ManageEngine

ADManager Plus

Workbook

Table of contents

1. About ADManager Plus

Introduction

ManageEngine ADManager Plus is a comprehensive identity governance and administration (IGA) solution for managing and reporting on hybrid AD identities. Some of the highlights of ADManager Plus are listed below.

- Automate provisioning users across AD, Microsoft 365, Exchange, Google Workspace, and various enterprise applications.
- Identify potential threats in AD and take immediate action with remediation measures.
- Run access certification campaigns to prevent privilege hoarding.
- Integrate with popular HCM, ITSM, and SIEM tools to streamline identity governance.
- Achieve secure, non-invasive delegation of tasks to non-admin users.
- Create customized workflows with SLAs for timely request handling.

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 hybrid environment easily as opposed to the native 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

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

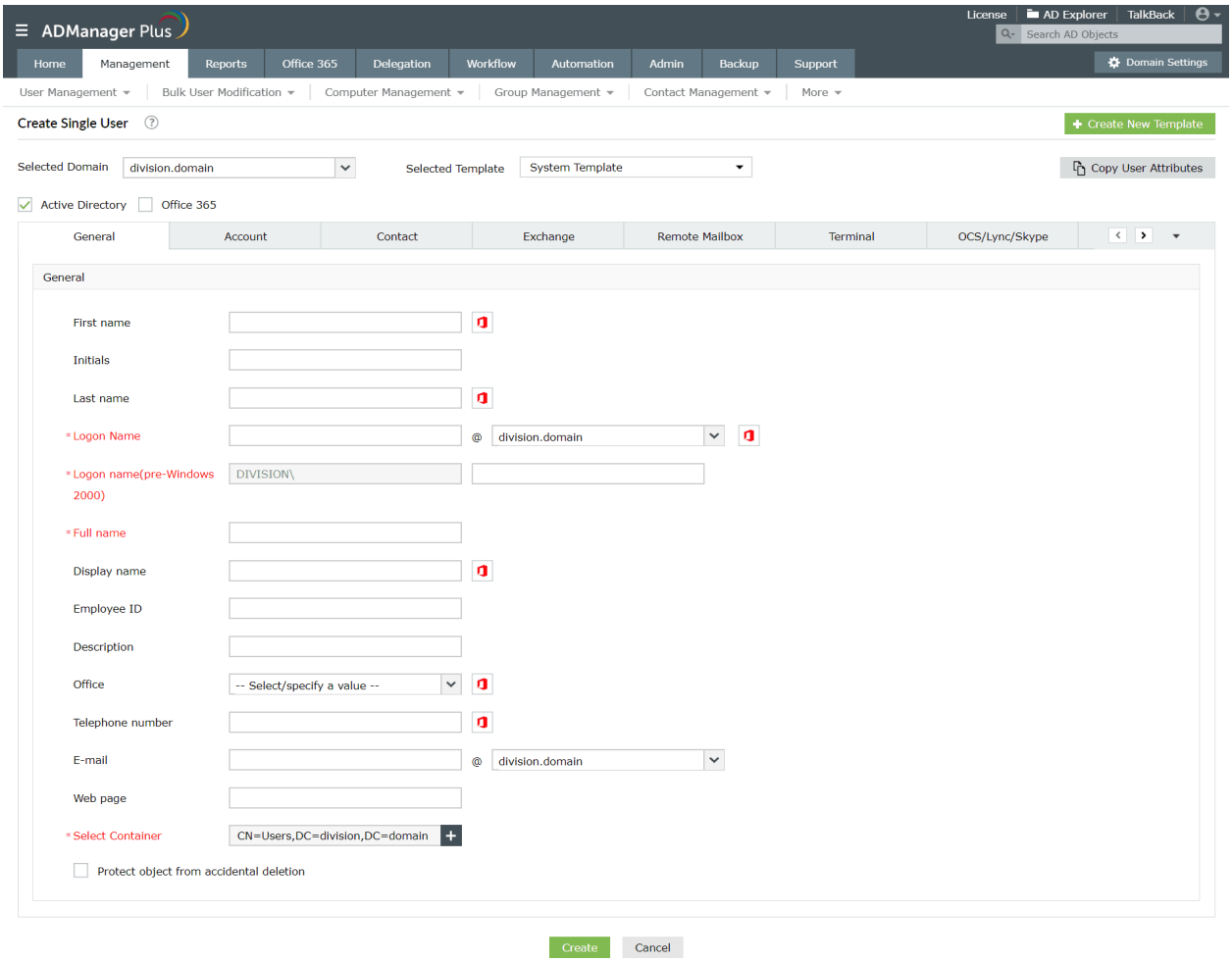
Objective: Create a user with the requirements given below.

- The user should be a member of the specified group.
- The user should belong to the specified department.
- The user's email address should not be listed in the Exchange Address list.

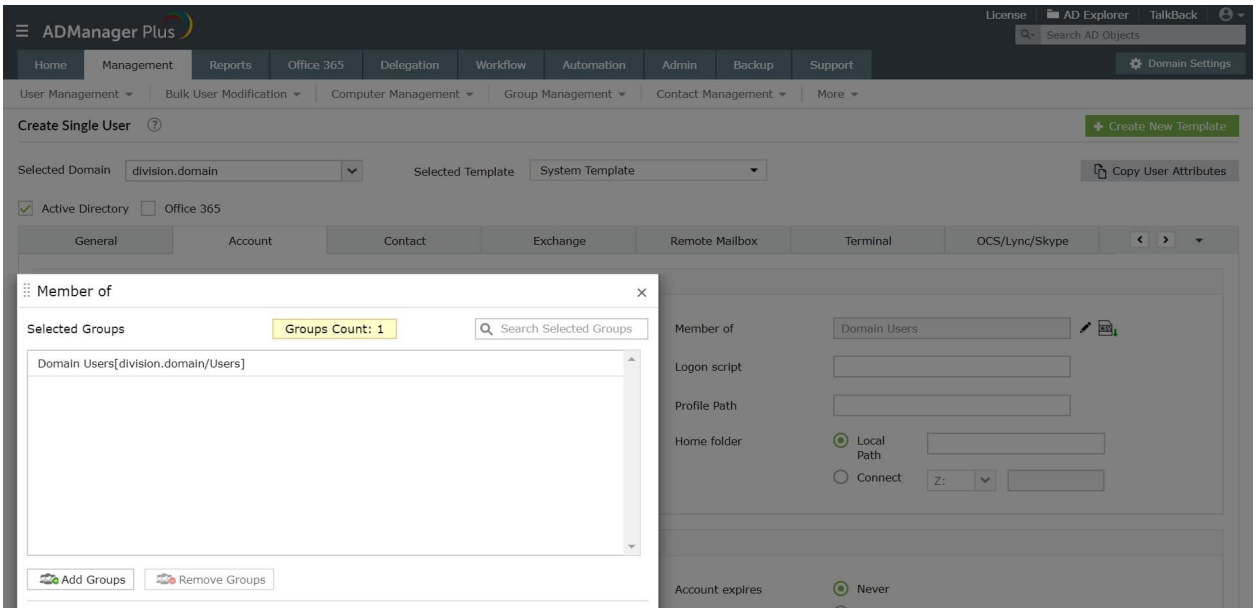
As opposed to native AD tools, where the above tasks require toggling between multiple windows and servers, or complex scripts, ADManager Plus facilitates one-stop user provisioning where a user with all the above mentioned criteria can be created from a single screen, in just a few clicks.

Steps for creating a single user with the aforementioned criteria:

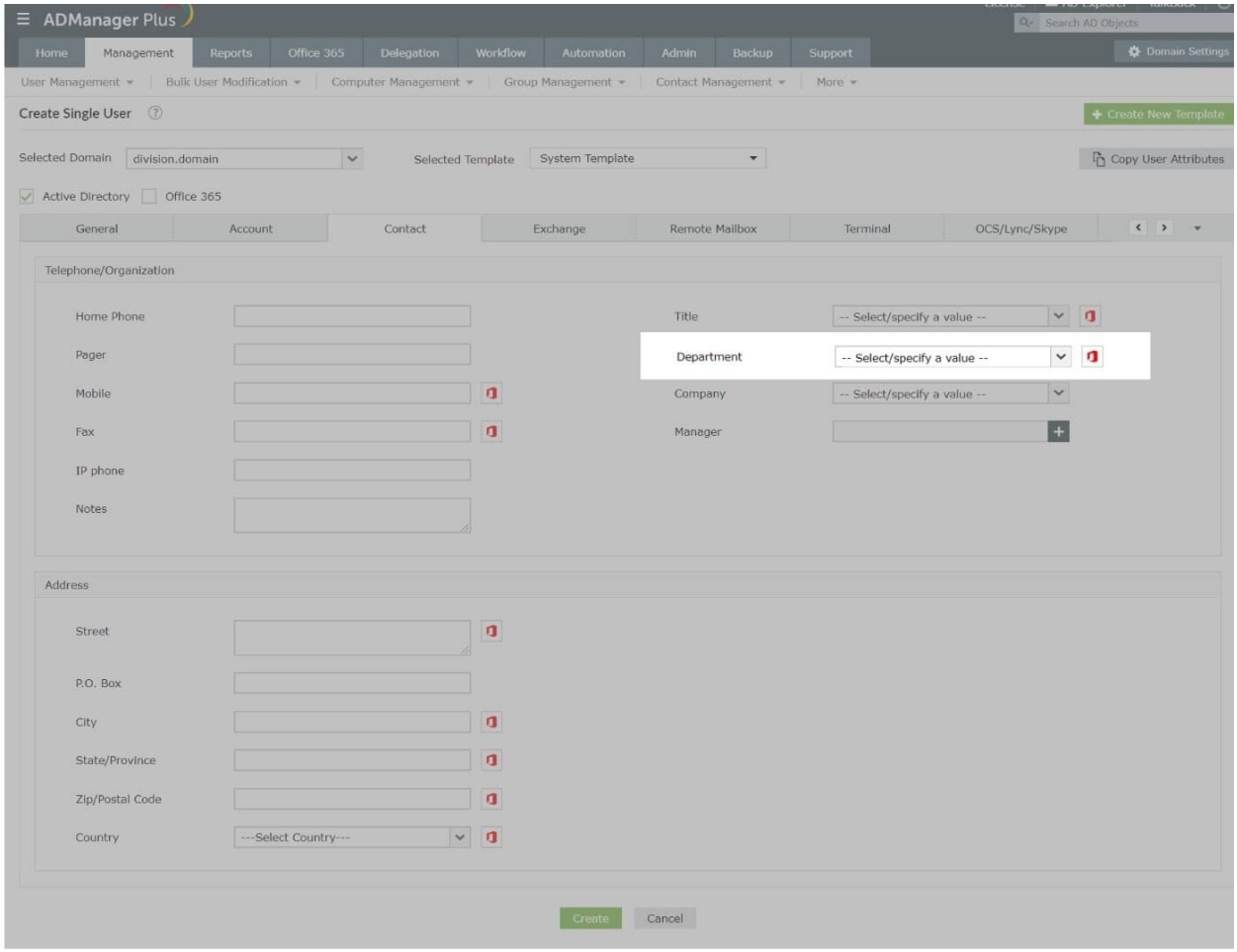
1. Logon to the ADManager Plus tool and Click the **Management** tab.
2. Select the **Create Single User** option, under **User Management**.



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 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 **Add groups** option. Choose the required groups from the *Select Groups* window and hit **OK.**

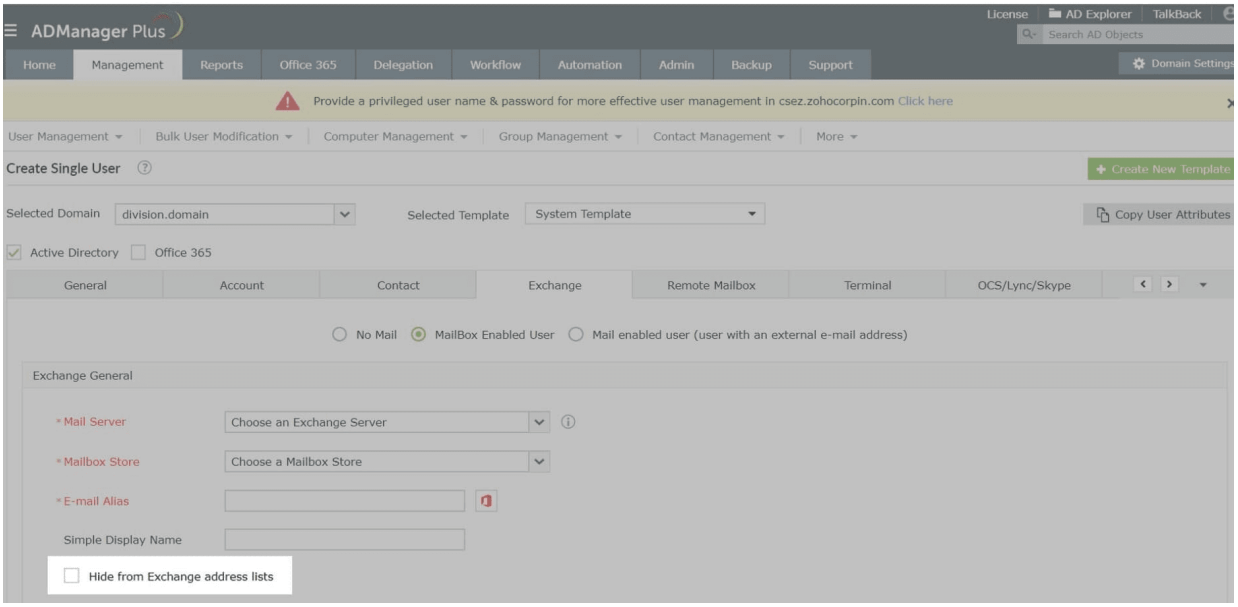


5. Switch to the **Contact** tab to configure the **Department** to which the user should belong. Click the drop-down box to select the department from the pre-defined list or type in your own department.



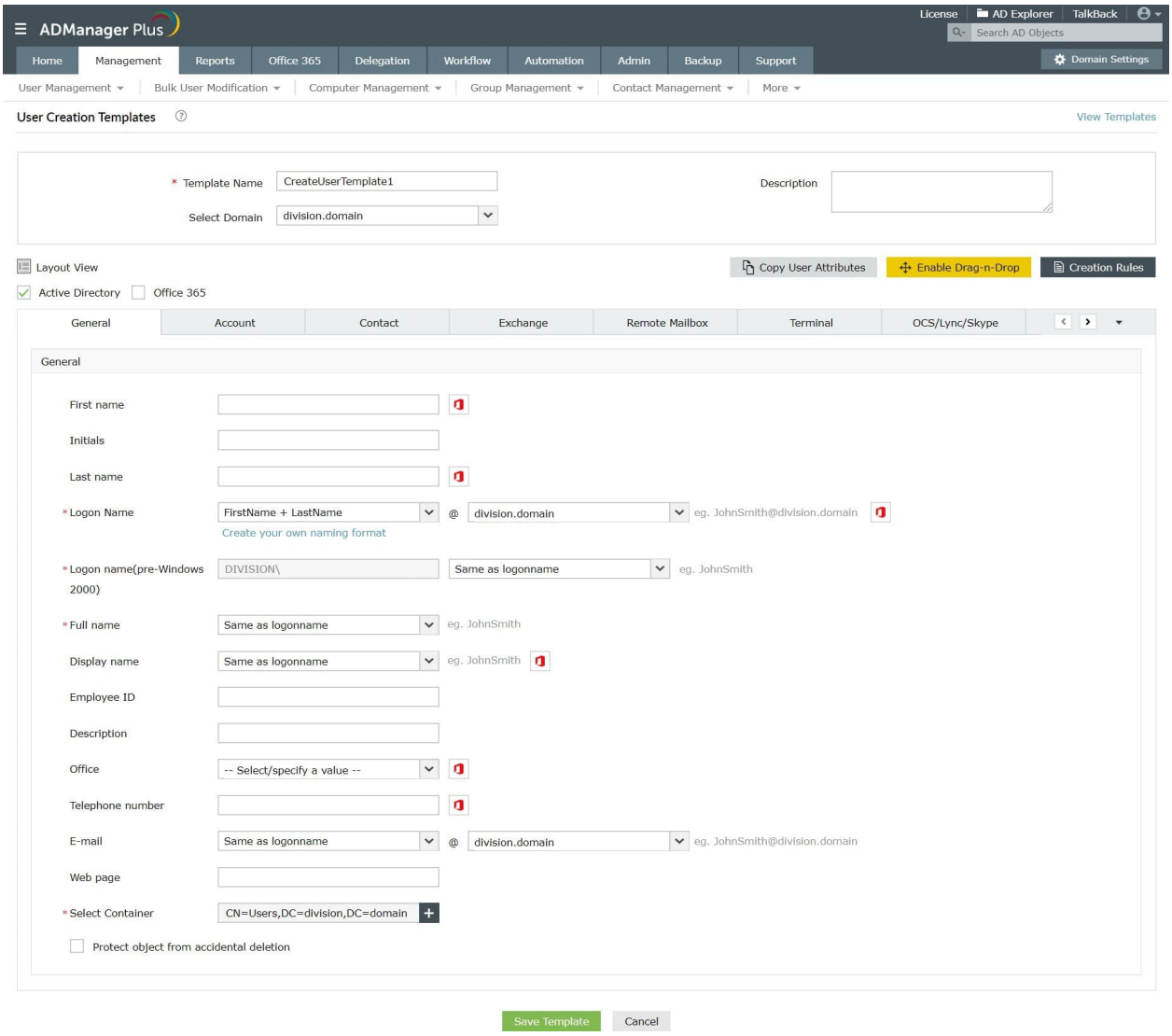
NOTE: You can also traverse to **Organizational Attributes** section in the **Admin** tab to pre-define departments conferring to your organizational requirements.

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

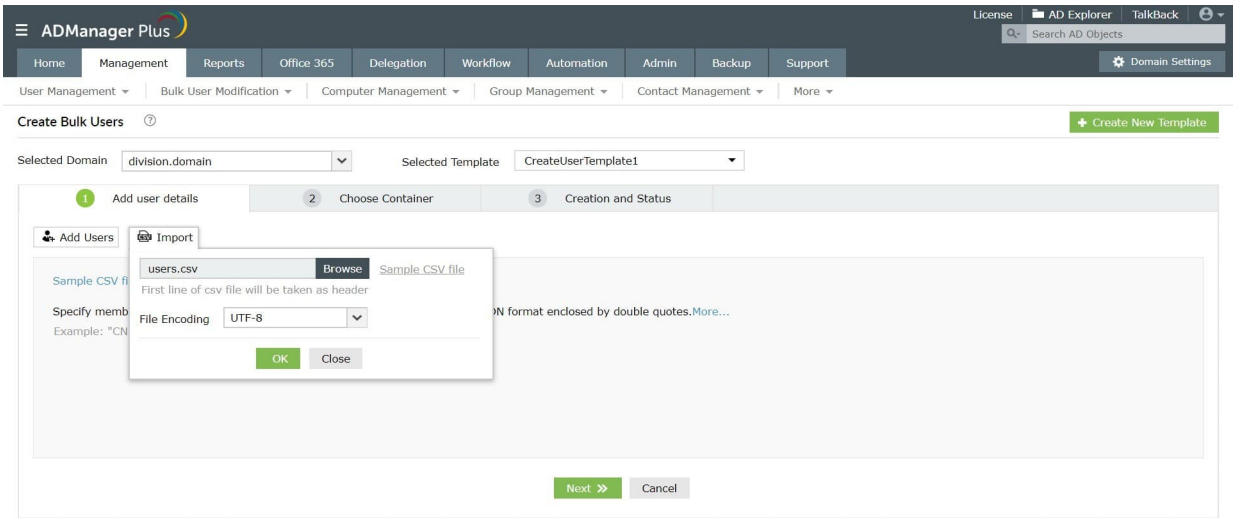


Steps to create users in bulk with the aforementioned criteria:

1. Logon to the ADManager Plus tool and go to the **Management** tab.
2. Select the **User Creation Templates** and click **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** tab.
5. Specify the **Department** in the **Organization** section under the **Contact** tab.
6. Select the **Hide from Exchange Address Lists** option in **Exchange General** section under the **Exchange** tab.
7. Click **Save the template**.



8. Switch back to the **Management** tab and select the **Create Bulk Users** option under the **User Creation** section.
9. 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.
10. 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.
11. Next, choose the container in which you want to place the users. You can also dynamically create a new OU by clicking the **Create New OU** option.
12. Click **Create Users.**



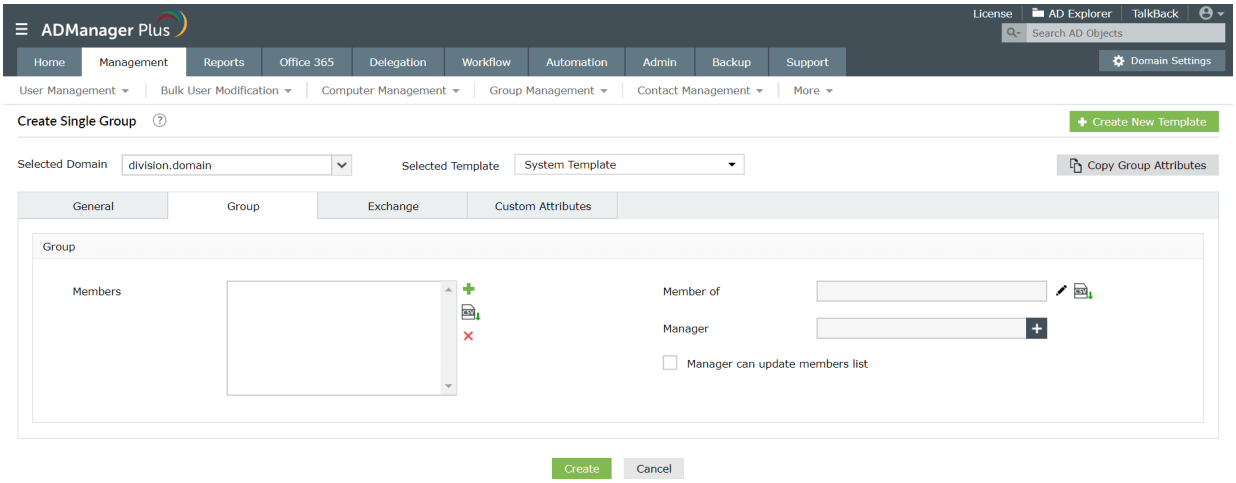
Exercise 2: Group provisioning

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. Navigate to **Management → Group Management → Create Single Group.**
2. Enter the attributes of the group in the **General** Tab.
3. Navigate to the **Group** tab and click the **add, remove or import csv** option located next to the **Members** section.
4. A *Select groups* 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 **Create.**

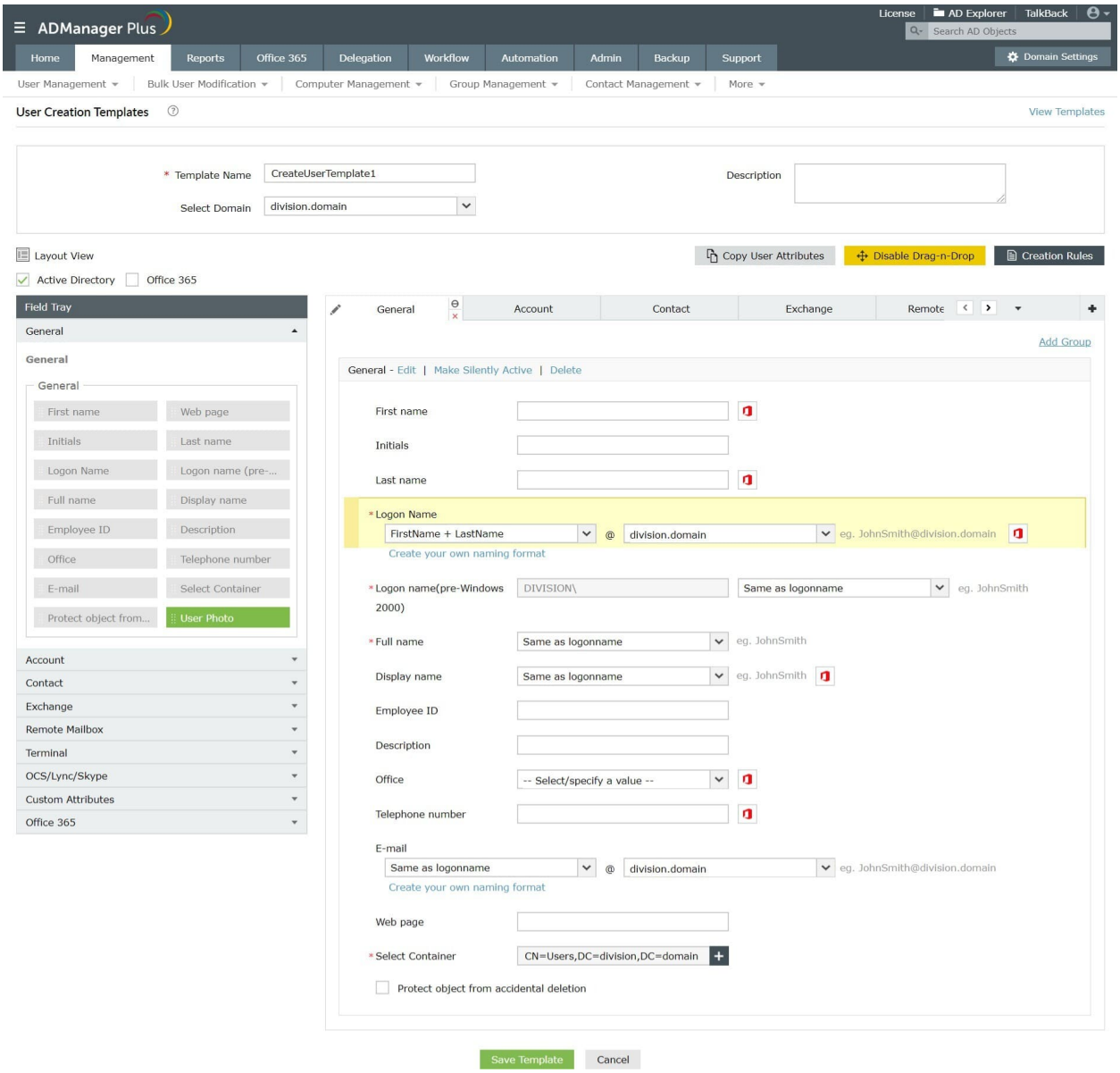


Exercise 3: Prevent duplication during AD user creation

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

Steps to accomplish the given objective:

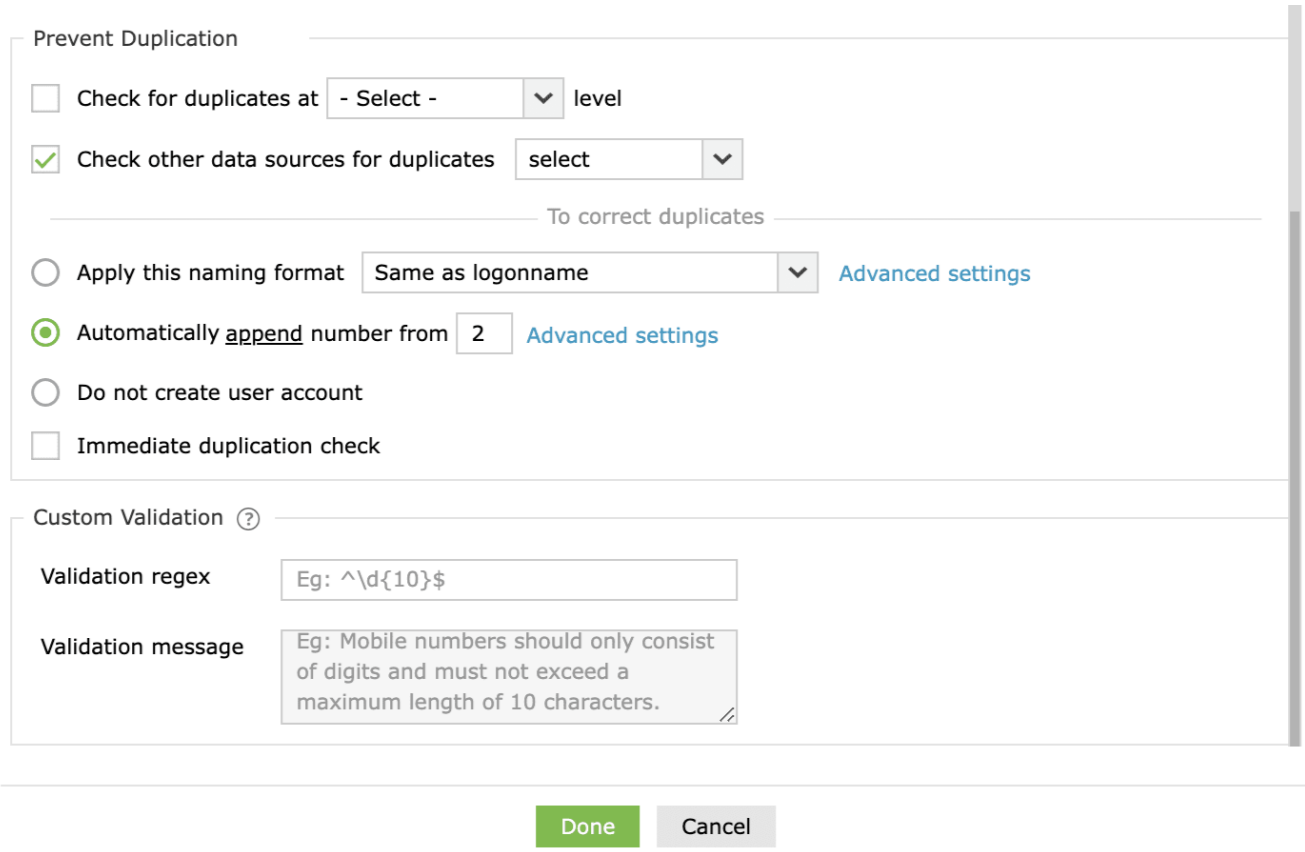
1. To create a user creation template:
    a. Login to ADManager Plus and Click the **Management** tab.
    b. Click on **User Management** and choose **User Creation Templates.** Then click **Create New Template**.
    c. Enter a suitable name and description for the template.
    d. Select the **Domain**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



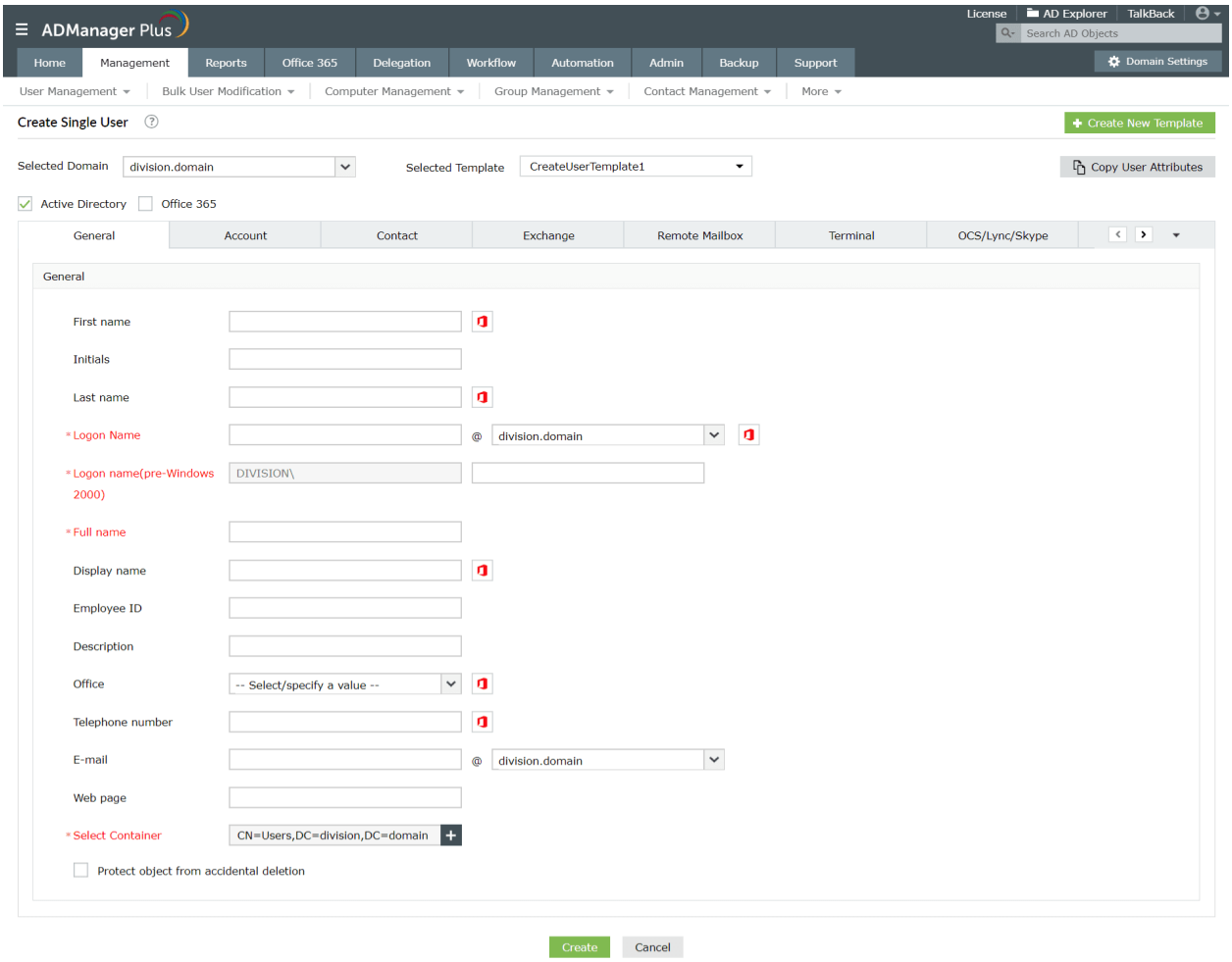
g. Under the **Prevent Duplication** section, select the **Check for duplicates** at the required level. You can also set **Check other data sources for duplicates**.

h. Select the **Apply this Naming format** in case a duplication occurs. For more detailed information, click here.

i. Click on **Done**.



2. To create users using the this template:
    a. Click 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**.



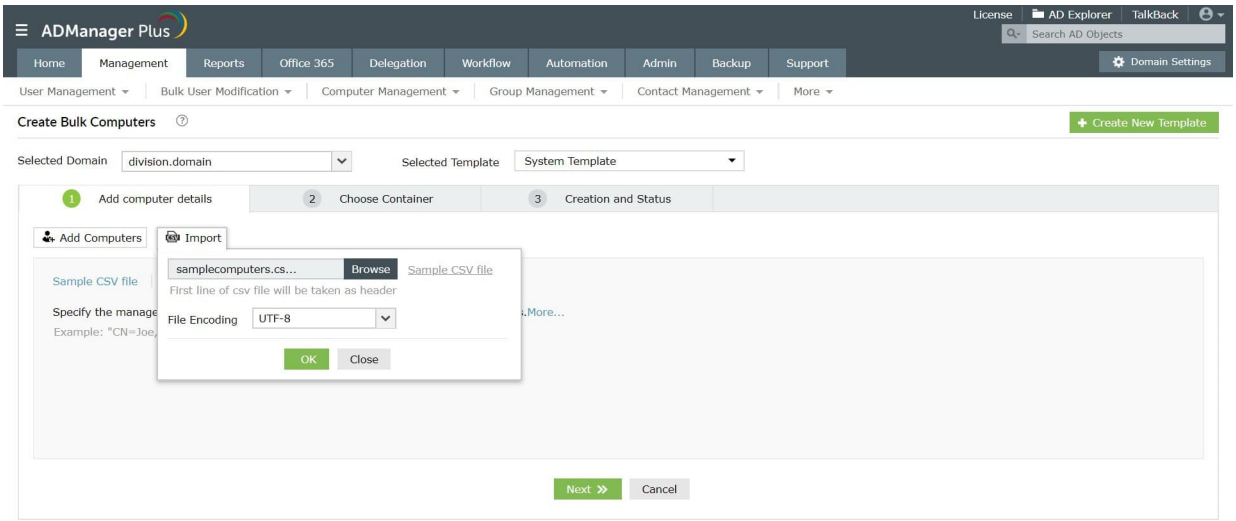
Exercise 4: Computer provisioning

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 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 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 for user creation

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

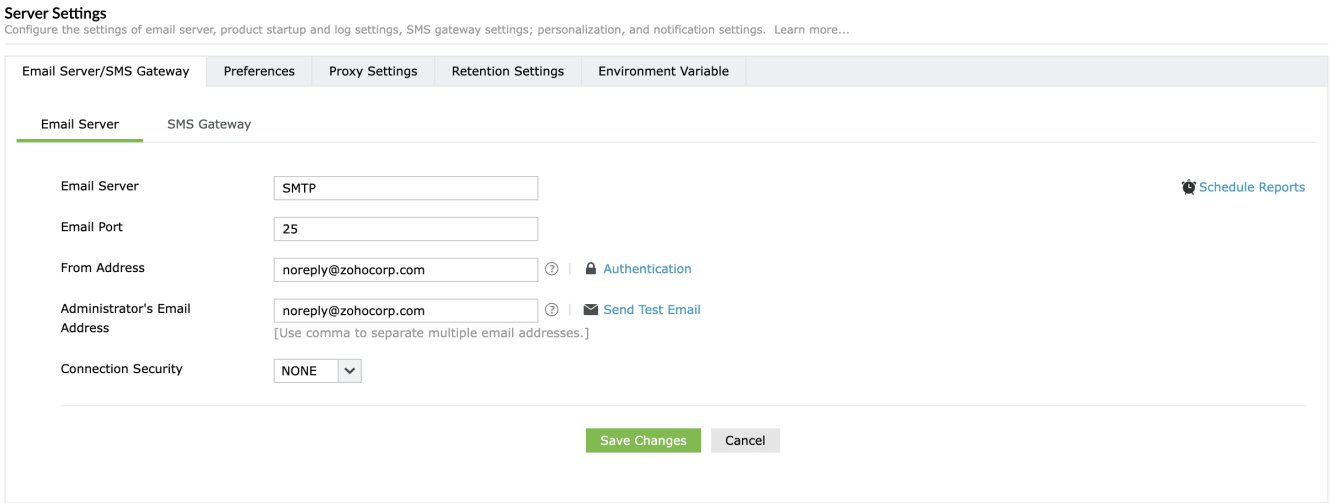
to accomplish the aforementioned objective:

1. Configure the email server settings:
    a. Log in to ADManager Plus and select the Admin tab.
    b. On the left pane under **General Settings**, click **Server Settings**.
    c. Navigate to the Email Server/SMS Gateway tab.
    d. Select **Email Server** to configure the email server settings.

        - **Email Server**: Enter the email server's hostname or IP address.
        - **Email Port**: Specify the port number used by the email server.
        - Click the **Authentication** link to secure your email server from anonymous logins. In the pop-up that opens, select the desired **Authentication Type**.
        - If you select **Basic Authentication** as the *Authentication Type*:
            - Enter the **username** and **password** of an account with administrator privileges for the email server.
            - Choose a communication protocol using which the email server can be accessed.
            - Click **Configure**.
        - If you select **OAuth Authentication** as the *Authentication Type*:
            - Select your **Mail Provider** from the options provided: Microsoft or Google. If your email provider is Microsoft, enter the **Username, Tenant ID, Client ID**, and **Client Secret** in the respective fields, and click Configure. Azure Cloud is the default Azure environment. You can select the Azure environment of your choice by clicking **Choose the appropriate Azure environment**.
                - If your email provider is Google, enter the **Username, Client ID**, and **Client Secret** in the respective fields, and click **Configure**. Learn how to find these values in the Google Developer Console.

- **Note**: When you are redirected to Microsoft 365 during OAuth authentication, authorize using the same username given during the configuration. It is mandatory to use a username associated with a mailbox. Find more information regarding OAuth authentication troubleshooting here.
- **From Address**: Enter the email address from which you would like to receive notifications.
- **Administartor's Email Address**: Enter the email address at which you would like to receive notifications.

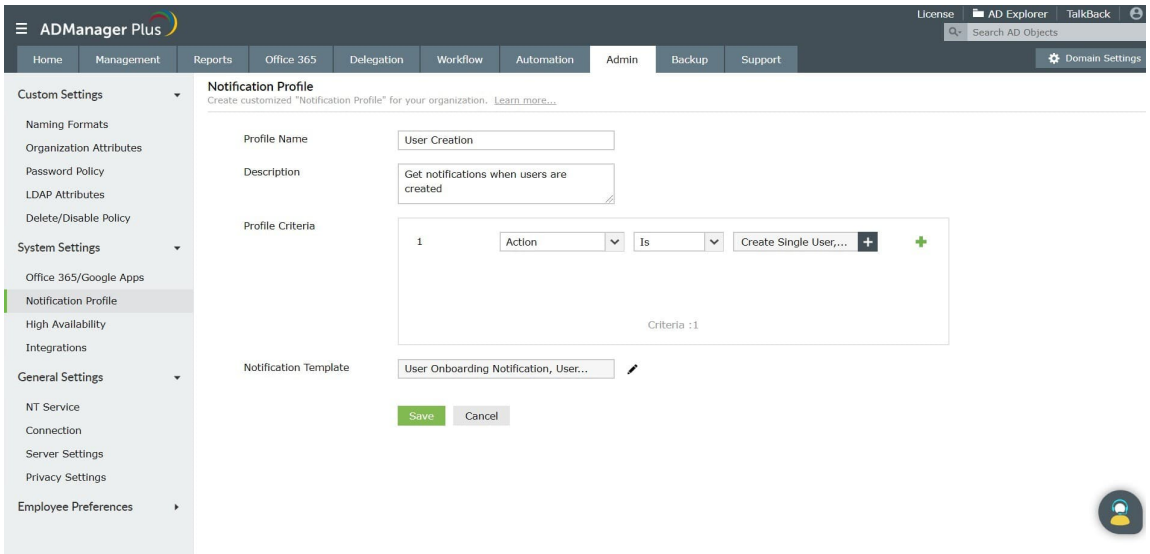
e. Click **Save Changes**.



2. Create a notification profile:
    a. Navigate to **Admin** -> **Notification Profile**.
    b. Click the **Create New Profile** button to create a new notification profile.
    c. Enter the desired name and a short description for the profile being created in the **Profile Name** and **Description** fields.
    d. In **Profile Criteria,**
        - In the first drop-down field, select the criteria based on which the notification has to be triggered. You can trigger notifications for a specific Active Directory management action, help desk technician who will be performing the action, the domain in which the action will be performed, or the user or group object that will be managed.
        - In the second drop-down field, select the condition that has to be satisfied.
        - In the third drop-down field, select the appropriate value that the criterion selected in the first drop-down must hold.
        - Click the **+** icon to add another profile criterion, if needed. If you have more than one criterion, please ensure that you select the desired option Or/And to specify whether all or only specific criteria must be satisfied to trigger this notification profile.
    e. Click the **edit** icon next to the **Notification Template** field and select the desired notification templates based on whether you'd like to send notifications via email, SMS, or both. If you wish to create a new notification template, click the **Create New Template** button located at the top right, and follow the steps listed here.
    f. If you want to update or modify the email and SMS attributes, Click the **Email/Mobile Attributes** button on the top-right corner of the window. In the pop-up that opens, select the domain and the type of attribute (email or mobile) that you would like to modify. Then you need to add the required attributes (alternate email ID or phone, proxy mail ID, etc).

Note: By default, the first attribute listed in the pop-up will be used. In case the first listed attribute does not contain any value, the subsequent attributes containing a value will be considered for use.

    g. Click **Save.**



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.

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 routine tasks and helps you perform them from a single screen.

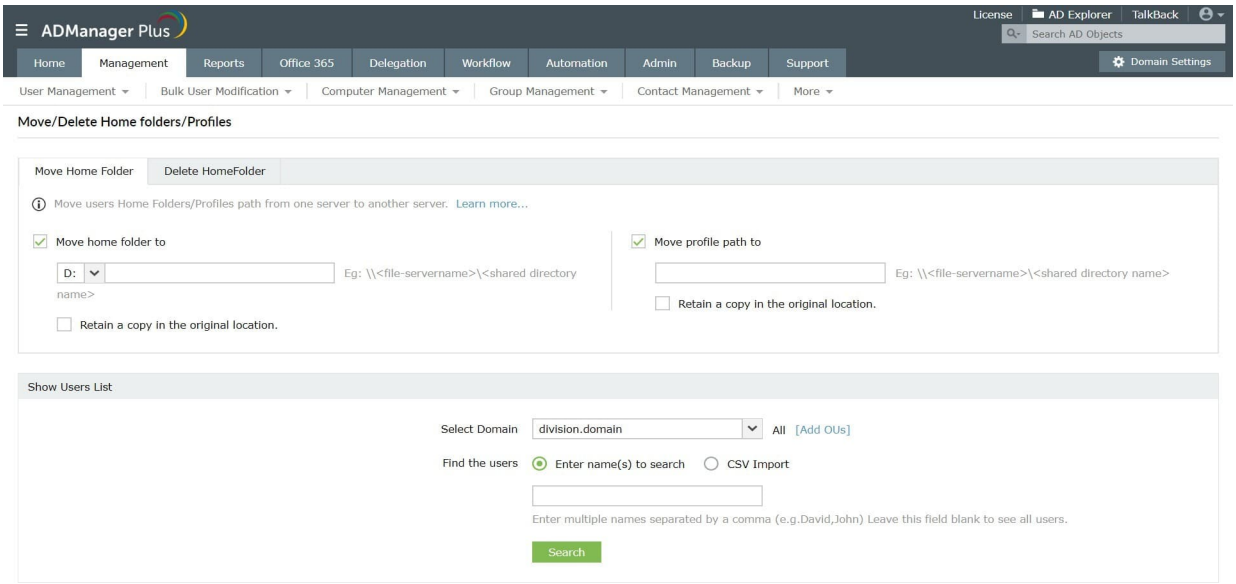
Exercise 1: Decommissioning a file server

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. Navigate to **Management → User Management** tab.
2. Select the **Move/Delete Home Folders** option located under the **Bulk User Modification** section.
3. Select **Move home folder to** option and specify the new location.
4. Similarly, select the **Move profile path to** option and specify the new server and share name.



5. Select the domain (and specific OUs, if you do not wish to perform this action for all users in the domain) to locate the users whose home folder/profile path attributes have to be modified.
6. You can use either of the following options to specify the users:
   a. Import a CSV file containing users' details.
      - Click **CSV Import**.
      - Choose the appropriate CSV file from your computer.
      - Click **Go**.

   b. The built-in **Search** option.
      - Enter the names and click **Search**. To list all the users available in the selected domain (or OU), simply click **Search** without typing anything in the field.
      - Select the desired user(s) from the list and click **Apply.**

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.

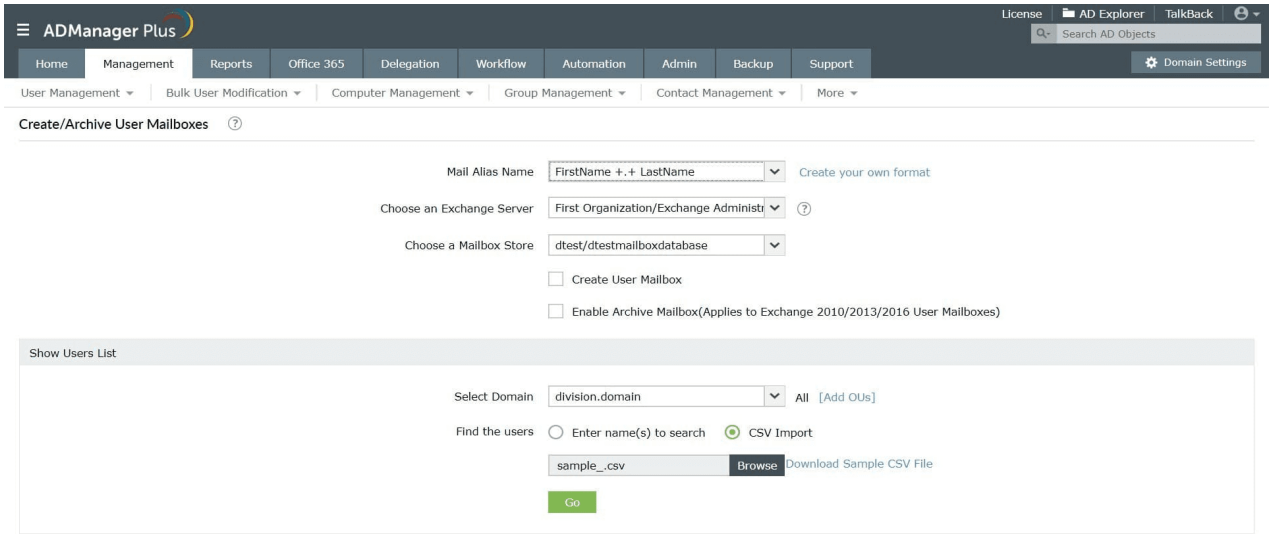
However, with ADManager Plus the task can easily be achieved using the following steps:

1. Navigate to **Management → User Management.**
2. Click **Create/Archive User Mailbox** located under the **Exchange Mailbox Tasks** section.
3. 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.

4. From the drop-down menu, select the Exchange Server and Mailbox Store.
5. Select **Create User Mailbox** option to create only the primary mailbox
6. Select **Enable Archive Mailbox** option if you wish to create only the archive mailbox for your users.
7. Select both *Create User Mailbox* and *Enable Archive Mailbox* options if you wish to a create a mailbox and also an archive mailbox for each user account.
8. You can now use one of the following options to list the users for whom you wish to create the mailboxes:
    - You can import the CSV file (sample CSV file) which contains the list of users. After importing the CSV file, from the drop down menu (on the right hand side), select the attribute based on which you want to display the user objects.

    Or

    - Use the Search option to find the users (Note: To list all the users, just click the Search button without typing anything in the Search box)
9. Now, use the check box to select the desired list of user (s) and then click **Apply.** To know more, click here.
10. To create additional mail addresses, follow the steps given here.



Exercise 3: Web-based password reset

Objective: 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:

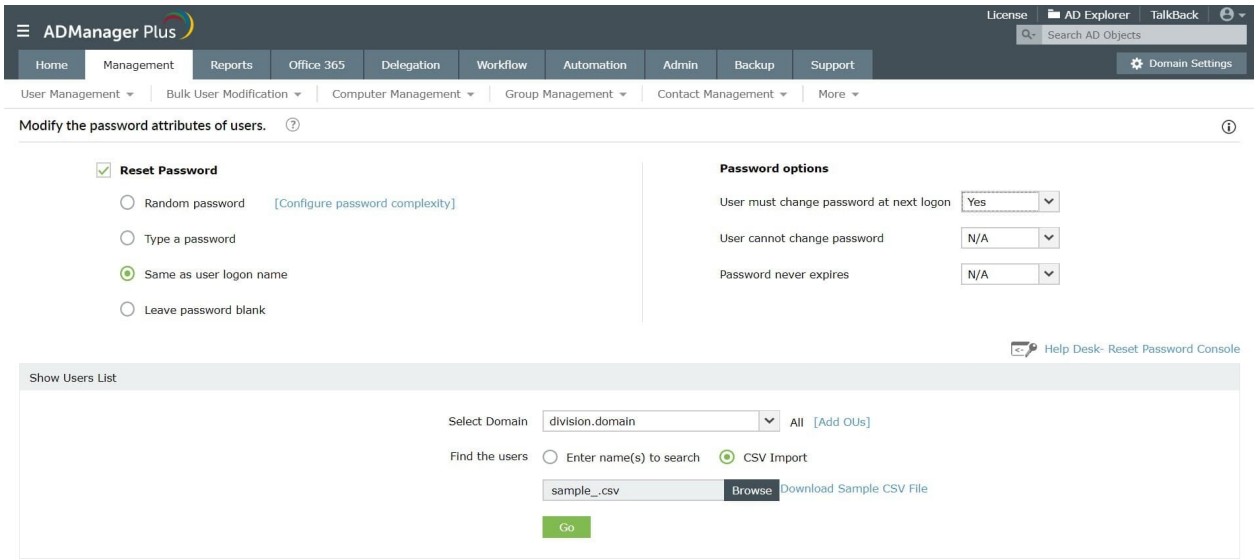
- Locating the user
- Selecting the User
- Selecting the reset password option.

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:
    - 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.



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

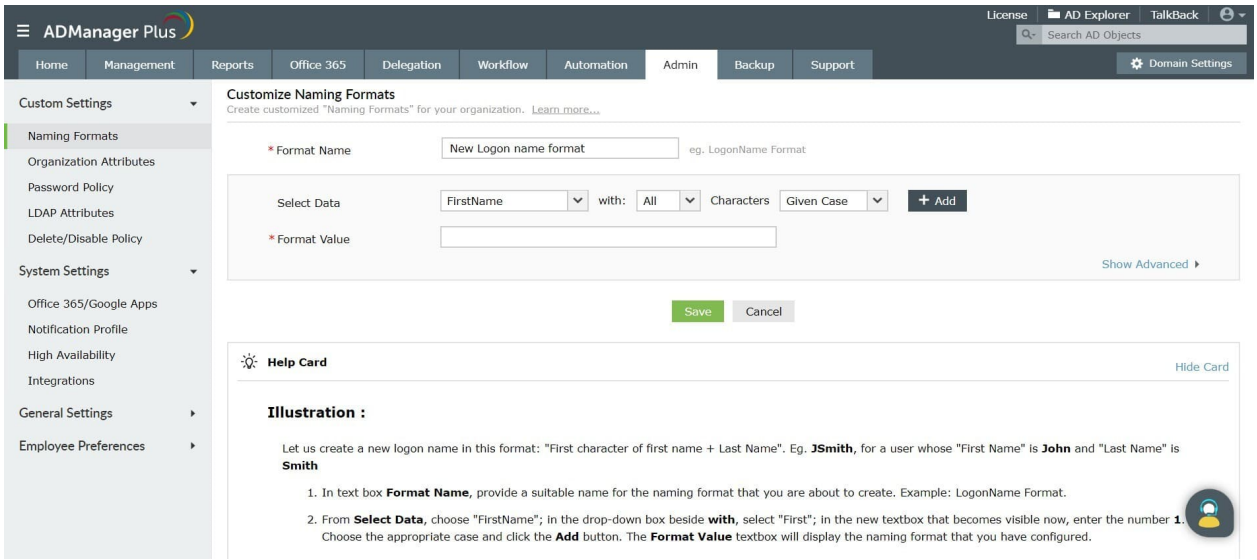
Objective: Create a new naming format using the first character of first name and last name and then update the existing logon name of all users in a specific department (OU).

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.

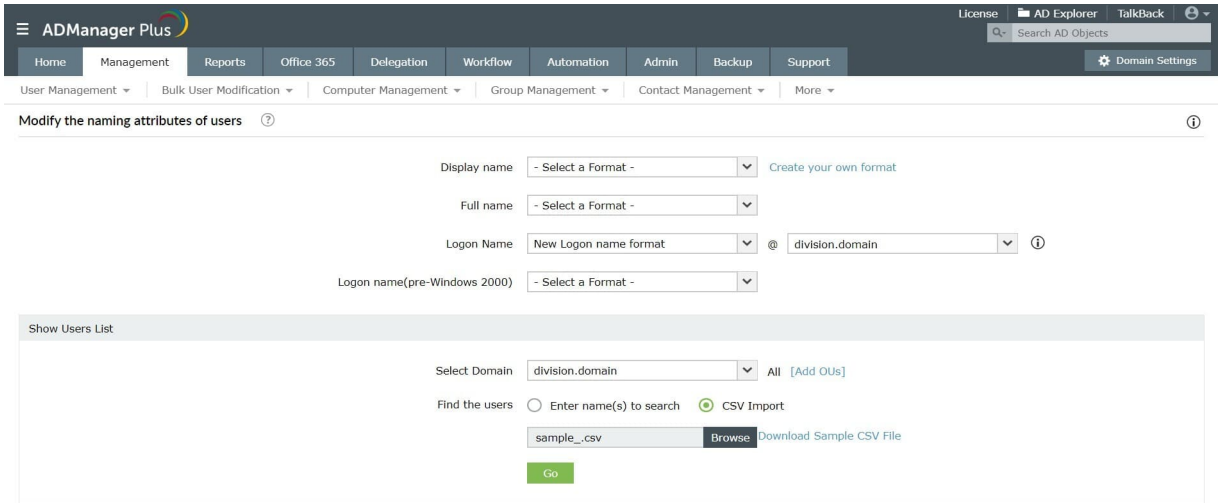
Follow the steps below to accomplish this objective easily through ADManager Plus:

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 word**. 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 word**. Choose the case. Click **Add**.
5. Click **Save**.



6. Navigate to **Management** → **User Management** → **Bulk User Modification** → **Naming Attributes**.
7. Select the newly created Naming Format from the drop-down box in the *Logon Name* field.
8. Select the required users by:
   - Importing a CSV file that has the list of the required users and Click **Go**.
   - 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. Click **Apply**.



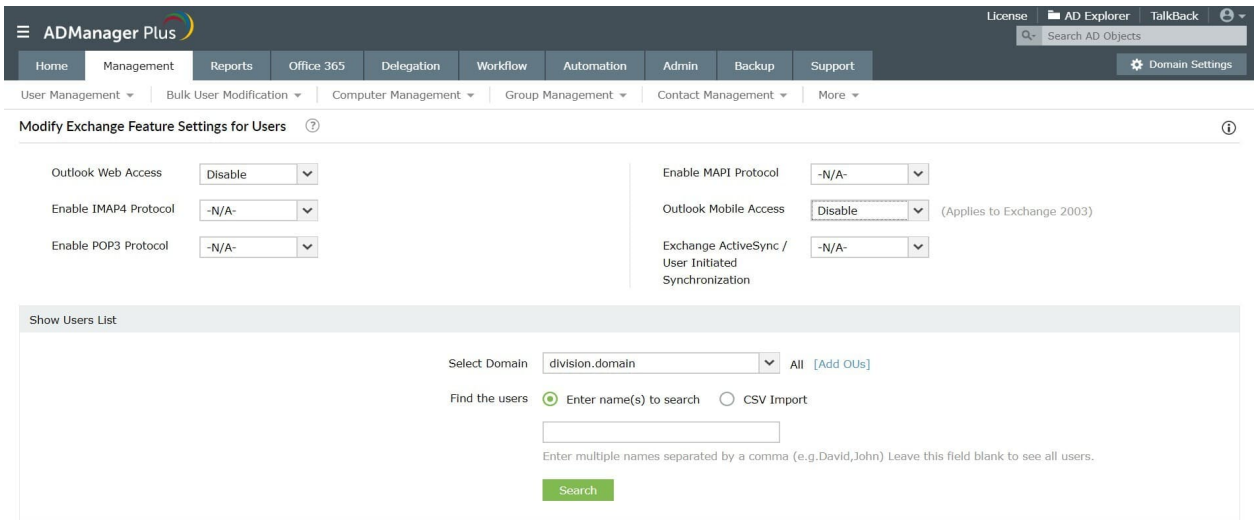
Exercise 5: Deny access to emails through web-browser and smartphones

Objective: Deny the access to Outlook through the web-browser 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. Navigate to **Management** → **User Management** → **Exchange Tasks** → **Exchange Features**.
2. **Disable** the **Outlook Web Access** and **Outlook Mobile Access** options.



3. Select the specified set of users by:
   - Import a CSV file that has the list of required users and click **Go**.
   - 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. Click **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.

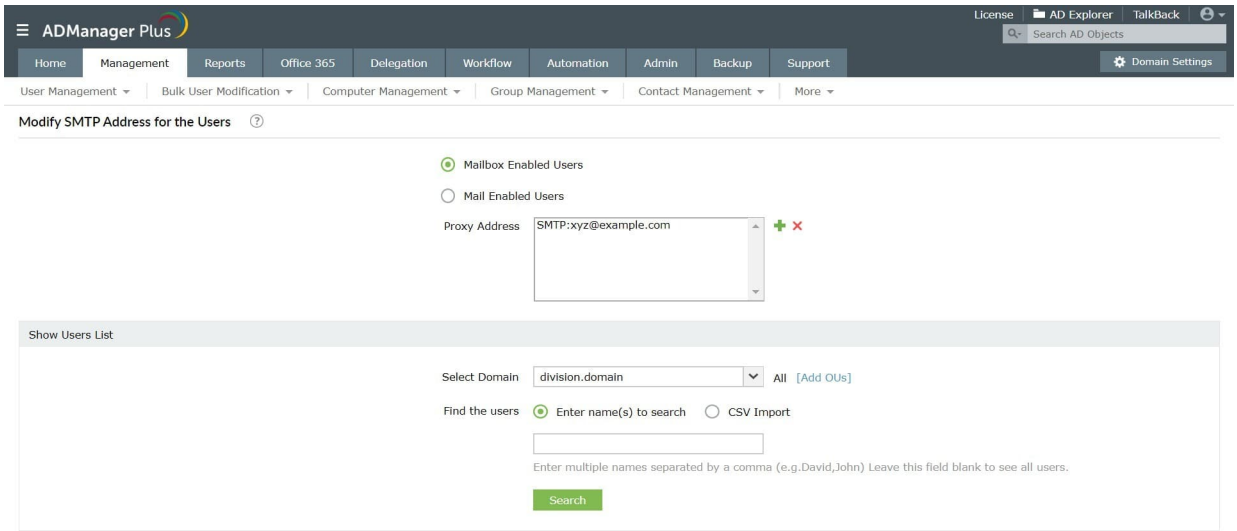
In a native AD environment, you need to switch to an Exchange Server to set a new Primary email address for existing users. However, ADManager Plus allows you to accomplish AD management as well as Exchange management tasks from a single console.

Follow the below to complete the exercise:

1. Navigate to **Management** → **User Management** → **Exchange Tasks** → **Modify SMTP Address**.
2. Select either **Mailbox Enabled Users** or **Mail Enabled Users**.
3. For **Mailbox Enabled Users**, click the **Add** option located next to the **Proxy Addresses** field and 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.

4. 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.
5. Select the required **Domain/OU** and specify the list of users using either a CSV file or by locating them using the **Search** option.



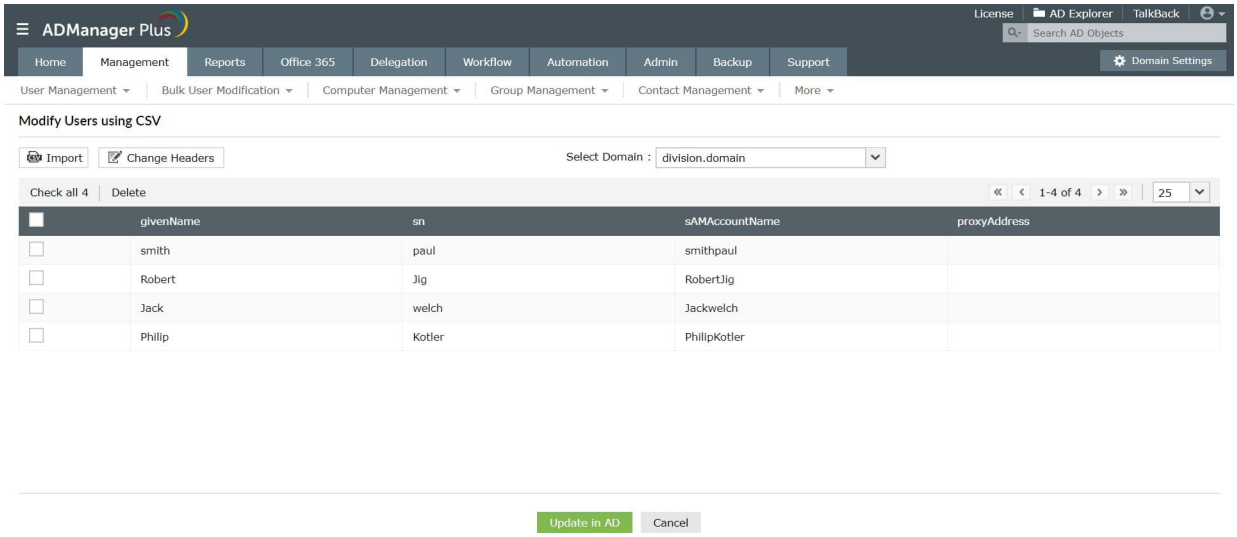
6. Click **Apply** for the changes to take effect.

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 the **Management** → **CSV Import** → **Modify Users**.
2. Select the required domain**.**
3. Click **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.
4. Select the required users and click **Update in AD**.
5. Select the **proxyAddresses** as the attribute that is to be modified.
6. Select the criteria to locate/match the user in AD.
7. Select the **Clear the attributes in AD if it's value in CSV is empty** option.
8. Click **OK**.



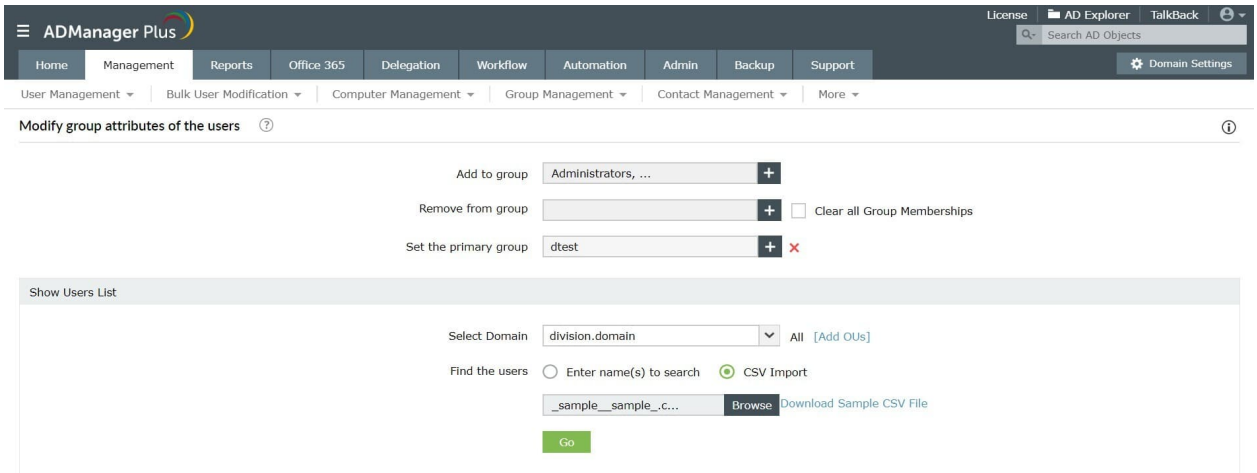
Exercise 8: Add a set of users in a CSV file to a group and set another group as their primary group

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 the **Management tab** → **User Management** → **Bulk User Modification.** 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.



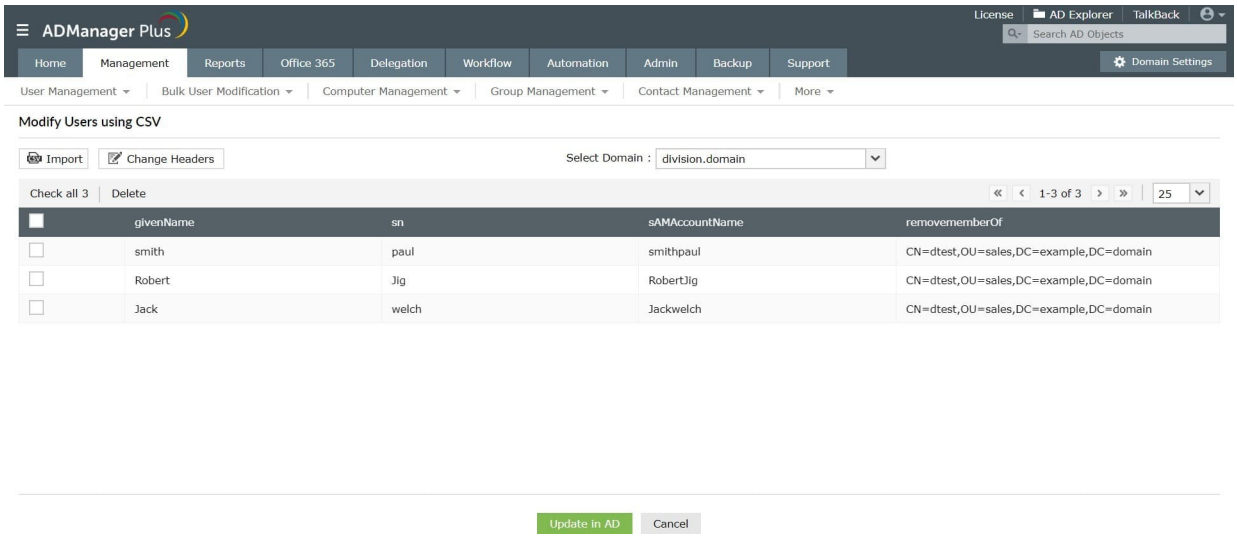
Exercise 9: Remove the members of a group using a CSV

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=c om"
2. Login to ADManager Plus and click the **Management** tab.
3. Click **CSV Import** and go to **Modify User Attributes**.
4. Select the required **Domain.**
5. Click on **Import** to import the 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 **OK**.



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, the *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 tab, all attributes except *remote control* and *remote access* permissions should be read-only.
- For Technician 2, the *Terminal* 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.

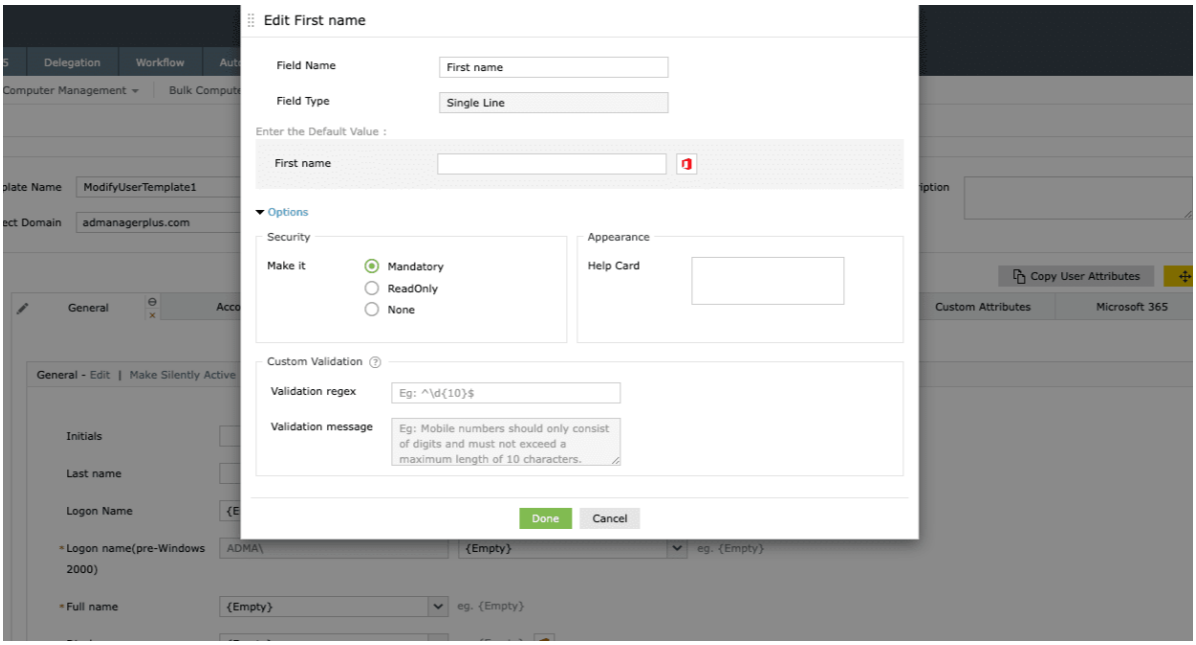
To accomplish this, you will have to create two different user modification templates, one with the conditions for Technician 1 and the other for Technician 2. You'll then have to assign these templates to the help desk technicians to allow them to modify user accounts in their designated domain(s) or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

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

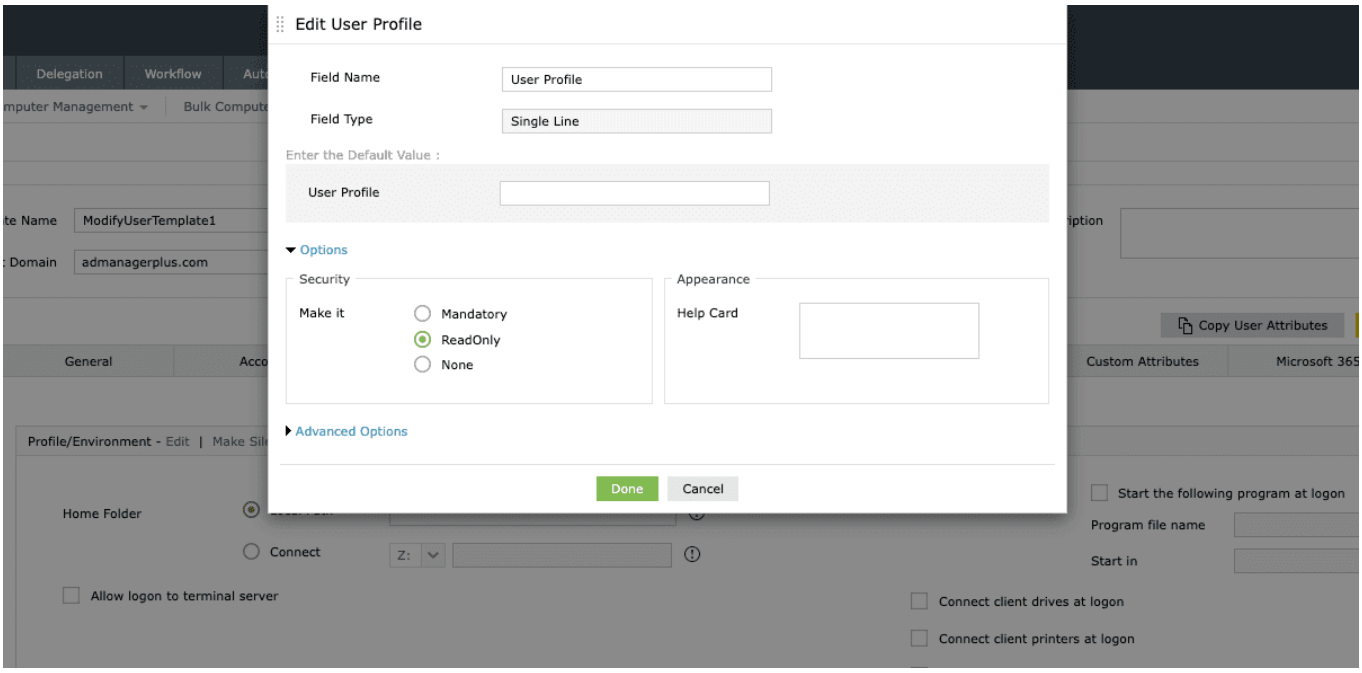
1. Click the **Management** tab and click **User Modification Templates** link in the **User**

Management section.

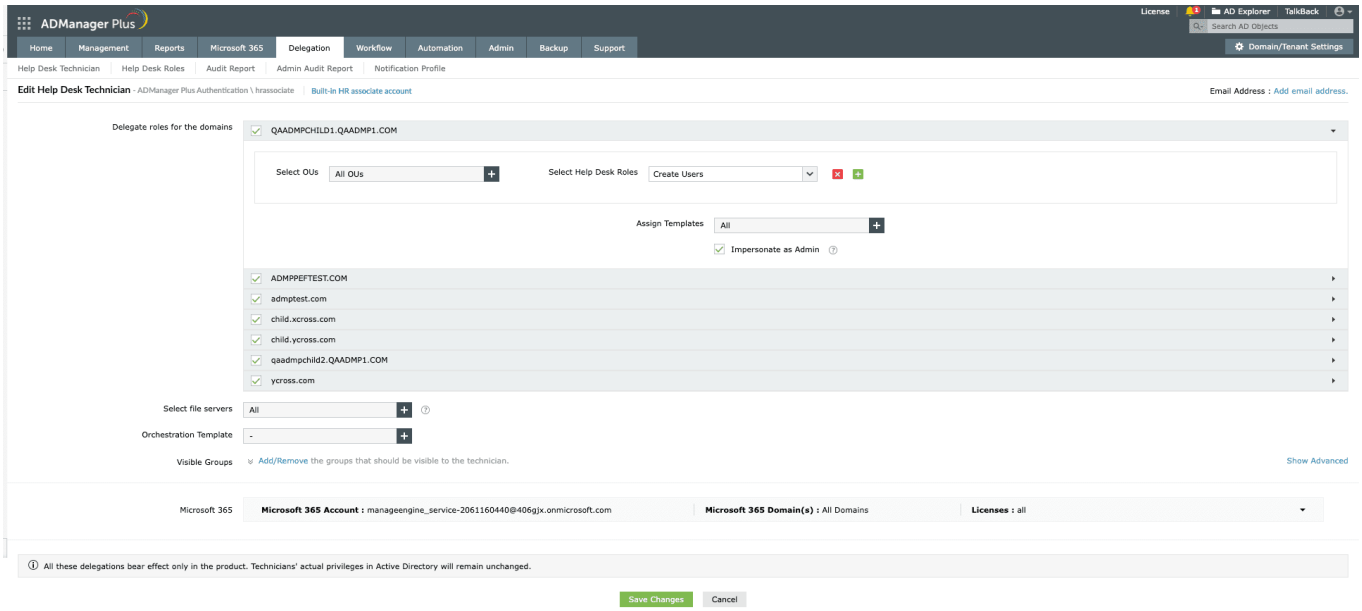
2. Click **Create New Template**.
3. Enter a name and description for the template.
4. For this illustration, let us name this template as **First Name Mandatory**.
5. Select the **Domain** of your choice.
6. Click the **Enable Drag-and-Drop** option.
7. To make the first name mandatory,
    a. Click the **General** tab.
    b. Hover 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 **Done**.



8. To hide **Account**, **Exchange** and **Custom Attributes** tabs,
    a. Click **Account** tab.
    b. Click the ⊖ 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** tab, except the *remote control* and *remote access* attributes read-only:
    a. Click the **Terminal** tab.
    b. Place the mouse over **User Profile** field; Click 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**.



10. Click **Save Template** to save the *First Name Mandatory* template.
11. Similarly, create another template with name **Employee ID Mandatory** which has **Terminal** 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 to the Create new Help Desk Role exercise under 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 to Create new Help Desk Technician exercise under Non-invasive Active Directory Delegation section)
14. To assign First Name Mandatory template to technician 1:
    a. Click **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 **Edit** icon in the *Action* column.
    c. Select the domain in which they have to be delegated.
    d. In **Assign Templates**, click the + button.
    e. In the **Select Template** window, click the **Modification Templates** and select the **First Name Mandatory** template. Click the icon beside the name of the templates to make it a default template. Click **Select**.
    f. **Save Changes** to complete this process.
    g. Similarly, assign the **Employee ID Mandatory** template to Technician 2.



15. The Technician 1 can login and use *First Name Mandatory* template to modify user accounts with satisfying all the specified conditions.
16. Similarly, 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 click the **Modify Bulk Users** link.
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 the **Advanced Options** 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 multi-valued 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.

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 have the following,
   - 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.

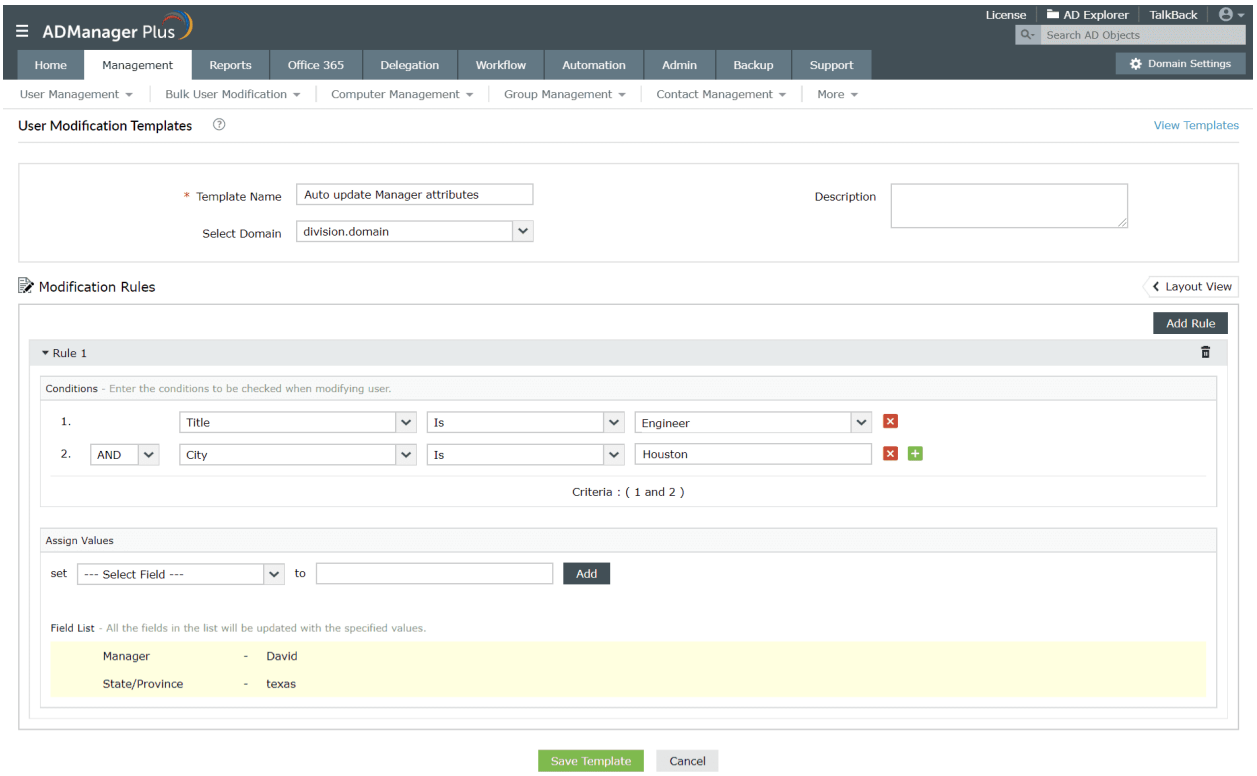
Steps:

I. Create a customized User Modification Template with Modification Rules

1. Navigate to the **Management** tab and click **User Modification Templates** under the **User Management** section.
2. Click **Create New Template** and 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 the **Modification Rules** and then click **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 **Add Conditions.**
   d. In the **Select field** option, click **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 **Add**. In the next **set** option, select the

State/Province attribute and specify the value as *Texas*.

5. 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.



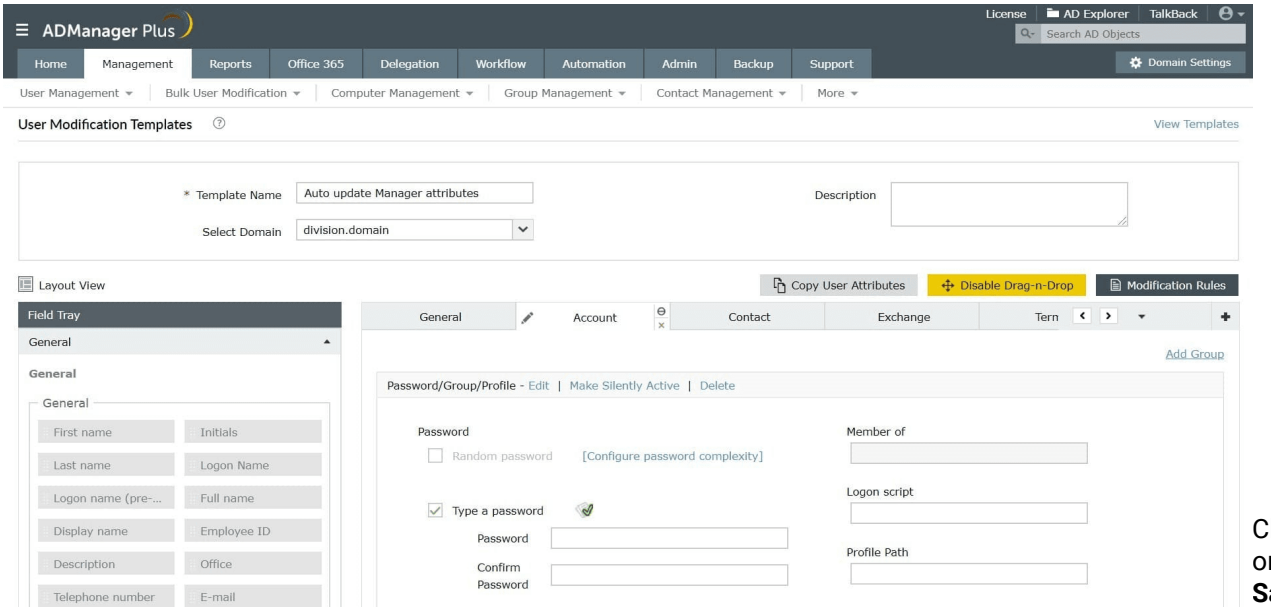
6. Hide all tabs except **General** and **Contact** tabs:

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

   b. Now Click the **Account** tab and Click 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.

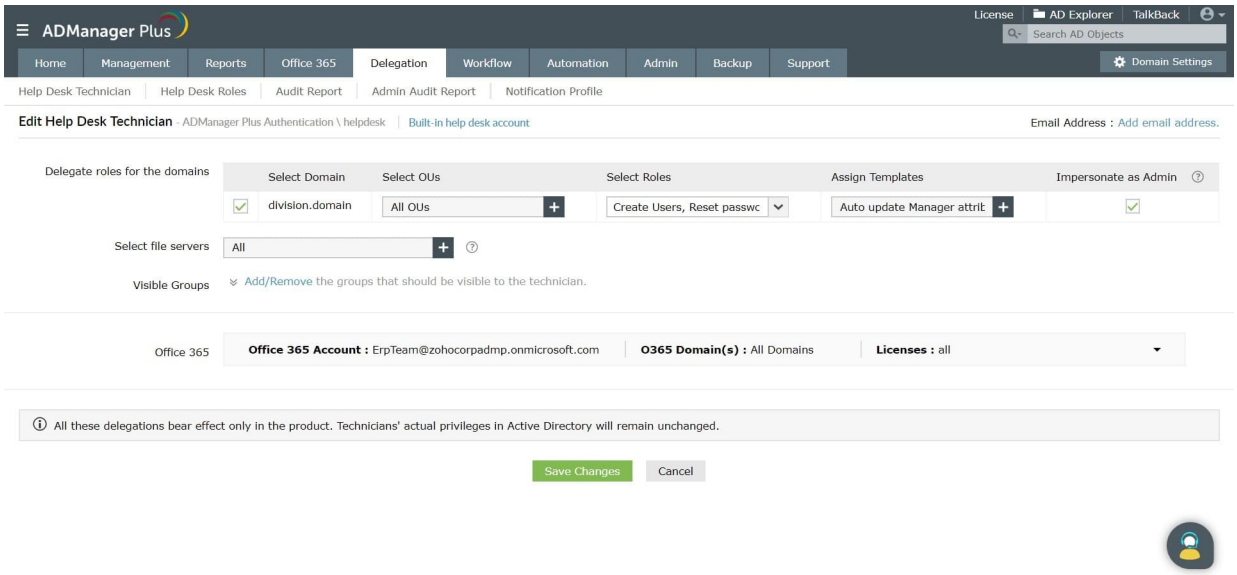
Note: To hide a specific attribute in a particular tab, just place your mouse over the edit icon that appears when you hover over that attribute and select **Make Silently Active** option.



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

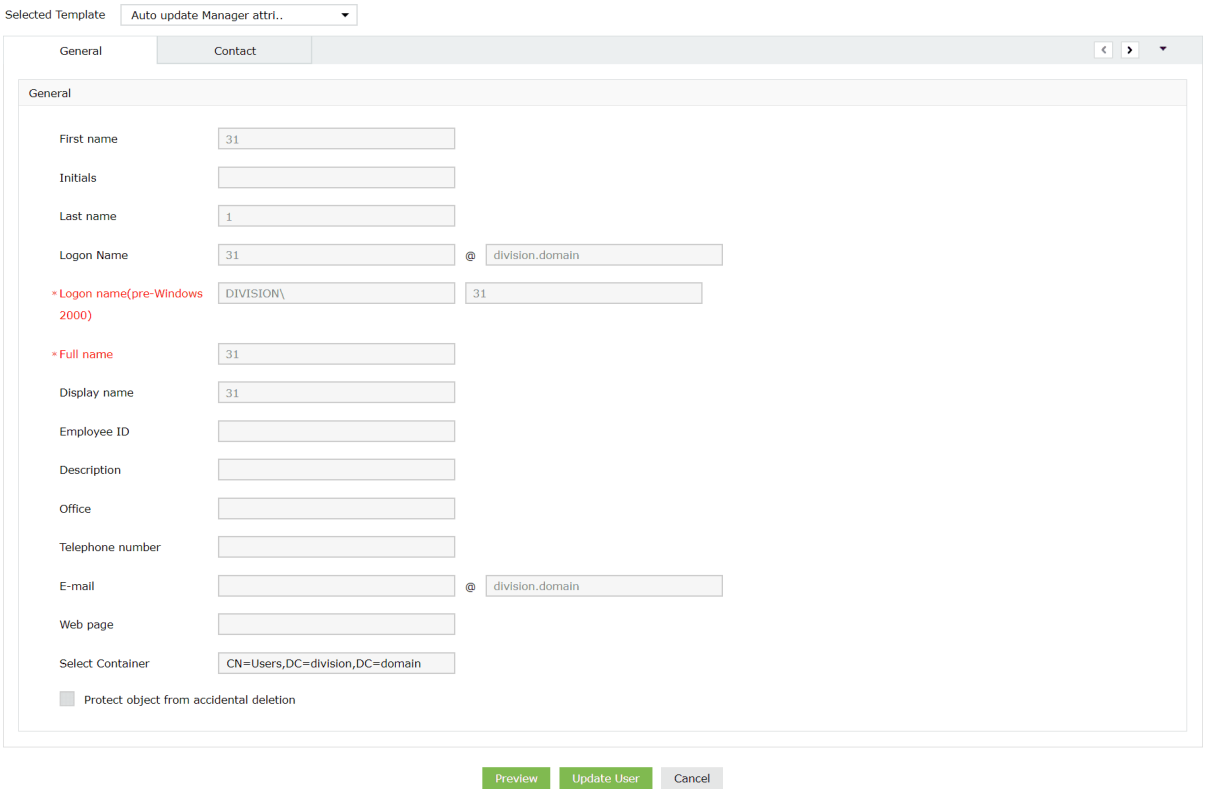
I. Assign this template to the required help desk technicians:

1. Click 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 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 the icon beside the name of the templates to make it a default template.)
8. Save the changes to complete this process.



II. 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** link.
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 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.



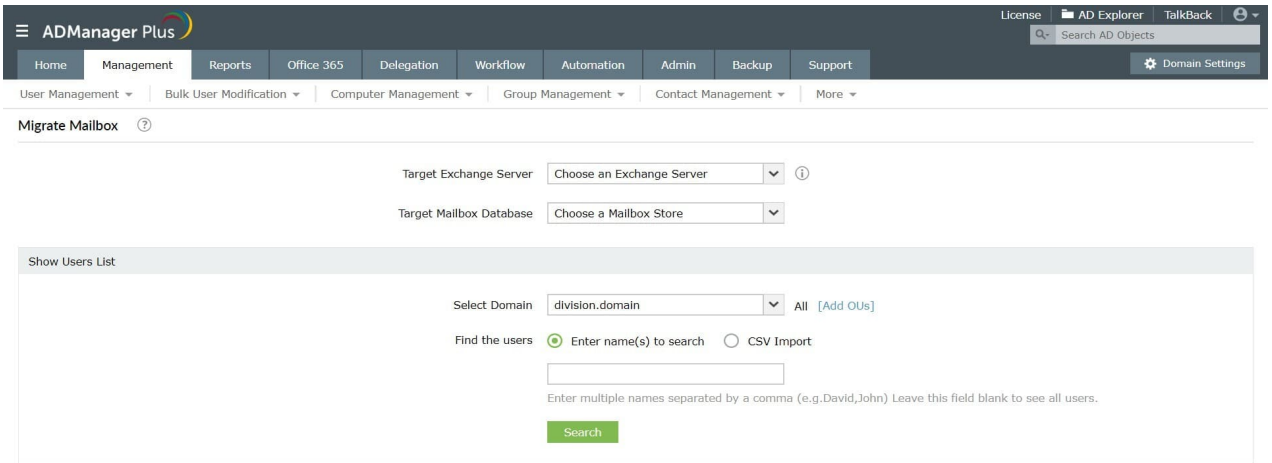
10. To view all the attributes that you have modified, click on **Preview**. This will list all the attributes along with their modified values.
11. Use the **Back** option at the top right corner of the preview window to go back to the template and update any other attribute(s) that you might have missed.
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 **User Management** section, click the **Migrate Mailbox** option.
3. Select the **Target Exchange Server** and **Target Mailbox Database**.
4. Select the required domains and OUs 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.



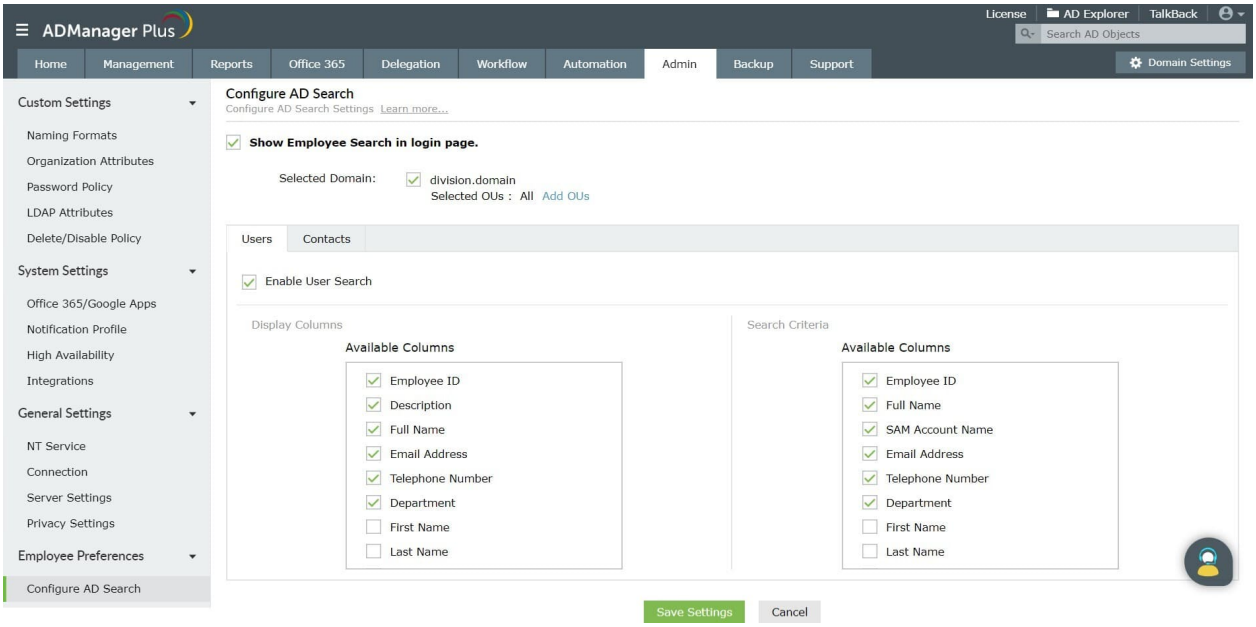
Exercise 14: Performing a secure directory/ address book wide search for domain users

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



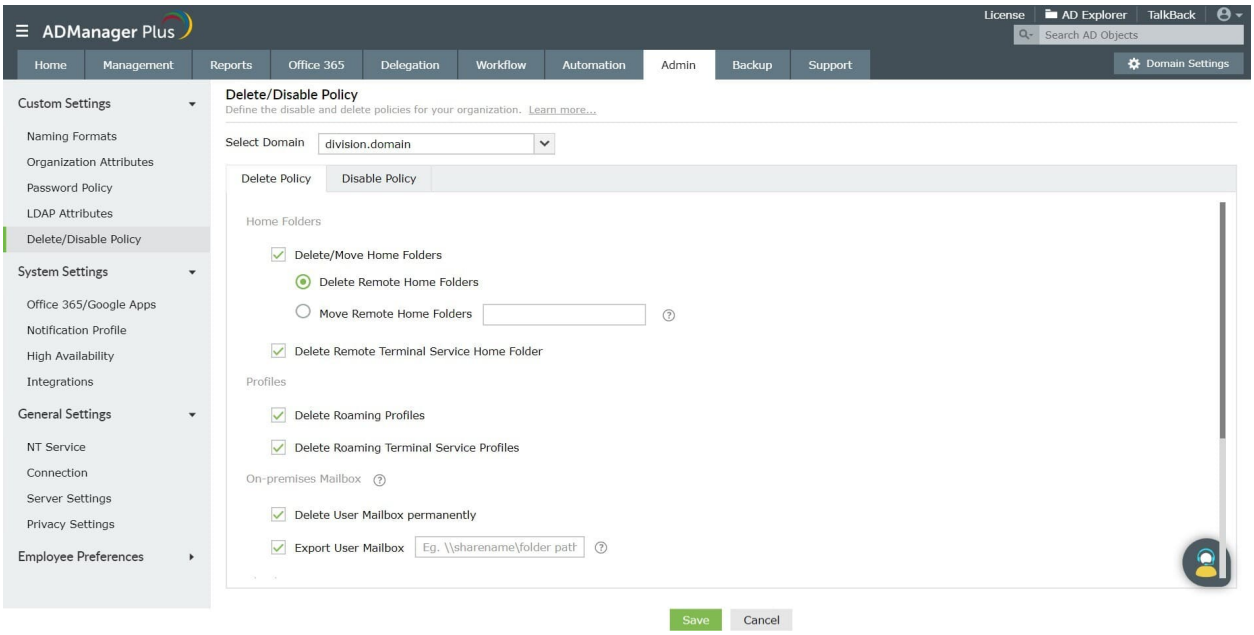
3.2 AD object deletion (de-provisioning)

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 the **Delete/Disable Policy** section, under the **Custom Settings** tab and select the **Home folders**, **Profiles**, **Mailboxes and Other accounts**, **Microsoft 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.



3. Navigate to the **Management** tab. Under **User Management,** select the **Delete users** link.
4. Select the required domain and OUs 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

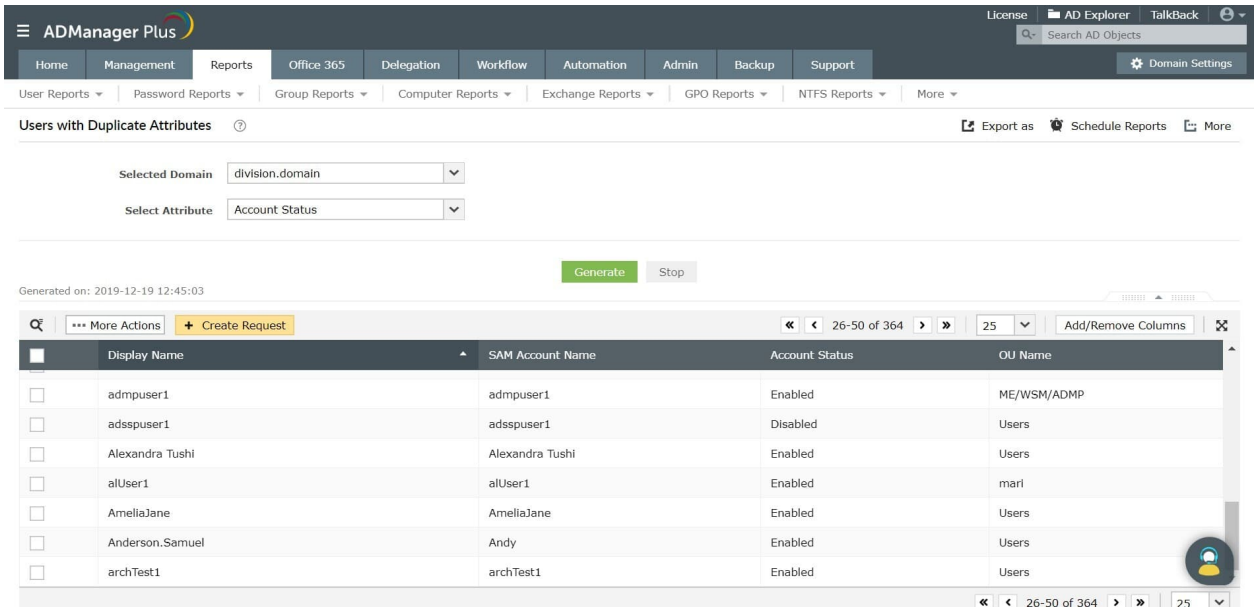
Objective: To find users in AD who have duplicate values for certain attributes, and modify those attributes.

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 the **Select Attribute** field to choose the attributes whose values might be duplicated.

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



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

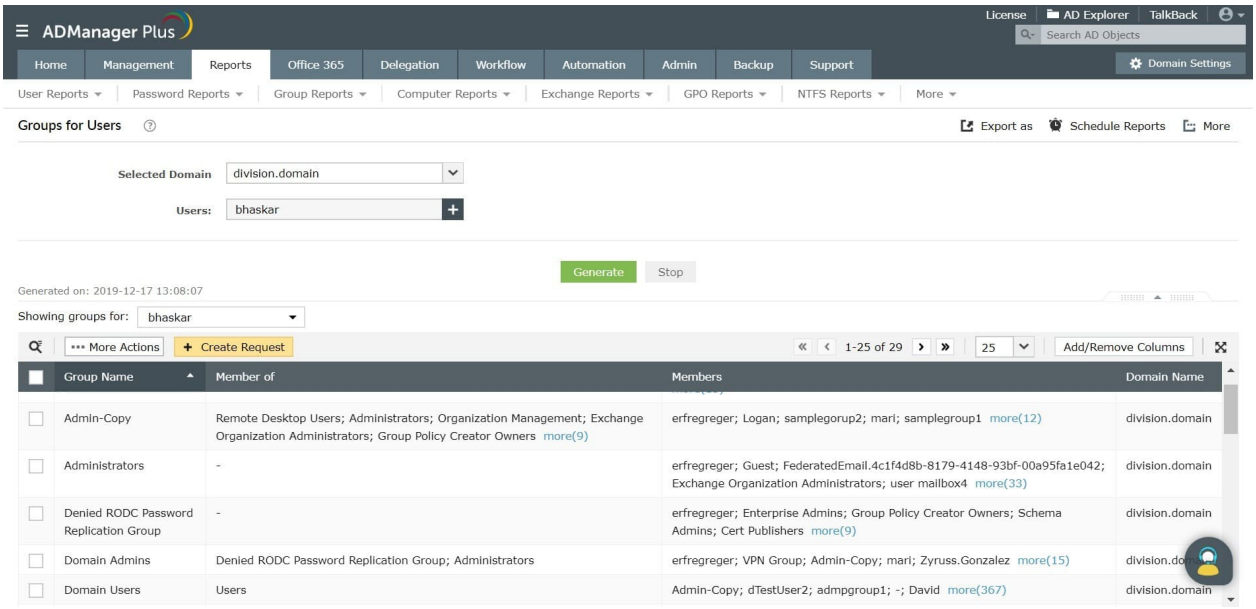
Objective: Search for a user in a specified group, and delete the group if the user is not a member of that group.

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 the **Reports** tab.
2. Click the **Groups for Users** report under the **User Reports** section.
3. Select the domain and the users of your choice.
4. Click **Generate.**



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 the **Management** tab and Click 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+ ready made 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.

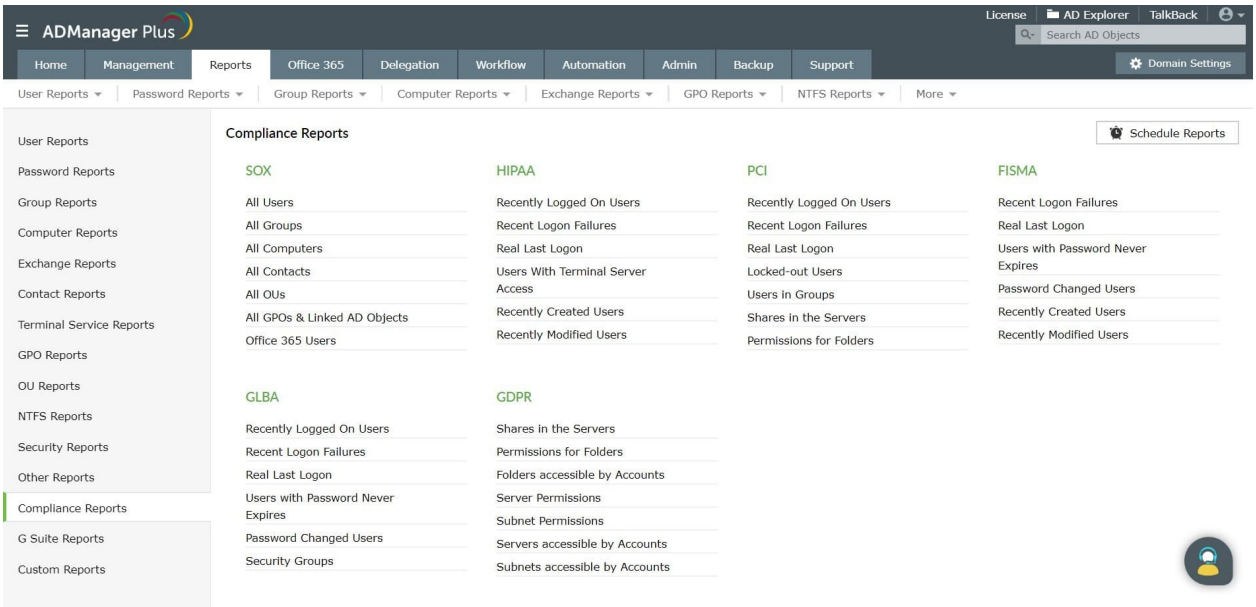
Active Directory reporting

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 the **Reports** tab and go to **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.



Exercise 2: Share permissions report

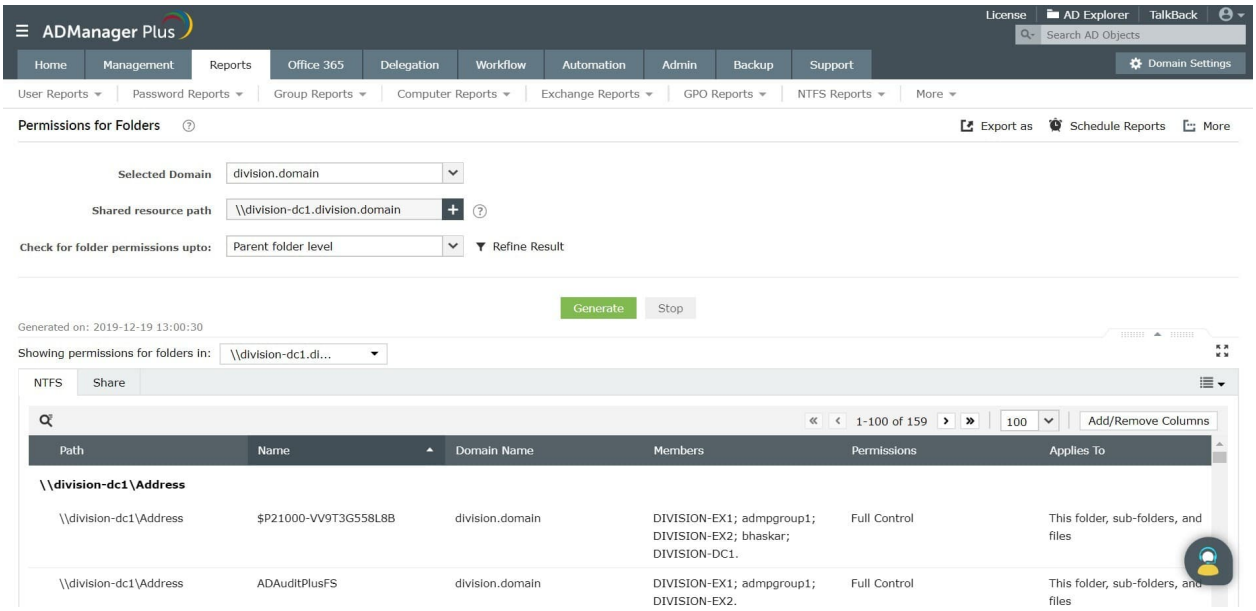
Objective: List down all the shares in a server and for any desired share, find out who's having what permission on the shares.

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 **Reports** and go to **NTFS Reports**.
2. Click **Permissions for Folders** report.
3. Select the domain of your choice.
4. Select the **Share resource path** for which you would like to see the list of users who have permissions on the share.
5. Select the **Check for folder permissions 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.
6. **Generate** the report.
7. You can search for any particular user, to see its permissions, using the **Quick Search** option.

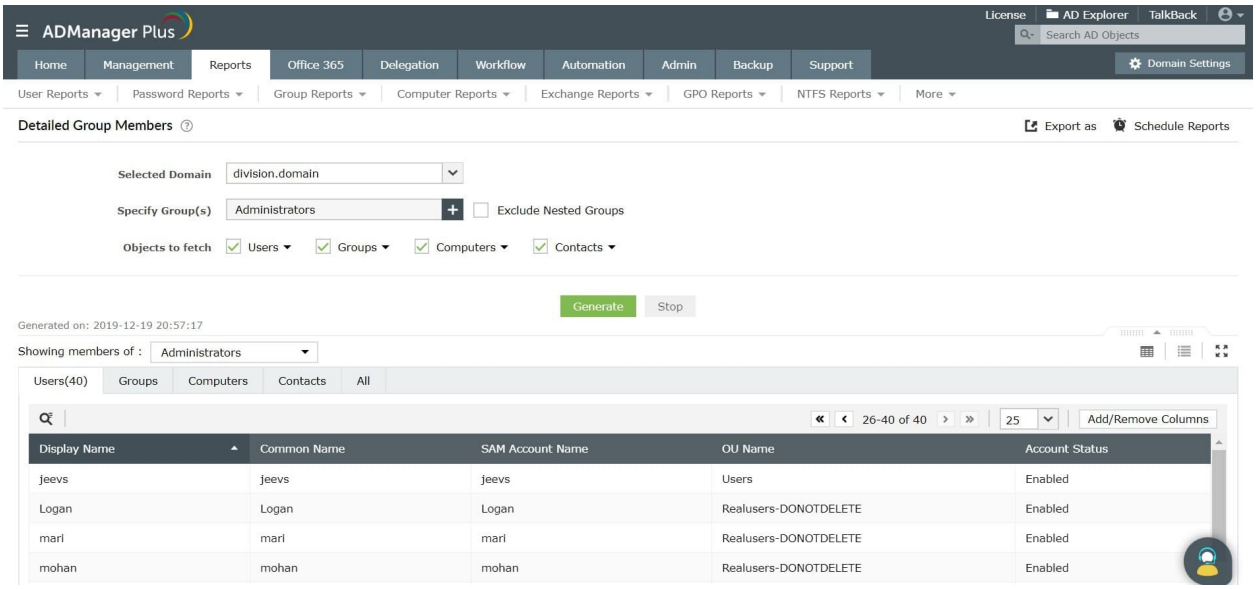


Exercise 3: List all the members of a group

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. Go to **Reports**.
2. Under **Group Reports**, click **Detailed Group Members** report.
3. Specify the domain and the groups 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).

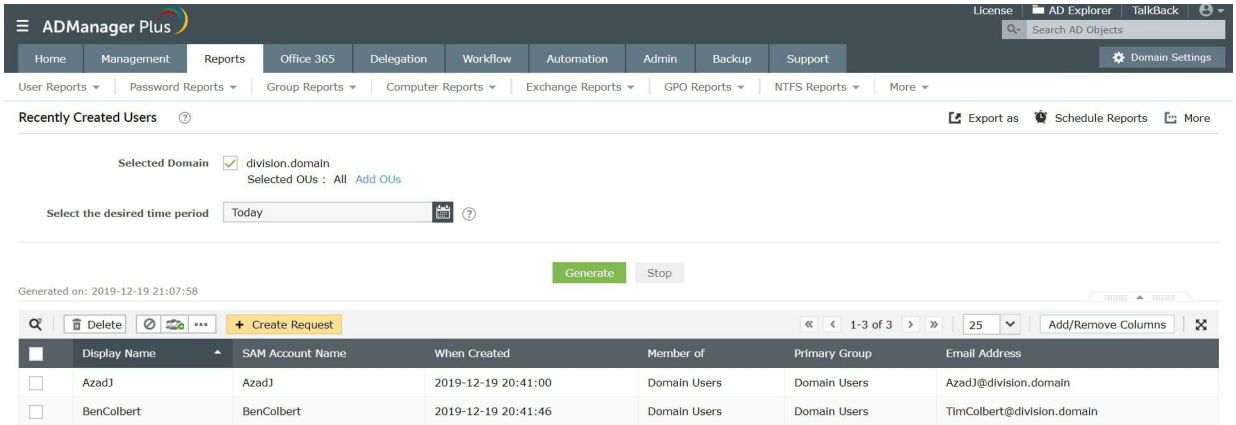


Exercise 4: Automatically send the list of users created in a particular day to a specified person

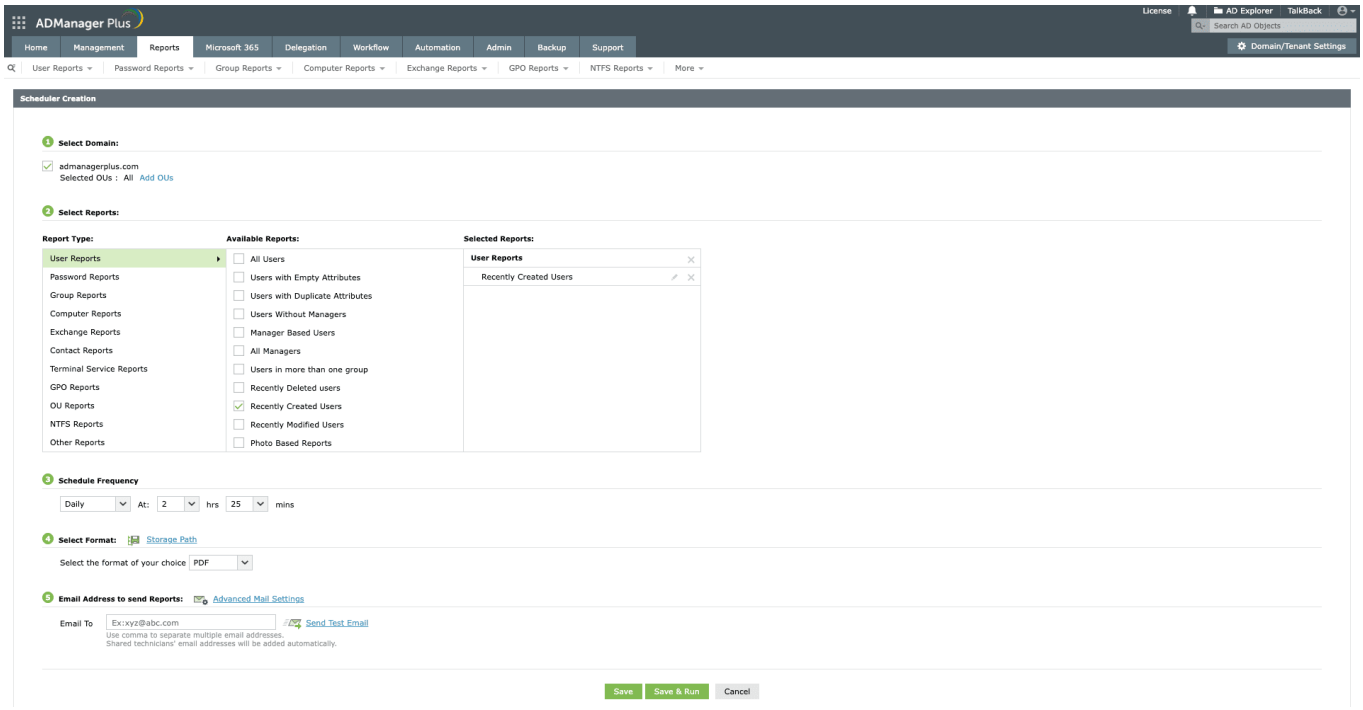
Objective: Generate a report of all the users who have been created in the day and send it in the required format to the concerned person over email . Also, send this report on a daily basis.

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

1. Click **Reports** tab.
2. Click **Recently Created Users** report under the **User Reports** section.
3. Select the domain and the OUs of your choice.
4. Select **Today** in the **Select the desired time period** field.
5. Click **Generate** to get a list of all the users created that day.



6. To schedule this report to be generated and emailed to the concerned person, on a daily-basis:
    a. Click **Schedule Reports**.
    b. Click **Create Schedule**
    c. Specify a suitable **Schedule Name**.
    d. Select the domain and the OUs of your choice.
    e. Under the **Select Reports** field, click **User Reports** under the *Report Type* section.
    f. In the **Available Reports** section, click **Recently Created Users**, and select **Today** in the **Select the desired time period** field.
    g. Click **Save.**
    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 Frequency* section.
    j. Specify the format in *Select Format*.
    k. Enter the email addresses to which the report has to be sent in the *Email Address to*
    l. *send Reports* section. More than one email address can be specified if you wish to send this report to more than one person.
    m. Click **Save**.

ii. 

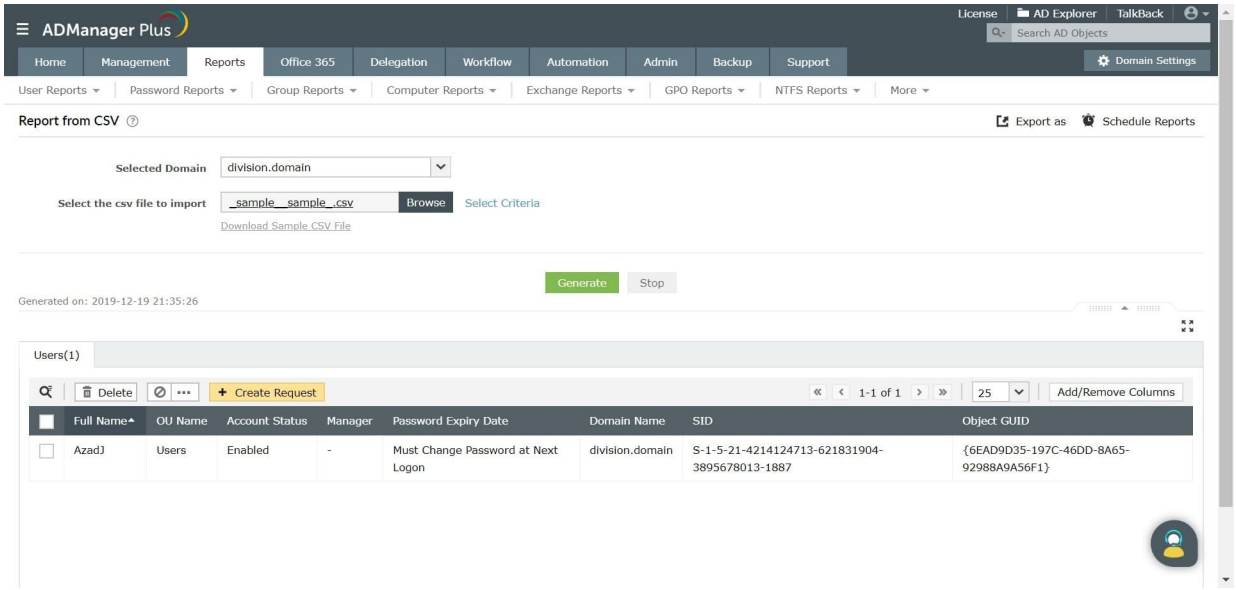
Exercise 5: Generating reports based on available attributes of users

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 **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.



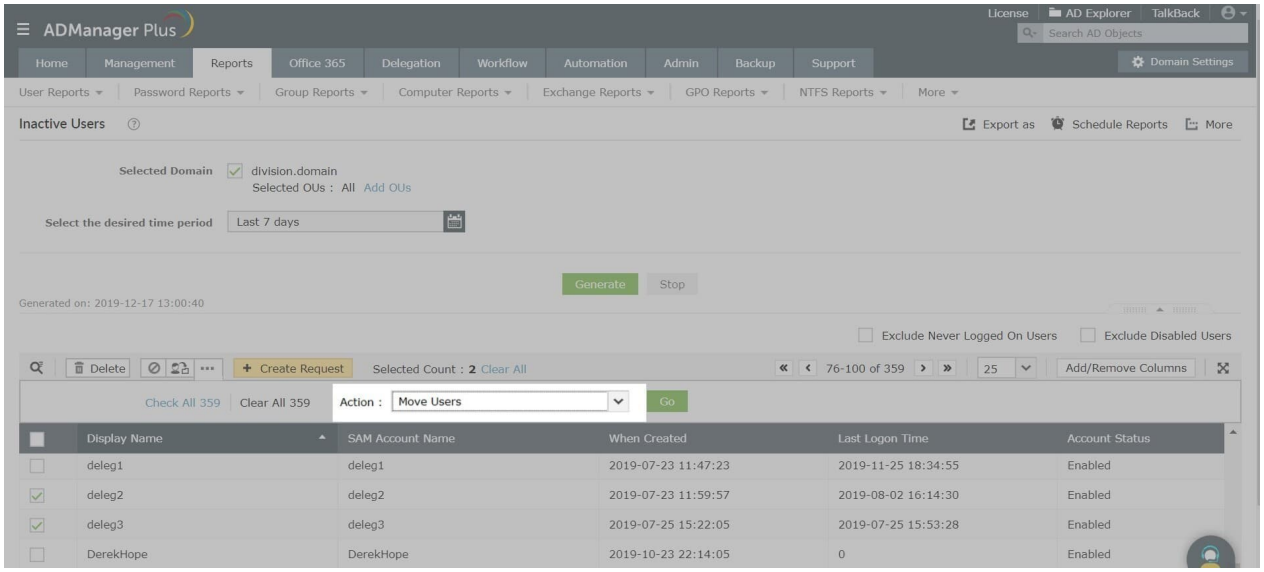
Management from AD reports

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 the **Reports** tab.
2. Under the **User Reports** section, click the **Inactive Users** report.
3. Select the domain of your choice.
4. Select the period of inactivity in the *Select the desired time period* field.
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 **Generate**.
7. You can modify the fields of this report by using the **Add or Remove columns** option.
8. Select the required users using the designated checkbox.
9. Click the **more actions** button and select the **Move Users** option listed under the **General attributes** section. Click **Go**.
10. You will now be directed to the **Move users to different container** page.
11. Specify the container of your choice.
12. Click **Apply** to move all the required inactive users to the specified OU.



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:

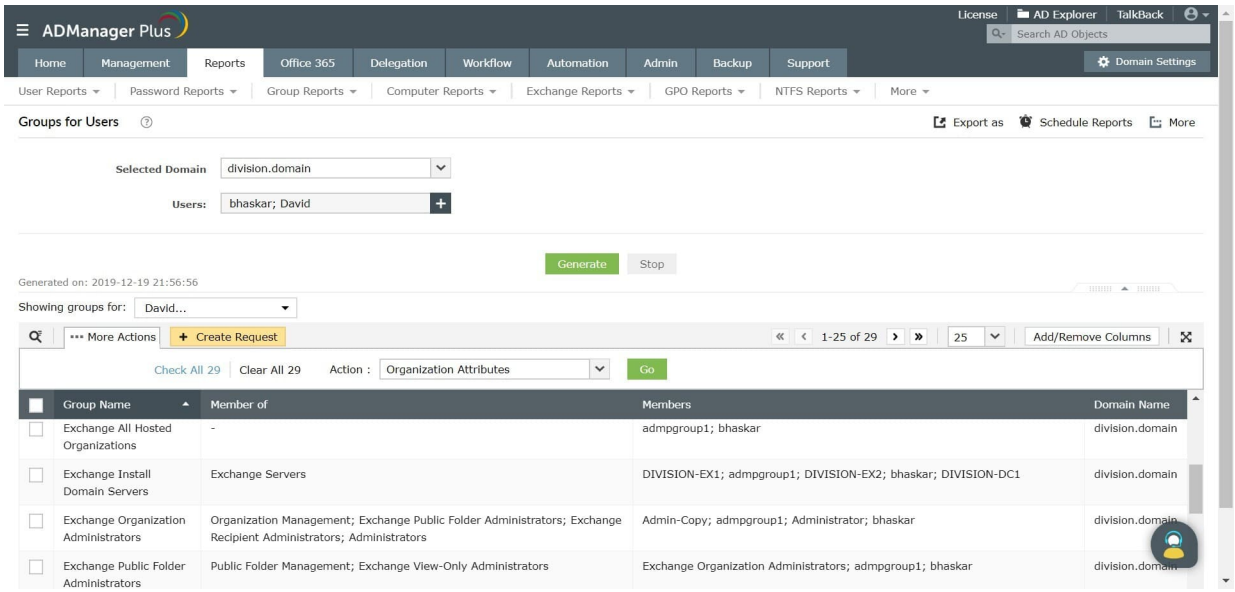
1. Click the **Reports** tab.
2. Under the **User Reports** section, click the **Locked-out Users** report.
3. Select the domain for which you would like to generate the list of locked-out users.
4. Click **Generate**.
5. Select all the users whose accounts you want to unlock and Click the **Unlock** icon.
6. Click **Apply** for the changes to take place.

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

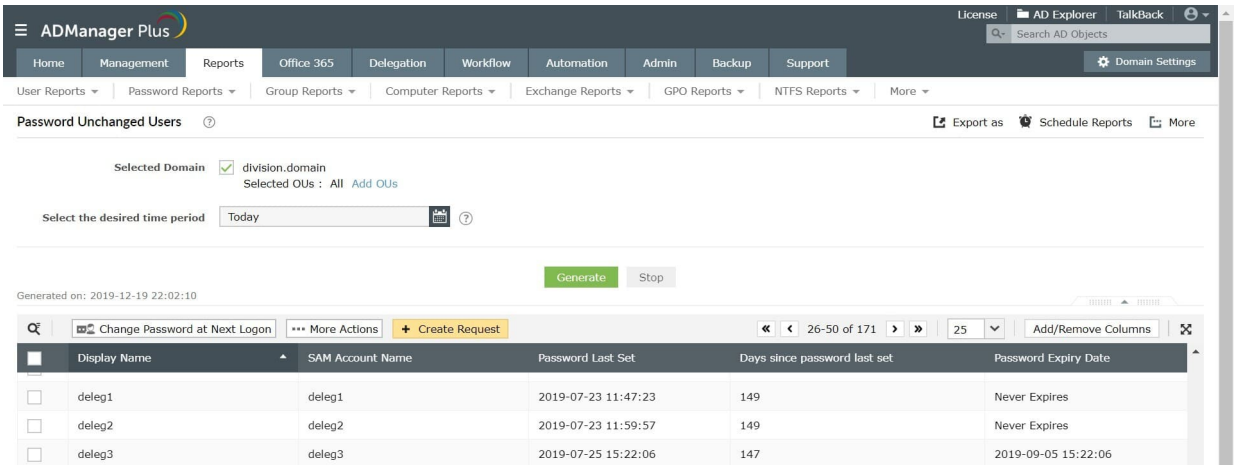


Exercise 4: Find the users who haven't changed their passwords and force them to change their passwords

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 the **Reports** tab.
2. Under **Password Reports,** select **Password Unchanged Users** report.
3. Select the domain of your choice.
4. Set the time since they last changed their passwords (say 60 days) in the *Select the desired time period* field.
5. Click **Generate**.
6. Select all the users and Click the **Change Password at Next Logon** option located next to the **Quick Search** option.
7. Click **OK**.

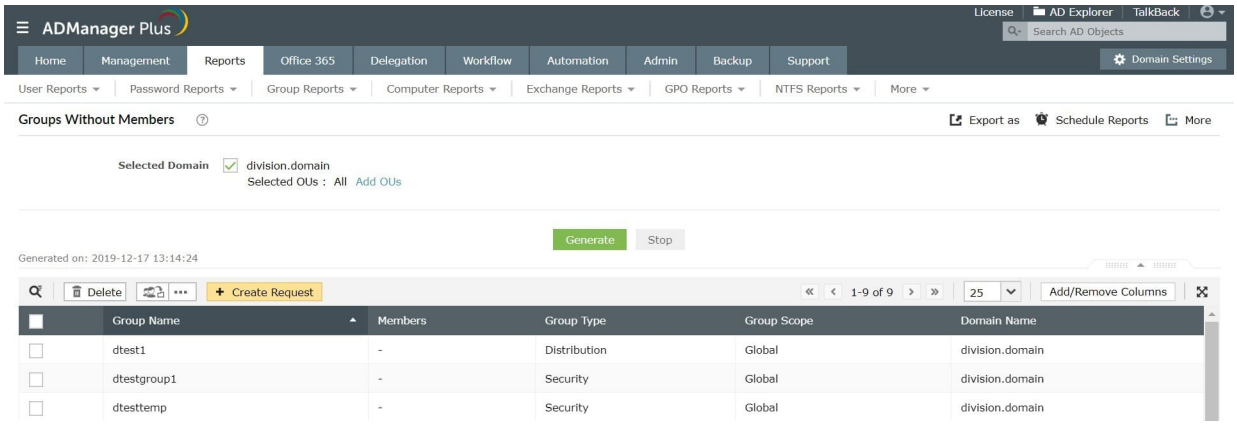


Exercise 5: Clean up empty groups

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 the **Reports** tab.
2. Click the **Group Reports** section and select the **Groups Without Members** report.
3. Select all the groups and Click the **Delete** icon.
4. Click **OK**.

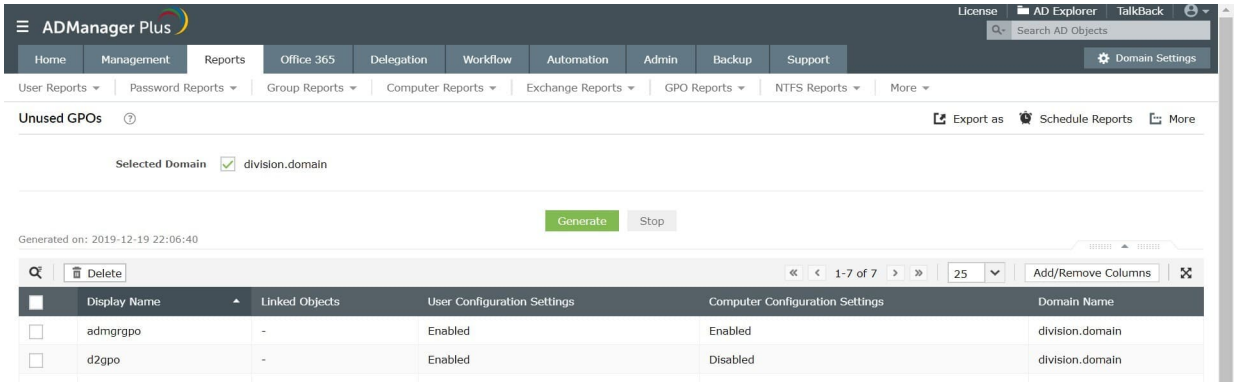


Exercise 6: Cleanup all the unused GPOs

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

Follow the steps given below:

1. Click the **Reports** tab and under the **GPO Reports** section, click the **Unused GPOs** report.
2. Select the domain and click **Generate**.
3. Select all the GPOs and click the **Delete** option.
4. Click **OK**.



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:

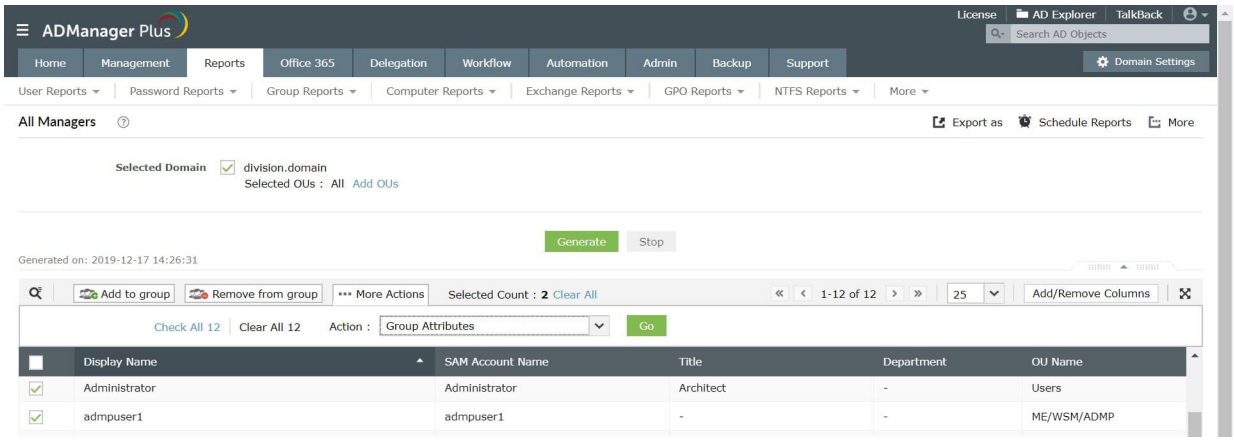
1. To list all the managers:

    a. Go to **Reports** tab.
    b. Click the **All Managers** report under the **User Reports** section.
    c. Select the domains and OUs 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 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 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.

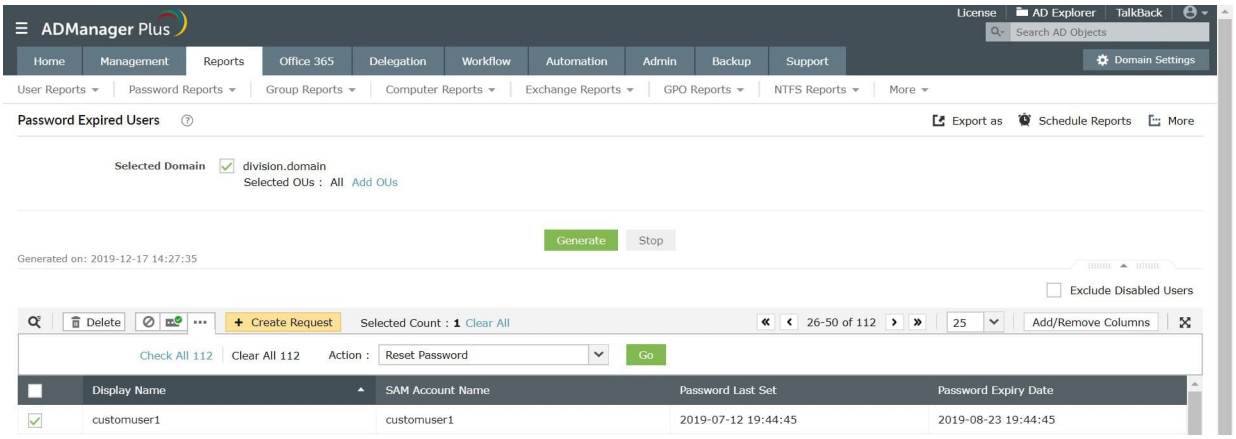


Exercise 8: Reset the passwords for all the password expired users

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. Go to the **Reports** tab.
2. Click the **Password Expired Users** report located under the **Password Reports** section.
3. Select the domains and OUs 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 **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.


ADManager Plus
License
AD Explorer
TalkBack
Search AD Objects
Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Backup
Support
Domain Settings
User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
GPO Reports
NTFS Reports
More
Password Expired Users
Export as
Schedule Reports
More
Selected Domain
division.domain
Selected OUs : All
Add OUs
Generate
Stop
Generated on: 2019-12-17 14:27:35
Exclude Disabled Users
Delete
Create Request
Selected Count : 1
Clear All
26-50 of 112
25
Add/Remove Columns
Check All 112
Clear All 112
Action :
Reset Password
Go
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. Microsoft 365 management and reporting

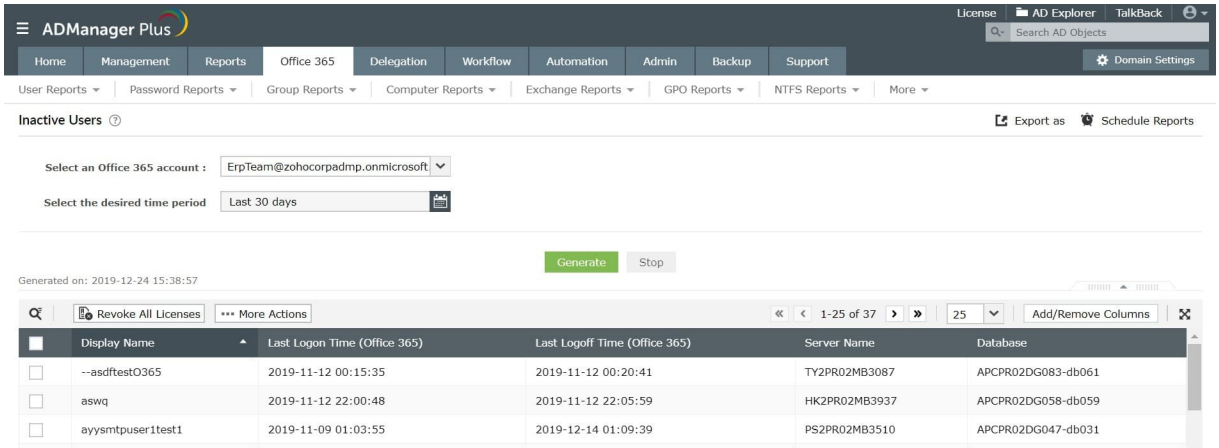
ADManager Plus helps you address the challenges of managing and reporting the cloud-based Microsoft 365, with ease. With this solution, you can manage user accounts in both on-premises and cloud-based environments from a single console, without struggling with numerous tools. It also allows parallel 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: Microsoft 365 users license modification

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

While making modifications in Microsoft 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 Microsoft 365 module.

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

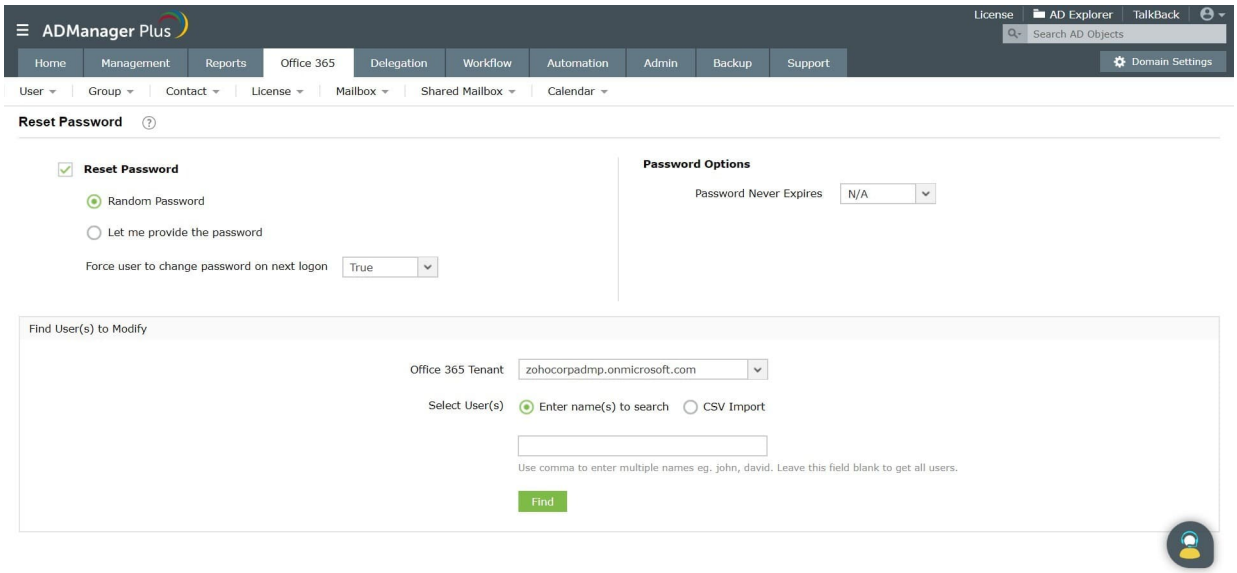


Exercise 2: Reset the passwords of Microsoft 365 users

Objective: To reset the passwords of multiple Microsoft 365 user accounts at one

go. Follow the steps given below:

1. Click the **Microsoft 365** tab.
2. Click the **Management** section.
3. Click 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 Microsoft 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.



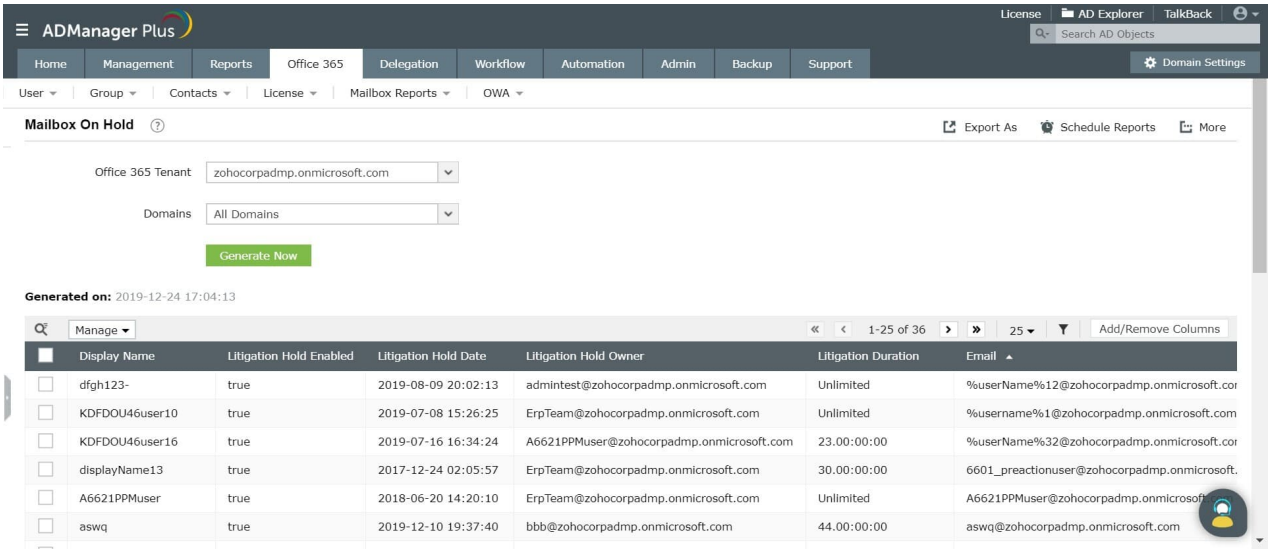
Exercise 3: Generate a report on all the users whose mailboxes are on litigation hold

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

Follow the steps given below:

1. Click the **Microsoft 365** tab and click the **Reports** section.
2. Click on **Litigation Hold Enabled Mailboxes** option located under the **Mailbox Reports** section.
3. Select the Microsoft 365 tenant account.
4. Use the *Filter By* option to show only domains or groups.

5. Click **Generate**.

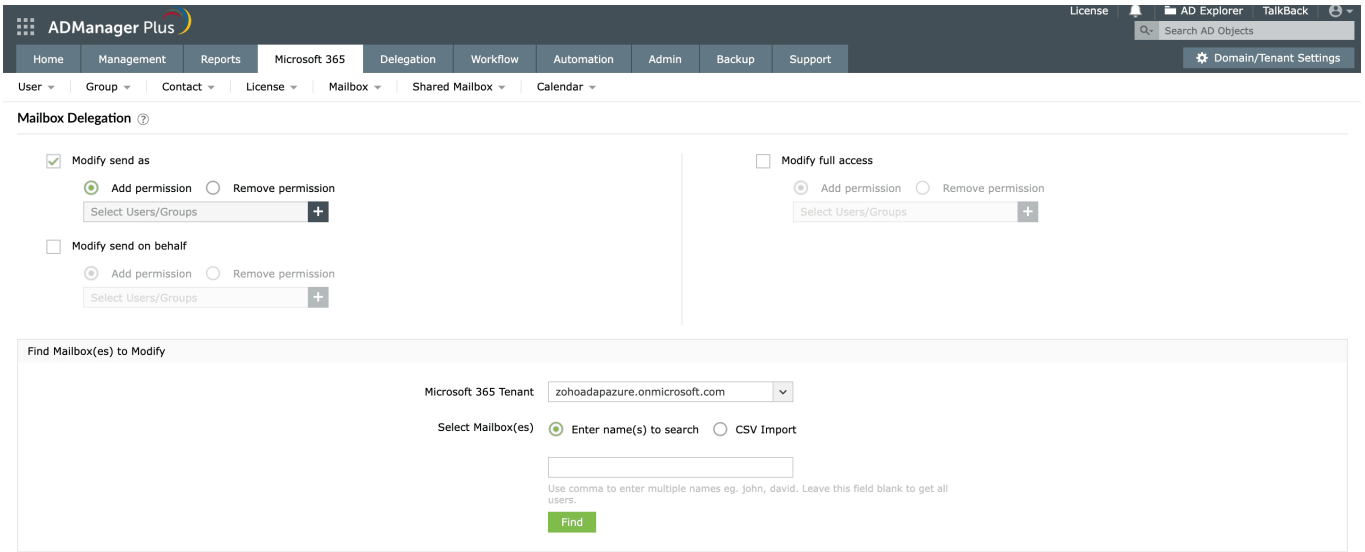


Exercise 4: Shared mailbox delegation

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

Follow the steps given below:

1. Click the **Microsoft 365** tab and click the **Management** section.
2. Click Shared **Mailbox Management** under the *Exchange Online* section.
3. Click **Mailbox Delegation**.
4. Enable the **Modify Send As** option and select the **Add permissions** option.
5. Click the **+** option to select the users to whom you want to assign the **Send As** permission.
6. Click **OK**.
7. Select the required Microsoft 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 **Apply**.

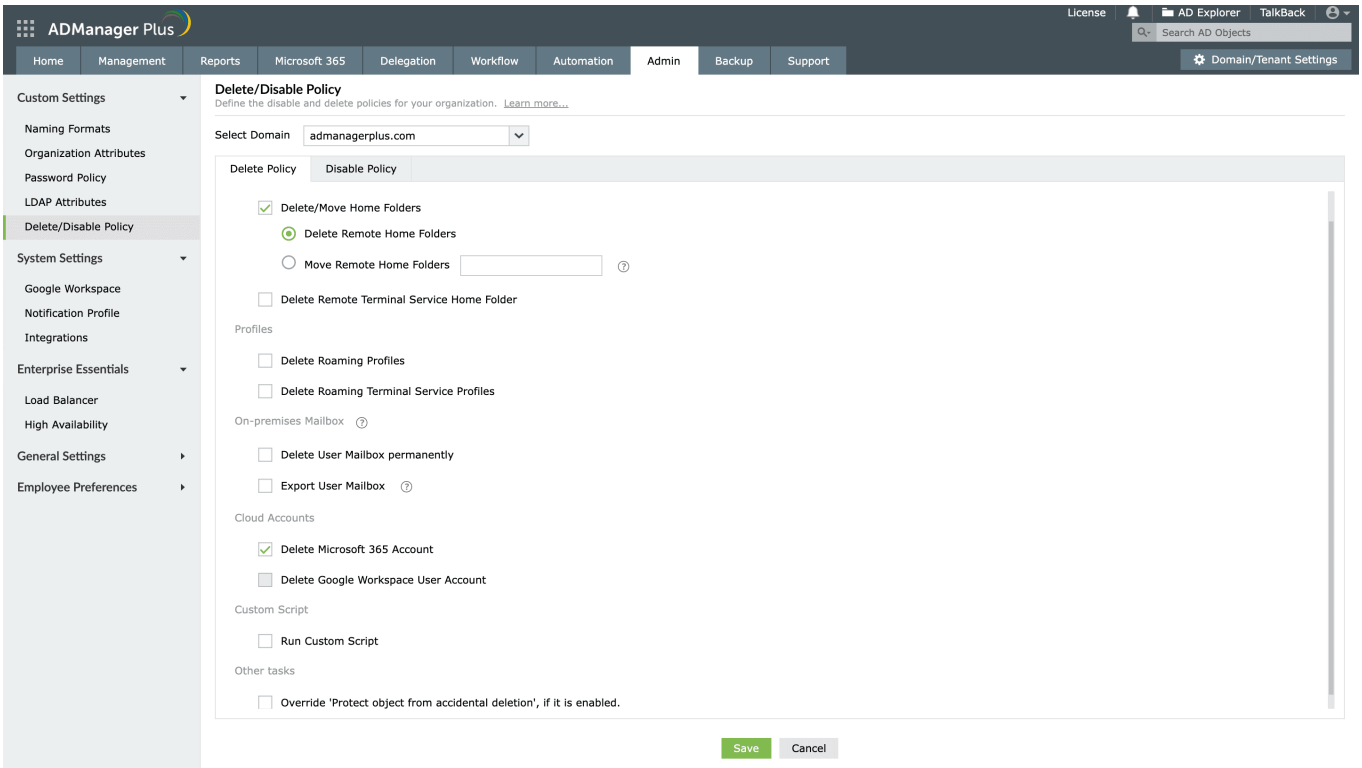


Exercise 5: Delete the Microsoft 365 account while deleting the linked AD user account

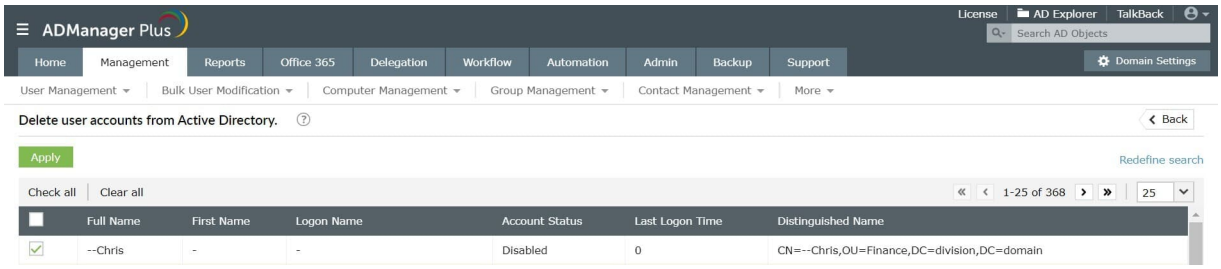
Objective: Delete the linked Microsoft 365 account whenever an AD user account is deleted.

Follow the steps given below:

1. Define the Delete/Disable Policy:
    a. Click the **Admin** tab.
    b. Under the **Custom Settings** section, click the **Delete/Disable Policy** option.
    c. Select the domain for which you want to define the policy.
    d. Click the **Delete Policy** tab.
    e. Under the *Cloud Accounts* section, select the **Delete Microsoft 365 Account** option.
    f. Click **Save**.



2. Delete a user:
    a. Click the **Management** tab.
    b. Click 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 **Apply**. Now, when the user is deleted, the linked Microsoft 365 account will also be deleted.



6. Backup and recovery

Accidental deletions and modification of 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 Safeguard your data effortlessly by backing up, restoring, and archiving AD and Azure AD objects. It also helps secure Google Workspace assets—including mailboxes, contacts, user drives, and calendar items—with ease.

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 in incremental backups

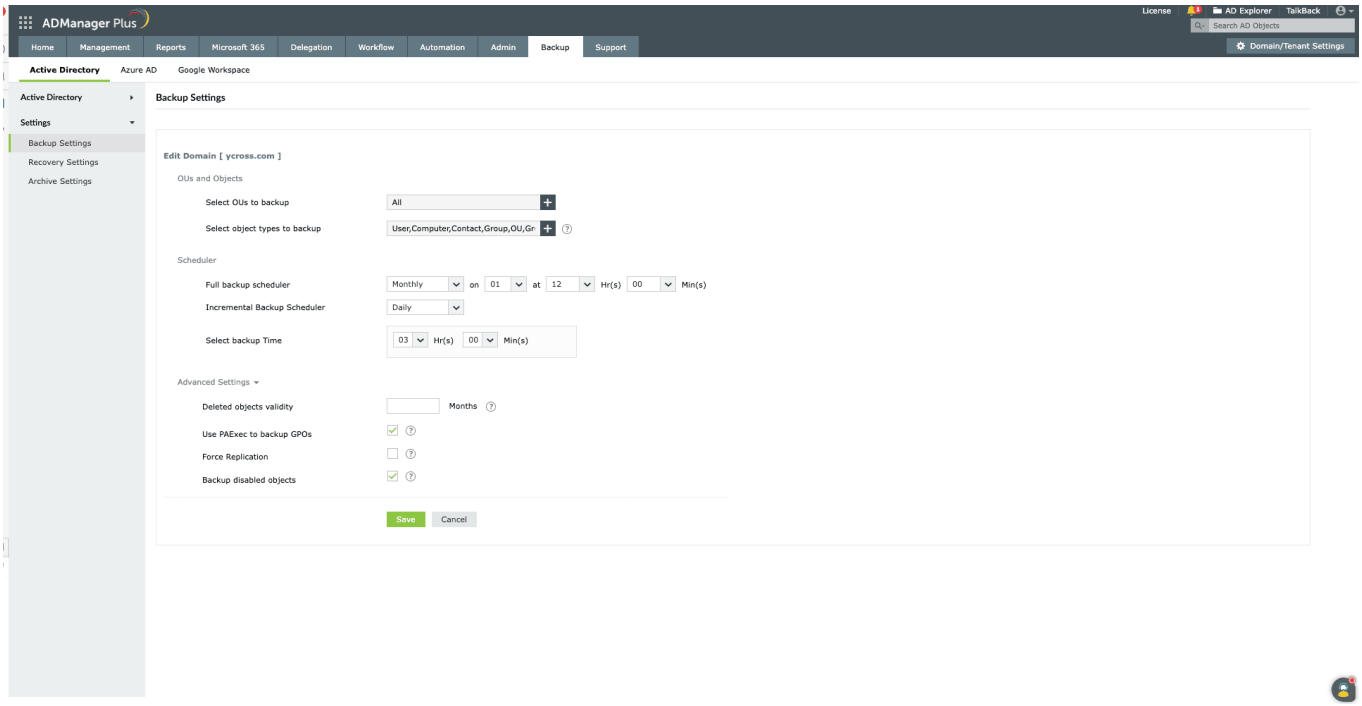
Objective: Create a backup schedule for a domain.

Solution**:**

1. Navigate to **Backup** → **Active Directory**. Under **Settings** on the left pane, select **Backup settings**.
2. Click the **Edit** icon next to the required domain name.
3. Click the **+** icon in the **Select object types to backup** field. In the pop-up that appears, select the objects and attributes that you wish to backup.

Note: All custom attributes created by you will be displayed, and you can easily add them. If any custom attribute is missing, search for the particular attribute by clicking the Add Attributes link and providing the LDAP name of the attribute.

4. In the **Increment Backup Scheduler** field, specify if you want the backup to be made daily.
5. Specify 3 Hrs in the **Select backup Time** field.
6. Enter the number of backups you would like to retain, and click **Advanced Settings** to configure the following:
7. In the **Deleted objects** validity field, specify the number of months you would like to hold deleted AD objects.
8. Enable the **Use PAExec to backup GPOs** option to back up GPOs using PAExec.
9. Check the **Force Replication** option to replicate the changes in your domain controllers before performing a backup.
10. Enable the **Backup disabled objects** option to back up disabled user and computer accounts as well.
11. Click **Save** to save the settings.

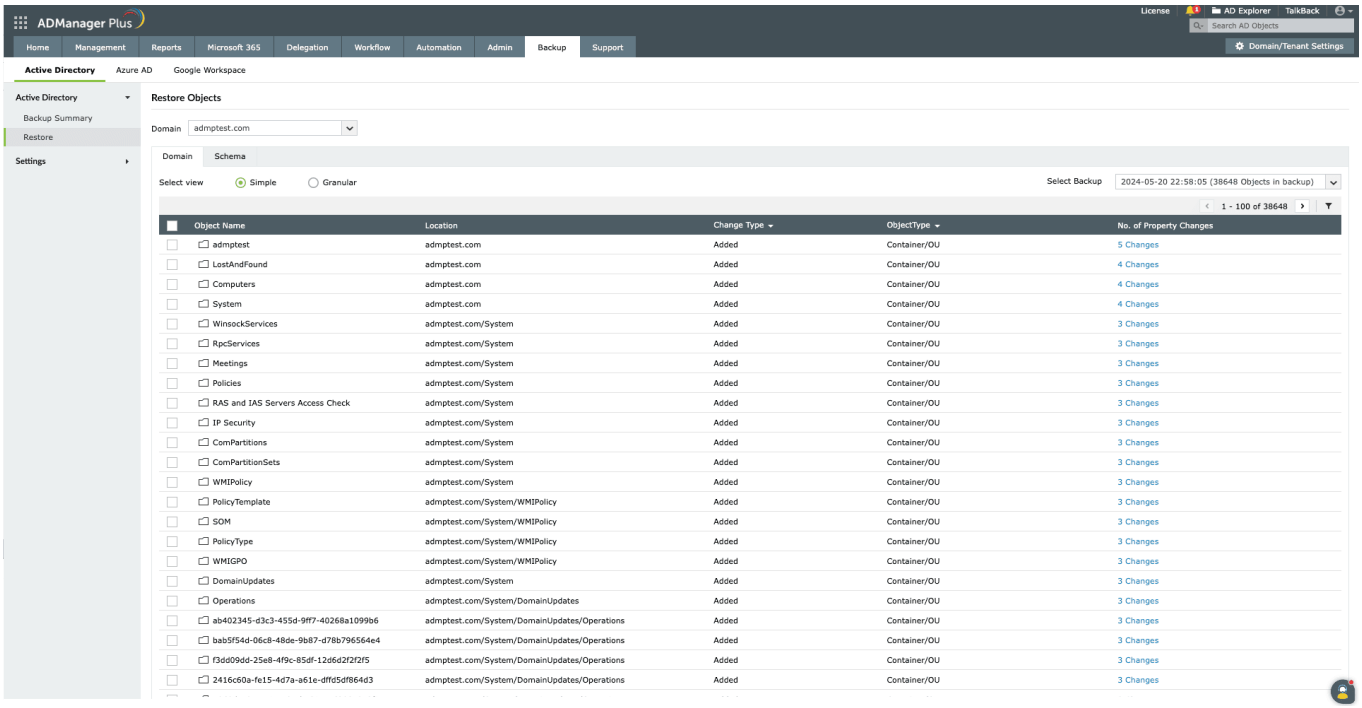


Exercise 2: You have inadvertently modified the attributes of all users, instead of a few specific users in an OU. Restore the attributes to their original values, for only the user objects which were modified accidentally

Objective: Restore specific attributes for AD users.

Solution:

1. Click 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.**

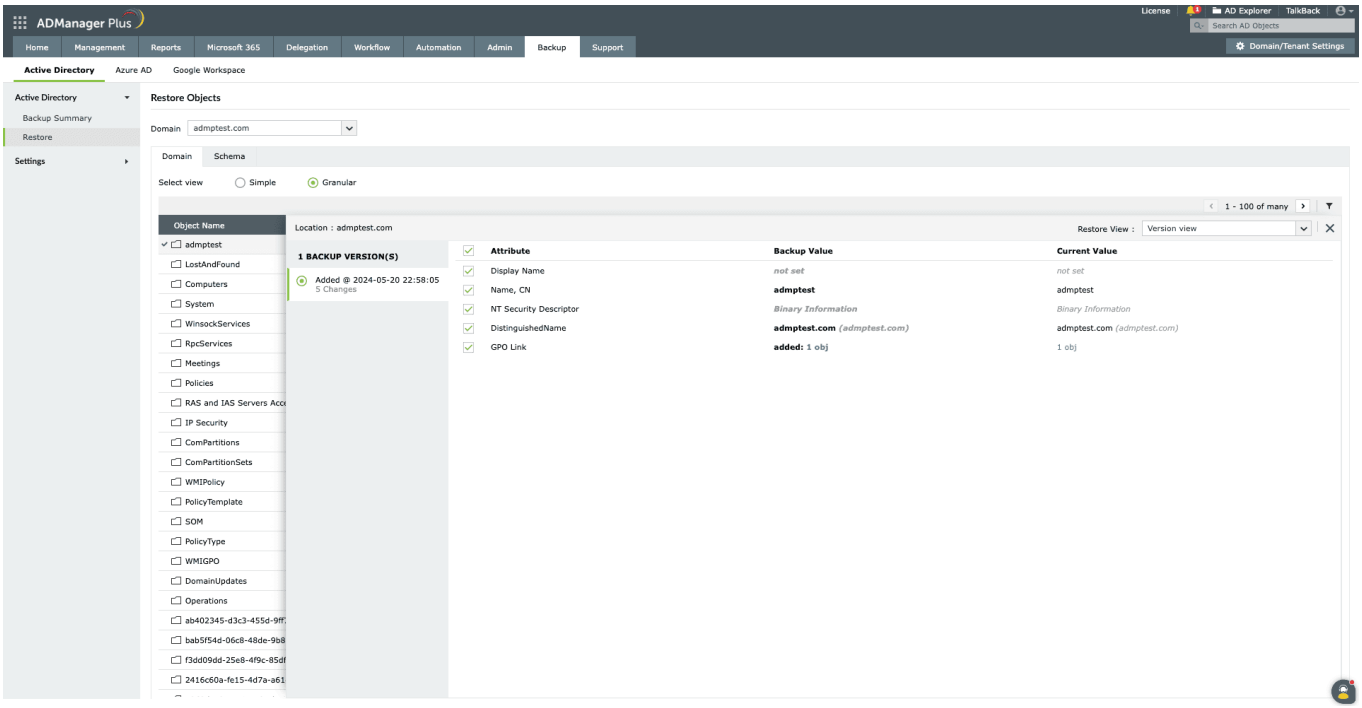


Exercise 3: You have accidentally modified an attribute. Revert to its original value.

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

Solution:

1. Click 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 in the *No. of backups* column. When you click the value, a pop-up opens with all the attributes. You can choose between **Version view** and **Attribute view**.
    - The **Version View** allows you to select a backup version from the specified 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 and the attribute you want to restore.
5. Click **Restore**.


ADManager Plus
License
AD Explorer
TalkBack
Search AD Objects
Home
Management
Reports
Microsoft 365
Delegation
Workflow
Automation
Admin
Backup
Support
Domain/Tenant Settings
Active Directory
Azure AD
Google Workspace
Active Directory
Backup Summary
Restore
Settings
Restore Objects
Domain
admptest.com
Domain
Schema
Select view
Simple
Granular
1 - 100 of many
Object Name
admptest
LostAndFound
Computers
System
WinsockServices
RpcServices
Meetings
Policies
RAS and IAS Servers Acc
IP Security
ComPartitions
ComPartitionSets
WMIPolicy
PolicyTemplate
SOM
PolicyType
WMIGPO
DomainUpdates
Operations
ab402345-d3c3-455d-9ff
bab5f54d-06c8-48de-9b8
f3dd09dd-25e8-4f9c-85df
2416c60a-fe15-4d7a-a61
Location : admptest.com
Restore View :
Version view
1 BACKUP VERSION(S)
Added @ 2024-05-20 22:58:05
5 Changes
Attribute
Backup Value
Current Value
Display Name
not set
not set
Name, CN
admptest
admptest
NT Security Descriptor
Binary Information
Binary Information
DistinguishedName
admptest.com (admptest.com)
admptest.com (admptest.com)
GPO Link
added: 1 obj
1 obj

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.

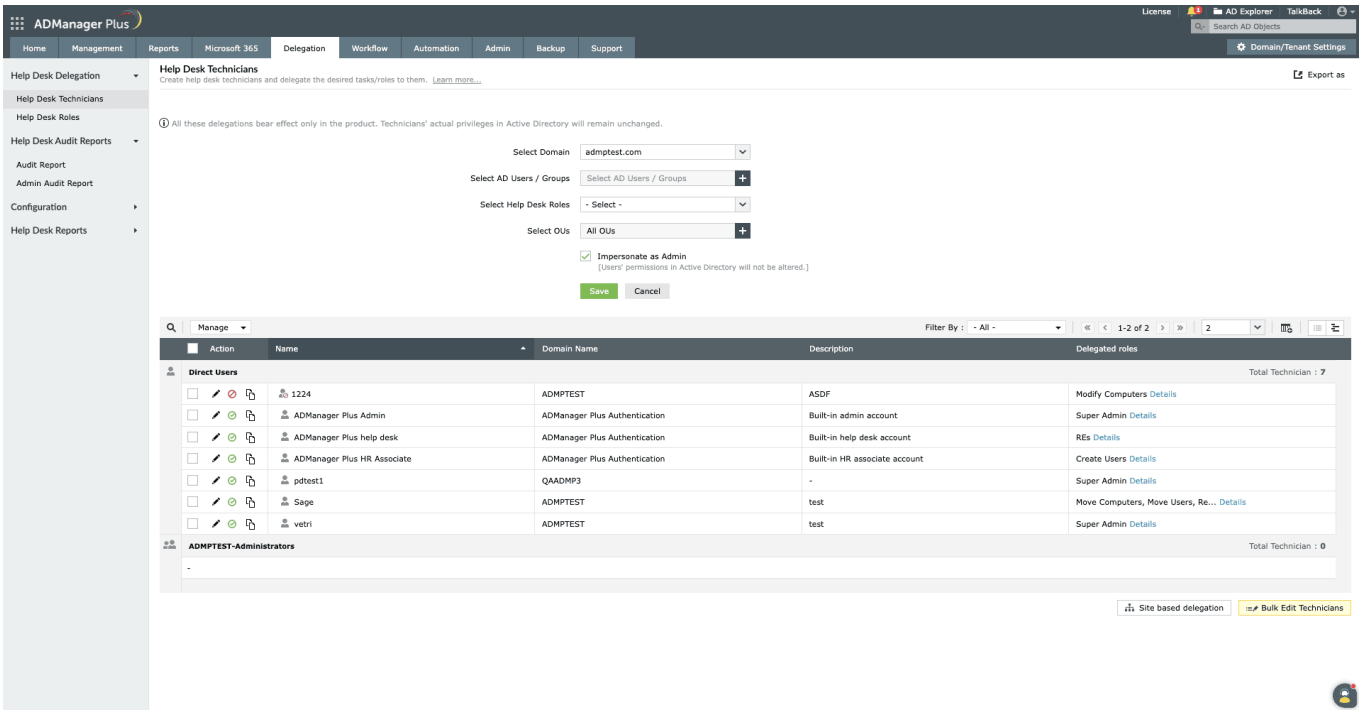
Exercise 1: Introduction to help desk technicians and help desk role

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 the **Delegation** tab and click on **Help Desk Roles** option, under **Help Desk Delegation** section on the left pane.
    b. Click **Create New Role** and enter a suitable name and description for the role.
    c. Navigate between the various tabs and select the designated check-boxes for delegating the required actions.
    d. Click **Save**.
2. To assign this role to a new technician:
    a. Click **Help Desk Technicians** and click **Add New Technician**.
    b. Select the domain of your choice.
    c. Select the AD user or Group, whom ever 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 **Save**.



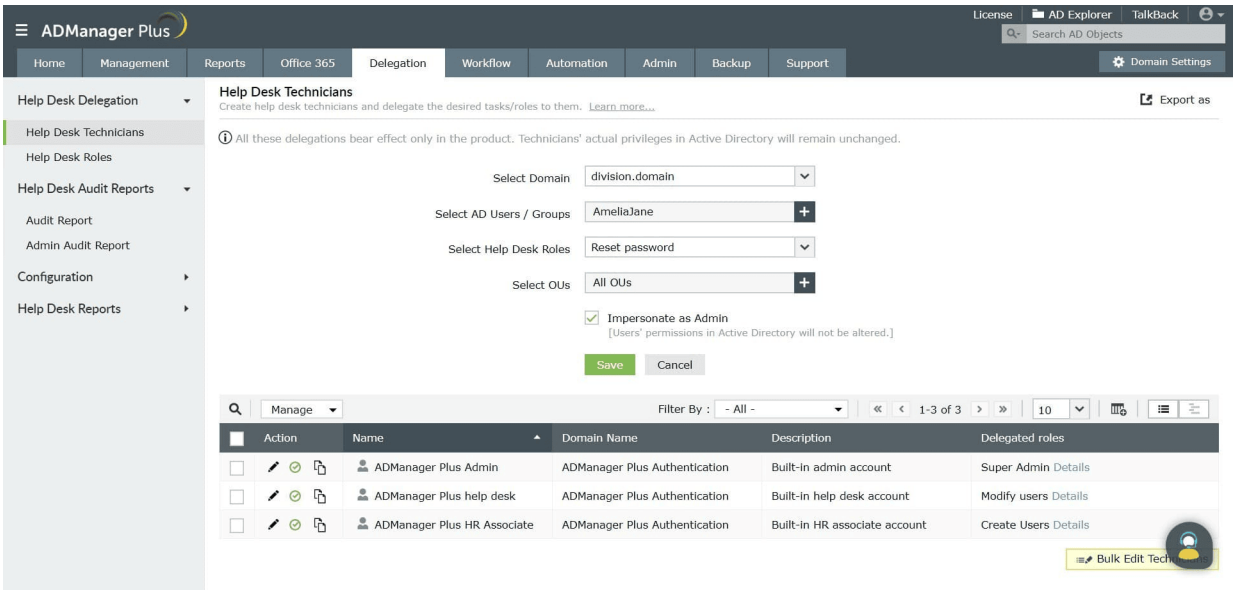
Exercise 2: Delegate the password reset action

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 objectives:

1. To create the Password Reset role:
    a. Click the **Delegation** tab and go to **Help Desk Roles**.
    b. Click **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 **AD Management** tab.
    e. Click on **+** beside the **Reset Password** option to specify the password options for the users.
    f. Click **Save**.

2. To assign the Password Reset role to a new technician:
    a. Click **Help Desk Technicians** and click **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 Help Desk Roles** field.
    e. Select the OUs 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 **Save** to make the selected user a help desk technician who can reset the passwords.



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 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).

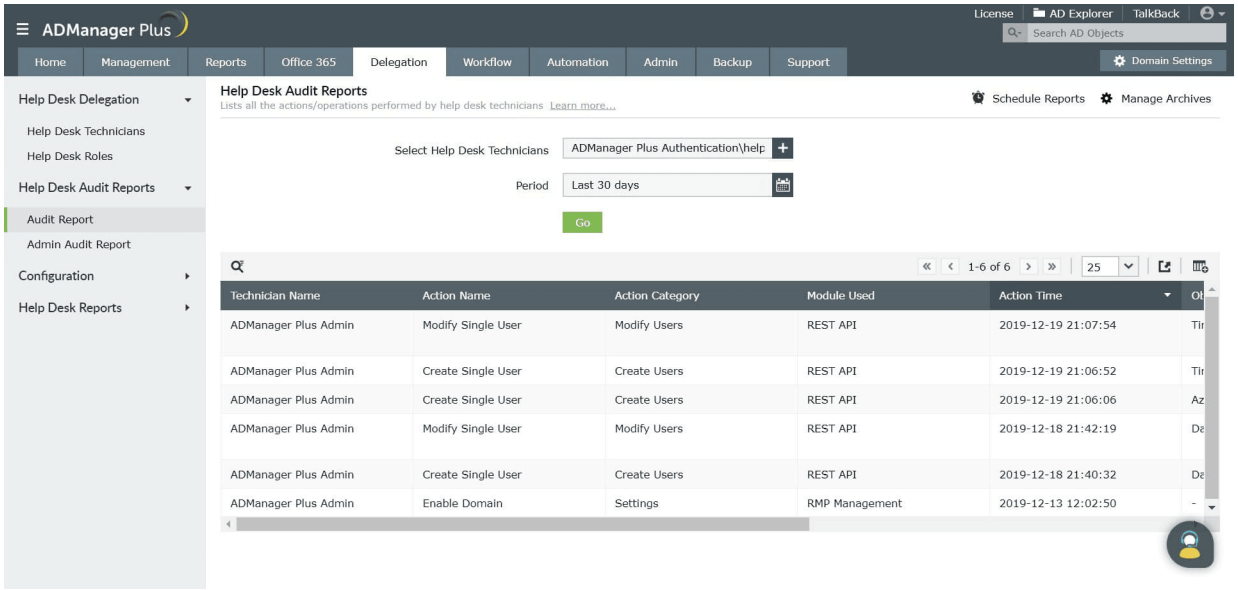
Exercise 4: Audit administrative activities by AD technicians

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 section under the Delegation tab, 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. Navigate to **Delegation** → **Help Desk Audit Reports** → **Audit Report.**
2. Select the name of the technician and the time-period.
3. Click **Go** to view the logs of the activities performed by the technicians.



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.

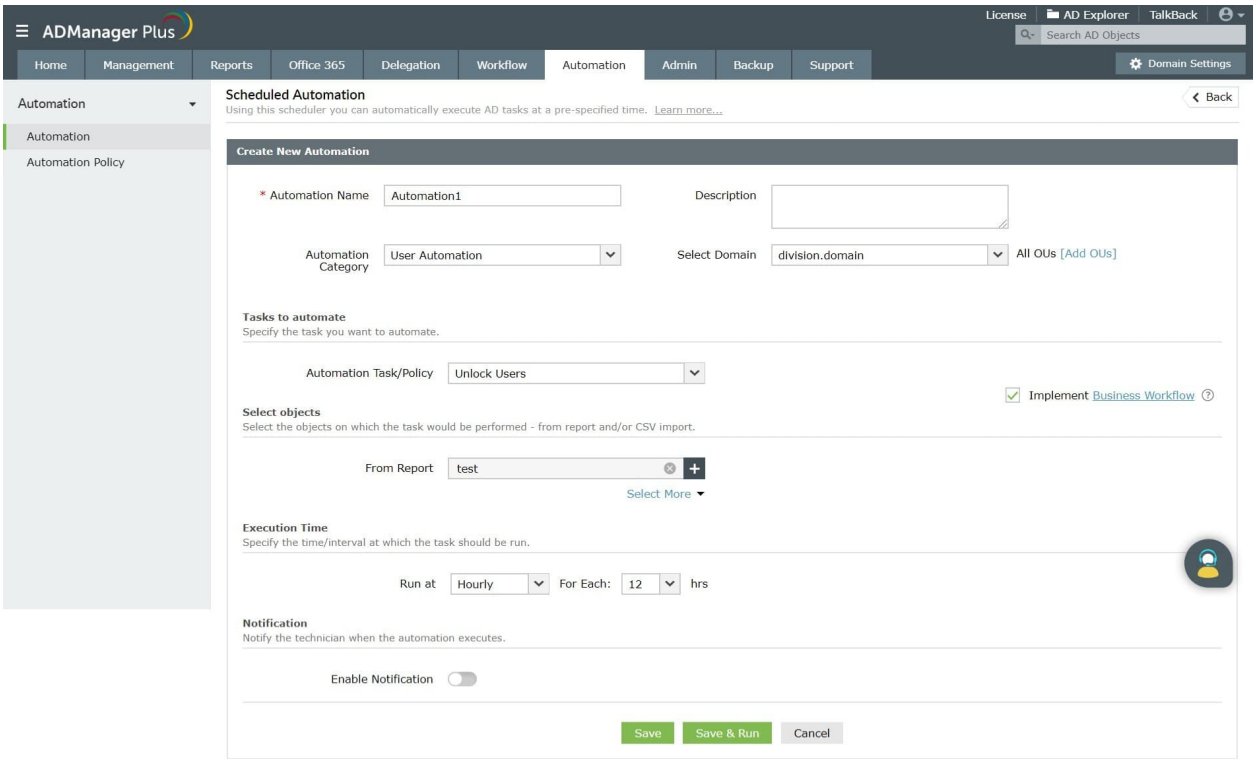
8.1 User automation

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 the **Automation** tab and go to the **Automation** option available on the left pane.
2. Click **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* field.
5. Select the domain in which the locked-out user accounts are located.
6. In the **Automation Task/Policy** field, select **Unlock Users**.
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 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 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**.
10. **Save** this automation to schedule the unlock operation.



Exercise 2: Automatically cleanup the inactive AD users

Objective: 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.

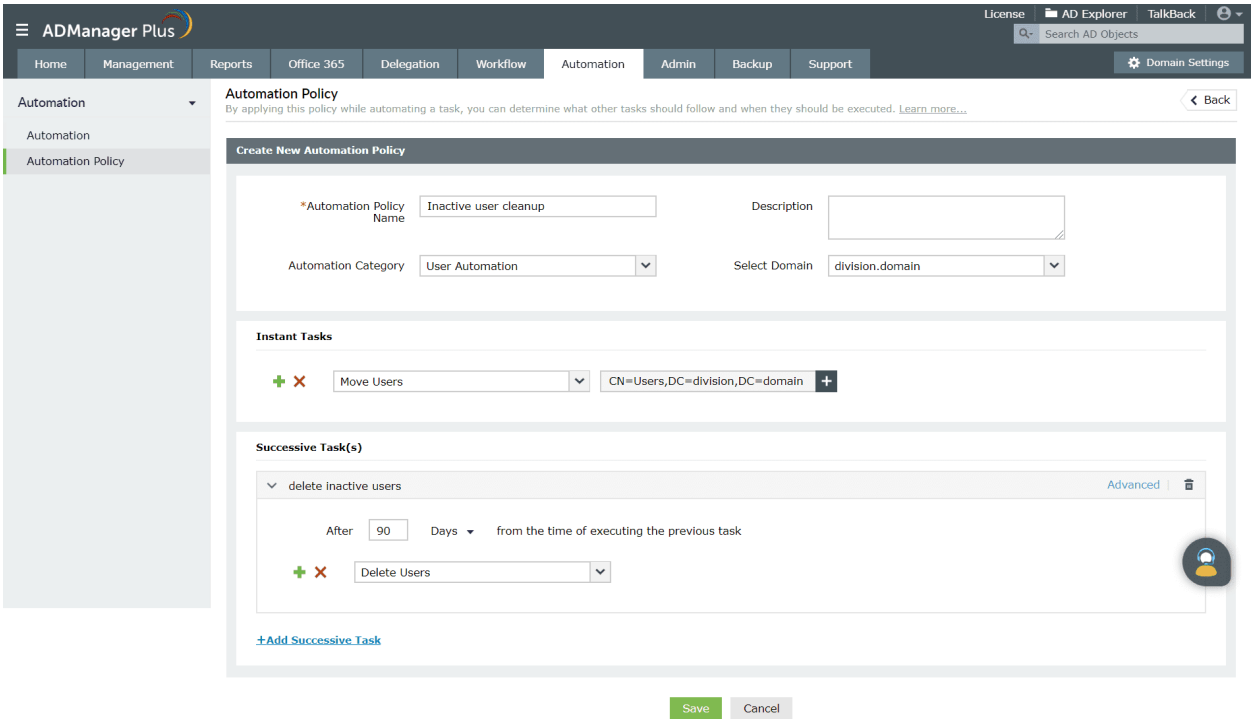
You can use the Automation Policy of ADManager Plus to accomplish the above requirement by:

- 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 the **Automation** tab.
    b. Click 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**.
   Set the time limit to After 90 days.
h. Set the task to **Delete Users**.
i. **Save** this automation policy.



2. To create an Automation,
   a. Click 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.

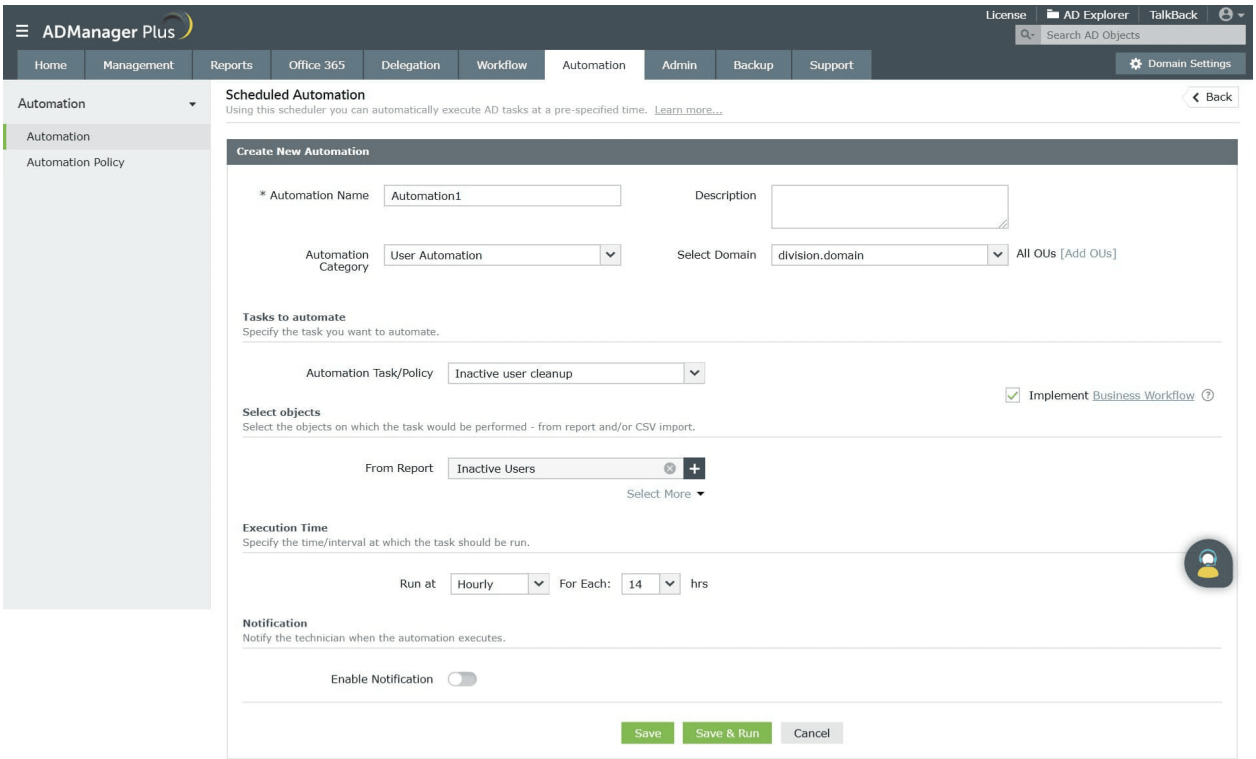
   From Reports,

Click 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.

From a CSV,

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

a. Select the **Implement Business Workflow** option, if you want to review or approve of every task before it is actually executed.
b. Specify the **Time Interval** at which the automation must be executed.
c. Specify the frequency for the automation to be repeated.
d. Enable notifications to be sent to either technicians or the administrator, whenever this automation is executed.



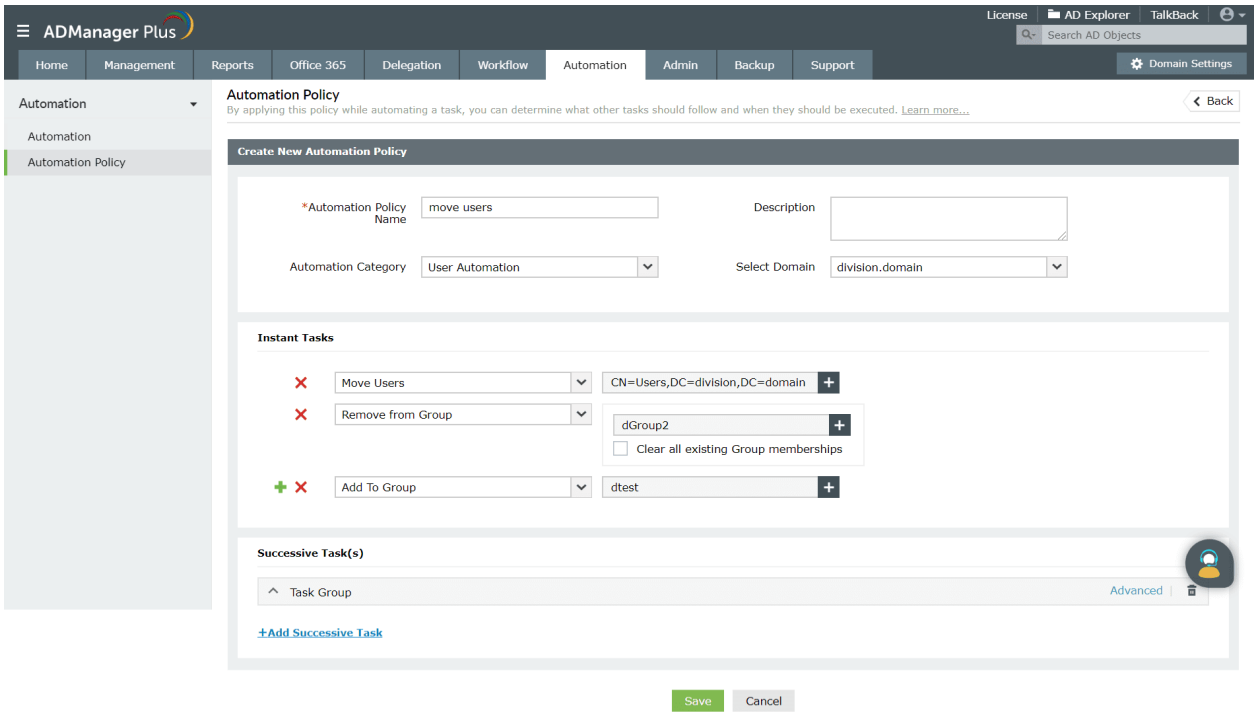
Exercise 3: Modify location specific user attributes using automation policy

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.

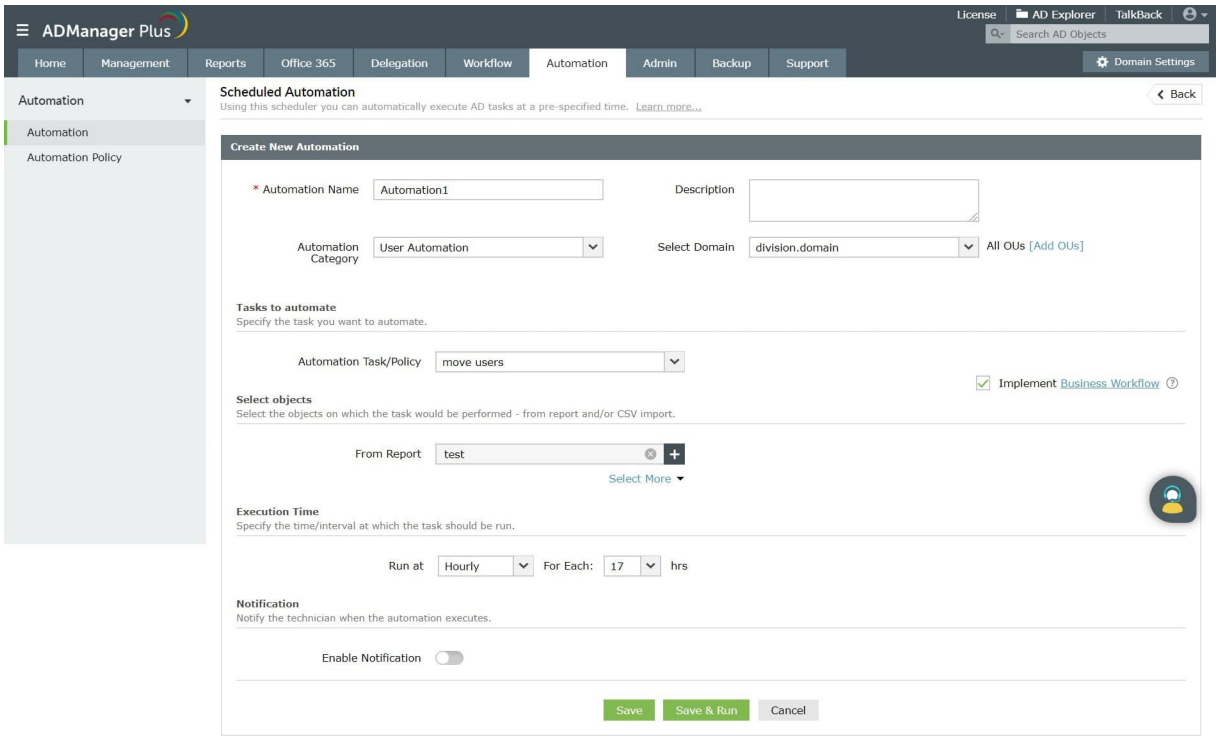
Such tasks need to be performed manually using native AD tools.
However in ADManager Plus, using Automation Policy we can add/remove group membership and move the users to different OUs quite easily.

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

1. To create a new policy
    a. Click the **Automation** tab.
    b. Click the **Automation Policy** option available on the left pane and click **Create New Automation 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. In the **Instant Tasks** section,
        i. Select **Move Users** and select the **Container** to which you want to move the users.
        ii. Click the green **+** option to the left to the **Move Users** task to add another task.
        iii. Select the **Remove from Group** option from the task list and enable the **Clear all existing Group memberships**.
        iv. Select the groups from which you want to remove these users.
        v. Click the **+** option to the left to the **Remove from Group** task to add another task.
        vi. Select the **Add to Group** option from the task list and select the required groups.
    g. **Save** this Automation Policy.



2. To create an automation,
    a. Click 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 the **Select** link and select the required report.
        ii. From a CSV:
        Click 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** .



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.

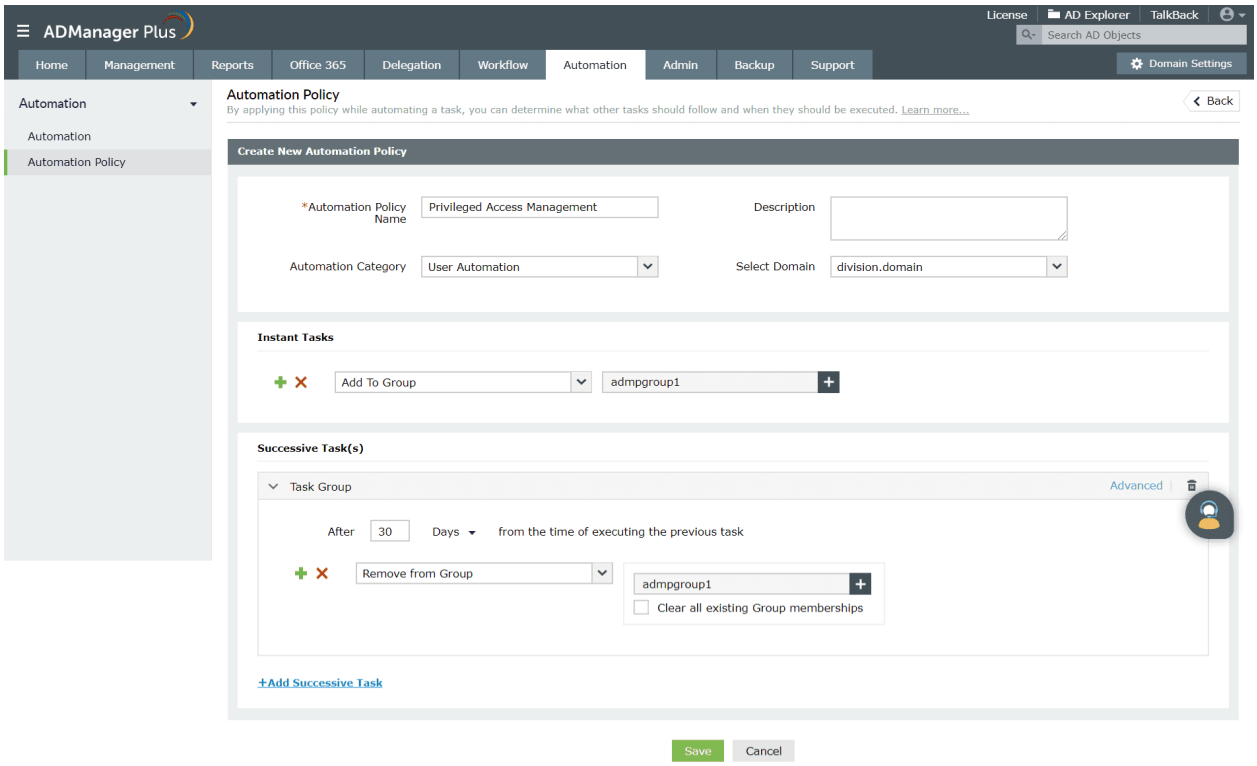
Follow the steps given below:

1. To create a new policy
    a. Click the **Automation** tab.
    b. Click 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.



2. To create an automation,

   a. Click 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.

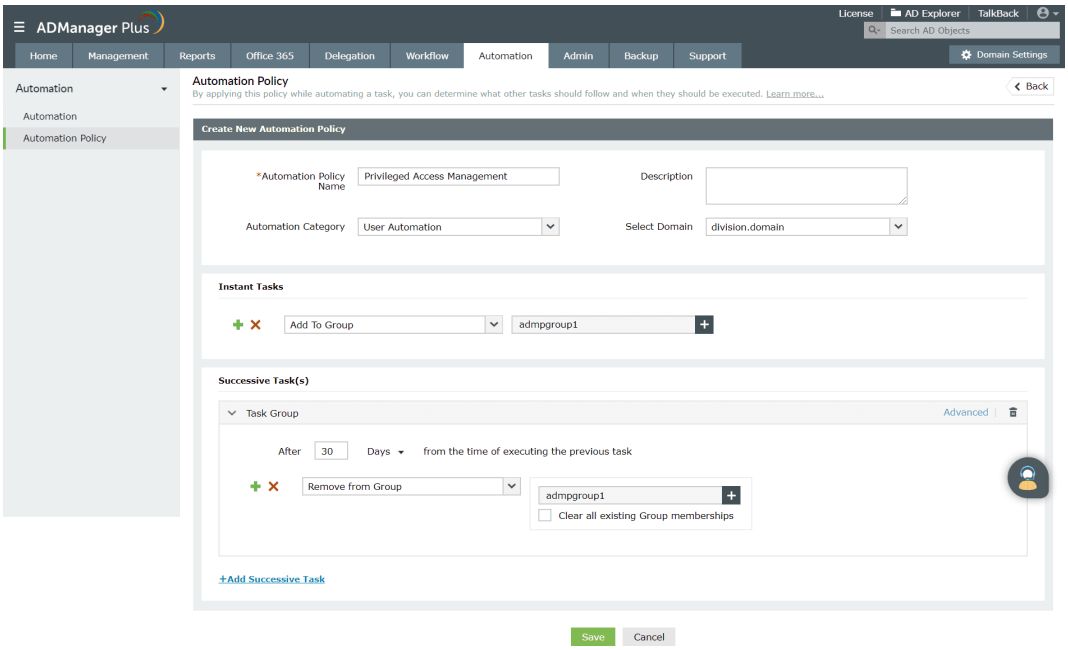
   g. You can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.

      i. From Reports:
      Click 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 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**.



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.

8.2 Access certification campaigns

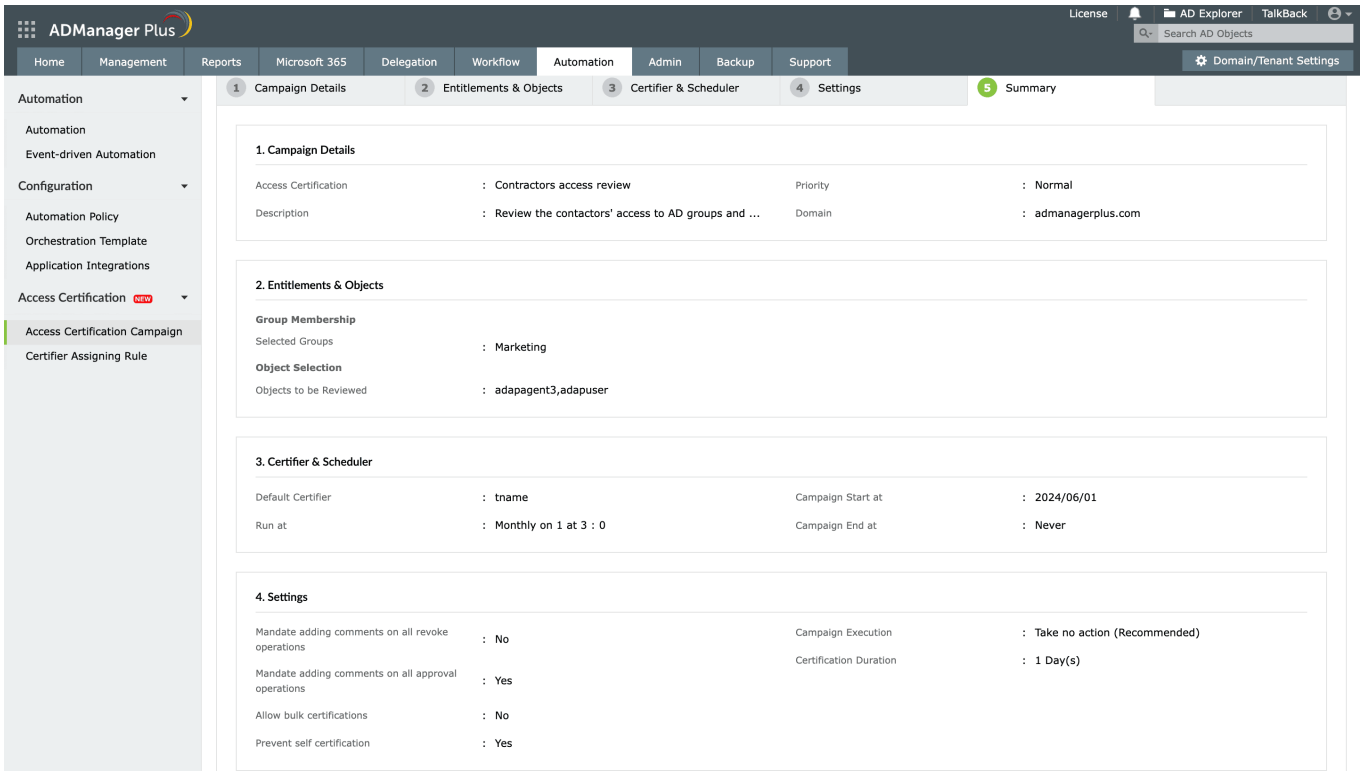
Exercise 1: Automatic reviewing of vendor and contractor access to resources

Scenario: Organizations have vendors or contractors that are given temporary access to enterprise systems. Automate reviewing their permissions at specified intervals to ensure they can only access what is necessary for their tasks and only for the duration they require.

` Follow the steps given below:

1. Navigate to **Automation** → **Access Certification** → **Access Certification Campaign**.
2. The resulting page will show all the existing campaigns and their details. To create a new campaign, click on **Create New Campaign** in the top-right corner.
3. Under **Campaign Details** tab, provide the below details:
    - **Certification Campaign Name**: Contractors access review
    - **Description**: Review the contactors' access to AD groups and revoke if not needed
    - **Priority**: High
    - **Select Domain**: Domain in which the campaign must be run.
4. Once all the above details are entered, click **Next**.
5. Under **Entitlements & Objects**, specify the below details:
    - In the *Entitlement Selection* section, under the **Active Directory** tab, toggle the button beside *Group Membership* and select the group(s) to be reviewed.
    - In the *Object Selection* section, select **User** and choose the filter mentioned below,
        - **Select User(s)**: Manually choose the contractors names that need to be reviewed.
6. After completing all the above steps, click **Next**.
7. In the **Certifier & Scheduler** tab, within the *Certifier* section, select a **Default Certifier** or choose an certifier assigning rule to assign a technician dynamically. Click here to learn how to create a certifier assigning rule.
8. In the *Scheduler* section, you can define the following details:
    - **Start Date**: Specify the current date.
    - **Run at**: Specify the frequency at which the campaign must be run. Here you can choose the campaign to be run on the 1st of every month at 10am.
    - **End**: Select **Never** to keep the campaign running indefinitely.
9. Click **Next**.
10. Under the **Settings** tab**,** you can select **Mandate adding comments on all revoke operations** in the *Configuration* section.
11. In the *Campaign Settings* section, you can define the below actions:
    - **Certification Request Expiration**: Configure as 1 week
        - Select **Send reminder to certifiers** and configure notifications to be sent everyday, continuously after 1 day of request creation.
    - **Campaign Execution**: You can select a default action to be performed when the certifier has not approved or revoked an access request. You can select Take no action (Recommended).

- Click **Next** and go to the *Summary* tab to review the campaign.
- Click **Save.**



Exercise 2: Run access certification campaign to review both AD and M365 group memberships in a single campaign

Scenario: To review both AD and M365 group memberships of the team members in a single campaign for every 2 months and assign it to the manager

Follow the steps given below:

1. Navigate to **Automation** → **Access Certification** → **Access Certification Campaign**.
2. The resulting page will show all the existing campaigns and their details. To create a new campaign, click on **Create New Campaign** in the top-right corner.
3. Under **Campaign Details** tab, provide the below details:
    - **Certification Campaign Name**: Group membership review
    - **Description**: Review AD and M365 group memberships
    - **Select Domain**: Domain in which the campaign must be run.
4. Once all the above details are entered, click **Next**.
5. Under **Entitlements & Objects**,
    - In the *Entitlement Selection* section, under the **Active Directory** tab, toggle the button beside *Group Membership* and select the group(s) to be reviewed.
    - In the *Object Selection* section, select **Group** and choose the filter mentioned below,
        - **Select Group(s)**: Manually choose the team whose access needs to be reviewed.
    - Under the **Microsoft 365** tab, toggle the button beside *M365 Group Membership* and select the

group(s) to be reviewed.
    - In the *Object Selection* section, select **Group** and choose the filter mentioned below,
        - **Select Group(s)**: Manually choose the team whose access needs to be reviewed.
6. After completing all the above steps, click **Next**.
7. In the **Certifier & Scheduler** tab, within the *Certifier* section, select a **Default Certifier** or choose an certifier assigning rule to assign a technician dynamically. Click here to learn how to create a certifier assigning rule.
8. In the *Scheduler* section, you can define the following details:
    - **Start Date**: Specify the current date.
    - **Run at**: Specify the frequency at which the campaign must be run. Here you can choose the campaign to be run on the 1st of every month at 10am.
    - **End**: Select **Never** to keep the campaign running indefinitely.
9. Click **Next**.
10. Under the **Settings** tab**,** you can select **Mandate adding comments on all revoke operations** in the *Configuration* section.
11. In the *Campaign Settings* section, you can define the below actions:
    - **Certification Request Expiration**: Configure as 1 week
        - Select **Send reminder to certifiers** and configure notifications to be sent everyday, continuously after 1 day of request creation.
    - **Campaign Execution**: You can select a default action to be performed when the certifier has not approved or revoked an access request. You can select Take no action (Recommended).
12. Click **Next** and go to the *Summary* tab to review the campaign.
13. Click **Save.**

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.

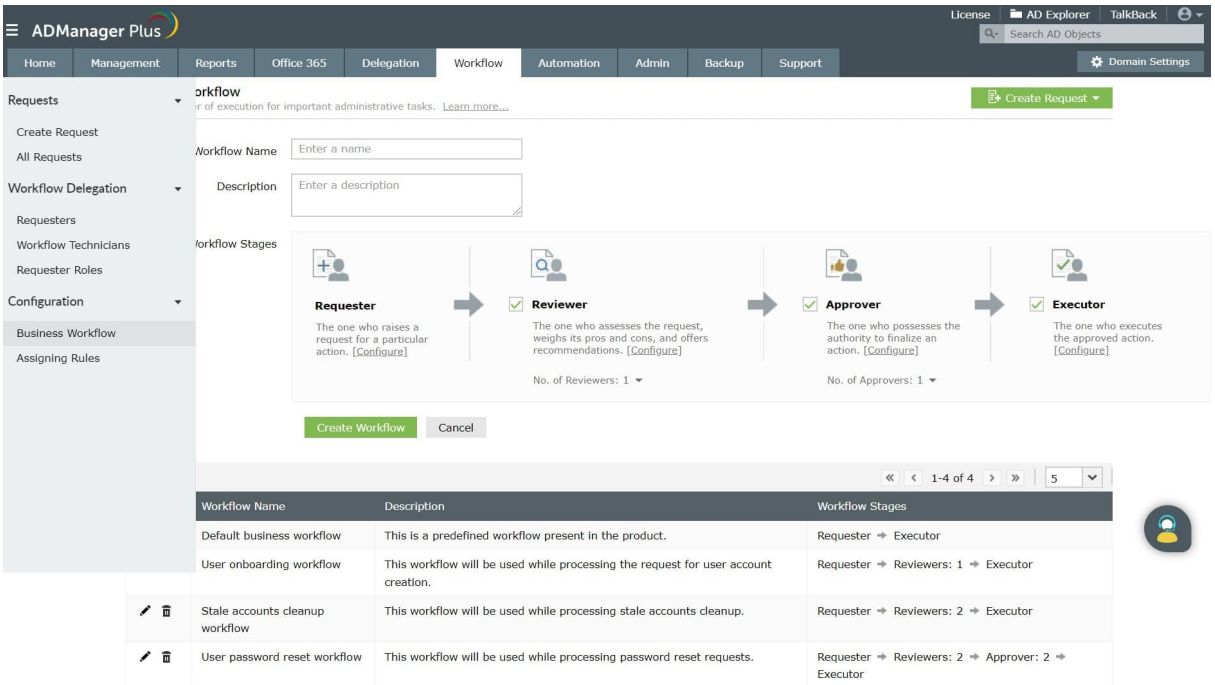
Consider a scenario where an IT technician creates user accounts for new employees, and wants the HR and the administrator to cross-check whether the details and the attribute values are right. In such a scenario, the technician will raise a request, enter all the details of the user, and create a workflow 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. Navigate to **Workflow** → **Configuration** → **Business Workflow**
    b. Select the **Edit** icon for the workflow.
    c. Configure the appropriate user for every workflow stage.



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.

d. Click 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 the **Reports** tab and click the **Inactive Users** report located under the **User Reports** section.
   b. **Generate** the Inactive Users report.
   c. Select the required users and click **Create Request**. Set the *Request Action* field to **Disable Users**.
   d. The HR will see the requests in his requests list and review and approve it. 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 the request and clicking the **Execute** button.

Exercise 2: Workflow based user accounts creation

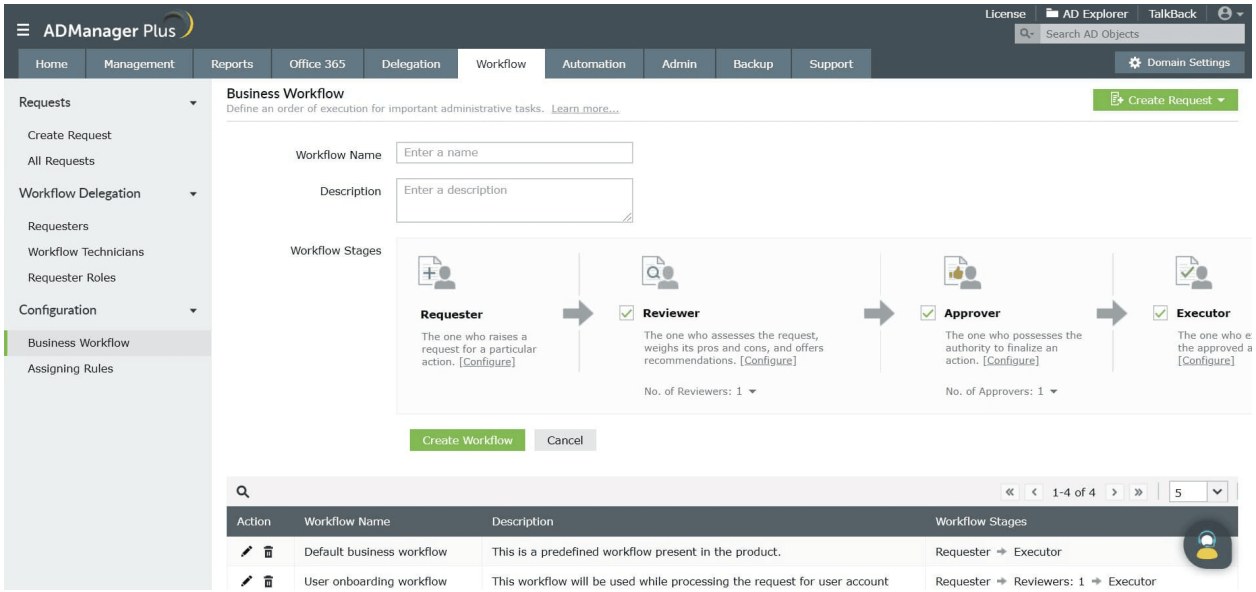
Scenario: Whenever new employees join the organization, the HR executives send the details of all the new employees to their administrator to create new user accounts in the domain of their organization. Instead of this, it would minimize the workload of the administrator if the HR executives can key 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:

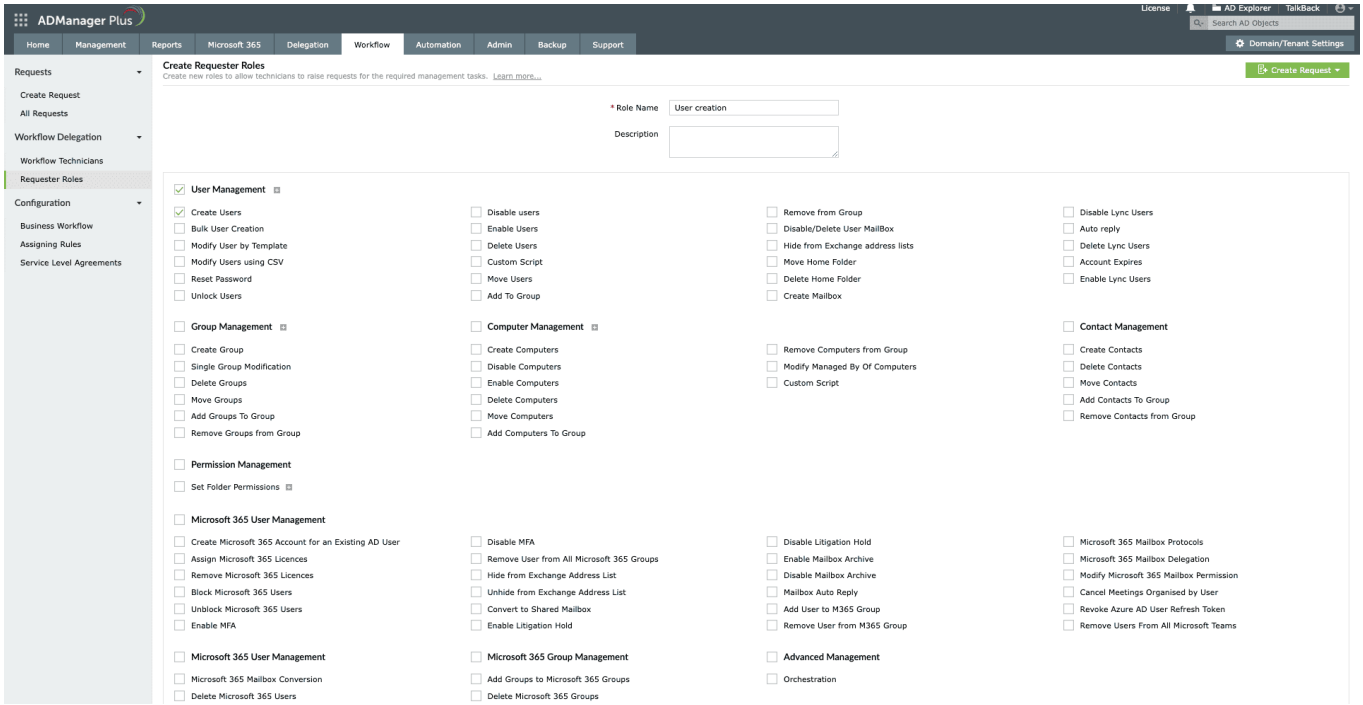
- Creating a workflow as per your organizational requirements.
- Assigning the requester role to HR Executives to enable them to create user creation requests.
- Assigning the executor rights to the appropriate technicians from the IT team to empower them to create new users in AD.

Steps to create users through the workflow:

1. Click the **Workflow** tab.
2. Click the **Business Workflow** in the left pane. Enter a *Name* and a *Description* for the new workflow.
3. Configure 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.**



5. To assign the requester role to HR executives:
   a. Go to the **Workflow** tab and from the left pane, click **Requester Roles**.
   b. Click **Create New Role.** Give the *Role Name* as User Creation and give a description.
   c. Click **Save Role.**



d. To assign the created role to the HR executive, click **Workflow Technician** from the left pane.

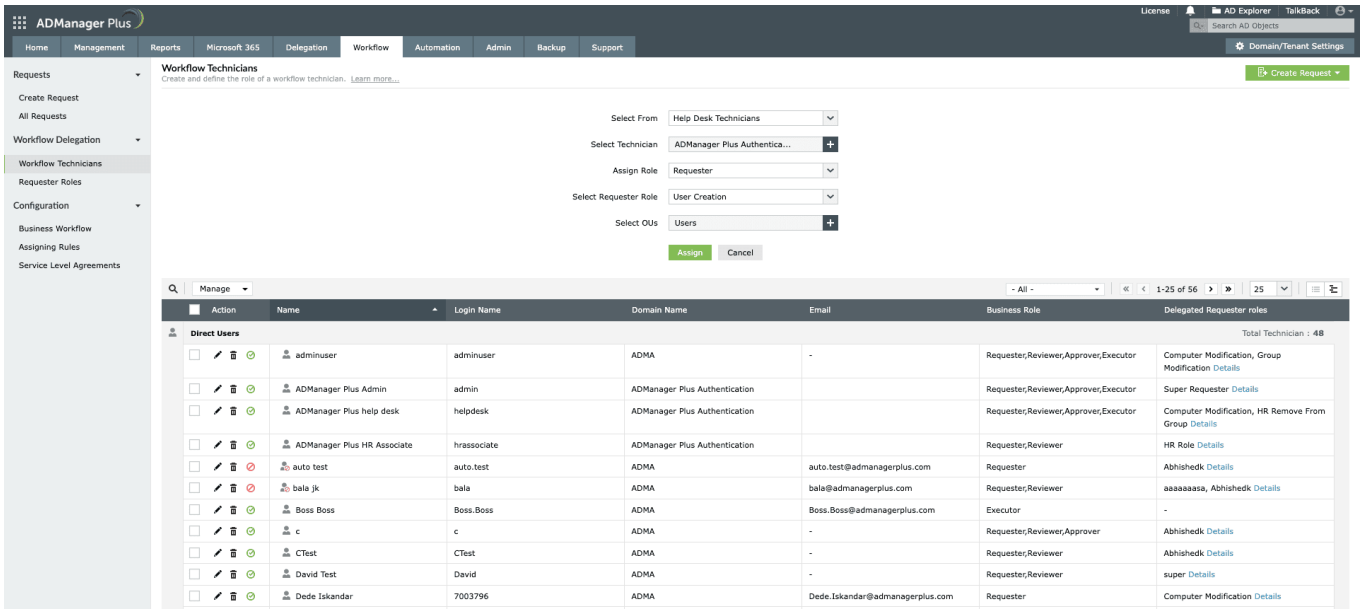
e. Click **Add New Technician** option and in the *Select Technician* field, select the HR executive.

f. In the *Assign Role* field, select **Requester**.

g. In the **Select Requester Role** field, choose **User Creation**.

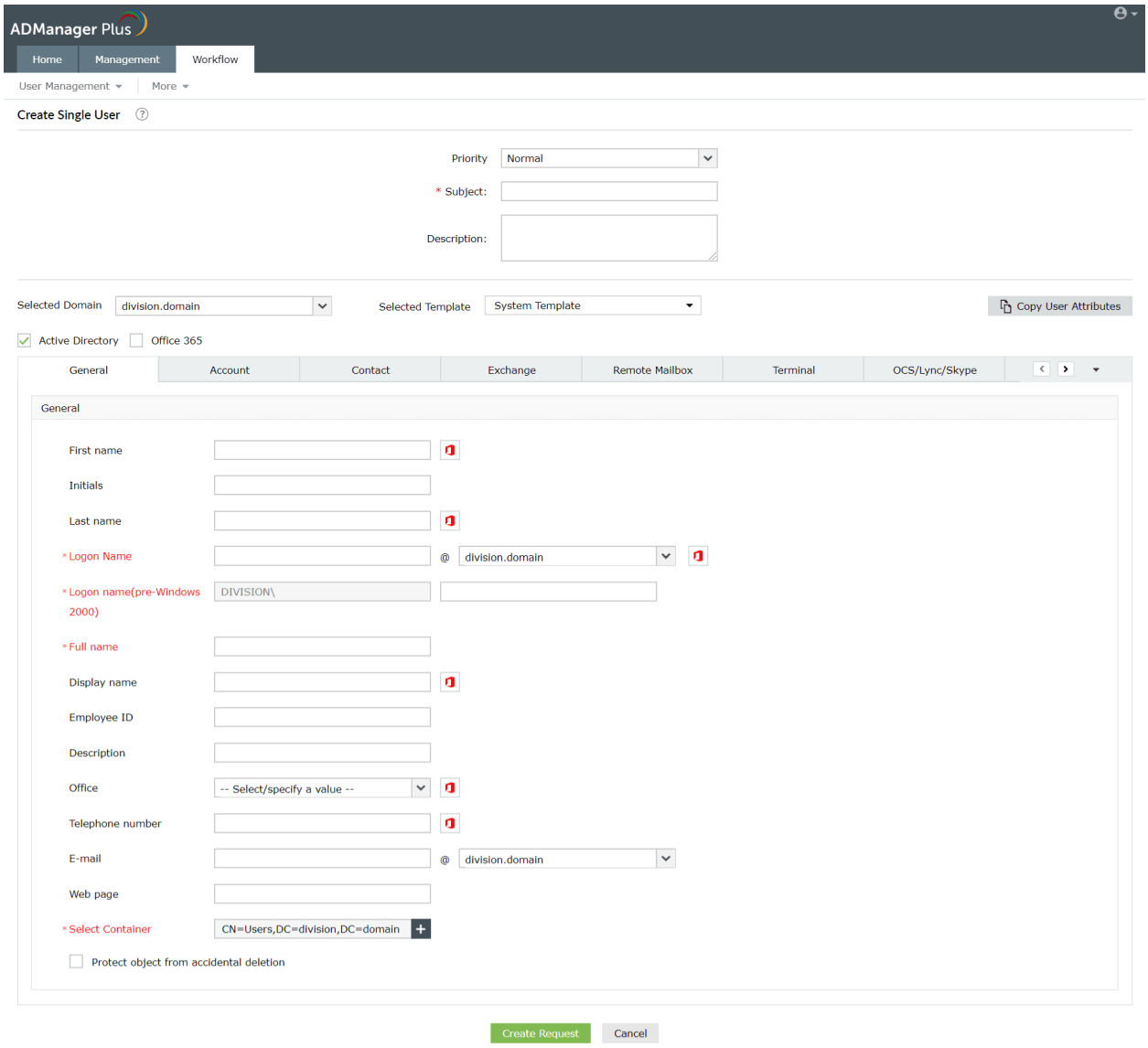
h. Select the OUs in which the HR executive can raise user creation requests using the **Select OUs** option.

i. **Assign** requester.

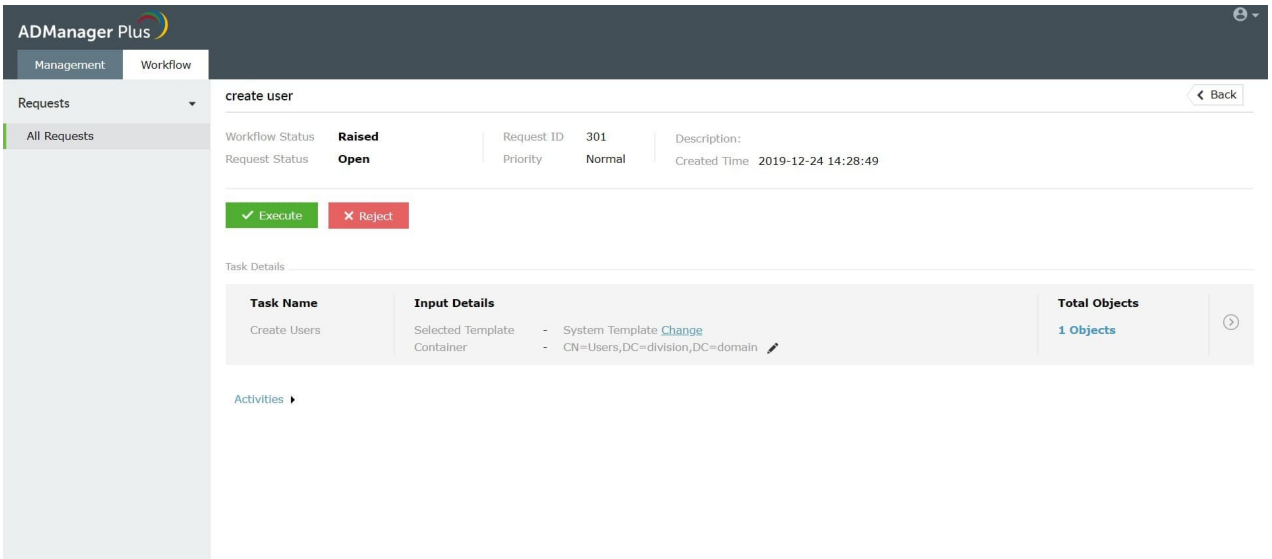


1. To create executors who can create new user accounts in AD:
    a. Go to the **Workflow** tab and click **Workflow Technicians** from the left pane.
    b. Click **Add New Technician** and select the required technicians from the list of all available technicians in the domain and add the executor role to them.
    c. Click **Assign** to add the selected technicians to the 'Executors' list.
2. To raise a request for new user account creation:
    a. Login to ADManager Plus using the credentials of the requester and click the **Workflow** tab.
    b. Click 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 the **Create Request** button to complete the request creation process.

        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.



1. To execute the user creation request:
    a. Login to ADManager Plus using the credentials of the technician with the 'execute' role.
    b. Click the **Workflow** tab and click on **All Requests**.
    c. In the requests list, go to **My Requests** and Click the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also Click 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.



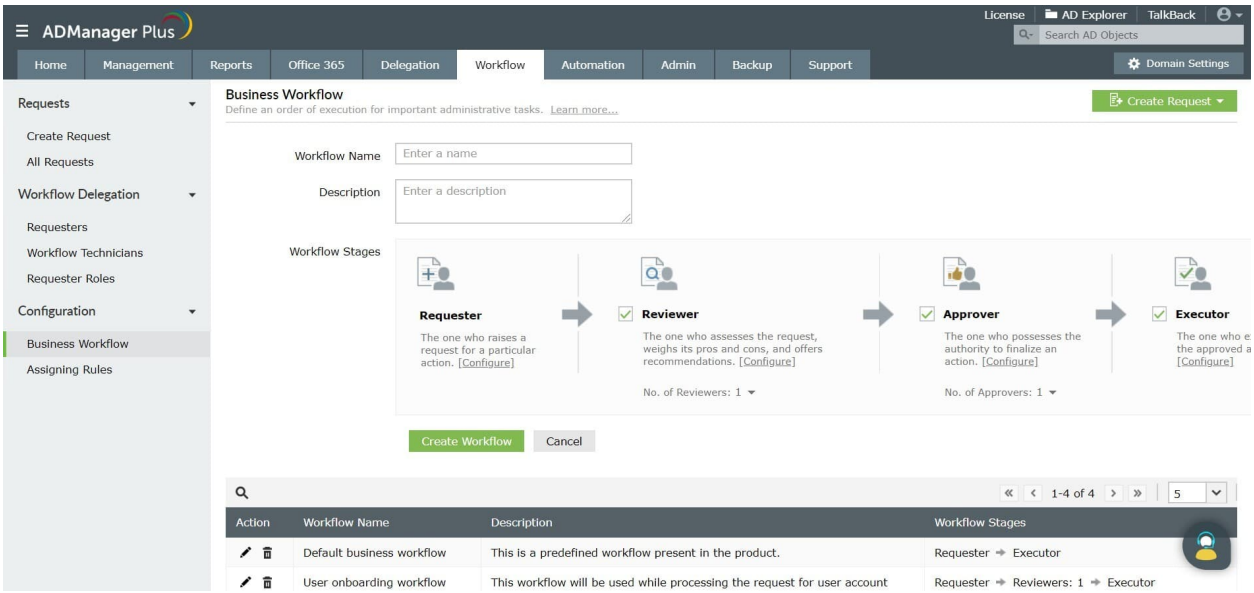
Exercise 3: Workflow based disabling of inactive user accounts

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.

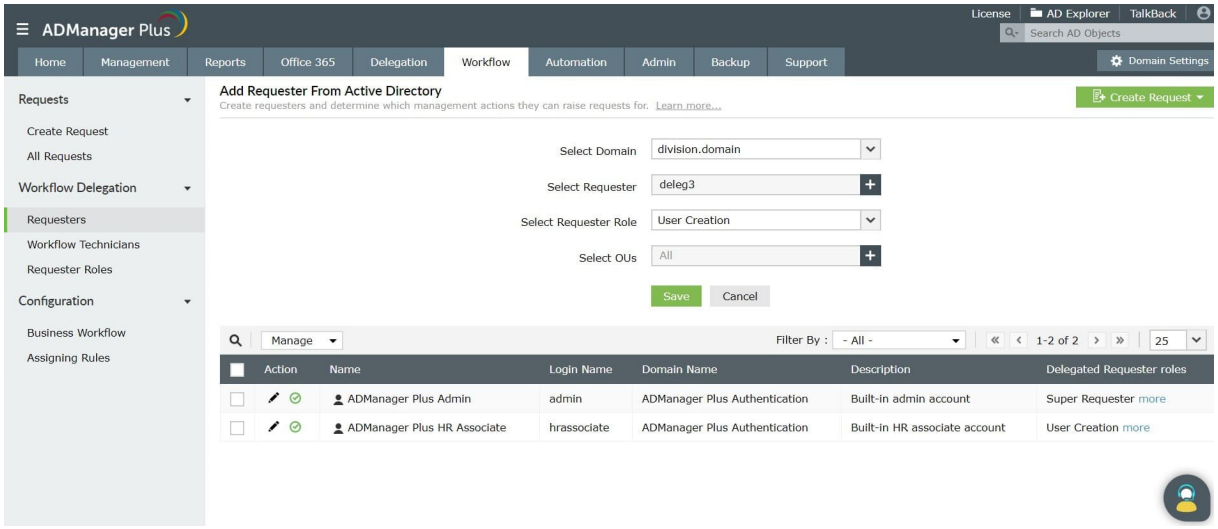
This can be accomplished using the components in the **Workflow** feature by:
- Creating a 3 level workflow with: Requester, Reviewer and Executor.
- Add the appropriate users/technicians to the Requester, Reviewer and Executor roles.
- Once the requester creates the request to disable user accounts, 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:

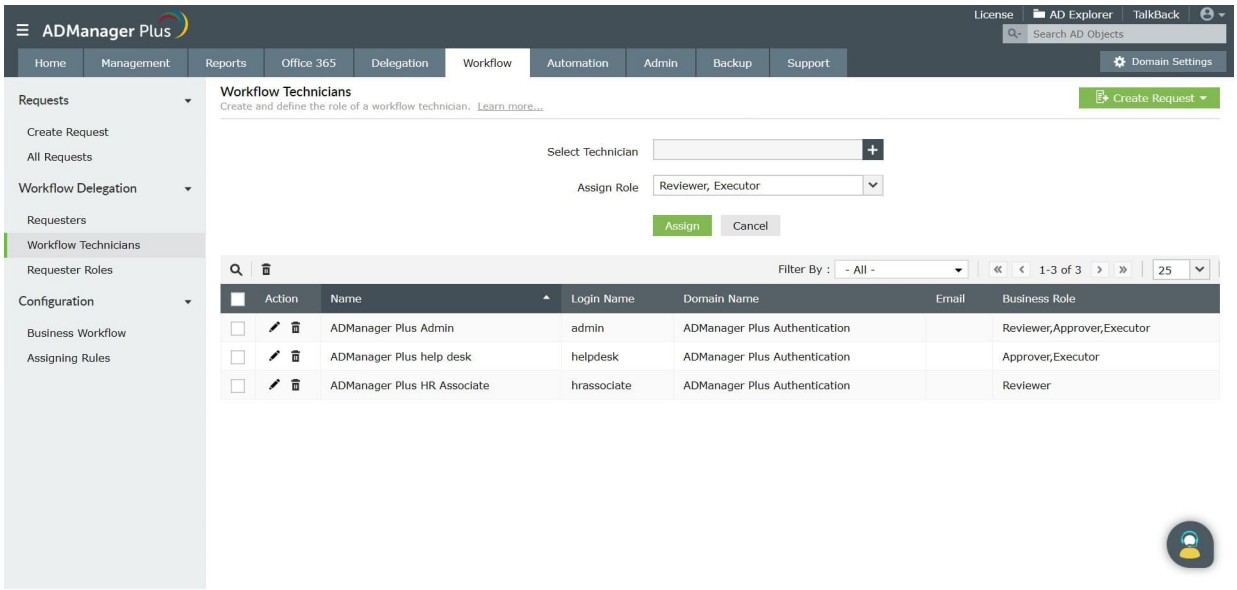
1. To create a customized workflow.
    a. Click the **Workflow** tab.
    b. In the left pane, under the **Configuration** section, click the **Business Workflow** option,
    c. Enter a **Name** and a **Description** for the new workflow.
    d. Configure the the **Workflow Stages** and assign the 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.**.



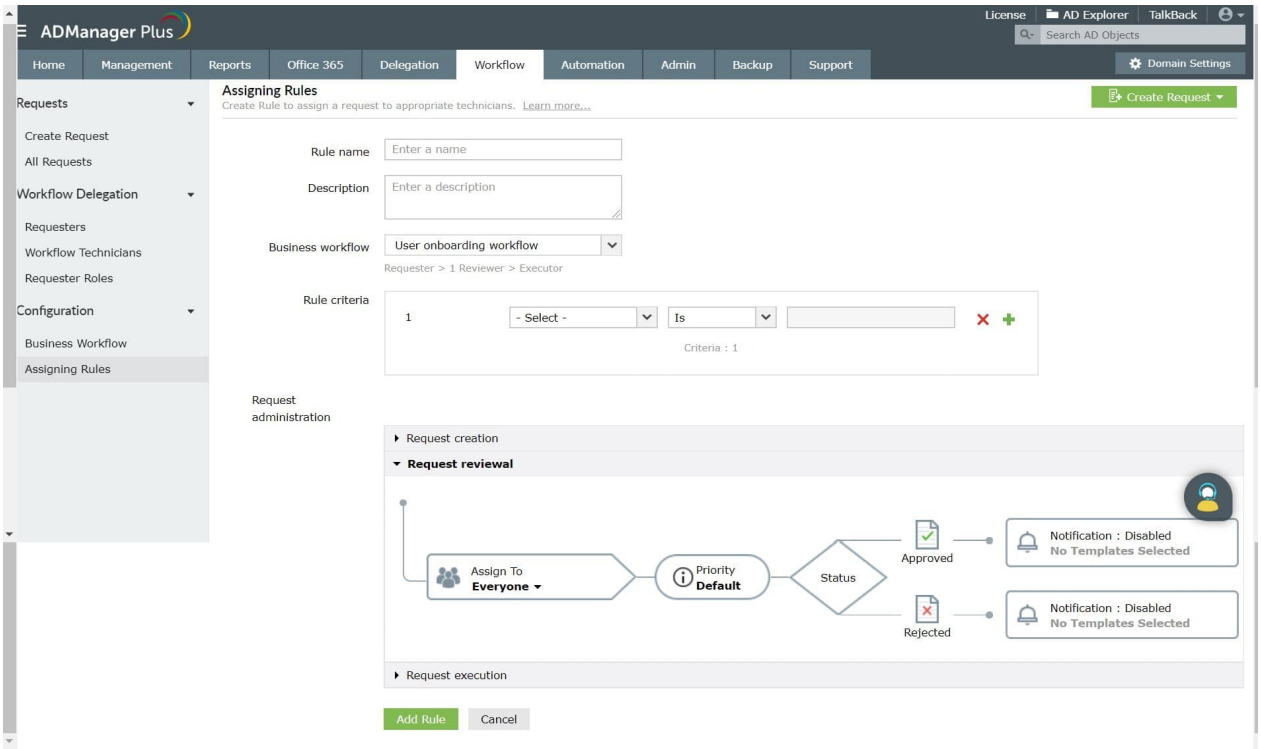
2. To add requesters:
   a. Go to the **Workflow** tab and from the left pane, click **Requester Roles**.
   b. Click **Create New Role.** Give the *Role Name* as User Creation and give a description.
   c. Click **Save Role.**
   d. To assign the created role to the HR executive, click **Workflow Technician** from the left pane.
   e. Click **Add New Technician** option and in the *Select Technician* field, select the HR executive.
   f. In the *Assign Role* field, select **Requester**.
   g. In the **Select Requester Role** field, choose **User Creation**.
   h. Select the OUs in which the HR executive can raise user creation requests using the **Select OUs** option.
   i. **Assign** requester.



3. To create reviewers and executors who can create new user accounts in AD:
    a. Go to **Workflow** → **Workflow Delegation** → **Workflow Technicians**.
    b. Click **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.



4. To create rules that help assign the requests to appropriate users/technicians after creation and review:
    a. Click the **Workflow** tab.
    b. Click **Assigning Rules** and click the **Add New Rule** option.
    c. Specify a name for the rule: **Disable Inactive Users**
    d. Choose the **Business Workflow** you created earlier.
    e. Set the **Rule Criteria** field value to **Action Is Disable Users**.
    f. Under the **Request Review** section,
        i. Click 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.



g. Under the **Request Execution** section,
   i. Click 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 **Add Rule**.

5. To create the disable user request:
   a. Login to ADManager Plus using the credentials of the technician.
   b. Click the **Reports** tab and go to 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 the **Workflow** tab and click **All Requests**.
   c. In the requests list, go to **My Requests.** Click the **Awaiting Review** option to view the list of all requests waiting for review. (You can also click the number displayed in Awaiting Review located just above the list of requests to view all tasks queued up for review).

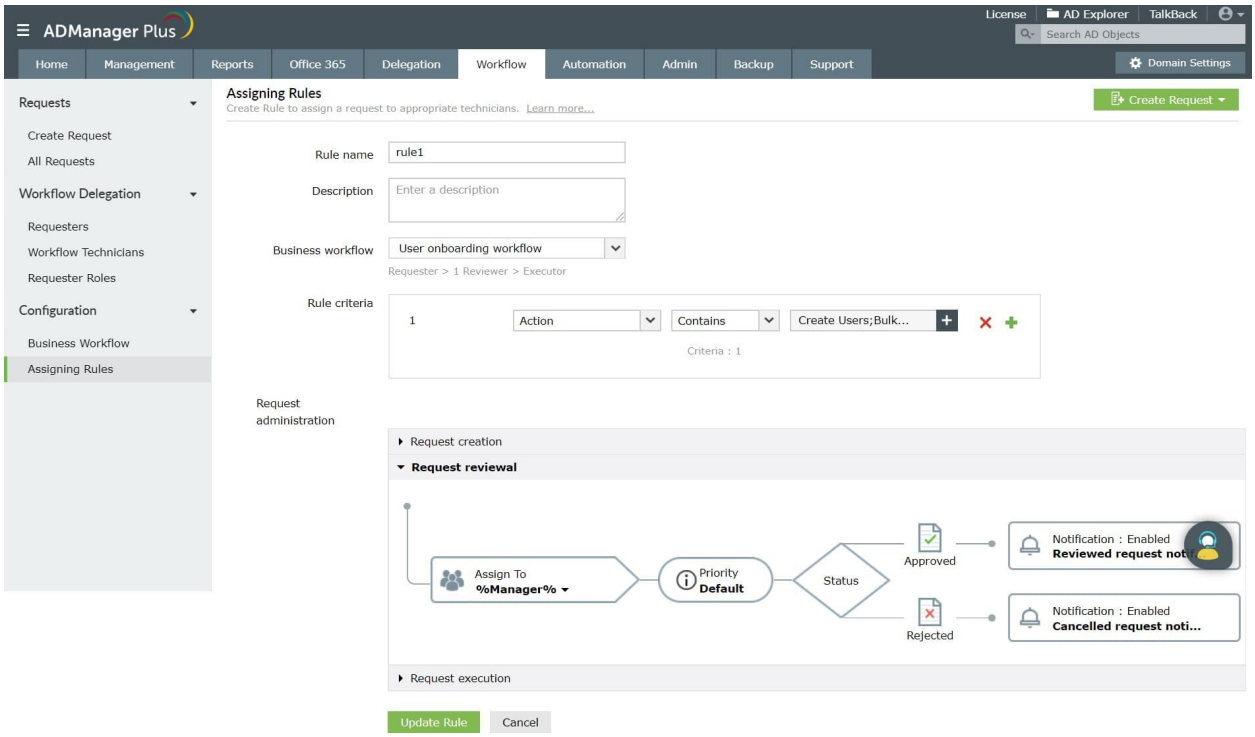
    d. **Review** this task.
7. To execute the disable user request:
    a. Login to ADManager Plus using the credentials of the technician with the 'approver' role.
    b. Click the **Workflow** tab and click on **All Requests**.
    c. In the requests list, go to **My Requests** and Click the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also Click 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 view the details of the object.
    e. **Execute** this task.

Exercise 4: Manager-based workflow

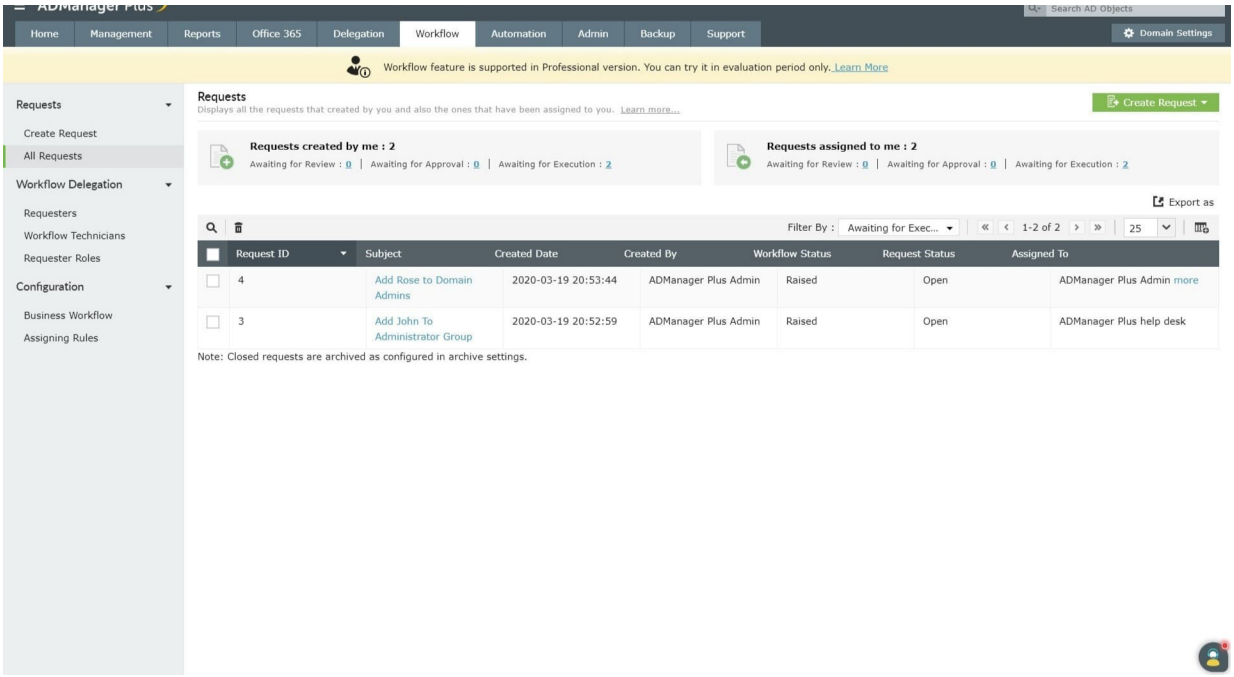
Objective: To add a user to a group only after obtaining the approval from the user's manager.

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 the **Workflow** tab and create a business workflow that has the requester, approver, executor roles.
    a. Click 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 the edit option located next to the **Assigned To** option and Click the **%Manager%** option. Set the priority of the task.
    a. Similarly, assign the task to the required executor.
    e. Click on **Save**.



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.
    b. Click the **Workflow** tab and click on **All Requests**.
    c. In the requests list, go to **My Requests** and Click the **Awaiting for Approval** option to view the list of all requests waiting for execution. (You can also Click the number displayed in 'Awaiting for approval' located just above the list of requests to view all tasks queued up for review).
    d. Select the add to group task and view the details of the object.
    e. **Approve** this task.



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 the **Workflow** tab and click **All Requests**.
    c. In the requests list, go to **My Requests** and Click the **Awaiting for Execution** option to view the list of all requests waiting for execution. (You can also Click 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 view the details of the object.
    e. **Execute** this task.

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.

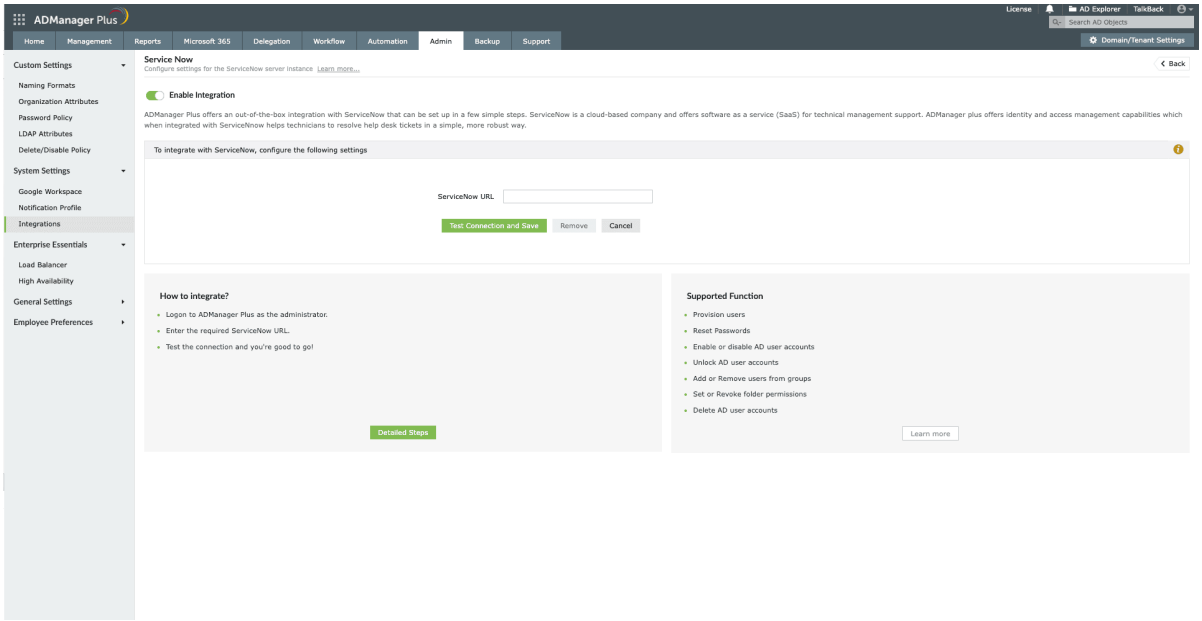
The exercises below focus on the most commonly performed Active Directory management tasks and how integrating ADManager Plus with other applications helps you get them all done from one place.

Exercise 1: Create an Active Directory user account from ServiceNow

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

Solution:

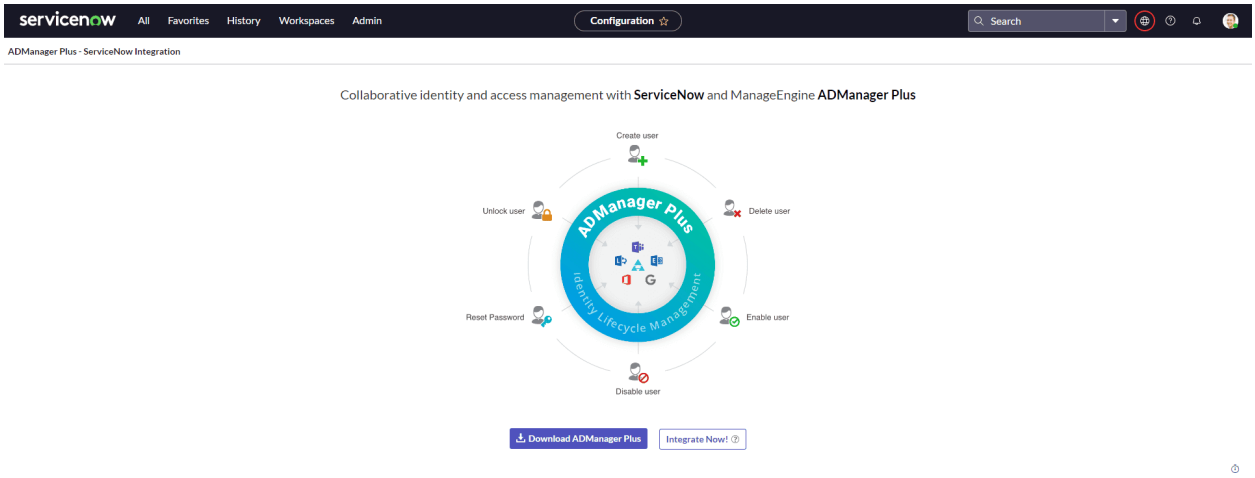
1. Steps to configure ServiceNow in ADManager Plus
    a. Navigate to the **Admin** tab.
    b. On the left pane of the window, under **System Settings**, choose **Integrations**.
    c. Under applications, click **ServiceNow**.
    d. Click **Enable Integration.**
    e. Enter the ServiceNow web service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



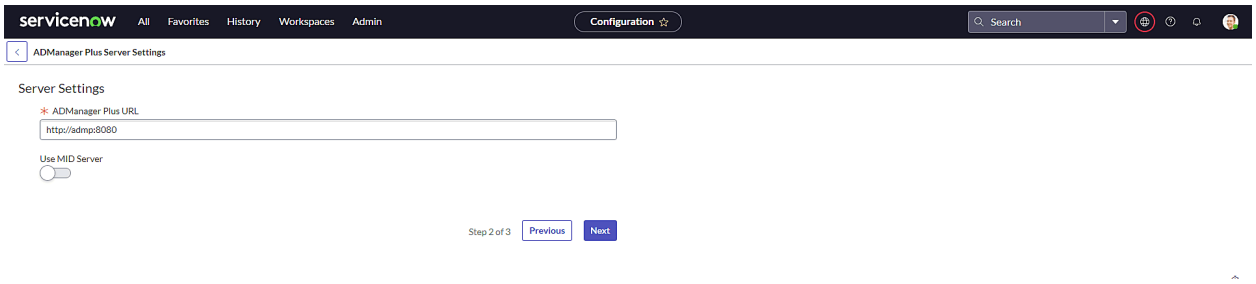
2. Steps to configure the ADManager Plus integration in ServiceNow

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

a. Download and install the **ADManager Plus plug-in** from the ServiceNow store.
b. In the *Navigation bar*, click **All** and expand **ADManager Plus**.
c. Click **Configuration**.
d. In the page that opens, click the **Integrate Now!** button.



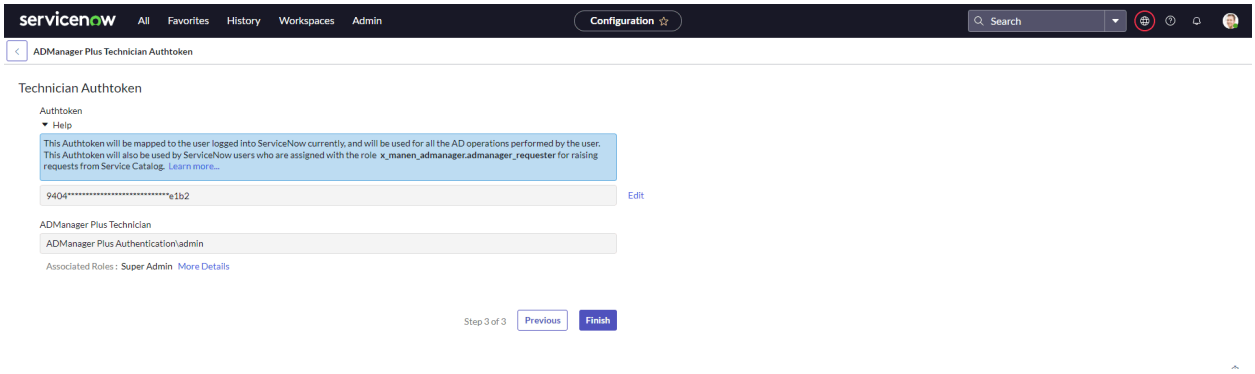
e. Fill in the following fields:
f. **ADManager Plus URL**: Enter ADManager Plus' URL.
g. **Use MID Server**: Enable this option if you'd like to use a MID server to communicate with ADManager Plus. Choose the desired MID server from the list of available servers.



h. Click **Next**.
i. Enter the **ServiceNow technician's authtoken** in the *Authtoken* field, and click **Validate** to fetch the associated technician from ADManager Plus.

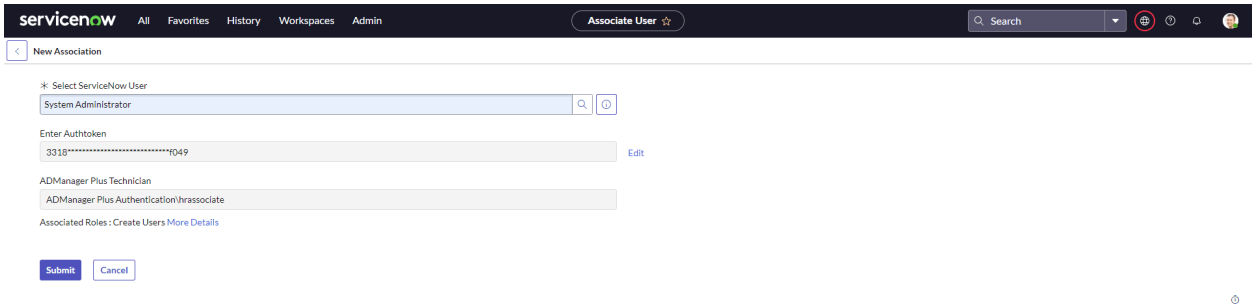
Note: The technician's authtoken can be obtained by navigating to **Delegation > Configuration > Technician Authtokens** in ADManager Plus. Technicians' authtokens are available only in the default admin account for security reasons.

j. Once the technician's details are auto-populated in the *ADManager Plus Technician* field, click **Finish**.



k. You can associate more ServiceNow technicians by selecting the **Associate Users** option under ADManager Plus. Select the ServiceNow user from the drop-down list, specify the technician's authtoken in the *Enter Authtoken* field, and click **Submit**.

Note: Authtokens can be easily edited in the future by clicking the **Edit** icon next to the Enter *Authtoken* field.



3. Steps to create users from ServiceNow

If you're an admin and would like to perform a user management action in ServiceNow:

a. Click **All** and expand **ADManager Plus**.
b. Select the desired **user management action or file management action** from the list of actions, and fill in the required fields.
c. Click **Submit**.

You can also raise a request to perform these actions from ServiceNow's Service Catalog after adding Active Directory Management as a category.

a. Click **All** and search for **Service Catalog**.
b. Select **Service Catalog** and click the **+ icon** located in the top-right corner.
c. Select **Active Directory Management** and click **Add here**.
d. Select the desired user management action and fill in the required fields.
e. Click **Submit**.

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 server settings
   a. Click the **Automation** tab.
   b. In the left pane, under *Configuration,* select **Application Integrations**.
   c. Under *Database*, click **Microsoft SQL Server** and select **Click to Configure**.
   d. In the *Microsoft SQL Server Details* section, configure the following:
      - **Server Name**: Enter the server name.
      - **Instance Name**: Enter the instance name and port number.
      - **Authentication**: Select any of the following authentication types:
        - **SQL Authentication**: Enter the Username and Password.
        - **Windows Authentication**: Enter the **Domain Name, Username,** and **Password**.
        - **Azure Active Directory - Password**: Enter the **Username** and **Password** of the Azure AD user account.

Note: The user account credentials used for authentication should at least have the *db_datareader* role in SQL Server.

   e. Click **Test Connection and Save** to establish the connection and save the settings.

Note:

- Click the **Add Server** option to configure multiple MS SQL servers.
- The **Enable Integration** button is turned on by default. Toggle it off to disable MS SQL integration.

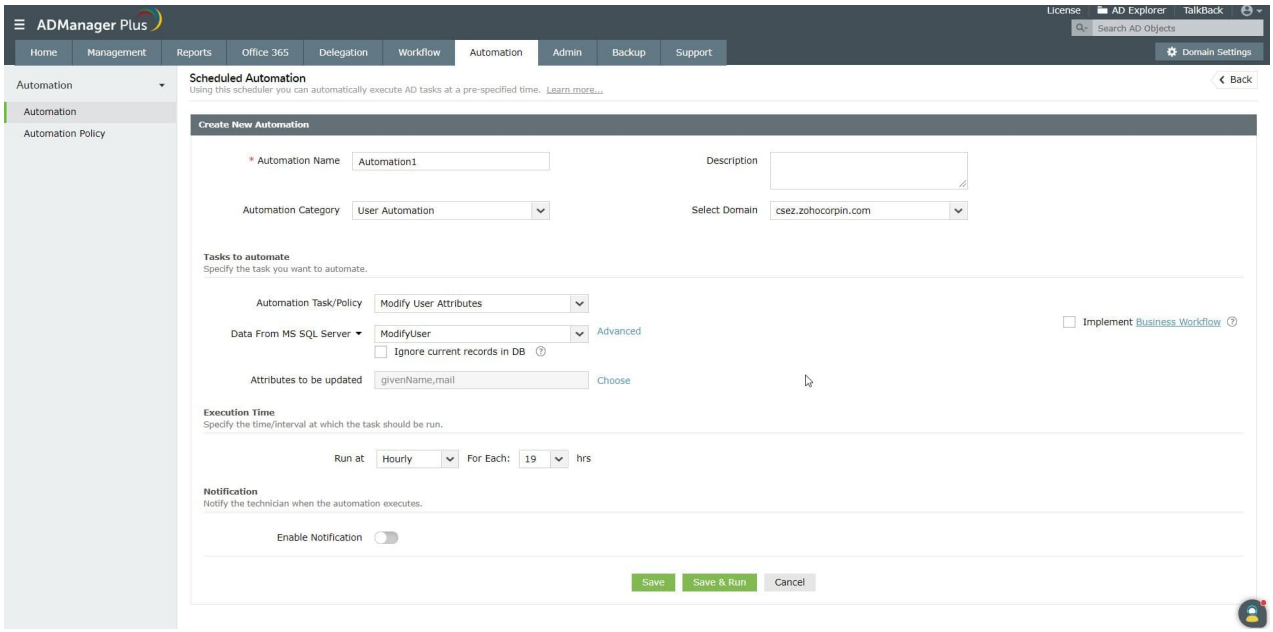
2. Steps to add a new configuration
   a. Click **Add New configuration** and enter a suitable name.
   b. In the **Description** field enter the details about the new configuration.
   c. Configure the following details:
      - **Select Server**: Select the server name from the drop-down menu.
      - **Select Database**: Enter the database name.
      - **Table Name**: Enter the name of the table in the MS SQL database.
      - **Automation Category**: Select the automation type from the drop-down menu.
   d. Fetch the input for user creation from the MS SQL table by mapping **DB Column Name** to the **LDAP Attribute Name**.
   e. Click **Save** to save the new configuration.

3. Steps to automate user modification
   a. Click on **Automation** tab.
   b. Select **Automation** from the left pane.
   c. Click on **Create New Automation** and configure the following:
      - **Automation Name:** Enter a name for the automation.
      - **Description:** Add a brief note about the automation.
      - **Automation Category:** Choose **User Automation** from the menu.
      - **Select Domain:** Select the domain/OUs where the automation should run. Child OUs can be

eliminated by selecting **Exclude Child OU(s)** option.

- **Automation Task/Policy:** Select **Modify User by Template** from the menu.
- **Select Template:** Select the template to be applied for user creation.
- **Select Objects:** Click **Select More.** Beside the *Location of CSV* option, select **MS SQL Server** from the menu. Enable **'Ignore current records in DB'** to ignore the already processed records and consider only the unprocessed records in the MS SQL table for user creation.
- **Select Config:** Select a configuration from the menu. Or click on Add New Configuration to add new configuration settings.
- **Implement Business Workflow:** Select this option if the automation has to be executed through a workflow.
- **Execution Time:** Configure the automation execution time.

d. Click **Save** to save the settings or **Save & Run** to save the settings and run the automation instantly.

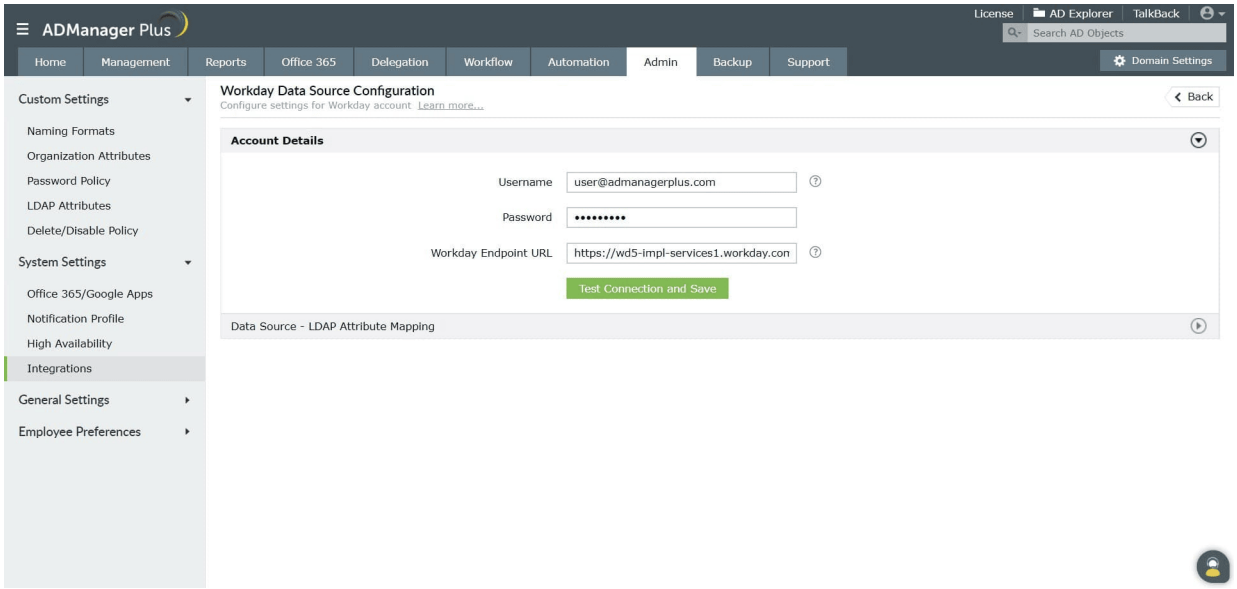


Exercise 3 : Automate user creation from the Workday HRMS application, integrated with ADManager Plus

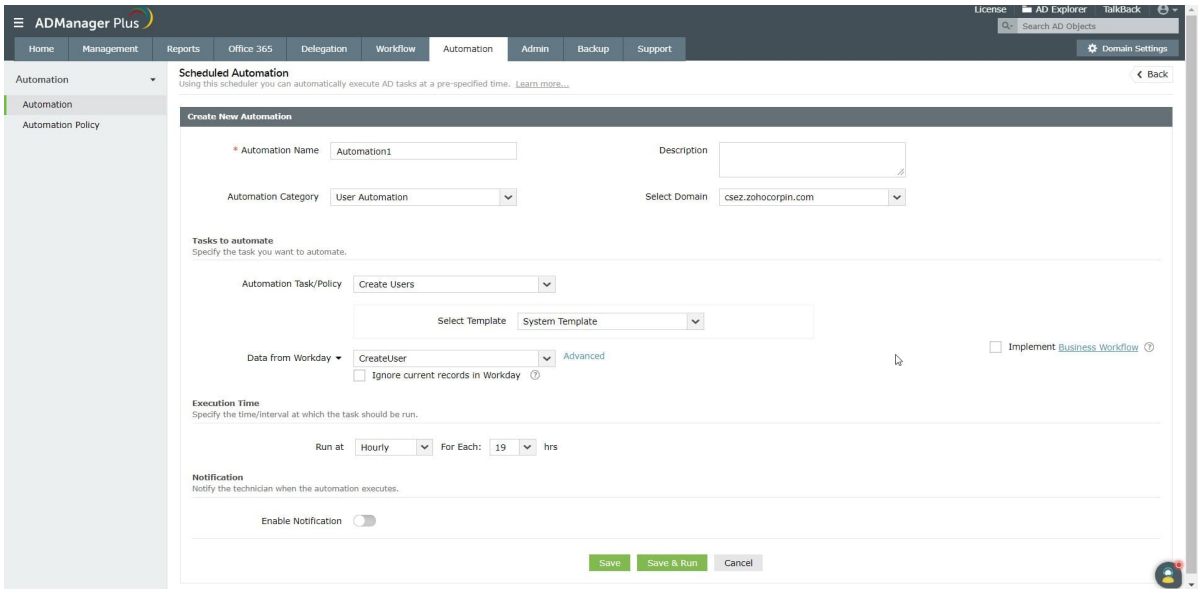
Objective: Integrate ADManager Plus with Workday and automate user creation.

Solution:

1. Steps to configure Workday in ADManager Plus
   a. Navigate to the **Automation tab → Configuration → Application Integrations.**
   b. Click **Workday** located under *Enterprise applications*.
   c. The **Click to configure button** will guide you to the configuration page.
   d. Enter the Workday admin account's **Username, Password**, and **Endpoint URL**.
   e. Click **Test Connection and Save** button to save your configuration settings.
   f. Under **Data Source - LDAP attribute and mapping**, you can map multiple AD LDAP attributes to its corresponding fields in the Workday. For example, you can set "sn" is equal to "Last_Name".
   g. Click **Add** to save the settings.



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**.



Exercise 4: Integrate Boomi using application integration

Scenario: Integrate Boomi application with ADManager Plus

Solution:
ADManager Plus offers flexible endpoint configuration options to suit your organizational goals and needs. Two types of webhooks—inbound and outbound webhooks—determine how data can be synchronized between Boomi and ADManager Plus. This integration can be achieved by performing the following steps:

a. **Authorization configuration**
Configure the authorization method to authorize API requests.

b. **Inbound webhook configuration**
Configure endpoints to fetch user data from Boomi.

c. **Outbound webhook configuration**
Configure an API to sync data between ADManager Plus and Boomi or to perform a task in Boomi.

Pre-requisites

Please ensure to provide an API key with permissions to retrieve desired information and perform tasks in Boomi. Refer to Boomi's API references for more details.

Authorization configuration

1. Log in to ADManager Plus and navigate to the **Automation** tab.
2. In the left pane, under *Configuration*, click **Application Integrations**.
3. Under *Enterprise Applications*, click **Boomi**.
4. Toggle the **Enable Boomi Integration** button on.mas
5. In the *Boomi Configuration* page, click **Authorization**.
6. Boomi uses **API Key** to authorize API requests. Perform the **steps to generate the API key in Boomi**, copy the key value for **x-api-key**, and paste it in the **Value** field.
7. Select **Header** from the **Add To** drop-down list.

8. Click **Configure**.

Inbound webhook configuration

Inbound webhook enables you to fetch users' data from Boomi to ADManager Plus. The pre-configured API allows you to import all the user from Boomi. However, if you would like to selectively import users, you can either modify the pre-configured endpoint, configure a new endpoint as per Boomi's API references, or use Advanced Filters in automation. The attribute mapping configured in this section can be selected as the data source while setting up an automation configuration. To configure an inbound webhook for Boomi:

1. Under *Inbound Webhook*, click **Boomi Endpoint Configuration**.
2. In the **Endpoint Configuration** tab, an endpoint (*Boomi USERS ENDPOINT)* comes pre-configured with an **Endpoint URL**, **API Method**, **Headers**, and **Parameters** fields to fetch user accounts from Boomi. If you would like to use this pre-configured endpoint, replace *{Domain-Name}* with the domain name of your Boomi instance in the **Endpoint URL** field. However, if you would like to use a new endpoint to import users, you can configure one using the **+ Add API endpoint** button and filling in the required fields as per Boomi's API references. Click here to learn how to configure a new endpoint.

Note:
   - The API key value pair is pre-configured as a header for authenticating API requests as configured during **Authorization Configuration**.
   - You can add macros to your endpoint URL to dynamically change it as per your requirement while fetching object-related data from the endpoint.
   - Refer to Boomi's API references and configure additional headers and parameters, if required.
3. Once done, click **Test & Save**. A response window will display all the requested parameters that can be fetched using the API call. Click **Proceed**.

Note:
   - Refer to Boomi's API references to know which **Parameters** must be configured to fetch only specific parameters.
   - You can configure multiple endpoints for Boomi.
4. Click **Data Source - LDAP Attribute Mapping** to match endpoints and to map AD LDAP attributes with the respective attributes in Boomi.

5. Click **+ Add New Configuration** and perform the following:

i. Enter the **Configuration Name** and **Description** and select the **Automation Category** from the drop-down menu.

ii. In the **Select Endpoint** field, select the desired endpoint and a **Primary Key** that is unique to a user (e.g. employeeIdenifier).

Note: When multiple endpoints are configured, this attribute will be used to locate the identity across them and map their data.

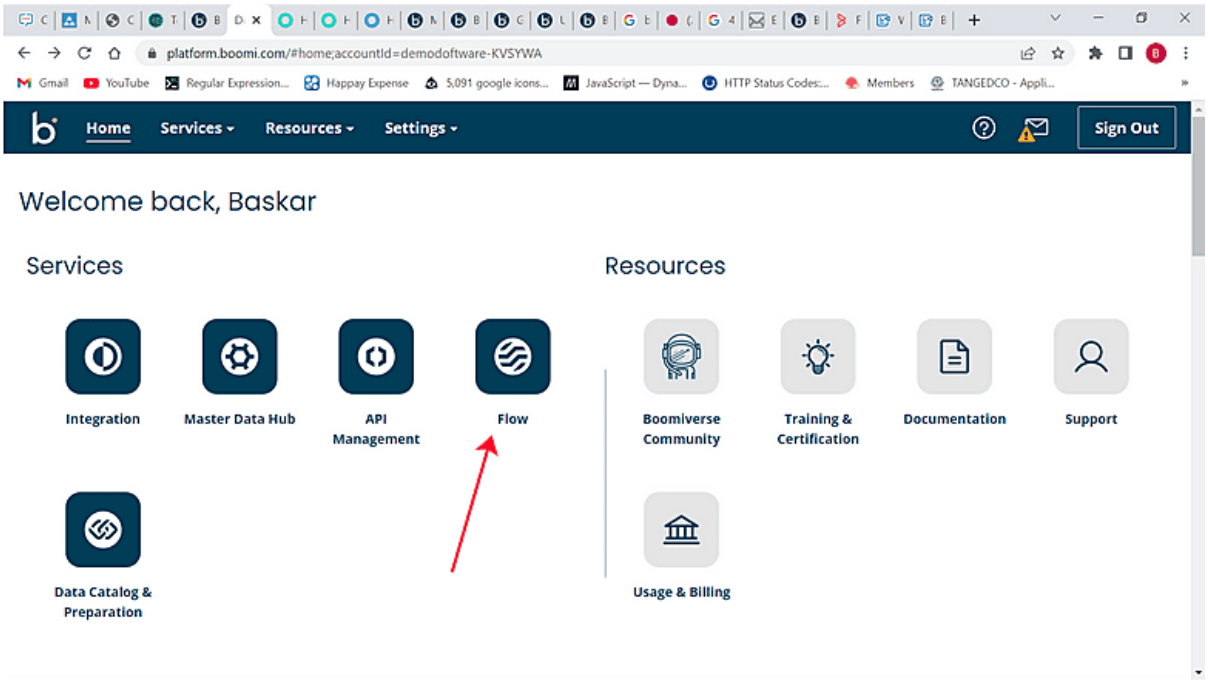
iii. In the **Attribute Mapping** field, select the attribute from the **LDAP Attribute Name** drop-down menu and map it with the respective column in Boomi.

Note: Click **Format Mapping Attributes** if you would like to create a new attribute format for the mapped attributes.

6. Click **Save**.

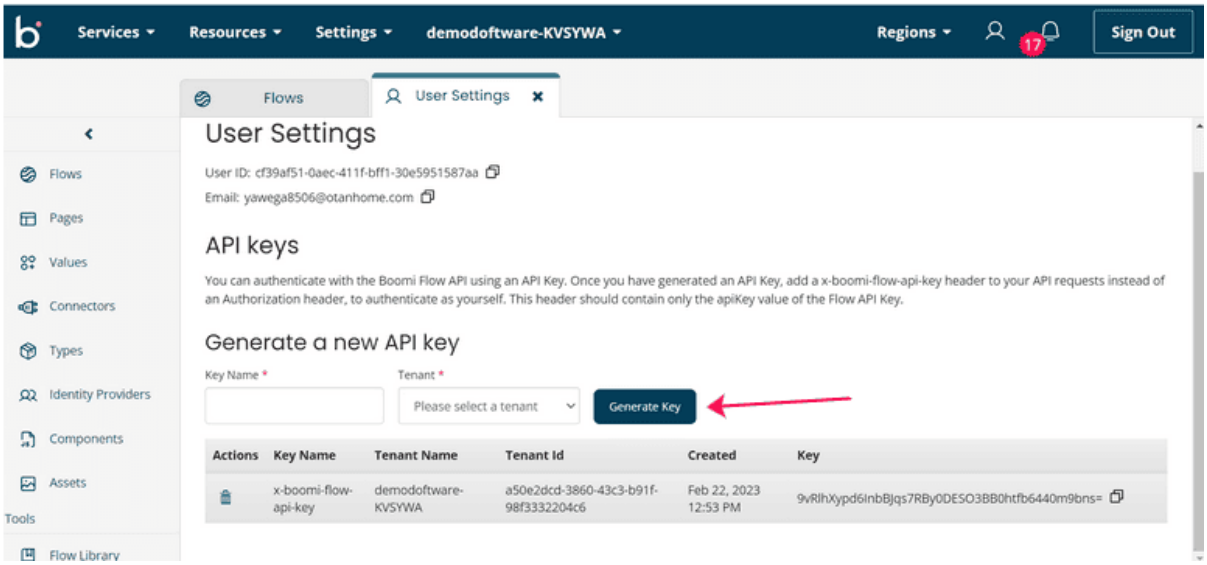
Steps to generate the API key in Boomi

1. From the home page of Boomi, navigate to **Flow**.

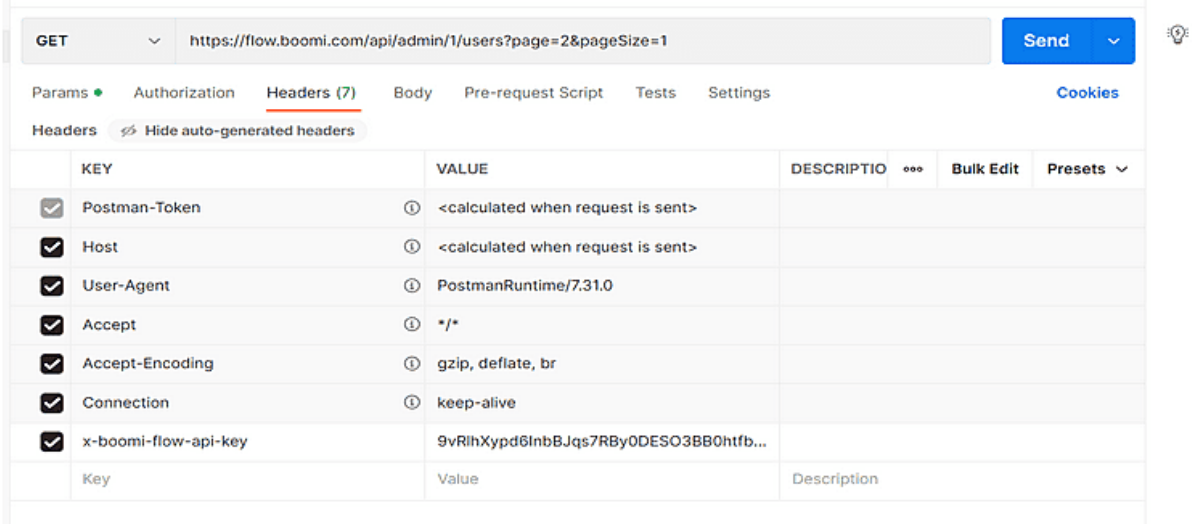


2. Click the user icon in the top-right corner.

3. Go to **User Settings** and click **Generate Key**.



4. Add *x-boomi-flow-api-key* as the header to your API requests (e.g., *x-boomi-flow-api-key : <API-key>*).



Note: The base API URL is *https://flow.boomi.com*.

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, Microsoft 365, Google Workspace, and other enterprise applications. ADManager Plus supports hybrid AD management and reporting, risk assessment, identity life cycle management, workflow orchestration, and integration with various enterprise applications to manage, govern, and secure enterprise identities.

If you need any more assistance with the product or use-cases, contact support@admanagerplus.com.