ManageEngine
ADManager Plus

Workbook

Table of Contents

1. Introduction:

ADManager Plus workbook is aimed to help you practice all the tasks and features that you got to know during the ADManager Plus training session.

The exercises are created keeping in mind the most important, most common and most needed tasks that are performed by any Active Directory Administrator.

As you progress through this workbook, you will realize how the easy, simple UIs of ADManager Plus help you to manage, monitor and report on your Active Directory and Exchange environment so much more easily and effectively compared to the native Active Directory interface.

2. Active Directory Management

The use-cases/exercises in this section will help you in getting familiar with the features will that will make the task of managing your Active Directory easy and simple, with just your mouse.

This section will deal with

- Creation
- Management
- Deletion of Active Directory Objects.

You will also learn how simple it is to create, manage and delete Active Directory objects, not just one object at a time but in bulk as well - through the simple, easy to understand, easy to navigate UI of ADManager Plus - and also to specify multiple conditions in a single step or from a single screen.

2.1 Active Directory Objects Provisioning

In this section you will learn how to create Active Directory Objects, in bulk and also perform additional tasks like adding them to Groups, specifying any desired value like Department, at the time of creation itself.

Exercise 1: User Provisioning

Objective: One-Stop User Provisioning with the following criteria:

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

In the native AD environment, this will involve multiple steps:

- creating the user

- edit the properties of the user to add them to a specific group and then specify a department

- hide the email address in the Exchange Address List, in yet another separate step.

To do this task for multiple users, it will be nothing short of a typing marathon and you will only end up with sore eyes, fingers and a totally exhausted mind and body.

Or you can depend on scripts, writing which is again a headache and a much bigger ache it will be to keep modifying it as the Active Directory grows and changes happen. Add to this the fact that you never know when a script could stop functioning or worse still, start malfunctioning, presenting to you problems that you could well have avoided.

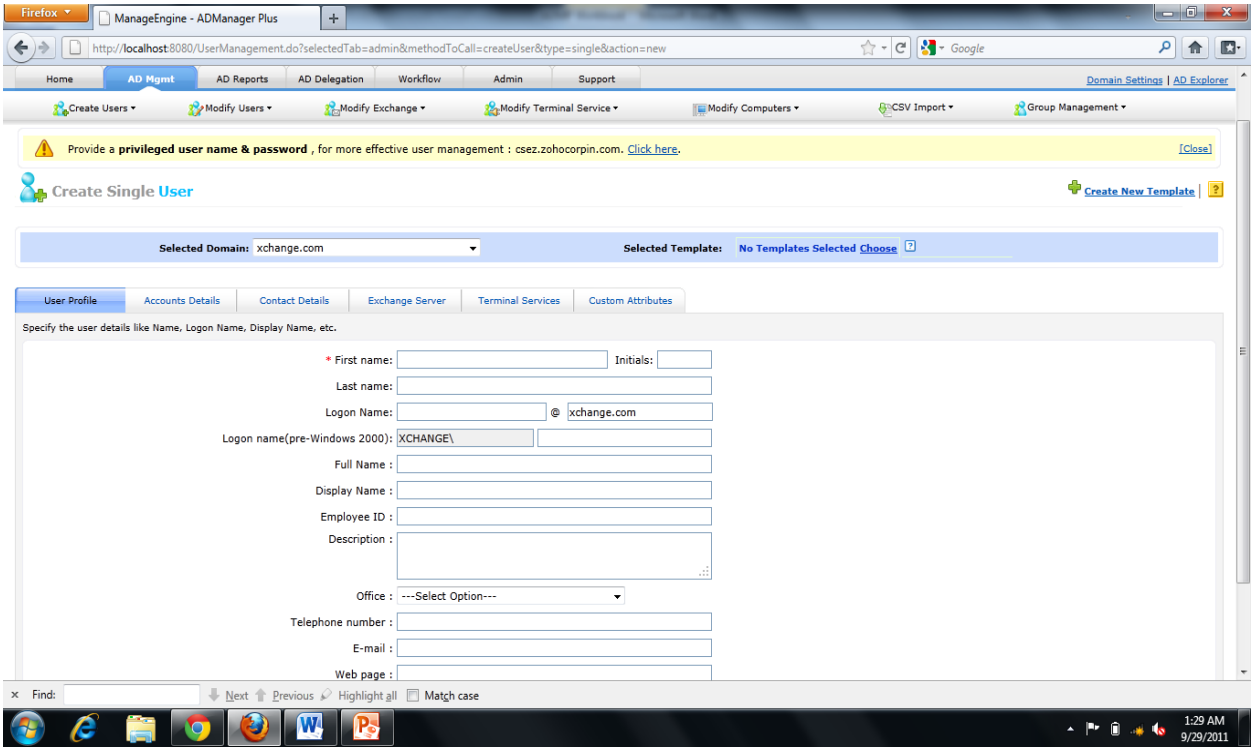
In ADManager Plus, a user can be created will all the above mentioned criteria, from a single screen in just a single step using a single template with just point and click operations. Yes, it is really as simple as that!!

Below are the steps for one-stop user provisioning.

Steps to accomplish the above objective:

1. Click on ‘AD Mgmt’ tab
2. Click on ‘User Management’ and then ‘Create Single User’ option.

You will now see the User Creation Page.



3. Select the domain to which this User has to be added in ‘Selected Domain’ and also specify the template that you would like to user in the ‘Selected Template’ option.
4. By default you will see the ‘User Profile’ tab – enter all the required information under the User Profile Tab.

To make this User a ‘member of’ a specific group:

5. Click on ‘Account Details’ Tab.
6. The ‘Member of’ option can be seen Under the Group / Profile section and by default the User will be a member of the Primary Group which is ‘Domain Users’ for the User objects.
7. Click on the ‘Edit’ option placed next to the ‘Member Of’ field to add the group to which this user has to be added.
8. In the new ‘Edit Groups’ window, select the require group from the groups listed under the ‘Available Groups’ option and click on ‘>>’ button to select the group.

To specify a ‘Department’ for the user:

9. Click on the ‘Contact Details’ Tab.
10. Select the required department from the options in ‘Department’ field under the ‘Organization’ section.
    To add a new department, click on the ‘Do you want to add more departments?’ link below the Department field. This will take you to the ‘Titles and Departments’ page where you can click on the ‘Add New’ option in the Departments section to add a new department.

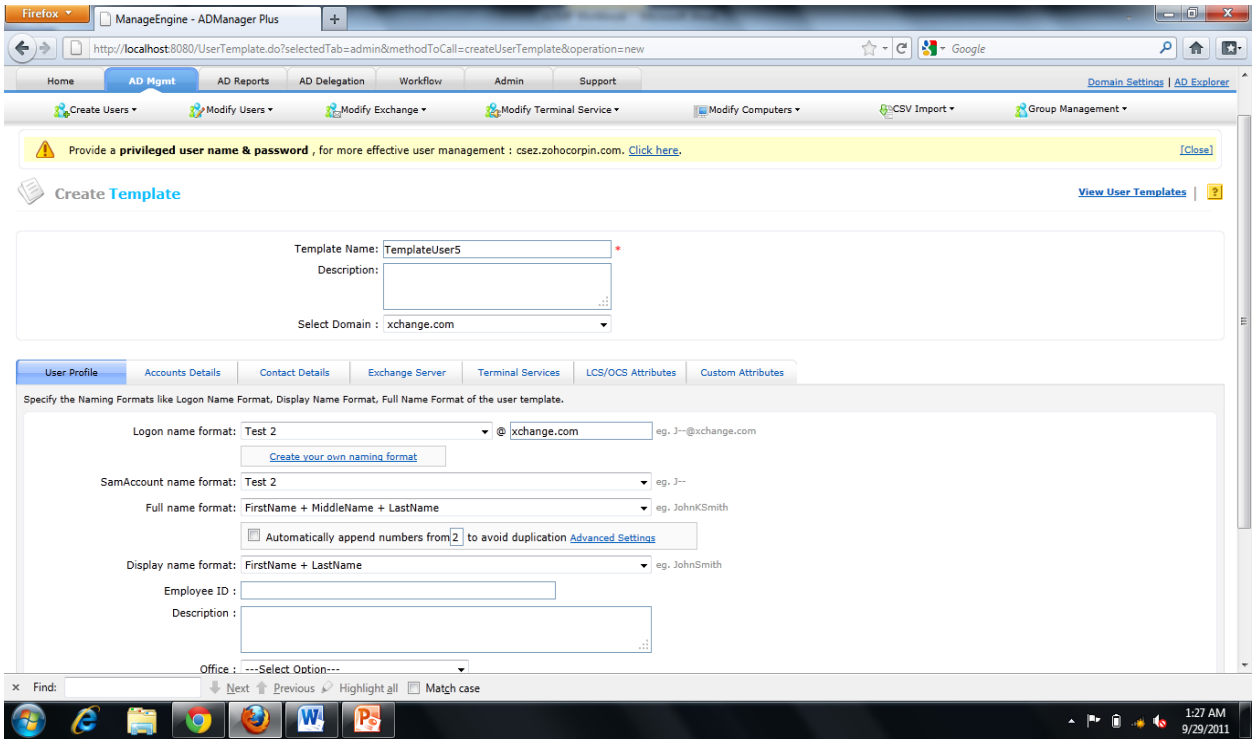
To not list the email address of this user in the Exchange Address List:

11. Click on ‘Exchange Server’ Tab.
12. Select the ‘Mailbox Enabled User’ option.
13. Select the ‘Hide from Exchange Address Lists’ option under the Exchange General section to hide the email address of this user from the Exchange Address List.

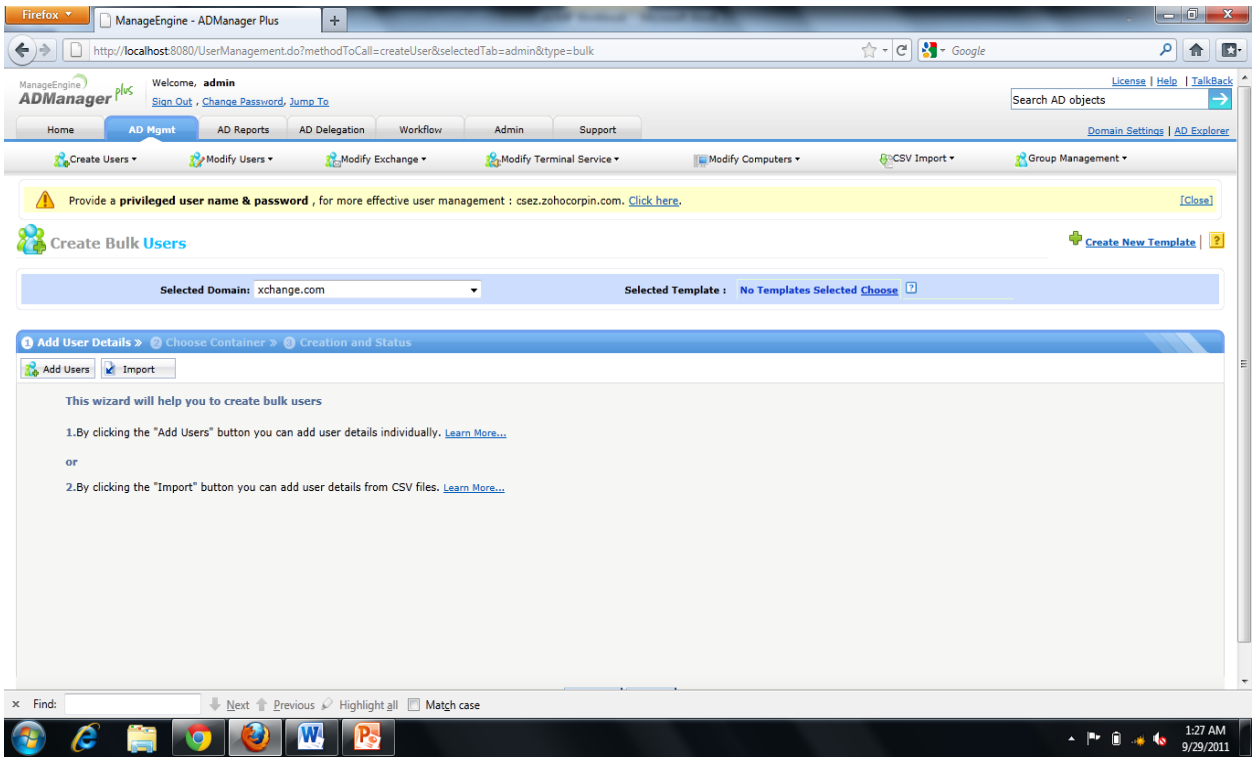
For ‘Bulk User Creation’ with the same set of conditions, you can create a new template which will help you in specifying the conditions.

To create a new ‘user creation template’:

14. Click ‘AD Mgmt’ → ‘Create User Template’ → enter a name for this template and also select the domain for which this template will work.
15. Specify the groups to which the users have to be added in the ‘Group Profile’ section in ‘Account Details’ tab.
16. Specify the ‘Department’ in the ‘Organization’ section in the ‘Contact Details’ tab.
17. Select the ‘Hide from Exchange Address Lists’ option in ‘Exchange General’ section in ‘Exchange Server’ tab. Save the template.



Creating Bulk Users:



18. Go to ‘AD Mgmt’ → ‘User Management’ → ‘Create Bulk Users’
19. Select the ‘Domain’ to add the users to.
20. Select the template that we created using the above steps.
21. Click on ‘Import’ → to import the list of users from a CSV file. → Click ‘Next’
22. Select a container in which the users have to be created → Click ‘Create Users’.

Exercise 2: Regulated User Creation and User Modification:

Objective: To track administrative activities leading to Active Directory malfunction.

When technicians are granted rights in AD they login to Domain Controllers and there is a fair possibility of creating a malfunction in the Active Directory environment.

While operating on ADManager Plus, the technicians are not provided absolute access to the Active Directory. Instead they can be granted access to the concerned OUs and can perform tasks like ‘user creation and user modification’ so that their actions can be controlled and any possible damage to the Active Directory can be prevented.

Additionally, it becomes easier to track the changes performed by technicians using Audit Reports in the AD Delegation section.

Exercise 3: Group Provisioning

Objective: Create a new Group. Add members of two specific groups to this new Group.

Trying to do this using the native interface is nothing short of trying to jump from a cliff, expecting to land on your feet unscathed and unscratched.

Using the native AD interface, you will have to first create the group.

To add members to this group, you will have to

- select the group
- edit its properties
- select the add option under Members tab
- search for the group(s)
- add them as members

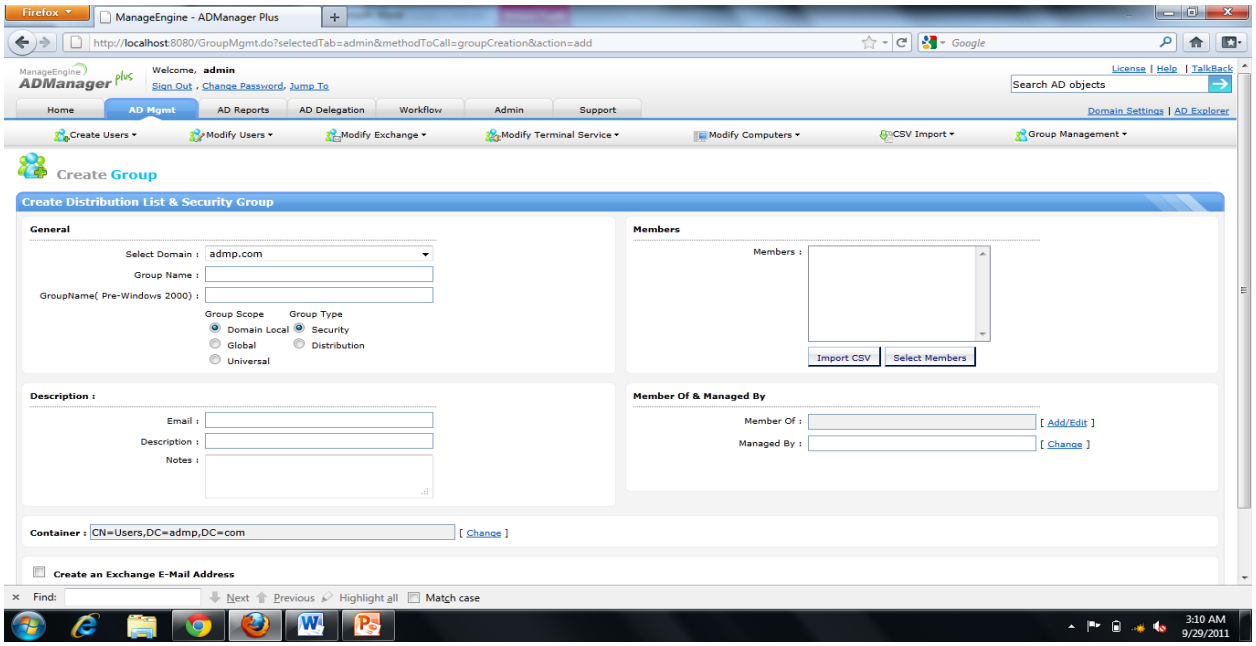
All these steps are for just one user, to add multiple users the effort and patience required can make one really frustrated and exhausted.

In ADManager Plus, all these operations can be done from a single screen and in one single step in just clicks. And do not forget the huge savings in time, effort and confusion. ADManager Plus makes turns this tedious task to not just a simple task but a ridiculously simple task!!

Steps:

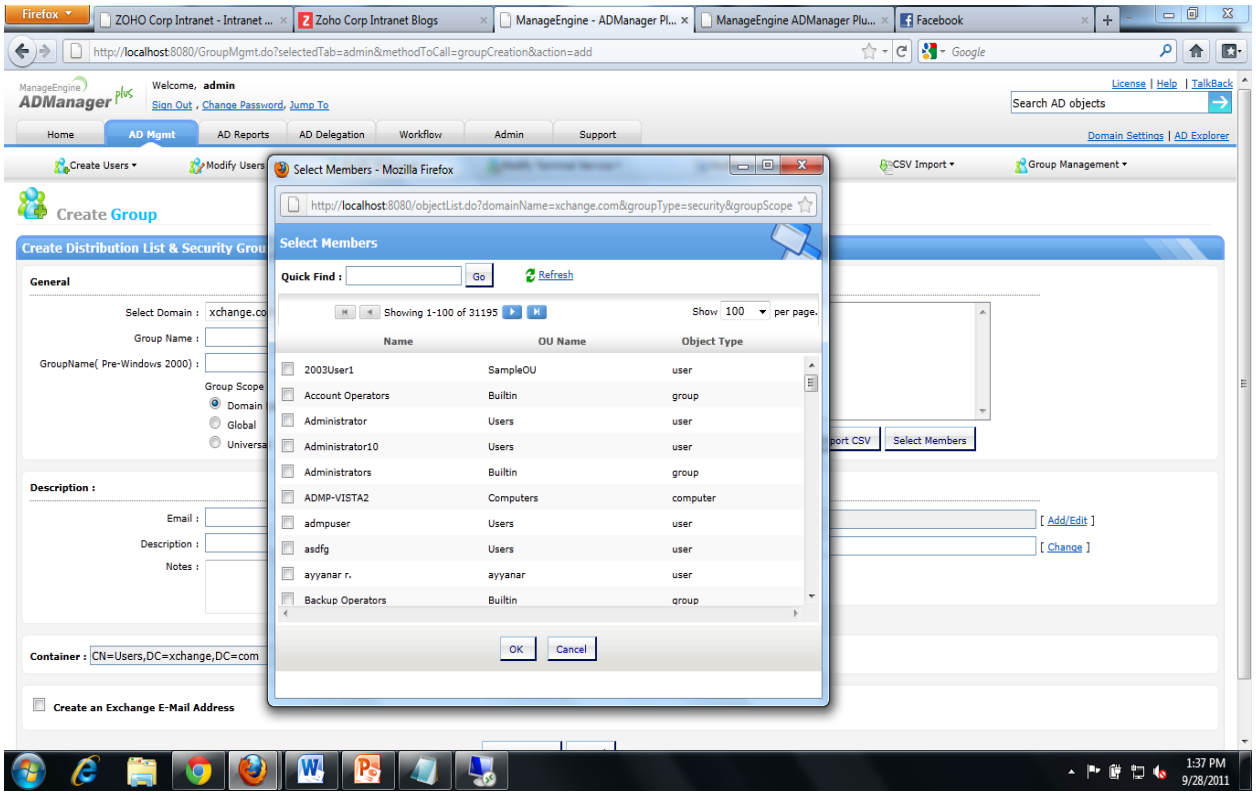
1. Click on ‘AD Mgmt’ Tab.
2. Click on ‘Group Management’ and then ‘Create Single Group’.

You will now see the ‘Create Group’ page.



3. Specify the domain in which this group is to be created in the ‘Select Domain’ option.
4. Specify the name for this group in the ‘Group Name’, ‘Pre-Windows’ Group Name fields.
5. Select the Group Scope and Type.
6. Under ‘Members’ section, click on ‘Select Members’ button.

This will open up a new window with the list of all available users, groups and computers in the entire domain.



7. Select the required group(s) whose members you would like to add to this new group. Click 'OK' to add all the members from these groups to the new group.

   You will find all the groups that you selected displayed under the 'Members' field which indicates that all the members from the selected groups have been added to the new group.

Exercise 3: Computer Provisioning.

Objective: Computer pre-staging and also adding the computer objects as member of the specified group.

In the native AD environment,

- First a computer has to be created.
- The computer has to be located.
- Then its properties have to be edited to add this computer to a group.

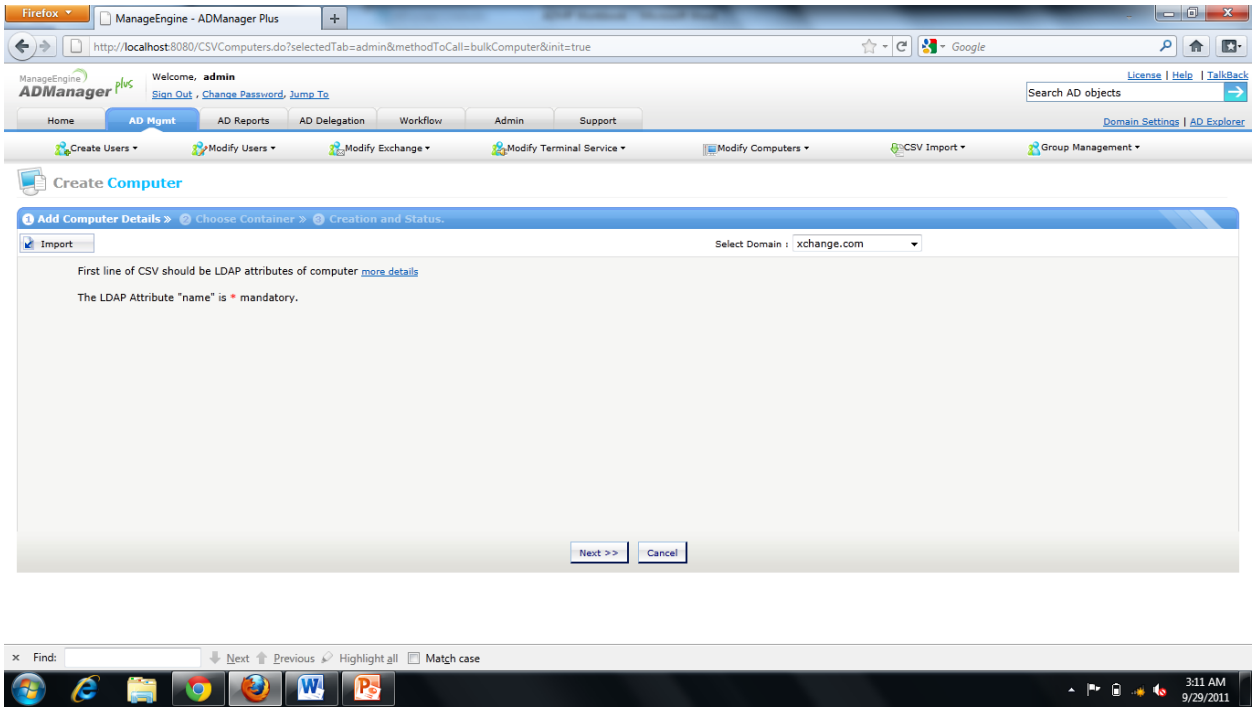
Also, there is no bulk create option available in the native AD environment, which means

- Each computer has to be created one by one.
- Then the properties of each computer have to be edited to add each computer to the required group.

In ADManager Plus, it is possible to create computer accounts in bulk using the 'Create Computer' option by importing the CSV file with all the required attributes of the computer accounts. To add these computers to any specific group while creating them, all you have to do is just specify the required group under the 'memberOf' attribute in the CSV file. And, voila! You have created computer accounts, in bulk, and have also made each computer, a member of a group.

Steps:

1. Click on 'AD Mgmt' Tab.
2. Click on 'Computer Management' and 'Create Computers'



3. Click on ‘Import’ and select the required CSV file with all the required attributes, including the ‘memberOf’ attribute for the computer accounts to be created.
4. Specify the domain in which these computer accounts have to be created in the ‘Select Domain’ field.
5. Click ‘Next’ after adding the CSV file and specifying the domain.
6. Select from the list, the‘Container’ in which these computer accounts have to be created.

If you wish to create a new OU to place all the computer objects that will be created, click on ‘create new OU’.

7. Click on ‘Create Computers’ to create the computer objects.

Below is a sample CSV file which has the memberOf attribute mentioned:

name,description,memberOf,location

computer1,James computer,"CN=GeorgexSimonJones,OU=NTest,DC=admp,DC=com";
"CN=admptestgroup,OU=NTest,DC=admp,DC=com",NewYork X98

The first line is the header with the LDAP names of the attributes to be added.

Exercise 4: Office 365 Users License Modification

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

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

Steps:

1. We can generate reports in AD Reports →Office 365 Reports → Licensed users.

2. Based on the report we can modify the license assigned to these users.

3. Go to AD Management → Office 365 Management → Assign / Remove Licenses

4. Click on Assign / Remove License → Import a .csv file or search for the user.

5. Apply the changes.

3. Common Active Directory Management Tasks

The use-cases 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, accomplishing these routine and common tasks usually require multiple steps. And to do these activities in bulk, it will nothing short of a herculean effort and even after such effort, you still run the risk of encountering errors, for after all the human elements of tiredness, lapse in concentration can absolutely make sure you redo these tasks again.

To avoid such difficulties, administrators usually are forced to take the more 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 the active directory.

With ADManager Plus, most of the Active Directory management tasks become really simple to perform and can also be accomplished from just a single screen or in just one step and as you would have found out by this time, just with clicks, most of the time.

Exercise 1: Decommissioning file server

Objective: Move all users' Home folder and profiles to another file server.

In native Active Directory environment,

- the home folders and profiles can be changed only for one user at a time
- properties of the users have to be edited

For multiple users the only options are

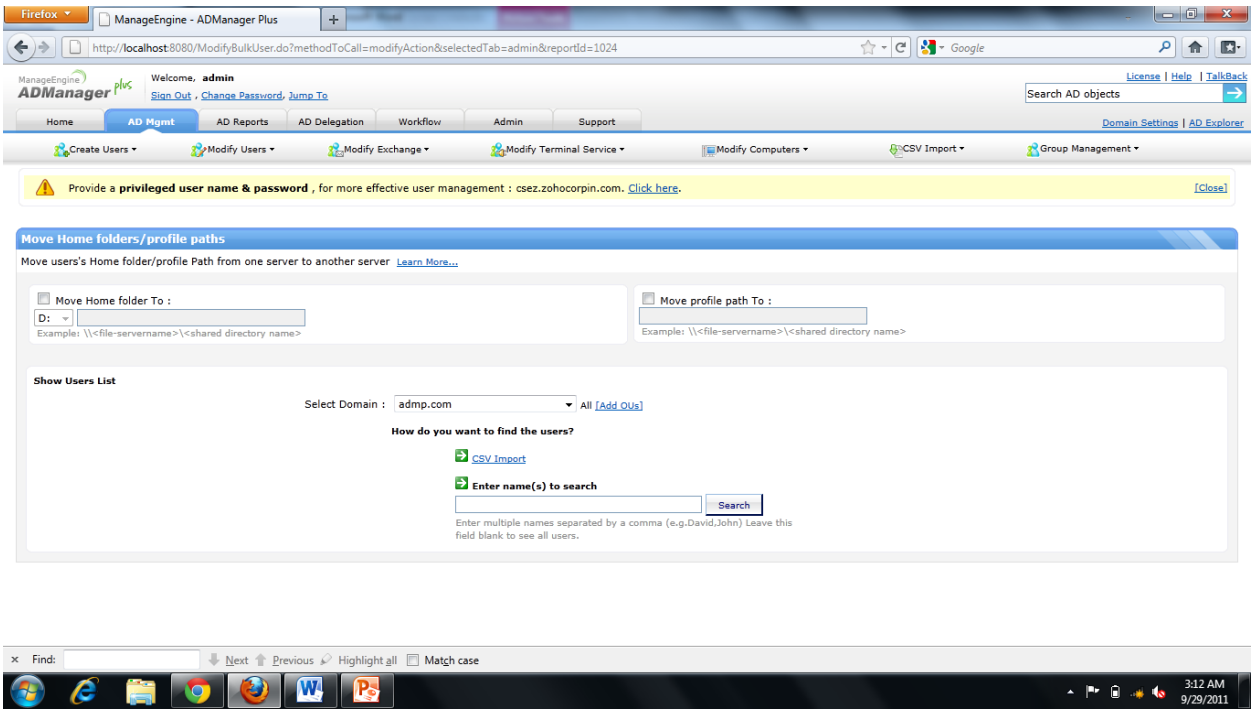
- Manually change the home folders and profile paths for each user, one by one.
- Or, take the even more tedious path of writing scripts.

Either way it is a demanding task and it could easily glue you down to your seats. Don't be surprised if you have to skip your lunch or your evening coffee and may be even your dinner and not to mention, your peace of mind.

With ADManager Plus, this task becomes really simple and this can be done for bulk users, from a single screen in a single step. No, it is not magic it is just that ADManager Plus puts in all this effort for you and you can do all these while you are enjoying your coffee.

Steps:

1. Click on 'AD Mgmt'
2. Click on 'Move HomeFolder' option under the 'Modify Users' Menu or 'User Management' → 'Move HomeFolders' under Bulk User Modification Section.
   This will take you to the 'Move Home Folders / Profile Paths' page.



3. Select ‘Move Home Folder To’ option and specify the new location.
4. Select ‘Move Profile Path’ option and specify the new server and share name.
5. Specify the Users for whom you would like to move the Home Folders and Profile Paths.

   You can specify the users in 2 ways:
   - Import a CSV file with the required list of users.
   - Search for the required users using the ‘Enter name(s) to search’ option in the required Domain and OU, if the users are limited to a specific OU.

Exercise 2: Create Exchange Mailbox for existing users along with additional email addresses.

Objective: Create Exchange mailbox for a set of existing users who are specified through a CSV file. Also create additional email addresses while creating Exchange Mailboxes for these users.

Using the native interface, it involves,

- Locating the user.
- Selecting the properties
- Choosing the Exchange Task
- Create Mailbox for the user
- To create additional email address, you need a few more additional steps.

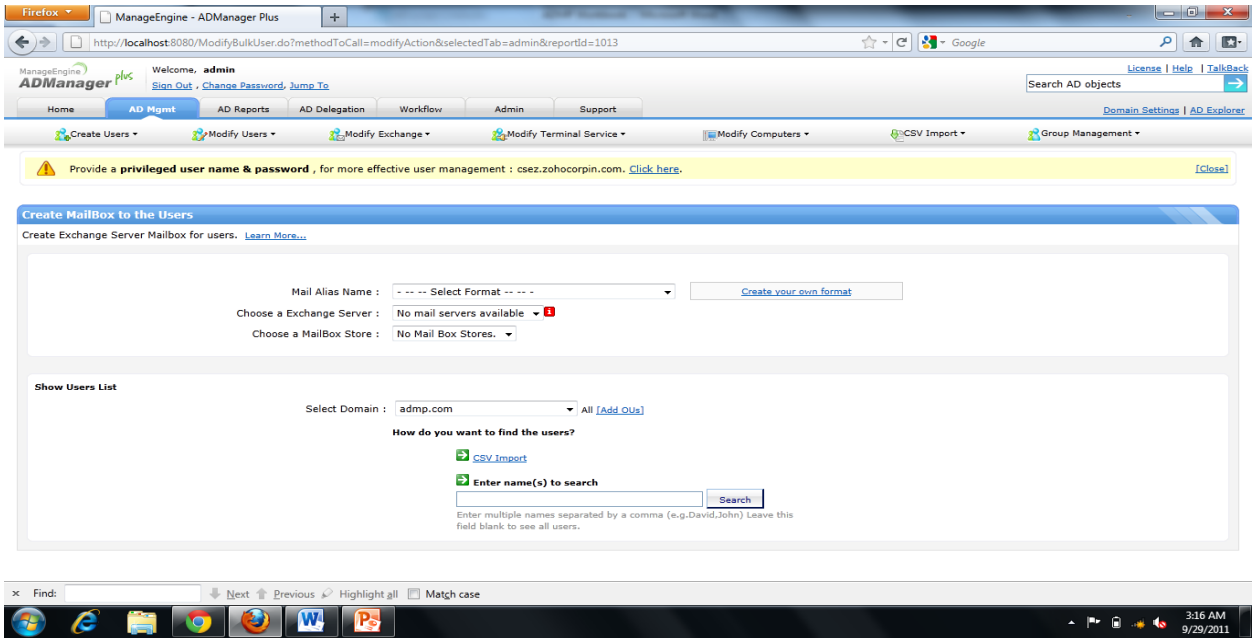
All these steps are to create a mailbox for just one user, yes, for only one user. Feeling really bad for the administrators? Just wait until someone wants to create mailbox for bulk users and that too with additional email address. You can really put a person's patience to test with these tasks.

With ADManager Plus, this is just as easy as lifting your finger, literally, as you can accomplish all these in just clicks in just a fraction of the time, for not just one user, but bulk users. With ADManager Plus, creating Exchange Mailbox is just a walk in the part and you will really have more time to spare for that evening walk on the park – you are totally stress free and you are an active directory administrator! Yes, it looks like it is one of those believe it or not stories, you better believe it!!

Steps:

1. Click on 'AD Mgmt'.
2. Click on 'User Management' → 'Exchange Tasks' → 'Create Mailbox'

You will now be in 'Create Mailbox to the Users' page.



3. Select a format for the email alias for users from one of the option in ‘Mail alias Name’ field.

To create your own format, click on ‘Create your own format’ where you can ‘Add New Format’ for your requirement. You can also specify conditions - which will allow you to use multiple formats based on specific conditions – using the ‘Add Advanced Format’ option.

4. ‘Choose an Exchange Server’ from the available servers.
5. ‘Choose a MailBox Store’ from the available options.
6. Select the Domain/OUs in which the users for whom the mailbox has to be created are located.
7. Click on ‘CSV Import’ to import the CSV file with the list of users.
8. Click ‘Apply’ to create mailbox for the users.

Exercise 3: Web-based Password Reset

Objective: Reset the password of active directory users, in compliance to the password complexities specified.

Resetting the password using native interface involves

- locating the user
- selecting the user
- selecting the reset option

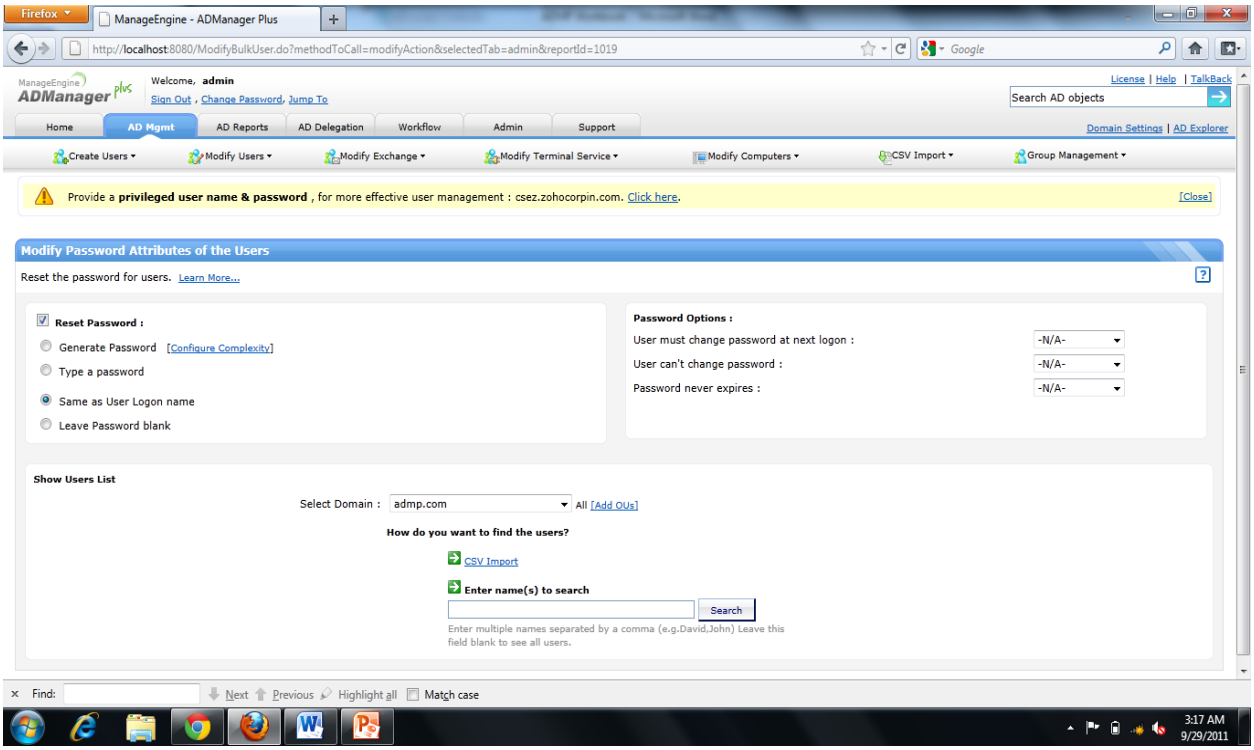
Yes, three different steps for just one task. For bulk users, the task becomes really bulky and too heavy and mundane to handle. Considering all the time and effort required, this task, a simple task, looks more intimidating!

But with ADManager Plus's 'Reset Password' feature, resetting password is just as easy as cutting through butter with a hot knife. Oh! Yes, with ADManager Plus, even the complex of tasks, become unbelievably simple.

Steps:

1. Click on 'AD Mgmt'.
2. Click on 'User Management' → 'Bulk User Modification' → 'Reset Password' or 'AD Mgmt' → 'Modify Users' → ' Modify General Attributes' → 'Reset Password'

You will now see the 'Modify Password Attributes of Users' page



3. Click on ‘Configure Complexity’ to set the complexities for the new password.
4. Select the ‘Reset Password’ option → Select an option to generate the new password.
5. Specify the ‘Password Options’ for the user.
6. Specify the domain/OUs to which the users belong to in ‘Select Domain’ option.
7. Specify the users for whom the password has to be reset through either a CSV file or search for the users using the ‘Search’ option.
8. Click ‘Apply’ for the changes to take effect.

Exercise 4: Modify the existing logon name of Users using a new naming format

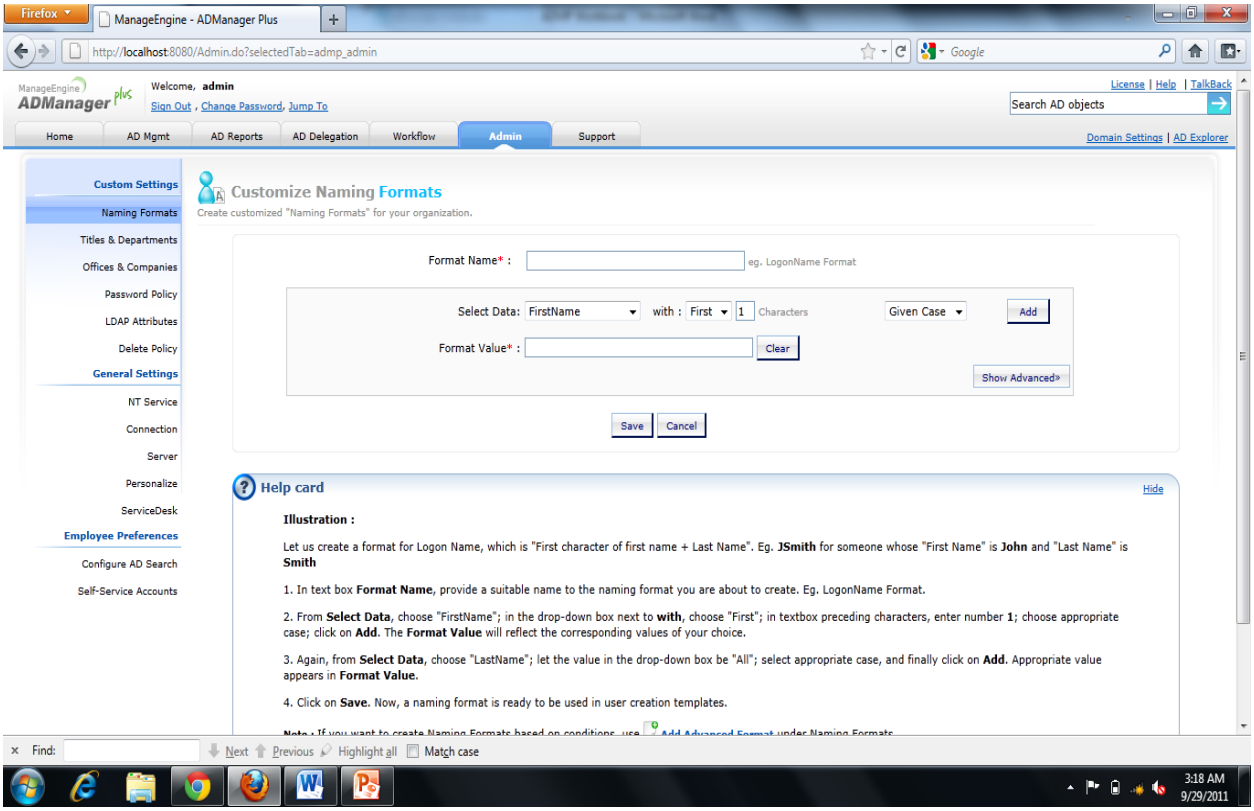
Objective: Create a new naming format with the "First character of first name and Last name", and then update the existing logon name of all users in any specific Department (OU)

Ever tried creating a new naming format using the native active directory interface and have your ever tried choosing a format from multiple naming formats using the native interface? Sculpting a statue out of a rock, with bare hands would be relatively easier.

With ADManager Plus, you can create any naming format as per your requirement or as per your liking. You can even have conditions, just for example, in case of the last name not being specified, you can fill that attribute with the department Id or the employee Id. And all you need is just a mouse to do this!

Create a new naming format:

1. Click on 'Admin' tab → 'Naming Formats' → 'Add New Format' on the top right corner.



2. Specify a 'Format Name' for this new naming format.
3. In 'Select Data' select 'FirstName' with 'First' '1' Character. Choose the case. Click 'Add'.
4. Select 'LastName' in 'Select Data', with 'First' '1' Character. Choose the case. Click 'Add'.
5. Click 'Save' to save the new format.

Modifying the existing logon name of all users in an OU

6. Click on ‘AD Mgmt’.
7. Click on ‘User Management’ → ‘Bulk User Modification’ → ‘Naming Attributes’

You will now be viewing the ‘Modify Naming Attributes of the Users’ page.

8. Select the new naming format that we created above from the dropdown box in the ‘Modify the Logon Name Format’ field.
9. Select the required Domain and OU.
10. Click ‘Apply’ for the changes to take effect.

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

Objective: Disable for the selected users, the option of allowing access to Outlook (emails) through the internet and also through the smartphones.

Using the native interface, one has to

- Locate the required user
- Modify the properties to edit the Exchange features that are specified for a user.
- Disable the options of accessing Outlook over web-browser and smartphones.

For multiple users or bulk users, simply repeat the steps until you have done this for all the users or until your fingers become numb or until you realize that you have missed your lunch, coffee and your supper too!

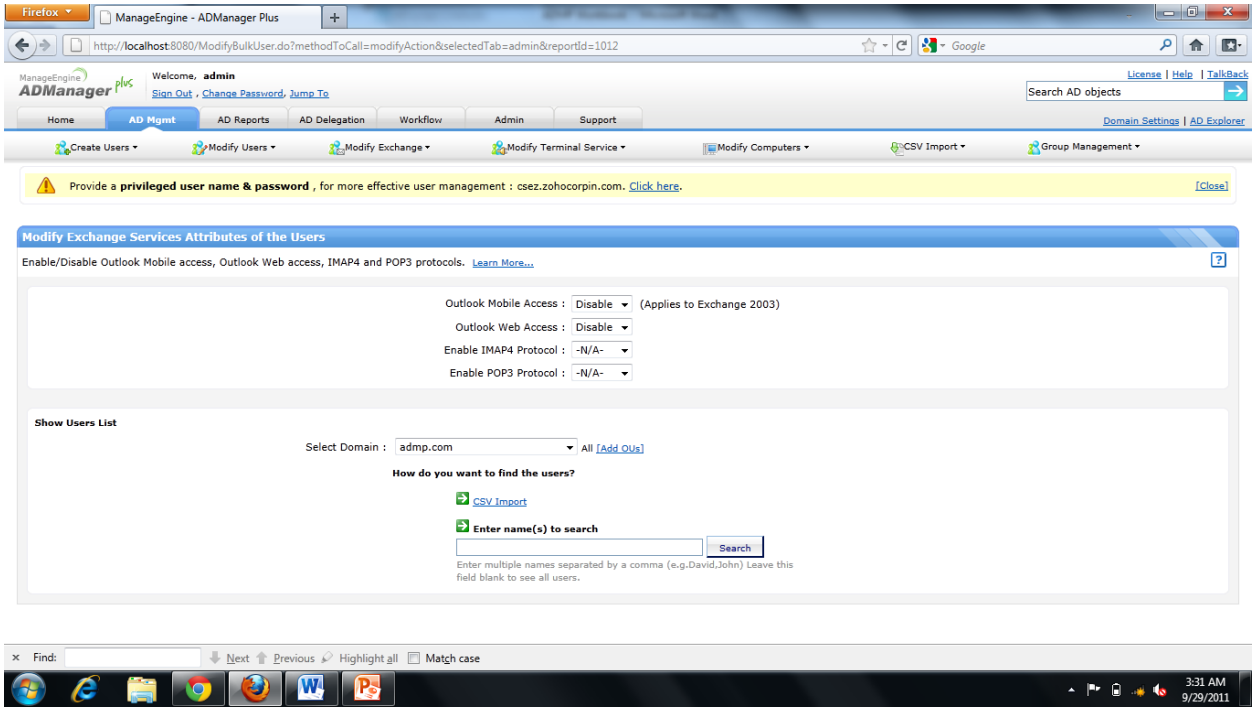
Or you can choose to use scripts and lose your sleep over writing the script, making it work or making the required modifications to the script, as and when there are changes in the Active Directory to make it work

With ADManager Plus, this demanding task becomes, just a point and click, single screen, single step task whether it is a single user or bulk users for whom these options have to be disabled.

Steps:

1. Click on 'AD Mgmt' Tab.
2. Click on ' User Management' → 'Exchange Tasks' → 'Exchange Features'

You will now be on the 'Modify Exchange Services Attributes of the Users' page.



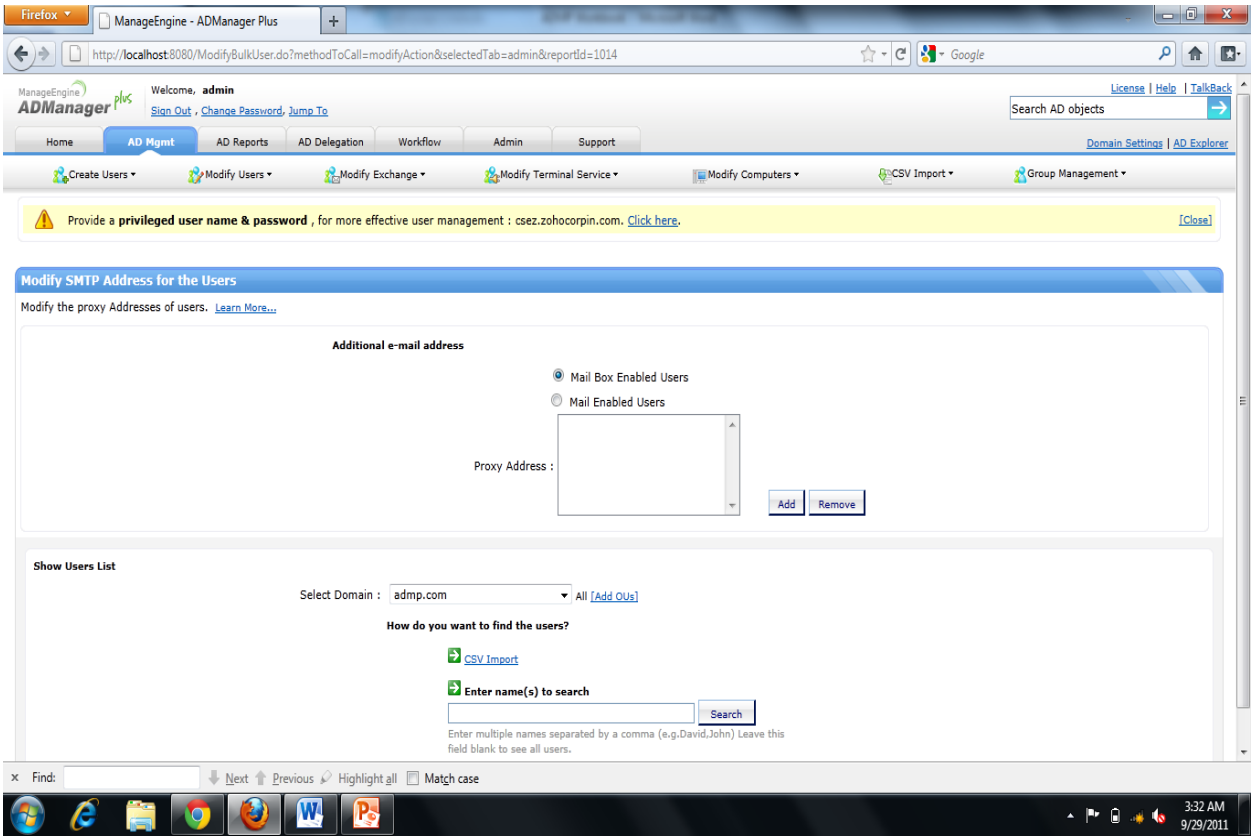
3. From the options in ‘Outlook Mobile Access’ and ‘Outlook Web Access’, select ‘Disable’ for both the features.
4. Select the Domain/OU in which the required User(s) are located.
5. Search for the required User(s) using the search option.
6. Click ‘Apply’ for the changes to take effect.

Exercise 6: Assign new Primary email address to users

Steps:

1. Click on ‘AD Mgmt’ Tab.
2. Click on ‘User Mangement’ → ‘ Exchange Tasks’ → ‘Modify SMTP’ Address.

You will now be in the ‘Modify SMTP Address for the Users’ page.



For ‘Mail Box Enabled Users’

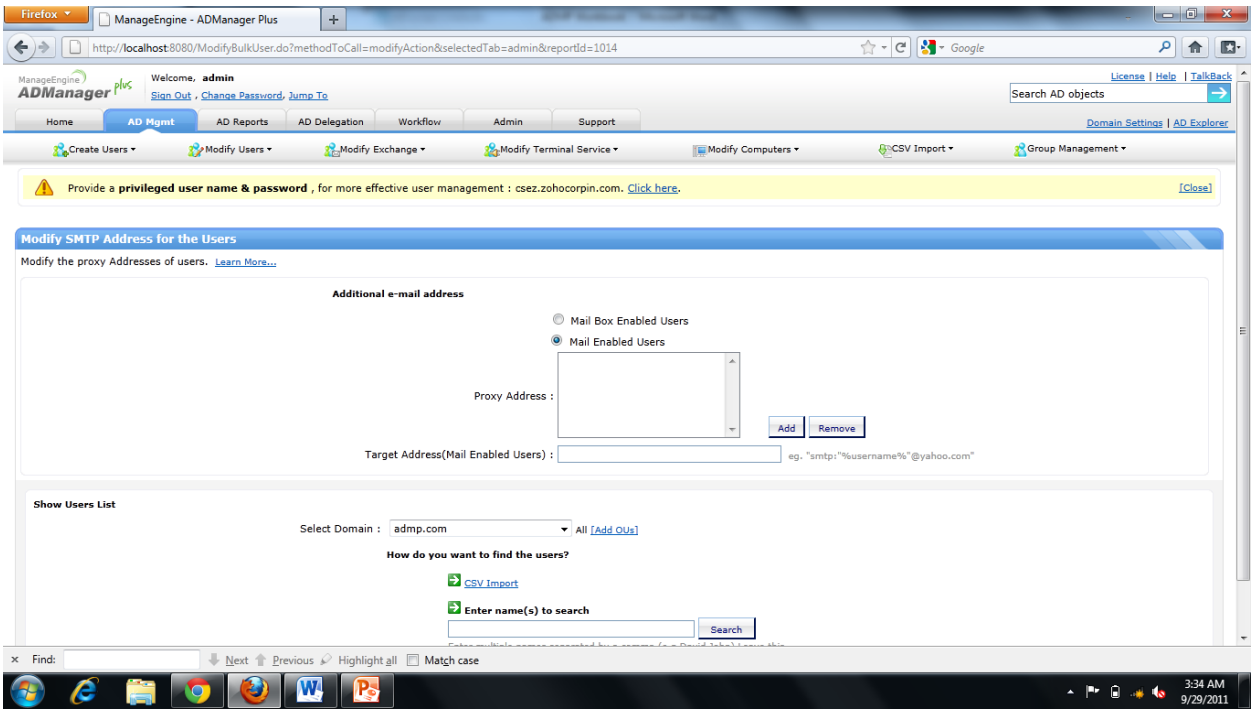
3. Click ‘Add’ next to the ‘Proxy Addresses’ field.
4. Specify the new ‘email Address Format’ with the prefix ‘SMTP:’ to set this new format as the ‘Primary email Address’.

For example, ‘SMTP: %givenname%%initials%@neworganization.com’ will have the firstname+middlename@neworganization.com as the naming format for the new email address for all the users in the new organization and will also set it as the primary email address.

5. Having the prefix ‘smtp:’ will set the email address as a secondary one.

For ‘Mail Enabled Users’

6. Specify the new format in the ‘Target Address’. Refer the previous step to specify a new format as per the requirement.



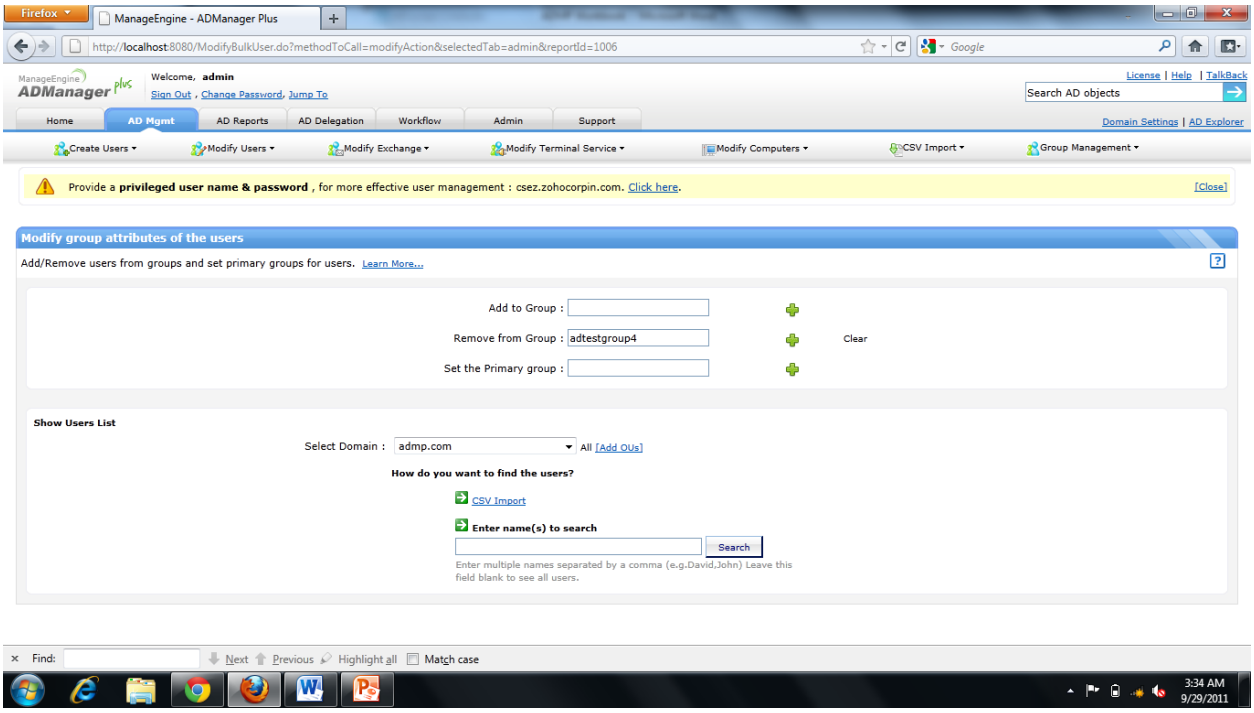
7. Select the required ‘Domain/OU’ and specify the list of users using either a CSV file or by locating them using the ‘Search’ option.
8. Click ‘Apply’ for the changes to take effect.

Exercise 7: Add set of users in a CSV file to a group and set another group as their primary group

Steps

1. Click on 'AD Mgmt' Tab.
2. Click on 'User Management' → 'Bulk User Modification' → 'Group Attributes'

You will now be in the 'Modify Group Attributes of the Users' page.



3. Click on '+' beside the 'Add to Group' field to specify the group to which the users have to be added.
4. Click on '+' beside the 'Set the Primary Group' field to set the required group as the primary group.
5. Select the 'Domain/OU' to which the users have to be added.
6. Click on 'CSV' import option to import the list of specific users.
7. Click 'Apply' to make the changes take effect.

Exercise 8: Modify user accounts through modification templates

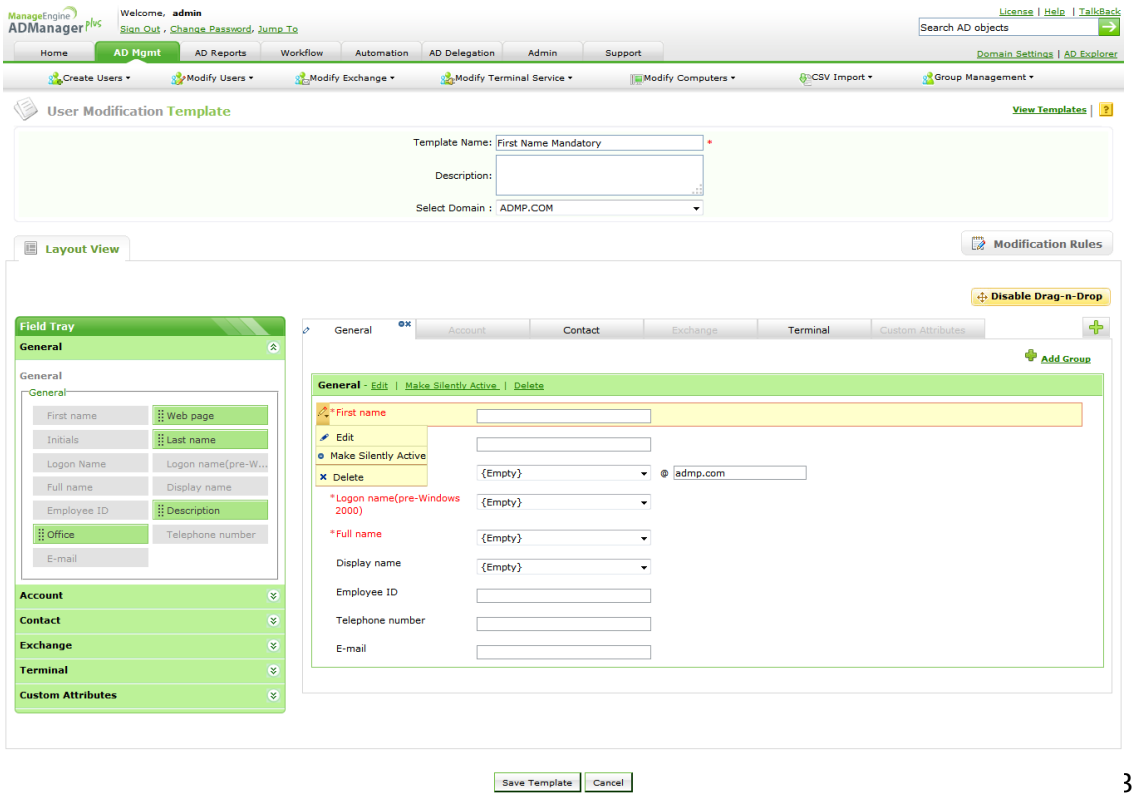
Scenario: Allow helpdesk technicians to modify user accounts through 'user modification templates' with the following conditions:

- For Technician 1'First Name' should be a mandatory attribute, for Technician 2 'Employee Id' must be mandatory.
- For Technician 1, the Account, Exchange and Custom Attributes tabs should be completely hidden; In Terminal Services tab, all attributes except 'remote control' and 'remote access' permissions should be read only.
- For Technician 2, the Terminal Services and Custom Attributes tabs should be hidden completely; in Exchange tab, all attributes except the Outlook web-access, protocols and mobile access related settings should be hidden.

To accomplish this, you will have to create two different user modification templates, one with the conditions for technician 1 and the other for technician 2. Assign them to the helpdesk technicians which will allow them to modify user accounts in their designated domain(s) or OUs.

Steps to create 'First Name Mandatory' user modification template for 'Helpdesk Technician 1':

1. Click on 'AD Mgmt' → 'User Management'
2. Under 'User Templates', click on 'User Modification Templates'
3. In the 'User Modification Templates' page, click on 'Create New Template'.
4. Enter a name and description for the template. For this illustration, let us name this template as 'First Name Mandatory'.



5. Select the domain in which this template will be used. Click on ‘Layout’ view → ‘Enable Drag-n-Drop’.
6. To make 'First Name' mandatory,

    a. In the 'Layout View' click on 'Enable Drag-n-Drop' button.
    b. Click on 'General' Tab.
    c. Place the mouse over the 'First Name' field and then on the edit icon that appears beside the field name.
    d. From the options listed, click on 'Edit'.
    e. In the 'Editing First Name' window that pops up, under 'Security', select 'Mandatory' and click on 'Done'.

7. To hide 'Account', Exchange' and 'Custom Attributes’ tabs,

    a. Click on 'Account' tab.
    b. Click on the '-' icon located at the top right corner of ‘Account’ tab. This will hide the tab and make it silently active.
    c. Similarly, make Exchange and Contract Attribute tabs hidden (silently active).

8. To make all attributes in Terminal Services tab, except the except ‘remote control’ and ‘remote access’ attribute read-only:

    a. Click on ‘Terminal’ tab.
    b. Place the mouse over 'User Profile' field; click on the edit icon that appears beside the field name.
    c. In ‘Editing User Profile’ window, click on Options → Make it: 'Read Only'.
    d. Click on ‘Done’ to save the changes.
    e. Similarly, make all the required attributes in the ‘Terminal’ tab read-only.

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

    Similarly, create another template with: 'Employee Id Mandatory', Terminal Services and Custom Attributes tabs hidden; all attributes except Outlook web-access, mobile-access and protocol related attributes in the ‘Exchange Tab’ have to be hidden.

10. Create a new 'User Modification Role' in 'AD Delegation'
    (Refer ‘Create new Help Desk Role’ exercise in ‘Non-invasive Active Directory Delegation’ section for steps to create a new role.)

11. Create Help Desk Technician 1or select this technician from the available help desk technicians. (For steps to a new technician, refer 'Create new Help Desk Technician' exercise in 'Non-invasive Active Directory Delegation' section)
12. To assign 'First Name Mandatory' template to technician 1:
    a. Click on 'AD Delegation' → Help Desk Delegation → Help Desk Technicians.
    b. Select 'technician 1' from the list of Click on 'Edit' icon in the 'Action' column of the required technician.
    c. In Assign Templates → 'Add/Edit Templates'.
    d. In the Select Template window, choose the require domain.
    e. Click on 'User Modification Templates' → Select the 'First Name Mandatory' template. (Click on the icon beside the name of the templates to make it a default template.)
    f. 'Save Changes' to complete this process.
    g. Similarly assign the 'Employee Id Mandatory' template to technician 2.

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

Exercise 9: Flexible CSV based User Modification

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

Performing modifications in the existing attributes of AD users is a mammoth task for AD admins. However, with ADManager Plus it becomes fairly simpler.

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

Steps:

1. Go to 'Ad Mgmt' → 'Modify users'

2. Import a csv file with LDAP headers

3. Click on Update in AD → Choose the attributes to be modified → Click on 'Advanced' to select the available flexible options.

4. Click OK to update the values in AD.

Exercise 10: Modify user accounts using 'modification templates' and 'modification rules' to auto-update critical user attributes.

Scenario: A Senior Sales Executive of ACME Corp. 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 automatically updated based on the changes made.

To accomplish this:

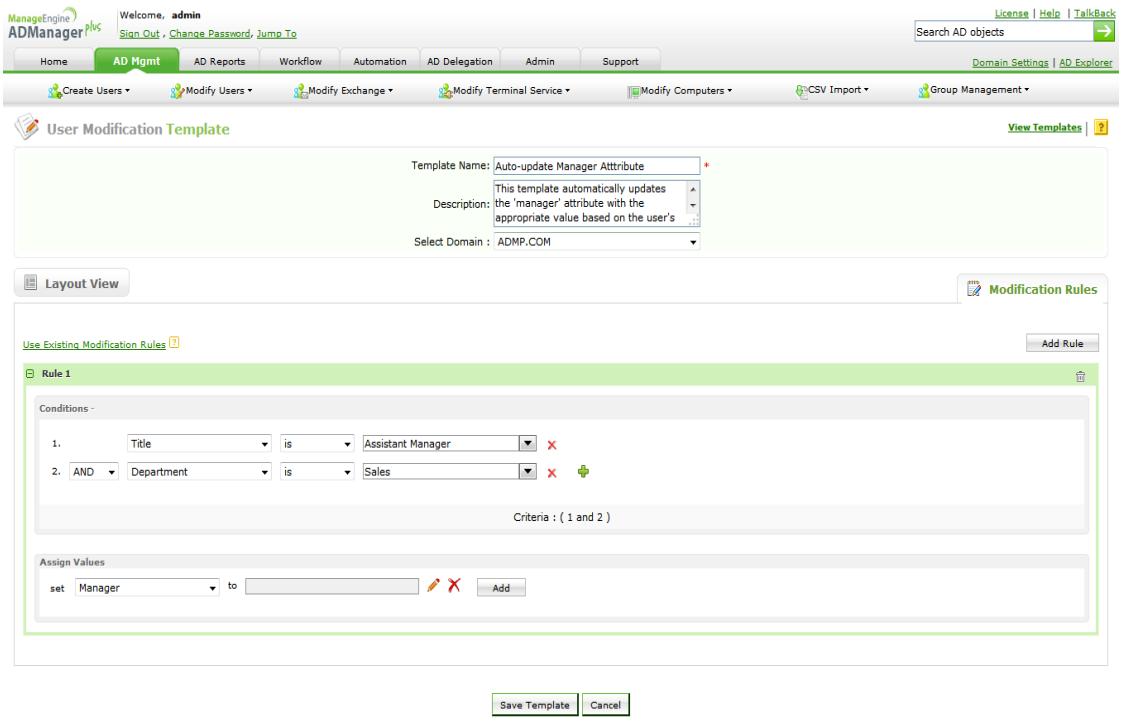
- Create a new 'User Modification Template' which will
  - Allow a technician to update the 'City and 'Title' attributes with new values.
  - Automatically update the 'Manager' and 'State' attributes of the user account based on the new values in 'Title' and 'City.
  - Hide all attributes, except the ones in the 'General' and 'Contact' tabs, from the helpdesk technician who will be using this template to modify the user account.
- Assign this template to the appropriate helpdesk technicians who have the permission to modify user accounts.
- The technician has to apply this template for modifying the user accounts.

Steps:

1. Create a customized User Modification Templates with Modification Rules

a. Click on 'AD Mgmt' --> 'User Management'
b. Under 'User Templates', click on 'User Modification Templates'
c. In the 'User Modification Templates' page, click on 'Create New Template' link
d. Specify a name and suitable description for this template. For this illustration, let us name this template as 'Auto-update Manager Attribute'.
e. Select the domain in which this template will be used.
f. Create a rule to assign values to the 'Manager', 'State/Province' attributes as per the values in 'Title', 'Department' fields,
   1. Click on 'Modification Rules' → 'Create New Rule'.
   2. Provide a suitable name for the new rule by clicking on 'Rule 1'. In this case, let us name this rule as 'Manager Update'.
   3. In 'Conditions' pane, click on 'Add Conditions'
   4. In 'select field' option, click on 'Title'. Select 'is' as the condition.
   5. In the value box, enter title – for this exercise, enter 'Assistant Manager' and click on '+' to add a new condition.
   6. In the second condition, select 'AND' as the criteria and 'City' in the 'select field' option.

7. Select 'is' in the condition and specify the city as ‘Houston’. Similarly, add Department is ‘Sales’ in the condition.



8. In the 'Assign Values' section, in the 'set' option, select 'Manager' attribute and in 'to' option, specify the manager name. For this illustration we will use 'David Smith' as manager and click on 'Add'. In the next 'set' option, select ‘State/Province’ and specify ‘Texas' in the 'to' field.
9. Add another 'Rule' to check for another set of 'Title', ‘City’ and ‘Department’ values to specify the corresponding ‘Manager’ and 'Stage/Province’ field values.
10. Repeat steps: a to h and add as many rules as needed to check for all possible 'Title', 'City' combinations and specify the corresponding 'Manager', 'State/Province' values.

g. Hide all tabs except ‘General’ and ‘Contact’ tabs:
    1. Click on ‘Account’ tab → ‘-‘ icon in 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 using this template for user modification.
    2. Similarly, hide all the other tabs: Exchange, Terminal and Custom Attributes.

Note: To hide a specific attribute, in the drag-n-drop’ mode just place your mouse over the edit icon that appears when you ‘mouse-over’ that attribute and select ‘Make Silently Active’ from the options.

h. Click on 'Save Template' to create and save this template.

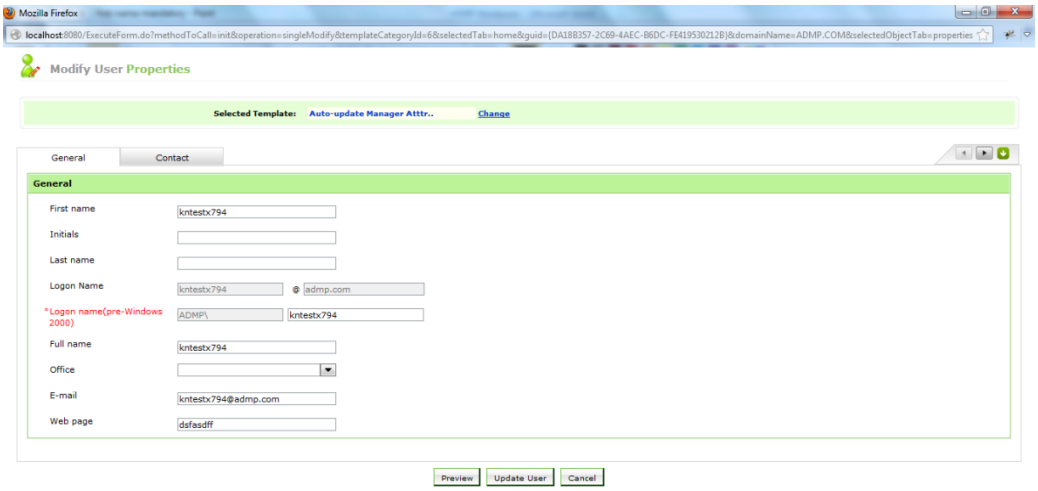
2. Assign this template to the required helpdesk technicians:

a. Click on ‘AD Delegation’ → Help Desk Delegation → Help Desk Technicians.
b. 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)
c. Click on ‘Edit’ icon in the ‘Action’ column of the required technician.
d. In Assign Templates → ‘Add/Edit Templates’.
e. In the Select Template window, choose the require domain.
f. Click on ‘User Modification Templates’ → Select the ‘Auto-update Manage Attribute’ template. (Click on the icon beside the name of the templates to make it a default template.)
g. ‘Save Changes’ to complete this process.

3. Modify user accounts through ‘user modification templates’:

a. Locate the required user account and choose the appropriate template:
   1. The helpdesk technician has to login to ADManager Plus
   2. Click on ‘AD Mgmt’ → ‘Modify Single User’.
   3. Select the ‘Domain’ in which the user account to be modified is located. Key in the user’s name in the search box and click on ‘Go’ to fetch the required user.
   4. Click on ‘Modify User’ button located in the ‘Action’ column of the user. The ‘Modify User Properties’ window will now pop up.
   5. 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.

b. Update the ‘Title’ & ‘City’ attributes manually; Auto-update ‘Manager’ & ‘State/Province’



1. Once you select ‘Auto-update Manager Attribute’ template, you will be able to view only the ‘General’ and ‘Contact’ tabs as this template makes all other tabs and properties ‘hidden’.
2. Click on ‘Contact’ tab since ‘Title’ and ‘City’ are located in the Contact tab. Enter the new values for both these attributes. In this case (Title= Assistant Manager, City=Houston)
3. To view all the attributes that you have modified, click on ‘Preview’. This will list all the attributes along with their old and new values that you have just entered.
4. 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.
5. To save the changes that you made, click on ‘Update User’.
   While saving the changes, in addition to the attributes that you manually modified, the attributes specified in the ‘modification rules’ will also be updated automatically.

Exercise 11: Exchange Tasks - Migrating Mailbox

Scenario: With rapidly evolving technology, architects have been designing new features and enhancements more frequently. Therefore, users have been receiving upgrades for their environments in shorter intervals. In a typical upgrade scenario, Active Directory or Exchange is configured with new machines. An IT Administrator's involvement during the time of such a scenario significantly increases in terms of volume as well as skills. Tasks such as migration of mailboxes from one exchange server to another could be a really tricky.

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

Sometimes hybrid environments also evolve as a result of an upgrade, involving multiple versions of Microsoft Exchange. To ensure a smooth, error-free process in such a scenario requires key administrative activities like mailbox migration. If you are looking for a console to move a mailbox from a specific server to any mailbox store in another server, the 'migrate mailbox' functionality in AD Manager Plus is just the thing you need.

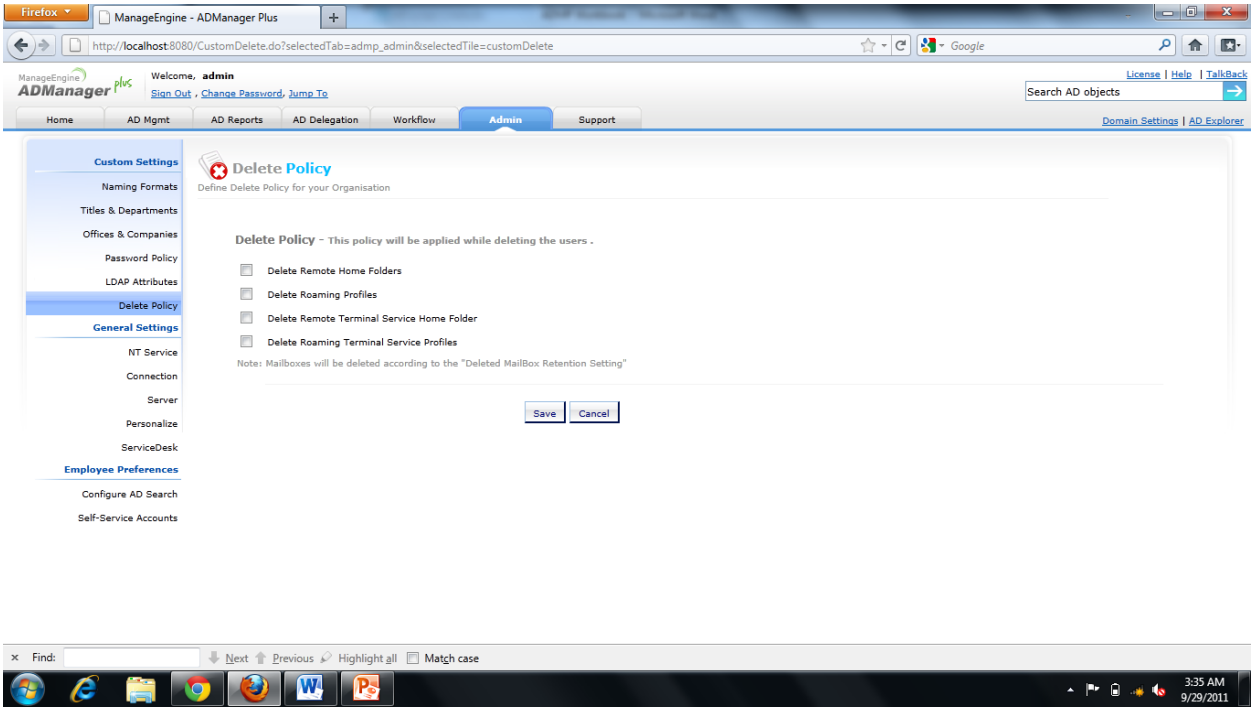
4. De-Provisioning:

De-provisioning is another vital task that every administrator has to do repeatedly for different 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, for now ADManager Plus 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 and also their home folders and profiles.

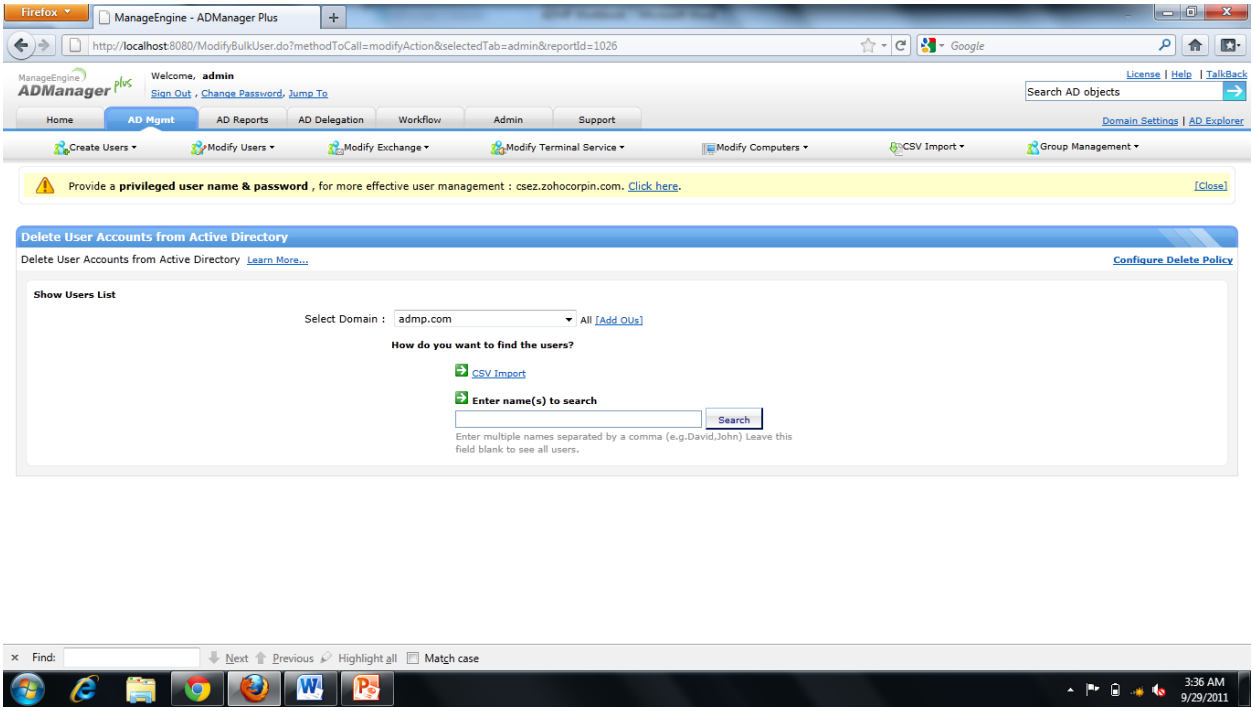
Configuring the Delete Policy

1. Click on 'Configure Delete Policy' to delete the user specific folders like 'Remote Home Folders', 'Roaming Profiles' as per the requirement from the options available.
   This can also be set from 'Admin' Tab → 'Custom Settings' → 'Delete Policy'. This policy will be used to delete user related folders while deleting the user accounts.



Deleting Users:

2. Click on 'AD Mgmt' Tab.
3. Click on 'User Management' → 'Bulk User Modification' → 'Delete Users'.
4. Select the 'Domain/OUs' in which the users are located.
5. Specify the exact set of users to the de-provisioned using the 'CSV Import' option or locate the users using the 'Search' option.



6. Click ‘Apply’ to delete/de-provision the users. 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 eliminate users with duplicate attributes

Objective: To find users in AD who have duplicate values for certain attributes, and take necessary actions.

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.

By using 'Users with duplicate attributes’ report, we can specify the attribute(s) that may have been duplicated. This would provide us a list of users from which we can perform the required action like search, disable, delete or modify the user attributes individually or in bulk.

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

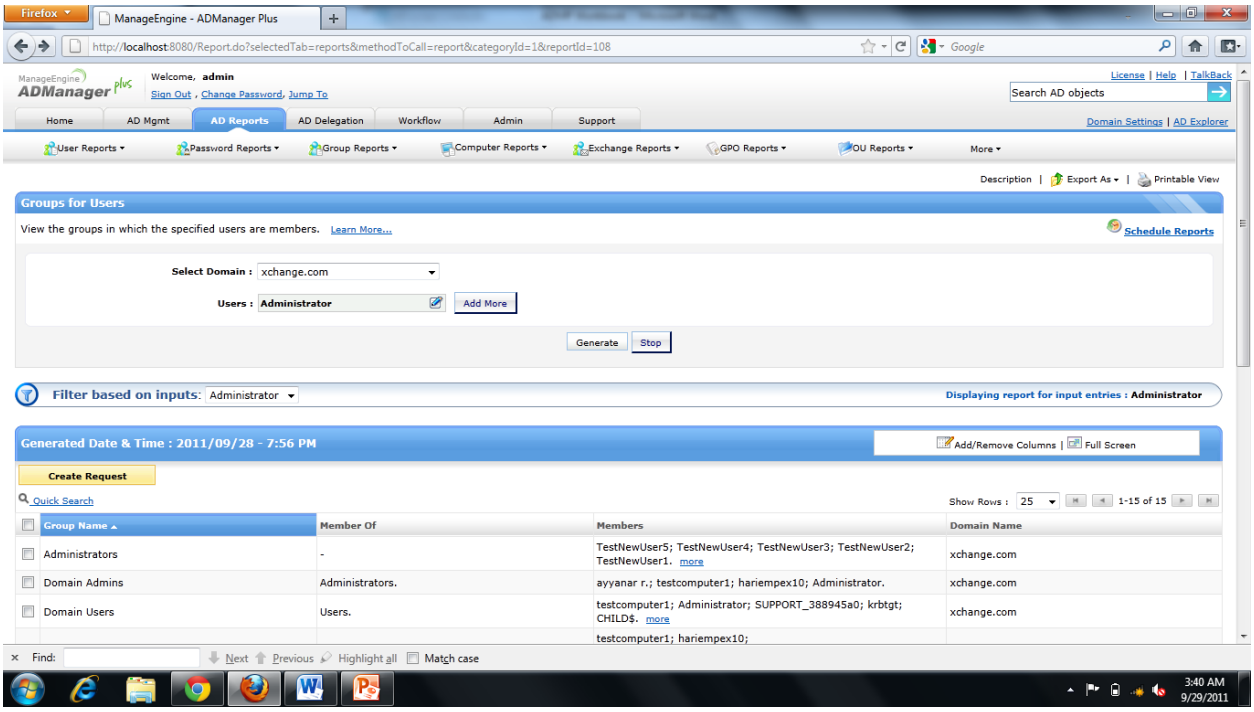
Objective: Search for an user in a specified group, delete the group if the user is not a member of this group.

To do this using the native AD interface, you will have to first locate the user using the find option and then find out if he is a member of the specified group from the MemberOf tab in the properties. If the user is not a member of the specified group, the group has to be located using the find option again and then delete the group.

ADManager Plus simplifies this procedure for you by breaking this down into two simple steps.

Check whether the mentioned user is part of the specified group:

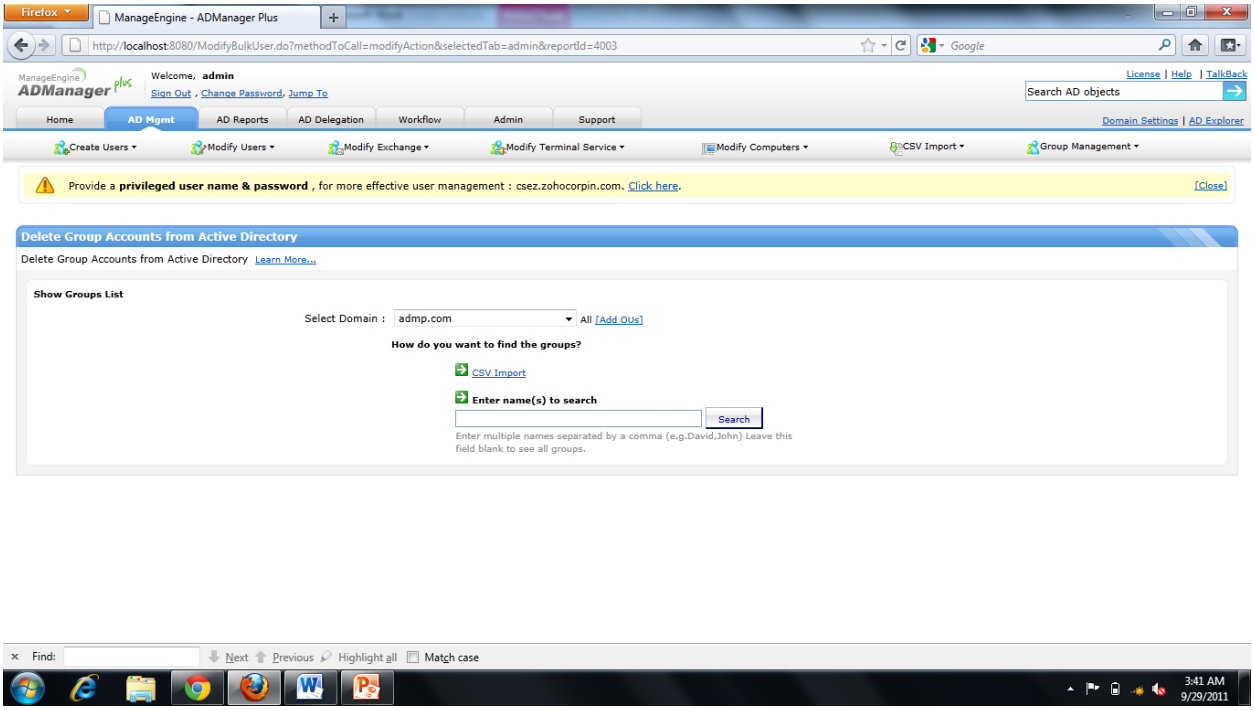
1. Click on 'AD Reports' → 'User Reports' → 'Nested Reports'→ 'Groups for Users'



2. Select the 'Domain' in which the user is located.
3. Click 'Generate' to get the list of all the groups that this user belongs to.
4. Search for the group in the 'Quick Search' option.
5. If the required group is not in the list of groups, we will proceed to delete the group.

Delete a group:

6. Click on ‘AD Mgmt’ → ‘Group Management’ → ‘Bulk Group Modification’ → ‘Delete Groups’



7. Select the ‘Domain’ in which the group is located.
8. Specify the name in the ‘Enter name(s) to search’ option and search.
9. Select the group and click ‘Apply’ to delete the group.

5. Active Directory Reporting

Reporting is a mandatory and a tedious task too for any Active Directory administrator. With so many IT standards that have to be followed, reporting to show compliance to the standards has become imperative. Audit reports are also vital to keep track of all that is happening in the Active Directory.

But the native Active Directory interface has nothing to help the administrators when it comes to reporting. Administrators most often are forced to rely on scripts which make the already tedious task of reporting more taxing, with so many scripts that have to be written for every single reporting need.

ADManager Plus makes reporting a walk in the park for every Active Directory administrator. With simple, UI based, 150+ readymade reports for every need and every purpose, you will find that Active Directory reporting is something that is no longer a hard and tedious task.

ADManager Plus reports are not just static reports, they are also actionable reports, that is, from the reports, and you can perform any management task if it is required. For example, you could find out a list of all the users whose password has expired and reset the password for all of them, in just one single step, from the report itself.

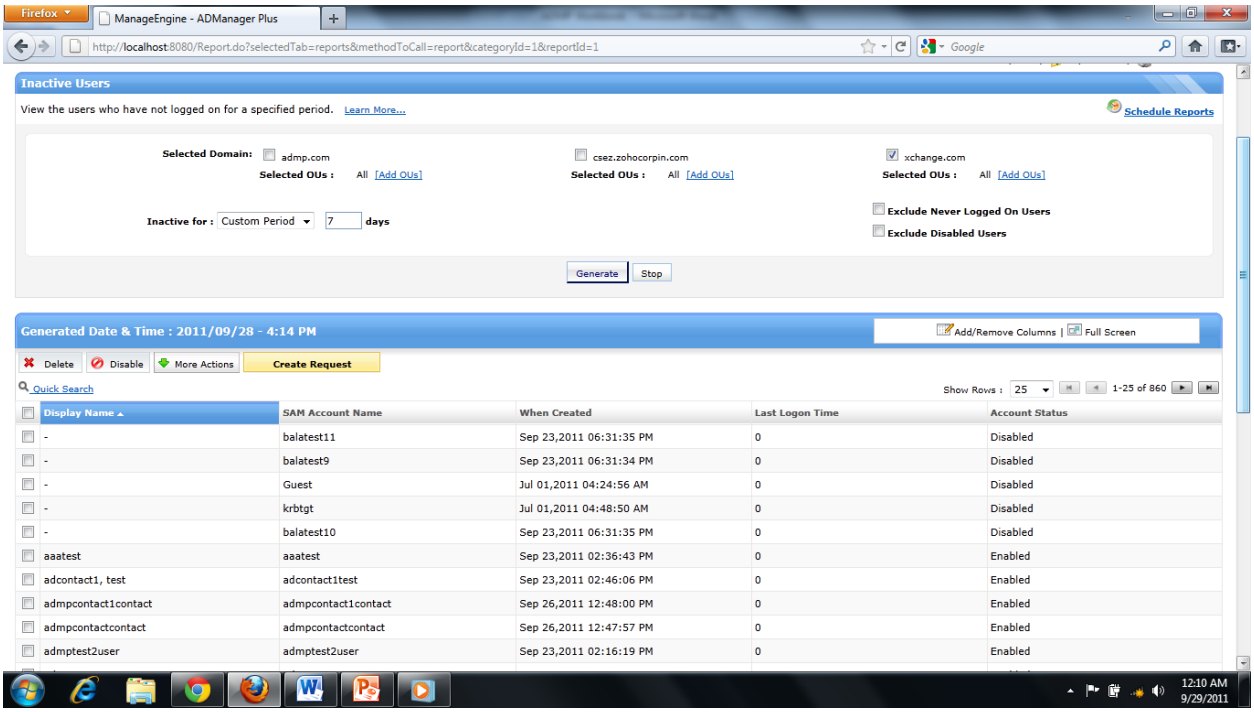
Exercise 1: Inactive Users Report

Objective: Pull out a list of all the users who have been inactive for a specific period of time in the Active Directory.

Steps:

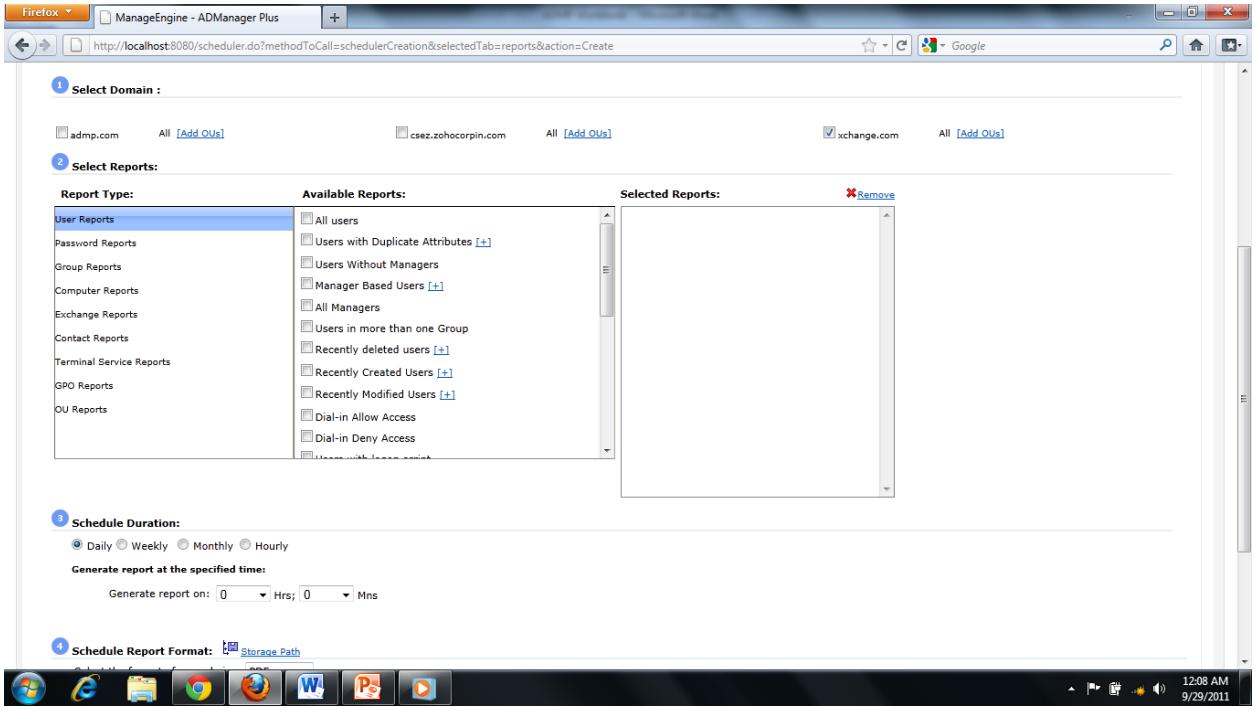
1. Click on 'AD Reports'
2. Click on 'User Reports' → 'Logon Reports' → 'Inactive Reports'

You will now be in the 'Inactive Users Page'.



3. Select the 'Domain' from which you would like to pull out the list of inactive users.
4. Select the period/time for which you would like to get this report. You can select any one of the options in 'Inactive for' field or specify a custom period.
5. You can also exclude the users who have been disabled or have never logged in by selecting the options.
6. Click 'Generate' to run the report.
7. From the list of users generated, you can choose to do any management task like disabling them, resetting the password, delete, etc as per the requirement using the management options present under the 'More Actions' option or if you do not have the privileges to perform the tasks, you can create a request for the required task using the 'Create Request' option.
8. You can also search for any specific user from the list of inactive users using the 'Quick Search' option.
9. Using the 'Export as' option, you can export this report in CSV, HTML, XLS, PDF, CSVDE formats.

10. Finally, this report can also be scheduled to run at the specified time daily, weekly, hourly or monthly as per the need using the ‘ Schedule Reports’ option.



11. You can also specify the format in which the report has to be exported and also send it to any specific person by mentioning their email id by using the appropriate options in the ‘Schedule Reports’ page.

Exercise 2: Office 365Reporting - Inactive Users

Objective: To trace inactive Office 365 users.

Microsoft assigns ‘inactive’ status to an Office 365 mailbox if the concerned user has not logged in for more than 30 days.

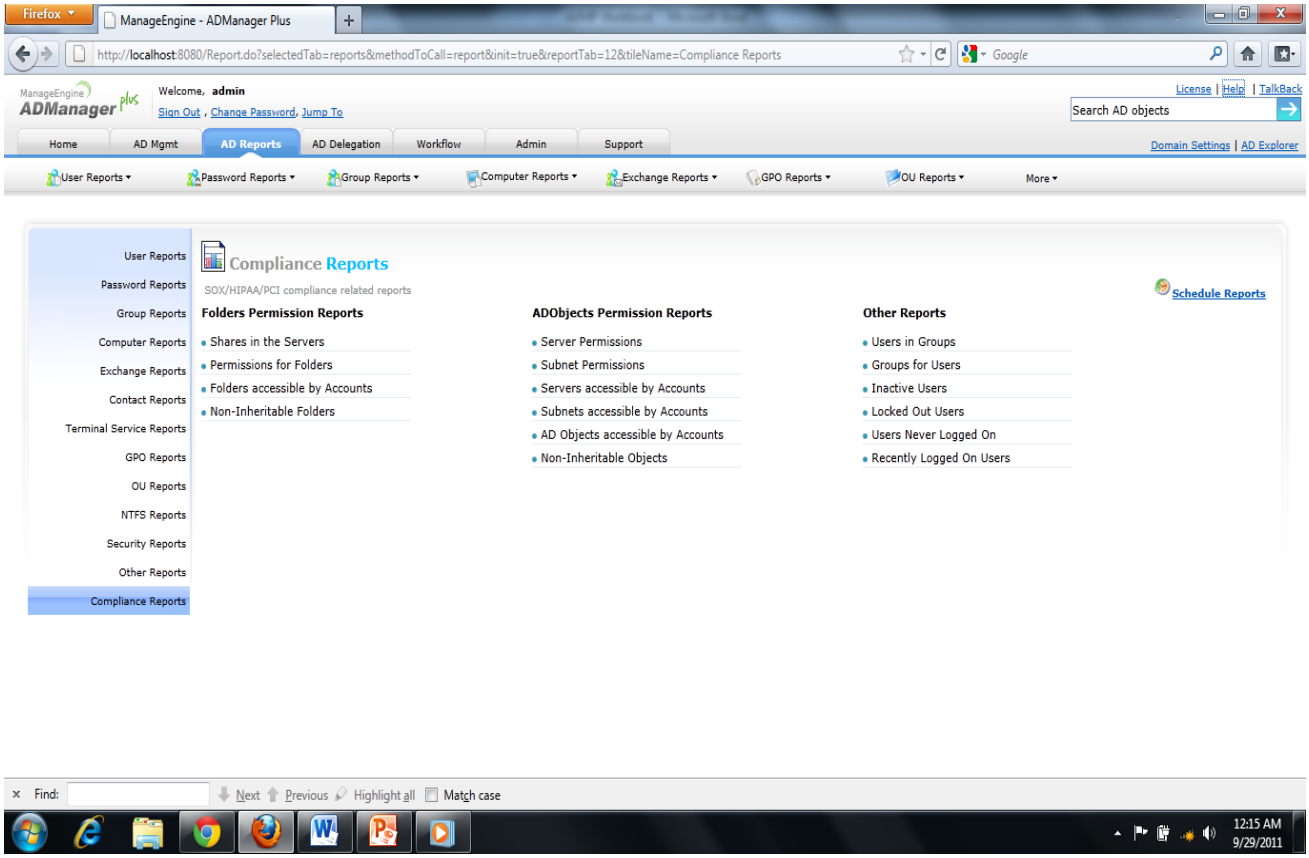
‘Inactive O365 user report’ in ‘AD Reports’ tab identifies such users and provides a list of the corresponding mailboxes and related details.

Exercise 3: IT Compliance Reports

Objective: Run reports that are specifically needed for proving the compliance to IT standards like SOX, HIPAA, PCI, etc.

Steps:

1. Click on ‘AD Reports’.
2. Click on ‘Compliance Reports’



3. There are pre-built reports that can be specifically used for showing compliance to IT standards.
4. You can select any report from the list of reports listed under three different categories in the ‘Compliance Reports’ page.

Exercise 4: Share(s) 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.

In the native environment, this will involve

- locating the desired server
- finding out all the shares that are in the server
- locate the specific share from among all the shares listed
- find out all the users who are have permissions for that specific share
- go through each user to see the exact permission that they have on the share.

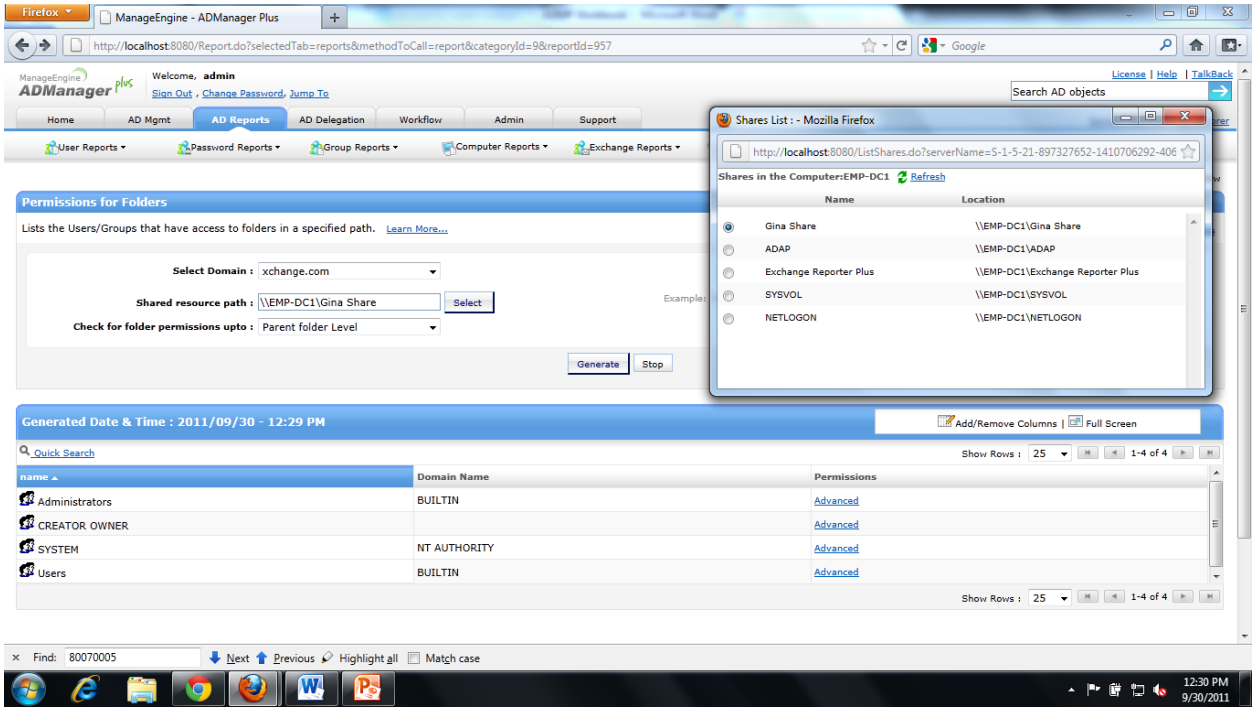
It took a few minutes to just type these steps. Just imagine the time that you will have to spend to actually do these in the native interface. To do this task of locating all the servers and the shares on them and also the users who have permissions on the shares, it will require so much time and effort that the administrator will have to do only this task on any particular day.

ADManager Plus gives you an easy way out for this scenario. All that you have to do is click on the specific report and click run which will fetch you all the required information and you can do all this without even breaking a sweat.

Steps:

1. Click on 'AD Reports'.
2. Go to 'NTFS Reports' → 'Permissions for Folders' report.

You will now be taken to the 'Permissions for Folders' page.



3. Select the ‘Domain’.
4. Select the Server for which you would like to list the available shares.
5. Select the share for which you would like to see the list of users who have permissions on the share.
6. Select the level upto which you would like to generate this report, that is, parent level or sub-folder level or the number of levels of sub-folders.
7. ‘Generate’ the report.
8. You can search for any particular user, to see his permissions, using the ‘Quick Search’ option.

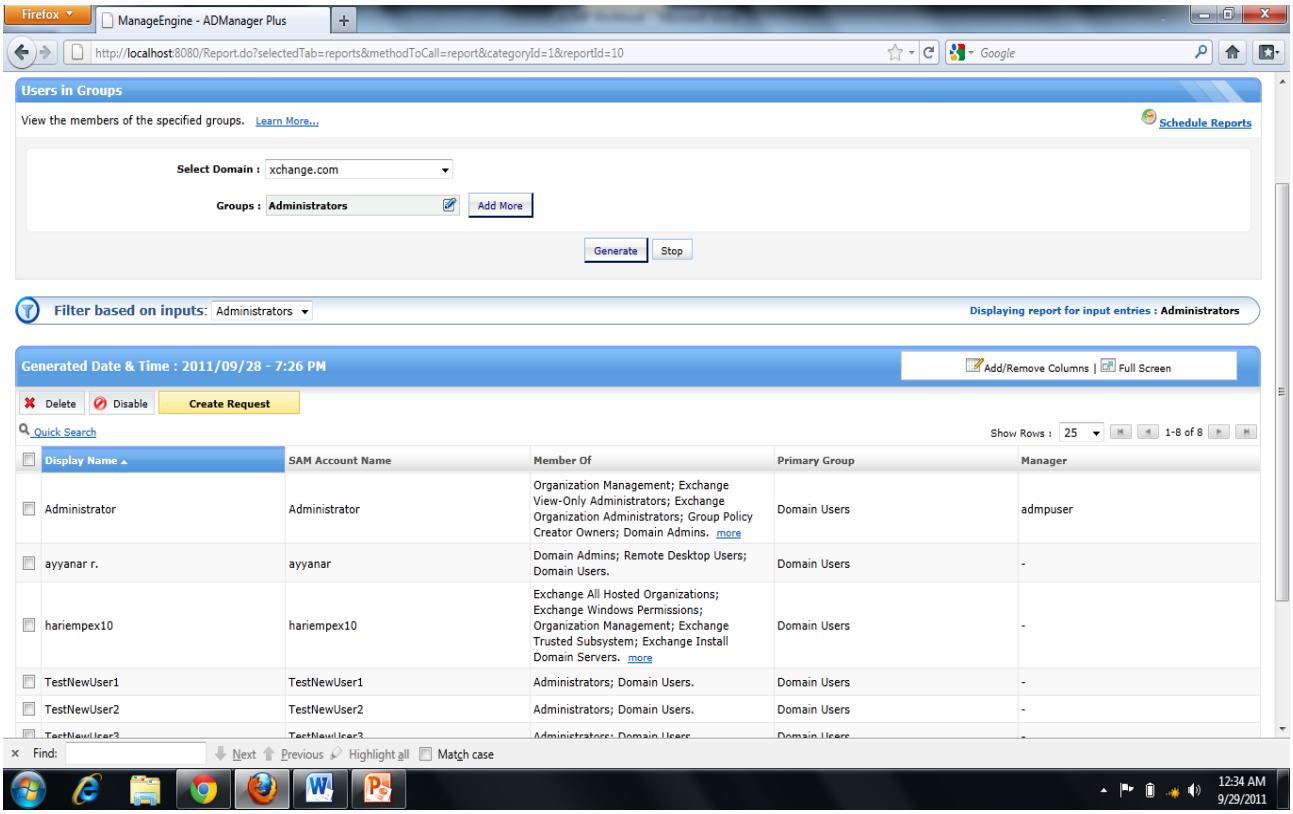
Exercise 5: List Users in a Group

Objective: For any given group(s), generate a report with the list of all the users who are members of the specific group(s).

Steps:

1. Click on 'AD Reports'.
2. Click on 'User Reports' → 'Nested Reports' → 'Users in Groups'

You will now see the 'Users in Groups' page.



3. Select the 'Domain' in which the group is located.
4. Specify the 'Group'. You can specify more than one group also.
5. Click 'Generate' to get the list of users in the specified group(s)
6. You can also do any management task, if needed, using the management options at the top of the report namely the 'Delete', 'Disable', 'Create Request' options.

Exercise 6: Performing a secure directory /Address Book wide search for Domain users

Objective: To enable user search option through browser.

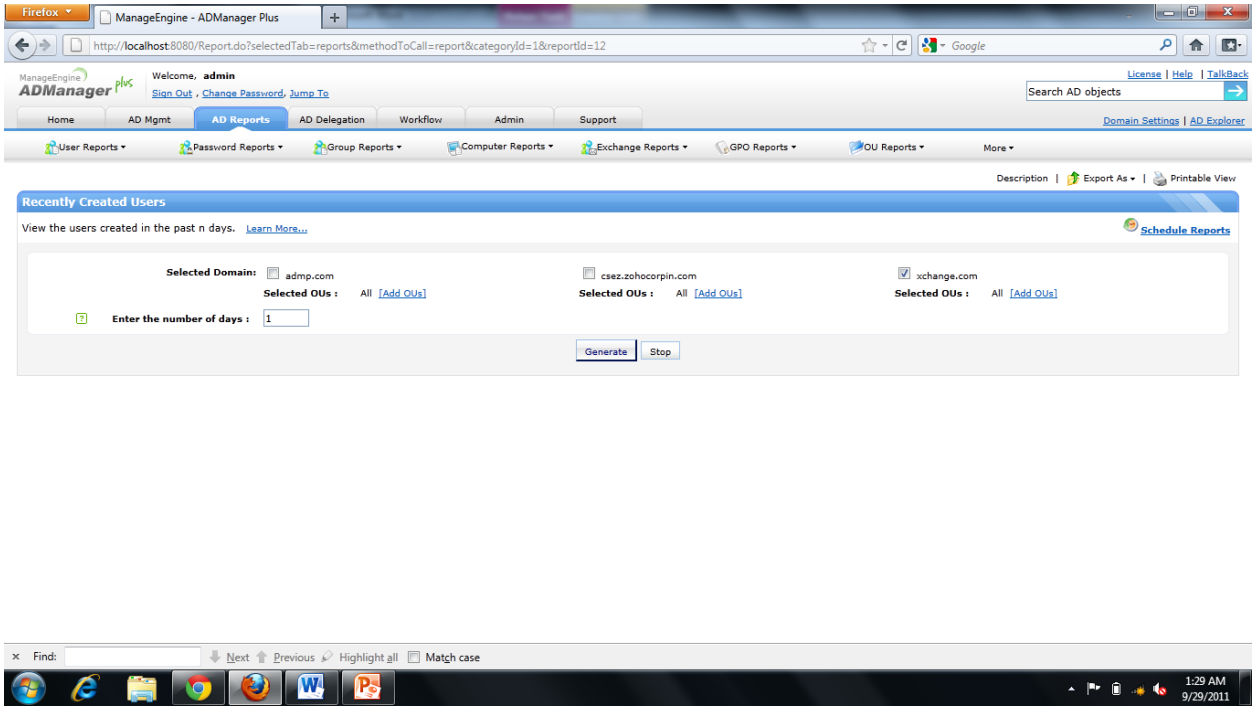
Granting AD Access to all users is not a secure move. By using ADManager Plus we can provide the product URL so that end users can use "Employee Search" to find fellow users/contacts without even logging into the product.

Exercise 7: Automatically send the list of users created in a day to the concerned person.

Objective: Generate a report of all the users who have been created in the day and send it to the concerned person on email in the required format. Also, this report has to be sent every day, automatically – that is, schedule this report to be generated and sent every day.

Steps:

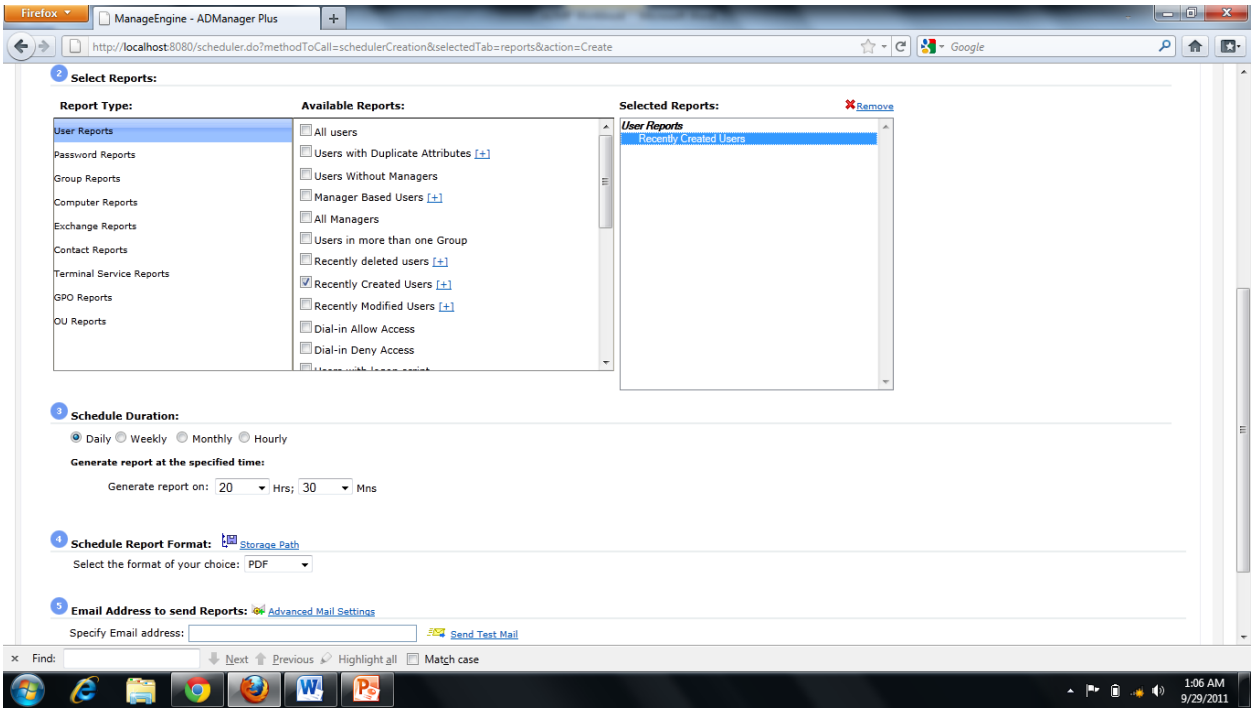
1. Click on 'AD Reports'
2. Click on 'User Reports' → 'General Reports' → 'Recently Created Users'



3. Select the 'Domain' and specify the 'OU(s)'.
4. Enter '1' in 'number of days'.
5. Click 'Generate' to get the list of all users who were created during that day.

Schedule this report to be generated and emailed every day to the concerned person.

6. Click on ‘Schedule Reports’
7. You will now see the list of all reports that have been scheduled.
8. Click on ‘Schedule New Reports’ to go to the ‘Schedule Report’ page.



9. Specify a name for this report in ‘Scheduler Name’
10. Select the ‘Domain’ and specify the OU(s).
11. In ‘Select Reports’ click on ‘User Reports’ in ‘Report Type’.
12. In ‘Available Reports’ click on ‘Recently Created Users’, enter ‘1’ in the ‘Enter no. of days’ field, click ‘OK’.
13. You will now see this report in the ‘Selected Reports’ column.
14. Select ‘Daily’ and mention the time at which the report has to be generated in the options under ‘Schedule Duration.
15. Specify the format in ‘Select the format of your choice’
16. Enter the email addresses to which the report has to be sent in the ‘email address to send reports’ field. More than one email address can be specified if you wish to send this report to more than one person.

Exercise 8: Generating Reports based on available attributes of users

Objective: To find out users having details with 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 an Active Directory. However, with ADManager Plus, we can make use of "Reports from CSV" and find out the user accounts using common fields like first name and last name and modify them in bulk.

Steps:

1. Go to ‘User Reports’ page in AD Reports

2. Click on ‘Reports from a CSV’

3. Choose the Domain Name which you want to generate the reports on

4. Import the CSV file which is provided by HR team or exported from a different tool or prepared by you.

5. Choose the Criteria to see the results.

6. Once the report gets generated we may add the required columns including schedule reports.

Exercise 9: Schedule reports for automatic data gathering and reporting.

Objective: To get notified upon creation or modification of a user account in the domain.

ADManager Plus offers a provision of manual scheduling of reports that can be configured to run at required intervals, and can also be emailed to specific users. So one can schedule 'recently created users' reports and 'recently modified users' reports and receive email notification about the modifications made.

6. On-the-fly Active Directory Management:

This section will throw more light on how the actionable, pre-built reports in ADManager Plus help the Active Directory administrators to take decisions based on the information in the reports.

For example, it is possible to find out all the users who have been inactive for more than a specific period and disable them or delete them.

This is not possible using the native Active Directory environment as there is no mechanism to list out all the users who have been inactive. Though writing scripts could be an option, it is a demanding and often tiring task as it requires great indepth knowledge of the intricacies of Active Directory.

ADManger Plus thus not only makes this difficult task easy but also allows you to do a variety of actions on the selected objects as per the need.

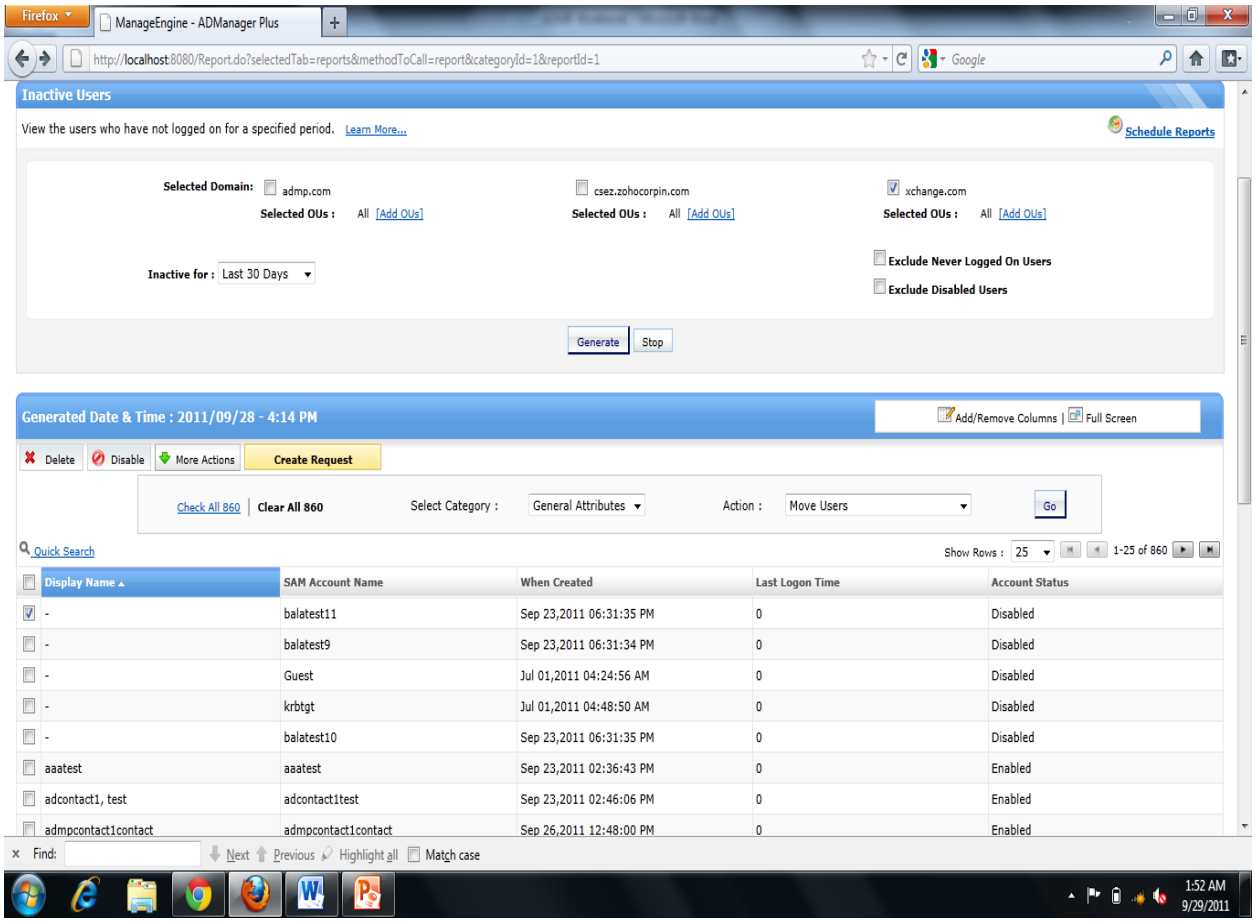
Exercise 1: Move Inactive Users

Objective: Find out all the users who have been inactive for the last 30 days and move them to a different OU.

Steps:

List all the users who have been inactive for the past 30 days.

1. Click on 'AD Reports'
2. Click on 'User Reports' → 'Logon Reports' → 'Inactive Users'

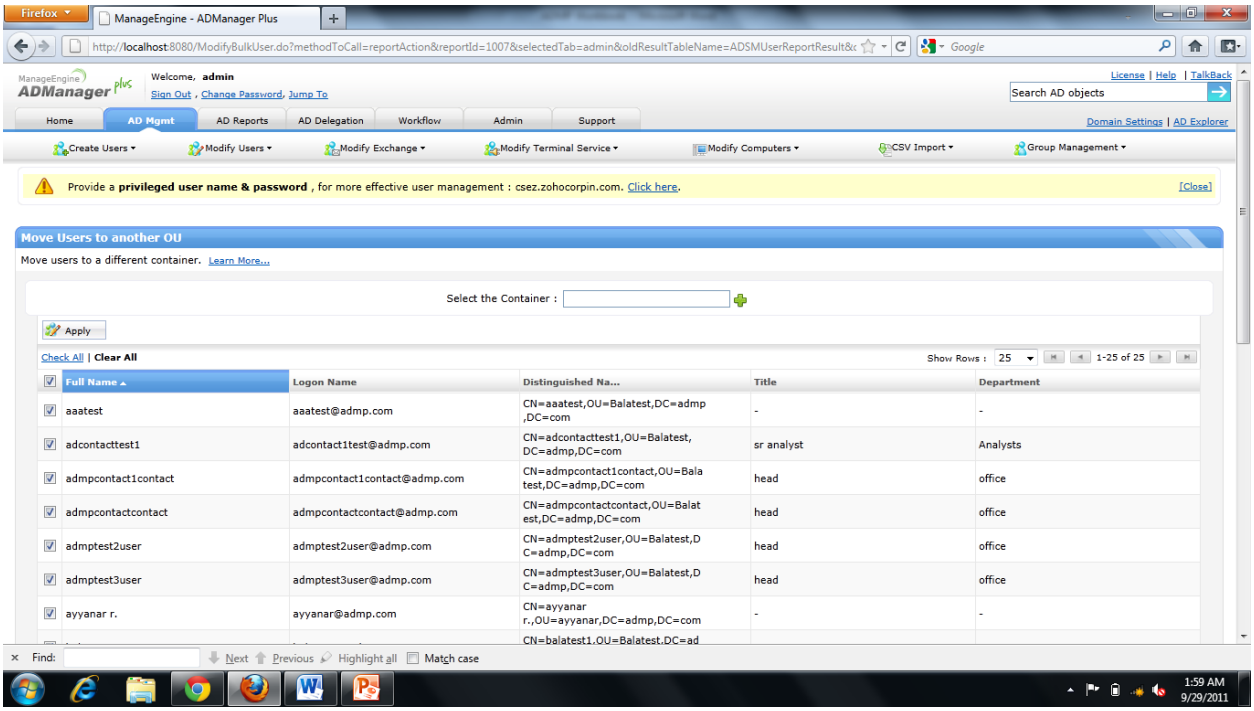


3. Select the 'Domain' and 'OU(s)' from where the inactive users have to be fetched.
4. Select 'Last 30 Days' in 'Inactive for' field, click 'Generate'. This will fetch all the users who have been inactive for the past 30 days.

Move the users to a different OU:

5. Click on ‘More Actions’ option above the report header.
6. In Select Category, choose ‘General Attributes’ → Action: ‘Move Users.

You will now be directed to the ‘Move Users to another OU’ page.



7. In ‘Select the Container’, specify the OU to which you would like to move the users.
8. Select all the users using the ‘Check All’ option. Click ‘Apply’ to move all the inactive users to another OU.

Exercise 2: Add all managers to the Domain Admins Group.

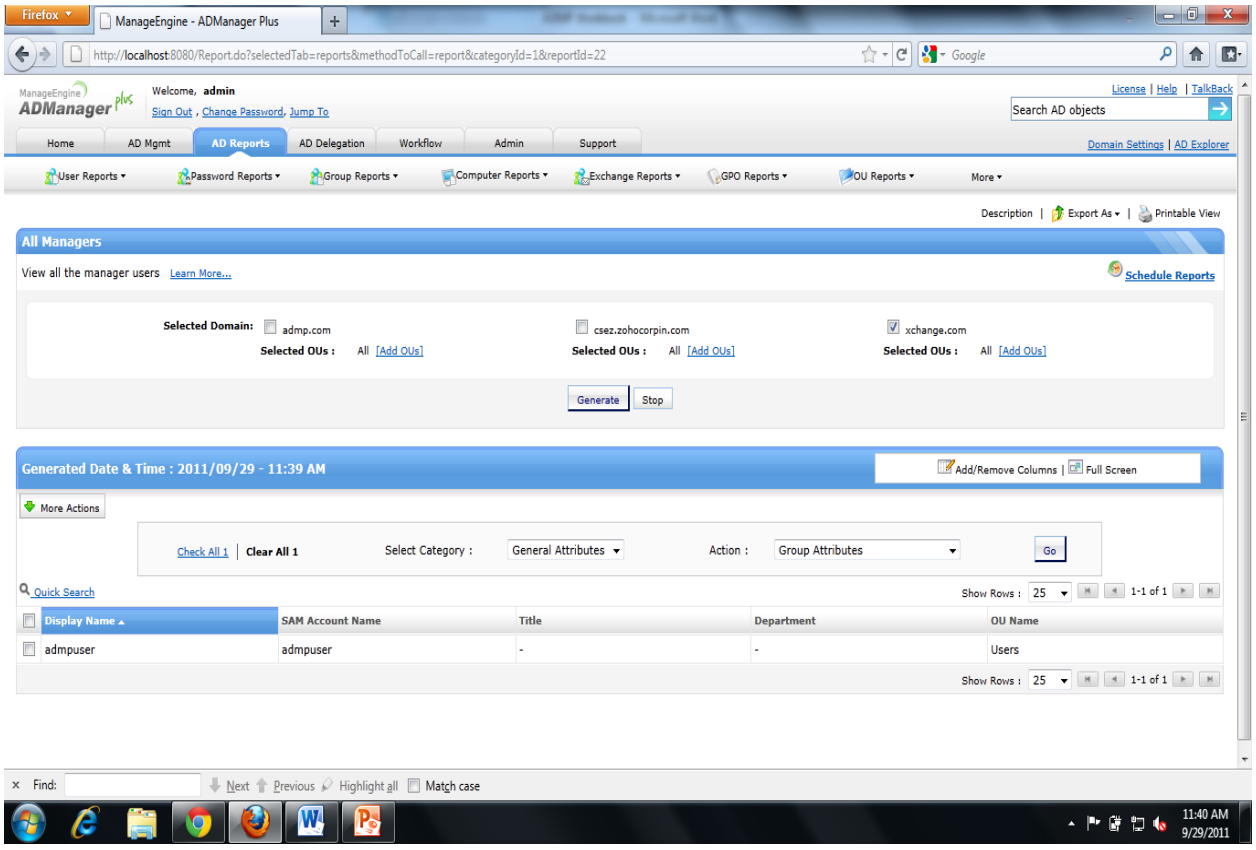
Objective: Generate a list of all the users who are managers and add them to the Domain Admins group.

Steps:

List all the managers:

1. Click on 'AD Reports'.
2. Click on 'User Reports' → 'General Reports' → 'All Managers'

   This will take you to the 'All Managers' page.

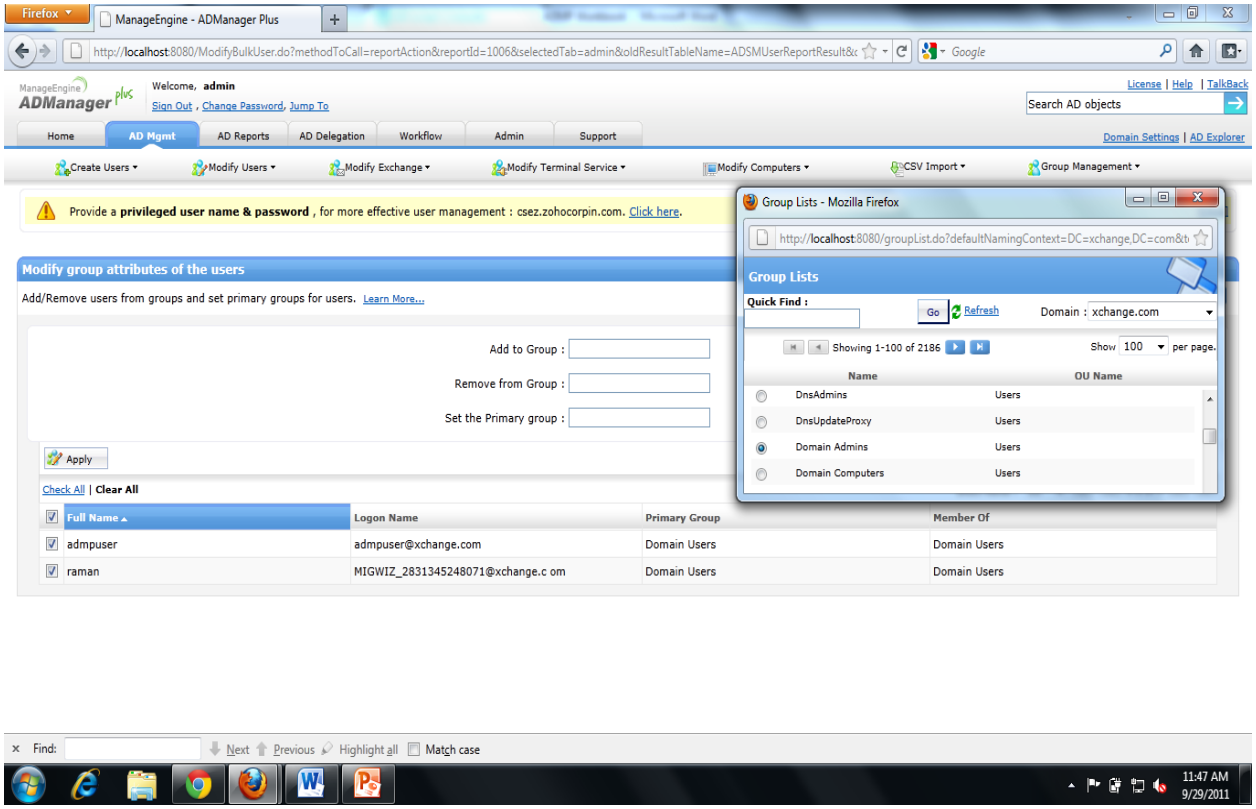


3. Select the 'Domain', 'OU(s)' from where to fetch all the managers.
4. Click 'Generate' to get the list of all the managers.

Add the managers to 'Domain Admins' group:

5. Click on 'More Actions' option above the report header.
6. In 'Select Category' select 'General Attributes' → 'Action': 'Group Attributes'. Click 'Go'.

You will now be in the ‘Modify Group Attributes of the Users’ page.



7. Click on ‘+’ beside the ‘Add to Groups’ option and select the ‘Domain Admins’ group.
8. Select all the users.
9. Click ‘Apply’ to make all the managers members of ‘Domain Admins’ group.

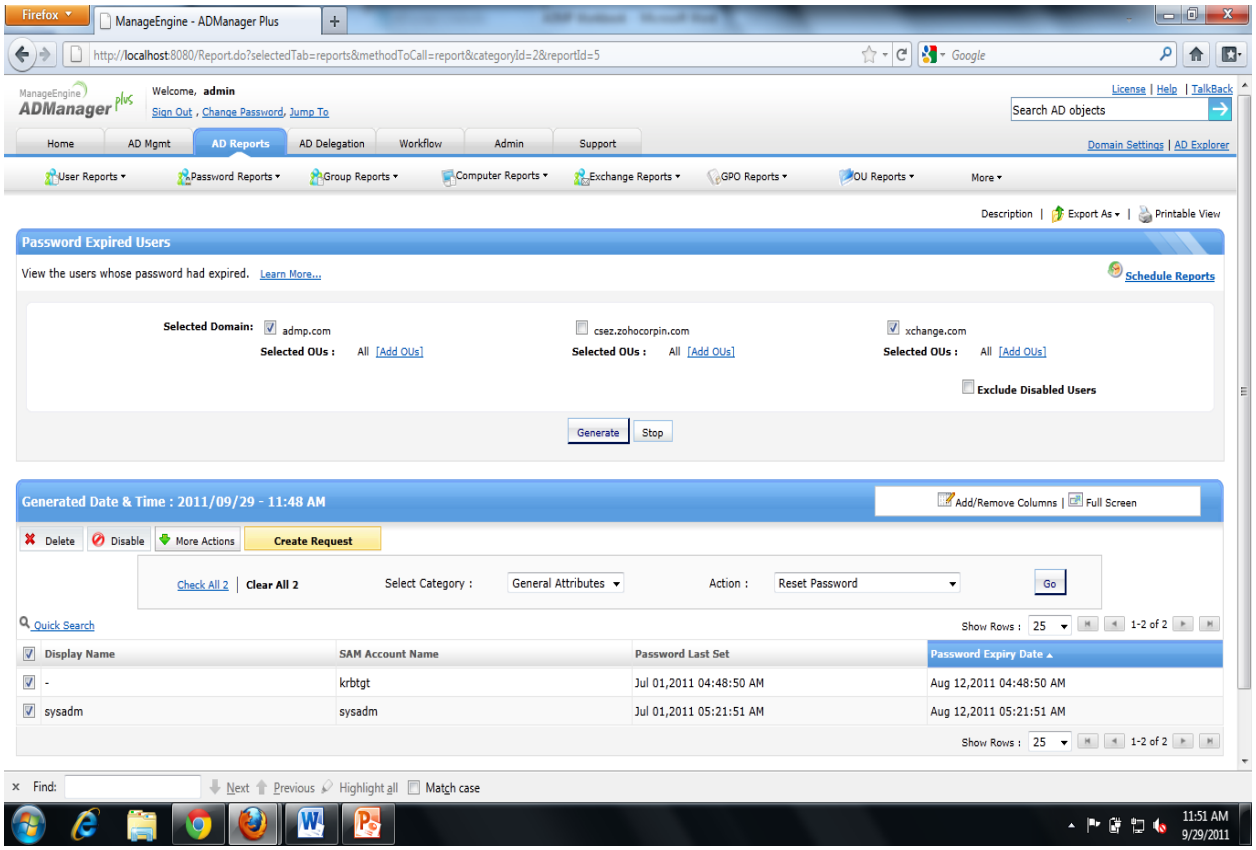
Exercise 3: Reset Password for all password expired users.

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

Steps:

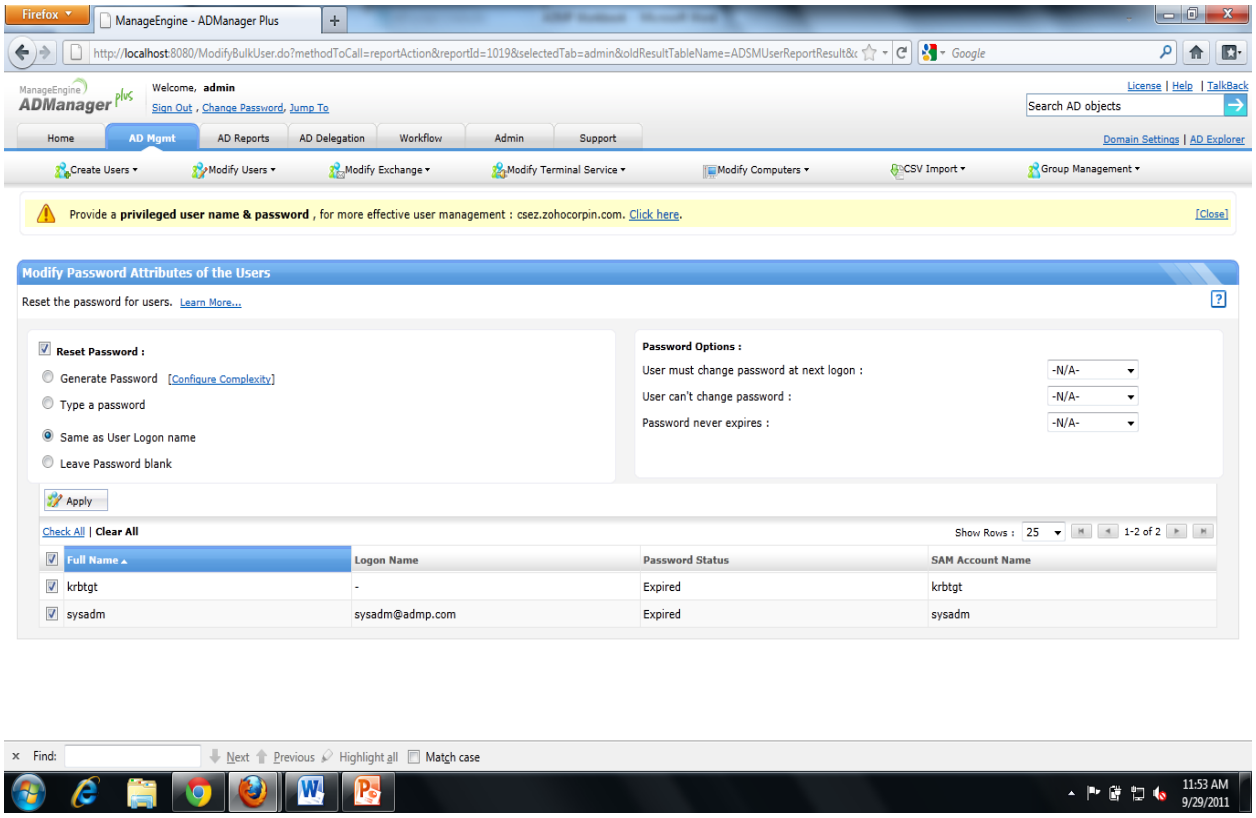
1. Click on 'AD Reports'.
2. Click on 'Password Reports' → 'Password Status Reports' → 'Password Expired Users'

You will be taken to the 'Password Expired Users' Report page.



3. Select the 'Domain', 'OU(s)' from which to fetch the password expired users.
4. Click 'Generate' to get the list of all password expire users.
5. Click 'More Actions' → 'Select Category: General Attributes' → 'Action: Reset Password'. Click 'Go'.

You will now see the 'Modify Password Attributes of the Users' page.



6. Select ‘Reset Password’ and select an option in ‘Reset Password’ section and also specify the Password Options for users.
7. Click ‘Apply’ to reset the password for all the users whose password has expired.

7. Active Directory Workflow

Most of the Active Directory tasks that an administrator has to do on a day-to-day basis are repetitive. It makes absolute sense to automate these recurring tasks. Automation is absolutely not supported in the native Active Directory environment and it is sheer headache to automate tasks using scripts.

ADManager Plus solves this issue through Workflow - controlled automation, where the required tasks can be initiated but completed or executed only after being approved by a specific authority.

Workflow, an ADManager Plus special, greatly reduces the burden of the Active Directory administrators as most of the mundane tasks are automated but still they can be at peace because no task can be completed without their knowledge and approval of the concerned authority.

There is also another feature called ‘Robo Requester’ that automatically raises the request for specific operation as required, like – request to disable inactive users, reset password for password about-to-expire users, etc.

This section will get you used to the Workflow and Robo Requester features.

Exercise 1: On the HR's approval the Administrato has to disable an user(s)

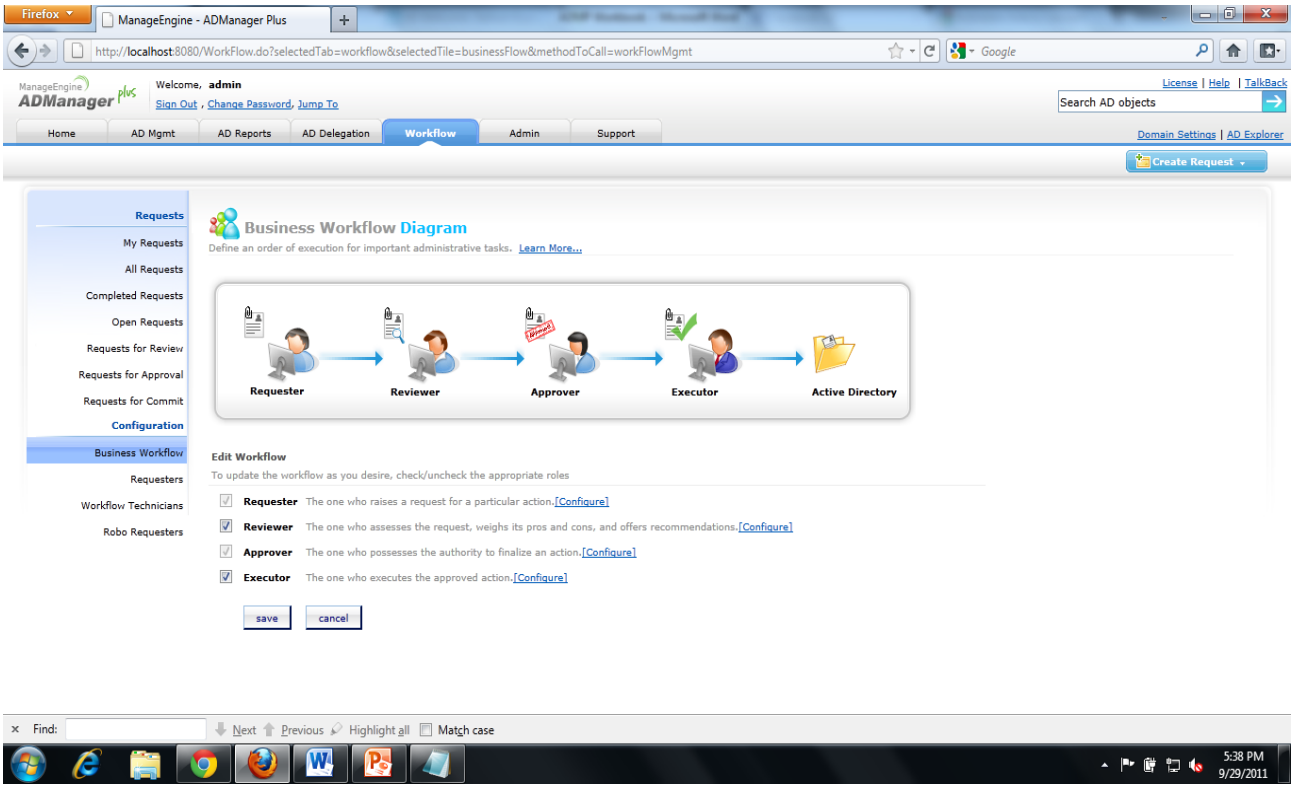
Objective: Raise a request to disable a user or a set of users. The request has to be sent to the HR Manager for approval. Once the approval happens, the Administrator has to disable the users.

This scenario is something that is totally impossible in the native Active Directory 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.

Creating Workflow:

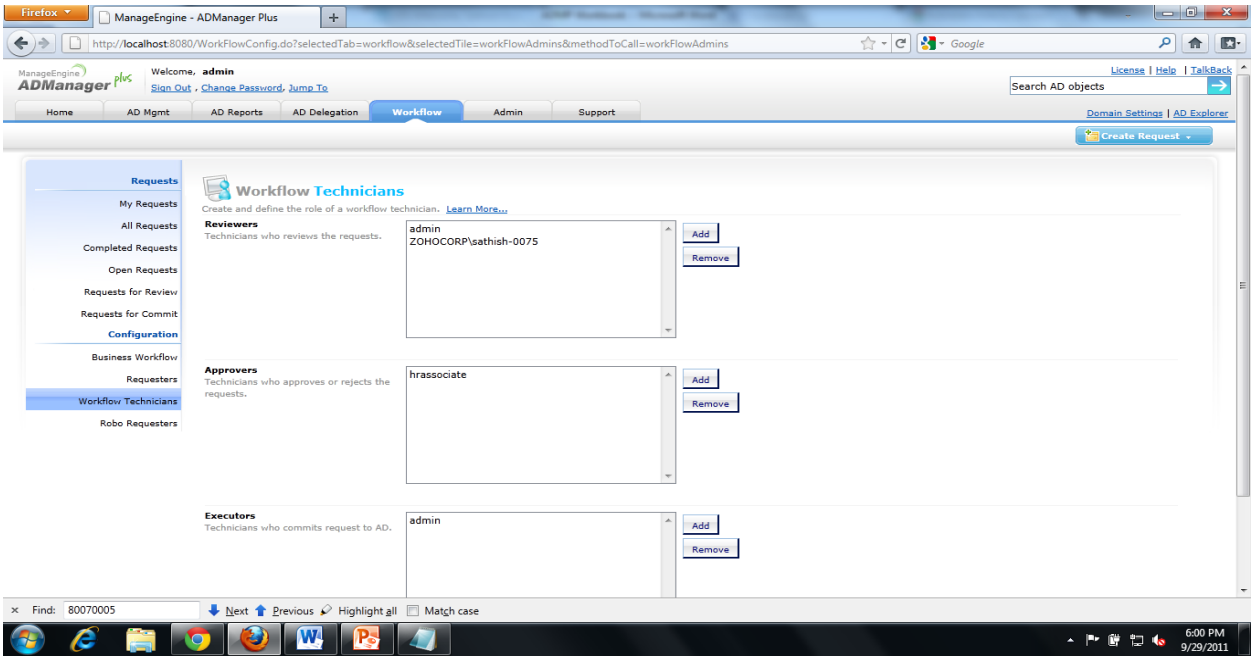
1. Click on 'Workflow' Tab.
2. Under 'Configuration', click → 'Business Workflow' → 'Edit Workflow'.



3. Configure the appropriate user for each of the workflow stages.
4. Requesters will be able to raise requests for tasks, reviewers review the request and provide their comments, based on the reviewers comments, the approver approves the execution of the task. Once the approval is obtained, the Executor executes the task.

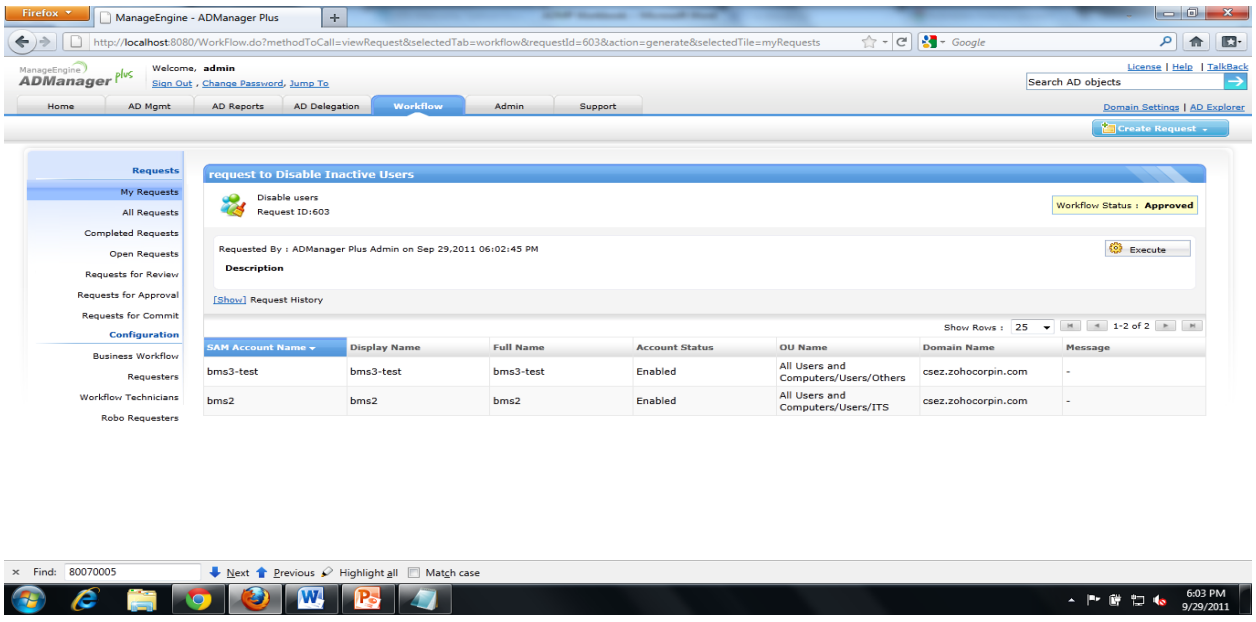
Click on 'configure' option in each line to specify users for these roles.

For our exercise, we have to configure ‘Administrator’ as Requester, ‘HR’ as the Approver, ‘Administrator’ as Executor.



To disable the inactive users after approval from the ‘HR’

5. Click on ‘AD Reports’ → ‘User Reports’ → ‘Inactive Users . Generate Inactive users report.
6. Select the required users and click on ‘Create Request’ → ‘Task’ – Disable Users.
7. The ‘HR’ – will see the requests in his requests list and review and approve it.
8. Since the administrator is not configured as approver, he cannot approve the request.
9. Once the ‘HR’ approves, the Administrator will execute the task by clicking on the request and clicking on ‘Execute’ button.



Exercise 2: Automated request for disabling inactive users.

Objective: Generate automatically, the request to disable inactive users, every month, on a specific day.

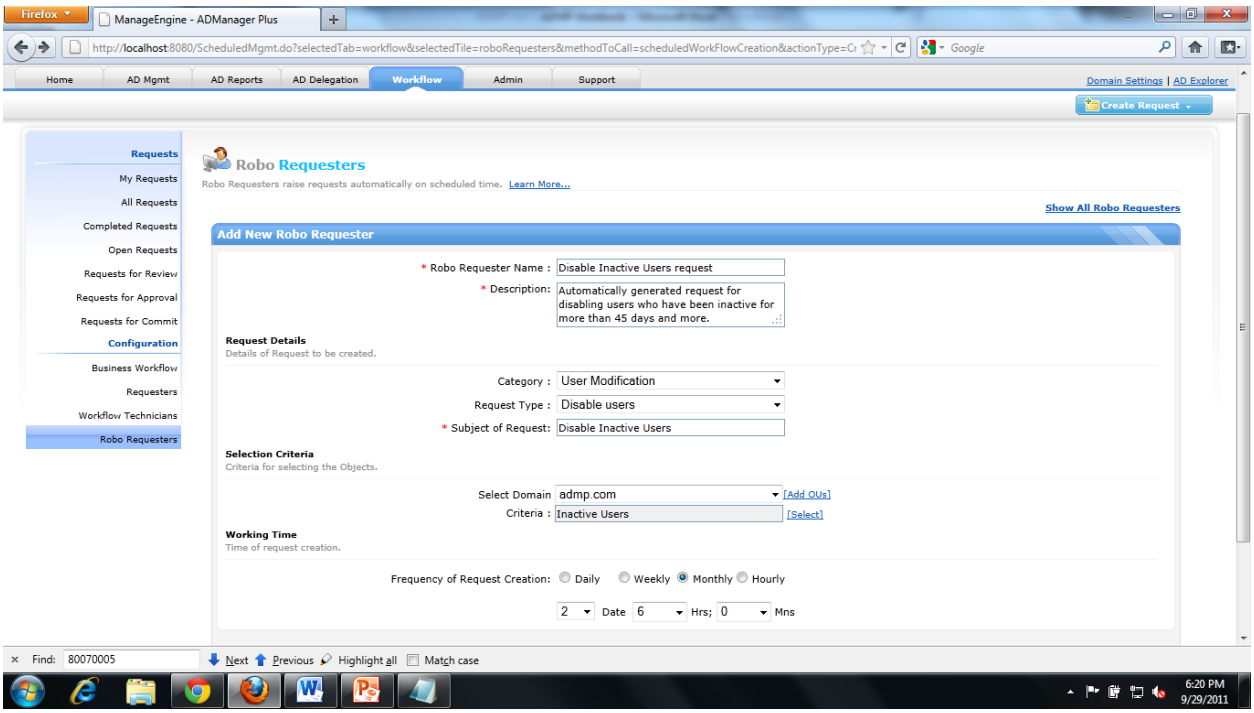
Administrators spend a lot of time in scouting for inactive users and then send the report to the concerned person for permission to take further action like disabling the user, deleting the user, etc.

This scenario cannot absolutely be automated using the native interface and also, writing scripts for these tasks and running them is an headache that every administrator hates.

The feature that will be helpful in this scenario is the 'Robo Requester'

Steps:

1. Click on 'Workflow' → 'Configuration' → 'Robo Requesters' → 'New Robo Requester'



2. Specify a name for the Robo Requester and describe the purpose of this requester.
3. Under 'Request Details' → 'Category: User Modification' → 'Request Type: Disable users'.
4. Enter a subject.
5. Select the 'Domain' and 'Criteria: Inactive Users'.
6. Specify the Frequency → 'Monthly' → Date and Time for raising this request.
7. 'Add' to save this request.

Exercise 3: Automated request to move computers.

Objective: Raise request to move inactive computers to a specific OU, every week.

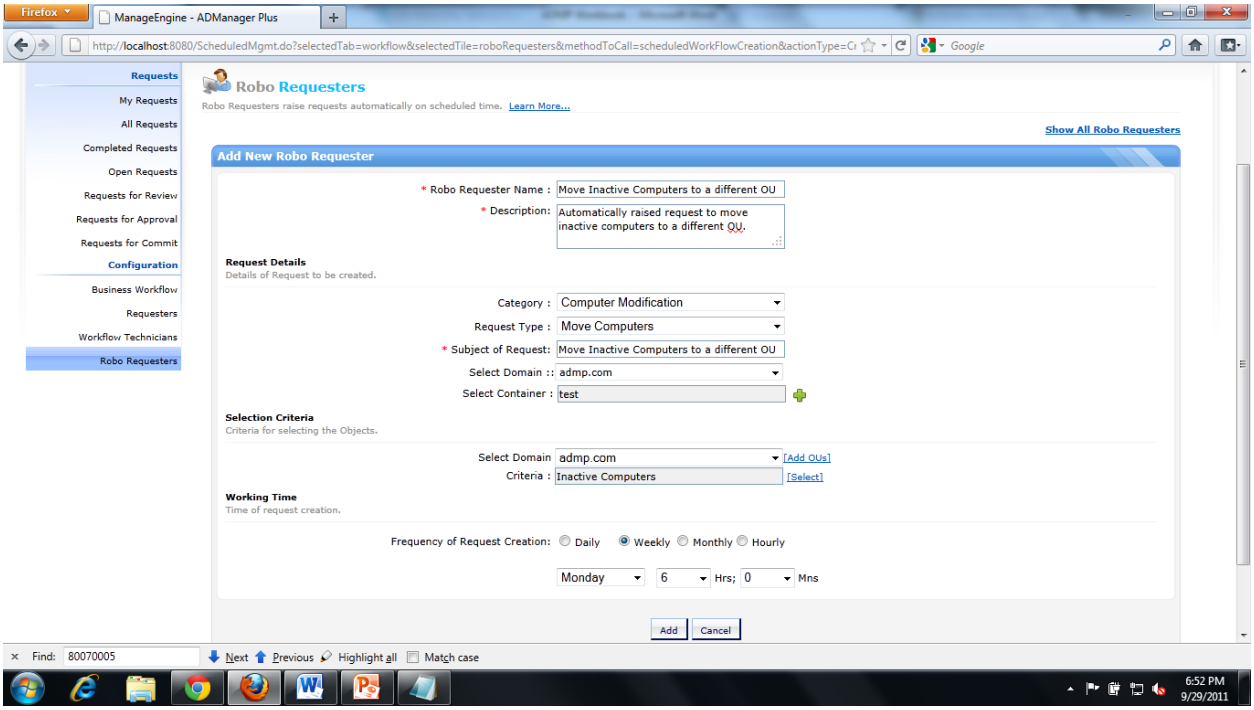
The Active Directory administrator has to frequently check for computers that are not being used and being idle and move them to a different OU so that there can be a track of computers that are available for user by users who do not have computers.

The native interface is helpless here and the scripts are also way too taxing and volatile to be depended upon.

ADManager Plus's Robo Requester will accomplish the task of raising the request to move the inactive computers and once the request is approved, the executor can execute the task of moving the computers as the request will be in the requests list of the approver and also the executor once it is approved. The administrator has to no longer do this ridiculously monotonous task again and again.

Steps:

1. Go to 'Add New Robo Requester' page.
2. Specify the Request Name, give a small description about the report.
3. Mention all the request details: Category, Request Type, Request Subject, Domain, Target container.
4. Specify the Selection Criteria: Domain from where to fetch the computers, Criteria.
5. Select the Frequency of request creation and the time for request creation.



Exercise 4: Automated request to reset the password for password soon-to-expire users.

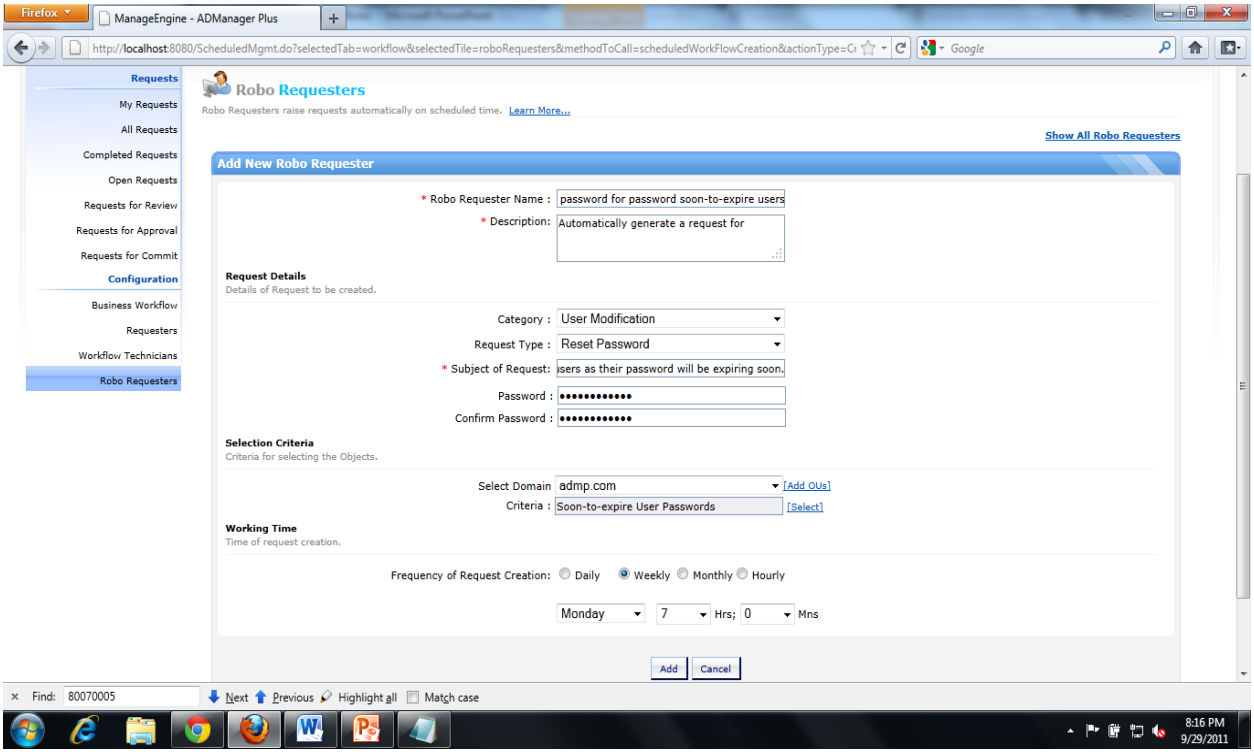
Objective: Find out the list of all users whose password will be expiring soon and then raise a request to reset their passwords.

With native interface, this will be virtually impossible as there is no option to raise a request for any specific task. Also, the password expiry date has to be checked for each user manually. The other option is to write scripts which need constant tweaking apart from the monumental task of writing the script.

With Robo Requester, this task becomes really simple and a request is automatically generated.

Steps:

1. Go to 'Add New Robo Requester' page.



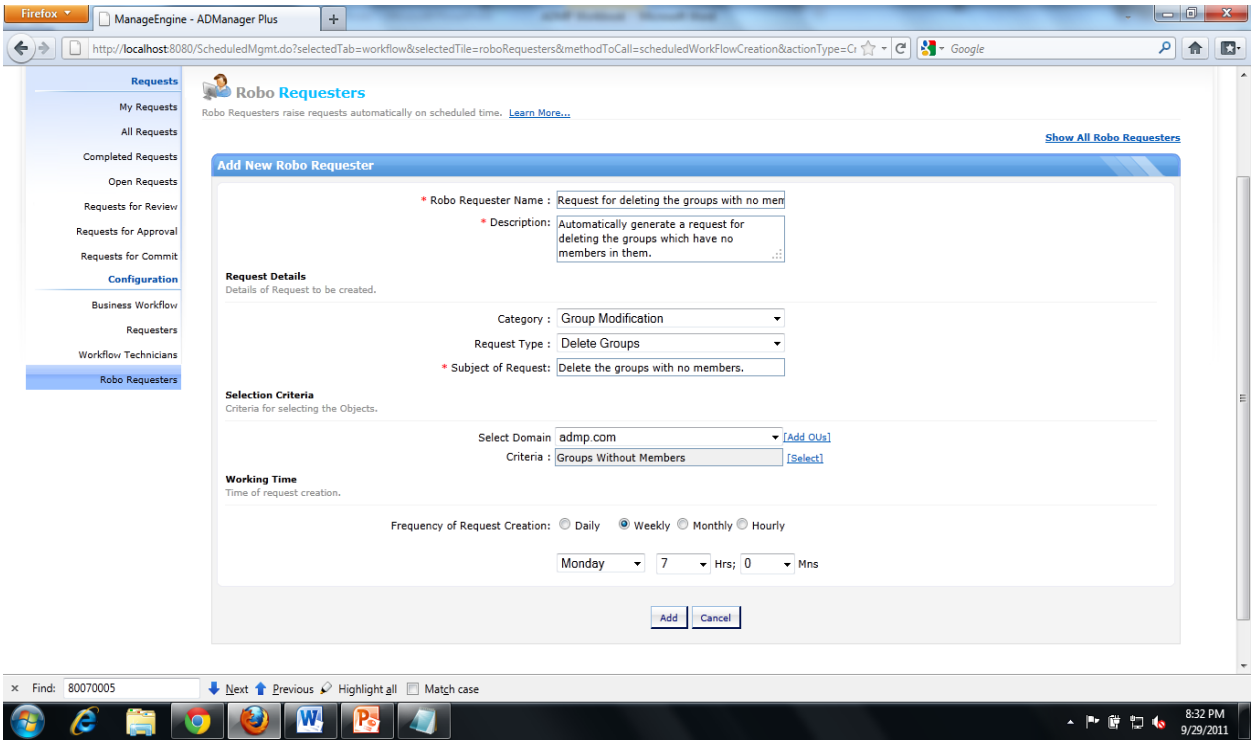
2. Mention a name for this request and also describe the purpose of the request.
3. In 'Requested Details', mention the following : 'Category: User Modification', 'Request Type: Reset Password', 'Subject of Request', New 'Password'.
4. In 'selection criteria', 'select the domain', 'Criteria: Soon-to-expire User Passwords'
5. In working time, choose 'weekly', mention the day and time for the request generation.
6. 'Add' to complete the process of creating this Robo Requester.

Exercise 5: Automated request to delete groups without members.

Objective: Find out the list of all the groups that do not have any members in them and then send a request automatically to delete these groups.

Steps:

1. Go to 'Add New Robo Requester' page.



2. Fill in all the required details in the Request Details.
3. In Selection Critera, choose – Group Modification (Category), Delete Groups (Request Type). and mention the subject.
4. Fill the required frequency and time for generating this request.
5. 'Add' to complete the creation of this robo requester.

Exercise 6: Workflow based User Accounts Creation

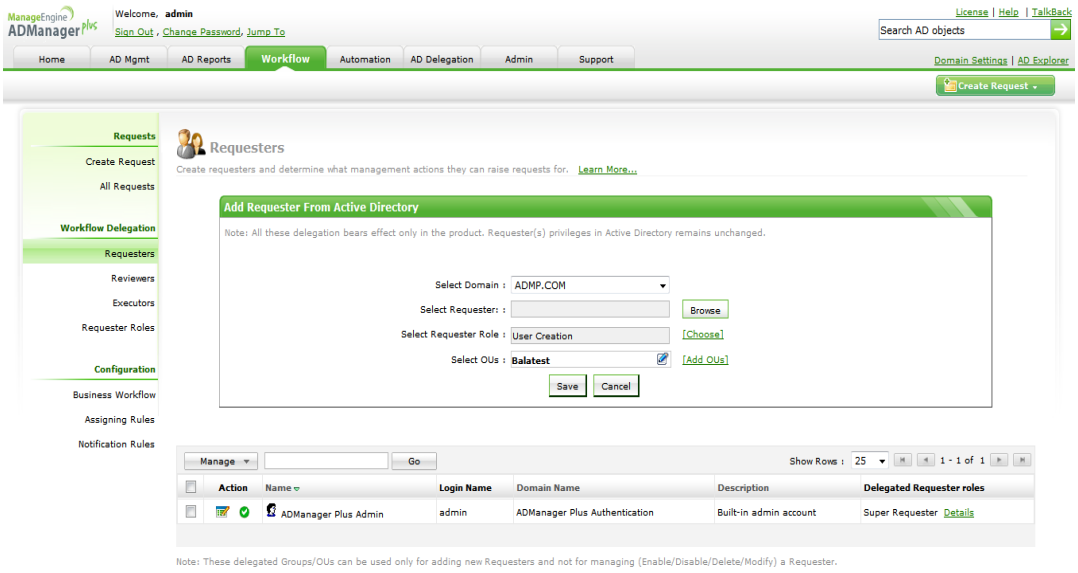
Scenario: Whenever new employees join the organization, the HR executives send the details of all new employees to their administrator to create new user accounts in their organizations domain. Instead of this, the HR executives should have the rights to key in the details of for all the new user accounts (for the new employees) to be created and just send a request to the concerned IT or helpdesk technician who can then create the new accounts with the details already entered.

You can accomplish this using the 'Workflow' feature by:

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

Steps to create users through the workflow:

1. Click on 'Workflow' → Configuration →Business Workflow → Edit Workflow.
2. Select the required levels (roles) in the workflow. For our case, let us choose Requester and Executor.
3. Save the workflow.
4. To assign the requester role to HR executives:



   a. Go to 'Workflow Delegation' →Requesters.
   b. Select the domain in which you would like to create this requester.
   c. Click on 'Browse' beside the 'Select requester' option and select the appropriate HR executive to whom you wish to assign the 'requester' role.

You can assign to individual Users or even Groups and OUs as a whole. Whenever a user is added to an OU or Group with the requester permission, the user automatically gets the required permissions to raise user creation requests.

d. In 'Select Requester Role', choose 'User Creation'.
e. Select the OUs in which the HR executive can raise user creation requests using the 'Add OUs' option.
f. 'Save' this requester.

5. To create 'executors' who can create new user accounts in AD:
    a. Go to 'Workflow Delegation' → Executors.
    b. Click on 'Add' and select the required technicians from the list of all available technicians in the domain. Click OK to add the selected technicians to 'Executors' list.
6. To raise a request for new user account creation:
    a. The requestor has to login to ADManager Plus.
    b. Click on 'Workflow' → Requests → Create Request
    c. In 'User Creation', select 'Single User Creation' or 'Bulk User Creation' based on your requirement.
    d. Single User Creation:
        i. Select the Domain in which the user account has to be created.
        ii. Choose the appropriate template.
        iii. Enter the values for all the necessary attributes.
        iv. Click on 'Create Request' to complete the request creation process.
    e. Bulk user Creation:
        i. Select the required Domain.
        ii. Choose the appropriate template.
        iii. User 'Add Users' 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'.
        iv. Select the required 'Container' or create a new container (OU) if required.
        v. Click on 'Create Request' to complete the user creation request.
7. To execute (create) the user creation request
    a. The technician with the 'execute' role has to login to ADManager Plus.
    b. Click on 'Workflow' → Requests → All Requests.
    c. In the requests list, go to 'My Requests' →'Awaiting for Execution' to view the list of all requests waiting for execution. (You can also click on the number displayed in 'Awaiting for Execution' located just above the list of requests to view all tasks queued up for execution).
    d. Select the 'user creation' task raised by the HR executive.
    e. Execute this task to complete the process of creating new users in AD.

Exercise 7: 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:

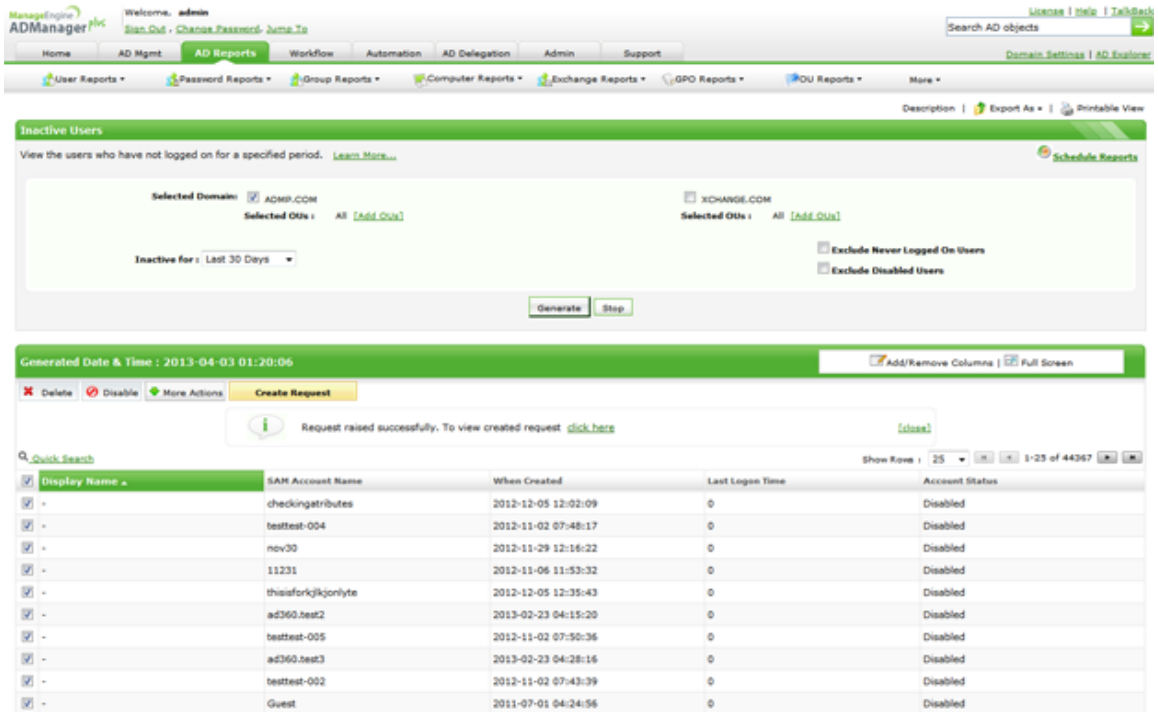
- Creating a 3 level workflow with: Requester, Reviewer and Executor.
- Add the appropriate users/technicians to the Requester, Reviewer and Executor roles.
- Once the requester creates the request to disable user accounts, the reviewer verifies the users list and approves it. Then, the executor can 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. Create a customized workflow.
    a. Click on 'Workflow' → Configuration →Business Workflow → Edit Workflow.
    b. Select the required levels (roles) in the workflow. For our case, choose the Requester, Reviewer and Executor.
    c. Save the workflow.
2. To add requesters:
    a. Go to 'Workflow Delegation' →Requesters.
    b. Select the domain in which you would like to create this requester.
    c. Click on 'Browse' beside the 'Select requester' option and select the appropriate technician or user to whom you wish to assign the 'requester' role.
    Assigning the requester role to Groups and OUs as a whole grants the permission to all the users in those OUs/Groups to create requests for the specified tasks.
    d. In 'Select Requester Role', choose 'User Creation'.
    e. Select the OUs in which the technicians can raise 'disable user' requests using the 'Add OUs' option.
    f. 'Save' this requester.
3. To add reviewers:
    a. Go to 'Workflow Delegation' → Reviewers.
    b. Click on 'Add' and select the appropriate HR users (Manager/Sr. Executives) from the list of all available technicians in the domain.
    c. Click OK to add the selected technicians to the 'Reviewers' list.
4. To add Executors:
    a. Go to 'Workflow Delegation' → Executors.

b. Click on ‘Add’ and select the required technicians list of all available technicians in the domain.
c. Click OK to add the selected technicians to the ‘Executors’ list.

5. Create Assign Rules to assign the requests to appropriate users/technicians after creation and review:
   a. Click on Workflow → Assigning Rules
   b. Click ‘When request is created’ link →Add New Rule
   c. Specify a name for the rule: Disable Inactive Users
   d. In Rule Criteria: Requests → Action; condition: Is
   e. ‘Choose’ Disable Users from the list of actions.
   f. In ‘Perform Action’, Assign To: Choose the HR Manager/appropriate technician.
   g. Set Priority as Normal (since this is a routine task) and ‘Save’ this assignment rule for request creation.
   h. Similarly, create an assignment rule in ‘When request is reviewed’ section by choosing ‘Disable Users’ as action and specifying the appropriate technician in ‘Assign To’. Name this rule also as ‘Disable Inactive Users’.
6. To create the ‘disable user’ request:



   a. The technician has to login to ADManager Plus.
   b. Click on ‘AD Reports’ → ‘User Reports’ → ‘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’→ ’Disable Users’ in Request Action.

e. Enter the subject and description and ‘
   Now, based on the ‘Disable Inactive Users’ assignment rule for requests created, it will be assigned to the appropriate technician (HR Manger / Executive).

7. To review the ‘Disable User’ request:
   a. The HR Manager/Executive (with reviewer role) has to login to ADManager Plus
   b. Click on ‘Workflow’ → Requests → All Requests.
   c. In the requests list, go to ‘My Requests’ →’Awaiting for Review’ to view the list of all requests waiting for review. (You can also click on the number displayed in ‘Awaiting for Review’ located just above the list of requests to view all tasks queued up for review).
   d. Select the ‘disable inactive users’ task.
   e. ‘Review’ this task and click on ‘review’ button to approve this request. (If you are not ok with the list of users or need any changes, click on ‘Reject’).
      Now, based on the assignment rule for reviewed requests, the task will be assigned to the appropriate IT administration/technician.

8. To execute (create) the user creation request
   a. The technician with the ‘execute’ role has to login to ADManager Plus.
   b. Click on ‘Workflow’ → Requests → All Requests.
   c. In the requests list, go to ‘My Requests’ →’Awaiting for Execution’ to view the list of all requests waiting for execution. (You can also click on the number displayed in ‘Awaiting for Execution’ located just above the list of requests to view all tasks queued up for execution).
   d. Select the ‘disable inactive users’ task raised by the HR executive.
   e. ‘Execute’ this task to complete the process of disabling inactive users in AD.

8. Active Directory Automation

This feature helps you to automate any Active Directory management task. You can automate not just a single task but also a sequence of Active Directory management tasks which will be performed in the specified order and also at the specified time frame through this feature's 'Automation Policy'.

For example, you can automate the complete User account lifecycle management process using this automation. That is, you can create user accounts and check for inactive user accounts among them after a specific period of time to move them to a new location after which you can choose to disable and/or delete the inactive user accounts at a pre-determined time frame.

ADManager Plus's offer two important components to automate user account management namely 'Automation' and 'Automation Policy'. The following exercises will help you understand the usage and benefits of these two components.

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 users/technicians. Refer 'Active Directory Workflow' section to know more.

Exercise 1: Automated unlocking of user accounts every morning at a specified time.

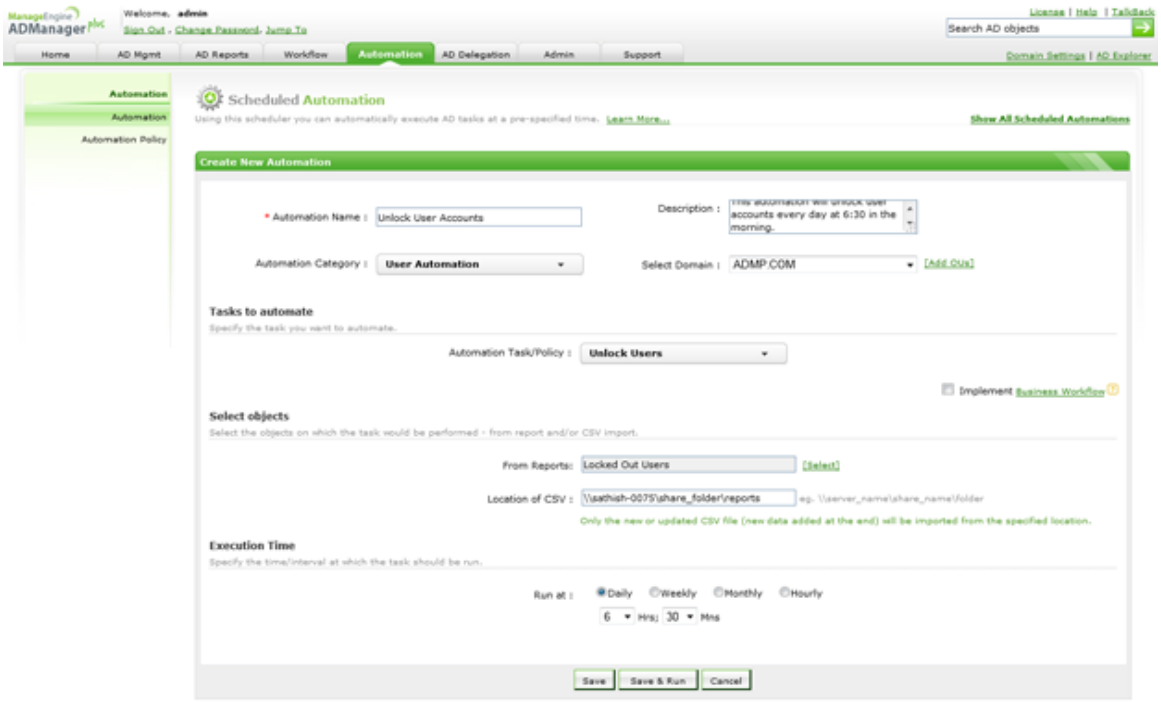
Scenario: One of your mandatory everyday tasks is to fetch the list of all locked out user accounts in you organization and unlock them one after the other. Immaterial of the number of locked out user accounts, be it a few or many, you have to complete this task sufficiently early so that users are not forced to wait for you to unlock their accounts which could affect the productivity of your organization.

'Automation' helps you to unlock all the locked out user accounts every day, without any human intervention. You can use automatically unlock all the locked our user accounts by:

- Creating an automated task or automation to fetch the list of all locked out user accounts in your Active Directory and unlock them all, at one go.
- Specify a time at which you would need this task to be performed, every day.

Steps to automate the task of unlocking locked out user accounts:

1. Click on 'Automation' tab.
2. In the left pane, click on Automation from the available options. This will open up the 'Create New Automation' pane.



3. Enter 'Unlock User Accounts' in 'Automation Name'
4. In Automation Category, select 'User Automation'.

5. Select the domain in which the user accounts to be unlocked are located.
   (You can also restrict the unlock users task to only specific OUs. Click on 'Add OUs' link to specify the required OUs.)
6. In 'tasks to automate' →Automation Task/Policy → Select 'Unlock Users'.
7. In 'Select Objects', you can specify the list of user accounts to be unlocked in the form of either a report or a CSV file or both.
   a. From Reports: Click on 'Select' link and select the required report. For this scenario, select 'Locked Out Users' report from the reports list.
   b. Location of CSV: Specify the location of the file in which the user accounts are specified in this option.
8. Specify the time at which the user accounts have to be unlocked using the options in 'Execution Time'. Since the 'unlock users' operation has to be performed every day, in 'Run at', select Daily and specify a time that matches your requirement, say 6 Hours 30 Minutes to unlock all locked our user accounts every day at 6:30 in the morning.
9. 'Save' this automation to schedule the unlock operation for 6:00 am every day.
10. 'Save & Run' to schedule the unlock users task for 6:30 every morning besides unlocking all the user accounts that are locked out at the time of saving this automation.

Exercise 2: Automate Inactive Users Cleanup process

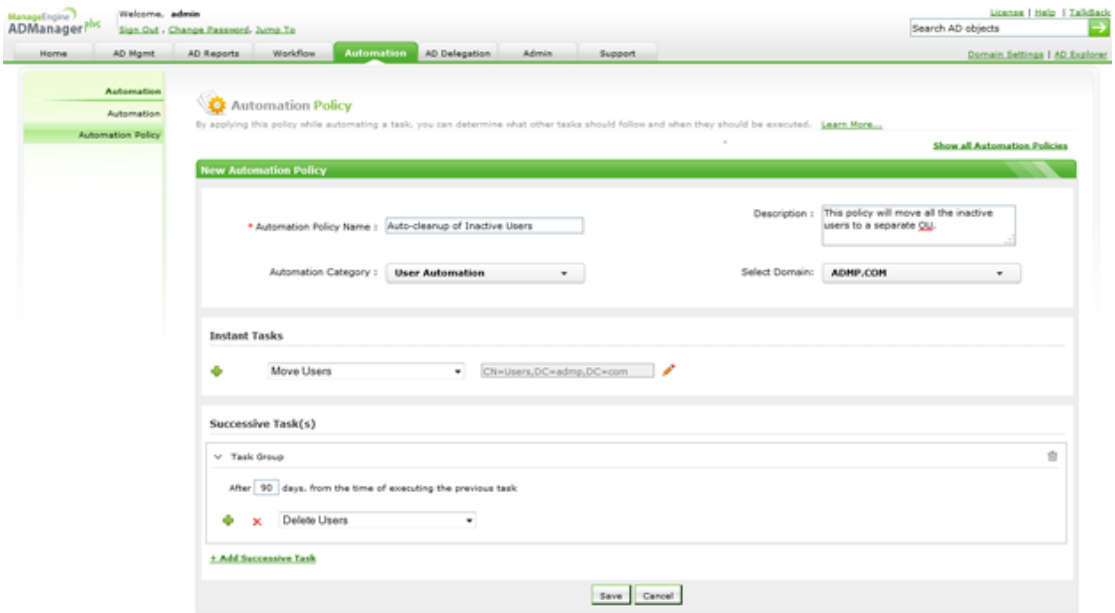
Scenario: As per your organizational policies, you will have to fetch and move all the inactive user accounts to a specific OU at the end of every month. 90 days after that, these users have to be deleted from your Active Directory. Automate the task of moving inactive user accounts from the present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

You can you 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 fetch the inactive users.
- Specify the frequency at which this automation has to be executed

Steps to automate moving inactive user accounts to a separate OU and delete them after 90 days

1. Click on Automation tab.
2. From the options under in LHS pane, click on Automation Policy.
3. To create a new policy



   a. Click on 'Create New Automation Policy' link.
   b. Enter a name for the automation policy. For this case let us use 'Inactive User Cleanup'.
   c. Select the Domain in which this automation policy will be used.
   d. In 'Instant Tasks' select 'Move Users' from task list.

e. Select the target OU (to which the inactive users will be moved).
f. In 'Successive Task(s):
    i. Specify a name for this task by click on 'Task Group'. Let us name this task as 'Delete Inactive Users'.
    ii. Enter 90 in the text box for days.
    iii. Select 'Delete Users' from the task list.
g. 'Save' this automation policy.

4. To create a new automation:
    a. Select Automation from the LHS pane.
    b. Click on 'Create New Automation' link.
    c. Key in the 'Automation Name'. For this case let us use: Move and Delete Inactive Users.
    d. In 'Tasks To Automate' → 'Automation Task/Policy' → Select Automation Policy →select the 'Inactive Users Cleanup' policy that we have already created.
    e. Specify the user accounts to be deleted in the form of either a report or a CSV file or both in the 'Select Objects' section.
        a. From Reports: Click on 'Select' link and select the required report. For this scenario, select 'Locked Out Users' report from the reports list.
        b. Location of CSV: Specify the location of the file in which the user accounts are specified in this option.
    f. In 'Execution Time' set the frequency at which you wish to run this automation. For our case, we will choose 'Monthly', Date: 1, Hours: 6 and Minutes: 30 to run this automation at 6:30 in the morning on the first day of every month.
5. 'Save' this automation to schedule the inactive user cleanup for 6:30 am on the 1st of every month.
6. 'Save & Run' to schedule this task for 6:30 on the first morning of every month besides moving all the inactive users at the time of saving this automation, to the specified target OU.

Exercise 3: Modify location specific user attributes using Automation Policy.

Scenario: When employees are moved to a different department changing the Group Membership and moving them to different OU's

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 may Add / Remove Group membership and Move the users to different OUs.

Exercise 4: 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.

In AD Manager Plus these service requests can be written into a CSV file and then the relevant attributes can be modified for the particular account to allow VPN. This process of granting access can also be automated by configuring a run once every 30 minutes.

Exercise 5: 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). The exercise is intended to grant specific privileges to the students so that they can gain access to certain network shares containing relevant study materials.

Solution: This can be achieved through Automation. In the 'Automation Policy' link, admins can add and remove users over a configurable period of time. The list of users is provided in a CSV file or even can be fetched through 'Enabled Users' report in 'User Reports' tab.

9. Non-Invasive Active Directory Delegation

Active Directory administrators are always kept on their toes; they are burdened with an almost never ending list of tasks that they have to perform, day in and day out. But most the tasks that eat into their time and take away a major chunk of their effort are repetitive simple tasks like password reset, unlock users, etc.

Active Directory administrators most often have to struggle between completing these 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 associated with it, the Active Directory security could so easily be compromised or just a small careless mistake could send the entire Active Directory for a toss.

The best option now is to have a mechanism that will allow non-administrators to take of the simple, repetitive task yet, prevent them from making any changes to the Active Directory set up. It is this simple but powerful and very useful option that ADManager Plus brings to the table – ADManager Plus's Non-Invasive delegation make the world of every Active Directory administrator a less stressful and pleasant one.

This section will familiarize you with the AD Delegation features of ADManager Plus.

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

Delegate crucial AD tasks to Level 1 technicians but with limited privileges, that is, the power carry out only the specified tasks and nothing else as the stability of Active Directory is of utmost importance.

Objective: Create a new 'Help Desk Role' and a 'Help Desk Technician'.

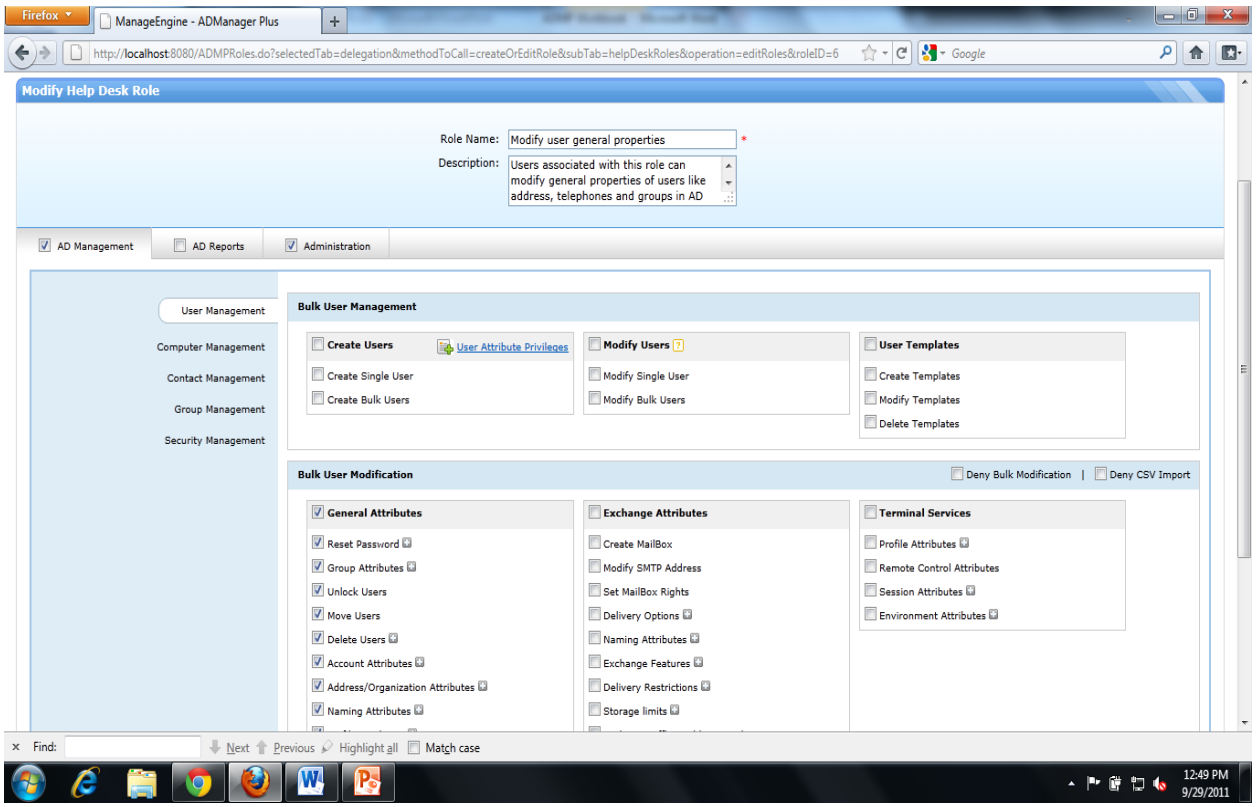
Help Desk Roles:

This feature allows you to specify the roles that you would like to delegate to the junior level technicians.

Create a new 'Help Desk Role'

1. Click on 'AD Delegation'.
2. Click on 'Help Desk Delegation' → 'Help Desk Roles' → 'Create New Roles'.

You are now on the 'Create Help Desk Role' page.



3. Specify a name for this new role.
4. Select the activities that you would like to delegate through this role – AD Management, Reporting or Administration.
5. Select the tasks and attributes changes that you wish this role to do.
6. 'Save Role' to save this new role.

The image in the previous page shows the role of 'Modify Users General Properties' and all the tasks that this role can perform. You can see that only those tasks that modify the general attributes alone have been selected and hence the help desk technician will be not be able to do other tasks like creation, modification of users, templates, modify exchange attributes, etc.

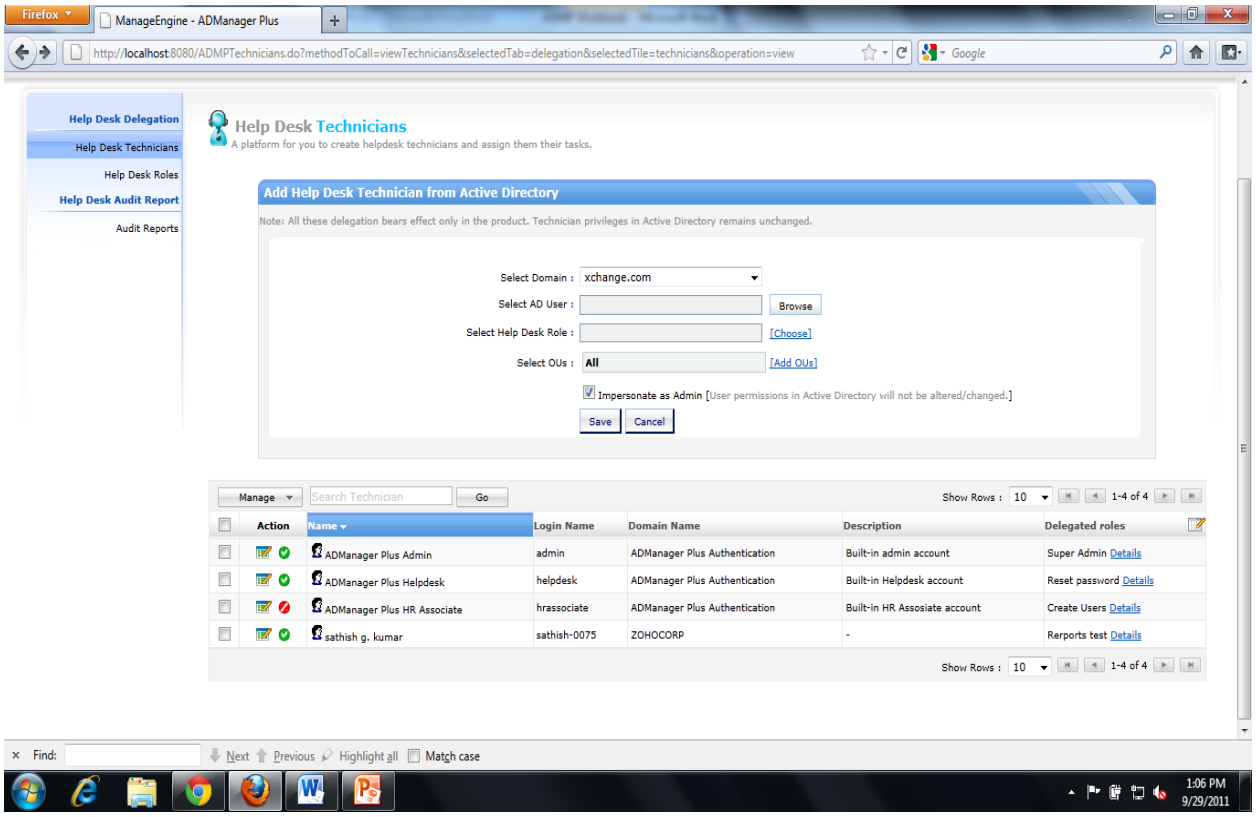
Help Desk Technicians

Help Desk Technicians are non-administrative users who have been permitted to perform specific administrative, management or reporting tasks that are usually performed by the administrators. Help Desk Technicians can only perform those tasks that they have been allowed to and cannot perform any other tasks or make any changes in the Active Directory.

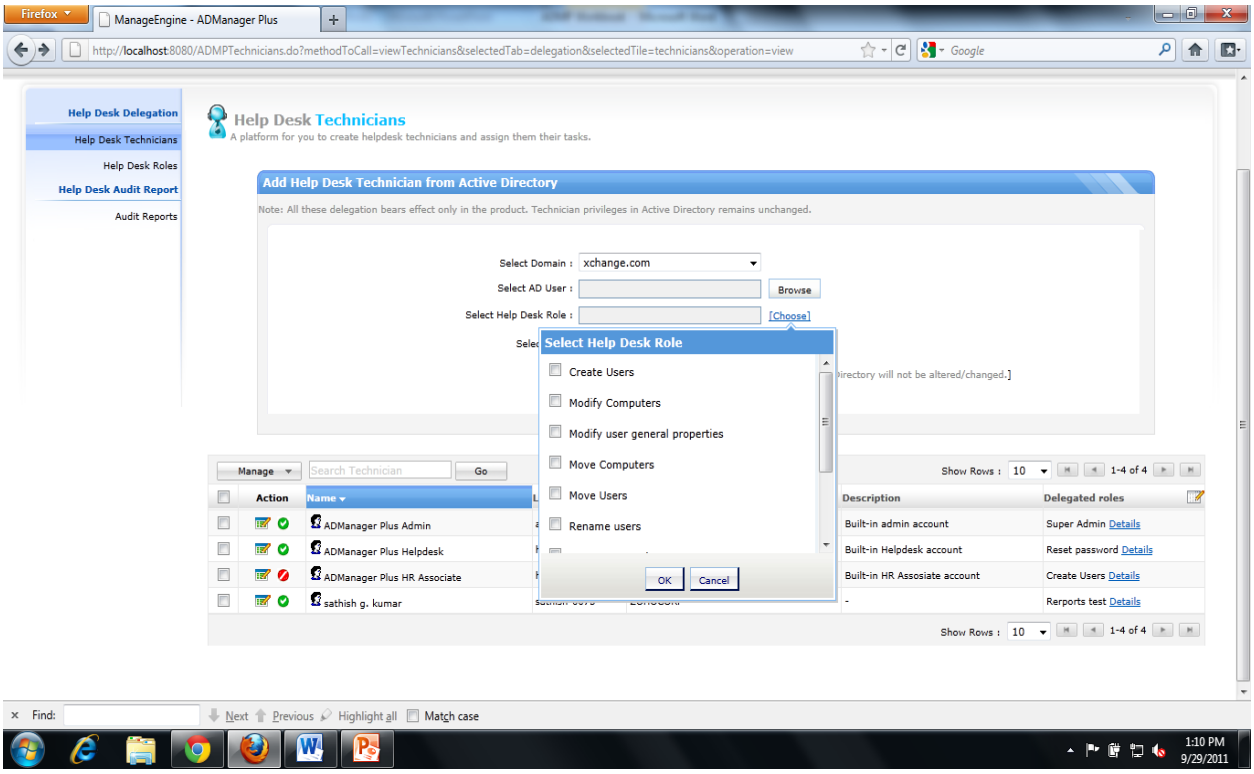
Create a new Help Desk Technician:

1. Click on 'AD Delegation'.
2. Click on 'Help Desk Delegation' → 'Help Desk Technician → ' Add New Technician'

You will now be viewing the 'Help Desk Technicians' page.



3. Select the 'Domain' in which you would like to delegate tasks to the Help Desk Technician.
4. Click 'Browse' to select the user to whom you would like to delegate the tasks.
5. Click 'Choose' to select the role that you would like this 'Help Desk Technician' to perform.



6. Select the roles and click ‘OK’.
7. Specify the OU(s) in which this ‘Help Desk Technician’ can perform the delegated tasks.
8. Click ‘Save’ to create this ‘Help Desk Technician’.

Exercise 2: Delegate Password Reset task.

Objective: Create a Help Desk Technician and assign only the role of resetting the passwords for users.

Steps:

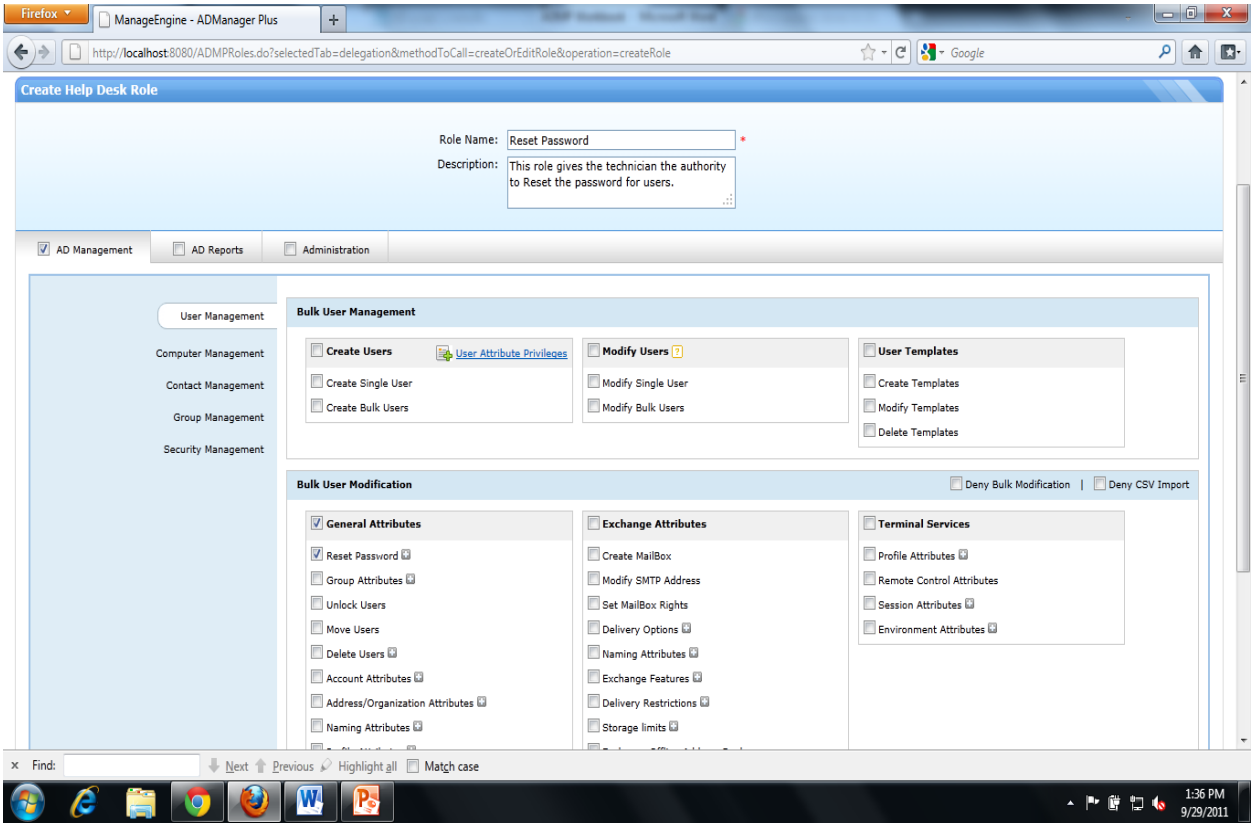
Create the 'Password Reset Role'

The tasks to be delegated have to be specified in the form of roles which can then be assigned to selected users. So before we can assign the 'Reset Password' task to a 'Help Desk Technician', we have to create a new role for the password reset task.

Steps:

1. Click on 'AD Delgation' → Help Desk Delegation' → 'Help Desk Roles' → 'Create New Role'

   You will now be in the 'Create Help Desk Role' page.

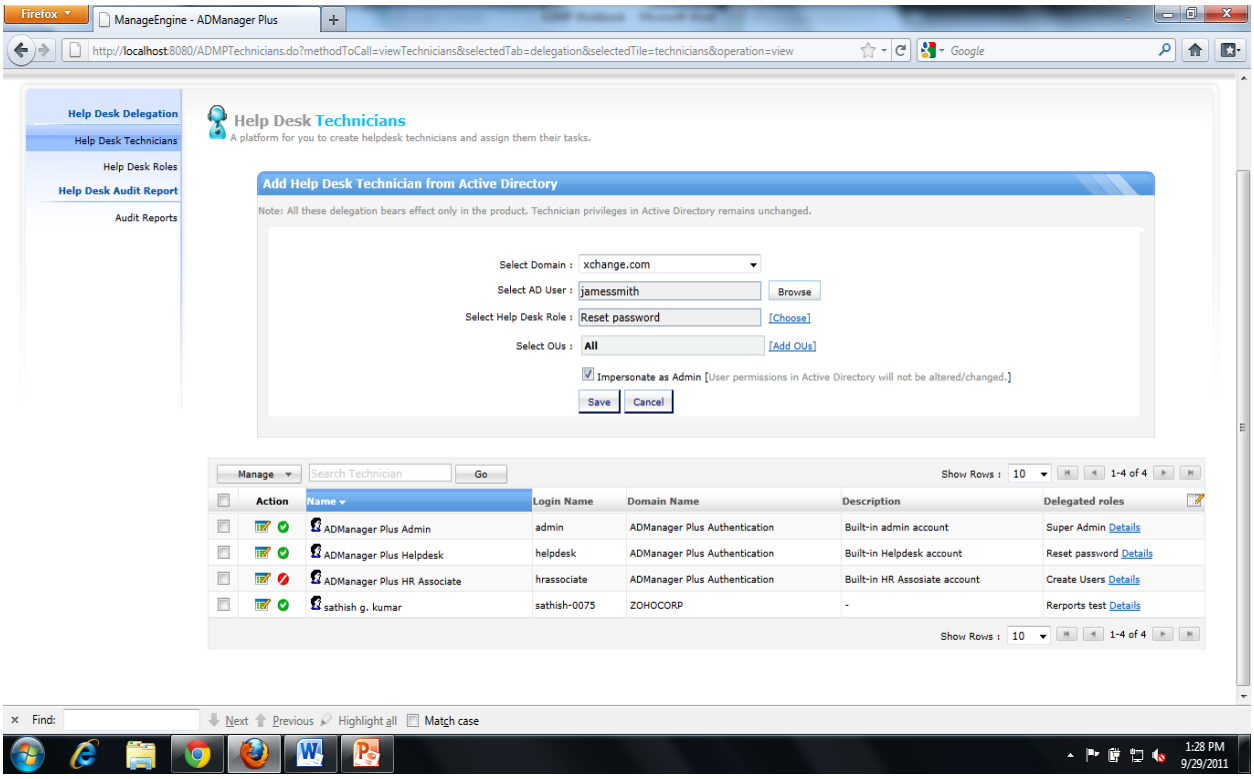


2. Specify a name for this role and describe this role to let others understand the purpose of this role.
3. Select 'AD Management' → 'User Management; → 'Bulk User Modification' → 'Reset Password'
4. Click on '+' beside "Reset Password' to specify password options for the users
5. 'Save Role' to create the 'Reset Password' role.

Create a new ‘Help Desk Technician’ with the ‘Reset Password’role

6. Click on ‘AD Delegation’ → ‘Help Desk Delegation’ → ‘Help Desk Technicians’ → ‘Add New Technician’.

   You will now be in the ‘Help Desk Technicians’ page.



7. Select the ‘Domain’.
8. Select the User to who you would like to delegate this task, using the ‘Browse’ option.
9. Select ‘Reset Password’ role from the list of available roles using the ‘Choose’ option.
10. Specify the ‘OU(s)’ in which the Help Desk Technician will can perform the ‘Reset Password’ task.
11. 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 for specific 'Department(s)' to a 'Help Desk Technician'.

In organizations, individual departments are usually individual OUs and it makes sense to assign a specific person to take care of all the administrative tasks for each department, to avoid confusions and ensure lesser load on the administrators and also quick turnaround time for all the tasks.

To achieve this, we first have to create a role which has only administrative tasks permissions. This administrative role has to be then assigned to a 'Help Desk Technician' and assign him to a specific OU.

Steps:

Create an 'Administrator Role'

1. Click 'AD Delegation'
2. Click on 'Help Desk Delegation' → 'Help Desk Roles' → 'Create New Role'.
3. In the 'Create Help Desk Role' page, click on 'Administration' and select the required options/tasks.
4. Save this role.

Create a Help Desk Technician and assign the Administrative role to this technician for a specific OU:

5. Go to 'AD Delegation' → 'Help Desk Delegation' → 'Help Desk Technicians' → 'Add New Technician'.
6. In the 'Help Desk Technicians' Page, select the 'Domain', User to whom you would like to delegate this administrative task.
7. Select the 'Administration Role' that you just created from the list of roles available, select the 'OU' for which this technician can do the administration.
8. '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".

Solution

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

Conclusion:

We are sure that all these exercises would have really have helped you to gain an even more deeper understating of ADManager Plus than what you had before you started working on the exercises in this workbook. We are also sure that you would have, by now, realized how simple and easy Active Directory Management and Reporting can be when you use ADManager Plus, which is an unbelievably simple and amazingly versatile to cater to all the complexities and challenges in Active Directory Management and Reporting.

If you have any use-case which you feel would really help other users of ADManager Plus in become experts in ADManager Plus, share it with us so that we can get it added to the exercises in this workbook.

If you have any use-case(s) for which you would like to know the solution or steps, do let us know. We would be happy to help you out.