ManageEngine

ADManager Plus

Workbook

Table of Contents

1. About ADManager Plus

ADManager Plus is a web-based management and reporting tool for Active Directory, Microsoft Exchange, Office 365, G Suite, and Skype for Business server.
ADManager Plus also helps you

- Manage NTFS and share permissions
- Perform management tasks from within prepackaged reports
- Securely delegate management and reporting to technicians
- Automate important AD routines
- Use an approval mechanism to keep a tab on all the actions performed

2. Document Summary

The ADManager Plus workbook helps you gain hands-on experience on all the crucial features of ADManager Plus The exercises given in this book are created keeping in mind the most common, yet extensively important tasks that are performed by any Active Directory administrator.

As you progress through this workbook, you will be able to identify how ADManager Plus, with its simplified UI, helps you manage, report, and administer your AD environment easily as opposed to the native AD tools.

3. Active Directory Management

The exercises mentioned in this section help you gain a better understanding of AD management features of ADManager Plus.

It includes activities related to:

- AD object creation
- AD object modification
- AD object deletion

3.1 AD Object Creation

In this section you will learn how to create Active Directory objects in bulk using ADManager Plus. You will also learn to perform additional tasks like adding them to groups and specifying any desired value like department during object creation.

Exercise 1: User Provisioning

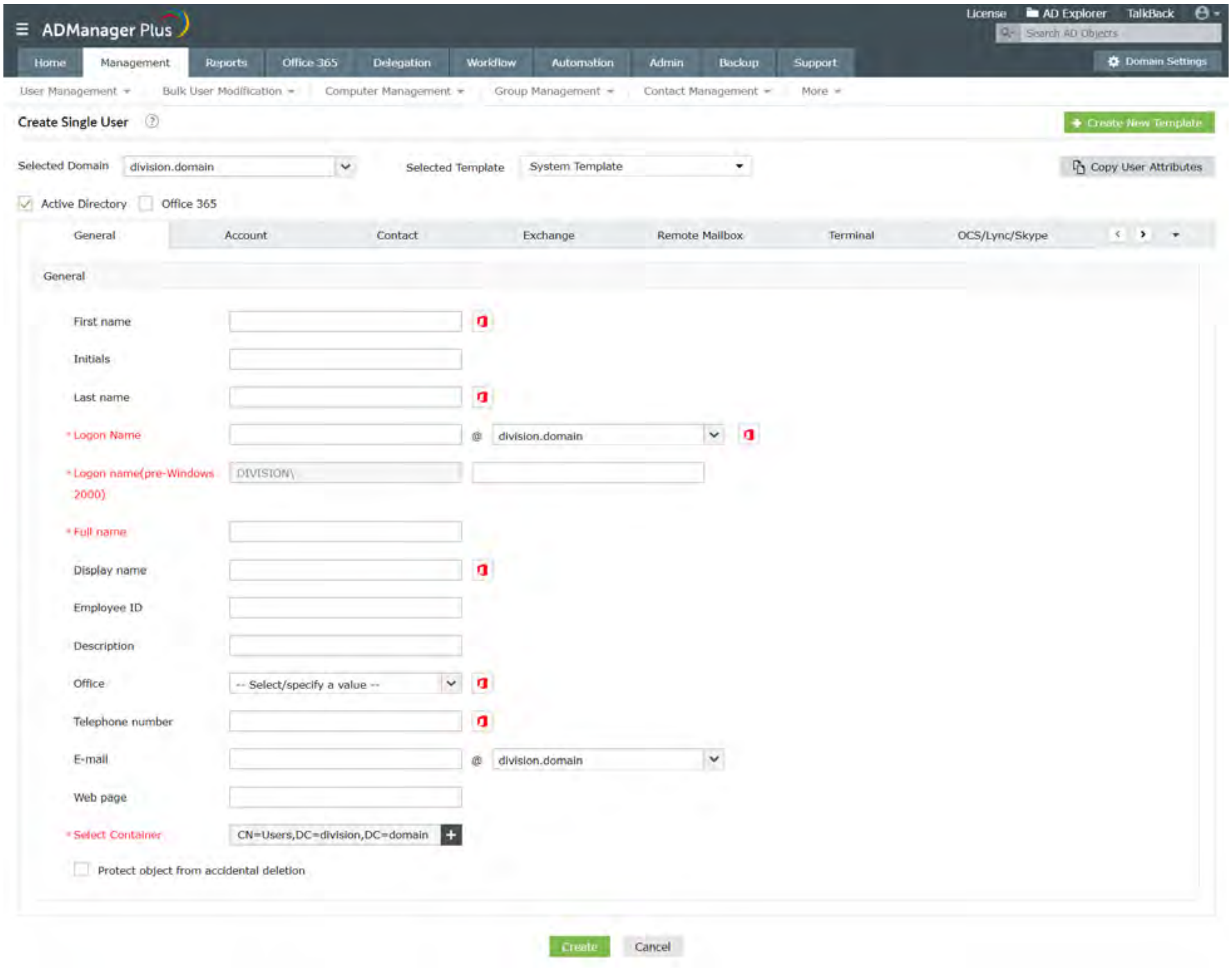
Objective: Create a user:

- Who should be a member of the specified group.
- Who should belong to the specified department.
- Whose email address should not be listed in the Exchange Address list.

As opposed to native AD tools, where the above tasks can be achieved by toggling between multiple windows and servers or through complex scripts, ADManager Plus facilitates one-stop user provisioning where a user with all the above mentioned criteria can be created from a single screen, in just a few clicks.

Steps for creating a single user with the aforementioned criteria:

1. Logon to the ADManager Plus tool and click on the **Management** tab.
2. Select the **Create Single User** option, under **User Management**.



Create Single User

Selected Domain: division.domain

Selected Template: System Template

☑ Active Directory □ Office 365

General

First name:

Initials:

Last name:

* Logon Name: @ division.domain

* Logon name(pre-Windows 2000): DIVISION\

* Full name:

Display name:

Employee ID:

Description:

Office: -- Select/specify a value --

Telephone number:

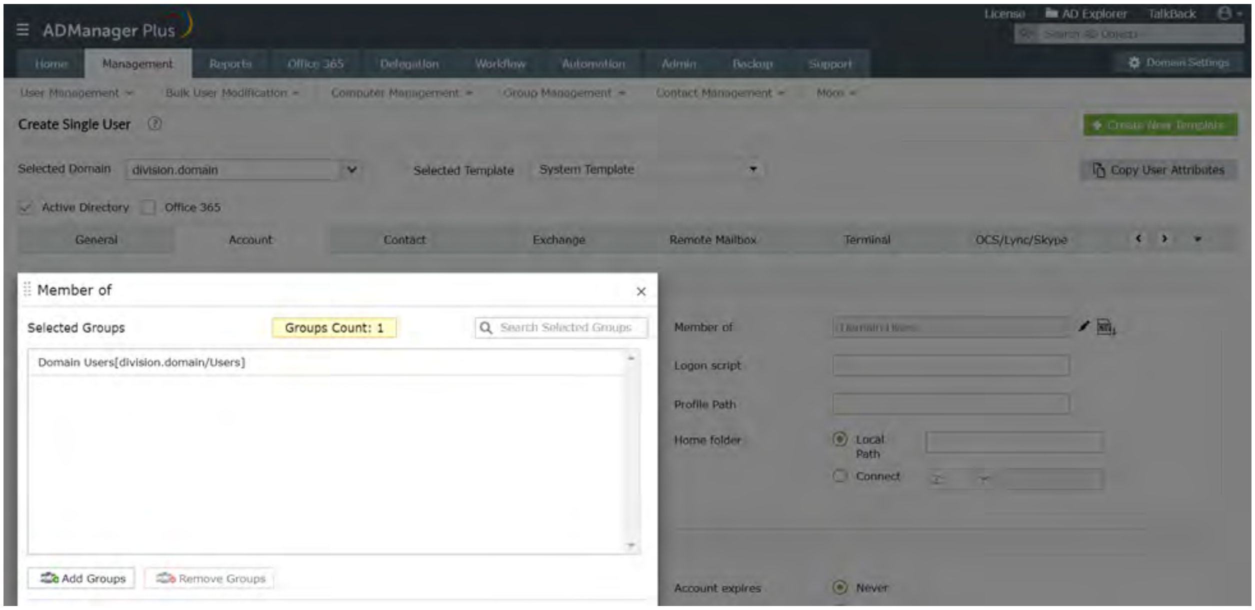
E-mail: @ division.domain

Web page:

* Select Container: CN=Users,DC=division,DC=domain

□ Protect object from accidental deletion

3. In the **General** tab, fill in the mandatory as well as required attribute fields.
4. Switch to the **Account** tab to configure the group membership. Click on the **edit** option located near the **memberOf** option to add the group to which the user should be a member. In the memberOf window, click on **Add groups** option. Choose the required groups from the **Select Groups** window and hit on **OK.**



Create Single User

Selected Domain: division.domain

Selected Template: System Template

☑ Active Directory □ Office 365

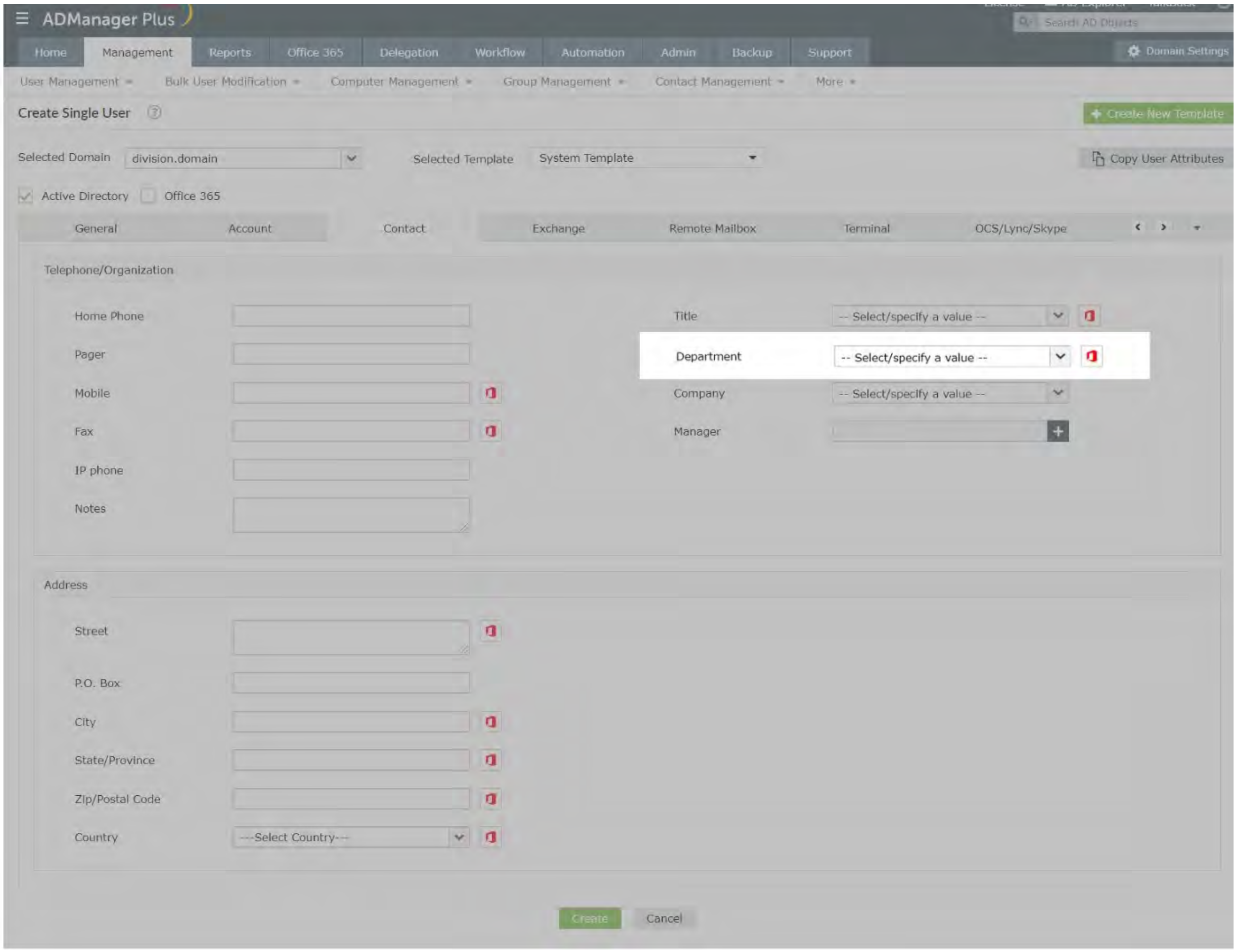
Member of

Selected Groups — Groups Count: 1

Domain Users[division.domain/Users]

Account expires: ● Never

5. Switch to the **Contact** tab to configure the **Department** to which the user should belong. Click on the drop-down box to select the department from the pre-defined list or type in your own department.



Create Single User

Selected Domain: division.domain

Selected Template: System Template

☑ Active Directory □ Office 365

Telephone/Organization

Title: -- Select/specify a value --

Department: -- Select/specify a value --

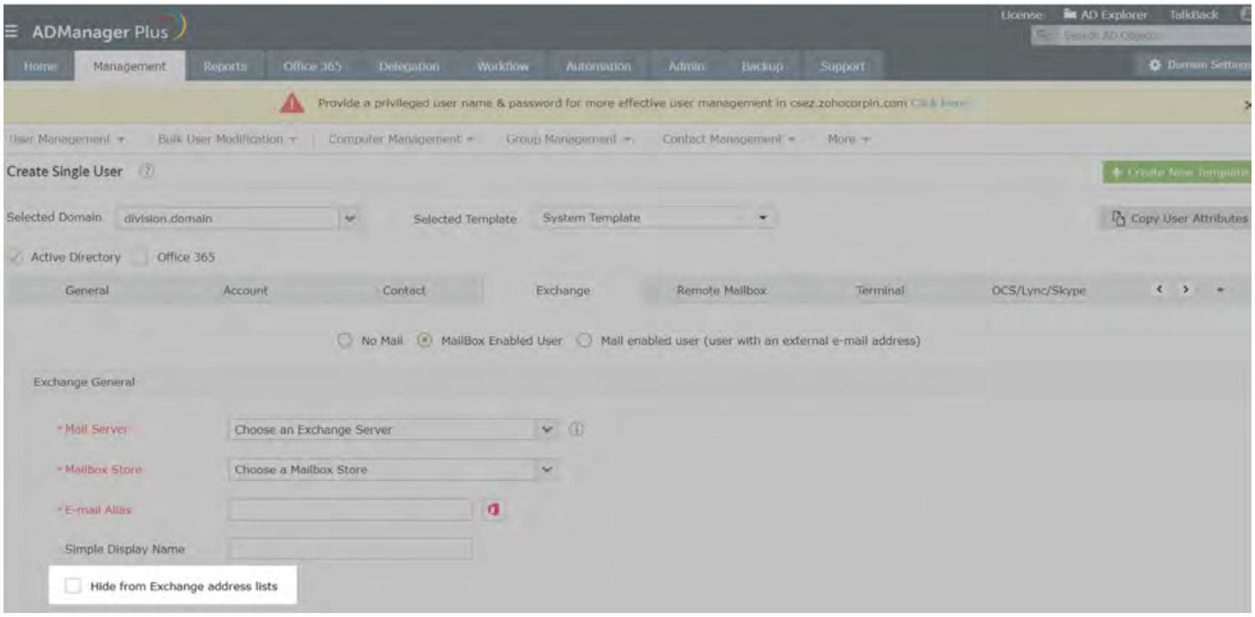
Company: -- Select/specify a value --

Address

Country: ---Select Country---

NOTE: You can also traverse to **Titles and Departments** section in the **Admin** tab to pre-define departments conferring to your organizational requirements.

6. To configure the Hide from exchange address lists, switch to the **Exchange** tab, click on the **Mailbox Enabled User** option and select the **Hide from Exchange Address Lists**.



Selected Domain: division.domain

Selected Template: System Template

○ No Mail ● MailBox Enabled User ○ Mail enabled user (user with an external e-mail address)

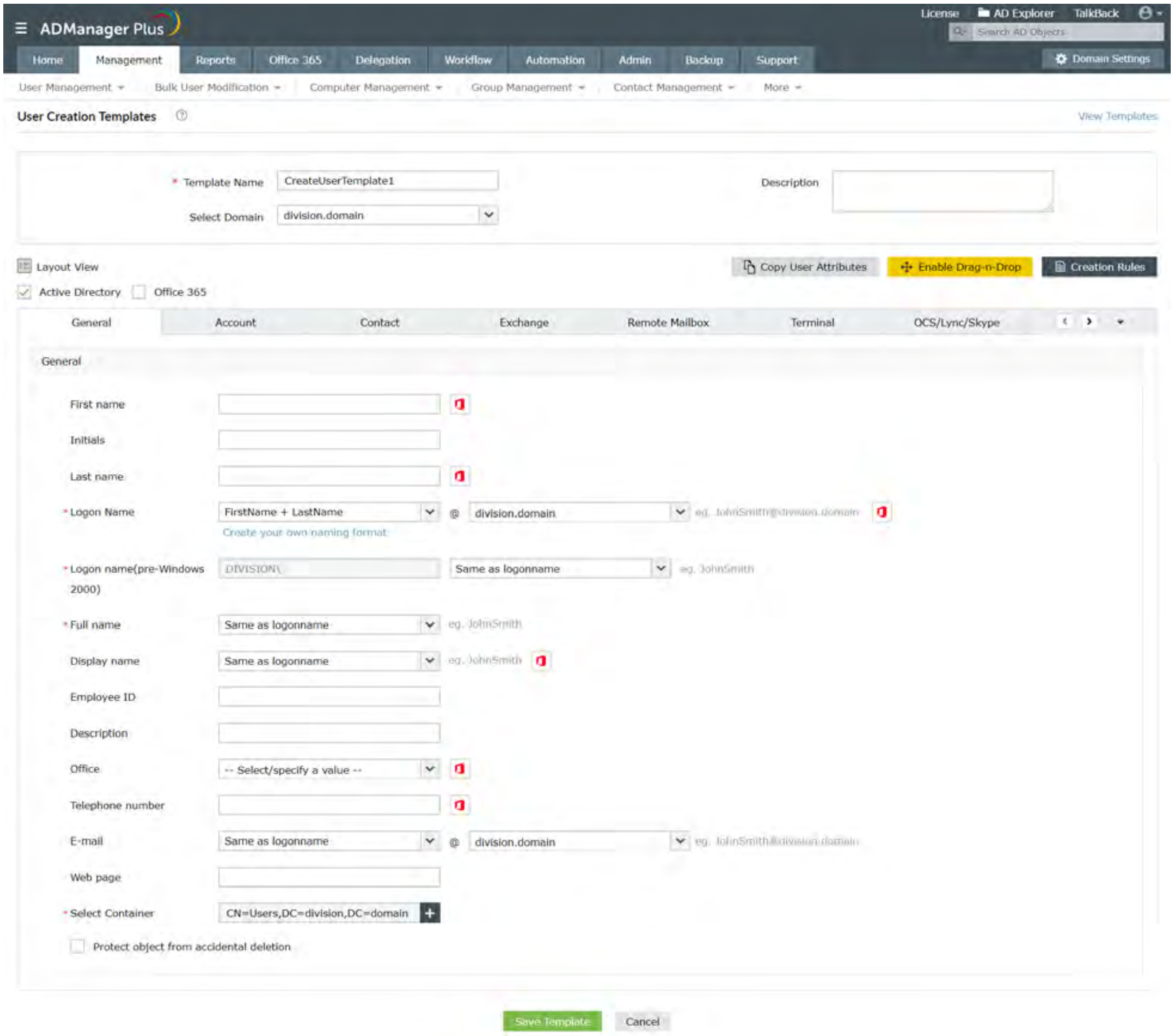
Mail Server: Choose an Exchange Server

Mailbox Store: Choose a Mailbox Store

□ Hide from Exchange address lists

Steps to create users in bulk with the aforementioned criteria:

1. Logon to the ADManager Plus tool and click on the **Management** tab.
2. Select the **User Creation Templates** and click on **Create new Template** option
3. Enter a name for this template and also select the domain for which you want to apply this template.
4. Specify the groups to which the users have to be added in the **Group** section of the '**Account Details**' tab.
5. Specify the **Department** in the **Organization** section in the **Contact** tab.
6. Select the **Hide from Exchange Address Lists** option in **Exchange General** section in the **Exchange** tab. Save the template.



User Creation Templates

* Template Name: CreateUserTemplate1

Select Domain: division.domain

Description:

☑ Active Directory ☐ Office 365

General

First name:

Initials:

Last name:

* Logon Name: FirstName + LastName @ division.domain eg. JohnSmith@division.domain

* Logon name(pre-Windows 2000): DIVISION\ Same as logonname eg. JohnSmith

* Full name: Same as logonname eg. JohnSmith

Display name: Same as logonname eg. JohnSmith

Employee ID:

Description:

Office: -- Select/specify a value --

Telephone number:

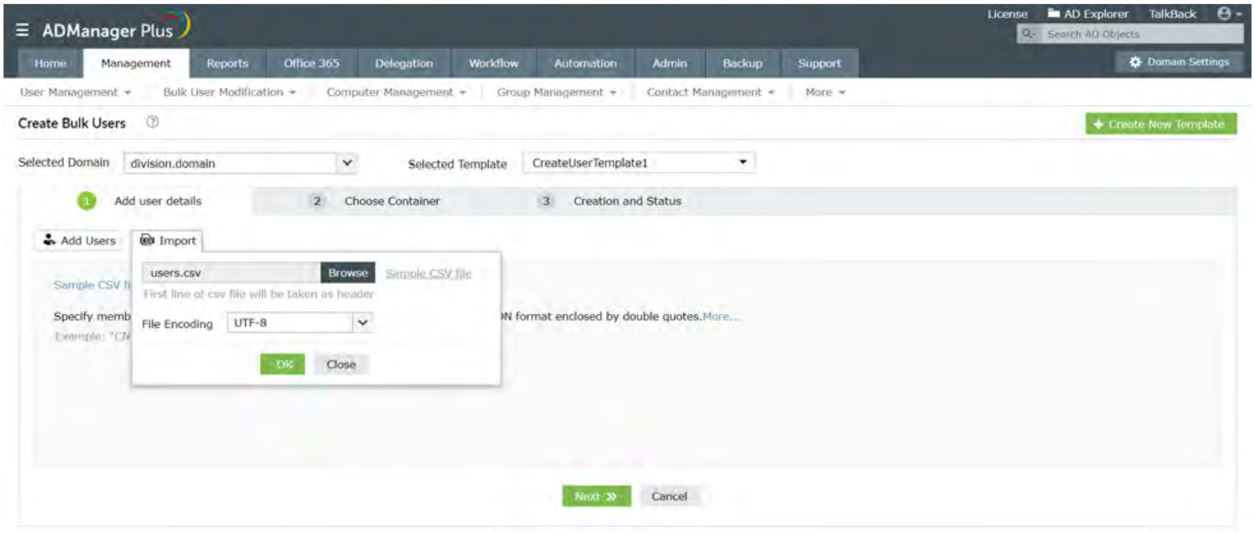
E-mail: Same as logonname @ division.domain eg. JohnSmith@division.domain

Web page:

* Select Container: CN=Users,DC=division,DC=domain

☐ Protect object from accidental deletion

7. Switch back to the **Management** tab and select the **Create Bulk Users** option under the **User Creation** section.
8. Select the **Domain** to which you want to add the users and also specify the name of the template that you've specified in step 3 under the **Selected Template** option.
9. Choose the **Import** option and specify the path of the CSV file that contains the details of the users. You can also use the **Add Users** option to enter the details of the users manually.
10. Next, choose the container in which you want to place the users. You can also dynamically create a new OU by clicking on the **Create New OU** option.
11. Click on **Create New Users**



Create Bulk Users

Selected Domain: division.domain

Selected Template: CreateUserTemplate1

users.csv

First line of csv file will be taken as header

File Encoding: UTF-8

Specify memb

Example: "CN

N format enclosed by double quotes.More...

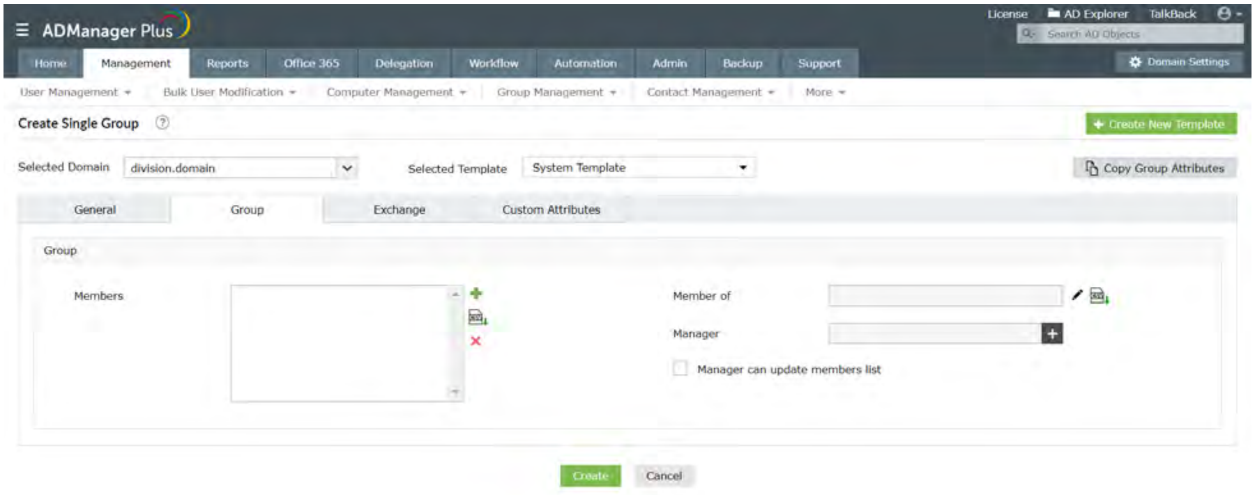
Exercise 2: Group Provisioning

Objective: Create a new group and add members of two specific groups to this new group.

To achieve the above using the native AD tools, you will first have to create a new group, edit its properties, select the add option under the *Members* tab, search for the groups and finally add them as members.

The following are the steps using which you can perform the above task easily using ADManager Plus:

1. Click on the **Management** tab and select the **Group Management** section located on the left side of the window.
2. Select the **Create Single Group** option**,** enter the attributes of the group in the **General** Tab .
3. Navigate to the **Group** tab and click on the **add, remove or import csv** option located next to the **Members** section.
4. A **Select Members** window will open using which you can add users, groups and computers to the new group. Type the names of the two specific groups in the search bar, select the checkbox located next to them and click **OK**.
5. Once the members are added, click on **Create.**



Selected Domain: division.domain

Selected Template: System Template

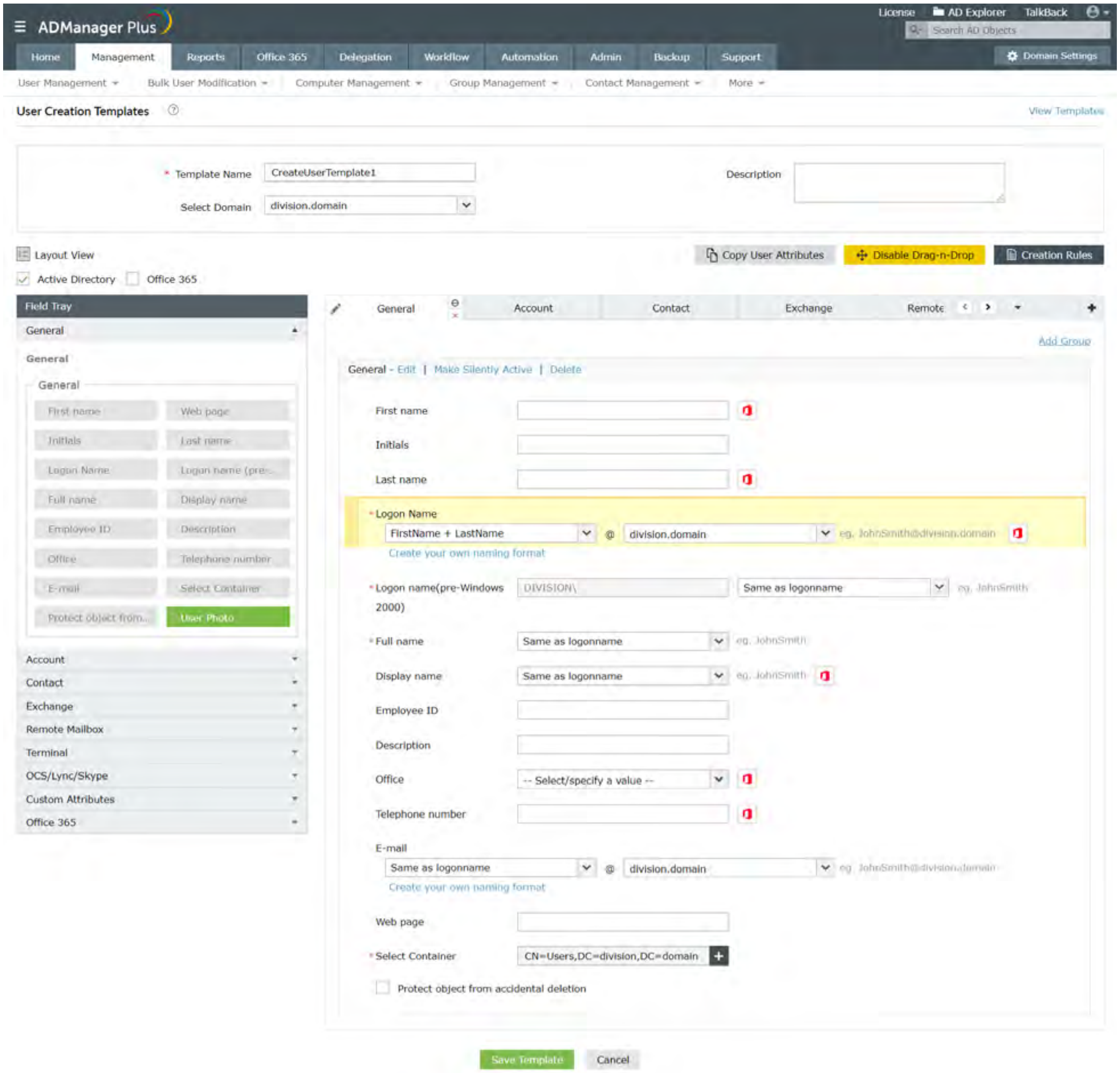
☐ Manager can update members list

Exercise 3: Prevent duplication during AD user creation

Objective: To avoid duplication during AD user creation by configuring an alternate naming format for user logon name.

Steps to accomplish the given objective:

1. To create a user creation template:
    a. Login to ADManager Plus and click on the **Management** tab.
    b. Click on **User Management** and choose **User Creation Templates . Then**click on **Create New Template**.
    c. Enter a suitable name and description for the template.
    d. Select the **Domain** of your choice.
    e. Click on **Enable Drag-n-Drop** option.
    f. Hover the mouse over the **Logon Name** and click on the E**dit** option.



* Template Name: CreateUserTemplate1

Select Domain: division.domain

Description:

☑ Active Directory ☐ Office 365

First name:

Initials:

Last name:

* Logon Name: FirstName + LastName @ division.domain eg. JohnSmith@division.domain

* Logon name(pre-Windows 2000): DIVISION\ Same as logonname eg. JohnSmith

* Full name: Same as logonname eg. JohnSmith

Display name: Same as logonname eg. JohnSmith

Employee ID:

Description:

Office: -- Select/specify a value --

Telephone number:

E-mail: Same as logonname @ division.domain eg. JohnSmith@division.domain

Web page:

* Select Container: CN=Users,DC=division,DC=domain

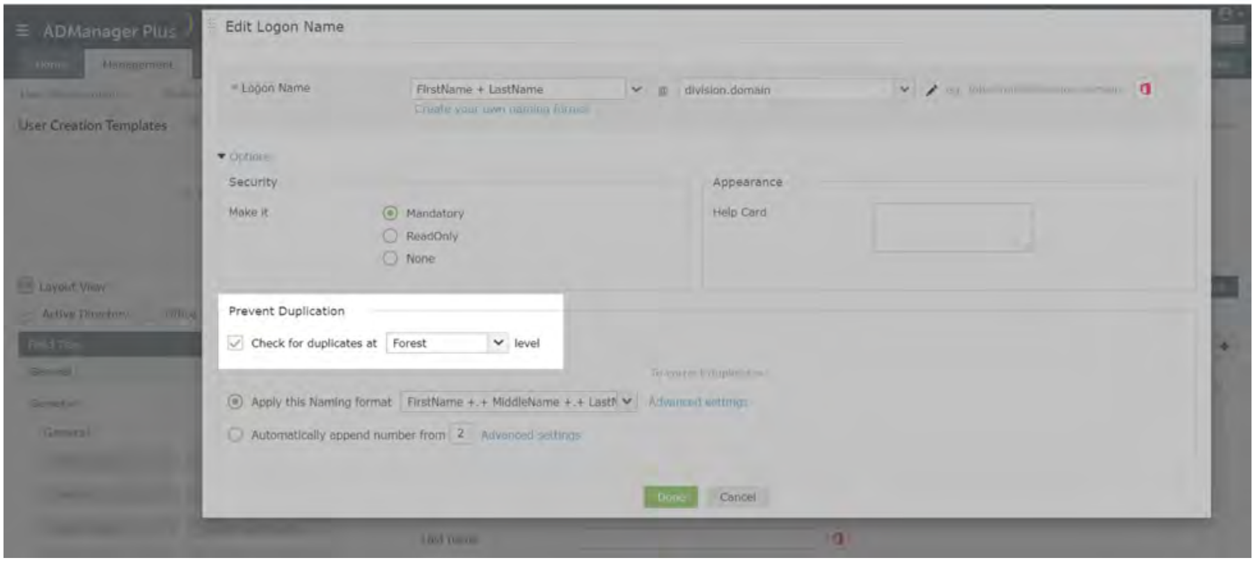
☐ Protect object from accidental deletion

g. Under the **Prevent Duplication** section, select the **Check for duplicates** option and set the duplication check at the forest level.

h. Select the **Apply this Naming format** in case a duplication occurs.

i. Click on the **Advanced Settings** option, if you want to set alternate naming formats that must be followed if a logon name with the pre-defined naming format already exists.

j. Click on **Done**.



Edit Logon Name

* Logon Name: FirstName + LastName @ division.domain

Create your own naming format

▾ Options

Security

Make it: ● Mandatory ○ ReadOnly ○ None

Appearance

Help Card

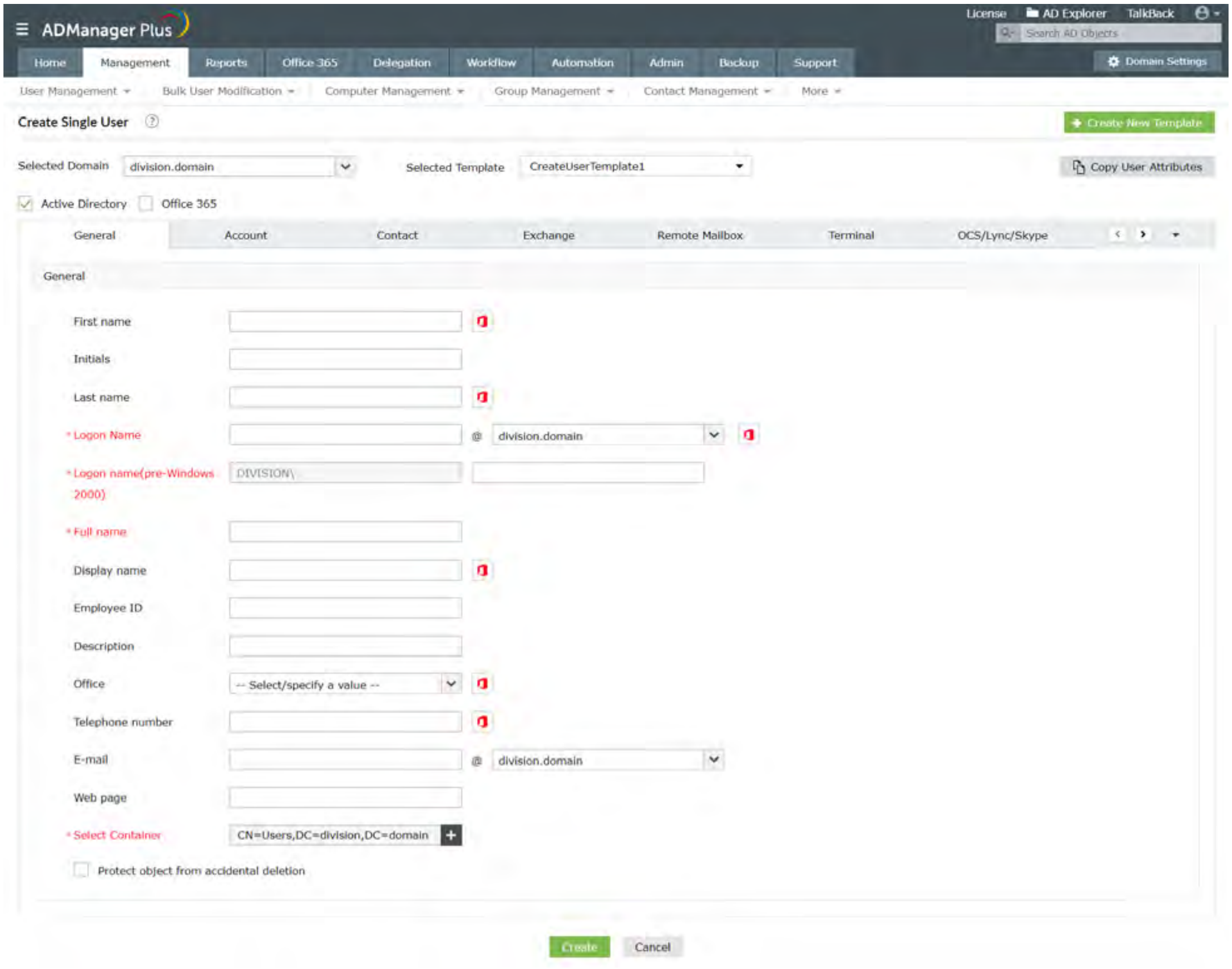
Prevent Duplication

☑ Check for duplicates at Forest level

● Apply this Naming format FirstName +.+ MiddleName +.+ LastN Advanced settings

○ Automatically append number from 2 Advanced settings

2. To create users using the this template:
    a. Click on the **Management** tab and click on **Create Single User**.
    b. Select the **Domain** of your choice.
    c. Select the template that you just created.
    d. Enter the details of the user.
    e. Click **Create**.



Selected Domain: division.domain

Selected Template: CreateUserTemplate1

☑ Active Directory ☐ Office 365

General

First name

Initials

Last name

* Logon Name @ division.domain

* Logon name(pre-Windows 2000) DIVISION\

* Full name

Display name

Employee ID

Description

Office -- Select/specify a value --

Telephone number

E-mail @ division.domain

Web page

* Select Container CN=Users,DC=division,DC=domain

☐ Protect object from accidental deletion

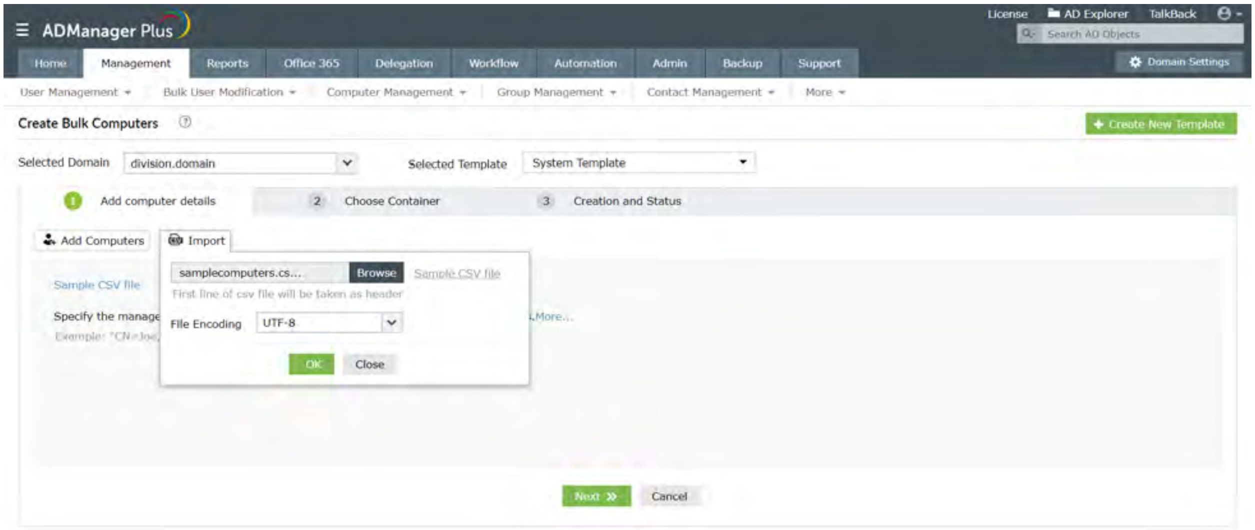
Exercise 4: Computer Provisioning

Objective: Computer pre-staging and adding computer objects as members of a specific group

In ADManager Plus, it is possible to create computer accounts in bulk quite easily. It is also identically easier to add these computers as members of specific groups using the ADManager Plus interface.

Follow the steps for the same:

1. Click on the **Management** tab and select the **Computer Management** section located on the left side of the window.
2. Select the **Create Bulk Computers** option and specify the **Domain** and the **Template** of your choice.
3. Click on the **Import** option and specify the path of the CSV file in which the attributes of the computers to be added are specified under appropriate headers. Specify the distinguished name of the group to which you want to add the computers under the **memberOf** header.
4. Select the container in which you want to place the computers and hit on **Create.**



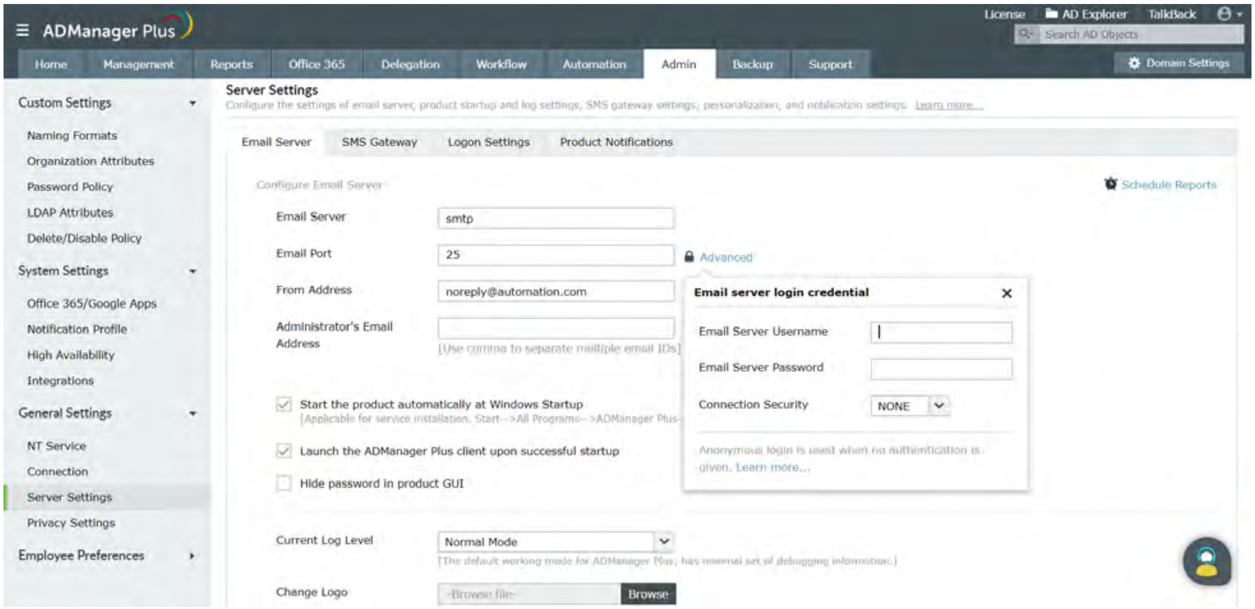
Exercise 5: Real-time notifications

Objective: Send an email notification to the administrator whenever a new user is created.

Steps to accomplish the aforementioned objective:

1. Configure the email server settings:
    a. Click on the **Admin** tab and click on **Server Settings**.
    b. Configure the **Email Server** name and **Port**.
    c. Click on the **Advanced** button to provide the **Email Server Username** and **Password**.
    d. Select the type of **Connection Security**.

    e. Type in the **Administrator's Email Address**.
    f. Click on **Send Test Mail** to test if the configured mail server works.
    g. Click on **Save Changes**.



Server Settings

Configure the settings of email server, product startup and log settings, SMS gateway settings, personalization, and notification settings. Learn more...

Configure Email Server

Email Server: smtp

Email Port: 25 Advanced

From Address: noreply@automation.com

Administrator's Email Address: [Use comma to separate multiple email IDs]

☑ Start the product automatically at Windows Startup [Applicable for service installation. Start-->All Programs-->ADManager Plus-

☑ Launch the ADManager Plus client upon successful startup

□ Hide password in product GUI

Current Log Level: Normal Mode [The default workong mode for ADManager Plus; has minimal set of debugging information.]

Change Logo: -Browse file- Browse

Email server login credential ✕

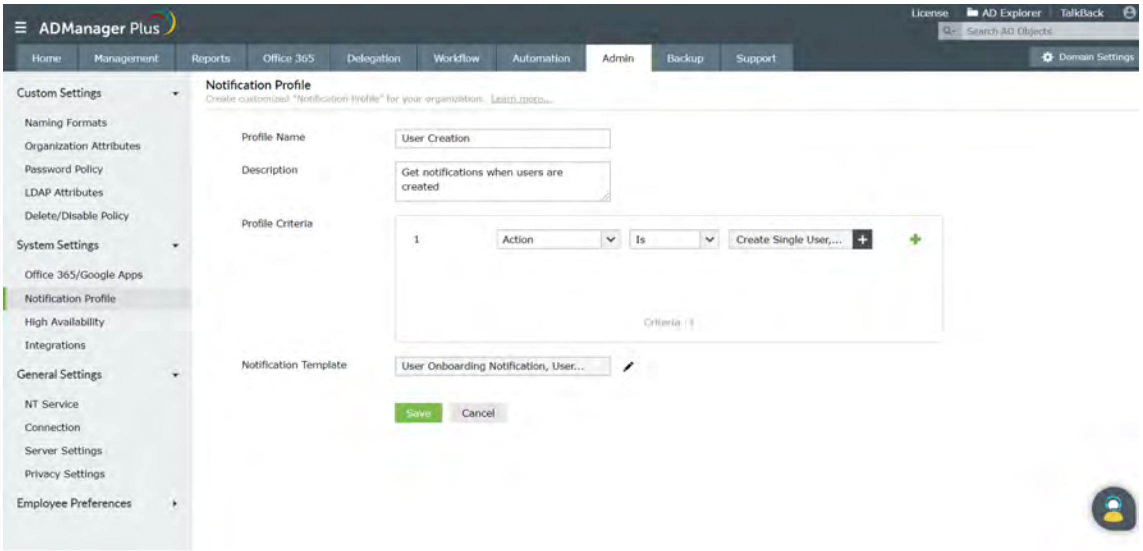
Email Server Username:

Email Server Password:

Connection Security: NONE

Anonymous login is used when no authentication is given. Learn more...

2. Create a notification profile:
    a. Click on the **Notification Profile** section on the left pane of the **Admin** tab.
    b. Click on the **Edit** option located next to the **User Creation** profile.
    c. Click on the edit option given next to the **Notification Template**.
    d. Select the **User Creation Admin notification** option.
    e. Click on **OK**.
    f. Click on **Save**.



Notification Profile

Create customized "Notification Profile" for your organization. Learn more...

Profile Name: User Creation

Description: Get notifications when users are created

Profile Criteria: 1 Action Is Create Single User,...

Criteria : 1

Notification Template: User Onboarding Notification, User...

3. Now whenever a user is created, the administrator will be notified automatically.

Note: You can also configure notifications for other management actions like password resets, account unlocks and more.

3.2 AD object modification (Common Active Directory Management tasks)

The exercises in this section have been framed taking into account the most frequent and common AD Management tasks that any Active Directory administrator has to perform, day in and day out, repeatedly.

Using the native interface to accomplish these common tasks usually requires multiple steps. Moreover, to perform these activities in bulk is nothing short of a herculean effort! To avoid such a scenario, you are forced to take the tedious and taxing route of writing scripts which have to be modified for each scenario or requirement and also for every change that might happen in Active Directory.

As opposed to the native tools, ADManager Plus simplifies all of these copious tasks and helps you perform them from a single screen.

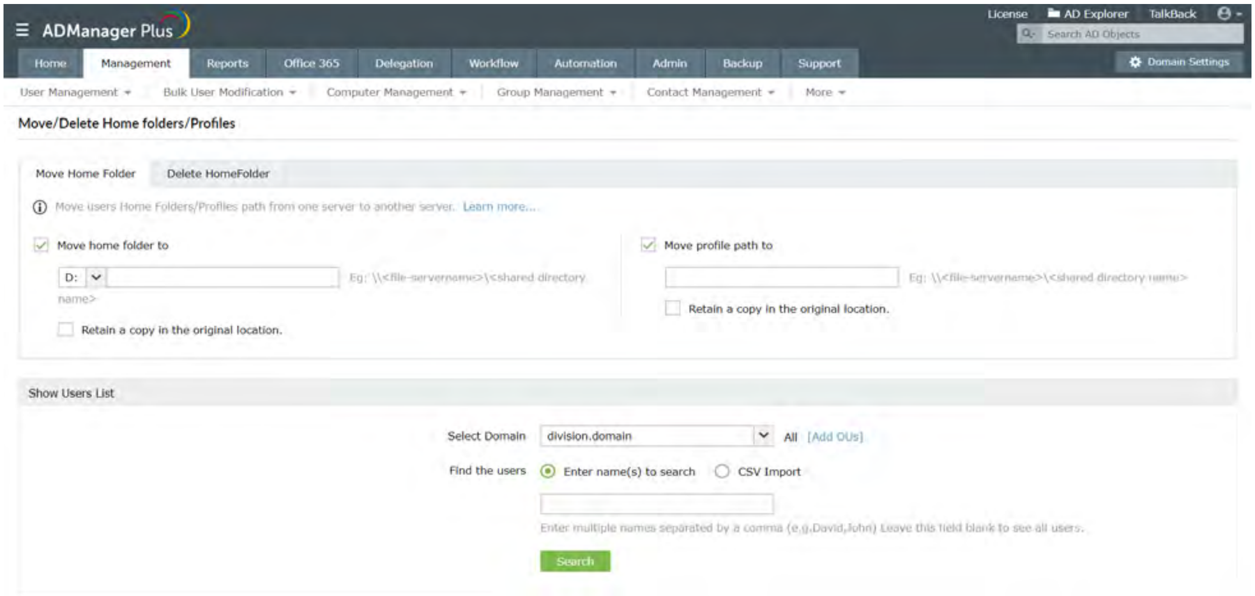
Exercise 1: Decommissioning a file server

Objective: Move/Copy the Home Folders and Profiles of all the users from one file server to another.

In the native Active Directory environment, the home folders and profiles can be changed only for one user at a time. For multiple users the only options are either manually changing the home folders and profile paths for each user, one by one, or using complex PowerShell scripts.

However, using ADManager Plus the task becomes straightforward and easy.
Follow the steps to accomplish the above-mentioned objective:

1. Click on the **Management** tab. select the **Move/Delete Home Folders** option located under the **Bulk User Modification** section of the **User Management** section.
2. Select **Move Home Folder To** option and specify the new location.
3. Similarly, select the **Move Profile Path** option and specify the new server and share name.



Move/Delete Home folders/Profiles

Move users Home Folders/Profiles path from one server to another server.

☑ Move home folder to

D: Eg: \\<file-servername>\<shared directory name>

□ Retain a copy in the original location.

☑ Move profile path to

Eg: \\<file-servername>\<shared directory name>

□ Retain a copy in the original location.

Select Domain: division.domain All

Find the users: ● Enter name(s) to search ○ CSV Import

Enter multiple names separated by a comma (e.g.David,John) Leave this field blank to see all users.

4. Finally, specify the Users for whom you would like to move the Home Folders and Profile Paths. You can specify the users in bulk by:
   - Importing a CSV file that has the list of users.
   - Searching for the required users using the **Enter name(s) to search** option in the required Domain and OU, if the users are limited to a specific OU.

Exercise 2: Create Exchange Mailboxes for existing users along with additional mail addresses

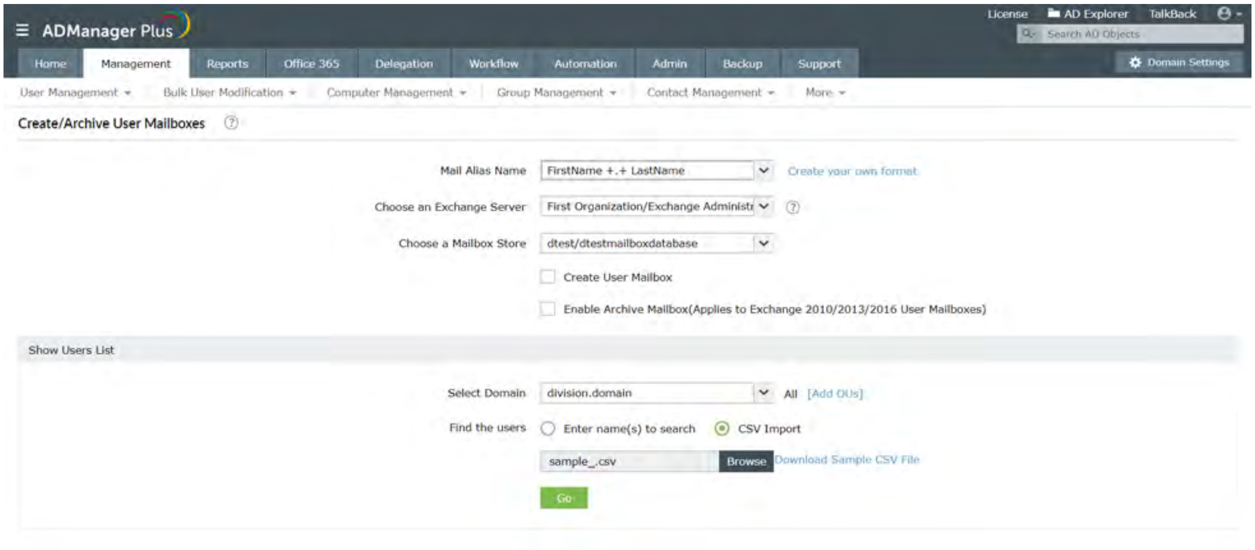
Objective: Create Exchange mailboxes for a set of existing users specified through a CSV file. Also, create additional mail addresses for these users.

Usually, in an AD environment, to create mailboxes for existing AD users, you have to switch to an Exchange Server. When it comes to performing these tasks for multiple users, the task becomes even more complicated and tiresome.

However, with ADManager Plus the task can easily be achieved using the following steps:

1. Click on the **Management** tab and select the **Create/Archive User Mailbox** located under **Exchange Mailbox Tasks** column of the **User Management** section.
2. Select a format from the drop down box for the **Mail Alias Name** or click on **Create Your Own Format** to create your own naming format.
3. Choose a required Exchange Server and Mailbox Store from your Exchange environment using the appropriate drop down boxes.
4. Enable the **Create User Mailbox** option.
5. Click on **CSV Import** to import the CSV file that has the list of users. Select the users and click on **Apply.**

6. To create additional mail addresses, follow the steps given here.



Create/Archive User Mailboxes

Mail Alias Name: FirstName +.+ LastName — Create your own format

Choose an Exchange Server: First Organization/Exchange Administ

Choose a Mailbox Store: dtest/dtestmailboxdatabase

□ Create User Mailbox

□ Enable Archive Mailbox(Applies to Exchange 2010/2013/2016 User Mailboxes)

Show Users List

Select Domain: division.domain — All [Add OUs]

Find the users: ○ Enter name(s) to search ● CSV Import

sample_.csv — Browse — Download Sample CSV File

Go

Exercise 3: Web-based Password Reset

Obejctive: Reset the password of Active Directory users so that they comply with the password policies of the domain and the OU they are a part of.

Resetting user passwords using the native AD interface requires three steps:

- Locating the user
- Selecting the User
- Selecting the reset password option.

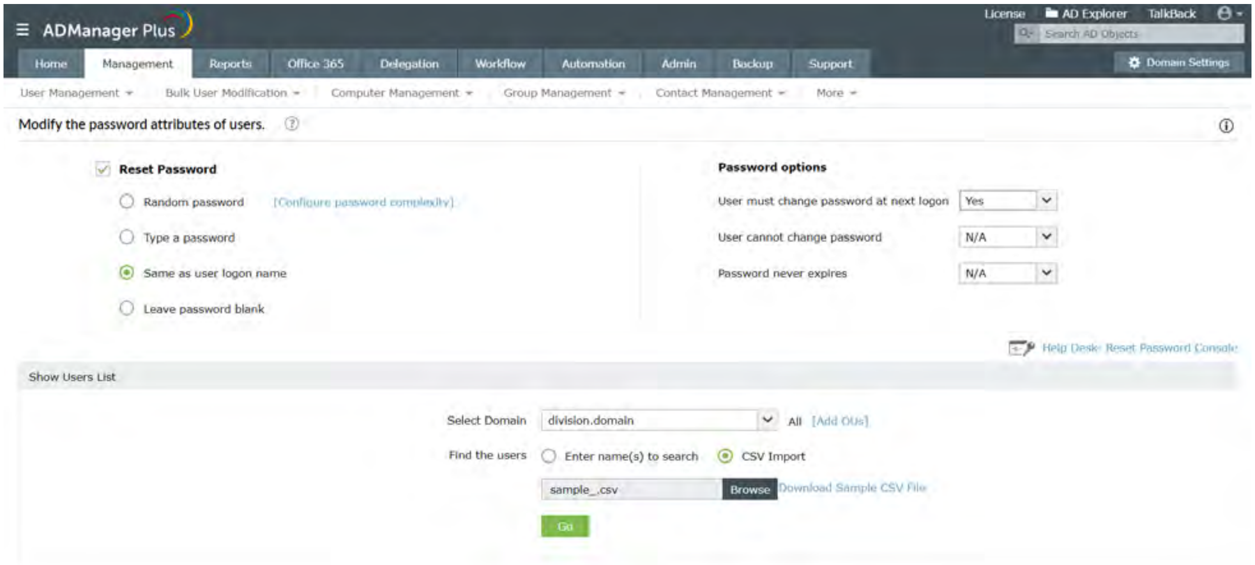
They seem like simple tasks, but when it comes to multiple users, the task becomes cumbersome and hence requires the use of complex scripts.
Also, another security concern that arises during user provisioning is that a common password is used for all the newly created accounts which are later to be changed by the users themselves. However, existing users already know the passwords for new users and they might misuse this information.

All these issues can easily be tackled by employing the capabilities of ADManager Plus.

Steps to perform web-based password reset for user accounts:

1. Logon to ADManager Plus and click the **Management** tab.
2. Go to the **User Management** section and select the **Reset Password** option under the **Bulk User Modification** section.
3. Under the **Reset password** section, you can select any of the following options for generating new passwords:
    - Generate password (for generating a random password)

    - Type a password
    - Same as user logon name
    - Leave password blank
4. Based on your needs you can select from different **Password options** like :
    - User must change password at next logon
    - User cannot change password
    - Password never expires
5. Specify the users whose passwords are to be reset by:
    - Importing a CSV file that has the list of all required users
    - Using the built-in search feature
6. Click **Apply** for the changes to take place.



Modify the password attributes of users.

☑ Reset Password

○ Random password [Configure password complexity]

○ Type a password

● Same as user logon name

○ Leave password blank

Password options

User must change password at next logon	Yes
User cannot change password	N/A
Password never expires	N/A

Select Domain: division.domain All [Add OUs]

Find the users: ○ Enter name(s) to search ● CSV Import

sample_.csv

Exercise 4: Modify the existing logon names of users using a different naming format.

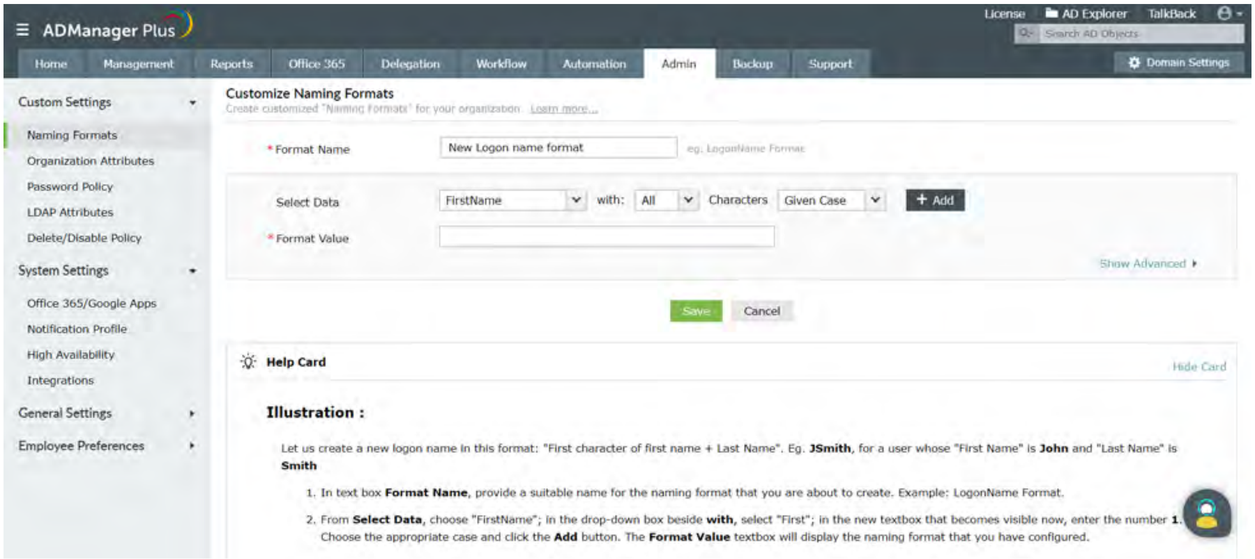
Objective: Create a new naming format using the 'first character of first name and last name' and then update the existing logon name of all users in a specific Department (OU).

In a native AD environment, creating multiple naming formats is a cumbersome task. Updating the logon names for multiple users to the newly created naming formats is another complicated task altogether.

Follow the steps below to accomplish this objective easily through ADManager Plus:

1. Click on **Admin** tab. Under the **Naming Formats** section, click on **Add New Format** on the top right corner.
2. Specify a **Format Name** for this new naming format.
3. In **Select Data** select ‘FirstName’ with ‘First’ ‘1’ Character. Choose whether the character is uppercase, lowercase or the given case using the drop-down. Click **Add**.

4. Select ‘LastName’ in **Select Data** again with ‘First’ ‘1’ Character. Choose the case. Click **Add**.
5. **Save** the new format.



Customize Naming Formats

Create customized "Naming Formats" for your organization Learn more...

*Format Name: New Logon name format (eg: LogonName Format)

Select Data: FirstName with: All Characters Given Case

*Format Value:

Help Card

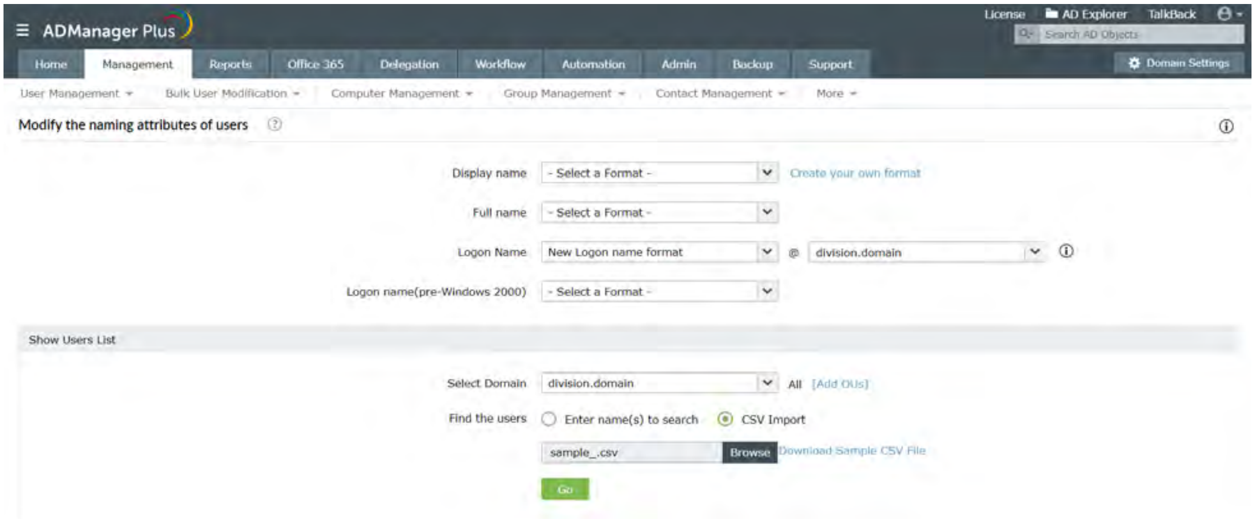
Illustration :

Let us create a new logon name in this format: "First character of first name + Last Name". Eg. **JSmith**, for a user whose "First Name" is **John** and "Last Name" is **Smith**

1. In text box **Format Name**, provide a suitable name for the naming format that you are about to create. Example: LogonName Format.
2. From **Select Data**, choose "FirstName"; in the drop-down box beside **with**, select "First"; in the new textbox that becomes visible now, enter the number **1**. Choose the appropriate case and click the **Add** button. The **Format Value** textbox will display the naming format that you have configured.

6. Click on **Management**. Under **User Management** go to **Bulk User Modification** section and select the **Naming Attributes** option.
7. Select the newly created Naming Format from the drop down box in the **Modify the Logon Name Format** field.
8. Select the required users by:
   - Importing a CSV file that has the list of the required users.
   - Searching for the required users using the **Enter name(s) to search** option in the required Domain and OU, if the users are limited to a specific OU.

9. Click on **Apply** for the changes to take place.



Modify the naming attributes of users

Display name: - Select a Format -

Full name: - Select a Format -

Logon Name: New Logon name format @ division.domain

Logon name(pre-Windows 2000): - Select a Format -

Select Domain: division.domain All

Find the users: ○ Enter name(s) to search ● CSV Import

sample_.csv

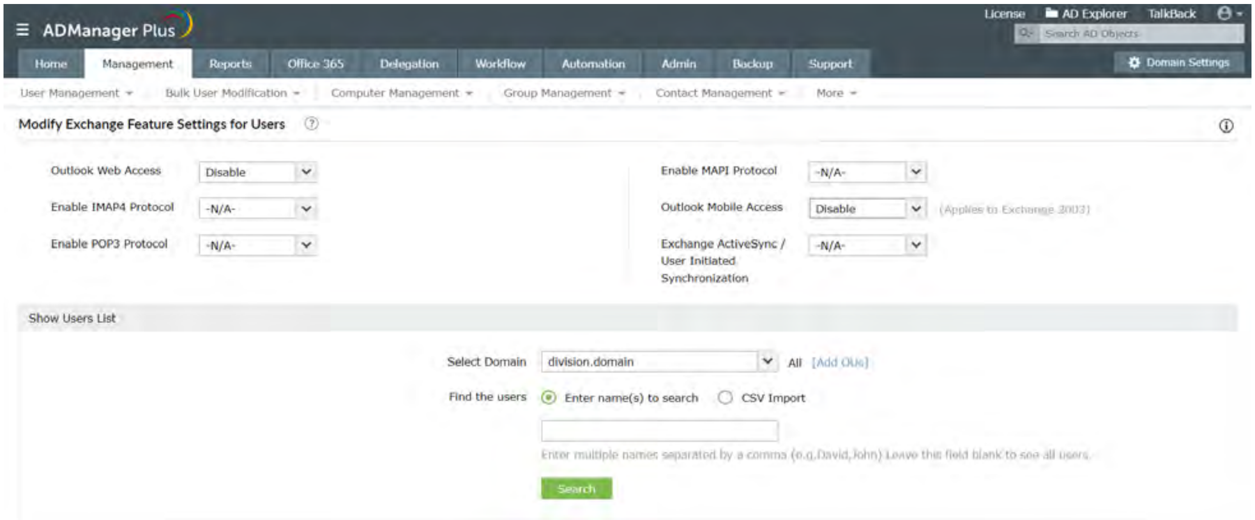
Exercise 5: Deny access to emails through web-browser and smartphones

Objective: Deny the access to Outlook through the internet or through smartphones, for a selected set of users.

In AD, to accomplish the above, one has to switch to an Exchange server, locate the user and modify the features and properties of that user, which is extremely tedious and time-consuming.
ADManager Plus facilitates bulk-user modification for Exchange-related tasks as well. This capability of ADManager Plus can be put to use to accomplish the given exercise.

Follow these steps to accomplish the objective discussed above:

1. Click on the **Management** tab. Under **User Management** section, navigate to the **Exchange Tasks** and select the **Exchange Features** option.
2. **Disable** the **Outlook Web Access** and **Outlook Mobile Access** options.



Modify Exchange Feature Settings for Users

Outlook Web Access	Disable	Enable MAPI Protocol	-N/A-
Enable IMAP4 Protocol	-N/A-	Outlook Mobile Access	Disable (Applies to Exchange 2003)
Enable POP3 Protocol	-N/A-	Exchange ActiveSync / User Initiated Synchronization	-N/A-

Show Users List

Select Domain: division.domain All [Add OUs]

Find the users: ◉ Enter name(s) to search ○ CSV Import

Enter multiple names separated by a comma (e.g.David,John) Leave this field blank to see all users.

Search

3. Select the specified set of users by:
   - Importing a CSV file that has the list of required users.
   - Searching for the required users using the **Enter name(s) to search** option in the required Domain and OU, if the users are limited to a specific OU.

4. Click on **Apply.**

Exercise 6: Assign a new Primary email address to existing users.

Objective: To assign an additional email address to existing users and set it as the primary email address.

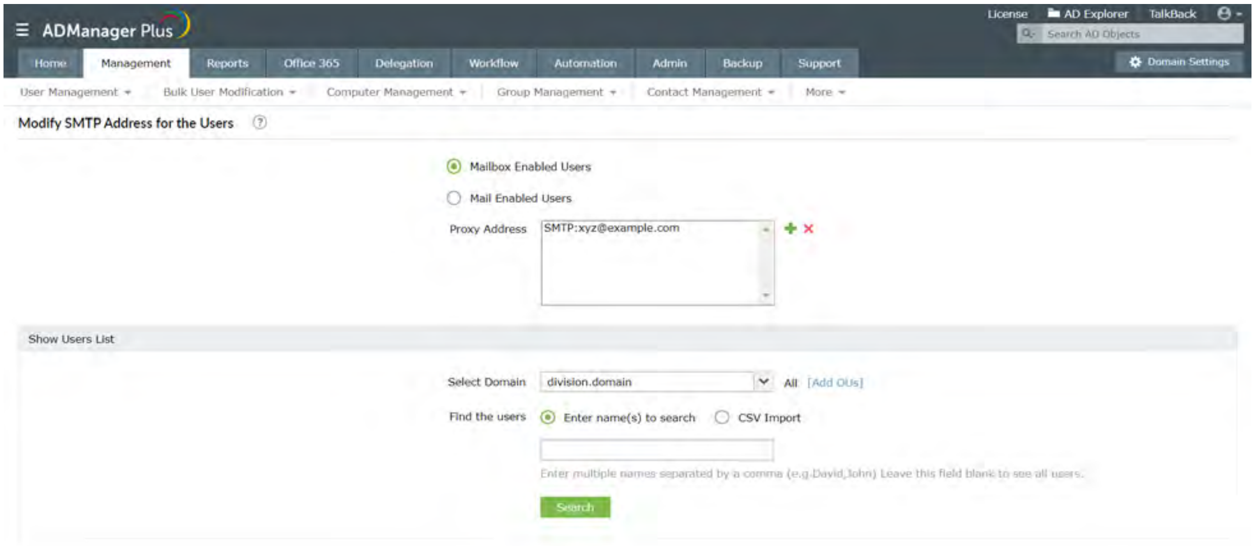
In a native AD environment, you need to switch to an Exchange Server to set a new Primary email address for existing users. However, ADManager Plus allows you to accomplish AD management as well as Exchange management tasks from a single console.

Follow the below to complete the exercise:

1. Click on the **Management** tab. Under **User Management** section, navigate to the **Exchange Tasks** column and select the **Modify SMTP Address** option.
2. Select the type of users.
3. For **Mailbox Enabled Users**, Click on the **Add** option located next to the **Proxy Addresses** field.
4. Specify the new **Email Address Format** with the prefix **SMTP:** to set this new format as the **Primary email Address**.

   NOTE: Setting the prefix to **smtp:** will set the email address as a secondary one.

5. For **Mail Enabled Users**, specify the new format in the **Target Address**. Refer the previous steps to specify a new format as per the requirement.
6. Select the required **Domain/OU** and specify the list of users using either a CSV file or by locating them using the **Search** option.



Modify SMTP Address for the Users

● Mailbox Enabled Users

○ Mail Enabled Users

Proxy Address: SMTP:xyz@example.com

Show Users List

Select Domain: division.domain All [Add OUs]

Find the users: ● Enter name(s) to search ○ CSV Import

Enter multiple names separated by a comma (e.g.David,John) Leave this field blank to see all users.

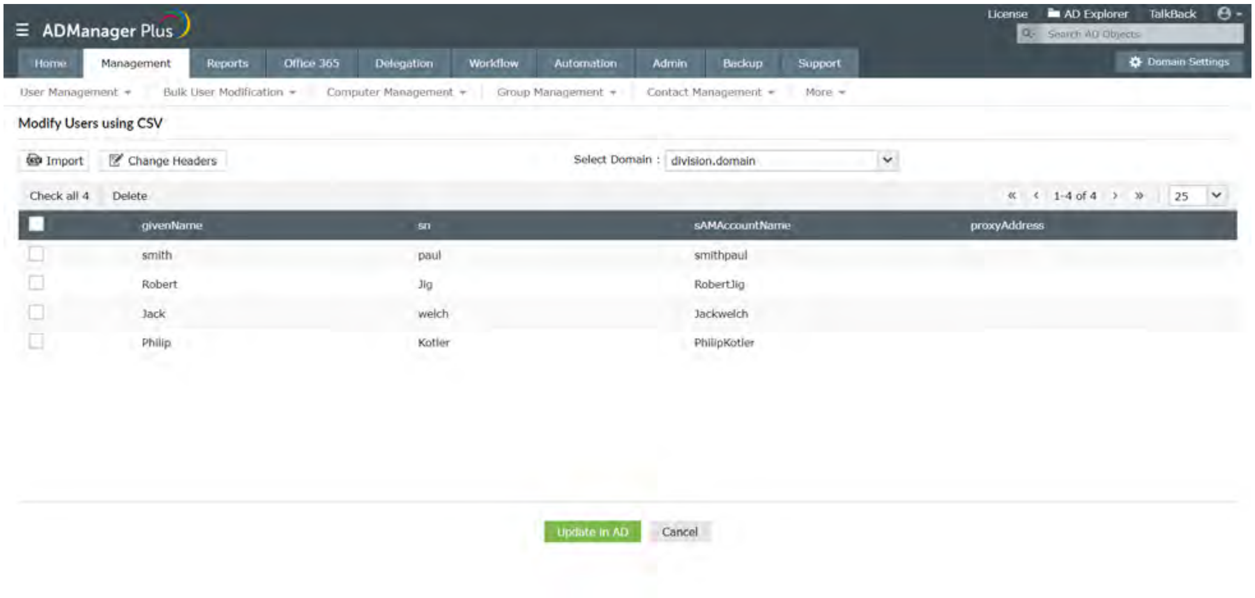
7. Click **Apply** for the changes to take effect.

Exercise 7: Remove the proxy addresses of users

Objective: To remove the proxy addresses of users in AD.

Follow the below to complete the exercise:

1. Click on the **Management** tab and click on **CSV Import** option.
2. Click on **Modify Users** option.
3. Select the required **Domain.**
4. Click on **Import** to import a CSV file that has the user details. In the CSV, leave the proxyAddress field as blank for all the users whose proxy addresses have to be deleted.
5. Select the required users and click on **Update in AD**.
6. Select the **proxyAddresses** as the attribute that is to be modified.
7. Select the criteria to locate/match the user in AD.
8. Select the **Clear the attributes in AD if it's value in CSV is empty** option.
9. Click on **OK**.



Modify Users using CSV

Select Domain : division.domain

givenName	sn	sAMAccountName	proxyAddress
smith	paul	smithpaul	
Robert	Jig	RobertJig	
Jack	welch	Jackwelch	
Philip	Kotler	PhilipKotler	

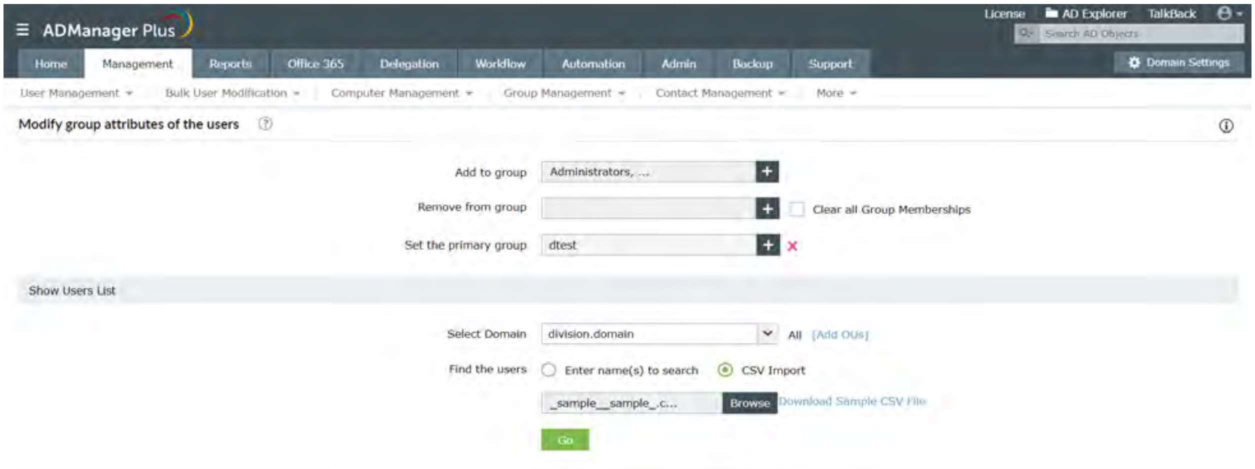
Exercise 8: Add a set of users in a CSV file to a group and set another group as their primary group.

Objective: Add users to a group using a CSV file and also set another group as a primary group for those users.

In the native AD environment, achieving the above objective requires you to locate the users first, modify their memberOf attributes and then choose a group to set up as their primary group. If you want to modify the memberships of the users in bulk you have to use complex scripts.
However, ADManager Plus helps you simplify all of the above to just a few steps.

Follow the steps below to get the task done:

1. Click on the **Management tab**. Under **User Management**, navigate to the **Bulk User Modification** tab, select the **Group Attributes** option in the **General attributes** section.
2. Click on '**+**' beside the **Add to Group** field to specify the group to which the users have to be added.
3. Click on **'+'** beside the **Set the Primary Group** field to set the required group as the primary group.
4. Click on **CSV import** option to import the list of specific users.
5. Click on **Apply** for the changes to take place.



Modify group attributes of the users

Add to group: Administrators, ...

Remove from group:

□ Clear all Group Memberships

Set the primary group: dtest

Show Users List

Select Domain: division.domain All [Add OUs]

Find the users: ○ Enter name(s) to search ● CSV Import

_sample__sample_.c...

Exercise 9: Remove the members of a group using a CSV

Objective: To remove all the members of a group by importing a CSV file.

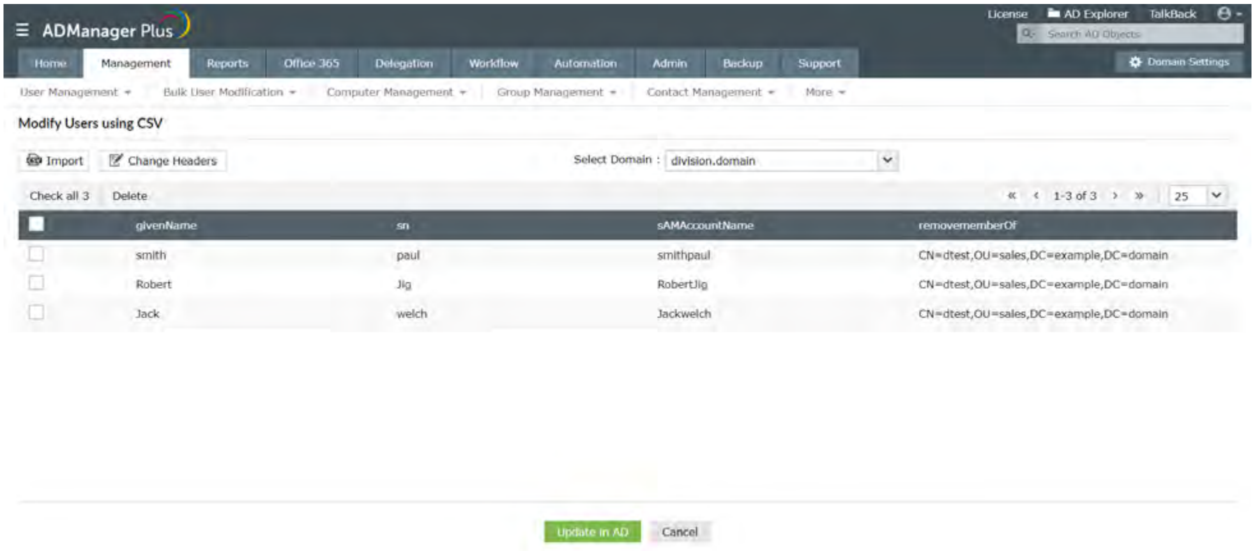
Follow the steps given below:

1. Create a CSV file that contains the following details:
   a. Specify the removememberOf attribute as the column name.
   b. Specify the group names for that field by giving the Distinguished Name of the groups separated by semicolon (;)

      Example:

      "CN=Group1,CN=Users,DC=domain,DC=com;CN=Group2,CN=Users,DC=domain,DC=com"
2. Login to ADManager Plus and click on the **Management** tab.
3. Click on the **CSV Import** option and click on **Modify User Attributes** option.
4. Select the required **Domain.**
5. Click on **Import** to import a CSV file that you just created.

6. Select the required users and click on **Update in AD**.
7. Select the removememberOf as the attribute that is to be modified.
8. Select the criteria to locate/match the user in AD.
9. Click on **OK**.



Modify Users using CSV

Select Domain : division.domain

25

□	givenName	sn	sAMAccountName	removememberOf
□	smith	paul	smithpaul	CN=dtest,OU=sales,DC=example,DC=domain
□	Robert	Jig	RobertJig	CN=dtest,OU=sales,DC=example,DC=domain
□	Jack	welch	Jackwelch	CN=dtest,OU=sales,DC=example,DC=domain

Exercise 10: Modify User Accounts through User Modification Templates.

Objective: Modify user account properties with user modification templates.

Scenario: Allow help desk technicians to modify user accounts through 'user modification templates' with the following conditions:
- For Technician 1 'First Name' should be a mandatory attribute, for Technician 2 'Employee Id' must be mandatory.
- For Technician 1, the Account, Exchange and Custom Attributes tabs should be hidden completely;
In Terminal Services tab, all attributes except 'remote control' and 'remote access' permissions should be read-only.
- For Technician 2, the Terminal Services and Custom Attributes tabs should be hidden completely; in Exchange tab, all attributes except the Outlook Web Access, protocols and mobile access related settings should be hidden.

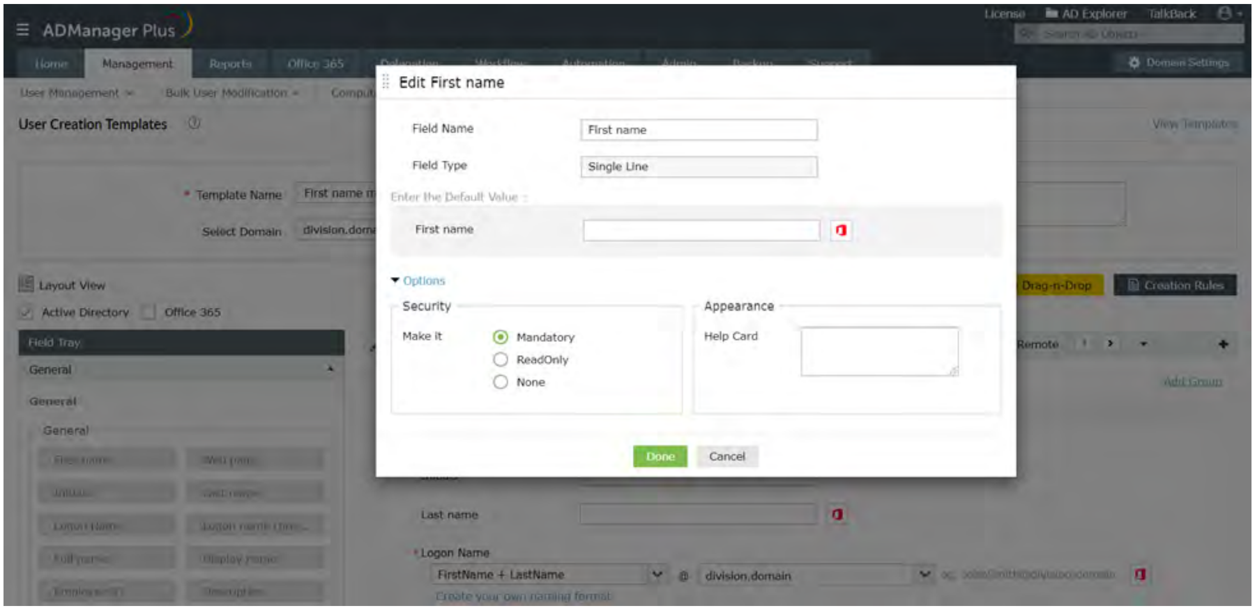
To accomplish this, you will have to create two different user modification templates, one with the conditions for technician 1 and the other for technician 2. You'll then have to assign these templates to the help desk technicians to allow them to modify user accounts in their designated domain(s) or OUs.

Steps to create a user modification template for 'Helpdesk Technician 1' to make first name mandatory:

1. Click on the **Management** tab and click on **User modification templates** in the **User**

Management section.

2. Click on **Create New Template**.
3. Enter a name and description for the template.
4. For this illustration, let us name this template as 'First Name Mandatory'.
5. Select the **Domain** of your choice.
6. Click on the **Enable Drag-n-Drop** option.
7. To make 'First Name' mandatory,
   a. Click on the **General** tab.
   b. Place the mouse over the **First Name** field and then on the edit icon that appears beside the field name.
   c. From the options listed, click on **Edit**.
   d. In the **Editing First Name** window that pops up, under **Security**, select **Mandatory** and click on **Done**.



Edit First name

Field Name: First name

Field Type: Single Line

Enter the Default Value :

First name

Options

Security

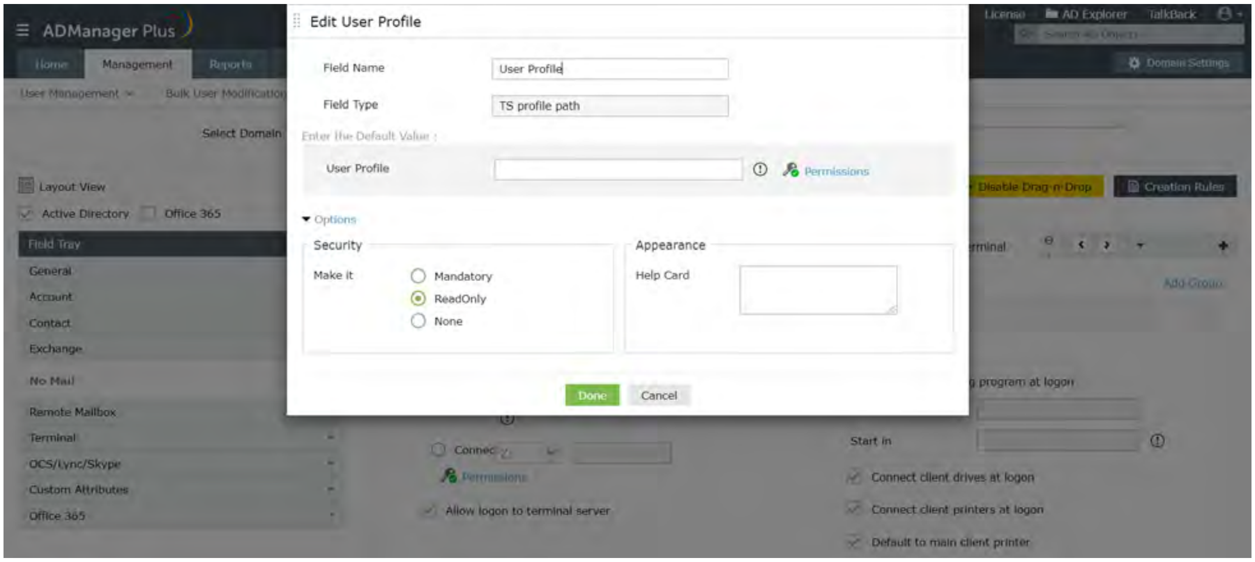
Make it ● Mandatory ○ ReadOnly ○ None

Appearance

Help Card

Done Cancel

8. To hide **Account**, **Exchange** and **Custom Attributes** tabs,
   a. Click on **Account** tab.
   b. Click on the hyphen (**-**) icon located at the top right corner of the **Account** tab. This will hide the tab and make it silently active, that is, the entire tab and all the attributes in the tab will be hidden from the technician who is using this template for user modification.
   c. Similarly, make **Exchange** and **Contract** attribute tabs hidden (silently active).
9. To make all attributes in **Terminal Services** tab, except the ‘remote control’ and ‘remote access’ attributes read-only:
   a. Click on the **Terminal** tab.
   b. Place the mouse over **User Profile** field; click on the edit icon that appears beside the field name.
   c. In **Editing User Profile** window, click on **Options** and set it to: **ReadOnly**.
   d. Click on **Done** to save the changes.
   e. Similarly, make all the required attributes in the **Terminal** tab **ReadOnly**.



Edit User Profile

Field Name: User Profile

Field Type: TS profile path

Enter the Default Value :

User Profile

Options

Security

Make it ○ Mandatory ● ReadOnly ○ None

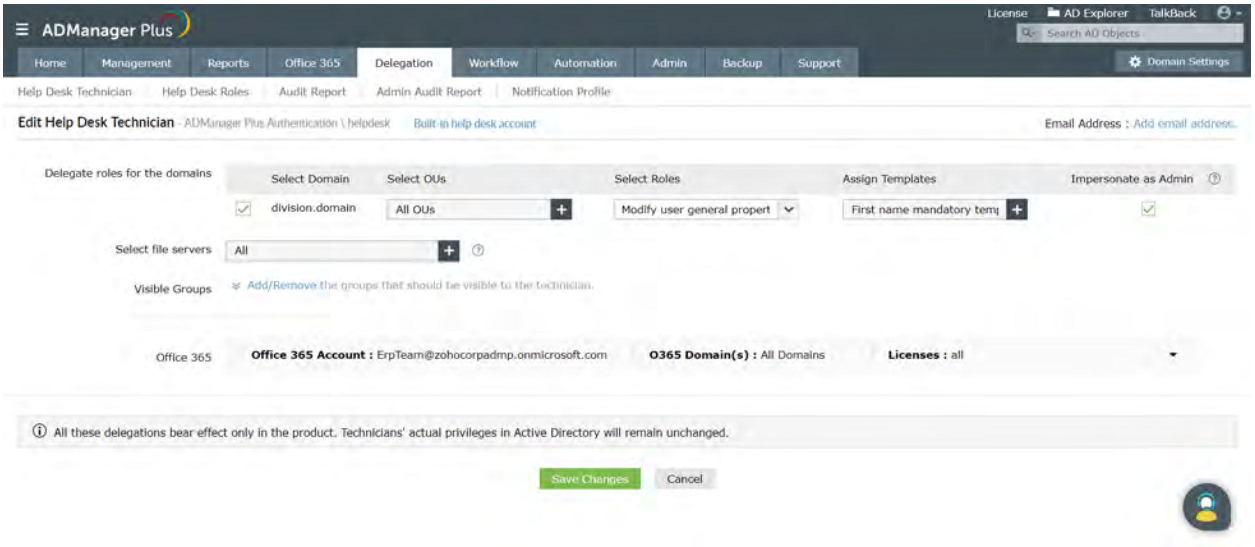
Appearance

Help Card

10. Click on **Save Template** to save the 'First Name Mandatory' template.

11. Similarly, create another template with: 'Employee Id Mandatory', **Terminal Services** and **Custom Attributes** tabs hidden; all attributes except **Outlook Web-access**, **mobile-access** and protocol related attributes in the **Exchange Tab** have to be hidden.
12. Create a new **User Modification Role** in **Delegation**. (Refer ‘Create new Help Desk Role’ exercise in ‘Non-invasive Active Directory Delegation’ section for steps to create a new role.)

13. Create Help Desk Technician 1 or select this technician from the available help desk technicians. (For steps to a new technician, refer ‘Create new Help Desk Technician’ exercise in ‘Non-invasive Active Directory Delegation’ section)
14. To assign 'First Name Mandatory' template to technician 1:
    a. Click on **Delegation** and select the **Help Desk Technicians** option under the **Help Desk Delegation section**.
    b. Select the **technician 1** from the list of technicians and click on **Edit** icon in the **Action** column of the required technician.
    c. Click on the edit option under **Assign Templates**.
    d. In the **Select Template** window, click on **User Modification Templates** and select the ‘First Name Mandatory’ template. (Click on the icon beside the name of the templates to make it a default template.)
    e. **Save Changes** to complete this process.
    f. Similarly, assign the ‘Employee Id Mandatory’ template to technician 2.



Edit Help Desk Technician - ADManager Plus Authentication \ helpdesk Built-in help desk account

Email Address : Add email address.

Delegate roles for the domains

	Select Domain	Select OUs	Select Roles	Assign Templates	Impersonate as Admin
☑	division.domain	All OUs	Modify user general propert	First name mandatory temp	☑

Select file servers: All

Visible Groups: Add/Remove the groups that should be visible to the technician.

Office 365: **Office 365 Account :** ErpTeam@zohocorpadmp.onmicrosoft.com **O365 Domain(s) :** All Domains **Licenses :** all

All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

15. ‘Helpdesk technician 1’ can login and use ‘First Name Mandatory’ template to modify user accounts with satisfying all the specified conditions.
16. Similarly, ‘helpdesk technician 2’ can modify user accounts using the ‘Employee Id Mandatory’ template to modify user accounts in exactly the way required.

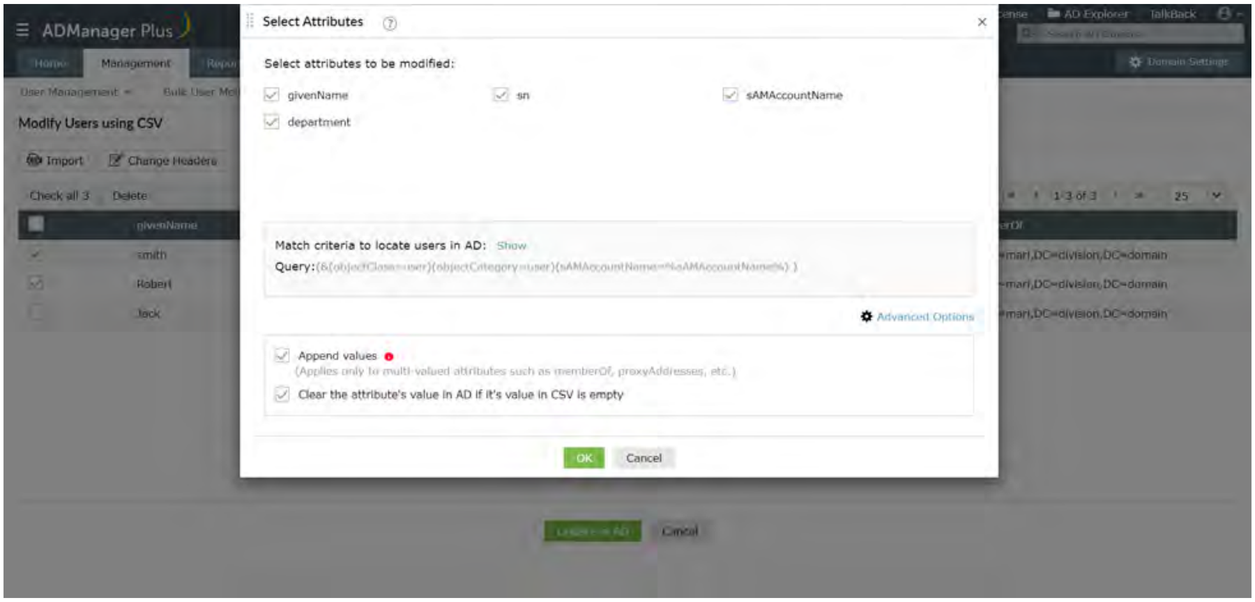
Exercise 11: Flexible CSV based User Modification

Objective: To append and/or remove values for existing users.

ADManager Plus allows you to either replace/clear the existing values or append them by using Flexible CSV based modification feature.

Steps:

1. Navigate to the **Management** tab and select the **Modify bulk users** option, under **UserManagement**.
2. **Import** a **CSV file** with the appropriate LDAP headers.
3. Click on **Update in AD**. The **Select Attributes** window will pop-up that displays all the LDAP Attributes provided in your CSV in which you can select the attributes that you wish to modify.
4. Click the **Show** link to specify the criteria to locate the desired user accounts in AD.
5. Click on the **Advanced** option to perform the following:
    i. If you select the **Append values** option, you can append the values imported from the CSV file to the existing values of an attribute in AD. When this option is not selected, the existing values in AD will be replaced with the ones imported from the CSV file. This option is applicable only to the multivalued attributes.
    ii. If you select the **Clear attribute value in AD if its value in CSV is empty** option, then the existing value of that AD attribute will be cleared if the CSV file does not contain any value for it. If this option is not selected, the existing AD value will remain untouched if the CSV file does not contain any value for it.
6. Click **OK** to update the values in AD.



Select Attributes

Select attributes to be modified:

☑ givenName ☑ sn ☑ sAMAccountName

☑ department

Match criteria to locate users in AD: Show

Query:(&(objectClass=user)(objectCategory=user)(sAMAccountName=%sAMAccountName%))

☑ Append values
(Applies only to multi-valued attributes such as memberOf, proxyAddresses, etc.)

☑ Clear the attribute's value in AD if it's value in CSV is empty

Exercise 12: Modify user accounts using ‘modification templates’ and ‘modification rules’ to auto-update critical user attributes.

Scenario: A senior sales executive of a company is being transferred to its sales office in Houston and is also being promoted to an assistant manager. As his ‘Title’ and ‘City’ are updated with new values, his ‘Manager and ‘State/Province’ attributes have to be updated automatically based on the change.

To accomplish this:

I. Create a new ‘User Modification Template’ which will

- Allow a technician to update the ‘City and ‘Title’ attributes with new values.
- Automatically update the ‘Manager’ and ‘State’ attributes of the user account based on the new values in ‘Title’ and ‘City.
- Hide all attributes, except the ones in the ‘General’ and ‘Contact’ tabs, from the help desk technician who will be using this template to modify the user account.

II. Assign this template to the appropriate help desk technician who has the permission to modify user accounts.

III. The technician has to apply this template for modifying the user accounts.

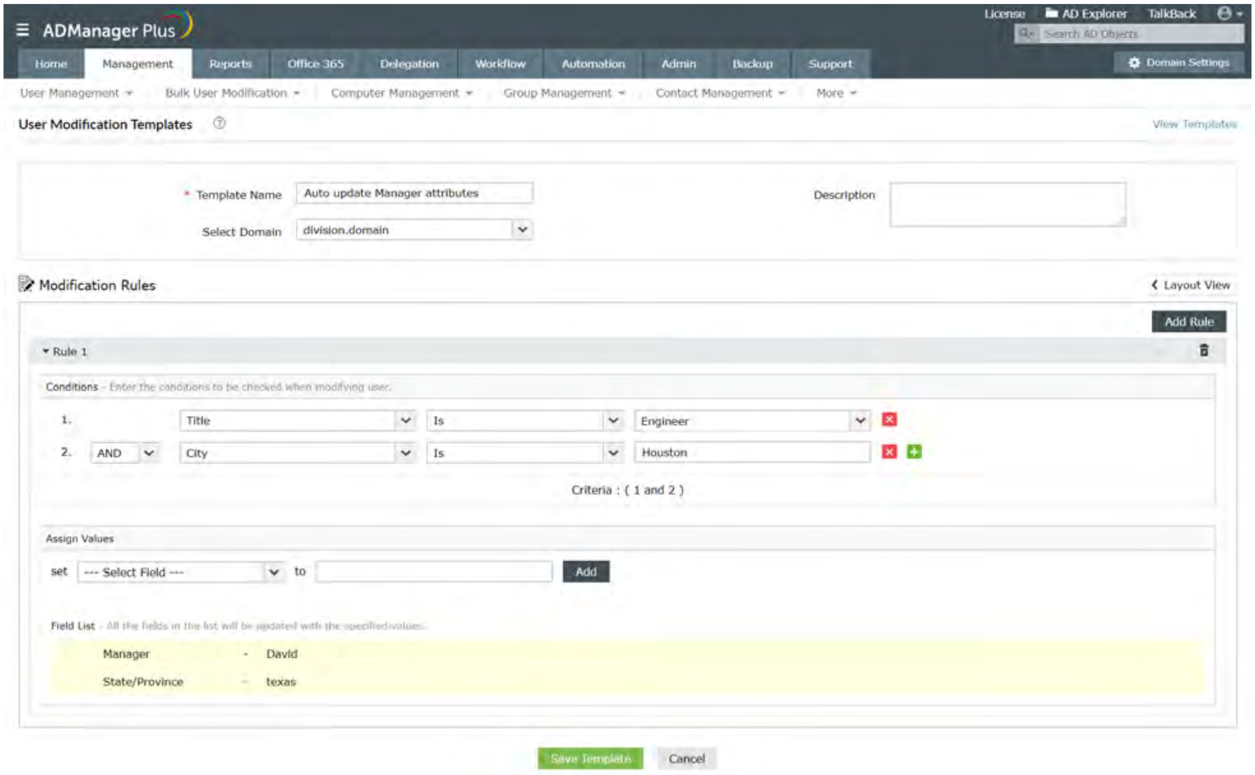
Steps:

I. Create a customized User Modification Template with Modification Rules

1. Navigate to the **Management** tab and click on **User Modification Templates** under the **User Management** section and click **Create New Template.**
2. Specify a name and suitable description for this template. For this illustration, let us name this template as *Auto-update Manager Attribute*.
3. Select the **Domain** of your choice.
4. Create a rule to assign values to the Manager, State/Province attributes as per the values

in Title and Department fields.

a. Click on the **Modification Rules** and then click on **Create New Rule**.
b. Provide a suitable name for the new rule by clicking on **Rule 1**. In this case, let us name this rule as **Manager Update**.
c. In **Conditions** pane, click on **Add Conditions.**
d. In the **Select field** option, click on **Title**. Select **Is** as the condition.
e. In the value box, enter the required title – for this exercise, enter 'Assistant Manager' and click on '+' to add a new condition.
f. In the second condition, select **AND** as the criteria, and **City** in the **Select field** option.
g. Select **Is** in the condition and specify the city as ‘Houston’. Similarly, add **Department** is ‘Sales’ in the condition.
h. In the **Assign Values** section, in the **set** option, select the **Manager** attribute, and in **to** option, specify the name of the manager. For this illustration we will use 'David Smith' as manager and click on **Add**. In the next **set** option, select the **State/Province** attribute and specify the value as 'Texas'.
i. Repeat steps: a to h to add as many rules as needed to check for all possible 'Title', 'City' combinations and specify the corresponding 'Manager', 'State/Province' values.



User Modification Templates

* Template Name: Auto update Manager attributes

Select Domain: division.domain

Description:

Modification Rules

Rule 1

Conditions - Enter the conditions to be checked when modifying user.

1. Title | Is | Engineer
2. AND | City | Is | Houston

Criteria : (1 and 2)

Assign Values

set --- Select Field --- to

Field List - All the fields in the list will be updated with the specified values.

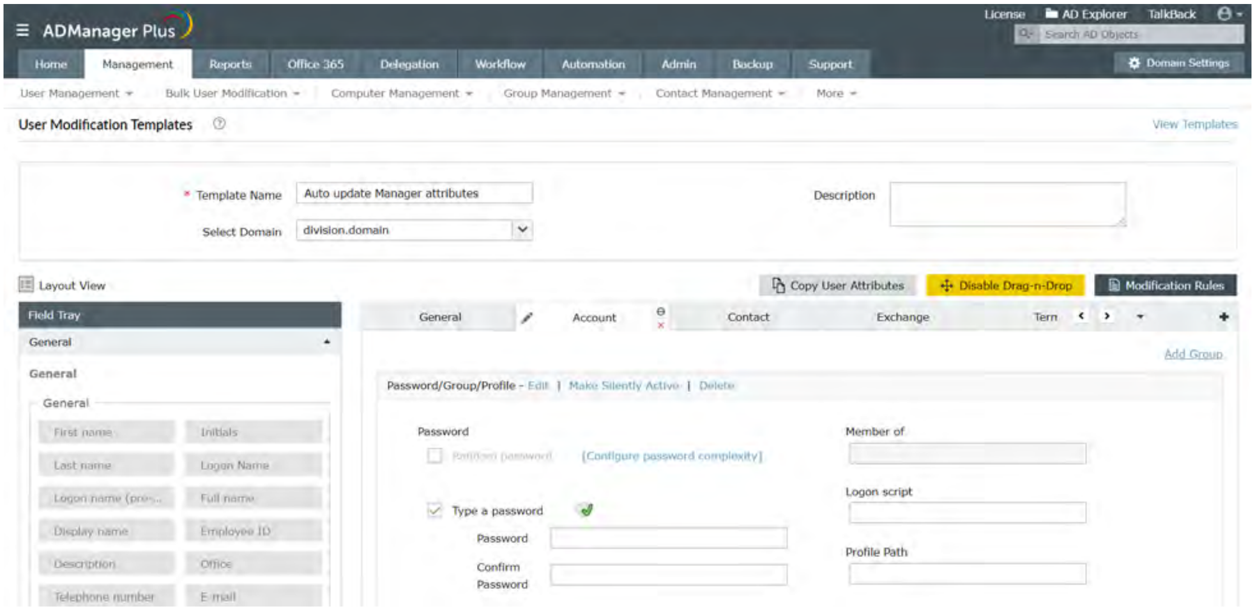
Manager	-	David
State/Province	-	texas

5. Hide all tabs except **General** and **Contact** tabs:

a. Click on the **Layout View** located at the top left corner. Click on **Enable Drag-n-Drop** option.

b. Now click on the **Account** tab and click on the minimization icon located at the right corner of the tab. This will make the **Account** tab silently active, that is, the entire tab and all the attributes in the tab will be hidden from the technician who is using this template for user modification.

c. Similarly, hide all the other tabs: Exchange, Terminal and Custom Attributes. **Note**: To hide a specific attribute in a particular tab, just place your mouse over the edit icon that appears when you hover over that attribute and select **Make Silently Active** option.



* Template Name: Auto update Manager attributes

Select Domain: division.domain

Description:

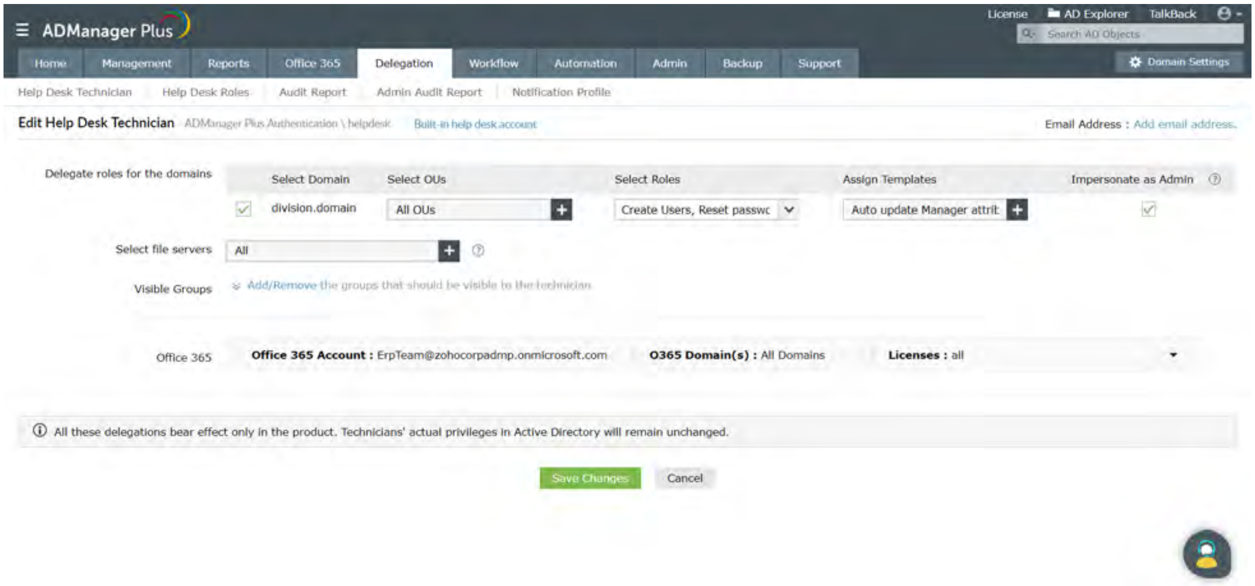
□ Random password

☑ Type a password

6. Click on **Save Template** to create and save this template.

II. Assign this template to the required help desk technicians:

1. Click on the **Delegation tab** and click on **Help Desk Technicians** option under the **Help Desk Delegation**.
2. Select any technician from the list of technicians (or create a new technician using the steps mentioned in 'Non-invasive Active Directory Delegation', section 9 of this workbook)
3. Click on the **Edit** icon located beside the name of the technician.
4. Choose **User modification** under roles. In case you haven't created one already, create a new **User Modification Role** in **Delegation**. (Refer 'Create new Help Desk Role' exercise in 'Non-invasive Active Directory Delegation' section for steps to create a new role.)
5. Under the **Assign Templates** section, click on **Add/Edit Templates**.
6. In the **Select Template** window, choose the required domain.
7. Click on **User Modification Templates** and select the template that we just created- which is Auto-update manager attribute template in this case. (Click on the icon beside the name of the templates to make it a default template.)
8. Save the changes to complete this process.



Edit Help Desk Technician ADManager Plus Authentication \ helpdesk Built-in help desk account

Email Address : Add email address.

Delegate roles for the domains

	Select Domain	Select OUs	Select Roles	Assign Templates	Impersonate as Admin
☑	division.domain	All OUs	Create Users, Reset passwc	Auto update Manager attrit	☑

Select file servers: All

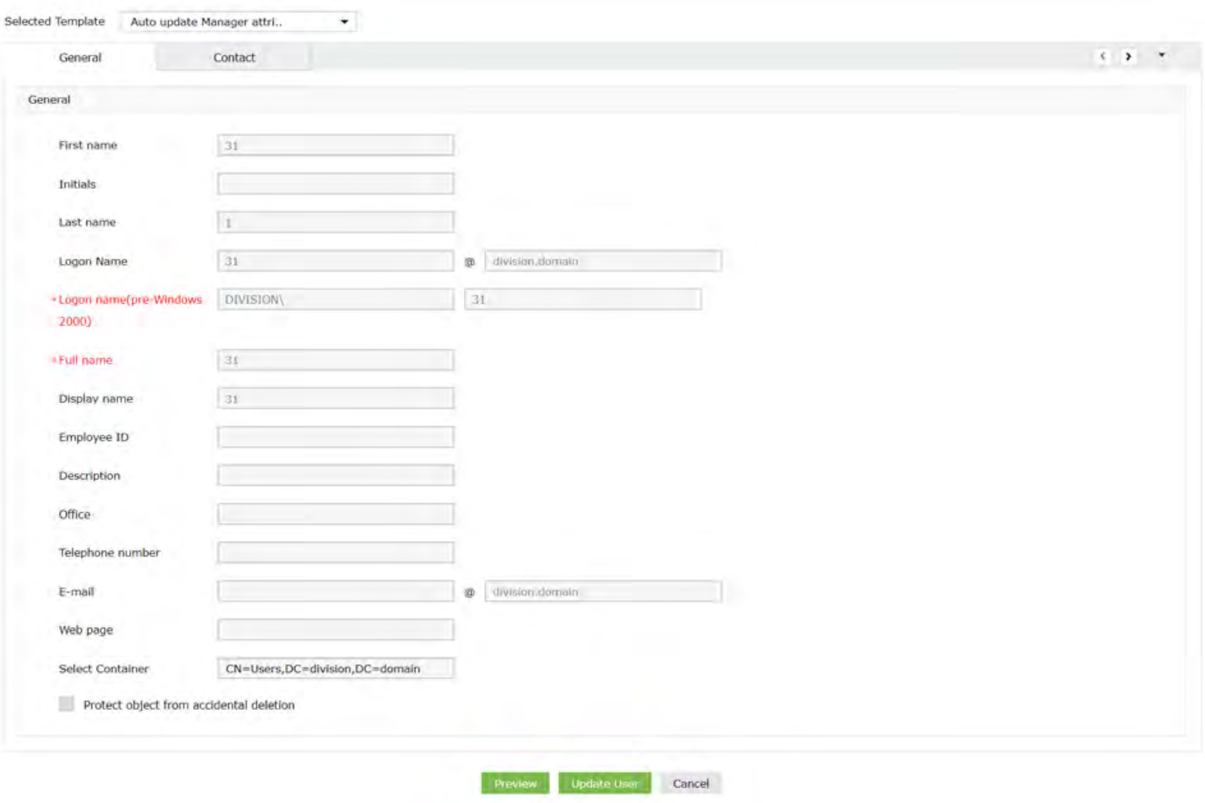
Visible Groups: Add/Remove the groups that should be visible to the technician

Office 365: **Office 365 Account :** ErpTeam@zohocorpadmp.onmicrosoft.com **O365 Domain(s) :** All Domains **Licenses :** all

All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

III. Modify user accounts through user modification templates:

1. Login to ADManager Plus using the credentials of the help desk technician.
2. Under the **Management** tab, select the **Modify Single User** option.
3. Select the **Domain** in which the user account that is to be modified is located.
4. Key in the user's name in the search box and click on **Go** to fetch the required user.
5. Click on the **Modify User** button located in the **Action** column of the user.
6. In the **Modify User Properties** window that pops up, select the required template by clicking on the **Change** link located beside the **Selected Template** list box. In this case, select **Auto-update Manager Attribute** template (template that you just created).
7. Once you select Auto-update Manager Attribute template, you will be able to view only the **General** and **Contact** tabs as this template hides all other tabs and properties.
8. Click on **Contact** tab since the **Title** and the **City** tabs are located in that tab.
9. Enter the new values for both these attributes. In this case Title= Assistant Manager, City=Houston.



Selected Template: Auto update Manager attri..

General

First name	31		
Initials			
Last name	1		
Logon Name	31	@	division.domain
*Logon name(pre-Windows 2000)	DIVISION\		31
*Full name	31		
Display name	31		
Employee ID			
Description			
Office			
Telephone number			
E-mail		@	division.domain
Web page			
Select Container	CN=Users,DC=division,DC=domain		

□ Protect object from accidental deletion

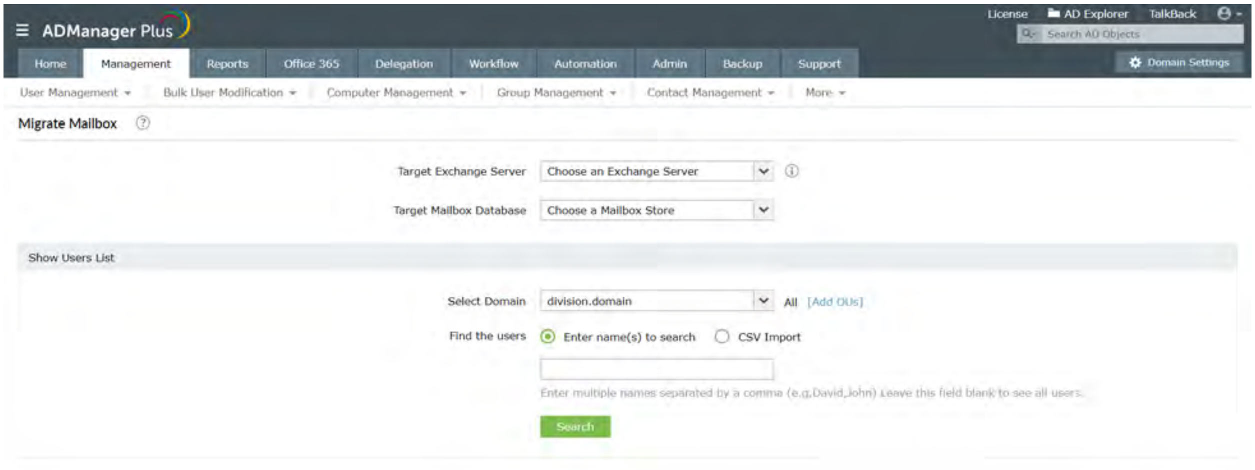
10. To view all the attributes that you have modified, click on **Preview**. This will list all the attributes along with their modified values.
11. Use the **Back** option at the top right corner of the preview window to go back to the template and update any other attribute(s) that you might have missed.
12. To save the changes that you made, click on **Update User**.
13. While saving the changes, in addition to the attributes that you have modified manually, the attributes specified in the **modification rules** will also be updated automatically.

Exercise 13: Migrating Exchange Mailboxes.

Objective: To migrate Exchange mailboxes from one environment to another.

ADManager Plus allows you to move a mailbox from one server to a mailbox store on another server without any hassle.
Following are the steps for mailbox migration:

1. Login to ADManager Plus and navigate to the **Management** tab.
2. Under the **Exchange Mailbox Tasks** section, click on the **Migrate Mailbox** option.
3. Select the **Target Mailbox Server** and **Target Mailbox Database**.
4. Select the required **Domain/OU** and specify the list of users either using a CSV file or by locating them using the **Search** option.
5. Click **Apply** for the changes to take place.



Migrate Mailbox

Target Exchange Server: Choose an Exchange Server

Target Mailbox Database: Choose a Mailbox Store

Show Users List

Select Domain: division.domain All [Add OUs]

Find the users: ● Enter name(s) to search ○ CSV Import

Enter multiple names separated by a comma (e.g.David,John) Leave this field blank to see all users.

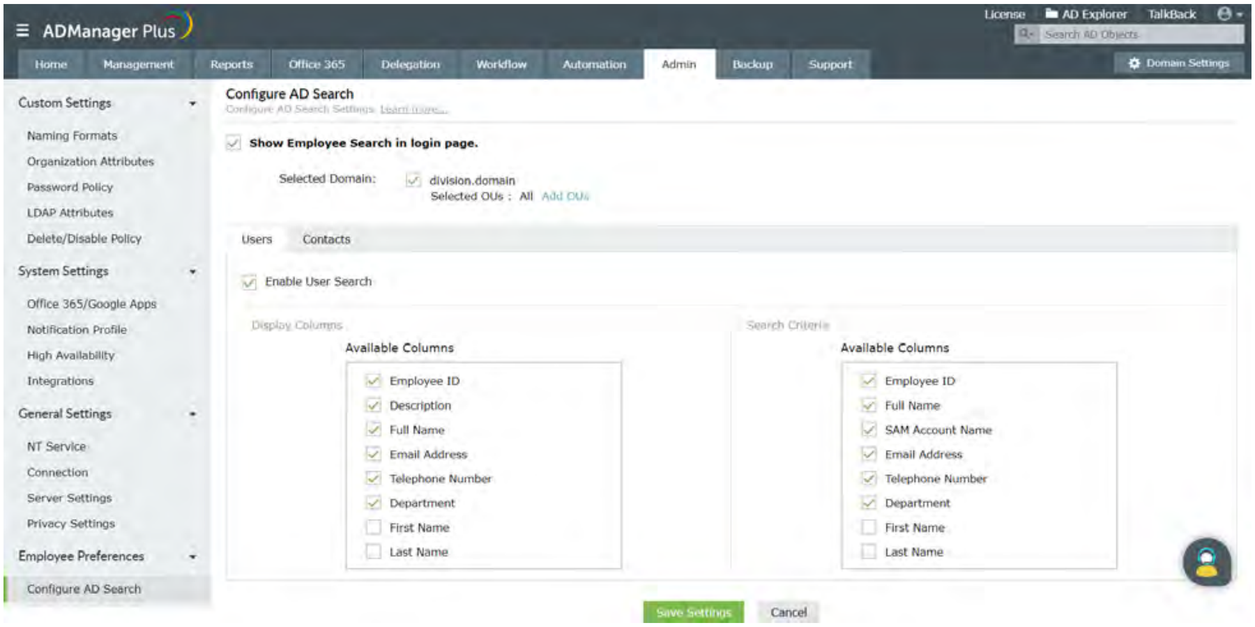
Exercise 14: Performing a secure directory/ Address Book wide search for Domain users

Objective: To enable the 'Search User' option through the browser.

ADManager Plus, being a web-based solution, can be accessed from anywhere. This solution also allows users to search and get their co-workers' details without logging into the console.

Steps to be followed for configuring AD search using ADManager Plus:

1. Login to ADManager Plus and click on the **Admin** tab.
2. Click on **Configure AD Search** under Employee Preferences.
3. Enable the **Show Employee Search in Login Page** option
4. Select the **Domain(s)** and **OUs** of your choice.
5. Select the **columns** that are to be displayed while searching for a user/contact account.
6. Select the **criteria** for the search.
7. Click on **Save Settings**.



Configure AD Search

Configure AD Search Settings. Learn more...

☑ Show Employee Search in login page.

Selected Domain: ☑ division.domain

Selected OUs : All Add OUs

☑ Enable User Search

Display Columns

Available Columns

☑ Employee ID
☑ Description
☑ Full Name
☑ Email Address
☑ Telephone Number
☑ Department
□ First Name
□ Last Name

Search Criteria

Available Columns

☑ Employee ID
☑ Full Name
☑ SAM Account Name
☑ Email Address
☑ Telephone Number
☑ Department
□ First Name
□ Last Name

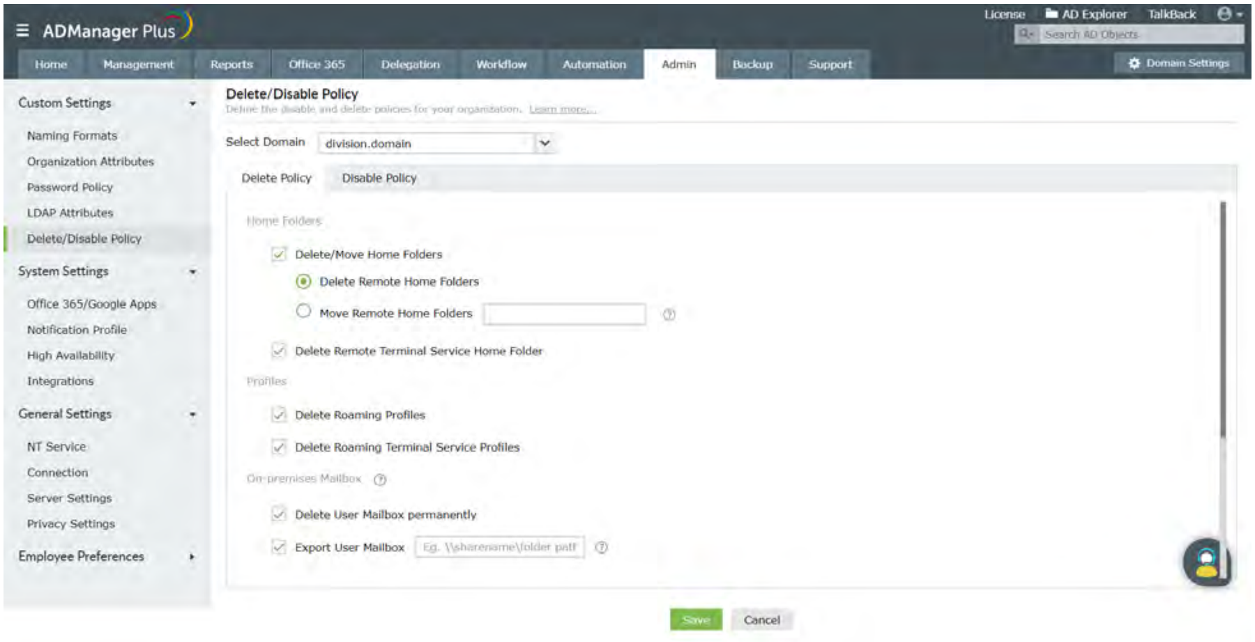
3.2 AD object deletion (de-provisioning)

De-provisioning is a crucial task that you have to perform repeatedly for different AD objects. Doing this task for every object one after the other is another one of those taxing tasks in Active Directoy that every administrator has to put up with, only till now. ADManager Plus now simplifies this tedious task so much that you will wish you had ADManager Plus from day one.

Exercise 1: De-provision a specific set of users along with their home folders and profiles

Following are the steps required for de-provisioning a set of AD users along with their home folders and profiles.

1. Login to ADManager Plus and navigate to the **Admin** tab.
2. Under the Delete/Disable policy,
    i. Select the **Domain** of your choice.
    ii. Click on the **Delete/Disable Policy** section, under the **Custom Settings** tab and select the **Home folders**, **Profiles**, **Mailboxes and Other accounts**, **Office 365/ G Suite** options if you want to delete them whenever the associated user account is deleted.
    iii. You can also associate a custom script to be run whenever a user account is deleted.
    iv. **Save** the changes.



Delete/Disable Policy

Define the disable and delete policies for your organization. Learn more...

Select Domain: division.domain

Delete Policy | Disable Policy

Home Folders

☑ Delete/Move Home Folders

● Delete Remote Home Folders

○ Move Remote Home Folders

☑ Delete Remote Terminal Service Home Folder

Profiles

☑ Delete Roaming Profiles

☑ Delete Roaming Terminal Service Profiles

On-premises Mailbox

☑ Delete User Mailbox permanently

☑ Export User Mailbox: Eg. \\sharename\folder path

3. Navigate to the **Management** tab. Under **User Management,** select the **Delete users** option in the **Bulk user modification** section.
4. Select the required **Domain/OU** and specify the list of users either using a CSV file or by locating them using the **Search** option.
5. Click **Apply** for the changes to take place. Since the home folders and profiles are selected in the delete policy, they will also be deleted while deleting the users.

Exercise 2: Identify and manage users with duplicate attributes

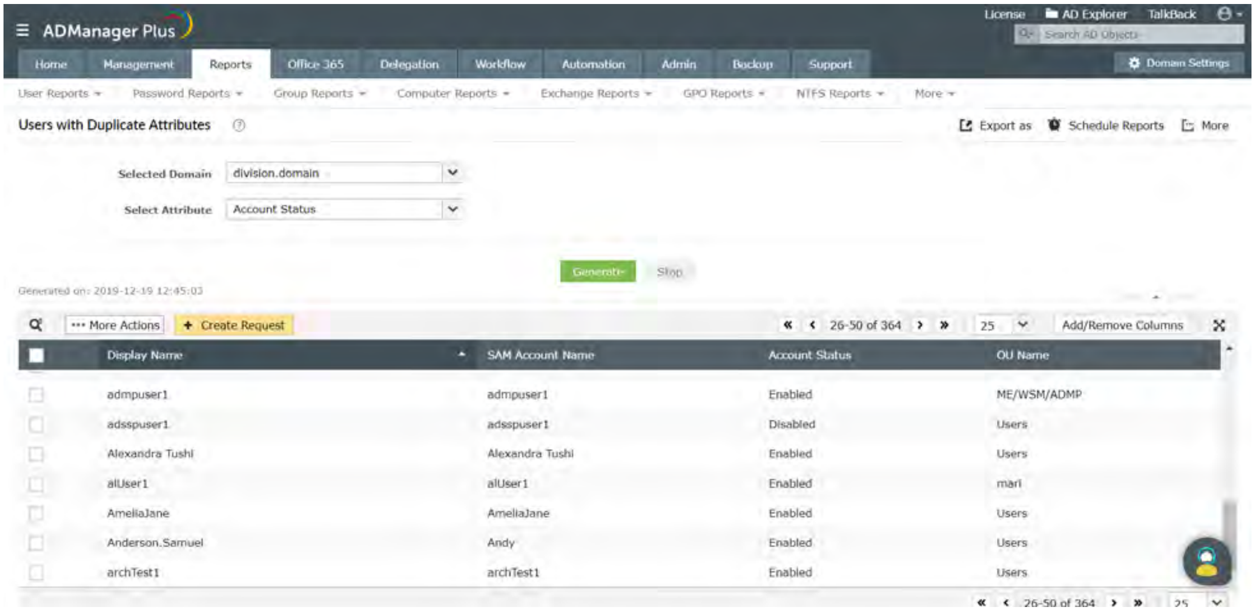
Objective: To find users in AD who have duplicate values for certain attributes, and modify those attributes.

In the native AD environment, a similar objective could be achieved by performing an attribute specific search for a particular value. To identify duplicate entries, this procedure has to be repeated for every known value, which is a lengthy process.
However, this objective can easily be achieved by using the 'Users with duplicate attributes' built-in report of ADManager Plus.

Following are the steps to be followed for accomplishing the given objective using ADManager Plus:

1. Login to ADManager Plus and navigate to the **Reports** tab.
2. Under the **General Reports** section of **User Reports**, click the **Users with duplicate attributes** report.
3. Select the **Domain** of your choice.
4. Click on the **Select Attribute** field to choose the attributes whose values might be duplicated.

5. Click on **Generate**
6. You can modify the fields of the report by using the **Add/Remove columns** option.
7. Select the users of this report whose attributes you want to modify and click on the **more actions** button to select the action that you wish to perform on these users and click on **Go**.
8. Configure the properties required for the action to be performed.
9. Click on **Apply** for the changes to take effect.



Users with Duplicate Attributes

Selected Domain: division.domain

Select Attribute: Account Status

Generated on: 2019-12-19 12:45:03

Display Name	SAM Account Name	Account Status	OU Name
admpuser1	admpuser1	Enabled	ME/WSM/ADMP
adsspuser1	adsspuser1	Disabled	Users
Alexandra Tushi	Alexandra Tushi	Enabled	Users
alUser1	alUser1	Enabled	mari
AmeliaJane	AmeliaJane	Enabled	Users
Anderson.Samuel	Andy	Enabled	Users
archTest1	archTest1	Enabled	Users

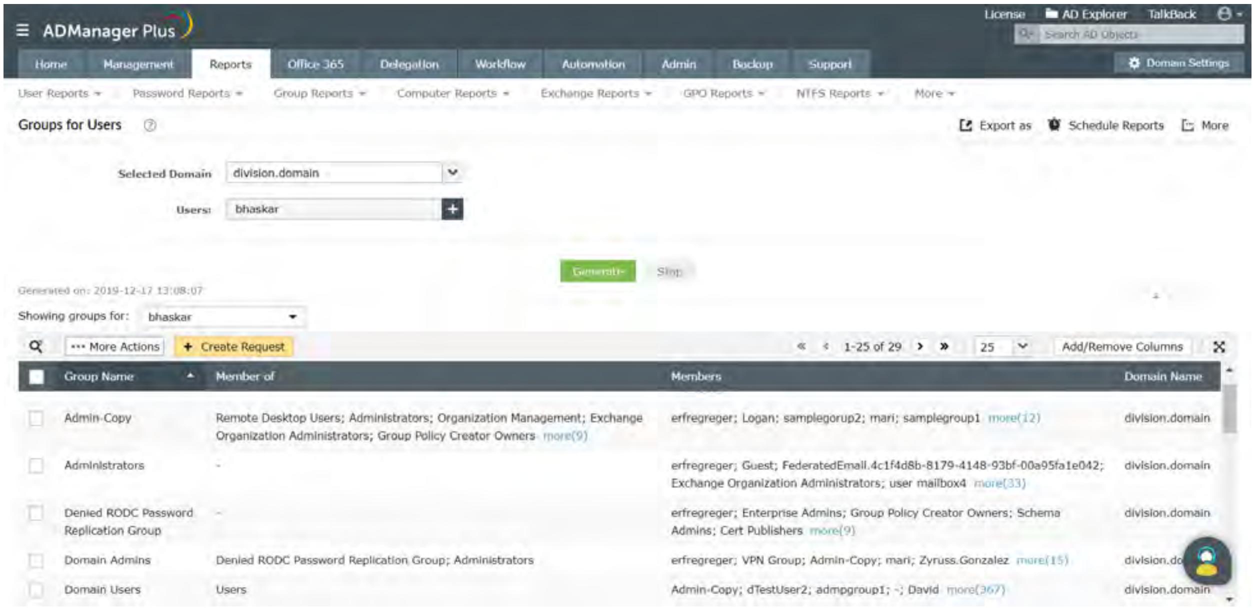
Exercise 3: Delete a group if a specific user is not a member of that group.

Objective: Search for a user in a specified group, and delete the group if the user is not a member of that group.

To perform the above actions using the native AD interface, you have to:
- Launch the ADUC
- Locate the user using the find option
- Check the value of the memberOf field in the properties of that user
- Search for that group using the find option
- Delete that group

ADManager Plus simplifies this procedure by breaking this down into the following steps:

1. Login to ADManager Plus and click on the **Reports** tab.
2. Click on the **Groups for Users** report under the **Nested Reports** section of **User Reports**.
3. Select the **Domain** and the **User** of your choice.
4. Click on **Generate**



Groups for Users

Selected Domain: division.domain

Users: bhaskar

Generated on: 2019-12-17 13:08:07

Showing groups for: bhaskar

Group Name	Member of	Members	Domain Name
Admin-Copy	Remote Desktop Users; Administrators; Organization Management; Exchange Organization Administrators; Group Policy Creator Owners more(9)	erfregreger; Logan; samplegorup2; mari; samplegroup1 more(12)	division.domain
Administrators	-	erfregreger; Guest; FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042; Exchange Organization Administrators; user mailbox4 more(33)	division.domain
Denied RODC Password Replication Group	-	erfregreger; Enterprise Admins; Group Policy Creator Owners; Schema Admins; Cert Publishers more(9)	division.domain
Domain Admins	Denied RODC Password Replication Group; Administrators	erfregreger; VPN Group; Admin-Copy; mari; Zyruss.Gonzalez more(15)	division.do
Domain Users	Users	Admin-Copy; dTestUser2; admpgroup1; -; David more(367)	division.domain

5. Search for the group using the **Quick Search** option.
6. If the group is not present in the list of groups, proceed to delete the group:
    i. Click on the **Management** tab and click on the **Group Management** option.
    ii. Select the **Delete Groups** action under the **Bulk Group Modification** section.
    iii. Select the required **Domain** and specify the list of groups either using a CSV file or by locating them using the **Search** option.
    iv. Click **Apply** for the changes to take place.

4. Active Directory Reporting and On-the-fly Management

With numerous IT standards to be followed, generating reports on Active Directory tasks and activities to comply with the standards have become imperative for upholding the credibility and accreditations of any organization. It is also crucial to keep track of all that is happening within the Active Directory via Audit reports. However, the native AD tools by no means provides an easy method for generating these vital reports. Administrators have to resort to complex scripts for Active Directory reporting.

ADManager Plus, on the other hand, simplifies Active Directory reporting. With its simple, UI-based, 180+ readymade reports for every need and purpose, you will find that Active Directory reporting is something that is no longer a hard and tedious task.

The reports generated using ADManager Plus are actionable reports, i.e., you can perform important management actions from within these reports. For instance, you can generate a list of users whose passwords have expired and reset the passwords of those users, directly from the report.

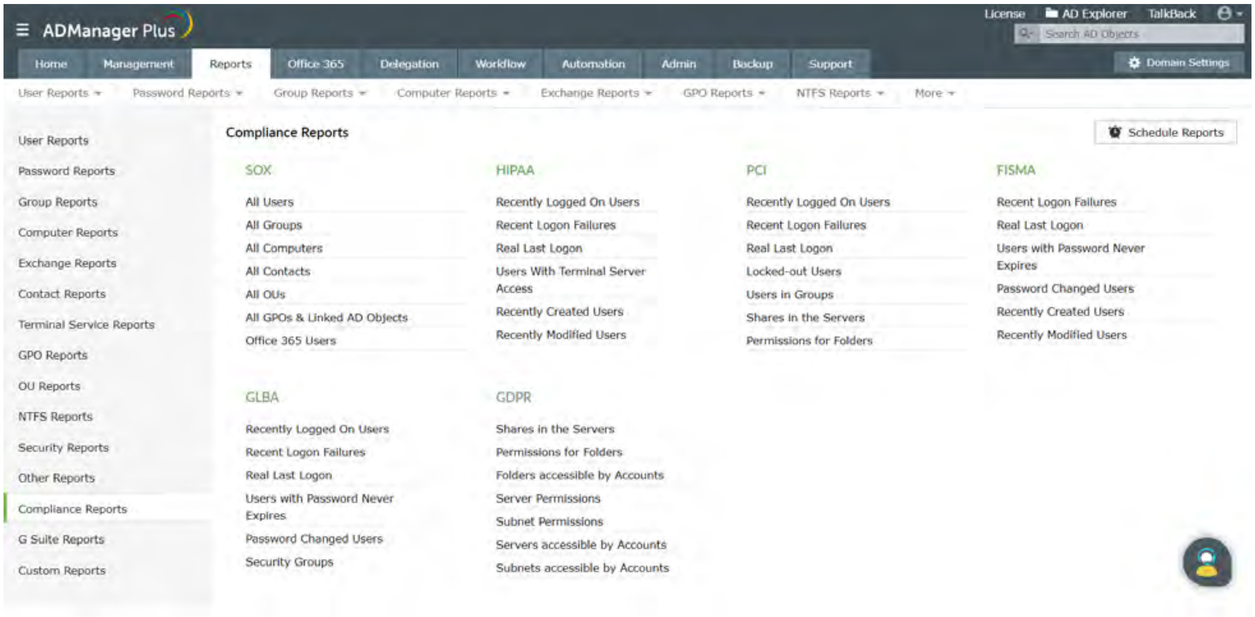
4.1 Active Directory Reporting

Exercise 1: IT compliance reports

Objective: Run reports that are specifically needed for proving compliance with IT standards such as SOX, PCI, HIPAA, GDPR and more.

Following are the steps that have to be performed to accomplish the above-mentioned objective:

1. Click on the **Reports** tab and click on **Compliance Reports**.
2. Select from any of the built-in reports categorized under the SOX, HIPAA, PCI, FISMA, GLBA and GDPR sections.
3. Give the required inputs and **Generate** the report.



User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
Contact Reports
Terminal Service Reports
GPO Reports
OU Reports
NTFS Reports
Security Reports
Other Reports
Compliance Reports
G Suite Reports
Custom Reports

Compliance Reports

SOX
All Users
All Groups
All Computers
All Contacts
All OUs
All GPOs & Linked AD Objects
Office 365 Users

HIPAA
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Users With Terminal Server Access
Recently Created Users
Recently Modified Users

PCI
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Locked-out Users
Users in Groups
Shares in the Servers
Permissions for Folders

FISMA
Recent Logon Failures
Real Last Logon
Users with Password Never Expires
Password Changed Users
Recently Created Users
Recently Modified Users

GLBA
Recently Logged On Users
Recent Logon Failures
Real Last Logon
Users with Password Never Expires
Password Changed Users
Security Groups

GDPR
Shares in the Servers
Permissions for Folders
Folders accessible by Accounts
Server Permissions
Subnet Permissions
Servers accessible by Accounts
Subnets accessible by Accounts

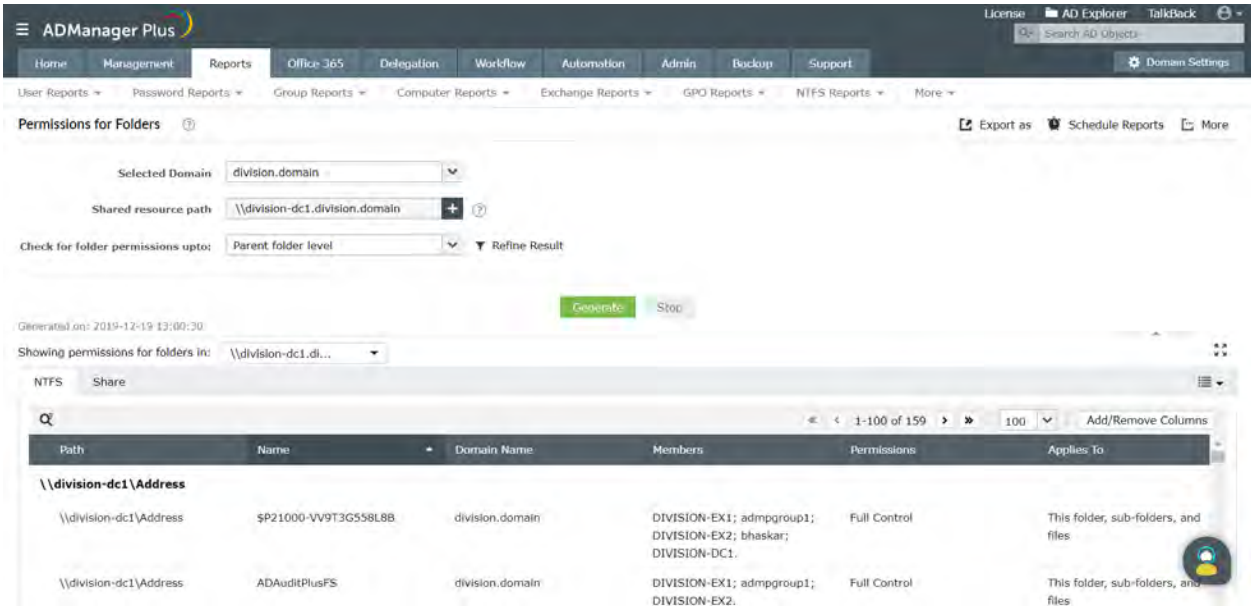
Exercise 2: Share Permissions report

Objective: List down all the shares in a server and for any desired share, find out who's having what permission on the shares.

To accomplish the above, using the native AD interface, you will have to:
- Locate the desired server
- Find out all the shares in that server
- Locate the required share from the listed shares
- Find the users that have all the permissions for that share
- Identify the exact permissions that the users have on that share

ADManager Plus helps you simplify the above operations using the following steps:

1. Click on**Reports** and go to **NTFS Reports**.
2. Click on **Permissions for Folders** report.
3. Select the **Domain** of your choice.
4. Select the **Server** for which you would like to list the shares.
5. Select the **share** for which you would like to see the list of users who have permissions on the share.
6. Select the **level** up to which you would like to generate this report, i.e., parent level or sub folder level or the number of levels of sub-folders. Using the **Refine Result** option you can choose to exclude folders in the search results.
7. **Generate** the report.
8. You can search for any particular user, to see its permissions, using the **Quick Search** option.



Permissions for Folders

Selected Domain: division.domain

Shared resource path: \\division-dc1.division.domain

Check for folder permissions upto: Parent folder level

Generated on: 2019-12-19 13:00:30

Showing permissions for folders in: \\division-dc1.di...

1-100 of 159 | 100

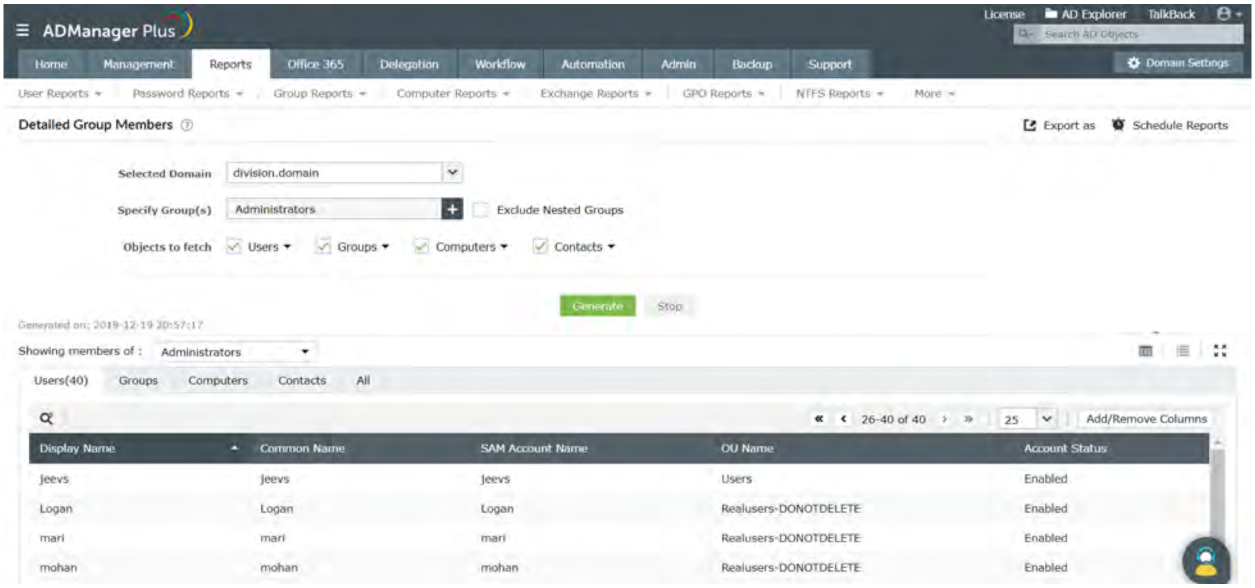
Path	Name	Domain Name	Members	Permissions	Applies To
\\division-dc1\Address					
\\division-dc1\Address	$P21000-VV9T3G558L8B	division.domain	DIVISION-EX1; admpgroup1; DIVISION-EX2; bhaskar; DIVISION-DC1.	Full Control	This folder, sub-folders, and files
\\division-dc1\Address	ADAuditPlusFS	division.domain	DIVISION-EX1; admpgroup1; DIVISION-EX2.	Full Control	This folder, sub-folders, and files

Exercise 3: List all the members of a group

Objective: Generate a report that lists all the members of a specific group.

Following are the steps that have to be followed for accomplishing the given objective:

1. Click on **Reports**.
2. Click on **Group Reports** and click on **Detailed Group Members** report.
3. Specify the **Domain** and the **Group(s)** of your choice.
4. Enable the **Exclude Nested Groups** option if you do not want the members of the nested groups to be listed in this report.
5. Specify the objects(users, groups, computers, contacts) that you want to list. You can also further exclude the different types of objects or include only specific objects in the report by clicking on the arrow given next to the object name.
6. **Generate** the report to get detailed group membership of the specified group(s).



Detailed Group Members

Selected Domain: division.domain

Specify Group(s): Administrators

□ Exclude Nested Groups

Objects to fetch: ☑ Users ☑ Groups ☑ Computers ☑ Contacts

Generated on: 2019-12-19 20:57:17

Showing members of : Administrators

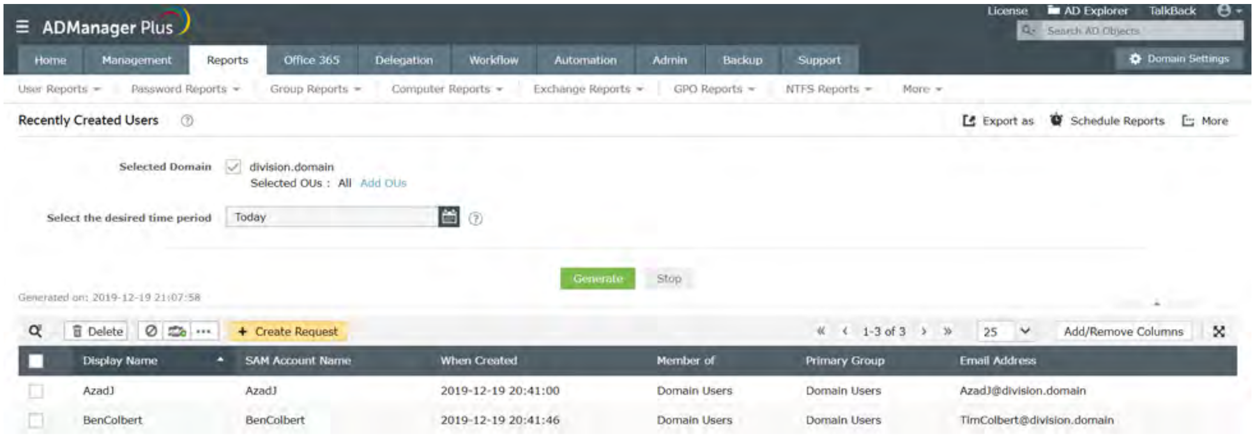
Display Name	Common Name	SAM Account Name	OU Name	Account Status
Jeevs	Jeevs	Jeevs	Users	Enabled
Logan	Logan	Logan	Realusers-DONOTDELETE	Enabled
mari	mari	mari	Realusers-DONOTDELETE	Enabled
mohan	mohan	mohan	Realusers-DONOTDELETE	Enabled

Exercise 4: Automatically send the list of users created in a particular day to a specified person

Objective: Generate a report of all the users who have been created in the day and send it in the required format to the concerned person over email . Also, send this report on a daily basis.

Following are the steps that are to be followed for accomplishing the given objective:

1. Click on the **Reports** tab.
2. Click on the **Recently Created Users** report located under the **General Reports** section of **User Reports**.
3. Select the **Domain** and the **OU(s)** of your choice.
4. Enter **Today** beside the **Select the desired time period** field.
5. Click **Generate** to get a list of all the users created that day.



Recently Created Users

Selected Domain: ☑ division.domain
Selected OUs : All Add OUs

Select the desired time period: Today

Generated on: 2019-12-19 21:07:58

□	Display Name	SAM Account Name	When Created	Member of	Primary Group	Email Address
□	AzadJ	AzadJ	2019-12-19 20:41:00	Domain Users	Domain Users	AzadJ@division.domain
□	BenColbert	BenColbert	2019-12-19 20:41:46	Domain Users	Domain Users	TimColbert@division.domain

6. To schedule this report to be generated and emailed to the concerned person, on a daily-basis:

a. Click on **Schedule Reports**.

b. Click on **Create Schedule**

c. Specify a suitable **Schedule Name**.

d. Select the **Domain** and the **OU(s)** of your choice.

e. Under the **Select Reports** field, click on **User Reports** under the **Report Type** section.

f. In the **Available Reports** section, click on **Recently Created Users**, and enter 1 in the **Enter no. of days** field.

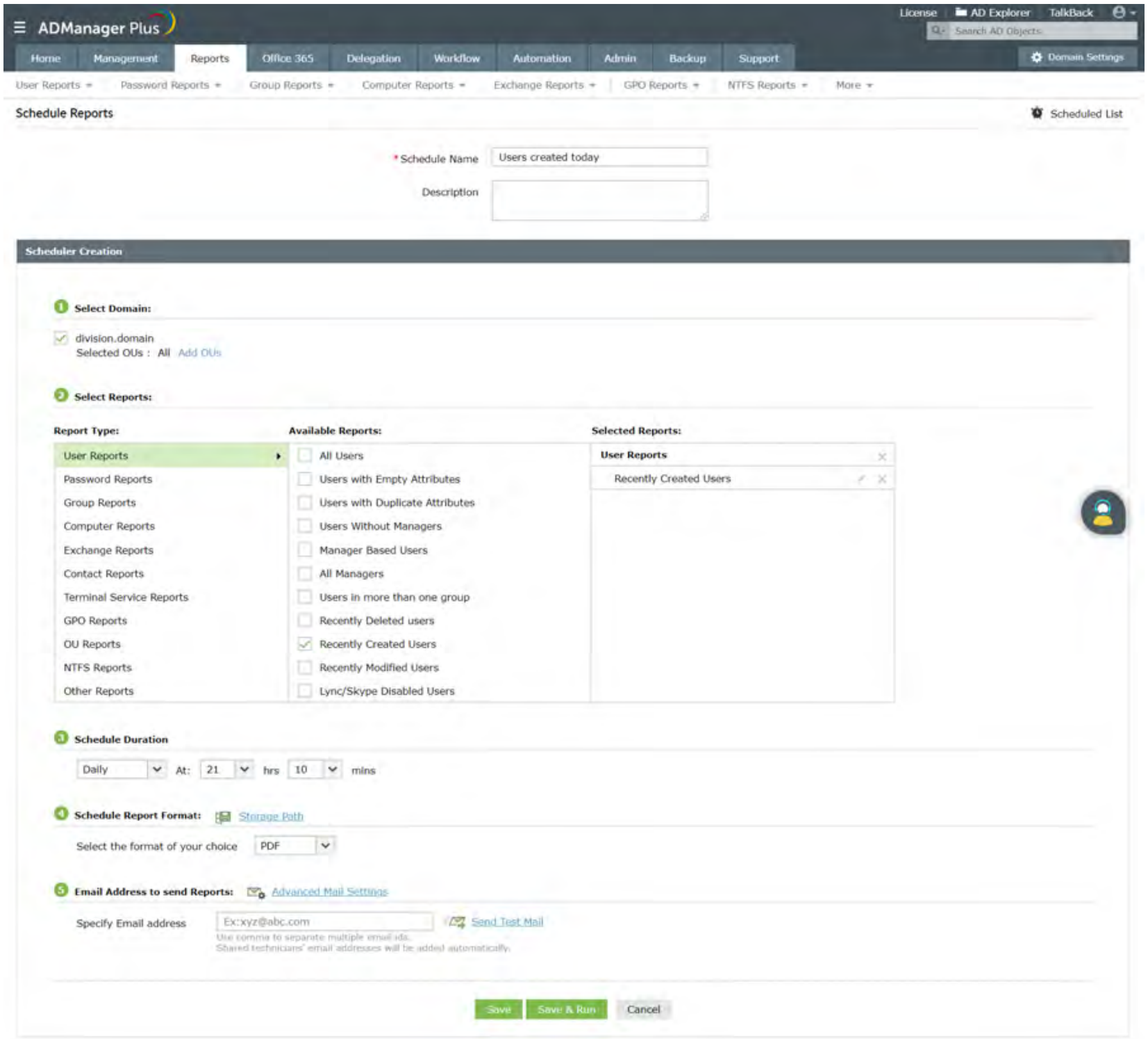
g. Click **OK.**

h. You will now see this report in the **Selected Reports** column.

i. Select **Daily** and mention the time at which the report has to be generated in the options under **Schedule Duration**.

j. Specify the format in **Select the format of your choice**.

k. Enter the email addresses to which the report has to be sent in the **email address to send reports**. More than one email address can be specified if you wish to send this report to more than one person.



Schedule Reports

*Schedule Name: Users created today

Description:

Scheduler Creation

1 Select Domain:

☑ division.domain
Selected OUs : All Add OUs

2 Select Reports:

Report Type:	Available Reports:	Selected Reports:
User Reports	□ All Users	User Reports
Password Reports	□ Users with Empty Attributes	Recently Created Users
Group Reports	□ Users with Duplicate Attributes	
Computer Reports	□ Users Without Managers	
Exchange Reports	□ Manager Based Users	
Contact Reports	□ All Managers	
Terminal Service Reports	□ Users in more than one group	
GPO Reports	□ Recently Deleted users	
OU Reports	☑ Recently Created Users	
NTFS Reports	□ Recently Modified Users	
Other Reports	□ Lync/Skype Disabled Users	

3 Schedule Duration

Daily At: 21 hrs 10 mins

4 Schedule Report Format: Storage Path

Select the format of your choice: PDF

5 Email Address to send Reports: Advanced Mail Settings

Specify Email address: Ex:xyz@abc.com Send Test Mail
Use comma to separate multiple email ids.
Shared technicians' email addresses will be added automatically.

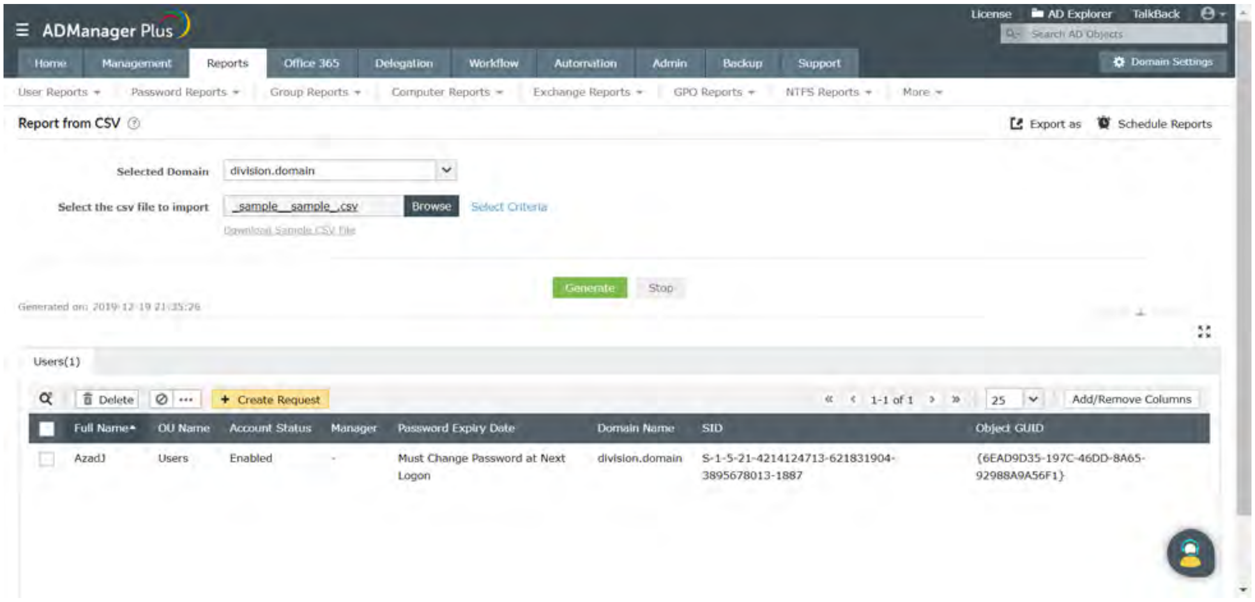
Exercise 5: Generating Reports based on available attributes of users

Objective: To find out users having details with the existing HRMS tool or from data provided by other departments.

When HR norms dictate multiple user modifications it becomes a tedious task for AD admins to perform changes to each user in Active Directory. However, with ADManager Plus, you can use the **Reports from CSV** option to find out the user accounts using common fields like first name and last name and modify them in bulk.

Following are the steps that have to be performed to accomplish the given objective:

1. Go to **User Reports** page in**Reports** tab.
2. Click on **Report from CSV** in the **CSV import** section.
3. Select the **Domain** of your choice
4. Import the CSV file which is provided by the HR team or exported from a different tool or prepared by you.
5. Click **Generate** to get the report.



Report from CSV

Selected Domain: division.domain

Select the csv file to import: _sample__sample_.csv

Generated on: 2019-12-19 21:35:26

Full Name	OU Name	Account Status	Manager	Password Expiry Date	Domain Name	SID	Object GUID
AzadJ	Users	Enabled	-	Must Change Password at Next Logon	division.domain	S-1-5-21-4214124713-621831904-3895678013-1887	{6EAD9D35-197C-46DD-8A65-92988A9A56F1}

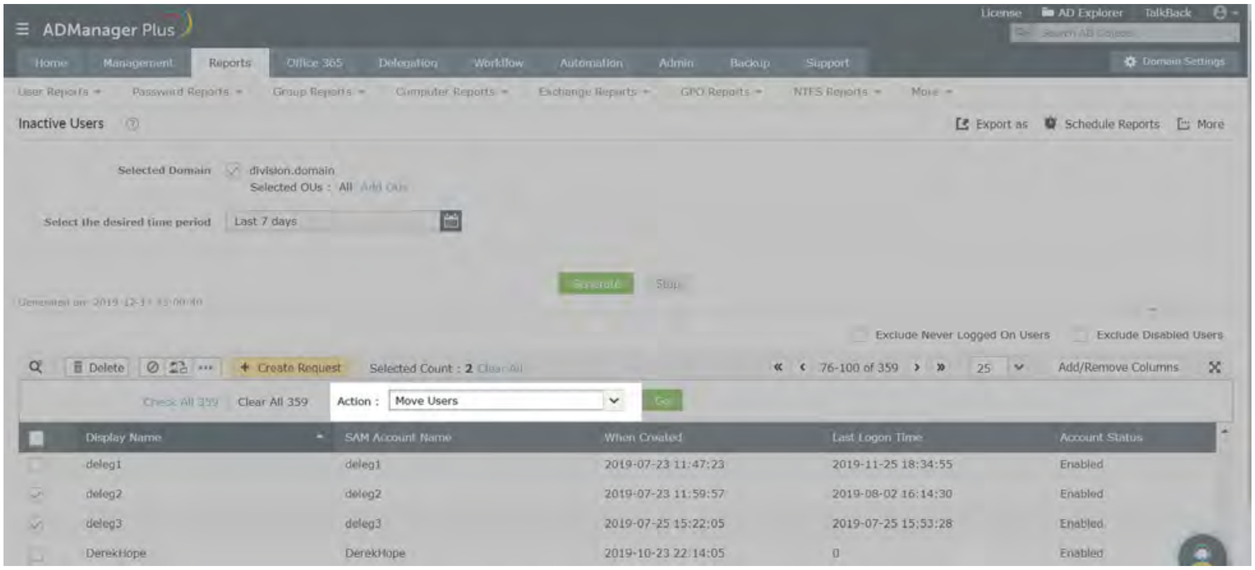
4.2 Management from AD reports

Exercise 1: Find the inactive users and move them to a different OU

Objective: Obtain a list of all the Active Directory users that have been inactive for a specific period of time.

Following are the steps that are to be followed for accomplishing the above-mentioned objective:

1. Login to ADManager Plus and click on the **Reports** tab.
2. Under the **Logon reports** section of **User Reports**, click on the **Inactive Users** report.
3. Select the **Domain** of your choice.
4. Select the period of inactivity.
5. Select the required options if you want to exclude the disabled users or users that have never logged on, from this report.
6. Click on **Generate**.
7. You can modify the fields of this report by using the **Add/Remove columns** option.
8. Select the required/ all users using the designated checkbox.
9. Click on the **more actions** button and select the **Move users to another OU** option listed under the **General attributes** section. Click on **Go**.
10. You will now be directed to the **Move users to another OU** page.
11. Specify the **Container** of your choice.
12. Click **Apply** to move all the required inactive users to the specified OU.



Inactive Users

Selected Domain ✓ division.domain
Selected OUs : All Add OUs

Select the desired time period: Last 7 days

Generated on: 2019-12-11 11:00:40

□ Exclude Never Logged On Users □ Exclude Disabled Users

Selected Count : 2 Clear All

76-100 of 359 25

Check All 359 Clear All 359 Action : Move Users

□	Display Name	SAM Account Name	When Created	Last Logon Time	Account Status
□	deleg1	deleg1	2019-07-23 11:47:23	2019-11-25 18:34:55	Enabled
☑	deleg2	deleg2	2019-07-23 11:59:57	2019-08-02 16:14:30	Enabled
☑	deleg3	deleg3	2019-07-25 15:22:05	2019-07-25 15:53:28	Enabled
□	DerekHope	DerekHope	2019-10-23 22:14:05	0	Enabled

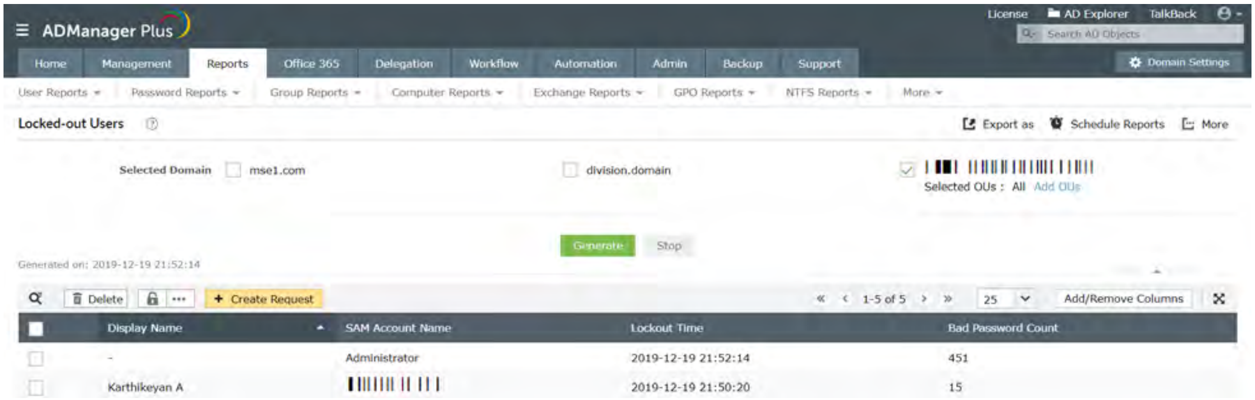
Exercise 2: Find the locked out users and unlock them

Objective: Obtain a list of all the locked out user accounts in Active Directory and unlock them.

Following are the steps that are to be followed for accomplishing the given objective:

1. Click on the **Reports** tab.
2. Under the **Account Status Reports** of the **User Reports** section, click on the **Locked-out Users** report.
3. Select the **Domain** for which you would like to generate the list of locked-out users.

4. Click on **Generate**.
5. Select all the users whose accounts you want to unlock and click on the **Unlock** icon.
6. Click on **Apply** for the changes to take place.



Locked-out Users

Selected Domain □ mse1.com □ division.domain ☑ [redacted]

Selected OUs : All Add OUs

Generated on: 2019-12-19 21:52:14

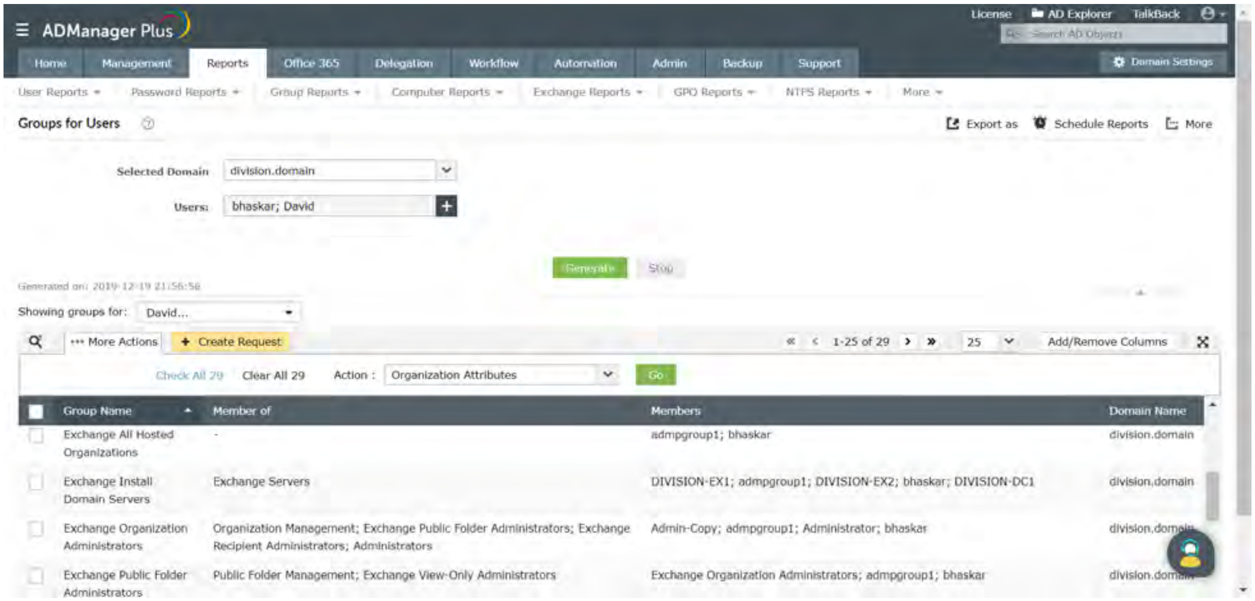
□	Display Name	SAM Account Name	Lockout Time	Bad Password Count
□	-	Administrator	2019-12-19 21:52:14	451
□	Karthikeyan A	[redacted]	2019-12-19 21:50:20	15

Exercise 3: Find the users who share a common group and add those groups to another group

Objective: Find the users who are a member of a particular group and add them to another group.

Following are the steps that have to be followed to obtain the aforementioned objective:

1. Click on the **Reports** tab.
2. Under the **Nested Reports** of the **User Reports** section, click on the **Groups for Users** report.
3. Select the **Domain** of your choice.
4. Select the users of your choice.
5. Click on **Generate**.
6. Under the **Showing groups for** field, select the **Show Only Common Groups** option.
7. Select the required groups and click on **More Actions**.
8. Select the **Organization Attributes** option under **Bulk User Modification** and click on **Go**.
9. Click on the '**+**' option next to the **Add To Group** field and select the required group.
10. Click on **Apply**.



Groups for Users

Selected Domain: division.domain

Users: bhaskar; David

Generated on: 2019-12-19 21:56:56

Showing groups for: David...

1-25 of 29 | 25

Check All 29 | Clear All 29 | Action : Organization Attributes

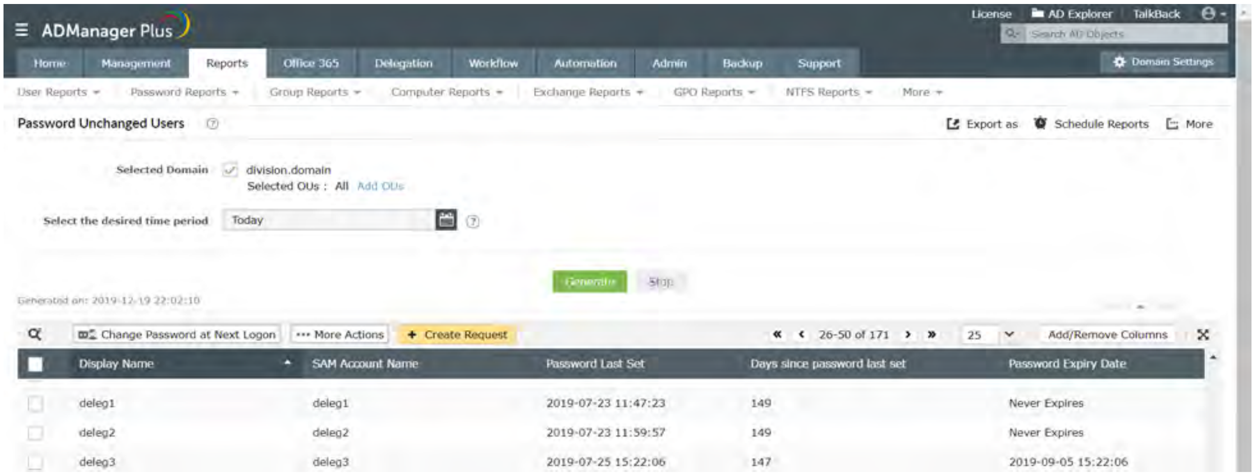
Group Name	Member of	Members	Domain Name
Exchange All Hosted Organizations	-	admpgroup1; bhaskar	division.domain
Exchange Install Domain Servers	Exchange Servers	DIVISION-EX1; admpgroup1; DIVISION-EX2; bhaskar; DIVISION-DC1	division.domain
Exchange Organization Administrators	Organization Management; Exchange Public Folder Administrators; Exchange Recipient Administrators; Administrators	Admin-Copy; admpgroup1; Administrator; bhaskar	division.domain
Exchange Public Folder Administrators	Public Folder Management; Exchange View-Only Administrators	Exchange Organization Administrators; admpgroup1; bhaskar	division.domain

Exercise 4: Find the users who haven't changed their passwords and force them to change their passwords.

Objective: Find the users who haven't changed their passwords in the past 60 days and force them to change their passwords at next logon.

Following are the steps that have to be followed to obtain the given objective:

1. Click on the **Reports** tab.
2. Under **Password Reports,** select **Password Unchanged Users** report in the **Password Status Reports** section
3. Select the **Domain** of your choice.
4. Set the time since they last changed their passwords (say 60 days) .
5. Click on **Generate**.
6. Select all the users and click on the **Change Password at Next Logon** option located above the **Quick Search** option.
7. Click **OK**.



Password Unchanged Users

Selected Domain ☑ division.domain
Selected OUs : All Add OUs

Select the desired time period: Today

Generated on: 2019-12-19 22:02:10

26-50 of 171 · 25

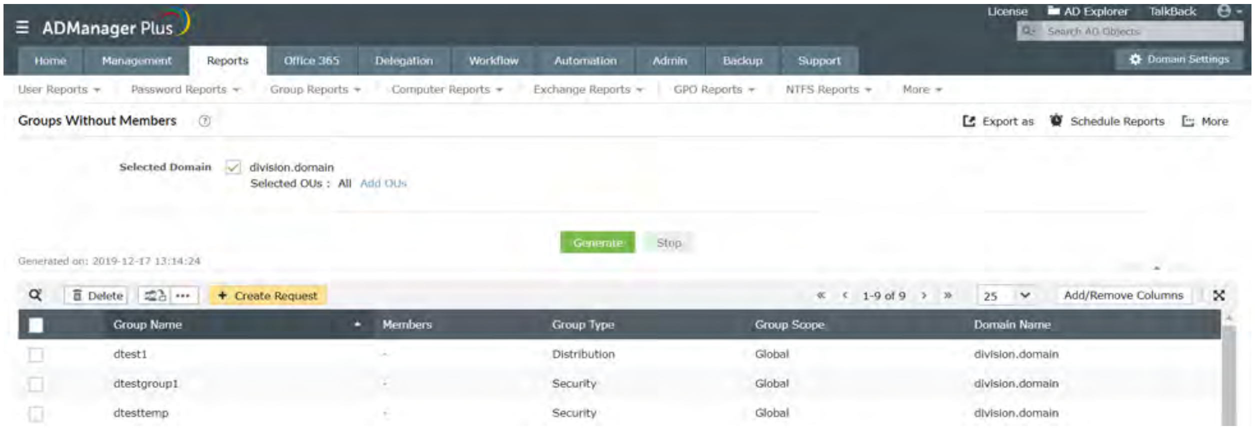
Display Name	SAM Account Name	Password Last Set	Days since password last set	Password Expiry Date
deleg1	deleg1	2019-07-23 11:47:23	149	Never Expires
deleg2	deleg2	2019-07-23 11:59:57	149	Never Expires
deleg3	deleg3	2019-07-25 15:22:06	147	2019-09-05 15:22:06

Exercise 5: Clean up empty groups.

Objective: Obtain a list of all the groups that do not have any members and delete them.

Following are the steps for accomplishing the given objective:

1. Click on the **Reports** tab.
2. Click on the **Group Reports** section and select the **Groups Without Members** report under **Member-based Reports**.
3. Select all the groups and click on the **Delete** icon.
4. Click on **OK**.



Groups Without Members

Selected Domain ☑ division.domain
Selected OUs : All Add OUs

Generated on: 2019-12-17 13:14:24

1-9 of 9 · 25

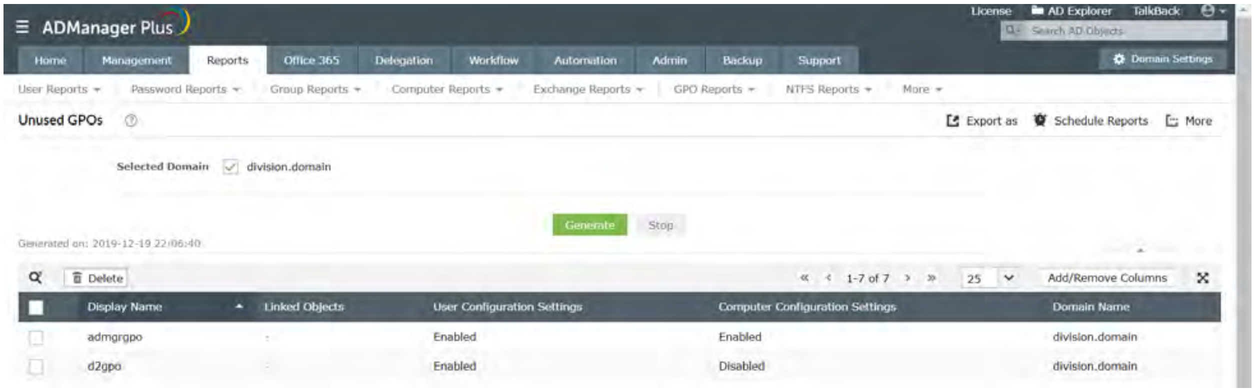
Group Name	Members	Group Type	Group Scope	Domain Name
dtest1	-	Distribution	Global	division.domain
dtestgroup1	-	Security	Global	division.domain
dtesttemp	-	Security	Global	division.domain

Exercise 6: Cleanup all the unused GPOs.

Objective: Obtain a list of all the unused GPOs and delete them.

Follow the steps given below:

1. Click on the **Reports** tab and click on the **GPO Reports** section.
2. Click on the **Unused GPOs** report.
3. Select the **Domain** and click on **Generate**.
4. Select all the GPOs and click on the **Delete** option.
5. Click on **OK**.



Unused GPOs

Selected Domain ☑ division.domain

Generated on: 2019-12-19 22:06:40

☐	Display Name	Linked Objects	User Configuration Settings	Computer Configuration Settings	Domain Name
☐	admgrgpo	-	Enabled	Enabled	division.domain
☐	d2gpo	-	Enabled	Disabled	division.domain

Exercise 7: Add all managers to the Domain Admins Group.

Objective: Generate a list of all the users who are managers and add them to the Domain Admins group.

Following are the steps that have to be followed to accomplish the aforementioned objective:

1. To list all the managers:

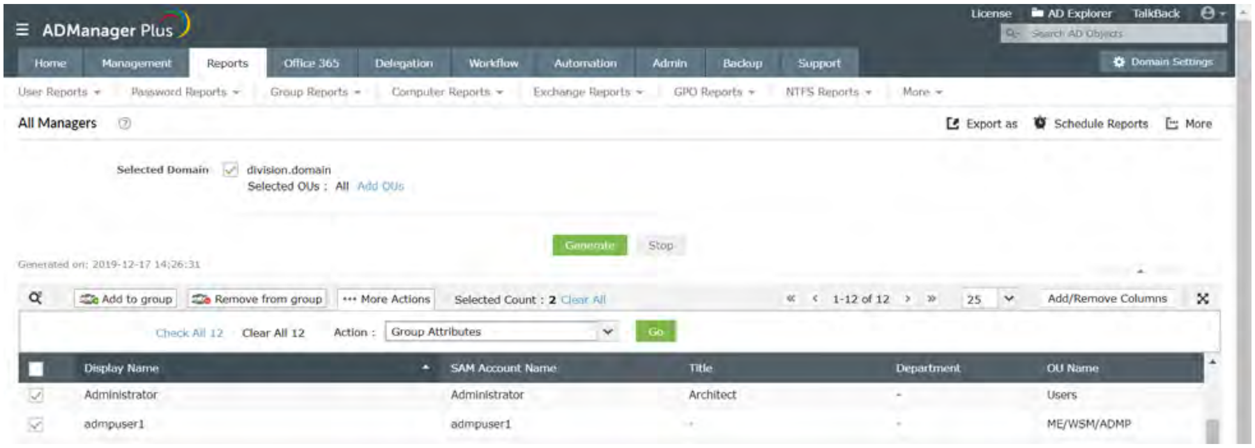
    a. Click on **Reports**.
    b. Click on the **All Managers** report under the **General Reports** section of **User Reports**.
    c. Select the **Domain/OU(s)** from where you want to retrieve the list of managers.
    d. **Generate** the report.

2. To add the Managers to the Domain Admins group:

    a. Select the required managers and click on the **More Actions** option located above the report header.
    b. In the **Select Category** field, select the **Group Attributes** option located under the **General Attributes** section.
    c. Click on **Go**.

d. Click on the **+** icon located beside the **Add to Groups** option and select the **Domain Admins** group.

e. Click **Apply** to make the selected managers members of the **Domain Admins** group.



All Managers

Selected Domain ☑ division.domain
Selected OUs : All Add OUs

Generated on: 2019-12-17 14:26:31

Selected Count : 2

25

Action : Group Attributes

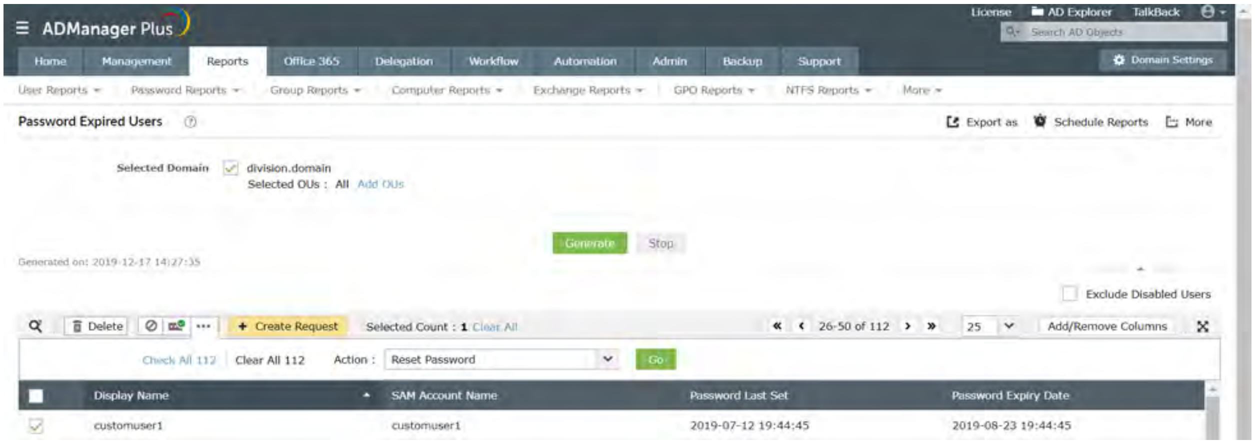
□	Display Name	SAM Account Name	Title	Department	OU Name
☑	Administrator	Administrator	Architect	-	Users
☑	admpuser1	admpuser1	-	-	ME/WSM/ADMP

Exercise 8: Reset the passwords for all the password expired users.

Objective: Find out all the users whose password has expired and reset the password for all of them.

ADManager Plus helps you simplify the above-mentioned objective by performing the following steps:

1. Click on the **Reports** tab.
2. Click on the **Password Expired Users** report located under the **Password Status Reports** of **Password Reports**.
3. Select the **Domain/OU(s)** from where you want to retrieve the password expired users.
4. Click **Generate** to get the list of all the password expired users.
5. Select the required users and click on **More Actions**.
6. Under the **Select Category** field, select the **Reset Password** action listed under the **General Attributes** section.
7. Click **Go**.
8. Select the **Reset Password** checkbox and select a method for resetting the password.
9. Also specify the **Password Options** for the users.
10. Click **Apply** for the changes to take place.



Password Expired Users

Selected Domain ☑ division.domain
Selected OUs : All Add OUs

Generated on: 2019-12-17 14:27:35

□ Exclude Disabled Users

Selected Count : 1 Clear All

« ‹ 26-50 of 112 › » 25

Action : Reset Password

□	Display Name	SAM Account Name	Password Last Set	Password Expiry Date
☑	customuser1	customuser1	2019-07-12 19:44:45	2019-08-23 19:44:45

5. Office 365 Management and Reporting

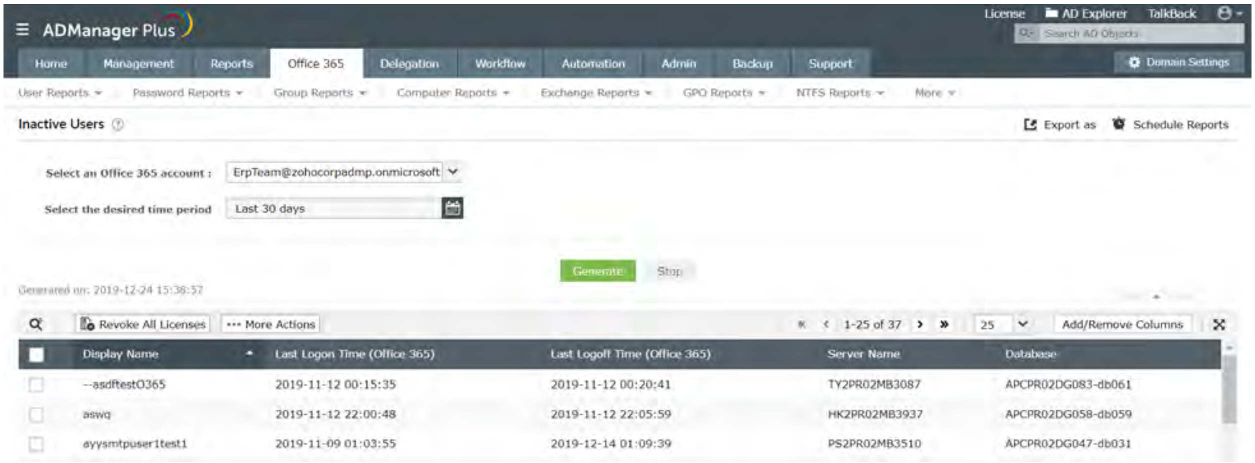
ADManager Plus helps you address the challenges of managing and reporting the cloud-based Office 365, with ease. With this solution, you can manage user accounts in both on-premises and cloud-based environments from a single console, without struggling with numerous tools. It also allows parallel provisioning of user accounts, in multiple platforms, which ensures that employees get the required privileges and access to all the relevant resources immediately, and start being productive right away.

Exercise 1: Office 365 Users License Modification

Objective: To modify assigned licenses in Office 365 online module to free licenses of Inactive users

While making modifications in Office 365 online module, it is only possible to address a single user at a time. However, with ADManager Plus one may assign or remove multiple licenses without even logging into the Office 365 module.

1. Navigate to the **Office 365** tab and click on the **Reports** section.
2. Under the **User Reports** section, generate the **Inactive Users** report. You can also exclude the active AD users from this report.
3. Click on **Generate**.
4. Select the required users and click on the **Revoke all Licenses** option. You can also click on **More Actions** link to perform other license or mailbox related modifications.
5. Click on **OK**.



Inactive Users

Select an Office 365 account : ErpTeam@zohocorpadmp.onmicrosoft

Select the desired time period Last 30 days

Generated on: 2019-12-24 15:38:57

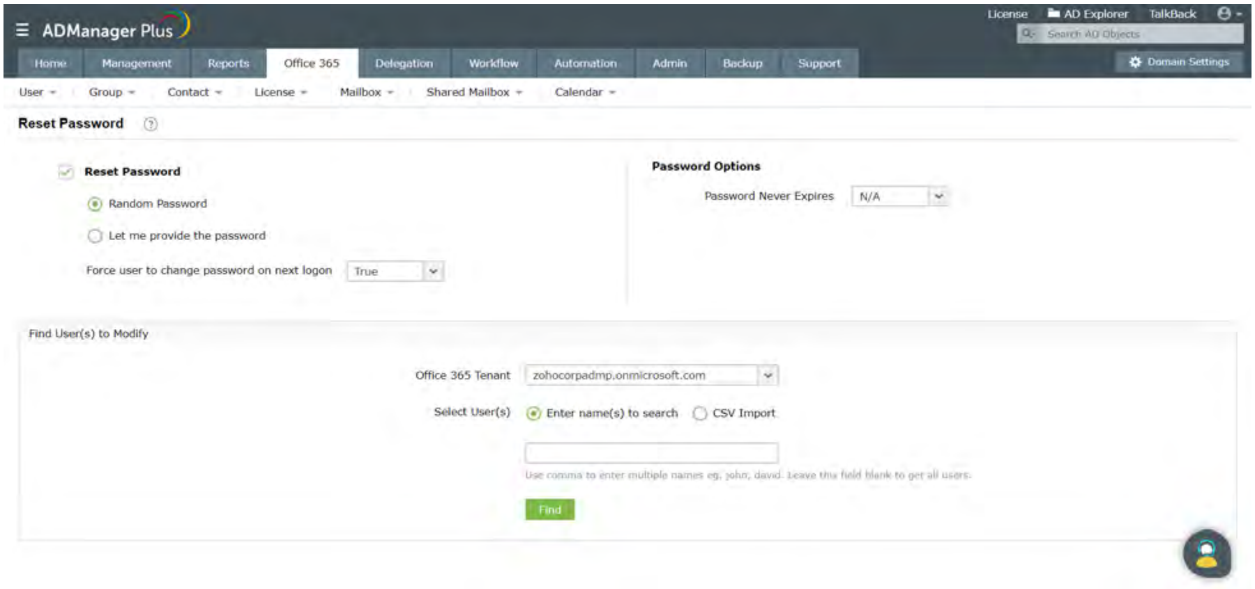
□	Display Name	Last Logon Time (Office 365)	Last Logoff Time (Office 365)	Server Name	Database
□	--asdftest0365	2019-11-12 00:15:35	2019-11-12 00:20:41	TY2PR02MB3087	APCPR02DG083-db061
□	aswq	2019-11-12 22:00:48	2019-11-12 22:05:59	HK2PR02MB3937	APCPR02DG058-db059
□	ayysmtpuser1test1	2019-11-09 01:03:55	2019-12-14 01:09:39	PS2PR02MB3510	APCPR02DG047-db031

Exercise 2: Reset the passwords of Office 365 users

Objective: To reset the passwords of multiple Office 365 user accounts at one go.

Follow the steps given below:

1. Click on the **Office 365** tab.
2. Click on the **Management** section.
3. Click on the **Reset Password** option under the **Bulk User Modification** section.
4. Select a mode for resetting the password- generate a password or provide a password manually.
5. Set Password Options like **Force user to change password at next logon** and **Password never expires**.
6. Select the Office 365 tenant account.
7. Specify users using any of these options:
   - CSV Import which allows you to fetch the required list of users.
   - Built-in search.
8. Click **Apply** for the changes to take place.



Reset Password

☑ **Reset Password**

● Random Password

○ Let me provide the password

Force user to change password on next logon: True

Password Options

Password Never Expires: N/A

Find User(s) to Modify

Office 365 Tenant: zohocorpadmp.onmicrosoft.com

Select User(s): ● Enter name(s) to search ○ CSV Import

Use comma to enter multiple names eg. john, david. Leave this field blank to get all users.

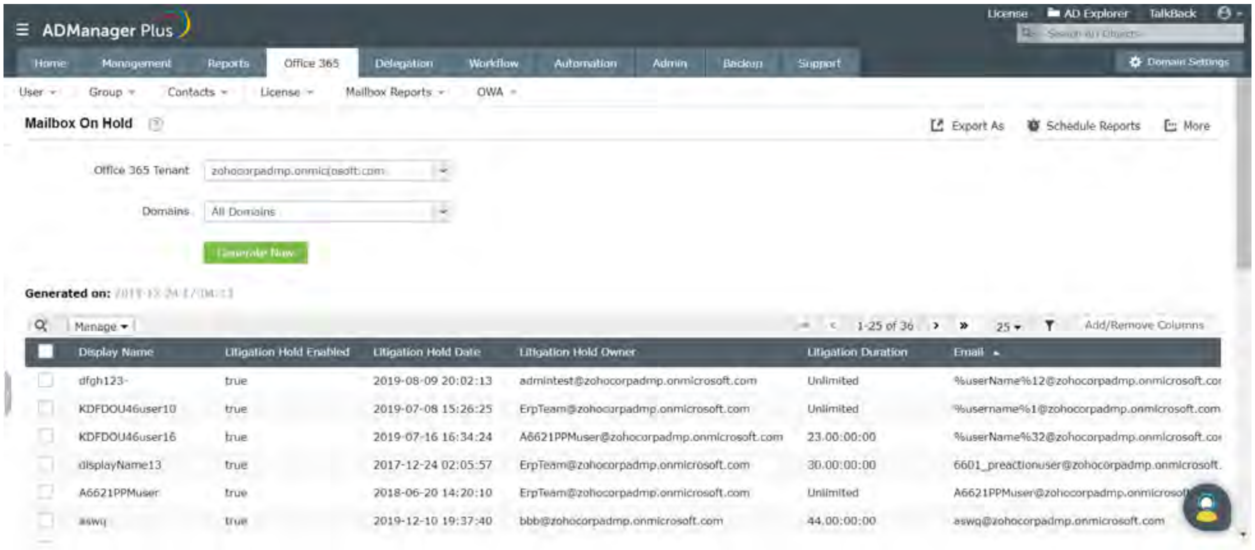
Exercise 3: Generate a report on all the users whose mailboxes are on litigation hold.

Objective: Generate a report on all the Office 365 users whose mailboxes have been put on litigation hold.

Follow the steps given below:

1. Click on the **Office 365** tab and click on the **Reports** section.
2. Click on **Litigation Hold Enabled Mailboxes** option located under the **User Reports** section.
3. Select the Office 365 tenant account.

4. Click on **Generate**.



Mailbox On Hold

Office 365 Tenant: zohocorpadmp.onmicrosoft.com

Domains: All Domains

Generated on: [illegible]

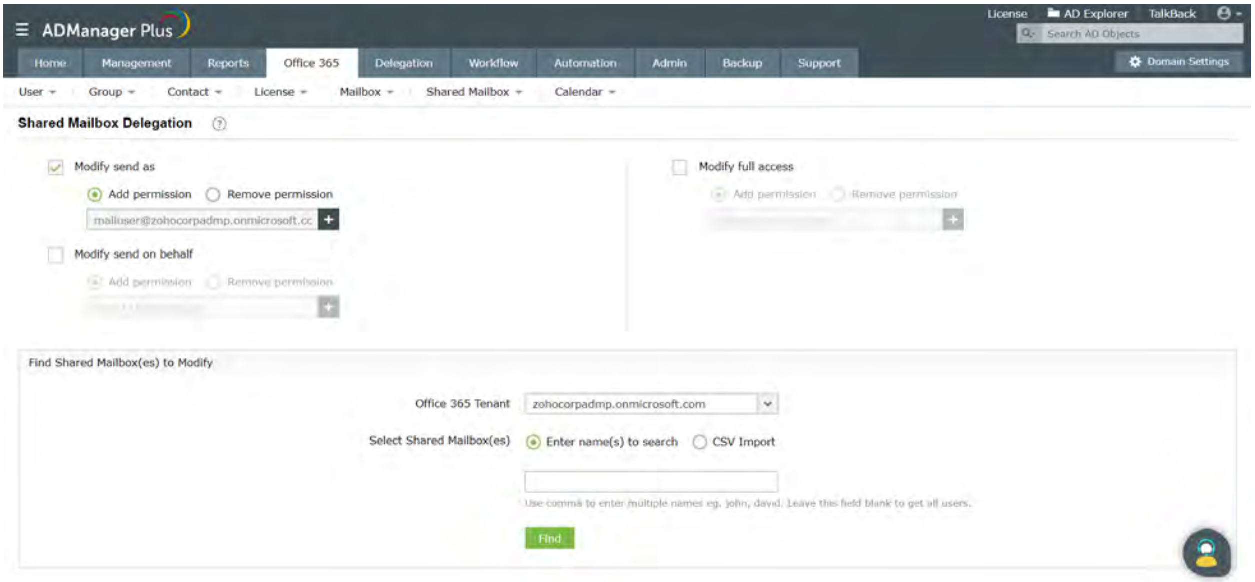
Display Name	Litigation Hold Enabled	Litigation Hold Date	Litigation Hold Owner	Litigation Duration	Email
dfgh123-	true	2019-08-09 20:02:13	admintest@zohocorpadmp.onmicrosoft.com	Unlimited	%userName%12@zohocorpadmp.onmicrosoft.co
KDFDOU46user10	true	2019-07-08 15:26:25	ErpTeam@zohocorpadmp.onmicrosoft.com	Unlimited	%username%1@zohocorpadmp.onmicrosoft.com
KDFDOU46user16	true	2019-07-16 16:34:24	A6621PPMuser@zohocorpadmp.onmicrosoft.com	23.00:00:00	%userName%32@zohocorpadmp.onmicrosoft.co
displayName13	true	2017-12-24 02:05:57	ErpTeam@zohocorpadmp.onmicrosoft.com	30.00:00:00	6601_preactionuser@zohocorpadmp.onmicrosoft.
A6621PPMuser	true	2018-06-20 14:20:10	ErpTeam@zohocorpadmp.onmicrosoft.com	Unlimited	A6621PPMuser@zohocorpadmp.onmicrosof
aswq	true	2019-12-10 19:37:40	bbb@zohocorpadmp.onmicrosoft.com	44.00:00:00	aswq@zohocorpadmp.onmicrosoft.com

Exercise 4: Shared mailbox delegation

Objective: Grant 'Send As' permissions to a user account for a shared mailbox.

Follow the steps given below:

1. Click on the **Office 365** tab and click on the **Management** section.
2. Click on Shared **Mailbox Management** under the **Exchange Online** section.
3. Click on the **Shared Mailbox Delegation** option.
4. Enable the **Modify Send As** option and select the **Add permissions** option.
5. Click on the **+** option to select the users to whom you want to assign the **Send As** permission.
6. Click on **OK**.
7. Select the required Office 365 tenant account.
8. Find the shared mailboxes either by:
    - Importing the CSV file that has the list of required mailboxes.
    - Using the built-in search option.
9. Click on **Apply**.



Shared Mailbox Delegation

☑ Modify send as

● Add permission ○ Remove permission

mailuser@zohocorpadmp.onmicrosoft.cc +

□ Modify send on behalf

○ Add permission ○ Remove permission

□ Modify full access

○ Add permission ○ Remove permission

Find Shared Mailbox(es) to Modify

Office 365 Tenant: zohocorpadmp.onmicrosoft.com

Select Shared Mailbox(es): ● Enter name(s) to search ○ CSV Import

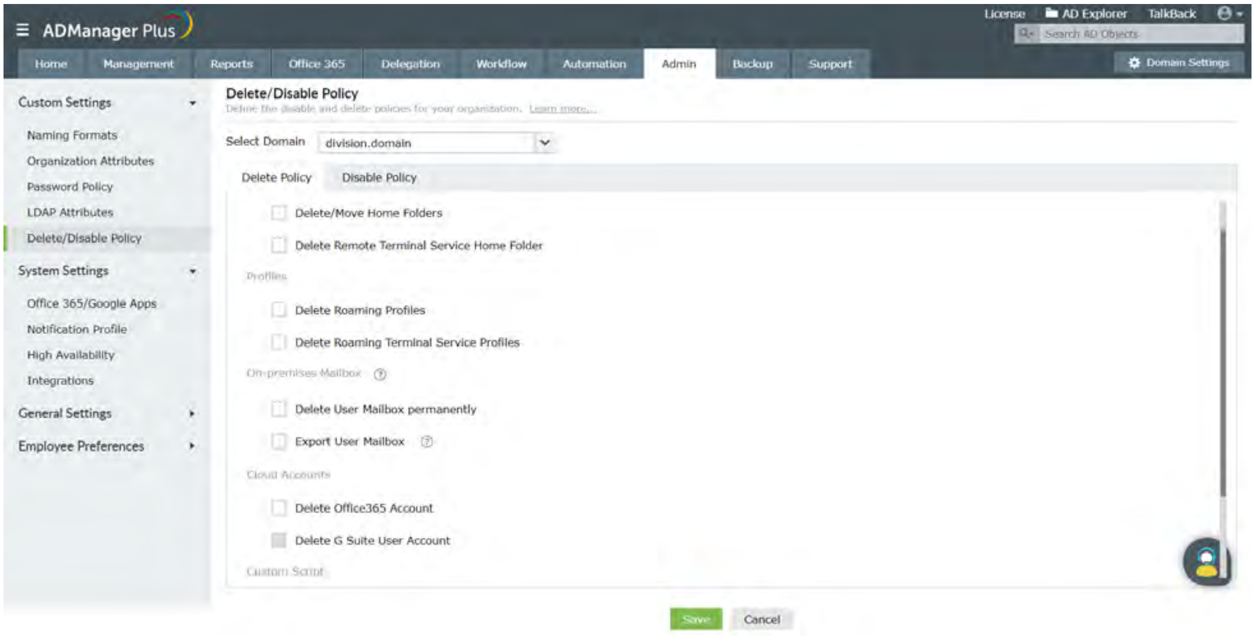
Use comma to enter multiple names eg. john, david. Leave this field blank to get all users.

Exercise 5: Delete the Office 365 account while deleting the linked AD user account.

Objective: Delete the linked Office 365 account whenever an AD user account is deleted.

Follow the steps given below:

1. Define the Delete/Disable Policy:
    a. Click on the **Admin** tab.
    b. Under the **Custom Settings** section, click on the **Delete/Disable Policy** option.
    c. Select the **Domain** for which you want to define the policy.
    d. Click on the **Delete Policy** tab.
    e. Under the **O365/G Suite** option, select the **Delete Office 365 Account** option.
    f. Click on **Save**.



Delete/Disable Policy

Define the disable and delete policies for your organization. Learn more...

Select Domain: division.domain

Delete Policy | Disable Policy

- □ Delete/Move Home Folders
- □ Delete Remote Terminal Service Home Folder

Profiles

- □ Delete Roaming Profiles
- □ Delete Roaming Terminal Service Profiles

On-premises Mailbox

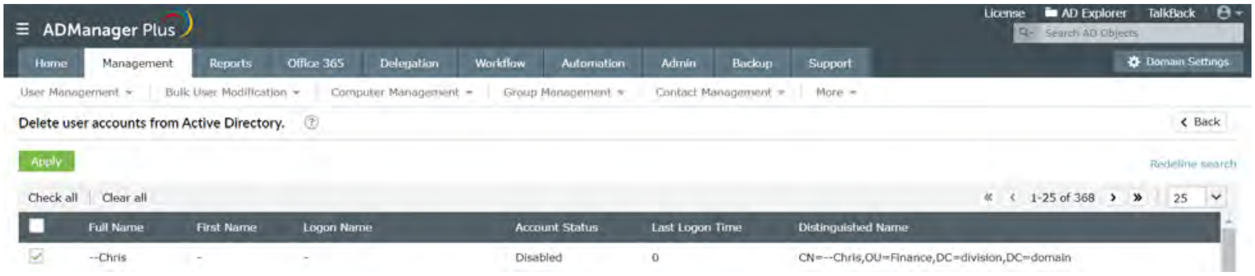
- □ Delete User Mailbox permanently
- □ Export User Mailbox

Cloud Accounts

- □ Delete Office365 Account
- □ Delete G Suite User Account

Custom Script

2. Delete a user:
    a. Click on the **Management** tab.
    b. Click on the **Delete Users** option under the **Bulk User Modification** section.
    c. Select the required **Domain.**
    d. Specify the users using any of these options:
        i. Importing a CSV file that has the list of required users.
        ii. Using built-in search option .
    e. Click on **Apply**. Now, when the user is deleted, the linked Office 365 account will also be deleted.



Delete user accounts from Active Directory.

□	Full Name	First Name	Logon Name	Account Status	Last Logon Time	Distinguished Name
☑	--Chris	-	-	Disabled	0	CN=--Chris,OU=Finance,DC=division,DC=domain

6. Back up and Recovery

Accidental deletions and modification of Active Directory objects can cause disruptions in the day-to-day activities of your business. Restoring those is often tedious and expensive. The backup and recovery feature of ADManager Plus helps you counter this problem with its simple yet efficient functionalities like scheduled and incremental backups, no-restart recovery(as the DCs needn't be restarted after every restoration), attribute and object level restoration, and recovery of objects after their tombstone period, etc.

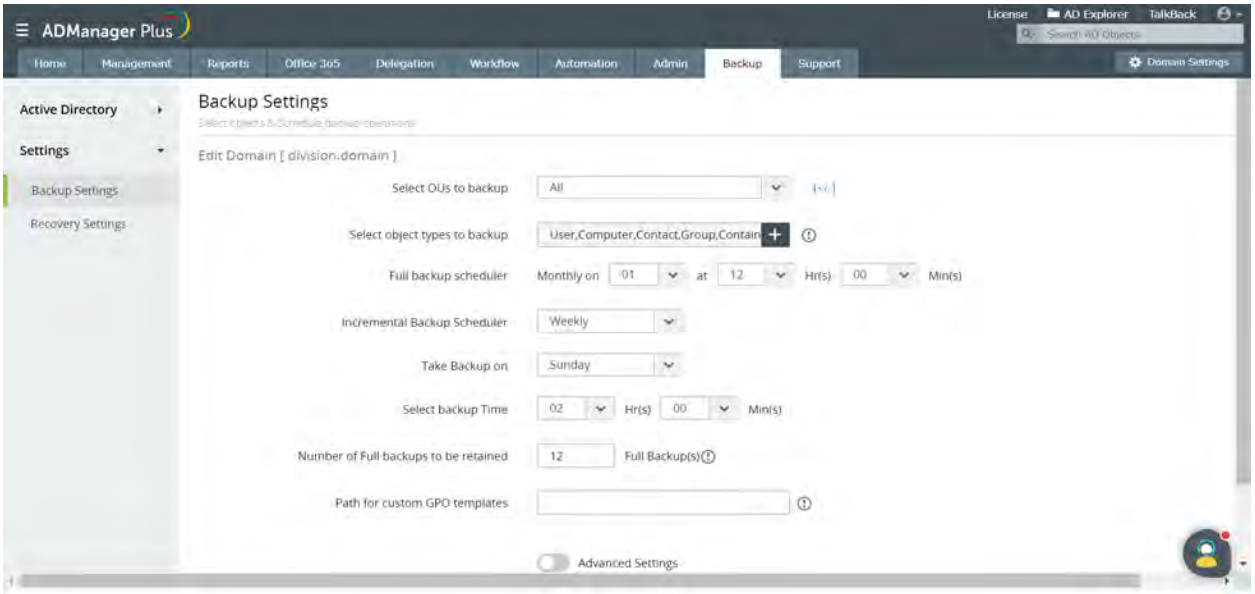
The exercises in this section focus on vital backup and recovery actions useful for IT administrators.

Exercise 1: Configure a backup schedule for your domain. All objects in a specific OU should be backed up every day at 3 am and 12 full backups, one for each month of the year, need to be retained.

Objective: Create a backup schedule for a domain.

Solution:

1. Click on the **Backup** tab. Under **Settings** on the left pane, select **Backup settings**.
2. Click on the **Edit** icon next to the required domain name.
3. Click on the **[+/-]** icon next to **Select the OU to be backed up** field. You can also choose the type of objects you want to backup.
4. Choose **Daily** in the **Incremental Backup Scheduler** field.
5. Set the **Back up Time** to '03' hrs.
6. Enter '12' for the **Number of full backups to be retained.** By default, the full backup time is set at the 1st of every month at 12 am, you can also customize this according to your organization's need.
7. Click **Save.**



Backup Settings

Select objects & Schedule backup operations

Edit Domain [division.domain]

Select OUs to backup: All

Select object types to backup: User,Computer,Contact,Group,Contain

Full backup scheduler: Monthly on 01 at 12 Hr(s) 00 Min(s)

Incremental Backup Scheduler: Weekly

Take Backup on: Sunday

Select backup Time: 02 Hr(s) 00 Min(s)

Number of Full backups to be retained: 12 Full Backup(s)

Path for custom GPO templates:

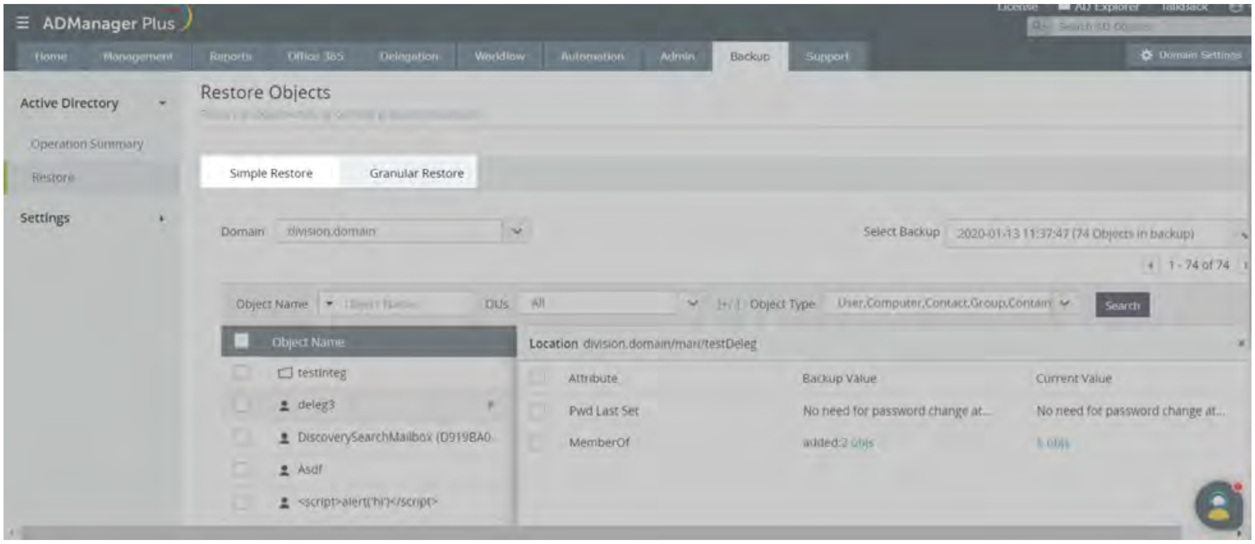
Advanced Settings

Exercise 2: You have inadvertently modified the attributes of all users, instead of a few specific users in an OU. Restore the attributes to their original values, for only the user objects which were modified accidentally.

Objective: Restore specific attributes for AD users.

Solution:

1. Click on the **Backup** tab. Under **Active Directory** on the left pane, select **Restore**.
2. You can either choose the **Simple Restore** view or **Granular Restore** view.
   - The **Simple Restore** view lists all changes made to attributes chronologically. It also allows you to filter attributes changes made during specific time periods.
   - The **Granular Restore** view lists the number of backups available and allows you to choose from the different versions of the attribute backed up.
   - In short, if you know which backup version you want to revert to, you can choose **Simple Restore**. If you only know the object name and not the backup version, then **Granular Restore** would be better for you to work with. For this case, since the changes have been recently made, it is easier to work with the **Simple Restore** view.
3. Select the specific **Domain**, **OU,** and **object type.** In this case, select **user** in object type and choose the OU and the domain to which it belongs.
4. Select the user(s) you want to restore. The search option also lets you search for particular users.
5. Click **Restore.**



Domain: division.domain

Select Backup: 2020-01-13 11:37:47 (74 Objects in backup)

1 - 74 of 74

Object Name: Object Name | OUs: All | Object Type: User,Computer,Contact,Group,Contain

- testinteg
- deleg3
- DiscoverySearchMailbox (D919BA0
- Asdf
- <script>alert('hi')</script>

Location division.domain/mari/testDeleg

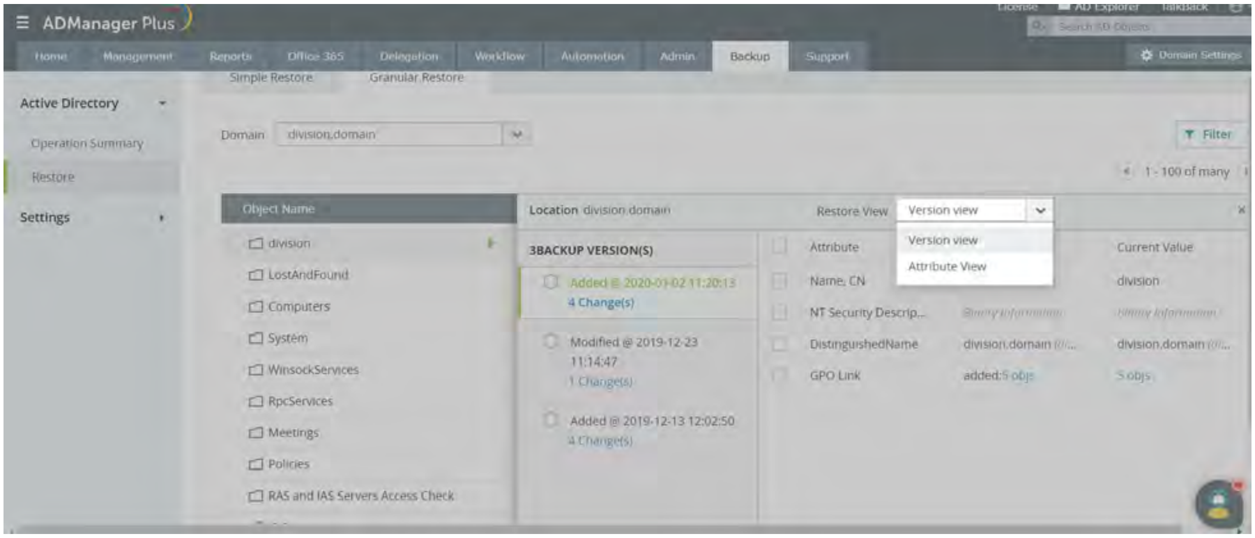
Attribute	Backup Value	Current Value
Pwd Last Set	No need for password change at...	No need for password change at...
MemberOf	added:2 objs	5 objs

Exercise 3: You have accidentally modified an attribute. Revert to its original value.

Objective : Restore a modified AD object to its previous version.

Solution:

1. Click on the **Backup** tab. Under **Active Directory** on the left pane, select **Restore**.
2. Select the **domain** which contains the object whose attribute is to be restored.
3. Choose **Granular Restore**. The available backups for the objects in the domain are listed. When you click on the no. of backups available for your chosen attribute, a pop-up opens. You can choose between **Version view** and **Attribute view**.
    - The **Version View** allows you to select a backup version from the specified time period. Select the required backup version from the left pane. Once the required backup is selected, you will see the values of different attributes backed up in that cycle, along with the present value of those attributes.
    - The **Attribute View** allows you to select from each object's modified attributes.Select the attribute for which you would like to see the past values for, from the left pane.
4. Select the version of the attribute you want to restore.
5. Click **Restore**.



Domain: division.domain

Object Name
division
LostAndFound
Computers
System
WinsockServices
RpcServices
Meetings
Policies
RAS and IAS Servers Access Check

Location division.domain

Restore View: Version view

3BACKUP VERSION(S)

- ○ Added @ 2020-01-02 11:20:13 4 Change(s)
- ○ Modified @ 2019-12-23 11:14:47 1 Change(s)
- ○ Added @ 2019-12-13 12:02:50 4 Change(s)

□	Attribute		Current Value
□	Name, CN		division
□	NT Security Descrip...	Binary information	Binary information
□	DistinguishedName	division.domain (0/...	division.domain (0/...
□	GPO Link	added:5 objs	5 objs

7. Non-invasive Active Directory Delegation

Often, Active Directory administrators face the dilemma of choosing between completing the mundane, repetitive tasks and the more important ones. The only option that they sometimes have is to hand over the routine, simple tasks to someone else. But they are reluctant to do so because of the risks involved as the Active Directory security can easily be compromised. A minute mistake could send the entire Active Directory for a toss.

ADManager Plus offers help desk delegation with which you can create help desk technicians and delegate desired tasks like reset passwords, unlock user accounts, create users, etc. In this way help desk users can share the workload of administrators and let them concentrate on core administrative activities instead. AD delegation in ADManager Plus is non-invasive i.e., the permissions provided in ADManager Plus do not hinder with the actual AD permissions of the technician. ADManager Plus allows administrators to delegate tasks to help desk technicians without worrying about them accessing the Domain Controllers directly and compromising the security of the AD environment.

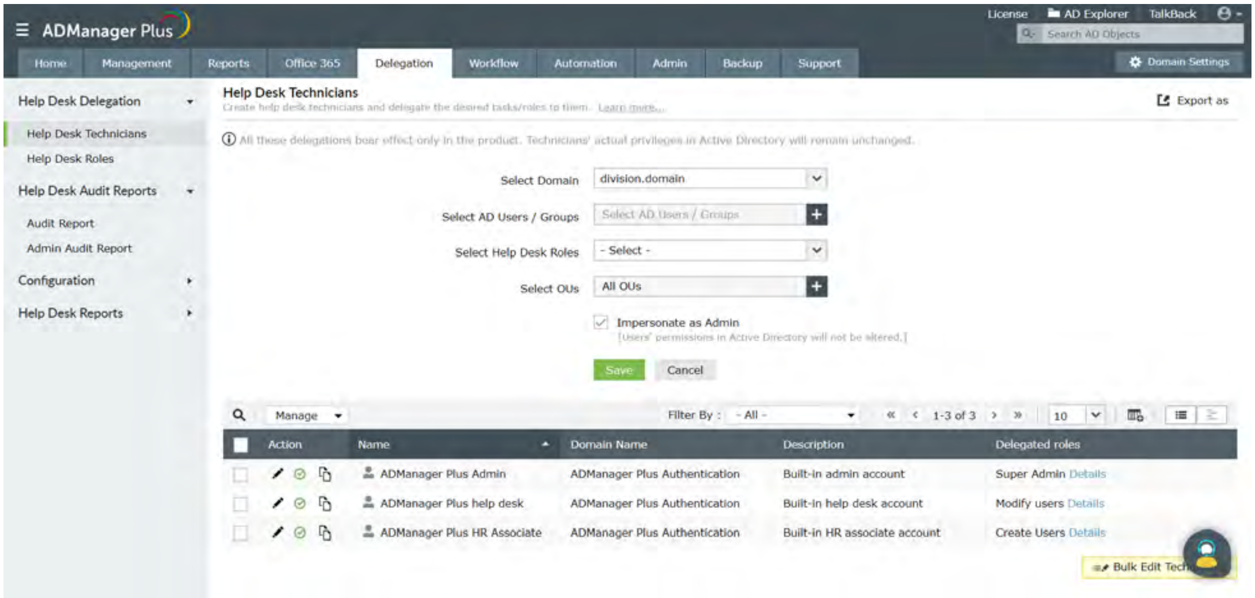
Exercise 1: Introduction to Help Desk Technicians, Help Desk Role

Objective: Create a new help desk role and assign it to a new help desk technician or to members of a particular AD group.

The technician created using ADManager Plus, will have paltry access, i.e., the technician will be able to exercise only the assigned role in the designated OU.

Follow the steps given below to obtain the above-mentioned objective:

1. To create a help desk role:
    a. Click on the **Delegation** tab and click on **Help Desk Roles** option, under **Help Desk Delegation** tab.
    b. Click on **Create New Role** and enter a suitable name and description for the role.
    c. Navigate between the various tabs like **AD Management**, **AD Reports**, **Administration** and **Office 365** to use the designated check-boxes for delegating the required actions.
    d. Click on **Save**.
2. To assign this role to a new technician:
    a. Click on **Help Desk Technicians** and click on **Add New Technician**.
    b. Select the **Domain** of your choice.
    c. Select the **AD user** or **Group**, whom you want to delegate as a technician.
    d. Select the **role** that you just created from the drop-down menu.
    e. Select the **OU** in which the assigned role can be exercised.
    f. Select the **Impersonate as an Admin** option, if the permissions assigned to the technicians in ADManager Plus are not assigned in AD.
    g. Click on **Save**.



Help Desk Technicians

Create help desk technicians and delegate the desired tasks/roles to them. Learn more...

ⓘ All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

Select Domain: division.domain

Select AD Users / Groups: Select AD Users / Groups

Select Help Desk Roles: - Select -

Select OUs: All OUs

☑ Impersonate as Admin
[Users' permissions in Active Directory will not be altered.]

Filter By : - All - 1-3 of 3 10

□	Action	Name	Domain Name	Description	Delegated roles
□		ADManager Plus Admin	ADManager Plus Authentication	Built-in admin account	Super Admin Details
□		ADManager Plus help desk	ADManager Plus Authentication	Built-in help desk account	Modify users Details
□		ADManager Plus HR Associate	ADManager Plus Authentication	Built-in HR associate account	Create Users Details

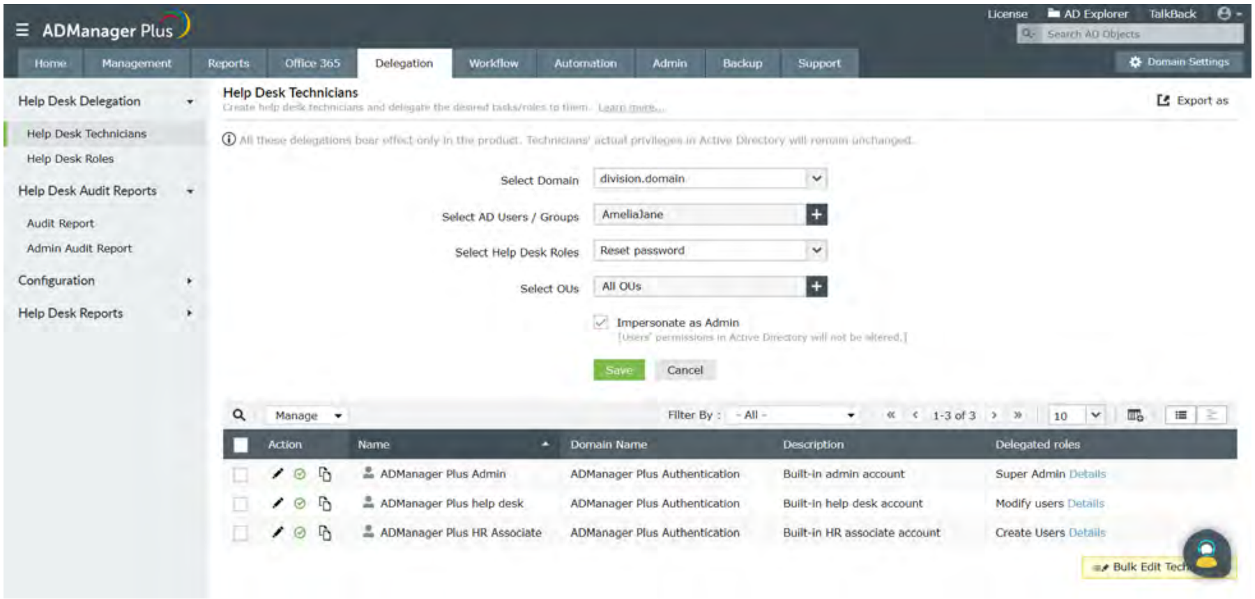
Exercise 2: Delegate the password reset action.

Objective: Create a help desk technician and assign only the role of resetting the passwords for users.

Following are the steps that have to be followed for accomplishing the aforementioned objective:

1. To create the Password Reset role:
    a. Click on the **Delegation** tab and click on Help Desk Roles.
    b. Click on **Create New Role**.
    c. Give a suitable name and description for the role. (For instance, Password Reset role).
    d. Select the **Reset Password** option given under the **Bulk User Modification** section of the **User Management** section.
    e. Click on **+** beside the **Reset Password** option to specify the password options for the users.
    f. Click on **Save Role**.

2. To assign the Password Reset role to a new technician:
    a. Click on **Help Desk Technicians** and click on **Add New Technician**.
    b. Select the **Domain** of your choice.
    c. Select the **AD user** or **group**, whom you want to delegate as a technician.
    d. Select the **Password Reset role** that you just created from the drop-down menu next to the **Select Role** field.
    e. Select the **OU** in which the technician can perform the reset password action.
    f. Select the **Impersonate as an Admin** option, if the permissions assigned to the technicians in ADManager Plus are not assigned in AD.
    g. Click on **Save** to make the selected user a help desk technician who can reset the passwords.



Help Desk Technicians

Create help desk technicians and delegate the desired tasks/roles to them. Learn more...

ⓘ All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

Select Domain: division.domain

Select AD Users / Groups: AmeliaJane

Select Help Desk Roles: Reset password

Select OUs: All OUs

☑ Impersonate as Admin
[Users' permissions in Active Directory will not be altered.]

Filter By : - All -   1-3 of 3   10

□	Action	Name	Domain Name	Description	Delegated roles
□		ADManager Plus Admin	ADManager Plus Authentication	Built-in admin account	Super Admin Details
□		ADManager Plus help desk	ADManager Plus Authentication	Built-in help desk account	Modify users Details
□		ADManager Plus HR Associate	ADManager Plus Authentication	Built-in HR associate account	Create Users Details

Exercise 3: Delegate Department based Active Directory Administration

Objective: Assign the Active Directory administrative tasks to be carried out for specific department(s) to a help desk technician.

Following are the steps that have to be followed to accomplish the above-mentioned objectives.

1. To create an Administrator Role:
    a. Click on the **Delegation** tab and click on **Help Desk Delegation.**
    b. Click on **Help Desk Roles** and click on **Create New Role**.
    c. Click on **Administration** and select the required options/tasks.
    d. Save this role.

2. To create a help desk technician and assign the administrative role to this technician for a specific OU:
    a. Under **Help Desk Delegation**, go to **Help Desk Technicians** and click on **Add New Technician**.
    b. Select the **Domain** and the user to whom you would like to delegate this administrative task.
    c. Select the **Administration Role** that you just created from the list of roles available.
    d. Select the OU for which this technician can do the administration.
    e. **Save** to complete the creation of a new help desk technician for taking care of the administration of a specific OU (Department).

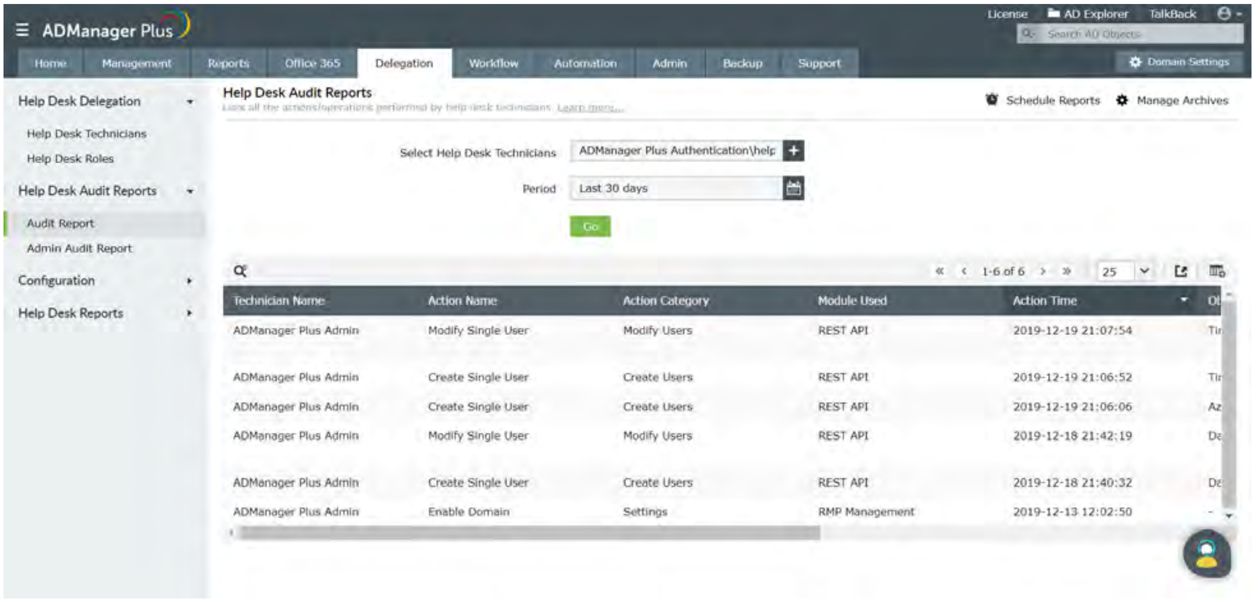
Exercise 4: Audit administrative activities by AD technicians

Scenario: Admins want to audit the activities performed by technicians on a regular basis. They find it difficult on most occasions because the technicians appear to "Impersonate as Admin" and the event log registers the Domain Account or the Service Account.

All management activities performed by the technicians are recorded in the ‘Audit Reports’ tab under AD Delegation, and can be scheduled at desired intervals. This report allows you to track a technician at the designated time through notifications by email or on a shared path.

Follow the steps given below to generate the audit reports:

1. Click on the **Delegation** tab and click on **Audit Report,** in the **Help Desk Audit Reports** .
2. Select the name of the technician and the time-period.
3. Click on **Go** to the view the logs of the activities performed by all the technicians.



Help Desk Audit Reports
Lists all the actions/operations performed by help desk technicians. Learn more...

Select Help Desk Technicians: ADManager Plus Authentication\help
Period: Last 30 days

Technician Name	Action Name	Action Category	Module Used	Action Time	Ol
ADManager Plus Admin	Modify Single User	Modify Users	REST API	2019-12-19 21:07:54	Ti
ADManager Plus Admin	Create Single User	Create Users	REST API	2019-12-19 21:06:52	Ti
ADManager Plus Admin	Create Single User	Create Users	REST API	2019-12-19 21:06:06	Az
ADManager Plus Admin	Modify Single User	Modify Users	REST API	2019-12-18 21:42:19	De
ADManager Plus Admin	Create Single User	Create Users	REST API	2019-12-18 21:40:32	De
ADManager Plus Admin	Enable Domain	Settings	RMP Management	2019-12-13 12:02:50	-

8. Active Directory Automation

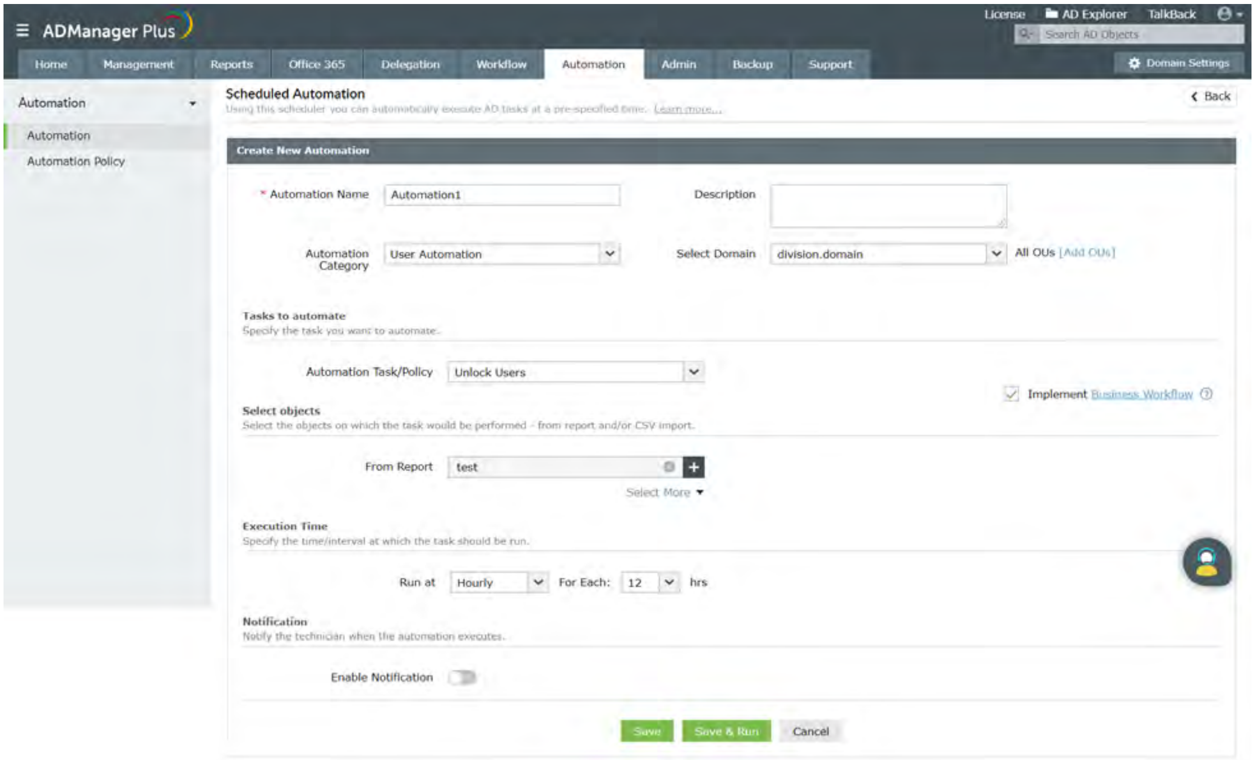
Simple, routine tasks such as creating users and deleting or disabling inactive users can be decisive to an organization's robust functioning. Hence these everyday tasks can be automated using the *Automation* feature of ADManager Plus for operational efficiency. Instead of manually configuring AD objects, you can automate these tasks, and utilize the time saved by automation for other high priority tasks. Moreover, you also have the option to set up a controlled automation (approval based mechanism) process using the 'Workflow' feature which will ensure that no task is executed unless it is reviewed and approved by the concerned authority.

Exercise 1: Automated unlocking of user accounts

Objective: Unlock the accounts of locked-out users automatically, at a specified time.

Following are the steps that are required to automate the task of unlocking locked out user accounts:

1. Click on the **Automation** tab and click on the **Automation** option available on the left pane.
2. Click on **Create New Automation**.
3. Enter a suitable name and description for the automation. (For instance, you can name this automation as Unlock User Accounts).
4. Select **User Automation** under the **Automation Category**.
5. Select the **Domain** in which the locked-out user accounts are located.
6. Set the **Select Tasks to Automate** field to **Unlock Users** specified under the **Automation Task/Policy** section.
7. You can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.
    a. From Reports:
    Click on the **Select** link and select the required report. For this scenario, select the **Locked Out Users** report from the reports list.
    b. From a CSV:
    Click on the **Select More** link and specify the location of the file in which the user accounts are specified.
8. Select the **Implement Business Workflow** option, if you want to review or approve of every task before it is actually executed.
9. Specify the time at which the user accounts have to be unlocked using the options given under the **Execution Time**. Set the time to 6:00 AM and frequency to **Once**.
10. **Save** this automation to schedule the unlock operation for 6:00 am every day.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: division.domain — All OUs [Add OUs]

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Unlock Users

☑ Implement Business Workflow

Select objects

Select the objects on which the task would be performed - from report and/or CSV import.

From Report: test

Select More

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly — For Each: 12 hrs

Notification

Notify the technician when the automation executes.

Enable Notification: ○

Exercise 2: Automatically cleanup the inactive AD users.

Scenario: As per your organizational policies, you will have to fetch and move all the inactive user accounts to a specific OU at the end of every month. After 90 days, these users have to be deleted from your Active Directory. The objective of this exercise is to automate the task of moving inactive user accounts from their present locations (containers) to a different OU and delete these user accounts after 90 days.

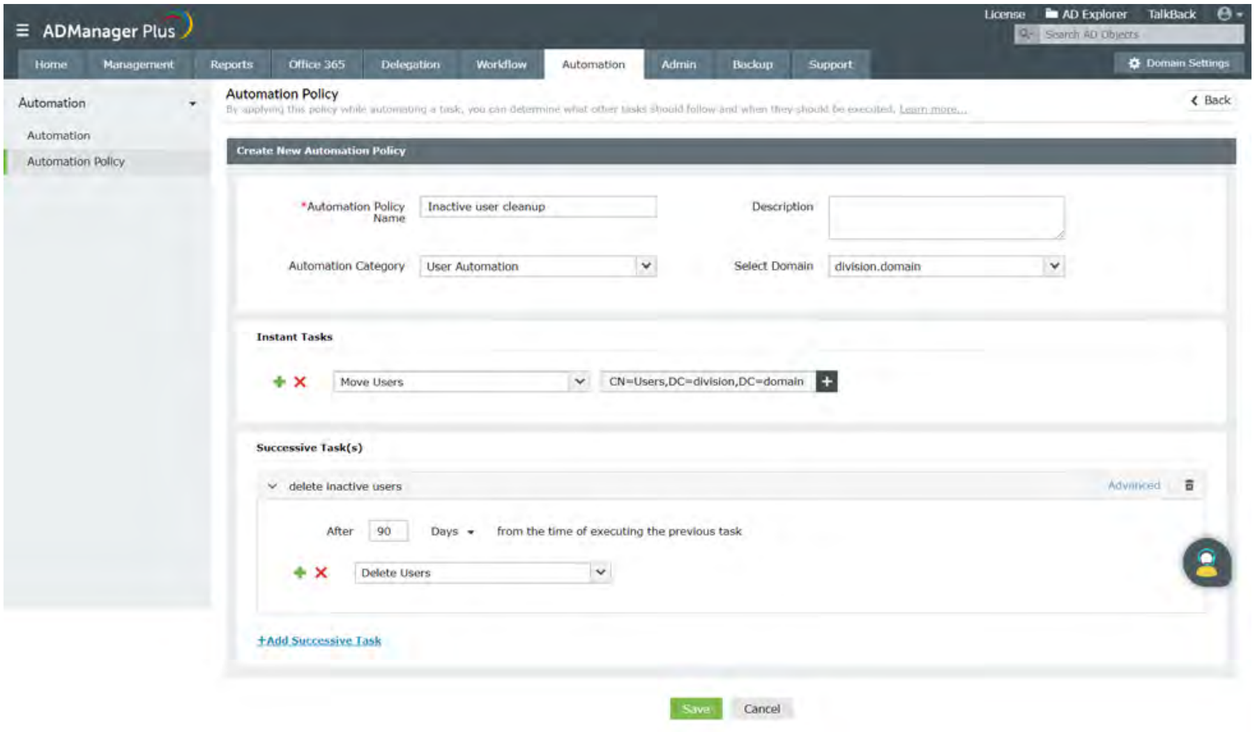
You can use the ‘Automation Policy’ of ADManager Plus to accomplish the above requirement by:

- Creating an ‘automation policy’ that will
  - Move inactive users to a specific OU.
  - Delete the moved inactive user accounts.
- Creating a new ‘automation’ and assigning the above ‘automation policy’ to this automation.
- Select the Domain (or OUs) from which you wish to fetch the inactive users.
- Specify the frequency at which this automation has to be executed.

Following are the steps that have to be performed to meet the above-mentioned requirements:

1. To create a new policy
   a. Click on the **Automation** tab.
   b. Click on the **Automation Policy** option available on the left pane and click on **Create New Policy**.

c. Enter a suitable name and description for the automation policy. For instance, you can set the name of the automation policy to 'Inactive user cleanup'.
d. Select the **Domain** in which this automation policy must be used.
e. Select **User Automation** as the category under which this policy must be listed.
f. Under the **Instant Tasks** section, select **Move Users** from the task list and select the **Container** to which you want to move the users.
g. Under the **Successive Tasks** section,
   i. Specify a name for this task by click on **Task Group**. Let us name this task as **Delete Inactive Users**.
   ii. Set the time limit to **After 90 days**.
   iii. Set the task to **Delete Users**.
h. **Save** this automation policy.



Automation Policy

By applying this policy while automating a task, you can determine what other tasks should follow and when they should be executed. Learn more...

Create New Automation Policy

*Automation Policy Name: Inactive user cleanup

Description:

Automation Category: User Automation

Select Domain: division.domain

Instant Tasks

Move Users — CN=Users,DC=division,DC=domain

Successive Task(s)

delete inactive users

After 90 Days from the time of executing the previous task

Delete Users

+Add Successive Task

2. To create an automation,
   a. Click on the **Automation** option available on the left pane.
   b. Click on **Create New Automation**.
   c. Give a suitable name and description for the automation
   d. Specify the **Domain** in which the **Automation** must be run.
   e. Select **User Automation** under the **Automation Category**.
   f. Set the **Select Tasks to Automate** field to the automation policy that you just created (Inactive users cleanup) that is specified under the **Automation Task/Policy** section.
   g. You can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.
      i. From Reports:

Click on the **Select** link and select the required report. For this scenario, select the **Inactive Users** report from the reports list and specify the period of inactivity.

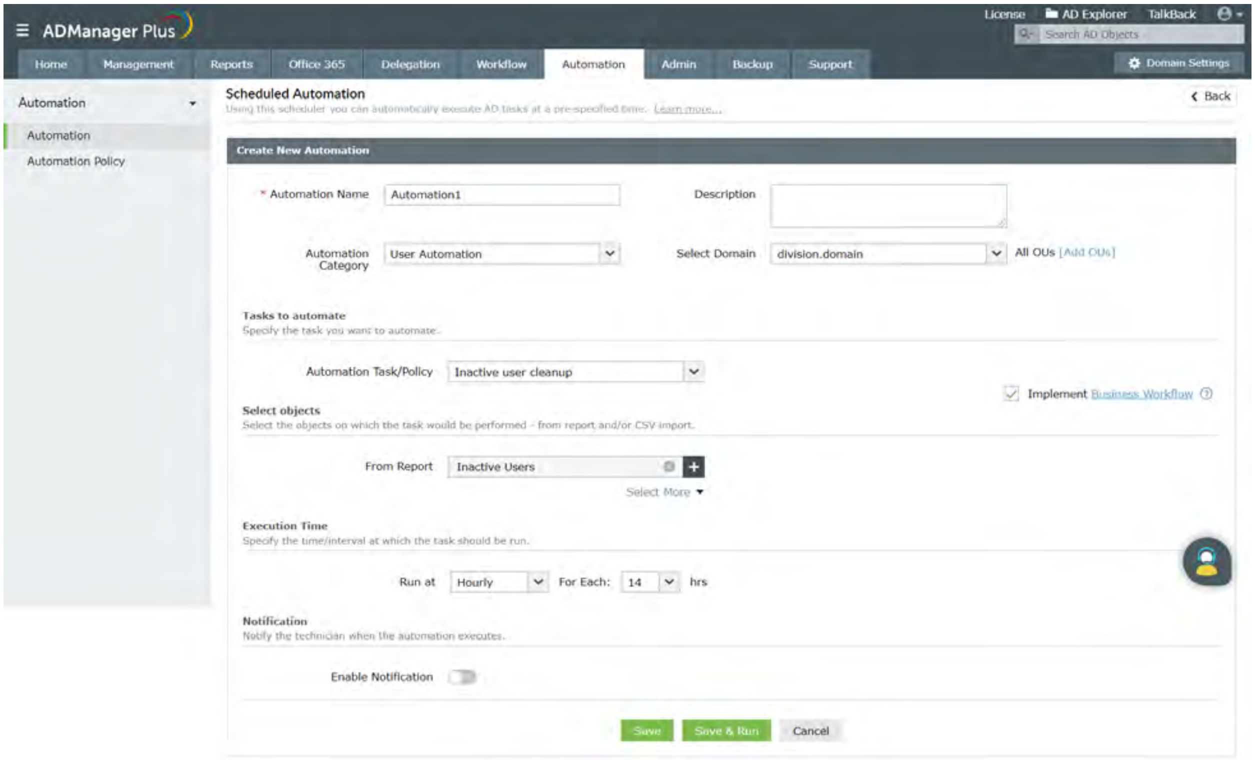
ii. From a CSV:
Click on the **Select More** link and specify the location of the CSV file in which the inactive user accounts are specified.

h. Select the **Implement Business Workflow** option, if you want to review or approve of every task before it is actually executed.

i. Specify the **Time Interval** at which the automation must be executed.

j. Specify the frequency for the automation to be repeated.

k. Enable notifications to be sent to either technicians or the administrator, whenever this automation is executed.



Scheduled Automation
Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1
Description:
Automation Category: User Automation
Select Domain: division.domain — All OUs [Add OUs]

Tasks to automate
Specify the task you want to automate.

Automation Task/Policy: Inactive user cleanup

☑ Implement Business Workflow

Select objects
Select the objects on which the task would be performed - from report and/or CSV import.

From Report: Inactive Users
Select More

Execution Time
Specify the time/interval at which the task should be run.

Run at: Hourly For Each: 14 hrs

Notification
Notify the technician when the automation executes.

Enable Notification: off

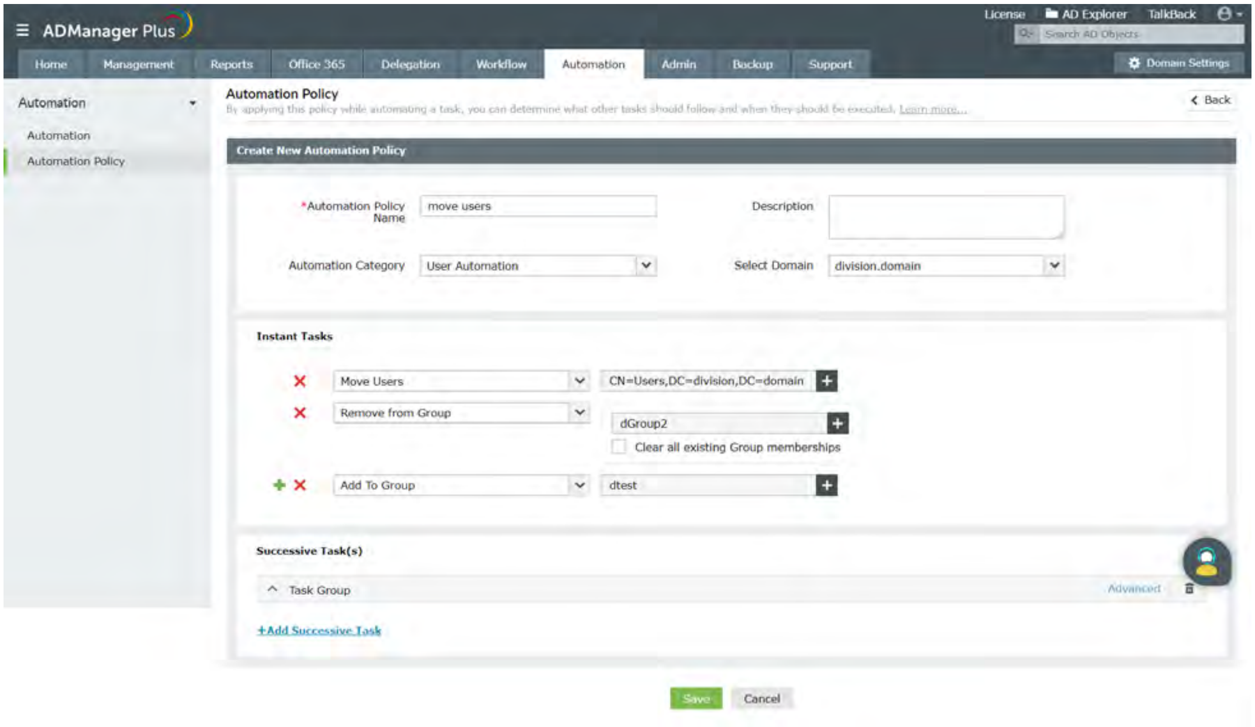
Exercise 3: Modify location specific user attributes using Automation Policy

Objective: To modify the group membership, OU, and other attributes of a user when they are relocated to a different team or to a different branch.

Such tasks need to be performed manually using native AD tools.
However in ADManager Plus, using Automation Policy we can add/remove group membership and move the users to different OUs quite easily.

Following are the steps that have to be performed to meet the above-mentioned requirements:

1. To create a new policy
   a. Click on the **Automation** tab.
   b. Click on the **Automation Policy** option available on the left pane and click on **Create New Policy**.
   c. Enter a suitable name and description for the automation policy. For instance, you can set the name of the automation policy to 'Moving users'.
   d. Select the **Domain** in which this automation policy must be used.
   e. Select **User Automation** as the category under which this policy must be listed.
   f. Under the **Instant Tasks** section,
      i. Select **Move Users** from the task list and select the **Container** to which you want to move the users.
      ii. Click on the **+** option next to the **Move Users** section to add another task.
      iii. Select the **Remove from Group** option from the task list and enable the **Clear all existing Group memberships**/select the groups from which you want to remove these users.
      iv. Click on the **+** option next to the **Remove from Group** section to add another task.
      v. Select the **Add to Group** option from the task list and select the required groups.
   g. **Save** this Automation Policy.



Automation Policy

By applying this policy while automating a task, you can determine what other tasks should follow and when they should be executed. Learn more...

*Automation Policy Name: move users

Description:

Automation Category: User Automation

Select Domain: division.domain

Move Users: CN=Users,DC=division,DC=domain

Remove from Group: dGroup2

□ Clear all existing Group memberships

Add To Group: dtest

2. To create an automation,
   a. Click on the **Automation** option available on the left pane.
   b. Click on **Create New Automation**.
   c. Give a suitable name and description for the automation.

d. Specify the **Domain** in which the automation must be run.

e. Select **User Automation** under the **Automation Category**.

f. Set the **Tasks to Automate** field to the automation policy that you just created (Moving users) that is specified under the **Automation Task/Policy** section.

g. You can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.

    i. From Reports:
    Click on the **Select** link and select the required report.

    ii. From a CSV:
    Click on the **Select More** link and specify the location of the CSV file in which the required user accounts are specified.

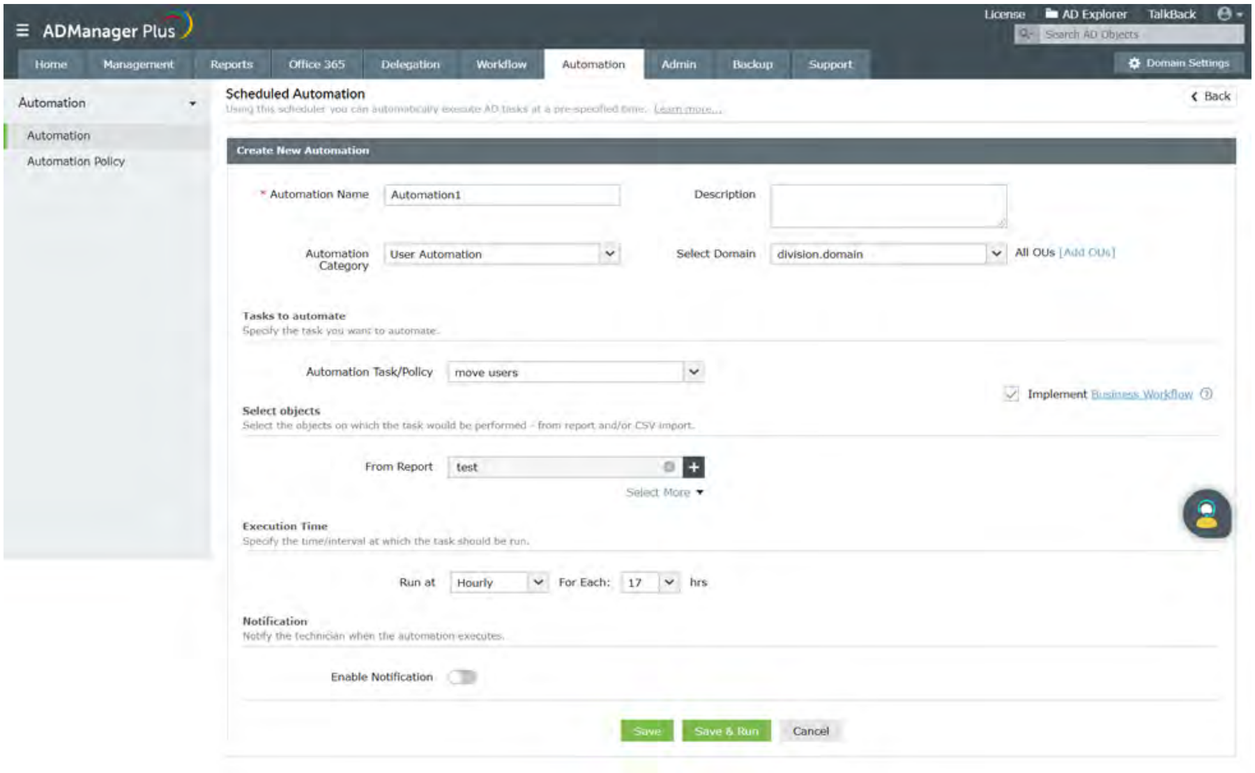
h. Select the **Implement Business Workflow** option, if you want to review or approve of every task before it is actually executed.

i. Specify the **Time Interval** at which the automation must be executed.

j. Specify the frequency for the automation to be repeated.

k. Enable notifications to be sent to either technicians or the administrator, whenever this automation is executed.

l. Click **Save** .



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: division.domain — All OUs [Add OUs]

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: move users

☑ Implement Business Workflow

Select objects

Select the objects on which the task would be performed - from report and/or CSV import.

From Report: test

Select More

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly — For Each: 17 hrs

Notification

Notify the technician when the automation executes.

Enable Notification

Exercise 4: Privileged Access Management

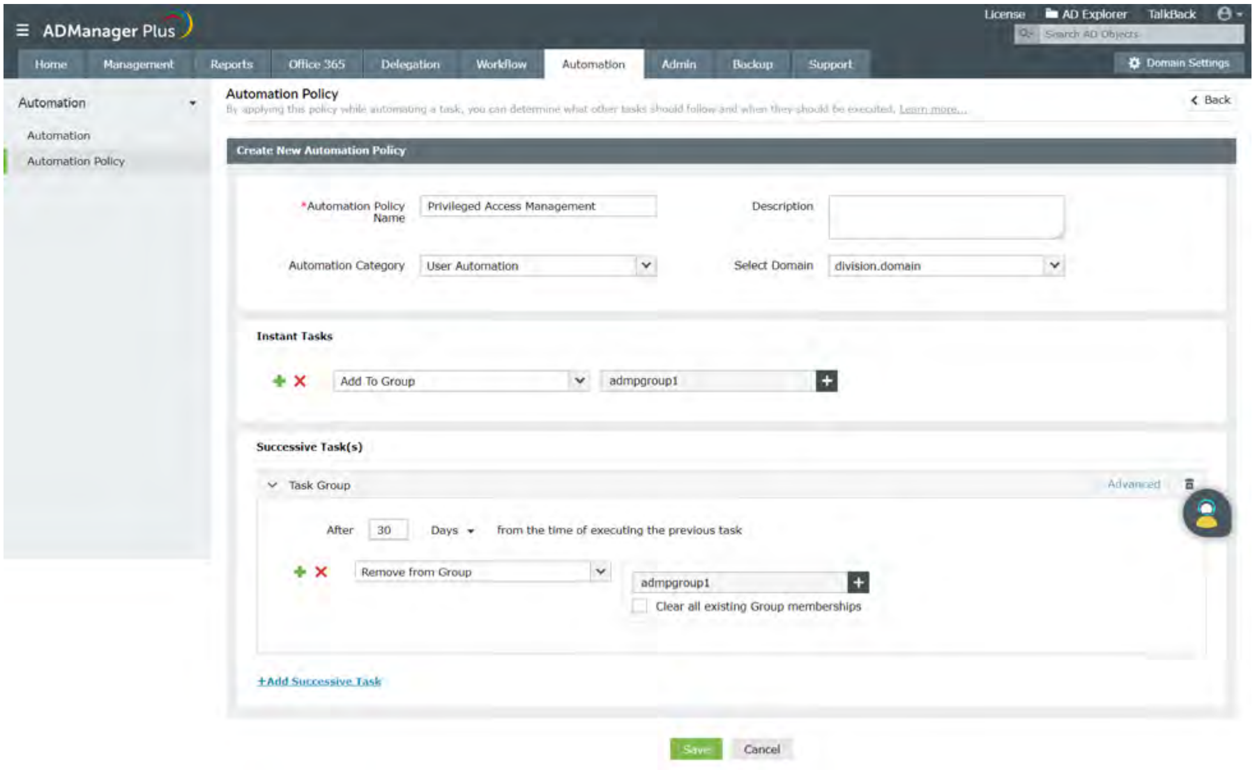
Scenario: Administrators might have to grant access to critical resources (say financial data) to specific users for a specific period of time to perform a particular task. This can easily be done by adding the required users to a group that already has the required privileges to access the critical resource.

However, there's a high chance that these users remain a member of these privileged groups, even after the required task is completed resulting in a security loophole. Such a scenario can jeopardize the security of your AD environment.

However, by using ADManager Plus, an admin can automate the process of adding and removing users from a specific group.

Follow the steps given below:

1. To create a new policy
    a. Click on the **Automation** tab.
    b. Click on the **Automation Policy** option available on the left pane and click on **Create New Policy**.
    c. Enter a suitable name and description for the automation policy. For instance, you can set the name of the automation policy to '**Privileged Access Management'**.
    d. Select the **Domain** in which this automation policy must be used.
    e. Select **User Automation** as the category under which this policy must be listed.
    f. Under the **Instant Tasks** section, select **Add to group** from the task list and select the **Group(s)** to which you want to add the users
    g. Under the **Successive Tasks** section, set the time limit (say **After 30 days**) and set the task to **Remove from Group**. Also select the group(s) from which you want to remove these users.
    h. **Save** this Automation Policy.



Automation Policy

By applying this policy while automating a task, you can determine what other tasks should follow and when they should be executed. Learn more...

Create New Automation Policy

*Automation Policy Name: Privileged Access Management

Description:

Automation Category: User Automation

Select Domain: division.domain

Instant Tasks

Add To Group — admpgroup1

Successive Task(s)

Task Group — Advanced

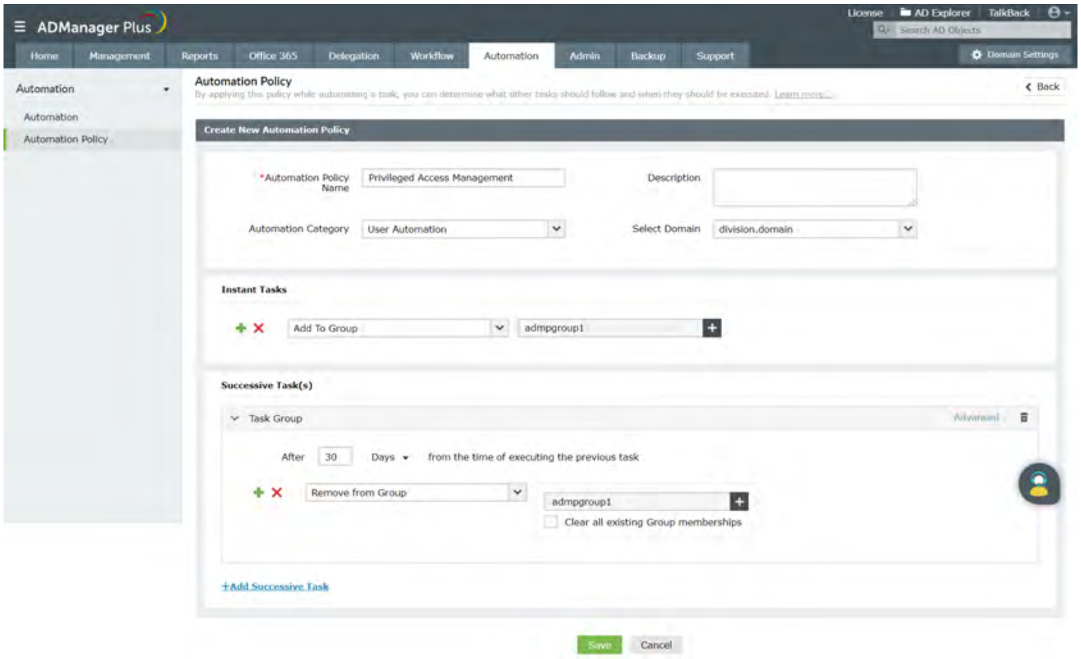
After 30 Days from the time of executing the previous task

Remove from Group — admpgroup1

□ Clear all existing Group memberships

2. To create an automation,
    a. Click on the **Automation** option available on the left pane.
    b. Click on **Create New Automation**.
    c. Give a suitable name and description for the automation.
    d. Specify the **Domain** in which the Automation must be run.
    e. Select **User Automation** under the **Automation Category**.
    f. Set the **Select Tasks to Automate** field to the automation policy that you just created (Privileged Access Management) that is specified under the **Automation Task/Policy** section.
    g. You can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.
        i. From Reports:
        Click on the **Select** link and select the required report. For this scenario, select the **Inactive Users** report from the reports list and specify the period of inactivity.
        ii. From a CSV:
        Click on the **Select More** link and specify the location of the CSV file in which the inactive user accounts are specified.
    h. Select the **Implement Business Workflow** option, if you want to review or approve of every task before it is actually executed.
    i. Specify the **Time Interval** at which the automation must be executed.
    j. Specify the frequency for the automation to be repeated.
    k. Enable notifications to be sent to either technicians or the administrator, whenever this automation is executed.

l. Click on **Save Automation**.



Automation Policy

By applying this policy while automating a task, you can determine what other tasks should follow and when they should be executed. Learn more...

Create New Automation Policy

*Automation Policy Name: Privileged Access Management

Description:

Automation Category: User Automation

Select Domain: division.domain

Instant Tasks

Add To Group: admpgroup1

Successive Task(s)

Task Group

After 30 Days from the time of executing the previous task

Remove from Group: admpgroup1

□ Clear all existing Group memberships

+Add Successive Task

Exercise 5: Automate service request

Scenario: In an environment with a lot of users who request to use VPN frequently, but are restricted by organizational policies, accessing and granting each such request is the IT admin's prerogative. By policy, VPN has to be disabled for all users, and the ones who want to access VPN must have to use a web page login and send a request.

With AD Manager Plus, such service requests can be written into a CSV file and then the relevant attributes can be modified for the particular account to enable VPN access. This process of granting access can also be automated by configuring an automation policy to run once every 30 minutes.

Exercise 6: Automate modification of group membership of users.

Scenario: A certain school would like to add a few users at the beginning of the academic year to certain groups and remove them from a few groups simultaneously (Modification of Group Membership). This exercise is intended to grant specific privileges to the students so that they can gain access to certain network shares containing relevant study materials.

This can be achieved through the automation option of ADManager Plus. In the **Automation Policy** section, admins can add and remove users over a configured period of time. The list of users is provided in a CSV file or even can be fetched through 'Enabled Users' report in 'User Reports' tab.

9. Business Workflow

The business workflow option lets you design a sequence for the execution of any AD task and also specify workflow agents. It takes care of intermediate hand offs and hand overs for you. Its repository of requests keep you updated on the status of the tasks at hand.

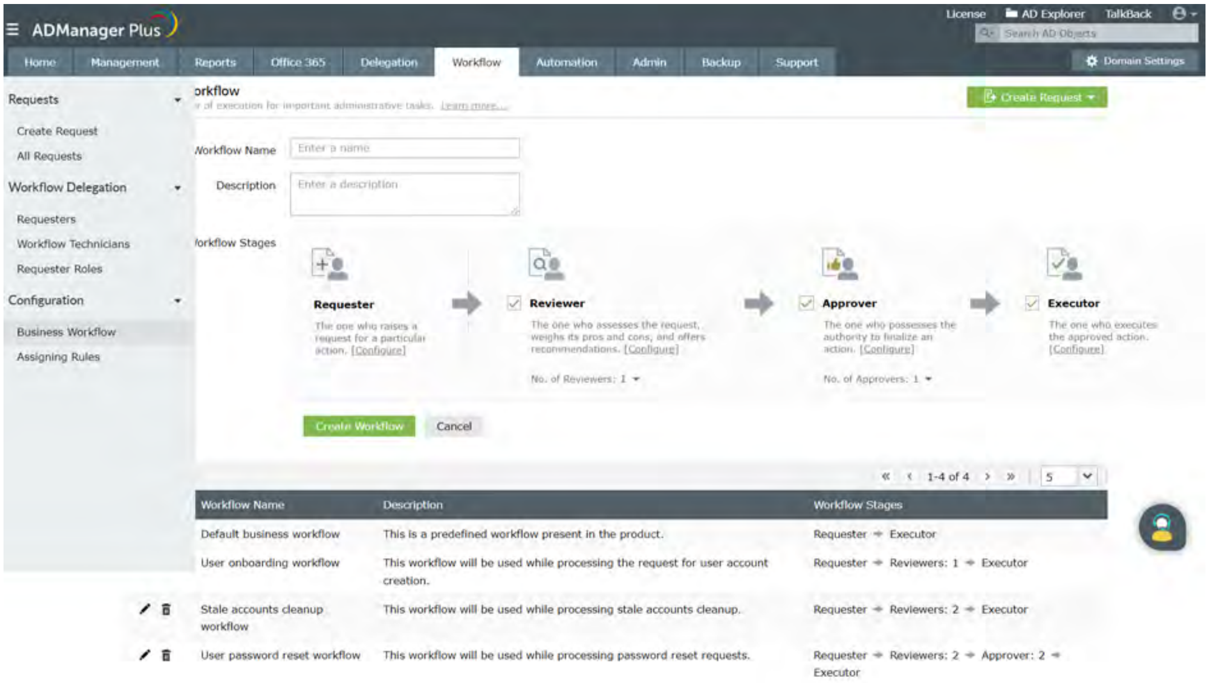
Consider a scenario where an IT technician creates user accounts for new employees, and wants the HR and the administrator to cross-check whether the details and the attribute values are right. In such a scenario, the technician will raise a request, enter all the details of the user, and create a workflow that includes the HR and administrator as the reviewer and approver respectively. Once the task is reviewed and approved, it can be executed either by the technician or by the administrator.

Exercise 1: On the HR's approval the Administrator has to disable a user(s)

Objective: Raise a request to disable a user or a set of users. The request has to be sent to the HR Manager for approval. Upon approval, the Administrator has to disable the users.

You cannot carry out such tasks with just the native AD interface. To achieve this, a workflow has to be created. Workflow can be set to a maximum of four levels – Requester, Reviewer, Approver, and Executor.

1. Creating a Workflow:
    a. Click on the **Workflow** tab and under the **Configuration** section, click on the **Business Workflow** option and then select the **Edit Workflow** option.
    b. Configure the appropriate user for every workflow stage.



orkflow

r of execution for important administrative tasks. Learn more...

Workflow Name: Enter a name

Description: Enter a description

Workflow Stages

Requester: The one who raises a request for a particular action. [Configure]

☑ **Reviewer**: The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure]

No. of Reviewers: 1

☑ **Approver**: The one who possesses the authority to finalize an action. [Configure]

No. of Approvers: 1

☑ **Executor**: The one who executes the approved action. [Configure]

Workflow Name	Description	Workflow Stages
Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
User onboarding workflow	This workflow will be used while processing the request for user account creation.	Requester → Reviewers: 1 → Executor
Stale accounts cleanup workflow	This workflow will be used while processing stale accounts cleanup.	Requester → Reviewers: 2 → Executor
User password reset workflow	This workflow will be used while processing password reset requests.	Requester → Reviewers: 2 → Approver: 2 → Executor

NOTE: Requesters raise requests for tasks, reviewers review the request and provide their comments, and based on the reviewers' comments, the approver approves the execution of the task. Once the approval is obtained, the Executor executes the task.

c. Click on the **Configure** option in each line to specify users for these roles.

2. For our exercise, we have to configure ‘Administrator’ as the Requester, ‘HR’ as the Approver, ‘Administrator’ as the Executor.
3. To disable the inactive users after approval from the HR
   a. Click on the**Reports** tab and click on the **Inactive Users** report located under the **User Reports** section.
   b. **Generate** the Inactive Users report.
   c. Select the required users and click on **Create Request** and set the **Task** field to **Disable Users**.
   d. The HR will see the requests in his requests list and review and approve it. 8. Since the administrator is not configured as an approver, he cannot approve the request.
   e. Once the ‘HR’ approves, the Administrator will execute the task by clicking on the request and clicking on the **Execute** button.

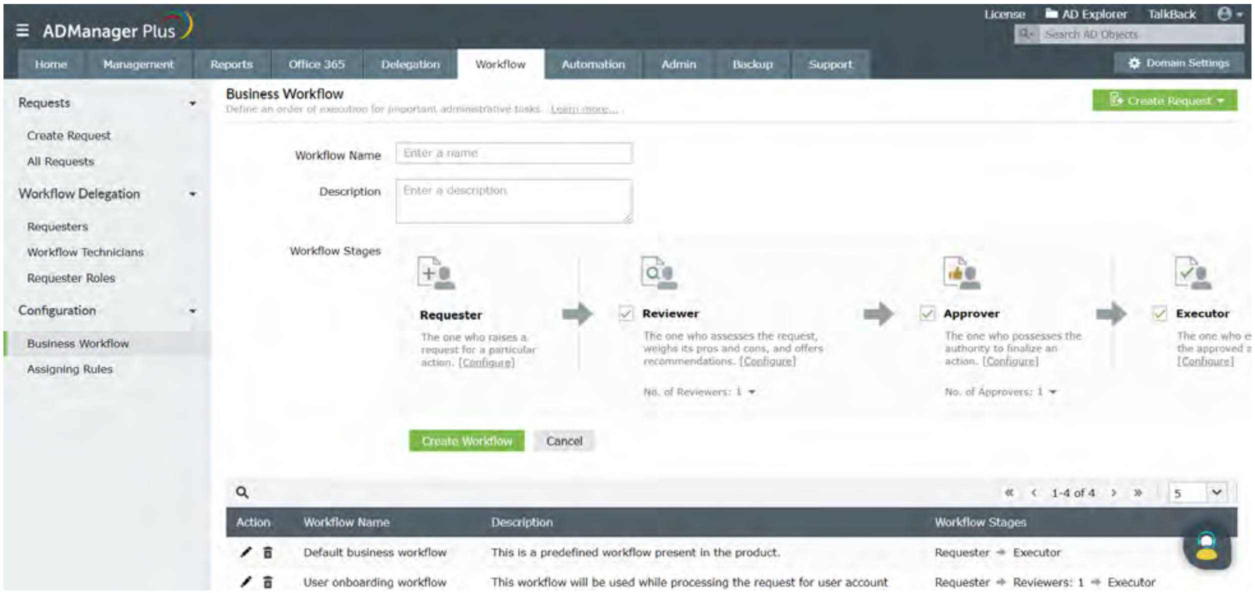
Exercise 2: Workflow based User Accounts Creation

Scenario: Whenever new employees join the organization, the HR executives send the details of all the new employees to their administrator to create new user accounts in the domain of their organization. Instead of this, it would minimize the workload of the administrator if the HR executives can key in the details of all the new user accounts (for the new employees) to be created and just send a request to the concerned IT or help desk technician who can then create the new accounts with the details already entered.

You can accomplish this using the ‘Workflow’ feature of ADManager Plus by:
-Creating a workflow as per your organizational requirements.
- Assigning the ‘requester’ role to HR Executives to enable them to create user creation requests.
- Assigning the ‘executor’ rights to the appropriate technicians from the IT team to empower them to create new users in AD.

Steps to create users through the workflow:

1. Click on the **Workflow** tab.
2. Click on the Business Workflow option located under the **Configuration** section. Enter a **Name** and a **Description** for the new workflow.
3. Configure the the **Workflow Stages** and assign the number of technicians for each role configured in the workflow.For this case, you may choose the Requester, Reviewer and Executor roles.
4. Click **Create Workflow.**



Business Workflow

Define an order of execution for important administrative tasks. Learn more...

Workflow Name: Enter a name

Description: Enter a description

Workflow Stages:

Requester – The one who raises a request for a particular action. [Configure]

☑ Reviewer – The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure] No. of Reviewers: 1

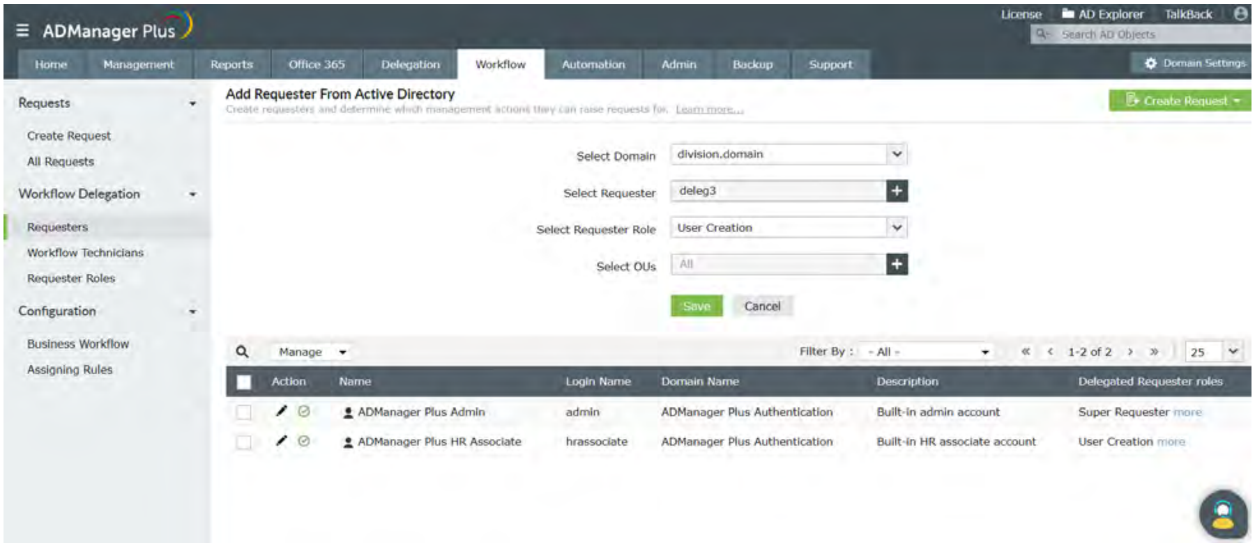
☑ Approver – The one who possesses the authority to finalize an action. [Configure] No. of Approvers: 1

☑ Executor – The one who e the approved a [Configure]

Action	Workflow Name	Description	Workflow Stages
✎ 🗑	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
✎ 🗑	User onboarding workflow	This workflow will be used while processing the request for user account	Requester → Reviewers: 1 → Executor

5. To assign the requester role to HR executives:
    a. Go to the **Workflow Delegation** section and click on **Requesters**.
    b. Click on **Add New Requester** option and select the **Domain** which you would like to create this requester.
    c. Click on **Browse** beside the **Select requester** option and select the appropriate HR executive to whom you wish to assign the ‘requester’ role.You can assign to individual users or even groups and OUs as a whole. Whenever a user is added to an OU or Group with the requester permission, the user automatically gets the required permissions to raise user creation requests.
    d. In the **Select Requester Role** field, choose **User Creation**.
    e. Select the OUs in which the HR executive can raise user creation requests using the **Add OUs** option.

f. **Save** this requester.



Add Requester From Active Directory

Create requesters and determine which management actions they can raise requests for. Learn more...

Select Domain: division.domain

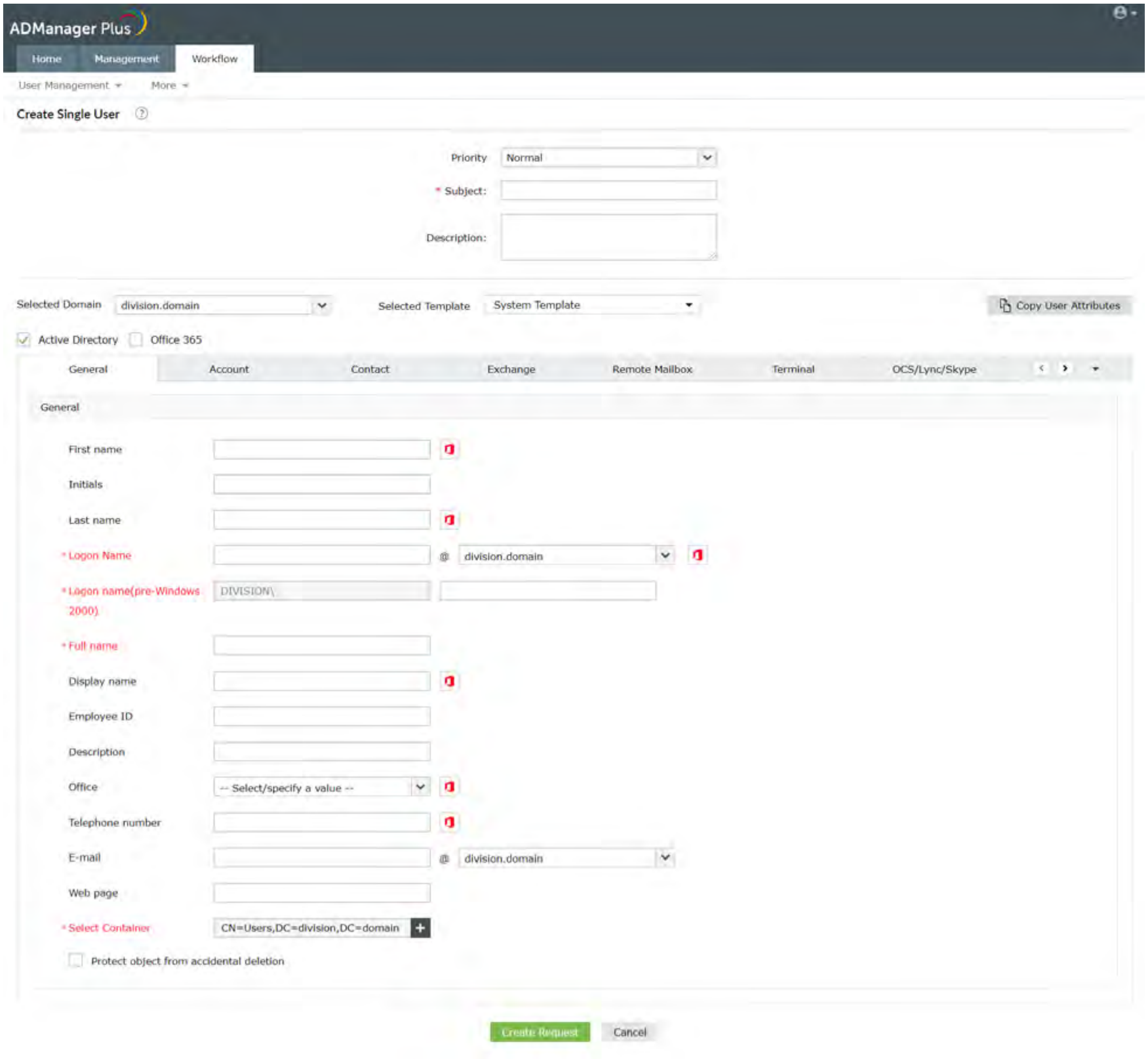
Select Requester: deleg3

Select Requester Role: User Creation

Select OUs: All

□	Action	Name	Login Name	Domain Name	Description	Delegated Requester roles
□		ADManager Plus Admin	admin	ADManager Plus Authentication	Built-in admin account	Super Requester more
□		ADManager Plus HR Associate	hrassociate	ADManager Plus Authentication	Built-in HR associate account	User Creation more

6. To create ‘executors’ who can create new user accounts in AD:
    a. Go to the **Workflow Delegation** section and click on **Workflow Technicians**.
    b. Click on **Add** and select the required technicians from the list of all available technicians in the domain and add the executor role to them.
    c. Click **Assign** to add the selected technicians to the ‘Executors’ list.
7. To raise a request for new user account creation:
    a. Login to ADManager Plus using the credentials of the requester and click on the **Workflow** tab.
    b. Click on the **All Requests** option and click on **Create Request.**
    c. In the **User Creation** section, select the **Single User Creation** or **Bulk User Creation** tasks based on your requirement.
        i. For single user creation:
            1. Select the **Domain** in which the user account has to be created.
            2. Choose the appropriate **Template**.
            3. Enter the values for all the necessary attributes.
            4. Click on the **Create Request** button to complete the request creation process.
        ii. Bulk user Creation:
            1. Select the required **Domain**.
            2. Choose the appropriate **Template**.
            3. Use the **Add Users** option to enter the values for each user account one after the other or just import a CSV file which has the details of all the new user accounts to be created. Click on **Next**.
            4. Select the required **Container** or create a new container (OU) if required.
            5. Click on **Create Request** to complete the user creation request.



Create Single User

Priority: Normal

* Subject:

Description:

Selected Domain: division.domain

Selected Template: System Template

☑ Active Directory □ Office 365

General

First name

Initials

Last name

* Logon Name @ division.domain

* Logon name(pre-Windows 2000): DIVISION\

* Full name

Display name

Employee ID

Description

Office: -- Select/specify a value --

Telephone number

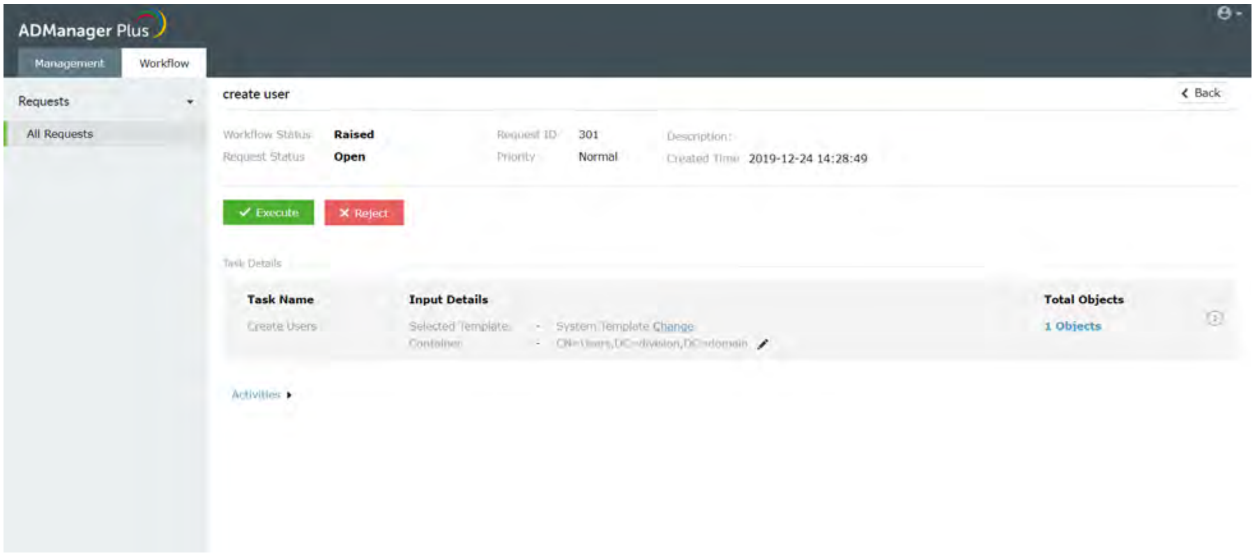
E-mail @ division.domain

Web page

* Select Container: CN=Users,DC=division,DC=domain

□ Protect object from accidental deletion

8. To execute the user creation request:
   a. Login to ADManager Plus using the credentials of the technician with the ‘execute’ role.
   b. Click on the **Workflow** tab and click on **All Requests**.
   c. In the requests list, go to **My Requests** and click on the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also click on the number displayed in ‘Awaiting for Execution’ located just above the list of requests to view all tasks queued up for execution).
   d. Select the ‘user creation’ task raised by the HR executive.
   e. **Execute** this task to complete the process of creating new users in AD.



create user

Workflow Status: **Raised**
Request Status: **Open**
Request ID: 301
Priority: Normal
Description:
Created Time: 2019-12-24 14:28:49

Task Details

Task Name	Input Details			Total Objects
Create Users	Selected Template	-	System Template Change	1 Objects
	Container	-	CN=Users,DC=division,DC=domain	

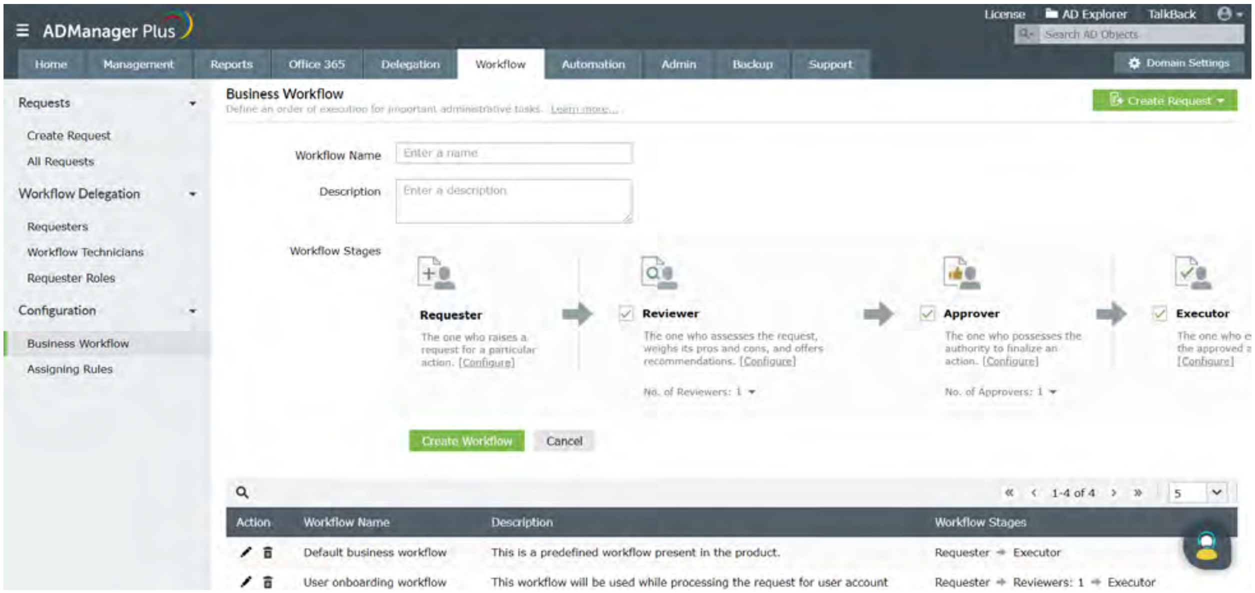
Exercise 3: Workflow based disabling of inactive user accounts

Scenario: As a part of your organizational security measures, your AD technician/administrator has to disable user accounts that have been inactive for a certain period of time (say 90 days). But before disabling user accounts the administrator must send the list of inactive user accounts to the HR manager for review. After the HR manager gives the go ahead the administrator can disable the inactive user accounts.

This can be accomplished using the components in the **Workflow** feature by:
- Creating a 3 level workflow with: Requester, Reviewer and Executor.
- Add the appropriate users/technicians to the Requester, Reviewer and Executor roles.
- Once the requester creates the request to disable user accounts, the reviewer verifies the users list and approves it. Then, the executor can disable the specified user accounts.
- Create 'Assigning Rules' to automatically assign the tasks to appropriate technicians/users as soon as a request is created or reviewed.

Steps to disable inactive user accounts based on workflow approval:

1. To create a customized workflow.
    a. Click on the **Workflow** tab.
    b. Under the **Configuration** section, click on the **Business Workflow** option,
    c. Enter a **Name** and a **Description** for the new workflow.
    d. Configure the the **Workflow Stages** and assign the number of technicians for each role configured in the workflow.For this case, you may choose the Requester, Reviewer and Executor roles.
    e. Click **Create Workflow.**.



Business Workflow

Define an order of execution for important administrative tasks. Learn more...

Workflow Name: Enter a name

Description: Enter a description

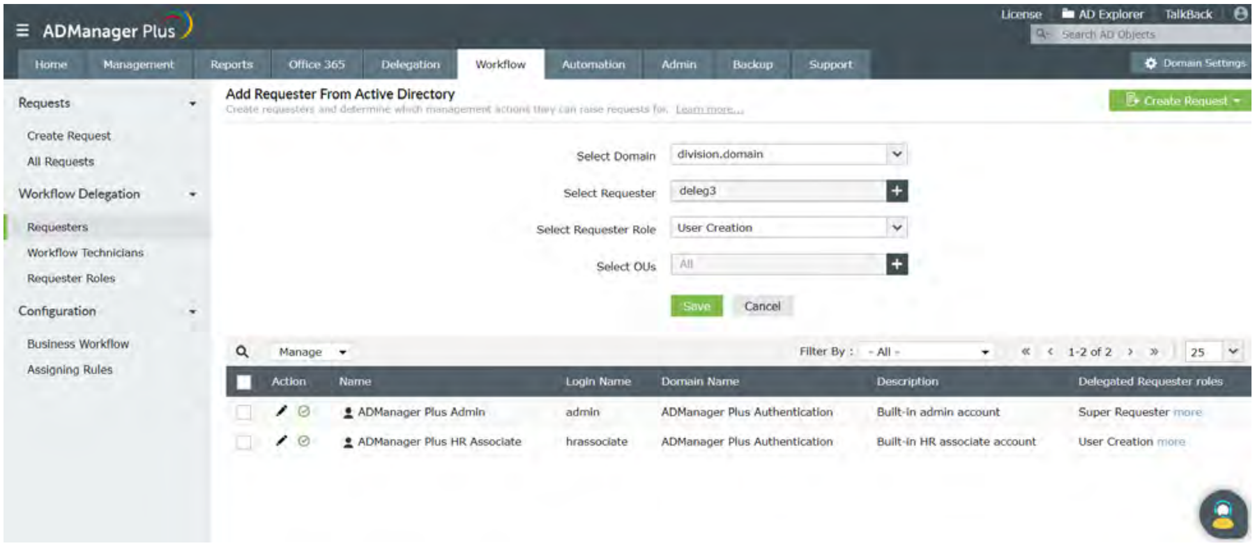
Workflow Stages

- **Requester** The one who raises a request for a particular action. [Configure]
- ☑ **Reviewer** The one who assesses the request, weighs its pros and cons, and offers recommendations. [Configure] No. of Reviewers: 1
- ☑ **Approver** The one who possesses the authority to finalize an action. [Configure] No. of Approvers: 1
- ☑ **Executor** The one who e the approved a [Configure]

1-4 of 4 | 5

Action	Workflow Name	Description	Workflow Stages
	Default business workflow	This is a predefined workflow present in the product.	Requester → Executor
	User onboarding workflow	This workflow will be used while processing the request for user account	Requester → Reviewers: 1 → Executor

2. To add requesters:
    a. Go to the **Workflow Delegation** section and click on **Requesters**.
    b. Click on **Add New Requester** option and select the **Domain** which you would like to create this requester.
    c. Click on **Browse** beside the **Select requester** option and select the user or technician to whom you wish to assign the ‘requester’ role. Whenever a user is added to an OU or Group with the requester permission, the user automatically gets the required permissions to raise user creation requests.
    d. In the **Select Requester Role** field, choose **User Creation**.
    e. Select the OUs in which the technicians can raise user creation requests using the **Add OUs** option.
    f. **Save** this requester.



Add Requester From Active Directory

Create requesters and determine which management actions they can raise requests for. Learn more...

Select Domain: division.domain

Select Requester: deleg3

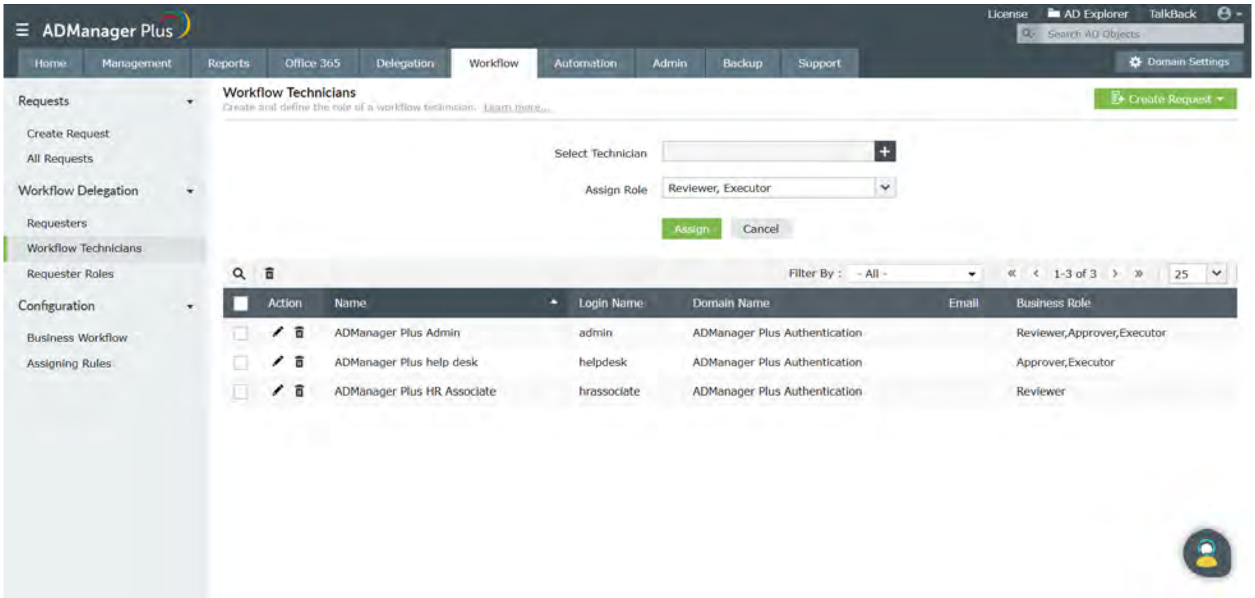
Select Requester Role: User Creation

Select OUs: All

Filter By : - All - | 1-2 of 2 | 25

□	Action	Name	Login Name	Domain Name	Description	Delegated Requester roles
□		ADManager Plus Admin	admin	ADManager Plus Authentication	Built-in admin account	Super Requester more
□		ADManager Plus HR Associate	hrassociate	ADManager Plus Authentication	Built-in HR associate account	User Creation more

3. To create ‘reviewers' and 'Executors’ who can create new user accounts in AD:
    a. Go to the **Workflow Delegation** section and click on **Workflow Technicians**.
    b. Click on **Add New technician** and select the required technician from the list of all available technicians in the domain. Assign the required roles.
    c. Click **Assign** to add the selected technicians.



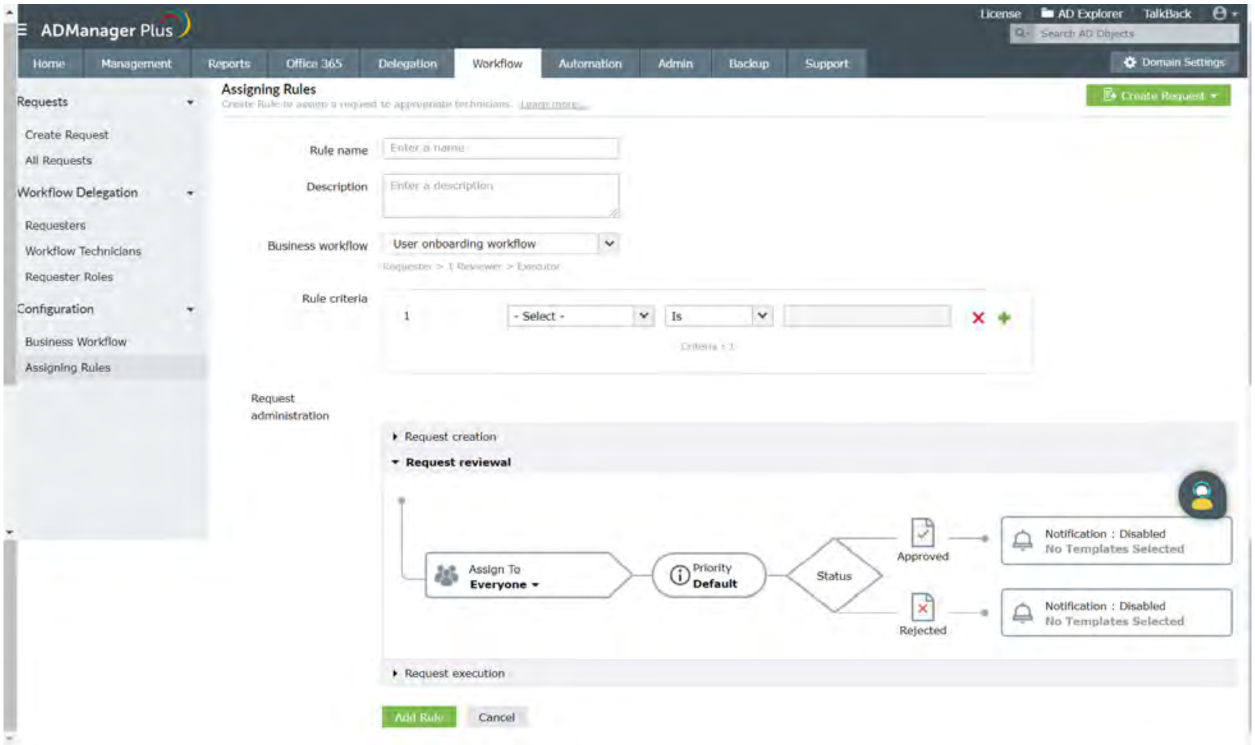
Workflow Technicians
Create and define the role of a workflow technician. Learn more...

Select Technician
Assign Role: Reviewer, Executor

Filter By : - All -   1-3 of 3   25

Action	Name	Login Name	Domain Name	Email	Business Role
	ADManager Plus Admin	admin	ADManager Plus Authentication		Reviewer,Approver,Executor
	ADManager Plus help desk	helpdesk	ADManager Plus Authentication		Approver,Executor
	ADManager Plus HR Associate	hrassociate	ADManager Plus Authentication		Reviewer

4. To create rules that help assign the requests to appropriate users/technicians after creation and review:
    a. Click on the **Workflow** tab.
    b. Click on **Assigning Rules** and click on the **Add New Rule** option.
    c. Specify a name for the rule: **Disable Inactive Users**
    d. Choose the **Bussiness workflow** you created earlier.
    e. Set the **Rule Criteria** field value to **Action Is Disable Users**.
    f. Under the **Request reviewal** section,
        i. Click on the edit option given next to **Assign To** and choose the appropriate technician to whom the reviewal task should be assigned.
        ii. **Set the Priority to Normal (since this is a routine task).**
        iii. Enable notifications to be sent to the required technician whenever the given task is approved or rejected.



Assigning Rules

Create Rule to assign a request to appropriate technicians. Learn more...

Rule name: Enter a name

Description: Enter a description

Business workflow: User onboarding workflow

Requester > 1 Reviewer > Executor

Rule criteria: 1 - Select - Is

Criteria : 1

Request administration

Assign To: Everyone

Priority: Default

Notification : Disabled
No Templates Selected

Notification : Disabled
No Templates Selected

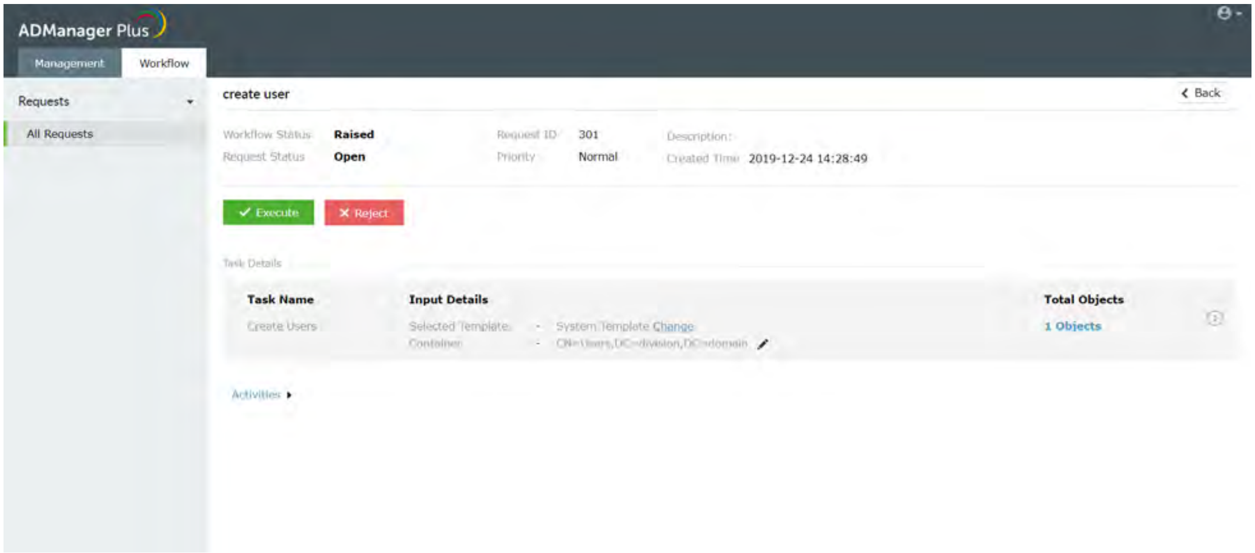
g. Under the **Request execution** section,
   i. Click on the edit option given next to **Assign To** and choose the appropriate technician to whom the execution task should be assigned.
   ii. Set the **Priority** to **Normal** (since this is a routine task).
   iii. Enable notifications to be sent to the required technician whenever the given task is approved or rejected.

h. Click on **Add Rule**.

5. To create the ‘disable user’ request:
   a. Login to ADManager Plus using the credentials of the technician.
   b. Click on **Reports** tab and click on the **Inactive Users** report.
   c. **Generate** this report for the desired period (in this case: 90 days) for the required domain.
   d. Select all the users and click on **Create Request** and enter **Disable Users** in Request Action.
   e. Based on the **Disable Inactive Users** assignment rule, this request will be assigned to the appropriate technician.
6. To review the 'disable user' request:
   a. Login to ADManager Plus using the credentials of the technician with the ‘reviewer’ role.
   b. Click on the **Workflow** tab and click on **All Requests**.
   c. In the requests list, go to **My Requests** and click on the **Awaiting for Review** option to view the list of all requests waiting for review. (You can also click on the number displayed in ‘Awaiting for review’ located just above the list of requests to view all tasks queued up for review).

    d. Select the ‘disable user’ task and click on the **View Objects** to view the details of the object.
    e. **Review** this task.

7. To execute the 'disable user' request:
    a. Login to ADManager Plus using the credentials of the technician with the ‘approver’ role.
    b. Click on the **Workflow** tab and click on **All Requests**.
    c. In the requests list, go to **My Requests** and click on the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also click on the number displayed in ‘Awaiting for execution’ located just above the list of requests to view all tasks queued up for review).
    d. Select the ‘disable user’ task and click on the **View Objects** to view the details of the object.
    e. **Execute** this task.



create user

Workflow Status: Raised
Request Status: Open
Request ID: 301
Priority: Normal
Description:
Created Time: 2019-12-24 14:28:49

Task Details

Task Name	Input Details			Total Objects
Create Users	Selected Template	-	System Template Change	1 Objects
	Container	-	CN=Users,DC=division,DC=domain	

Exercise 4: Manager-based workflow

Objective: To add a user to a group only after obtaining the approval from the user's manager.

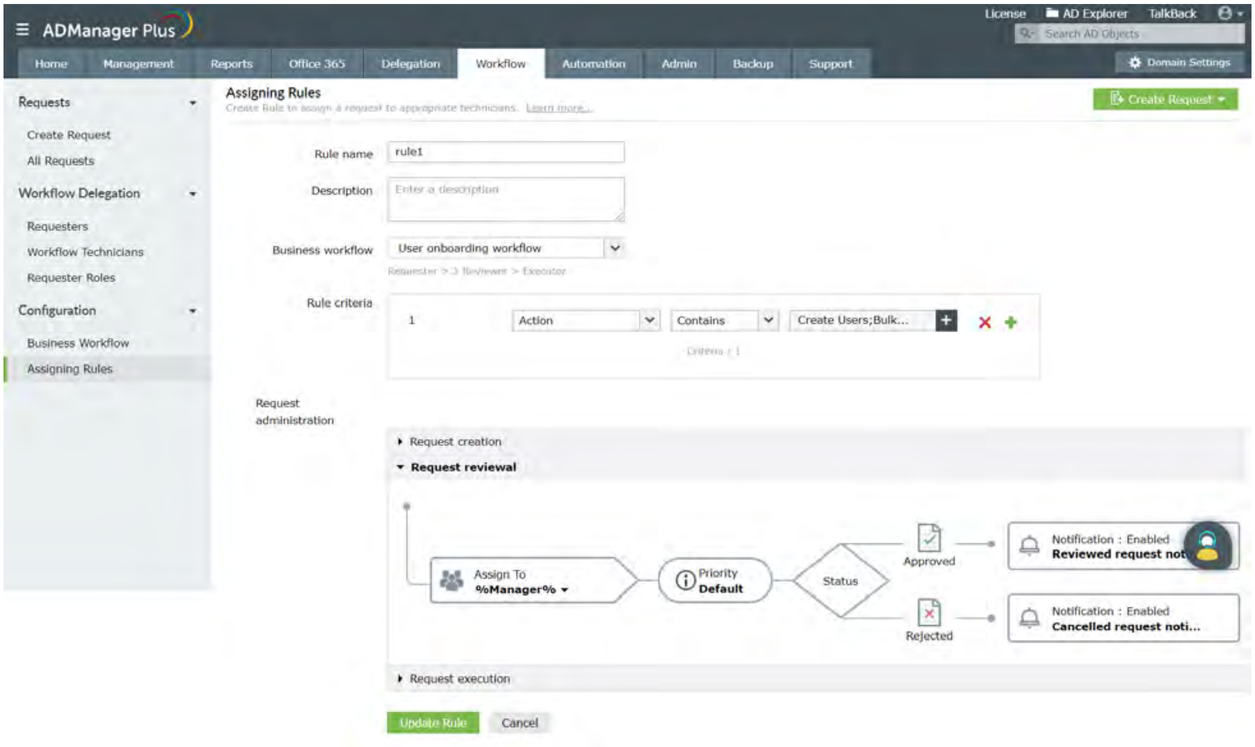
Follow the steps given below to accomplish the given objective:

1. Add the manager as a help desk technician.
2. Delegate the required role to the manager.
3. Click on the **Workflow** tab and create a business workflow that has the requester, approver, executor roles.
    a. Click on the **Assigning Rules** option, and click on **Add New Rule**.
    b. Specify the name and description of the rule.
    c. Select the business workflow that you just created.
    d. Under the **Request Approval** section, click on the edit option located next to the

Assigned To option and click on the **%Manager%** option. Set the priority of the task.

e. Similarly, assign the task to the required executor.

f. Click on **Save**.



Assigning Rules

Create Rule to assign a request to appropriate technicians. Learn more...

Rule name: rule1

Description: Enter a description

Business workflow: User onboarding workflow

Requester > 3 Reviewer > Executor

Rule criteria: 1 Action Contains Create Users;Bulk...

Criteria : 1

Request administration

Assign To %Manager%

Priority Default

Notification : Enabled Reviewed request not

Notification : Enabled Cancelled request noti...

4. Create a request for adding a user to a group. The request will be assigned to the manager of that user automatically.

5. To approve the 'add to group' request:

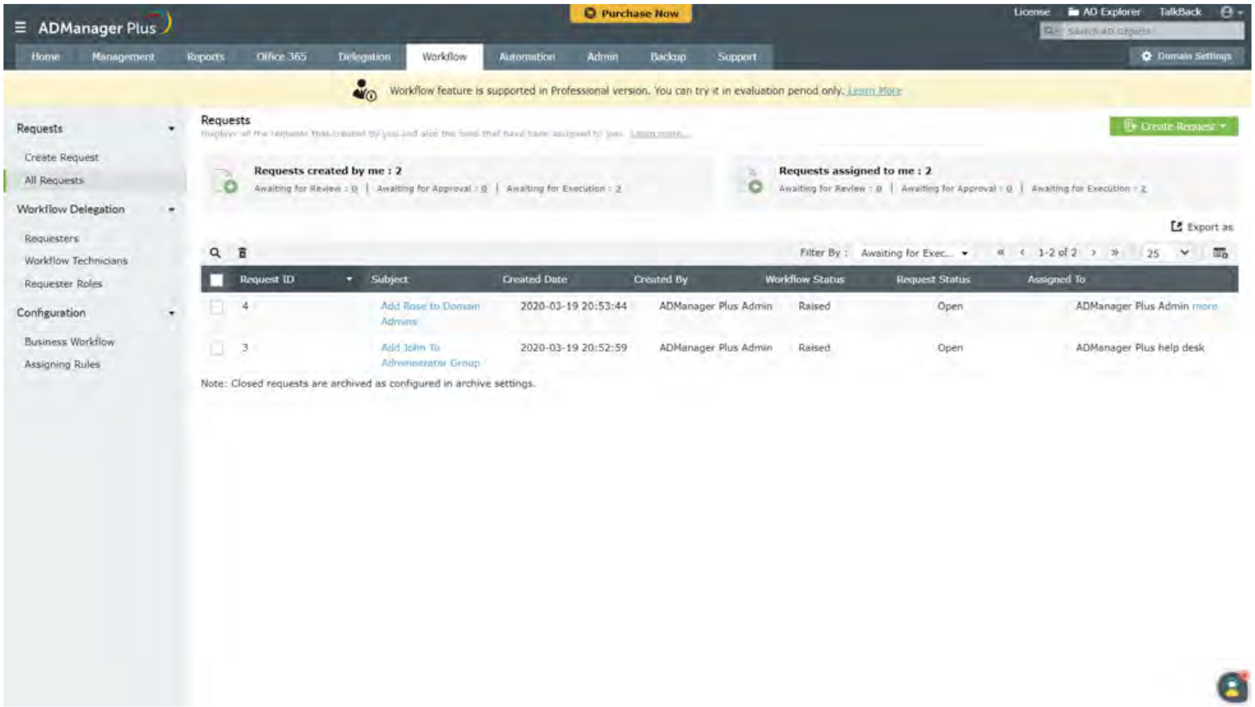
   a. Login to ADManager Plus using the credentials of the manager.

   a. Click on the **Workflow** tab and click on **All Requests**.

   b. In the requests list, go to **My Requests** and click on the **Awaiting for Approval** option to view the list of all requests waiting for execution. (You can also click on the number displayed in 'Awaiting for approval' located just above the list of requests to view all tasks queued up for review).

   c. Select the 'add to group' task and click on the **View Objects** to view the details of the object.

   d. **Approve** this task.



Workflow feature is supported in Professional version. You can try it in evaluation period only. Learn More

Requests

Displays all the requests that created by you and also the ones that have been assigned to you. Learn more...

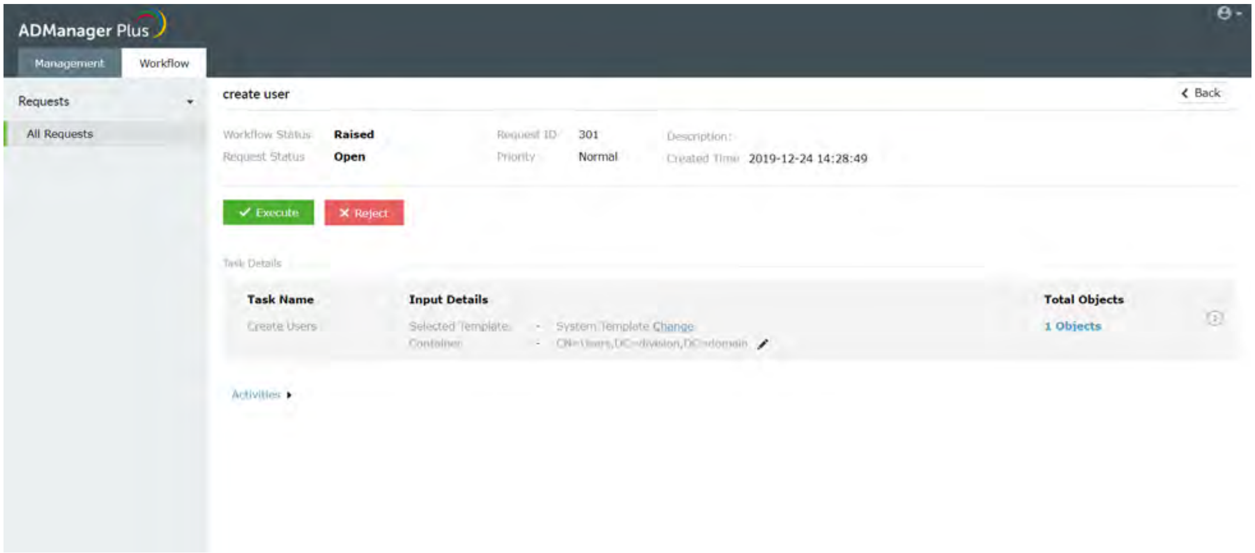
Requests created by me : 2
Awaiting for Review : 0 | Awaiting for Approval : 0 | Awaiting for Execution : 2

Requests assigned to me : 2
Awaiting for Review : 0 | Awaiting for Approval : 0 | Awaiting for Execution : 2

Request ID	Subject	Created Date	Created By	Workflow Status	Request Status	Assigned To
4	Add Rose to Domain Admins	2020-03-19 20:53:44	ADManager Plus Admin	Raised	Open	ADManager Plus Admin more
3	Add John To Administrator Group	2020-03-19 20:52:59	ADManager Plus Admin	Raised	Open	ADManager Plus help desk

Note: Closed requests are archived as configured in archive settings.

6. To execute the 'add to group' request:
   a. Login to ADManager Plus using the credentials of the technician with the ‘approver’ role.
   b. Click on the **Workflow** tab and click on **All Requests**.
   c. In the requests list, go to **My Requests** and click on the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also click on the number displayed in ‘Awaiting for execution’ located just above the list of requests to view all tasks queued up for review).
   d. Select the ‘add to group’ task and click on the **View Objects** to view the details of the object.
   a. **Execute** this task.



create user

Workflow Status: **Raised**
Request Status: **Open**
Request ID: 301
Priority: Normal
Description:
Created Time: 2019-12-24 14:28:49

Task Details

Task Name	Input Details		Total Objects
Create Users	Selected Template Container	- System Template Change - CN=Users,DC=division,DC=domain	1 Objects

10. Integration

ADManager Plus' integration capabilities were developed with a need to break the barrier between multiple administration tools. It offers integration with important IT applications such as help desk applications, HRMS, databases used by HR applications, password self-service management tools, and SIEM tools.

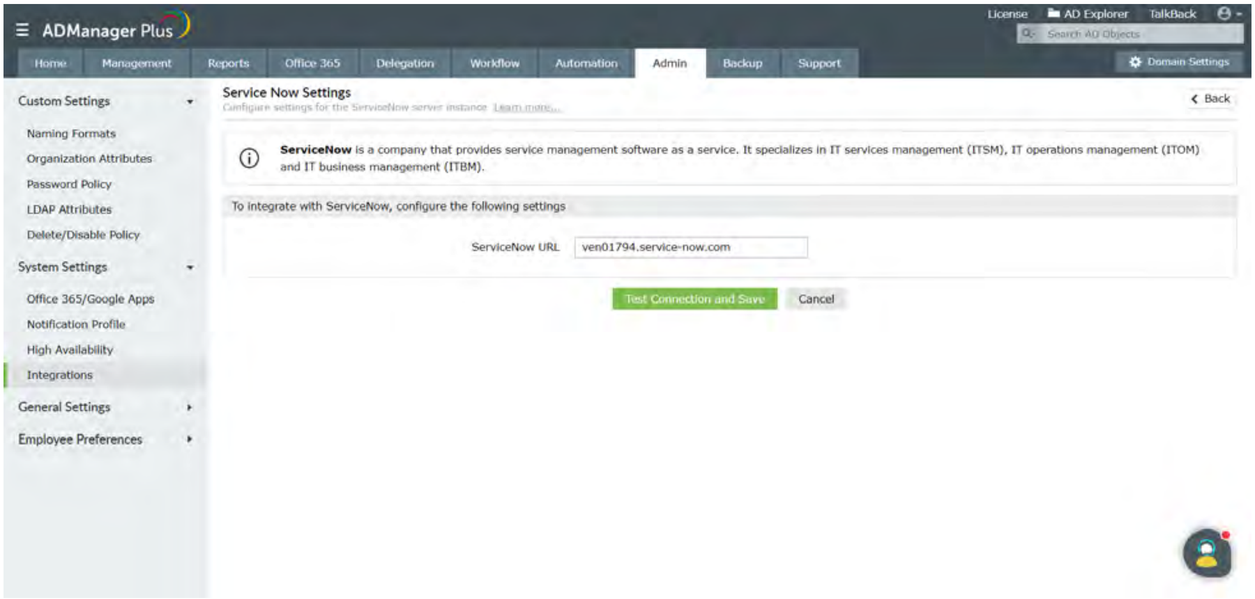
The exercises below focus on the most commonly performed Active Directory management tasks and how integrating ADManager Plus with other applications helps you get them all done from one place.

Exercise 1: Create an Active Directory user account using ServiceNow

Objective: Integrate ADManager plus with ServiceNow and provision an AD user.

Solution:

1. Steps to configure ServiceNow in ADManager Plus
    a. Navigate to the **Admin** tab.
    b. On the left pane of the window, under **System Settings**, choose **Integrations**.
    c. Under applications, click **ServiceNow**.
    d. The **Click to configure** button will guide you to the configuration page.
    e. Enter the ServiceNow web service URL in the **ServiceNow URL** field.
    f. Click **Test Connection and Save** to save your configuration settings.



Service Now Settings

Configure settings for the ServiceNow server instance Learn more...

ServiceNow is a company that provides service management software as a service. It specializes in IT services management (ITSM), IT operations management (ITOM) and IT business management (ITBM).

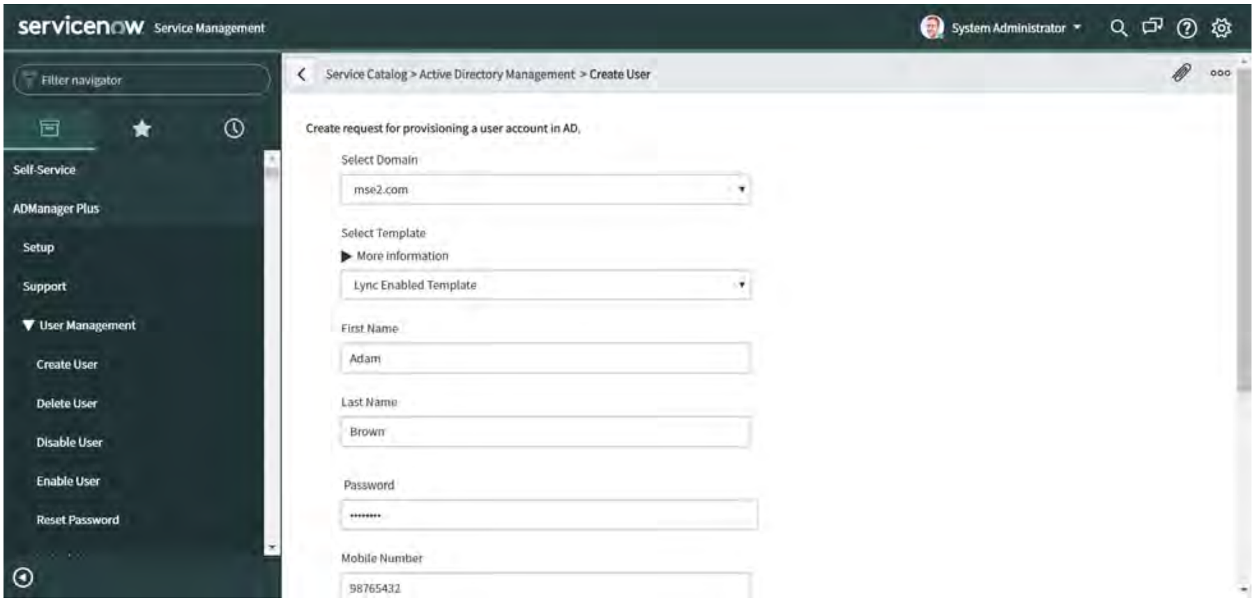
To integrate with ServiceNow, configure the following settings

ServiceNow URL: ven01794.service-now.com

2. Steps to perform user provisioning in ServiceNow

Prerequisites : You should be a ServiceNow customer, and should have installed the ADManager Plugin in ServiceNow.

a. After logging into ServiceNow, on the left side of the window, select the **setup** option under **ADManager Plus**.
b. Enter the **Server Name**, **Port Number** and the **MID Server Name** if ADManager Plus is running on an internal network. For more details about configuring a MID server, go here.
c. Next, enter your ADManager Plus **username** and **password**.
d. Click **Submit.**
e. Depnding upon the roles delegated to you, various Active Directory management actions will be visible on the left pane of the window.
f. Select **Create user**.
g. Select the **domain** where the user is to be created. You can also choose the user provisioning templates, fetched from ADManager Plus. You can also create your own templates in ADManager Plus. Check out this page for further guidance.
h. Add the **First Name**, **Last Name, Password, Manager**, etc. Based on the template used, the other attributes will be populated automatically.
i. Click **submit**.



Service Catalog > Active Directory Management > Create User

Create request for provisioning a user account in AD.

Select Domain: mse2.com

Select Template
▶ More information
Lync Enabled Template

First Name: Adam

Last Name: Brown

Password: ••••••••

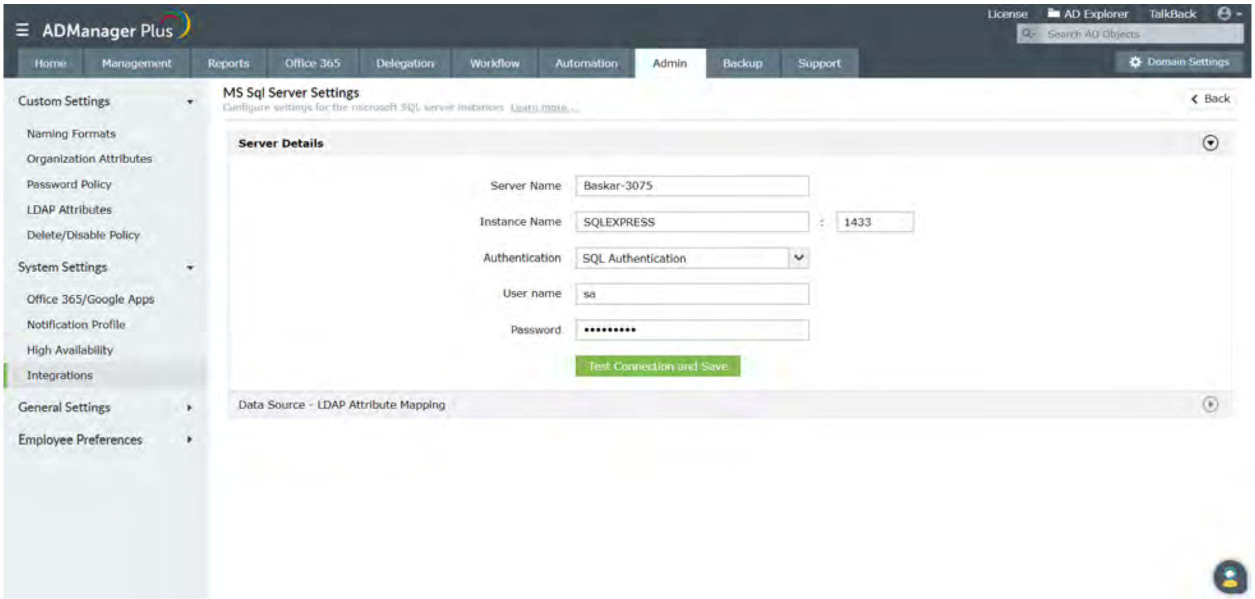
Mobile Number: 98765432

Exercise 2: Automate user modification from the MS SQL database, integrated with ADManager Plus.

Objective : Integrate ADManager Plus with MS SQL database and modify a user with automation.

Solution:

1. Steps to configure MS SQL in ADManager Plus
    a. Go to the **Admin** tab.
    b. On the left pane of the window, under **System Settings**, choose **Integrations**.
    c. Under Database, click **MS SQL Server**.
    d. The **Click to configure** button will guide you to the configuration page.
    e. Enter the **Server Name**, **Instance Name** and **Port Number** of the MS SQL server.
    f. Select the **Authentication type** and enter the **Domain name**, **Username** and the **Password** for authentication.
    g. Click on **Test Connection and Save** button to save your configuration settings.
    h. Under **Data Source - LDAP attribute and mapping**, click on **Add New Configuration**. Map the Active Directory LDAP attributes to the predefined Database Column name provided in the MS SQL database. For example, if you want to map the 'givenName' attribute in Active Directory to the 'First_Name' attribute in the MS SQL database, you can do so by selecting them under the respective drop down menu on either side of the '=' in the **Attribute Mapping** tab. Multiple attributes can be mapped similarly.



MS Sql Server Settings

Configure settings for the microsoft SQL server instances Learn more...

Server Details

Server Name: Baskar-3075

Instance Name: SQLEXPRESS : 1433

Authentication: SQL Authentication

User name: sa

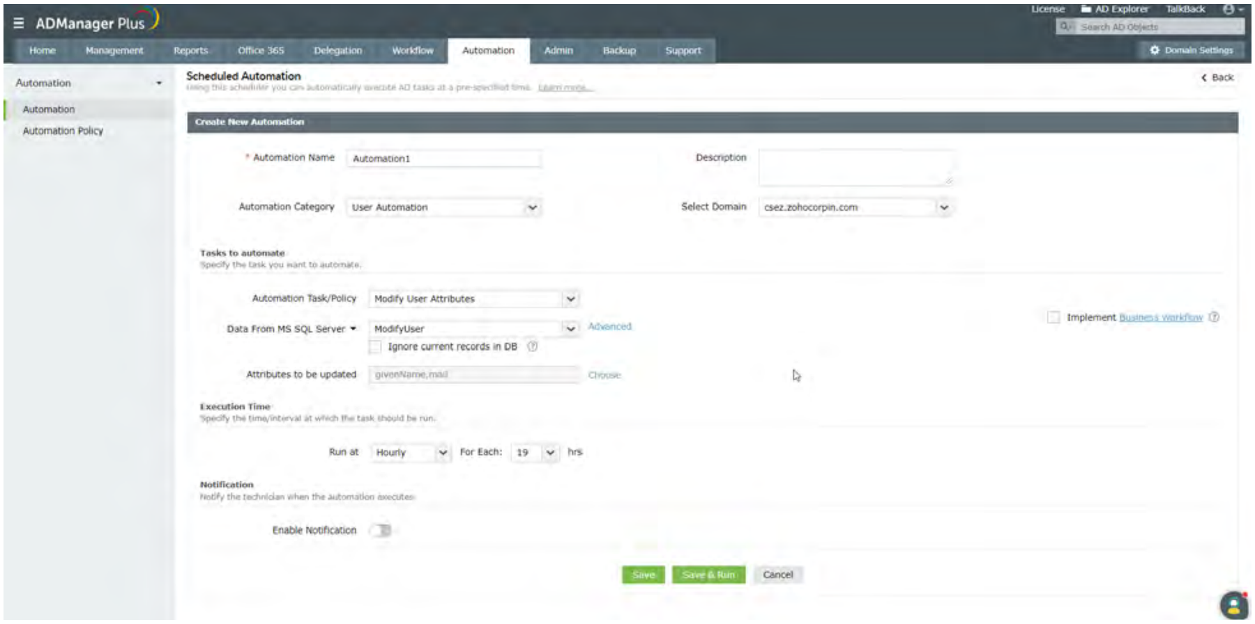
Password: •••••••••

Data Source - LDAP Attribute Mapping

2. Steps to automate user modification
    a. Navigate to the **Automation** tab.
    b. Click on **Create New Automation**.
    c. Provide a suitable **Name** and **Description** for the automation schedule.
    d. Choose User Automation as the **Automation Category**. Select the Domain and OU(s) to which

the user belongs.

e. Under **Automation Task/Policy** choose **Modify user attributes.**
f. In the **Select objects** section**,** Click **Select more**. By default, the data source is set to **Data from CSV**, change it to **Data from MS SQL Server**.
g. Enable the **Implement Business Workflow** option.
h. Specify the time interval and frequency at which you want to run this automation.
i. Click on **Save & Run**.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: csez.zohocorpin.com

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Modify User Attributes

Data From MS SQL Server: ModifyUser (Advanced)

□ Ignore current records in DB

□ Implement Business workflow

Attributes to be updated: givenName,mail (Choose)

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly For Each: 19 hrs

Notification

Notify the technician when the automation executes

Enable Notification

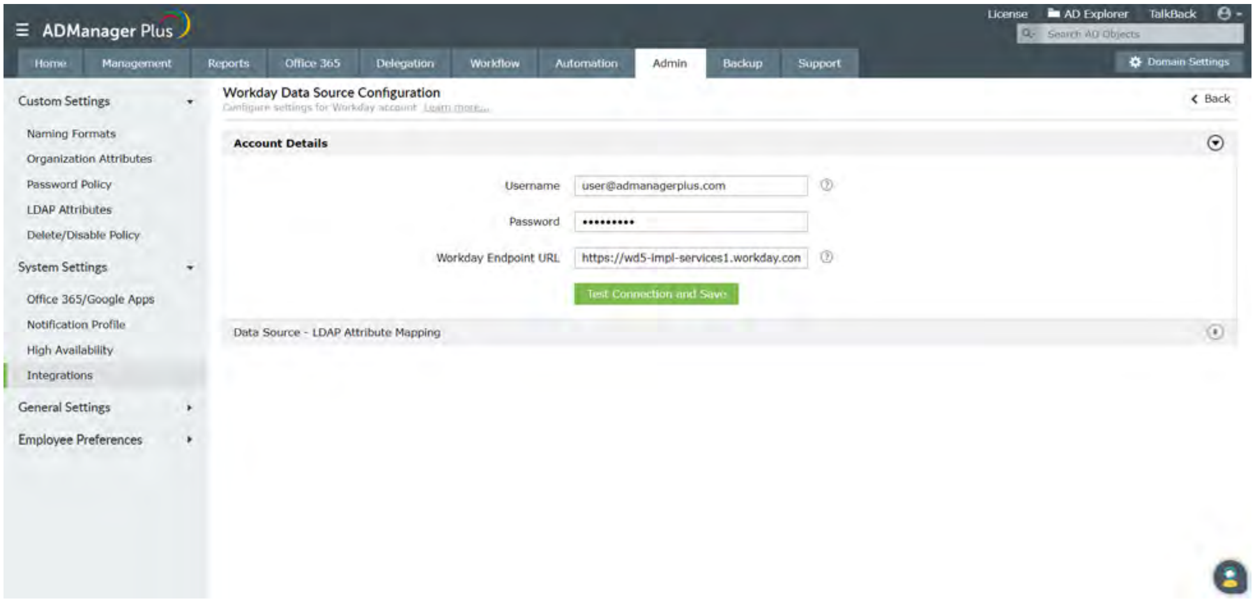
Exercise 3 : Automate user creation from the Workday HRMS application, integrated with ADManager Plus.

Objective: Integrate ADManager Plus with Workday and automate user creation.

Solution:

1. Steps to configure Workday in ADManager Plus
   a. Navigate to the **Admin** tab.
   b. On the left pane of the window, under **System Settings**, choose **Integrations**.
   c. Under HRMS, click on **Workday**.
   d. The **Click to configure button** will guide you to the configuration page.
   e. Enter your Workday **Username** and **Password** in the respective fields. Enter the Workday web service URL in the **Workday Endpoint URL** field.
   f. Click on **Test Connection and Save** button to save your configuration settings.
   g. Under **Data Source - LDAP attribute and mapping**, click on **Add New Configuration.** Map the Active Directory LDAP attributes to the predefined Database Column name provided in the Workday database. For example, if you want to map the 'givenName' attribute in Active Directory

to the 'First_Name' attribute in the Workday database, you can do so by selecting them under the respective drop down menu on either side of the '=' in the **Attribute Mapping** tab. Multiple attributes can be mapped similarly.



Workday Data Source Configuration

Configure settings for Workday account Learn more...

Account Details

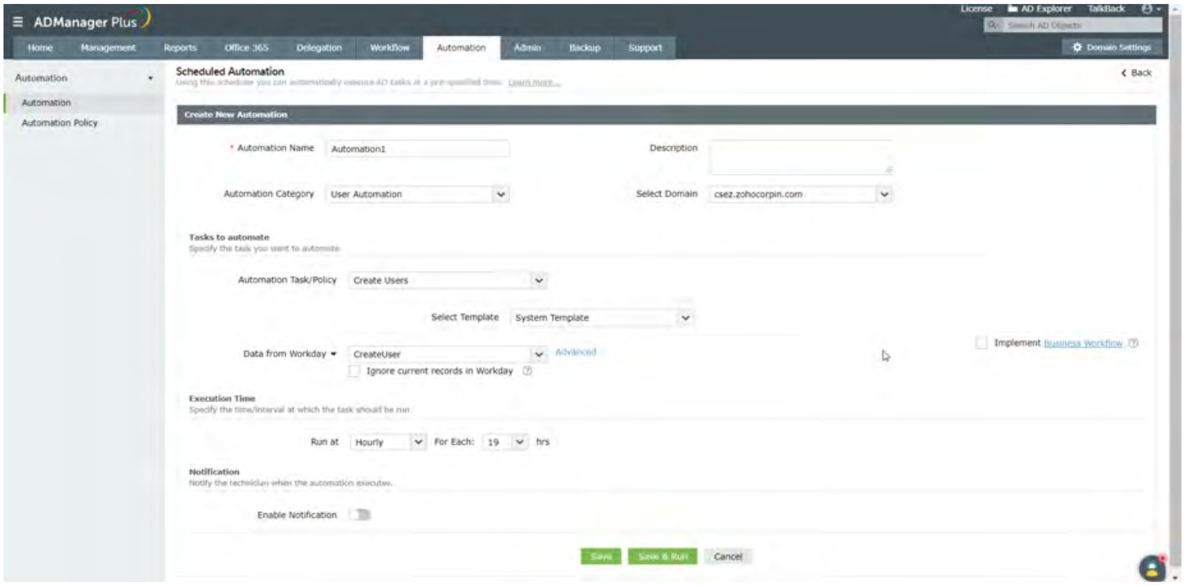
Username: user@admanagerplus.com

Password: •••••••••

Workday Endpoint URL: https://wd5-impl-services1.workday.con

Data Source - LDAP Attribute Mapping

2. Steps to automate User provisioning
    a. Navigate to the **Automation** tab.
    b. Click on **Create New Automation**.
    c. Provide a suitable **Name** and **Description** for the automation schedule.
    d. Choose User Automation as the **Automation Category**. Select the Domain and OU(s) where the user provisioning needs to be automated.
    e. Under **Automation Task/ Policy,** choose **Create Users.**
    f. In the **Select objects** section**,** click **Select more**. By default, the data source is set to **Data from csv**, change it to **Data from Workday**.
    g. Enable the **Implement business workflow** option.
    h. Specify the time interval and frequency at which you want to run this automation.
    i. Click on **Save & Run**.



Scheduled Automation

Using this scheduler you can automatically execute AD tasks at a pre-specified time. Learn more...

Create New Automation

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: csez.zohocorpin.com

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Create Users

Select Template: System Template

Data from Workday: CreateUser

□ Ignore current records in Workday

□ Implement Business Workflow

Execution Time

Specify the time/interval at which the task should be run.

Run at: Hourly For Each: 19 hrs

Notification

Notify the technician when the automation executes.

Enable Notification

Conclusion

The exercises mentioned in this workbook help gain a deeper understanding of the capabilities of ADManager Plus.

As you must now be aware of, ADManager Plus is a one-stop solution that caters to all your Active Directory, Microsoft Exchange, Office 365, G Suite and Skype for Business server management and reporting needs. ADManager Plus also simplifies delegation and automation multifold. Moreover, the simple and easy-to-use UI of ADManager Plus helps you convert complex tasks into point-and-click activities.

If you wish to know more about ADManager Plus, or want more use cases to be included in this workbook, write to us at support@admanagerplus.com.

ManageEngine

ADManager Plus

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates an exhaustive list of AD reports, some of which are essential requirements to satisfy compliance audits. It also helps administrators manage and report on their Exchange Server, Office 365, and G Suite environments, in addition to AD, all from a single console.

For more information about ADManager Plus, visit www.manageengine.com/products/ad-manager/

$ Get Quote

Download