) (accountExpires >= SpecifiedTime) (accountExpires <= CurrentTime)"

To view the report, select the domain(s), specify the number of days, and click Generate.

## Soon-to-expire User Accounts

Provides the details of the user accounts that will expire within the specified number of days.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(!!(accountExpires=0))(!(accountExpires=never))(!(accountExpires<=CurrentTime))(accountExpires<=SpecifiedTime)"

To view the report, select the domain(s), specify the number of days, and click Generate.

### Account never expire users

Provides the details of the user accounts which will never expire.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(&(objectCategory=person)(objectClass=user)(!(accountExpires=0)(accountExpires=never)))"

To view the report, select the domain(s), specify the number of days, and click Generate.

### Smart Card Enabled Users Report

Provides the details of all users in the domain enabled with smart card login permissions.

**How it works:** The report is generated by querying the LDAP for users with their account properties set to 'smart enabled for login'.

To view the report, select the Domain, OUs (By clicking on ) and click Generate.

### Users with Duplicate Attributes

Provides the details of all users in a domain, having duplicate attributes. This report is available under the General category of User Reports.

**How it works:** The report is generated by querying the LDAP for all users with duplicate attributes specified.

To view the report, select the Domain, Attribute (By clicking on ) and click Generate.

### Logon Reports

- [Inactive Users](#)
- [Recently Logged on Users](#)
- [Logon Hour Based Report](#)
- [Users Never Logged On](#)
- [Enabled Users](#)
- [Real Last Logon](#)



## Inactive Users

Provides details of the users who have not logged on for the past 'n' days. The inactive users are determined based on their last logon time. All the configured domain controllers are scanned for the last logon time to ensure accuracy. However, if any of the DC's could not be contacted while report generation, the data may be incomplete.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(|(&(objectClass=user)(objectCategory=person)(!lastlogon=\*))(&(objectClass=user)(objectCategory=person)(lastlogon<=SpecifiedTime)))"

This report is auto-generated everyday at 6.00 AM. To view the details for a different period, specify the number of days and click Generate.



**Note:** Users logged on through VPN and users who have not logged out for the specified period will be shown as inactive.

## Recently Logged on Users

Provides the details of the users who have logged on in the past 'n' days. The recently logged on users are determined based on their last logon time. All the configured domain controllers are scanned for the last logon time to ensure accuracy. However, if any of the DC's could not be contacted while report generation, the data may be incomplete.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(&(objectCategory=person)(objectClass=user)(lastLogon>= SpecifiedTime))"

To view the report, select the domain(s), specify the recently logged on user count and click Generate.

## Logon Hour Based Report

Enables to determine the users who have/do not have permission to login on the specified time for the specified days. For example, you can find the list of users who have login permissions on all days from 9.00 to 17.00 hrs

**How it works:** The report is generated by querying the LDAP for all users with the attribute "logonHours" for specified time.

To view the report, specify the following parameters and click Generate:

- Select the domain(s)
- Select the days.
- Specify the start and end time
- Specify whether you require the permitted users list or denied users list for the above period.

## Users Never Logged On

Provides the list of users who have not logged on to the domain. All the configured domain controllers are scanned to get the details.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(&(objectCategory=person)(objectClass=user)(!(lastlogon=0)(!(lastlogon=\*)))))"

To view the report, select the domain(s) and click Generate.

## Enabled users

This report generates the list of all the enabled user accounts in desired domain, to see the results for a specific Organizational Unit click **ADD OU's**.

**How it works:** The report is generated by querying the LDAP for all users with the attribute

"(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))"

To view the report select a domain and click Generate .

## Real Last Logon Report

Provides the details of the latest last logon time of all users in a domain.

**How it works:** The report is generated by querying all the Domain controllers in the domain, i.e. DCs configured under domain settings of ADManager plus, for the users' last logon time and logon count.

**Note:** To obtain accurate results, configure all the DCs available in the domain under the domain settings of ADManager Plus.

To view the report,

- Click on Real Last Logon link under AD Reports.
- Select the domain.
- Click the Advanced Filter link to obtain more options.
- Click on the Generate button.

## Nested Reports

- [Users in Groups](#)
- [Groups for Users](#)
- [Users not in a Group](#)
- [Members only of Domain User Group](#)

## Users in Groups

Provides the details of the users of selected groups.

**How it works:** The report is generated by querying all users and checking whether 'memberOf' value is same as specified Group.

To view the report, select the domain and the groups and click Generate.

## Groups for Users

Provides the details users in the nested groups, i.e., groups that contain other groups as its members in the domain. This will list the group that the specified user is a member and all the other groups where the users' group is a member.

**How it works:** The report is generated by querying the LDAP for all groups and checking whether member is specified user.

To view the report, select the Domain, Users (By clicking on select) and click Generate.

## Users not in a Group

Provides the details of the users who are not members of a specified group.

**How it works:** The report is generated by querying the LDAP for all users and check 'memberOf' is specifiedGroup.

To view the report, select the domain and the group and click Generate.

## Users not in a Group

Provides the details of the users who are not members of a specified group.

**How it works:** The report is generated by querying the LDAP for all users and check 'memberOf' is specifiedGroup.

To view the report, select the domain and the group and click Generate.

## Members only of Domain User Group

Provides the details of the users that are members of the Domain User Group alone.

**How it works:** The report is generated by querying the LDAP for all users with attributes (&(objectCategory=person)(objectClass=user)(!(sAMAccountType=805306370))(primaryGroupID=513)(!(memberOf=\*))

To view the report, select the domain and click Generate.

## Active Directory Contacts Reports

---

- [All Contacts Report](#)
  - [Mail Enabled Contacts Report](#)
- 

### All Contacts Reports

This report provides the list of all Contacts in a domain.

**How it works:** The report is generated by querying the domain for Contact Objects. The LDAP Query associated with this operation is  
(&(objectCategory=person)(objectClass=contact)).

To View the reports,

- Click on All Contacts under AD Reports.
- Select the domain
- Select the OU using ADD OUs link.
- Click on the Generate button.

### Mail Enabled Contacts Report

This report provides the list of mail enabled contact objects in the domain.

**How it works:** The report is generated by querying the domain for mail enabled contacts. The LDAP Query associated with this operation is  
(&(objectCategory=person)(objectClass=contact)(mailnickname=\*)(targetAddress=\*))

To View the report,

- Click on All Contacts under AD Reports.
- Select the domain
- Select the OU using ADD OUs link.
- Click on the Generate button.

## Active Directory Password Reports

---

- [General Password Reports](#)
  - [Password Status Reports](#)
- 

### General Password Reports

#### Recently Bad Logged on Users

This report provides the list of users who failed to login.

**How it works:** The report is generated by querying users with LDAP attributes (badPasswordTime>=specified time).

To View the reports Select the domain, enter the number of days and click generate.

#### Users who cannot change their password Report

This report provides the list of users who cannot change their password.

**How it works:** The report is generated by querying users with userAccountControl flag set to "Password Cannot Change".

To View the reports Select the domain and click generate.

#### Users whose Password Never Expires Report

This report provides the list of users whose passwords never expire.

**How it works:** The report is generated by querying the users with userAccountControl flag set to "Password Never Expires".

To View the reports Select the domain and click generate.

#### Users with Change Password at Next Logon

This report provides the list of users whose passwords must be changed in their next Logon.

**How it works:** The report is generated by querying the LDAP for all users with attributes (&(objectCategory=person)(objectClass=user)(pwdLastSet=0))

To View the report, select the domain and click generate.

### Password Status Reports

#### Know the Tabs

**Disable:** You can select the user accounts that you need to disable and click on Disable. This helps in keeping Active Directory free from Password Expired users preventing an unauthorized access to the expired accounts.

**Change Password at Next Logon:** This Prompts the selected users to change their password in their next logon. This helps in having Passwords active and secure.  
**More Actions:** This will enable you to change the Attributes settings of the selected user. Clicking on this will lead you to AD Management where in you can select the attribute type and define the new settings by Domain wise.

### **Password Expired Users Report**

This report provides the list of users whose passwords are expired.

**How it works:** The report is generated by querying the users with userAccountControl flag not set to "Password Never Expires" and attributes "`(!(pwdLastSet=0))(pwdLastSet<=time based on domain password policy)`".

To View the reports Select the domain, enter the number of days and click generate.

### **Soon-to-expire User Passwords Report**

This report provides the list of users whose passwords will expire in given 'n' days.

**How it works:** The report is generated by querying the users with userAccountControl flag not set to "Password Never Expires" and attributes "`(!(pwdLastSet<=time based on domain password policy))(pwdLastSet<=specified time)`".

To View the reports Select the domain, enter the number of days and click generate.

**Recently Password Changed users Report:** This report provides the list of users whose passwords are modified in given 'n' days.

**How it works:** The report is generated by querying the LDAP for attributes `(&(!(pwdLastSet=0))(!(pwdLastSet>=specified time)))`.

To View the reports Select the domain, enter the number of days and click generate.

### **Recently Password Unchanged users Report**

This report provides the list of users whose passwords are not modified in given 'n' days.

**How it works:** The report is generated by querying the LDAP for attributes `(&(!(pwdLastSet=0))(pwdLastSet>=specified time))`.

To View the reports Select the domain, enter the number of days and click generate.

## Active Directory Group Reports

---

- [General Reports](#)
  - [Group Type Reports](#)
- 

### General Reports

- [Groups without Members](#)
- [Top N Big Group](#)
- [All Groups](#)
- [Managed Groups](#)
- [Unmanaged Groups](#)
- [Group Members](#)

### Groups without Members

Provides you the details of group that has no members. This report will be useful to find the unwanted groups in the domain.

**How it works:** The report is generated by querying the LDAP for all groups and check member status and then lists.

To view the report, select the domain(s) and click Generate.

### Top N Big Group

Provides the details of the large groups in the domain based on its members count. This will be helpful in determining the large groups in the domain.

**How it works:** The report is generated by querying the LDAP for all groups and check members then list top n

To view the report, select the domain(s), specify the number of top big groups you wish to see, and click Generate.

### All Groups

Provides the details of all the groups of the given domain.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "(objectcategory=group)".

To view the report, select the domain(s) and click Generate.

### Managed Groups

Provides the details of the groups that have managers.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "&(objectcategory=group)(managedBy=\*)".

To view the report, select the domain(s) and click Generate.

## Unmanaged Group

Provides the details of the groups that do not have managers.

**How it works:** The report is generated by querying the LDAP for all users with the attribute "&(objectcategory=group)(!managedBy=\*)".

To view the report, select the domain(s) and click Generate.

## Group Members

Provides the details of the users in the selected Group.

**How it works:** The report is generated by querying the LDAP for all users and check 'memberOf' is specifiedGroup.

To view the report, select the domain(s) and click Generate.

## Group Type Reports

- [Security Groups](#)
- [Group types and Scope](#)
- [Distribution Groups](#)

## Security Groups

Provides the details of the security groups available in the selected domain(s).

**How it works:** The report is generated by querying the LDAP for all groups with grouptype set to security enabled.

To view the report for a different domain, click the Create New Report link, select the required domains, and click Generate.

## Group Types and Scopes

This reports provides the details of Groups based on their 'type' and 'scope'. The group type can be either security or distribution and its scope can be Global, Domain Local, or Universal.

**How it works:** The report is generated by querying the LDAP for all groups with grouptype set to specified type and scope.

To view the report, select the domain(s), their type, scope, and click Generate.

## Distribution Groups Report

It provides the list of all distribution groups available. Distribution groups arrange the users with one or more common attributes into one group and eases the information convention.





**How it works:** The report is generated by querying the LDP.P to specify the 'group type' of that particular group. This information differentiates distribution groups from security groups.

To view the report, select the domain(s) and click **Generate**.



# Active Directory Computer Reports

---

- [General Reports](#)
  - [Account Status Reports](#)
- 

## General Reports

- [Workstation Computers](#)
- [Domain Controllers](#)
- [OS Based Report](#)
- [Computers Trusted for Delegation](#)
- [Recently Modified Computers](#)
- [Recently Created Computers](#)
- [Recently Deleted Computers](#)
- [Managed Computers](#)
- [Unmanaged Computers](#)

### Workstation Computers

Provides the details of the workstations in the domain. All the computers except Servers and Domain Controllers are termed as workstations. This report is auto-generated everyday at 6.00 AM.

To view the details for a different domain, select the domain(s) and click **Generate**.

### Domain Controllers

Provides the details of the domain controllers in the domain. This report is auto-generated everyday at 6.00 AM.

To view the details for a different domain, select the domain(s) and click **Generate**.

### OS Based Report

Provides the details of the computers based on the operating system versions.

To view the report, select the domain(s), select the OS version, and click **Generate**.

### Computers Trusted for Delegation

Provides the details of the computers that are trusted for delegation. If a machine is set to **Trusted for delegation**, the service can impersonate a user to use other network services.

To view the report, select the domain(s) and click **Generate**.

## Recently Created Computers

Provides the details of the computer objects that were created recently. This is determined based on the user specified days in the domain.

**How it works:** The recently created computers list is picked up by querying the domain with the associated LDAP query, (&(objectCategory=computer)(objectClass=computer)(createTimeStamp>=20080815042538.0Z)).

To view the report, select the domain(s) and OUs, specify the number of days, and click **Generate**.

## Recently Modified Computers

Provides the details of the computer objects that were modified recently. This is determined based on the value contained in the ModifyTimeStamp attribute.

To view the report, select the domain(s), specify the number of days, and click **Generate**.

## Recently Deleted Computers

Provides the details of the computer objects that were deleted recently. This is determined based on the user specified days in the domain.

**How it works:** The recently created computers list is picked up by querying the computer objects from the deleted objects container in AD. The associated LDAP query is , (&(isDeleted=TRUE)(whenChanged>=20080815042700.0Z)).

To view the report, select the domain(s) and OUs, specify the number of days, and click **Generate**.

## Managed Computers

Provides the details of the computer objects that are managed by any of the domain users.

To view the report, select the domain(s) and click **Generate**.

## Unmanaged Computers

Provides the details of the computer objects that are not managed by the domain users.

To view the report, select the domain(s) and click **Generate**.

## Account Status Reports

- [Inactive Computers](#)
- [Disabled Computers](#)

### Inactive Computers

Provides the details of the inactive computers for the specified number of days. The inactive computers are determined based on their last logon time. All the configured domain controllers are scanned for the last logon time to ensure accuracy. However, if any of the DCs could not be contacted while report generation, the data may be incomplete.

This report is auto-generated everyday at 6.00 AM. To view the details for a different period, specify the number of days and click **Generate**.

### **Disabled Computers**

Provides the details of the computer objects that are disabled in the domain. Disabling computer account breaks that computer's connection with the domain and that computer will not be able to authenticate to the domain. This report is auto-generated everyday at 6.00 AM.

To view the details for a different domain, select the domain(s) and click **Generate**.

## Active Directory Exchange Reports

---

- [General Reports](#)
  - [Distribution Lists](#)
  - [Delivery Recipient Settings](#)
  - [Feature Based Reports](#)
- 

### General Reports

- [Mail-Box Enabled Users](#)
- [Mail Enabled Users](#)
- [Mail Enabled Groups](#)
- [Users with Email Proxy Enabled](#)
- [Groups with Email Proxy Enabled](#)

### Mailbox enabled users Report

It provides the list of all mailbox-enabled users. All mailbox-enabled users have a mailbox in exchange server.

How it works: The report is generated by querying the LDAP for all users with the attributes 'mailNickName' and 'msExchHomeServer'

To view the report, select the domain(s) and click Generate. You can also select the OU's of each domains to view the users of that OU's.

### Mail enabled users Report

It provides the list of all mail-enabled users. Mail enabled users can receive messages only at an external mail address, they have no mail boxes in exchange server but still their names will be listed in the global address list.

How it works: The report is generated by querying the LDAP for all the users with attributes 'mailNickname' and 'Targetaddress'.

To view the report, select the domain(s), attribute, and click Generate.

### Mail enabled groups Report

A mail-enabled group represents a collection of recipient objects. Its purpose is to speed up the distribution of messages to multiple email addresses. Mail-enabled groups can be either security or distributed.

How it works: The report is generated by querying the LDAP for all groups with attributes 'mailNickname' and object category as group.

To view the report, select the domain(s) and click Generate.

[Top](#)

## Users with Email Proxy addresses Report

It provides the list of all users with Email proxy address. ADMP searches for the LDAP attribute "proxyAddresses" with the value specified.

How it works: The report is generated by querying the LDAP for the users by the value specified to the attribute "proxyAddresses" i.e. Proxy address=\*searchstring\*.

To view the report, select the Domain, enter proxy address and click Generate.

## Groups with Email proxy addresses Report

It provides the list of all groups with Email proxy address. ADMP searches for the LDAP attribute "proxyAddresses", with the value specified.

How it works: The report is generated by querying the LDAP for the users by the value specified to the attribute "proxyAddresses" i.e. Proxy address=\*searchstring\*.

To view the report, select the Domain, enter proxy address and click Generate.

## Distribution Lists

- [Distribution List Members](#)
- [Non-Distribution List Members](#)

## Distribution List Members Report

It provides the list of users who is a member in any one of the distribution groups.

How it works: The report is generated by querying the LDAP for the distribution groups for the attribute "member".

To view the distribution list members of a different domain, select the domain(s) and click Generate.

## Non-Distribution List Members Report

It provides the list of members who do not belong to any distribution group.

How it works: The report is generated by querying the LDAP for the attribute "member" in all the groups except distribution.

To view the non-distribution list members report of a different domain, select the domain(s) and click Generate.

## Delivery Recipient Settings

- [Default Sending Size](#)
- [Restricted Sending Size](#)
- [Default Recipient Size](#)
- [Restricted Recipient Size](#)
- [Default Receiving Size](#)
- [Restricted Receiving Size](#)
- [Default storage Limit](#)

- [MailBox Size Limits](#)
- [Users Hidden From Exchange Address Lists](#)
- [Accept Messages From Everyone](#)
- [Accept Messages Restricted](#)
- [Users Mail Forwarded To](#)

## Default sending size Report

This report provides the list of all users who have assigned a default size for the messages they send i.e. these users can send messages only of default size that is set.

How it works: The report is generated by querying all users with the LDAP attribute "submissionContLength", set to no value.

To view the details for a different period, specify the number of days and click Generate.

## Restricted sending size Report

This report provides the list of all users who have restrictions on the size of the message they can send.

How it works: The report is generated by querying all users with the LDAP attribute "submissionContLength", set to a value.

To view the report, select the domain(s) and click Generate.

## Default recipient size Report

This report provides the list of all users who can send messages to default number of recipients.

How it works: The report is generated by querying the LDAP for all users with the attribute "msExchRecipLimit", without a value

To view the report, select the domain(s) and click Generate.

## Restricted recipient size Report

This report provides the list of all users who have restriction on sending message to number of recipients.

How it works: The report is generated by querying the LDAP for all users with the attribute "msExchRecipLimit", containing a value.

To view the report, select the domain(s) and click Generate.

## Default receiving size Report

This report provides the list of all users who can receive messages of default size.

How it works: The report is generated by querying the LDAP for all users with the attribute "delivContLength", without a value.

To view the report, select the domain(s) and click Generate.

### Restricted receiving size Report

This report provides the list of all users who have restriction on size of receiving messages.

How it works: The report is generated by querying the LDAP for all users with the attribute "delivContLength", containing a value.

To view the report, select the domain(s) and click Generate.

### Default storage limit Report

While creating a mailbox-enabled user, AD prompts to specify the storage limit to a user. If there are no specific properties applied to this user account, then default storage limits are applied. This report provides the list of all users who have default storage limits.

How it works: ADMP sends a query to LDAP database for all the users with attribute "mDBUseDefaults", **set to TRUE**.

To view the report, select the domain(s) and click Generate.

### Mailbox size limits Report

This report provides the list of all users who have limitation in the mailbox size.

How it works: ADMP sends a query to LDAP database for all the users with attribute "mDBUseDefaults", **set to FALSE**.

To view the report, select the domain(s) and click Generate.

### Users hidden from exchange address lists Report

This report provides the list of all users with their mail addresses hidden from exchange address list.

How it works: ADMP sends a query to AD for all users with the attribute "msExchHideFromAddressLists", **set to TRUE**.

To view the report, select the domain(s) and click Generate.

### Accept Messages from everyone Report

This report provides the list of users who can receive messages from all users.

How it works: ADMP retrieves the value for all users who does not have LDAP attribute "authoring".

To view the report, select the domain(s) and click Generate.

### Accept messages restricted Report

This report provides the list of users who have restriction in receiving messages i.e. they are restricted to receive messages from a set of users.




How it works:ADMP retrieves the value from LDAP attribute **unauthOrig** and **authoring** set to a value.

To view the report, select the domain(s) and click Generate.

## Users mail forwarded to Report

This provides the list of users whose mails are forwarded to a specified user.

How it works: ADMP retrieves the value from LDAP attribute **Query-altRecipient=specific user**.

To view the report, select the domain(s) and user (click on ) and click Generate.

## Feature Based Reports

- [OMA Enabled](#)
- [OMA Disabled](#)
- [OWA Enabled](#)
- [OWA Disabled](#)
- [POP3 Enabled](#)
- [POP3 Disabled](#)
- [IMAP4 Enabled](#)
- [IMAP4 Disabled](#)

### OMA Enabled users Report

This provides the list of "Outlook Mail Access" enabled users. LDAP contains different values for the attribute "protocolSettings"

How it works: ADMP retrieves the respective value for OWA enabled users and lists.

To view the report, select the domain, user and click Generate.

### OMA Disabled users Report

This provides the list of "Outlook Mail Access" disabled users. LDAP contains different values for the attribute "protocolSettings"

How it works: ADMP retrieves the respective value for OWA disabled users and lists.

To view the report, select the domain, user and click Generate.

### OWA Enabled users Report

This provides the list of outlook web access enabled users.

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for OWA enabled users and provides the list.

To view the report, select the domain, user and click Generate.

## **OWA Disabled users Report**

This provides the list of outlook web access disabled users.

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for OWA disabled users and provides the list.

To view the report, select the domain, user and click Generate.

## **POP3 Enabled Report**

This provides the list of POP3 enabled users

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for POP3 enabled users and provides the list.

To view the report, select the domain, user and click Generate.

## **POP3 Disabled Report**

This provides the list of POP3 disabled users

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for POP3 disabled users and provides the list.

To view the report, select the domain, user and click Generate.

## **IMAP4 Enabled Report**

This provides the list of IMAP4 enabled users.

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for IMAP4 enabled users and provides the list.

To view the report, select the domain, user and click Generate.

## **IMAP4 Disabled Report**

This provides the list of IMAP4 disabled users.

How it works: For the attribute "protocolSettings", LDAP contains different values; ADMP retrieves the respective value for IMAP4 disabled users and provides the list.

To view the report, select the domain, user and click Generate.

## Active Directory Terminal Services Reports

---

- [Users with Terminal Services Properties](#)
  - [Users with Terminal Server Access](#)
- 

### Users with Terminal Services Properties

This report provides the list of all users in a domain with their respective terminal services properties.

How it works: The report is generated by querying(LDAP) the domain for Users and their associated Terminal Services properties.

To View the reports,

- Click on Terminal Services Reports under AD Reports.
- Select the domain.
- Select the OU using ADD OUs link.
- Click on the Generate button.

### Users with Terminal Server Access

This report provides the list of users in a domain, having 'Terminal Server' Access.

How it works: The report is generated by querying the domain for users with "allow logon to terminal server access" attribute enabled.

To View the report,

- Click on All Contacts under AD Reports.
- Select the domain.
- Select the OU using ADD OUs link.
- Click on the Generate button.

# Active Directory GPO Reports

---

## GPO Reports

- [All GPO's Report](#)
  - [Recently Created GPO's Report](#)
  - [Recently Modified GPO's Report](#)
  - [Disabled GPO's Report](#)
  - [Unused GPO's Report](#)
  - [Frequently Modified Computer Settings GPO's Report](#)
  - [Frequently Modified User Settings GPO's Report](#)
  - [OU Linked GPO's Report](#)
  - [Site Linked GPO's Report](#)
  - [GPO Blocked Inheritance Containers Report](#)
  - [Computer Settings Disabled GPO's Report](#)
  - [User Settings Disabled GPO's Report](#)
  - [Frequently Modified GPO's Report](#)
- 

## All GPO's Report

This provides the list of all Group Policy Objects present in the Active Directory.

How it works: The report is generated by querying the LDAP for all *objectClass* set to *groupPolicyContainer* i.e. "objectClass=groupPolicyContainer".

To view the report, select the domain, enter the number of days and click Generate.

## Recently created GPO's Report

This provides the list of Group Policy Objects and Active directory objects linked to it, that are recently created in the past "n" days.

How it works: The report is generated by querying the LDAP for *createTimeStamp* set to more than or equal to *SpecifiedTime* i.e. "createTimeStamp>=SpecifiedTime".

To view the report, select the domain, enter the number of days and click Generate.

## Recently modified GPO's Report

This provides the list of Group Policy Objects and Active directory objects linked to it, that are recently modified in the past "n" days.

How it works: The report is generated by querying the LDAP for *modifyTimeStamp* set to more than or equal to *SpecifiedTime* i.e. "modifyTimeStamp>=SpecifiedTime".

To view the report, select the domain, enter the number of days and click Generate.

### Disabled GPO's Report

This provides the list of all disabled GPO's. Both the computer configuration and user configuration settings are disabled.

How it works: The report is generated by querying the LDAP for all *objectClass* set to *groupPolicyContainer* and with a flag value 3 i.e. "objectClass=groupPolicyContainer" with flag=3.

To view the report, select the domain and click Generate.

### Unused GPO's Report

This provides the list of Group Policy Objects that are not used since they are linked to a GPO.

How it works: The report is generated by querying the LDAP for all GPO's that are not linked to any other objects in the domain and reiterating the search to all GPO's.

To view the report, select the domain and click Generate.

### Frequently modified computer settings GPO's Report

This provides the list of Group Policy Objects with frequently modified computer settings.

How it works:: The report is generated by querying the LDAP for attribute *versionNumber*; as the computer settings are modified the version number also changes.

To view the report, select the domain, enter the number of days and click Generate.

### Frequently Modified user Settings GPO's Report

This provides the list of Group Policy Objects with frequently modified user settings.

How it works: The report is generated by querying the LDAP for attribute *versionNumber*; as the user settings are modified the version number also changes.

To view the report, select the domain, enter the number of days and click Generate.

### Domain Linked GPO's Report

This provides the list of Group Policy Objects that are linked to domains.

*How it works:* The report is generated by querying the LDAP for all GPO's that are linked to any domain object by reiterating the search to all GPO's.

To view the report, select the domain and click Generate.

### OU linked GPO's Report

This provides the list of Group Policy Objects that are linked to organizational units.

How it works: The report is generated by querying the LDAP for all GPO's that are linked to any domain object by reiterating the search to all GPO's.

To view the report, select the domain and click Generate.

### Site linked GPO's Report

This provides the list of Group Policy Objects that are linked to any site.

How it works: The report is generated by querying the LDAP for all GPO's that are linked to any site by reiterating the search to all GPO's.

To view the report, select the domain and click Generate.

### GPO blocked inheritance container Report

This provides the list of Group Policy Objects that are blocked from inheritance from their parent objects.

To view the report, select the domain and click Generate.

### Computer settings disabled GPO's Report

This provides the list of Group Policy Objects with computer settings disabled.

How it works: The report is generated by querying the LDAP for *objectClass* set to *groupPolicyContainer* with a flag value 3 or 2 i.e. "objectClass=groupPolicyContainer" (|(flags=3)(flags=2)).

To view the report, select the domain and click Generate.

### User settings disabled GPO's Report

This provides the list of Group Policy Objects with user settings disabled.

How it works: The report is generated by querying the LDAP for "objectClass" set to *groupPolicyContainer* with a flag value 3 or 1 i.e. "objectClass=groupPolicyContainer" (|(flags=3)(flags=1)).

To view the report, select the domain and click Generate.

### Frequently modified GPO's Report

This provides the list of Group Policy Objects that are frequently modified.

How it works: The report is generated by querying the LDAP for attribute *versionNumber*; as the computer settings are modified the version number also changes.

To view the report, select the domain, enter the number of days and click Generate.

# Active Directory OU Reports

---

## OU Reports

- [All OU's](#)
  - [Empty OU's](#)
  - [Users Only OU's](#)
  - [Computers Only OU's](#)
  - [Recently Created OU's](#)
  - [Recently Modified OU's](#)
  - [GPO Linked OU's](#)
  - [GPO Blocked Inheritance OU's](#)
- 

## All OU

This provides the list of all Organizational units present in a selected Domain.

How it works: The report is generated by querying the LDAP for attribute objectClass set to organizationalUnit i.e. *objectClass=organizationalUnit*

To view the report, select the domain(s) and click Generate.

## Empty OU

This provides the list of all empty Organizational units in a selected Domain.

How it works: The report is generated by querying the LDAP for all OU's and check for child objects.

To view the report, select the domain(s) and click Generate.

## Users only OU

This provides the list of all Organizational units that contain only users in a selected Domain.

How it works: The report is generated by querying the LDAP for all OU's and check for user objects.

To view the report, select the domain(s) and click Generate.

## Computers only OU

This provides the list of all Organizational units that contain only computers in a selected Domain.

How it works: The report is generated by querying the LDAP for all OU's and check for computer objects.

To view the report, select the domain(s) and click Generate.

### Recently created OU

This provides the list of all Organizational units that were created in past n days in a selected Domain.

How it works: The report is generated by querying the LDAP for attribute *createTimeStamp* set to greater than equal to specified time i.e. *createTimeStamp* >= *specifiedtime*.

To view the report, select the domain(s), enter the number of days and click Generate.

### Recently modified OU

This provides the list of all Organizational units that are modified in past n days in a selected Domain.

How it works: The report is generated by querying the LDAP for attribute *modifyTimeStamp* greater than or equal to *specifiedtime* i.e. *modifyTimeStamp* >= *specifiedtime*.

To view the report, select the domain(s), enter the number of days and click Generate.

### GPO Linked OU

This provides the list of all Group Policy Objects that are linked to an Organizational unit in a selected Domain.

How it works: The report is generated by querying the LDAP for attribute gPo Link set equal to any gPo i.e. *gPLink* = *anygpo*.

To view the report, select the domain(s) and click Generate.

### GPO blocked inheritance OU

This provides the list of all Organizational units with Group Policy Objects blocked from inheritance.

How it works: The report is generated by querying the LDAP for attribute gPOptions set to 1 i.e. *gPOptions* = 1

To view the report, select the domain(s) and click Generate.



## Active Directory NTFS Reports

---

NTFS Reports Provides detailed information about the Permissions on Folders/ Sub folders and Files/ Sub Files.

- [Shares in the Servers](#)
- [Permissions for Folders](#)
- [Folders Accessible by Accounts](#)
- [Non-Inheritable Folders/Files](#)

### Shares in the Servers

This report can be used to list all the Shares and their Permissions in specified Server.

To View the report:

1. Select the domain
2. Click on Select to choose the computers (you can also search for the computers using QUICK FIND)
3. Click on Generate button

### Permissions for Folders

This report can be used to list the Users/Groups that have access to files and folders in a specified path

To View the Report:

1. Select domain
  2. Enter Shared resource path      Example: \\<file-servername>\<sharename>\<directory>
  3. Click on Generate button
- or
1. Select Domain
  2. Select the computer
  3. Choose Get Shares
  4. Check Parent Folder or Sub Folders also
  5. Click on Generate button

### Folders Accessible by Accounts

This report can be used to list all the folders and files over which the specified account has any permission

To View the Report:

1. Select Domain
2. Select Accounts
3. Check for Folders in
4. Choose type of Access
5. Click on Generate button

## **Non-Inheritable Folders/Files**

Provides the list of all folders and files that are restricted to inherit the permissions from their parent objects.

To View the Report:

1. Enter the directory path
  2. Click on Generate button
-

# Active Directory Security Reports

---

## Access Over Objects Reports

- [AD Objects accessible by Accounts](#)
- [Non-Inheritable Objects](#)
- [Subnets accessible by Accounts](#)
- [Servers accessible by Accounts](#)

### AD Objects accessible by Accounts

This report is used to view the Active Directory objects that are accessible by Users/Groups specified.

To view the report:

1. Select domain. Select OUs if needed.
2. Select the accounts.(More than one account can be selected)
3. Select Access Type
4. Click on Generate button

### Non-Inheritable Objects

This report is used to view the non-inheritable objects in the selected domain(s).

To view the report:

1. Select domain. Add OUs if needed
2. Click on Generate button

### Subnets accessible by Accounts

This report can be used to list all the subnets that can be accessed by the specified Users/Groups.

To view the report:

1. Select domain
2. Select Accounts ( You can select more than one Account)
3. Click on Generate button

### Servers accessible by Accounts

Generate this report to list the servers that can be accessed by the specified Users/Groups.

To view this report:

1. Select Domain
2. Select Accounts (You can select more than one Account)

3. Click on Generate button

### **Permission Reports**

- [Subnet Permissions](#)
- [Server Permissions](#)

#### **Subnet Permissions**

Generate this report to list the Users/Groups that have access to the given subnets.  
To view this report:

1. Select Domain
2. Select Subnets (You can choose more than one Subnet)
3. Click on Generate button

#### **Server Permissions**

Generate this report to list the Users/Groups that have access to the given servers.  
To view Report:

1. Select Domain
2. Select Computers ( You can select more than one computer)
3. Click on Generate button

## Active Directory Policy Reports

---

- [Password Policy](#)
  - [Account Lockout Policy](#)
  - [Printer Reports](#)
- 

### Password Policy

Provides the details of the password policies, such as Maximum Password Age, Minimum Password Age, Maximum Password Length, Complexity, and so on, of the selected domain(s).

To view the report, select the domain(s) and click **Generate**.

### Account Lockout Policy

Provides the details of the account lockout policies, such as Lockout Duration, Lockout Threshold, and so on, of the selected domain(s).

To view the report, select the domain(s) and click **Generate**.

### Printer Reports

Provides the list of Printers for the selected domain(s).

To view the report, select the domain(s) and click **Generate**.

# Scheduling Reports

---

## Overview

This section would help you to schedule reports and perform effective schedule management. The topics covered are listed below:

- [Scheduling Reports](#)
  - [Scheduler Creation](#)
- [Managing Schedules](#)
- [Column Customization in Scheduled Reports](#)

## Scheduling Reports

You can schedule the reports generation by adhering to the steps mentioned below:

- Select the **AD Reports** Tab.
- Select the **Schedule Reports** link at the top right corner of the page.
- Select the **Schedule New Reports** link at the top right corner to create a new schedule.

Note: You will encounter a Pop up message if the Mail Server is not configured. You can do that using the [Configure Mail Server Settings](#) link to proceed further.

- Specify the **Scheduler Name** and **Description** details.
- Choose the appropriate Domain from the **Select Domain** list. Click on the **Add OUs** link, to specify the OUs for the **Domain**.

## Scheduler Creation

The Scheduler creation enables you to create a schedule based on the three criteria mentioned below:

1. [Select Reports](#)
2. [Schedule Duration](#)
3. [Select Report Format](#)
4. [Email Address to send Reports](#)

### 1. Select Reports- The Select Reports feature comprises of three sections

- Click on the **Report Type** you want to schedule.
- Select the reports from the **Available Reports** list. Enter the **Input parameter** details if asked for.
- You can view the reports in the **Selected Reports** list.
- Use the **Remove** link to eliminate any report from the selected list.

### 2. Schedule Duration

The time span of report generation can be set based on your requirements. The **duration** and **time** can be set with the following options:

- **Daily**-This option is for scheduling a report everyday at a particular time desired by you.
- **Weekly**-This option is for scheduling a report at a particular time on a certain day of the week desired by you.
- **Monthly**-This option is for scheduling a report on a particular day of the month at a particular time desired by you.
- **Hourly**-This option is for scheduling a report generation to be performed on an hourly basis, starting at the specified date and time desired by you.

### 3. Select the Report Format to be mailed

You can select the format in which you would like to have the report mailed. Select the PDF, HTML, CSV, XLS or CSVDE formats, based on your choice. The Storage Path link will enable you to specify the location where you would like the reports to be stored.

### 4. Email Address to send Reports

The **email** address of the **recipient** can be mentioned in this field.

You can use the **Advanced Mail Settings** link to receive the Report as an attachment in your email. Select the "**Enable Attachment**" checkbox to choose amongst the "**Send As Files**" or "**Send as Zip format**" options. In case, no choice of format is specified, a report link will be sent in the email, from which the zipped file of the report can be obtained. However, if the "**Mail Content: Send link in mail**" checkbox is not enabled (left unchecked), the recipient will be inhibited from receiving the link in his mail. The report mails can be sent to **Multiple recipients** by separating their IDs by **comma**.

**Tip:** You can use the **Send Test Mail** option to confirm if the recipient email id is a valid one.

Click the **SAVE** button to add the schedule to the schedule reports list.

### View Scheduled tasks

Click the View Scheduled Tasks link to see the list of tasks you have scheduled.

## Scheduled Reports History

Click the **Scheduled Reports History** link. to view scheduled reports details from the **Report Center**. Details like **Scheduler name**, **Description**, **Configured OUs**, **Started Time**, **Scheduler Status** ( **SUCCESS/ SKIPPED/ PROCESSING**), **Report Details** and **Message** are available here. The **Scheduled Reports** link under **Report Details** gives you a zipped version of the scheduled report that had been generated.

### Managing Schedules

The scheduled tasks once created, can be managed from the UI. From the schedules UI, you can

- **Enable/Disable** schedules
- **Remove** the schedules
- **Edit** the scheduled reports

### Enabling/Disabling a Schedule

At times, you would require to temporarily stop the generation of a scheduled report and would like to resume it again at some other point of time.

**To disable a schedule.**

- Click the **AD Reports** Tab
- Click the Schedule Report link to open the Schedule Reports page
- You will find a list of **Scheduled reports** on this page.
- Click on the **Enable** icon in the Action tab column, appropriate to the Scheduled Report you want to disable.
- The **Enable** icon will be replaced by the **Disable** icon.

**To enable a schedule.**

- Click on the **Disable** icon in the **Action** tab column, appropriate to the Scheduled Report you want to enable
- The **Disable** icon will be replaced by the **Enable** icon.

**Deleting a Schedule**

When a Schedule is no longer useful, you can **delete** it from the Schedule Reports list.

**To delete a schedule.**

- Click the **AD Reports** Tab
- Click the Schedule Report link to open the Schedule Reports page
- You will find a list of **Scheduled reports** on this page.
- Click on the **Delete** icon in the **Action** tab column, appropriate to the Scheduled Report you want to delete.
- The deleted Schedule will no longer be listed.

**Edit a Schedule**

You can make changes to the existing schedule as may be required using the **Edit** option.

Follow the steps to edit a schedule:

- Click the **AD Reports** Tab
- Click the Schedule Report link to open the Schedule Reports page
- You will find a list of **Scheduled reports** on this page
- Click on the **Edit** icon in the Action tab column, appropriate to the Scheduled Report you want to update.
- You can make the changes in the Schedule Reports page.
- Click on the **UPDATE** button to save the changes.
- Click on the **View scheduled tasks** link to see the updated schedule in the list.

**Column Customization in Scheduled Reports(for HelpDesk)**

HelpDesk Technicians can also schedule report generation depending on the permissions of the HelpDesk Role they belong to. The procedure to schedule report generation is the same as explained in the previous section. While scheduling the reports, the HelpDesk Technician can also customize the columns that need to appear in the report that is scheduled. So everytime, the scheduler runs, the column settings applicable to that particular HelpDesk Technician will be applied.



## Audit Logs

---

**Audit Log** is a file/document which records the details of any **AD Management task** you perform using your **AD Manager Plus**. The Audit Log is an effective tracking tool which helps in tracing down events like Reset Password, Delete Users, Create/Modify Users, etc.,

Audit Logs essentially help you to:

- **Identify** what **accounts** are associated with certain tasks.
- **Review chronologically** and determine what was happening before and during the AD Management task.
- **Detect problems** like investigating casual factors of failed jobs.

Audit Logs can be found under **audit-data/audit/technicians/<log folder>** of the **Program Files** of the product.

An Audit Log essentially contains the following three basic details of the Task.

- **What**
- **When**
- **Who**

### What of the Task

Audit Logs store information about the task that was performed while the event got triggered. Details of all those attributes, whose values were updated gets recorded in the Log file for future reference. For example, if a user is moved from one Organizational unit to another using ADManager Plus, the audit log generated will contain the details of the source and destination OUs under the **From** and **To** headings respectively.

### When of the Task

Audit files save the Date and Time of Event occurrence. This serves as a useful resource to find out the time of occurrence of a AD Management Task, at a later date.

### Who of the Task

The details of the person who had performed a AD Management task is also tracked in the Audit Log file. If the task was performed by the Administrator, the log is stored in **admin** under **technician** folder. For a Help Desk Technician, the logs get stored in a folder named after the Technician and his associated domain. For example, John-ADMP means that this folder contains the logs which got generated while the Help Desk Technician, John initiated AD Management Tasks in the ADMP domain.

## Help Desk Delegation Overview

---

ADManager Plus help desk delegation supports the administrator to focus on the matters that really do require his attention and delegate other tasks to dedicated help desk technicians.

The help desk technicians provided with limited access and privileges handle tasks assigned to them like reset passwords, create users, unlock users, rename users etc., with ease and efficiency.

- [What is help desk delegation](#)
- [What is Help Desk Technician](#)
- [What is Help Desk Role?](#)
- [What is OU based Delegation?](#)
- [How to create a help desk technician?](#)
- [How to create a help desk role?](#)
- [Work Flow for Help Desk Delegation](#)
- [Granular Authorization](#)
- [OU Restriction](#)
- [Enable/Disable HelpDesk Technicians](#)
- [Multiple Domain Management for HelpDesk Technicians](#)
- [Group Delegation for Help Desk Technicians](#)
- [Login Using Sample HelpDesk Technician](#)
- [How help desk delegation helps you](#)
- [What is the scope of delegation?](#)
- [What about security](#)
- [How to use Help desk delegation](#)
- [Help desk Implementation Scenario's](#)

## Help Desk delegation

---

### What is help desk delegation

This feature helps administrators to assign or delegate selected activities to non-administrative desk users. It is recommended to delegate non-core administrator activities to help desk technicians.

### What is Help Desk Technician

A person who is entitled to perform the operations delegated by the administrator is called help desk technician. These operations can deviate from the regular end user functions with a bias of administrative tasks aimed to increase the productivity and reduce administrator's workload.



### What is Help Desk Role?

A specific role or a set of roles that are delegated by administrator to a unique non-administrative user to perform are called help desk roles.

### What is OU based Delegation?

The OU based administration lets the administrator to delegate the tasks with a scope limited to a specific Organizational Unit i.e. help desk users can perform the delegated activities that fall under the purview of the assigned OU. This ensures that the security issues are intact and the delegation runs smooth.

### How to create a help desk technician?

1. Click AD Delegation
2. Click on Help desk technicians
3. Select  Add New Technician.
4. Select domain
5. Select user by clicking on **Browse**.
6. Select a role by clicking on **choose** (Note: You can customize the roles. Learn more).
7. Select the Organizational Unit (OU). This step ensures that the user's help desk operations are restricted to this OU only.
8. Click on **save**.
9. To modify technician details, click the  icon present near the technician's name on the summary page.
10. You can modify Help Desk Role, OUs and also restrict the user to choose from a selected list of templates.
11. Enable **Impersonate as Admin** option to allocate admin permissions to the user.



**Note:**

1. The **Impersonate as Admin** option updates User permissions only in **ADMP** and retains original settings in **AD**.
2. You can also set a particular template as Default to allocate roles to the HelpDesk Technicians that are created. The Default template can be selected from the given list under Modify HelpDesk Technician option.


## How to create a help desk role?

There are some predefined help desk roles that you find under Help Desk Roles Tab.

To create a new help desk role:

1. Click AD Delegation
2. Click on Help Desk Roles
3. Select  Create Help Desk role.
4. Specify the role name and description.
5. Check in one or more of the boxes available. This will define the scope of the user operations i.e. you can create a help desk role which is limited to AD Reports or AD management etc.
6. For further exclusive role, click on the image '+'.  

7. In case of Create / Modify users, click on **user properties** to specify the attributes.
8. Click on Save Role.

## How to add more than one role/domain to a help desk technician?

1. Click AD Delegation
2. Click on Help desk technicians
3. To modify technician details, click the  icon present near the technician's name on the summary page.
4. Enable the required Domains in the Manageable Domains section
5. You can now assign multiple roles by clicking on choose/change for the corresponding domain.
6. You can modify Help Desk Role, OUs and also restrict the user to choose from a selected list of templates.
7. Enable Impersonate as Admin option to allocate admin permissions to the users.
8. Click Save Changes

## Work Flow for Help Desk Delegation

The core functional theme of Help Desk Delegation is that the technician can login to the ADMP console and perform the functions delegated by Administrator. For this to happen the Administrator should perform the following steps to authorize a help desk technician.

1. Modify (click on ) or delete (click on ) existing technician or [create a help desk technician](#)

2. Select or modify the predefined the help desk roles or [create a new help desk role](#).
3. Define the scope of each operation. Click on the images '+' for [granular authorization](#).
4. All the operations can be restricted to a specific OU. More about [OU Restriction](#)

## Granular Authorization

Administrator can restrict the help desk technicians function to a specific part of OU or to specific attributes in a function.

Example: Help desk technicians can be allowed to modify Group attributes at the same time restricting or avoiding them to any of the sub functions like **add to group** or **remove from group** or **set primary group**.

## OU Restriction

All the functions that are being performed by help desk technicians can be restricted to specific OU's. This enhances the security of Active Directory by authorization.

## Restrict Report Viewing

You can restrict the HelpDesk Technicians from viewing certain reports and can be imposed at the time of creating the HelpDesk Role. This restriction can be imposed on all of the reports under a particular reports category say like User Reports, Computer Reports, etc., or on specific reports under each of these Report types. The view for those reports whose checkboxes have been enabled will be restricted for the HelpDesk Role.

## Enable/Disable HelpDesk Technician

Super Admin can enable/disable one or more HelpDesk Technicians based on his discretion. Click on the appropriate Enable or Disable icon adjacent to the respective Technician's name to achieve this operation. This enhances the security of Active Directory by authorization.

## Multiple Domain Management for HelpDesk Technician

This feature allows the Administrator to allocate Multiple Domain Support for HelpDesk Technician(s). The following steps will help perform this operation:

- Select the AD Delegation Tab.
- Select the Modify User Icon under Action of Help Desk Technicians. This opens the Modify HelpDesk Technician Dialog.
- Enable the required Domains in the Manageable Domains section.
- Select the roles for the technician in the new domain.
- Click on Add OUs link to select the OUs of that domain.
- Click on Save Changes button to update the changes.

## Delegating Groups for HelpDesk Technicians

Administrator can associate HelpDesk Technicians with specific groups using the Include/Exclude option of HelpDesk Delegation. The following steps will help perform this operation:

- Select the AD Delegation Tab.
- Select the Modify User Icon under Action of Help Desk Technicians. This opens the Modify HelpDesk Technician Dialog.
- Click on Add/Remove buttons adjacent to Included Groups to include the required groups for the HelpDesk Technician.
- Click on Add/Remove buttons adjacent to Excluded Groups to exclude the required groups for the HelpDesk Technician.
- Click on Save Changes button to update the changes.

**Note:**

1. If the Included Groups List is alone mentioned, then the HelpDesk Technician permissions only on those mentioned groups.
2. If the Excluded Groups List is alone mentioned, then the HelpDesk Technician will have permissions on all groups except for the ones mentioned.
3. If both Included and Excluded columns contain data, then the ones that are unique with respect to Included List will hold good.
4. In case both the lists are empty, then the groups associated with the delegated OUs will be considered.

## Login Using Sample HelpDesk Users

ADManager Plus offers "Login Options Using Sample HelpDesk Technicians" for first time installations. Two sample HelpDesk Logins will be allocated for HR and HelpDesk, with create and reset password options respectively.

## How help desk delegation helps you

Help Desk delegation helps in disseminating the workload from administrator's desk. It reduces the burden on administrator there by allowing him to concentrate on core administrator activities.

It increases the productivity of users by eliminating administrator's intervention in self-manageable activities.

## What is the scope of delegation?

Administrator can limit the scope of delegated activities according to his wish. He can limit the technicians to a specific organizational units or a part of organizational unit.

## What about security

Help desk delegation is delivered with a security shield. All the actions performed by help desk technicians will be in the purview defined, enabling security settings intact. To prevent security breach the technicians and their activities are fenced to a specific party of Active Directory and enforced authentication zeroes security pitfalls.

## How to use Help desk delegation

For a successful implementation of this feature follow the below steps:

1. Select the **AD Delegation** tab.
2. Click the **Help Desk Technician**
3. Select the domain

4. Select the Active Directory user. Click Browse to select user. The selected user will be eligible to perform the roles defined in next steps.
5. Select the role by clicking on 'choose'. This role will be assigned to the user selected. Be cautious in selecting the role. At a time you can delegate only one role to a user.
6. Select the Organizational Unit. This limits the user's role only to that OU.
7. Save.

## **Help desk Implementation Scenario's**

HR Department in your organization need not wait for the System Administrator to confirm that the newly joined employees are enrolled in the active directory. Help Desk Delegation allows an administrator to grant rights to the HR People to create new user accounts whenever a person is recruited. This saves time for both the departments and enhances productivity.

## Help Desk Reset Password Console

---

The **Help Desk Reset Password Console** can be used in Web access mode to provide an easy way for Help Desk technicians to provide password resets for individual users.

Follow the steps below to Reset Password:

- Click on the **Help Desk Reset Password Console** link in the right pane of the **Home** page to get the **Reset Password** page.
- Select the **Domain** appropriate to the user whose password is to be reset.
- Enter name of the user in the **Search User** field and click the **GO** button.
- Click **RESET PASSWORD** button in **Action** tab, appropriate to the User name.
- Enter a new **Password** and also confirm the same.



**Note:** Click **User must change the password at next log on** check box, if you want the user to change his password when he logs in after the password is reset. Else leave it unchecked.

- Click on **OK** button.

**Tip:** You can filter the viewing options by either selecting the **Show All** option to view all the users or can simply view the names beginning with a particular alphabet using the **Sort By** alphabet feature.

Click on [Help Desk Delegation](#) to know more about this feature.



## Active Directory Delegation

---

Security roles gives you the ability to delegate permissions to specific Active Directory objects. ADManager Plus provides you the ability to create different security roles based on the Active Directory permissions to suit your need. The roles can then be delegated to the users/administrators who need to have these permissions. You also have the flexibility to either change the permissions of a specific role or to add/remove users delegated to a specific role.

The following topics guides to create and delegate security roles:

- [Creating Security Roles](#)
- [Viewing Security Roles](#)
- [Modifying Security Roles](#)
- [Applying Security Roles](#)
- [Built-in Security Roles](#)

## Creating Security Roles

1. Select the **AD Delegation** tab and Click the **Create Security Role** from the quick links. This opens the Create Security Role Wizard.
2. Click **Go to Step1**.
3. Specify a name and description for the role and click **Go to Step2**.
4. The most common Active Directory objects are displayed in the combo box. You also have an option to include more objects to this combo box by clicking the **Edit** link. Select the required Active Directory object to view its security permissions.
5. The available permissions for the selected object are displayed. Select the appropriate permissions that you wish to apply. You also have an option to search the permissions list to choose the required permissions.
6. Select the appropriate option to specify the objects for applying the permissions. You can choose from the following options:
  1. *This object only*: This means during delegation, the role will only be applied to the selected target container.
  2. *This object and all child objects*: This means during delegation, the role will be applied to the selected target container and all its child objects.
  3. *Child object only*: This means during delegation, the role will be applied to all the child objects of the selected target container.
  4. *Specific object*: This can be any specific AD object, such as Computer object, Container object, Domain object, etc. Selecting this option will apply the role to all of these objects in the selected target container, during delegation.
7. Click **Allow** or **Deny** to add it to the selected permissions list.
8. After adding all the required permissions, click **Finish** to view the summary of the role defined.
9. Click **Save Role** to save and quit the wizard.





**Note:** Creating a security role will not grant or revoke permissions to the users. Only when the role is applied/delegated to the users, the permissions defined in the role are granted/revoked.

## Viewing Security Roles

---

Selecting the AD Delegation tab lists all the security roles that have been created. The name, description of the role and the selected security permissions are shown here. You can initiate the following actions:

1. Click the Delegate button to delegate the selected role. This will open the Delegate Security Role wizard with the role selected.
2. Click the  icon to modify the security role.
3. Click the  icon to delete the security role.
4. Select the Delegated Roles tab, to view the list of security roles that have been delegated.
5. Select the Non-Delegated Roles tab, to view the list of security roles that have not been delegated.

## Modifying Security Roles

---

To modify a security role, follow the steps below:

1. Select the **Security Roles** tab. This will list all the security roles that have been defined.
2. Click the role you wish to modify. This will show the details of the selected security role.
3. Click **Modify**.
4. Modify the details of the permissions on the Active Directory objects as desired and click **Finish**.
5. The summary of the modified role is displayed. Click **Save Role** to complete the modification.



**Note:**

1. Modifying a role that has been already applied, will automatically modify the permissions to the delegated users.
2. Removing a user from the applied list, will automatically revoke the granted permissions for that user.

## Applying Security Roles

---

Once created, the security roles act as a template which can then be applied to users to grant or revoke permissions as defined in the role. Follow the steps below to delegate the security roles

1. Select AD Delegation tab and Click the **Delegate Security Role** from the Quick links. This opens the **Delegate Security Role** Wizard.
2. Click **Go to Step1**.
3. All the available users, groups, and computers of the selected domain are listed. Select the security principals (users, groups, and computers) for whom the roles have to be delegated and click **Add**.
4. After adding the security principals, click **Go to Step2**.
5. Select the active directory objects to which the permission needs to be applied and click **Add**.
6. Click **Go to Step3** and add the roles that have to be delegated.
7. After adding the desired roles, click **Finish** to view the delegation details.
8. Click **Apply Role** to complete delegation.

## Built-in Security Roles

---

ADManager Plus comes with a set of built-in security roles that can be delegated to the security principals. The built-in roles can be used to grant the following permissions:

1. To reset the user password
2. To unlock the user accounts
3. To add or remove members from groups
4. To move users to a different OU within the domain
5. To move computers to a different OU within the domain
6. To add/remove workstations in the domain
7. To create user accounts
8. To create, delete, and modify attributes of the user accounts

# Admin Settings

## Administrator Settings

---

These settings help Administrator to customize ADManager Plus to his organizations policies and convenience. You can also configure settings of server, connection and Active Directory Search.

The following features are available in Administrator settings:

- Customize Naming Formats
- Customize Title & Department
- [Customize Offices & Companies](#)
- [Customize Password Settings](#)
- Customize LDAP Attributes
- Customize Delete Policy
- AD Search Settings
- Connection Settings
- Server Settings
- Mail Server Settings
- Personalize Settings
- ServiceDesk Settings

## Customizing Naming Format

---

Using this administration can customize the naming template to the organization policies. Follow the following steps:

1. Click on Admin Tab and then on customize naming Format.
2. Click on the **+Add New Format**.
3. Click on the select data and specify the name with which it should start
4. In the space next to **with** enter the number of characters you want to choose from name.
5. Click **Add to format**
6. Continue the process until you arrive at the format value desired.
7. Enable the **Select Case** checkbox to specify the case (Lower/Upper) in which you want to store the name.
8. Enable the **Remove spaces** checkbox to avoid unwanted spaces in the name.
9. Save it at the end.

Refer to the following example for a clear understanding.

Ex: Suppose a user name is john smith and you want it to be as josmi in directory, for that perform the following steps:

- Click on the **+Add New Format**
- Click on the select data-first name
- In the space next to **with** enter 2.
- Click on the select data-last name
- In the space next to **with** enter 3.
- Click **Add to format**
- Save it at the end.



## Titles & Departments

---

The **Titles & Departments** feature on the left pane of the **Admin** tab allows you to add/remove titles and departments based on the needs of your organization. This section will guide you to Add/Remove values under the appropriate attributes.

### To Add a new Title:

1. Select the **Add New** link of **Titles** attribute.
2. Type the Title name in the **Add Titles** dialog.
3. Click the **Add** button to see the updated Title list.

### To Remove an Existing Title:

1. Click on the Title name you want to remove from the list.
2. Select the **Remove** button and click **OK** to confirm the same.  
You can now see the updated Title list.

Follow the same instructions to add/remove **Department** names in your existing Department list.

## Offices & Companies

---

The **Offices & Companies** feature on the left pane of the **Admin** tab allows you to add/remove Offices and Companies based on the needs of your organization. This section will guide you to Add/Remove values under the appropriate attributes.

### To Add a new Office:

1. Select the **Add New** link of **Offices** attribute.
2. Type the Office(s) name in the **Add Offices** dialog.
3. Click the **Add** button to see the updated Offices list.

### To Remove an Existing Office:

1. Click on the Office name you want to remove from the list.
2. Select the **Remove** button and click **OK** to confirm the same.  
You can now see the updated Offices list.

Follow the same instructions to add/remove **Company** names in your existing **Companies** list.

## Customizing Password Settings

---

You can customize the randomly generated password while creating the users.

Steps to customize the random password:


1. Click on **Admin** tab.
2. Select the "**Password settings**" under Custom Settings.
3. Set the minimum, maximum lengths and you may set the special character, starting with alphabet or both upper or lower case if you need more complexity to the random password.
4. Click Save to set the settings.

## Customizing LDAP Attributes

This option will enable you to add Your own LDAP attributes and retrieve the information for them in reports:

1. Select the **Admin** tab.
2. Click the **Customize LDAP Attributes** .
3. Click + **ADD New Field**
4. Type the display name
5. Type the LDAP name (either pre defined or defined by you)
6. Enter the data type
7. Select the object associated with it.
8. Check in the associated reports for that i.e. if you have added a LDAP attribute for user check in the relevant box to generate reports for that LDAP.
9. Add.

If you want to delete any fields, click on  adjacent to display name.

	<p><b>Note:</b></p> <p>1.First create a CSV with all the updated information and then start the process.</p> <p><b>2.Data Type:</b></p> <p>Unicode string: Select this data type when the defined attribute or defined by you as a value containing any text like name, role, etc.</p> <p>Integer: Select this data type when the defined attribute or defined by you as a value containing numerical (integer) value with in limits like employee id, phone number, etc.</p> <p>Boolean: Select this data type when the defined attribute or defined by you as a value containing any true or false options values like Dail in Access,Default Storage Limit.</p> <p>Large Integer: Select this data type when the attribute value contains or defined by you as a value containing any lager integer value like last login time,accountExpires etc.</p>
---	---

## Customizing Delete Policy

---

You can customize the Delete Policy for users that will be applied during user deletion.

Steps to customize the Delete Policy:

1. Click on **Admin** tab.
2. Select the "**Delete Policy**" under Custom Settings.
3. Enable the appropriate checkboxes to delete **Remote Home Folders, Roaming Profiles, Remote Terminal Service Home Folder** and **Roaming Terminal Service Home folders**.
4. Click Save to store the settings.

## AD Search Settings

---

You can Configure Active Directory search settings.

This Feature enables users search for the information of other users. The operation can be performed without user logging into the console. Administrator can configure the People finder more efficiently by appending required information and adding more attributes available in the 'Result column' like phone number, country, address etc.

Perform the following steps to configure Search settings.

1. Select the **Admin** tab.
2. Click the **AD search settings**.
3. Check in the box configure search.
4. Select the domain.
5. Select the attributes which you want to add to the information of the users.  
Confirm that the attributes added are reflecting in 'selected attributes'
6. click on 'Save changes'.



**Note:** This feature will be present in the Home page of ADMP console. Users need not login to the console to access to people finder. The user information can be customized to your policy

## Connection Settings

---

You can Change the connection settings using this feature. Perform the following steps

1. Select the **Admin** tab.
2. Click the **Connection settings**.
3. Enter the port number
4. Check in the Enable ssl port[https] to enable secure sockets layer and enter the number. Select the session expiry time.
5. Click on save changes.

## Server Settings

---

You can Change Configure ADManager Plus startup & log settings.

1. Select the **Admin** tab.
2. Click on the **Server settings** link on the left hand side.
3. Specify the **Mail Server**, **Mail Port** and **From Address** in the corresponding fields.
4. Enable the check boxes based on your personal preferences.
5. Select the **Mode** for the Current Log Level.
6. Select the **Locale Settings** of the Computer in which the ADManager Plus needs to be installed. The default working mode is 'Normal' with minimal debugging information.
7. Click on 'Save changes'.



## Configure Mail Server

---

The **Mail Server Settings** need to be configured before you proceed with **Scheduling Reports**. Follow the steps given below to specify the mail server details:

- Click the **Configure Mail settings** link at the top right corner to open the **Server Settings** page
- Specify the **name** and **port** of the Mail Server.
- Click the **Authentication** link to specify the **username** and **password** for Mail Server access and thereby avoid anonymous login..
- In the **From Address** field, mention the e-mail address from which you are likely to receive the report mails.

Your Mail Server has been configured and you can now proceed with the [Scheduling Reports](#) task.

## Personalize Settings

---

ADManager Plus provides users with the functionality to configure user accounts based on personal priorities and requirements. The Personalize option enables you to change an existing password and a user interface theme.

### To change the password

1. Enter the existing password in the **Old Password** field.
2. Enter the new password in the **New Password** field.
3. Enter the new password again for confirmation in the **Confirm Password** field.
4. Enable the **Show forget password link for ADManager Plus Admin Login** checkbox to have a Forgot Password Link on the Login Page. Else leave it unchecked.
5. Click the **Save Changes** button.

The new password get updated. Subsequently, you have to use the new password to login to the client.

### To change the theme

1. Select the theme from the available options
2. Click **Save Changes** button.

## ServiceDesk Settings

---

ServiceDesk Plus is a combined HelpDesk & Asset Management software that integrates Trouble Ticketing, Asset Tracking, Purchasing, Contract Management and Knowledge base in one package. ServiceDesk Plus can be installed on any remote machine and can be run from the same machine where ADManager Plus is installed. The below steps will help you configure the server settings and login details to perform the above remote operation.

You can Change, update & Configure ServiceDesk Plus settings from here.

1. Select the **Admin** tab.
2. Click the **ServiceDesk settings**.
3. Enter the Information.
4. Test connection and save.

## Web based people search

---

People search allows users in your organization to search for employees (people) information without logging into ADManager Plus with its configured settings. The search results can be customized to a specific OU Level or Domain Level and the result columns can be selected as per requirement. To perform this operation follow the steps below:

1. Click on the **Admin** tab.
2. Check the Enable Employee Search option.
3. Click on the **Configure AD Search**.
4. Select the desired domain for which the search should be enabled.
5. Select the Result Columns.
6. Save the settings.

## Searching Security Permissions

---

ADManager Plus provides you the ability to search the permissions granted to security principals, such as users, groups, and computers. It simplifies search by specifying active directory object, security principal, and the permissions in the search criteria. Follow the steps given below to search the active directory permissions:

1. Select the **AD Delegation** tab and click the Search ACEs from the Quick Links.
2. The search panel is displayed. The search panel consists of three text fields with a **Select Criteria** link for each, to specify the active directory objects, security principals, and permissions respectively.
3. Browse and select the active directory object on which the search has to be performed. Leave it blank, if the search has to be made on all the active directory objects.
4. Browse and select the security principals to search their permissions. If not specified, the search includes all the security principals of that domain.
5. Browse and select the permission for which you want to perform the search. If left blank, all the permissions are included in the search.
6. Click **Search**.

Windows ADManager Plus searches the active directory based on the specified search criterion and displays the result in the bottom panel. The search results include the name of the object, the object class, and the location of the object in the active directory.

## Active Directory Explorer

---

The AD Explorer tab provides you the windows explorer view of the active directory objects of the selected domain. While left tree lists all the active directory objects, the right panel displays the properties, security permissions, and the mailbox rights to the selected object in the tree.

**Properties:** This will list out all the below properties of the specified object.

- user details
- contact details
- exchange server details
- object details
- terminal server details
- account details

**Security permissions:** This will list out all the permissions of the object with security principal and the scope of its application.

**Mailbox rights:** This will display all the users and their rights over a selected user's mailbox.

## Troubleshooting Tips

---

- [Domain Settings](#)
  - [Active Directory User Management](#)
  - [Active Directory Reports](#)
  - [Active Directory Delegation](#)
- 

### Domain Settings

1. [When I start ADManager Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?](#)
2. [When I add my domains manually, the Domain Controllers are not resolved. Why?](#)
3. [When I add the Domain Controller, I get an error as "The Servers are not operational". What does it mean?](#)
4. [When I add the Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?](#)
5. [The status column in the domain settings says that the user do not have Admin Privilege?](#)

#### **1. When I start ADManager Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?**

ADManager Plus, upon starting, discovers the domains from the DNS Server associated with the machine running the product. If no domain details are available in the DNS Server, it shows this message.

#### **2. When I add my domains manually, the Domain Controllers are not resolved. Why?**

When the DNS associated with the machine running ADManager Plus do not contain the necessary information. You need to add the Domain Controllers manually.

#### **3. When I add the Domain Controller, I get an error as "The Servers are not operational". What does it mean?**

This error could be due to any of the following reasons:

1. DCs are down.
2. Servers not available.
3. Firewall has been enabled, and port 389 is closed.
4. Busy - try after some time?

#### **4. When I add the Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?**

This error could be due to any of the following reasons:

1. When the specified user name or the password is invalid.
2. Anonymous login (when no user name and password is provided)
3. When IP Address of the Domain Controller is specified instead of its name.

## 5. The status column in the domain settings says that the user do not have Admin Privilege?

This is a warning message to indicate that the specified user do not have administrator privileges i.e, the user is not a member of Domain Admins Group. Hence permissions applicable to Administrator may not be available to this user.

## Active Directory User Management

1. While creating an user, I get the following error "Error in setting the Password. The network path not found - Error Code: 80070035"
2. While creating an user, I get the following error "Error in setting the Password. There is a naming violation - Error Code : 80072037"
3. While creating/modifying an user, I get the following error "The server is unwilling to process the request - Error Code : 80072035"
4. While creating an user, I get the following error " Error In Setting Terminal service Properties. The specified user does not exist - Error Code : 525"
5. I have updated the exchange attributes using ADManager Plus, but the properties are not updated in the Exchange Server yet.
6. I am not able to set the Terminal Services properties for the user?
7. I am getting an error as "The attribute syntax specified to the directory service is invalid - Error Code : 8007200b"?
8. When I create/modify an user, I get the following error "Error In Creating User. A device attached to the system is not functioning - Error Code : 8007001f "
9. Email address for user not showing up or not set properly?
10. Error - The server is unwilling to process the request while setting Password, which did not match password complexity
11. Error code: 8007052e
12. Error code: 80070775
13. Error code: 800708c5
14. 5 -Access is denied (Terminal Service / Folder Creation)
15. No such user matched. Verify the LDAP attribute in search query
16. Error Code: 80072035
17. Error Code: 80072030
18. Error Code:80070005
19. Error Code: 80072014
20. Error Code: 80072016
21. Error Code 35
22. Error Code b7

## 1. While creating an user, I get the following error "Error in setting the Password. The network path not found - Error Code: 80070035"

While setting the password for the user if the target machine could not be contacted, this error is shown. This could happen when the DNS associated with the machine running ADManager Plus does not point to the Domain Controller where the user account has been created (possibly both are in different domains).



**2. While creating an user, I get the following error "Error in setting the Password. There is a naming violation - Error Code : 80072037"**

One possible reason for this error could be creation of a user in an invalid container.

**3. While creating/modifying an user, I get the following error "The server is unwilling to process the request - Error Code : 80072035"**

The possible reasons for this error could be:

1. While setting the password, if the password complexity requirement as defined in the password policy is not met. For example, the password policy might state that the password should be alphanumeric and if the password specified do not comply this, you might get this error.
2. When you try to remove a non-existing user object from a group.
3. When your try to remove a user from his/her primary group.
4. When modifying the SAM Account Name format for multiple users and when more than one user happen to have the same SAM Account Name.

**4. While creating an user, I get the following error " Error In Setting Terminal service Properties. The specified user does not exist - Error Code : 525"**

One possible reason could be that the user or the system account as which the product is run do not have an account in the target domain. Terminal Service properties can only be set if the user account or the system account (applies when ADManager Plus is run as a service) that runs ADManager Plus has an account on the target domain.

**5. I have updated the exchange attributes using ADManager Plus, but the properties are not updated in the Exchange Server yet.**

ADManager Plus modifies the exchange properties in the Active Directory. The changes may not immediately reflect in the Exchange Server. It will get updated after some time.

**6. I am not able to set the Terminal Services properties for the user?**

One possible reason could be that the user or the system as which the product is run do not have an account in that domain.

Refer to [here](#) for starting ADManager Plus in User or System account.

**7. I am getting an error as "The attribute syntax specified to the directory service is invalid - Error Code : 8007200b"?**

This could happen in the following scenarios:

1. When modifying multiple users, if you try to remove (or making the value as blank) an non-existing attribute
2. When adding a user, if you specify a blank value for an attribute.

**8. When I create/modify an user, I get the following error " A device attached to the system is not functioning - Error Code : 8007001f "**

The possible reasons for this error could be:

1. When creating an user, if the naming attributes, such as Name, Logon Name, SAM Account Name, etc., has some special characters in it.
2. When modifying an user, if an unacceptable format is chosen for the naming attributes. For example, if the format chosen for the Logon Name is LastName.FirstName.Initials and if the user do not have any one of these attributes specified, this error will occur.

#### **9. Email address for user not showing up or not set properly?**

The possible reason could be:

1. Email may **Not be set** as per Recipient Policy. check whether all ldap attributes in recipient policy query are set to specific value.
2. Check in the user account properties whether you entered the attribute for email. Ex: xyz@**company.com**. The company should be entered to the users.

#### **10. Error-The server is unwilling to process the request while setting Password which not matches to password complexity**

The possible reason could be:

You may not have specified or opt for any options in 'Password Complexity' while creating user account.

Ex: There will be options for password complexity like length of password, Characters that can be used or number of bad login attempts etc. You need to select any degree of complexity, ignoring so will throw above error.

#### **11. Error code: 8007052e**

The reason is, the Supplied credentials are invalid.

#### **12. Error code: 80070775**

Reason: The referenced account is currently locked out and may not be logged on.

#### **13. Error code: 800708c5**

Reason: The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

#### **14. 5 -Access is denied (Terminal Service / Folder Creation)**

Reasons:

1. User does not have rights to create a homefolder.
2. Users do not have access over terminal services.

#### **15.No such user matched. Verify the LDAP attribute in search query**

Reason: No Users in AD matches with the criteria provided by you.Try choosing the correct matching attributes by checking with the query provided in the "Match criteria for Users in AD",this is obtained by clicking on "Update in AD" button and expanding "Select Attributes" box.

#### **6.Error Code 80072035 : Error In Setting Attributes,The server is unwilling to process the request.**

Reason: The primary group specified in User Creation has been moved or deleted.

**17.Error Code : 80072030 : Error In Setting Attributes,The server is unwilling to process the request.**

Reason: The primary group/container specified in User Template that was selected during User Creation has been moved or deleted. (You are trying create a child object inside an OU, but that parent OU does not exist)

**18.Error Code : 80070005 - Access Denied**

Reason: The User may be trying to access an object to which he has no permissions granted.

**19.Error Code : 80072014 - Error In Setting Attributes, The requested operation did not satisfy one or more constraints associated with the class of the object**

Reason: You may encounter this type of error when the CSV file you are using to import values, does not satisfy the conditions associated with the attribute.

**20.Error Code : 80072016 - Error In Setting Attributes, The directory service cannot perform the requested operation on the RDN attribute of an object**

Reason: You may encounter this type of error if any of the LDAP headers in the CSV file are mentioned inappropriately.

**21.Error Code 35 : Error in Creating Terminal Services Home Directory/ Error in Creating Home Directory,The network path was not found.**

Reason: The remote server path might not be accessible.

**22.Error Code: 800704c3 - Error While accessing User in Setting Account Properties.**

Reason:Multiple connections to a server or shared resource by the same user, using more than one user name, is not allowed. Disconnect all previous connections to the server or shared resource and try again.

**23.Error Code b7 : Error in Creating Profile Path**

Reason: There may be a File/Folder that already exists with the same name.

**Active Directory Reports**

1. [When I specify the details and generate the report, it says "No Result available" or incomplete data](#)
2. [AD Reports shows an object that do not exist in the Active Directory?](#)

**1. When I specify the details and generate the report, it says "No Result available" or incomplete data**


It could be because of any of the following reasons:

1. When ADManager Plus could not contact the Domain Controller as it is not operational or due to network unavailability.
2. In case of multiple Domain Controllers, when the data is not replicated in all the Domain Controllers.
3. The LastLogonTime that is used to determine the inactive users and computers is not replicated in all the Domain Controllers. Hence, you need to specify all the

Domain Controllers in the [Domain Settings](#) to enable ADManager Plus to retrieve the data from all the Domain Controllers.

4. When the password policy is not set (i.e., Max Password Age is set to zero), the Password Expired Users report and Soon to Password Expiry users report will not show any data.
5. For time-based reports like inactive users, inactive computers, recently logged on users, etc., the date and time of the machine running ADManager Plus should be in sync with the domain controllers.

## **2. AD Reports shows an object that do not exist in the Active Directory?**

This mismatch could occur when the data is not synchronized with the Active Directory. The data synchronization with the Active Directory happens everyday at 1.00 hrs. If ADManager Plus is not running at that time, you can initiate the data synchronization manually by clicking the  icon of that domain from the [Domain Settings](#).

## **3. Error Code : 80070035- Error in getting Shares. The network path was not found**

Reason - The remote server path might not be accessible.

## **Active Directory Delegation**

### **1. When a role is delegated, I get the error as "Permission Denied"**

One possible reason could be, the user or system as which the product is started do not have necessary privileges to perform this operation.

Refer to [here](#) for starting ADManager Plus in User or System account.

### **2. I am not able to login through my account!**

The following are the possible reasons for that:

1. UserName/ Password Wrong
2. Log on to restriction.
3. Account Disabled / Locked out / Expired
4. User must change password on next logon checked.

## FAQ

---

### General

1. [What is ADManager Plus?](#)
2. [What operating systems are supported by ADManager Plus?](#)
3. [What is the difference between Free and Professional Editions?](#)
4. [ADManager Plus runs in a web browser. Does that mean I can access it from anywhere?](#)
5. [How is ADManager Plus licensed?](#)
6. [Do I need any prerequisite software to be installed before using ADManager Plus ?](#)
7. [Can ADManager Plus work if DCOM is disabled on remote systems?](#)
8. [Does ADManager Plus support other than English ?](#)

### Advanced

1. [I want to stop running ADManager Plus during machine boot up, what to do?](#)
  2. [Can I add Multiple Domains?](#)
  3. [Can I add domains of different forest?](#)
  4. [How do i configure child domain details?](#)
  5. [What does the term default domain mean?](#)
  6. [How do I change the password of the admin account?](#)
  7. [What are the advantages of Bulk User Management compared to Active Directory Tools?](#)
  8. [What is a User Template? What is the advantage of using Template in Bulk User Creation?](#)
  9. [What are the standards of csv file used for bulk user creation?](#)
  10. [What are the types of Reports available in ADManager Plus?](#)
  11. [What is the difference between account disabled users and account locked out users?](#)
  12. [What is the difference between account disabled users and inactive users?](#)
  13. [What is the difference between account expired users and password expired users?](#)
  14. [Is there any customized reports?](#)
  15. [What is a Security Role?](#)
  16. [What are the advantages of Delegation through ADManager Plus?](#)
  17. [What will happen if modify a delegated Security Role?](#)
  18. [Can I search the ACEs to see what permission is available for a user?](#)
-

## General

### 1. What is ADManager Plus?

ManageEngine ADManager Plus is a 100% web-based product that provides centralized administration and management of Windows Active Directory. You can use ADManager Plus to perform the following:

- Create bulk user accounts in the Active Directory with the flexibility to import properties from a csv file.
- Modify the existing user account properties including Exchange Mailbox and Terminal Services properties.
- Generate and view granular reports of users, computers, groups like Inactive Users, Disabled Users, Users in Nested Groups, Distribution Groups, Security Groups, Inactive Computers, etc.
- Create and delegate security roles for granting/revoking permissions to security principals.
- Search ACEs and Active Directory objects.

### 2. What operating systems are supported by ADManager Plus?

ADManager Plus support the following Windows operating systems:

- Windows 2000.
- Windows XP.
- Windows 2003.
- Windows Vista.

### 3. What is the difference between Free and Professional Editions?

The free edition of ADManager Plus can be used to manage up to 100 objects in a single domain and cannot have more than one domain configured.

The professional edition can be used to manage the number of domains and objects for which it is licensed for.

The free edition can be upgraded to professional edition at any point of time by obtaining a valid license from ZOHO Corp.

### 4. ADManager Plus runs in a web browser. Does that mean I can access it from anywhere?

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

### 5. How is ADManager Plus licensed?

ADManager Plus is licensed on annual subscription based on the number of Domains t would manage.

### 6. Do I need any prerequisite software to be installed before using ADManager Plus ?

No, ADManager Plus do not require any prerequisite software to be installed.

## 7. Can ADManager Plus work if DCOM is disabled on remote systems?

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

## 8. Does ADManager Plus support other than English ?

No. The support for languages other than English is yet to be added.

## Advanced

### 1. I want to stop running ADManager Plus during machine boot up, what to do?

To make ADManager Plus not to start during system bootup,

1. Click the **Personalize** link from the top right of the ADManager Plus client.
2. Clear the option "Start the product automatically on machine bootup"
3. Click **Save Changes**.

### 2. Can I add Multiple Domains?

During startup, ADManager Plus adds all the domains that it could resolve. You can also add Domains manually by clicking the Domain Settings link from the client.

### 3. Can I add domains of different forests?

Yes, you can add domains belonging to different forests.

### 4. How do i configure child domain details?

The procedure for adding child domains is no different from adding other domains. Click the Domain Settings link can add the domains.

### 5. What does the term default domain mean?

Default domain is a term used to represent the domain for which the delegation of security roles can be made. If you want to delegate the roles to the security principals of a different domain, you have to make it as default domain and then delegate.

### 6. How do I change the password of the admin account?

To change the password,

1. Click the **Personalize** link from the top right of the ADManager Plus client.
2. Specify the old and new password.
3. Click **Save Changes**.

### 7. What is the advantages of Bulk User Management compared to Active Directory tools?

The following are the advantages over Active Directory tools:

1. Can create multiple users simultaneously.
2. Can modify all the properties including Exchange and Terminal Services properties for multiple users.

3. Web-based management.

### **8. What is a User Template? What is the advantage of using a Template in Bulk User Creation?**

A user template contains the values of the user attributes defined in it. When you want to create user accounts with similar privileges and permissions, you can create a template with the common attributes and just change the values that differ, say the logon name, display name, etc. This save your time and avoid any possible errors.

### **9. What are standards of csv file used for bulk user creation?**

The first line in the csv file should contain the attribute names as defined in the Active Directory. Enter the attribute values for each user in separate lines in the same order. If you do not wish to specify the value for an attribute, just put a comma and proceed. [Sample CSV file](#).

### **10. What are the types of Reports available in ADManager Plus?**

There are 100+ different reports about the Active Directory infrastructure components grouped under User, Computer, Groups, and Security Reports. For more details refer to [Active Directory Reports](#).

### **11. What is the difference between account disabled users and account locked out users?**

The user accounts that are disabled by the administrator is termed as account disabled users. The account locked out users are those accounts that are locked by the Active Directory based on a policy, for example, three continuous failed login attempts would disable login for certain period. This is a temporary period during which the user will not be able to login.

### **12. What is the difference between account disabled users and inactive users?**

The user accounts that are disabled by the administrator is termed as account disabled users. They do not have login permissions in the domain. Inactive users are those who have login permissions in the domain, but have not logged on to the domain for the specified period.

### **13. What is the difference between account expired users and password expired users?**

The account expired users are those whose user account has become invalid. This may happen in cases where a temporary account is created for a specific period beyond which the account expires.

The Password expired users are those who are not able to use their account as the password has expired. As a security policy, the users might require to change the password within a specified period after which they may not be able to login using their old password. The password has to be reset for the user to login again.

### **14. Is there any customized reports?**

Yes, you can customize the reports based on the criteria available for all the reports. For example, to view the inactive users for a specified period, you can specify the period and generate. Also, you can customize the columns in the report.



### **15. What is a Security Role?**

Security roles are those you define for granting/revoking specific permissions. For example, you can define a role to grant permissions for creating a user. This can then be delegated to the security principals for granting the permissions.

### **16. What are the advantages of Delegation through ADManager Plus?**

The following are the advantages:

1. Minimises the error when granting/revoking same permissions for different users.
2. Modifying a security role automatically delegates the permissions for the previously delegated objects as well.
3. Can create as many roles as required and can be delegated as and when required.
4. Web-based.

### **17. What will happen if modify a delegated Security Role?**

When you modify the delegated security role, it gets automatically delegated for the previously delegated objects.

### **18. Can I search the ACEs to see what permission is available for a user?**

Yes, you can search the permissions granted to security principals, such as users, groups, and computers. You can even include the active directory object, security principal, and the permissions in the search criteria to confine your search.

## Known Issues and Limitations

---

### Known Issues

1. In Vista --Service Installation --- Tray Icon does not show up and auto launch of the browser does not work.
2. In Scheduled Reports, only the default columns can be listed.

### Limitations

1. Inability to delete shared home folders, while deleting Users.
2. Custom Script execution while User Creation is limited to three seconds.
3. Need for a separate Exchange Management Console to create User Mailbox in Exchange 2007.
4. Inability to schedule "Real last logon" , "Logon hour report" and all reports under the Other Reports category.

## ADMP - ADSSP Integration

---

ManageEngine **ADSelfService Plus** is a secure, web-based end-user password reset program for domain users. ADSelfService Plus primarily helps with self-password reset, self-account unlock to perform self-password reset, self-account unlock and self update of personal details in Active Directory.

Key features of ADSelfService Plus include:

- **Secret Questions:** Admin user can configure secret question/answer settings for domain users.
- **Self Update Policy:** This feature enables the Admin user to restrict the attributes which the domain user can access and update.
- **Scheduler Notification:** Notification mails will be automatically sent to everyone who falls under the Soon to Expire Password Users category.

Thus it helps in a large scale to eliminate a leading source of help desk calls and associated expenses by automating password resets and account unlocks thereby optimizing employee productivity.

To know more about ADSelfService Plus, visit our website url:

<http://www.adselfserviceplus.com>