

## Exercise 5

# Creating Organization Units And Users

## Exercise 5 : Creating Organizational Units And Users

In this section, you'll use active directory to view the default settings that apply to user accounts when they are created. These settings can be overridden for a particular user, a group of users, or all users.

You will create a number of organizational units. An OU acts as a container that holds objects such as users.

### Creating Organization Units

In the following exercise, you will create some organizational units that will act as containers for some users. These organizational units model the departments within a small organization.

#### **EXERCISE 5.1**

##### **Creating Organization Units**

1. Logon server as **administrator**.
2. Launch **Active Directory Users and Computers**. Click Start ► Administrative Tools ► Active Directory Users and Computers (Figure 0114)



Figure 0114 : Run Active Directory Users and Computers

3. Click on the **myserver.com** icon to select it (Figure 0115).

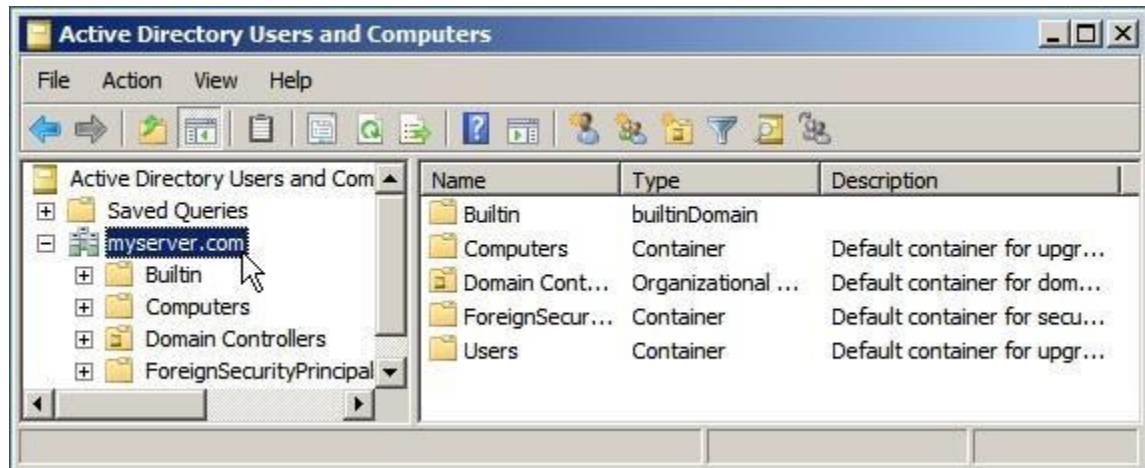


Figure 0115 : Expand Domain

4. On the menu bar, click **Action, New, Organizational Unit** (Figure 0116).



Figure 0116 : Create New Organization Unit

5. Enter **Stkm** as the name for the new organizational unit (Figure 0117).
6. Uncheck **Protect container from accidental deletion** (Figure 0117).
7. Click **OK** (Figure 0117).



Figure 0117 : Create Organization Unit

8. Repeat step 3 to 7 to create the organizational units **Sted** and **Sklr** (Figure 0118).

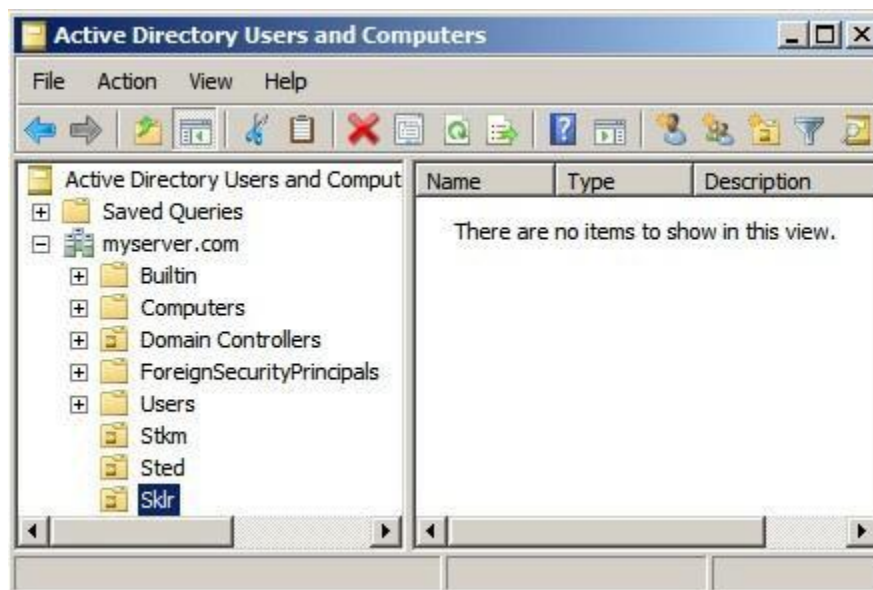


Figure 0118 : Organization Unit

Creating organizational units lets you place users directly into units and assign permissions and rights based on these units. This leads to better administration and delegation control than if you placed users directly into the user container.

When users move from one department to another, it is a simple matter to move the user to the corresponding organizational unit. In this way, they inherit all the new features and rights and of the new organizational unit, ensuring they have full access to all the resources they are entitled to.

## EXERCISE 5.2

### Creating Users within Organizational Units

For proper control, it is better to create users within an OU rather than the Users container. In the following exercise you will create a number of users, modify their properties, and move them from one organizational unit to another.

9. Click the **Stkm** OU to highlight it (Figure 0119).

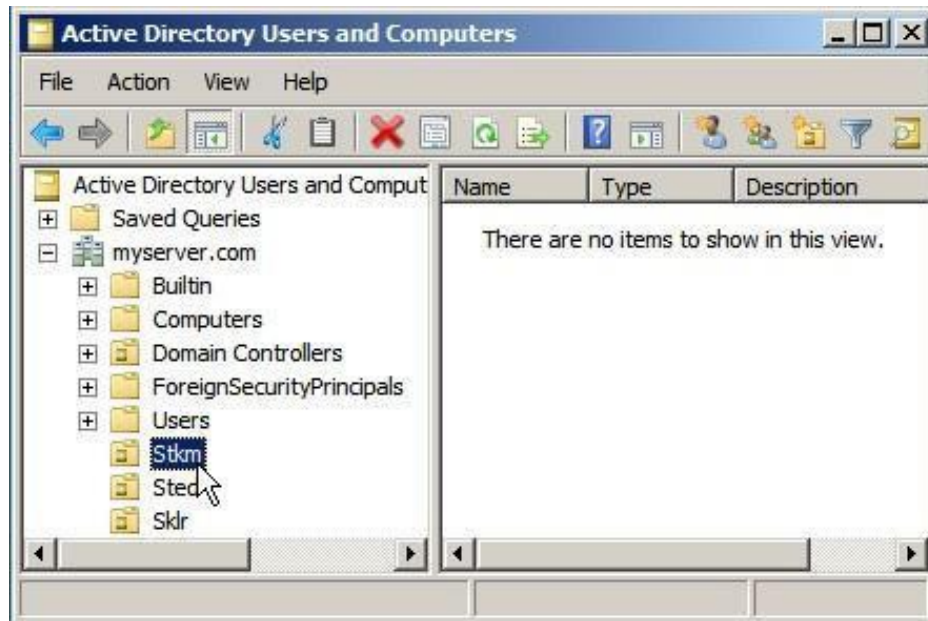


Figure 0119 : Stkm OU

### Creating new user accounts for **Zul**

10. Right click **Stkm** and select **New ► User** from the menu (Figure 0120).



Figure 0120 : Stkm OU

11. Enter the following details for Zul (Figure 0121).

First Name	Last Name	Full Name	User logon name
Zul	Zcomby	Zul Zcomby	zul.zcomby



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: myserver.com/Stkm'. Below this, there are several input fields: 'First name:' with 'Zul', 'Last name:' with 'Zcomby', 'Full name:' with 'Zul Zcomby', 'User logon name:' with 'zul.zcomby' and a dropdown menu showing '@myserver.com', and 'User logon name (pre-Windows 2000):' with 'MYSERVER\' and 'zul.zcomby'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 0121 : Create New User

12. Click **Next**.

13. Enter the password as **comby**. Check the boxes "User cannot change password" and "Password never expires", then click **Next** (Figure 0122).



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: myserver.com/Stkm'. Below this, there are two password input fields: 'Password:' and 'Confirm password:', both containing 'comby'. Below the password fields, there are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (checked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 0122 : Create Password



14. Click Finish to create the new user *Zul* (Figure 0123).

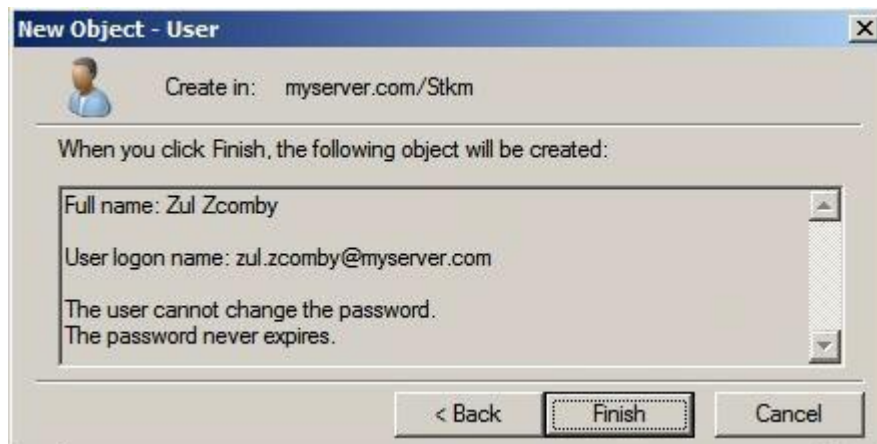


Figure 0123 : New User Account Confirmation

15. The warning below will appear. This warning appears because your password does not meet the password policy requirements. Click **OK** to continue (Figure 0124).



Figure 0124 : Password Policy Warning

16. Click **Cancel** to close new user account confirmation window (Figure 0125).

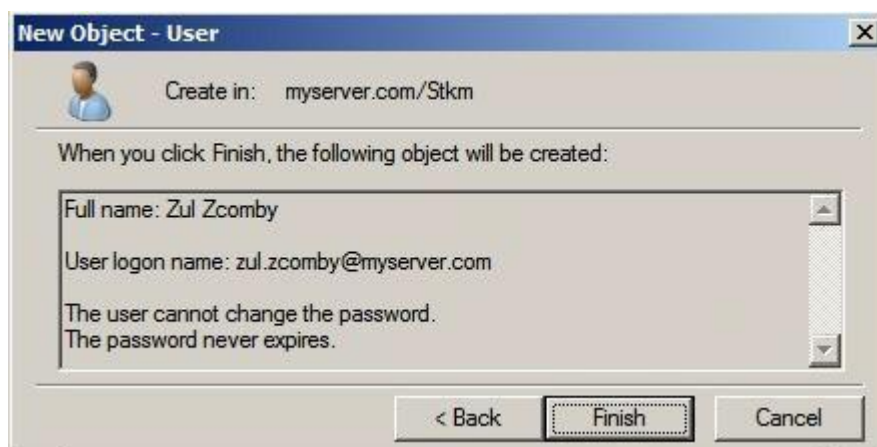


Figure 0125 : New User Account Confirmation

### **EXERCISE 5.2.1**

#### **Configuring Password Policy**

17. To disable password policy requirements; launch **Group Policy Management**.  
Click Start ► Administrative Tools ► Group Policy Management (Figure 0126)

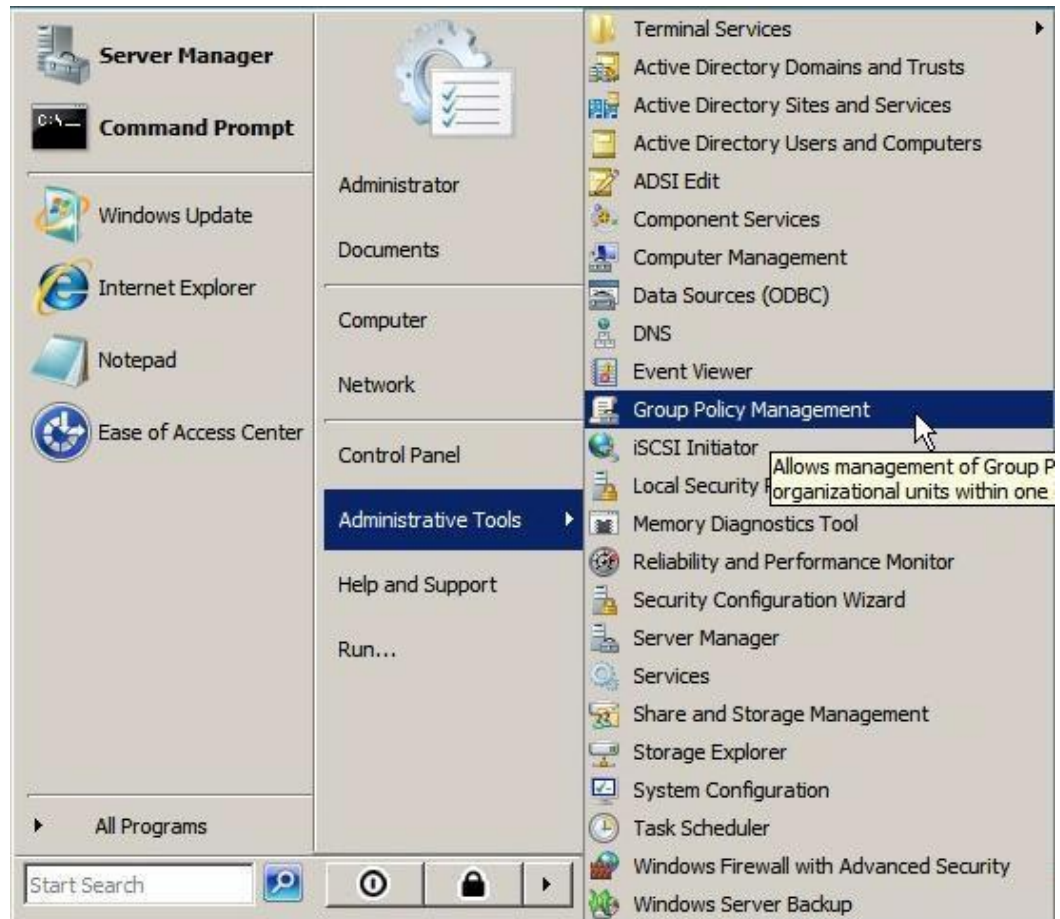


Figure 0126 : Launch Group Policy Management



18. Double click to expand **Forest: myserver.com**.
19. Expand **Domains**.
20. Expand **myserver.com**.
21. Click **Default Domain Policy** (Figure 0127).

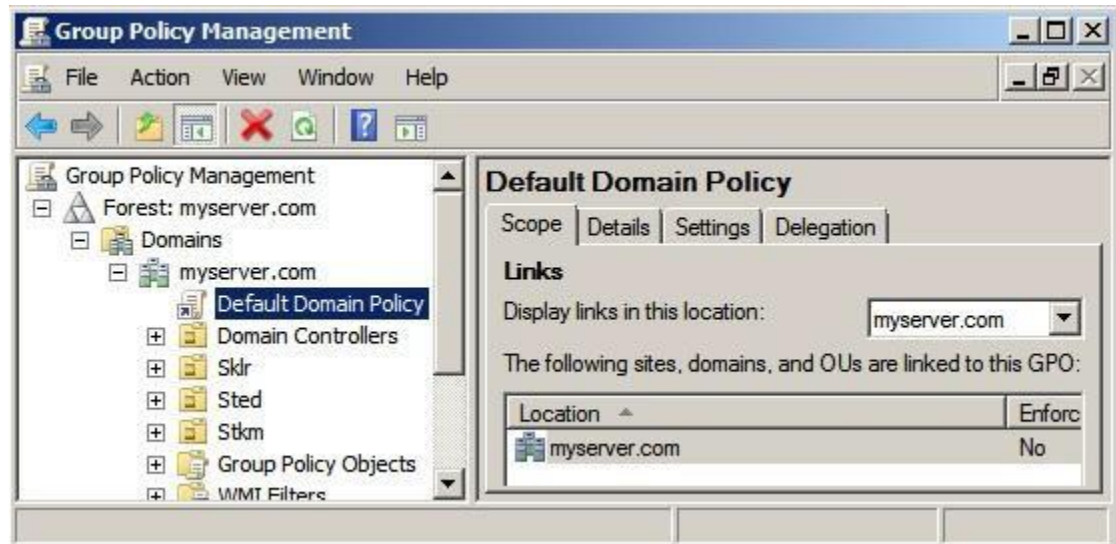


Figure 0127 : Group Policy Management

22. If any warning box appeared; just click **OK** (Figure 0128).

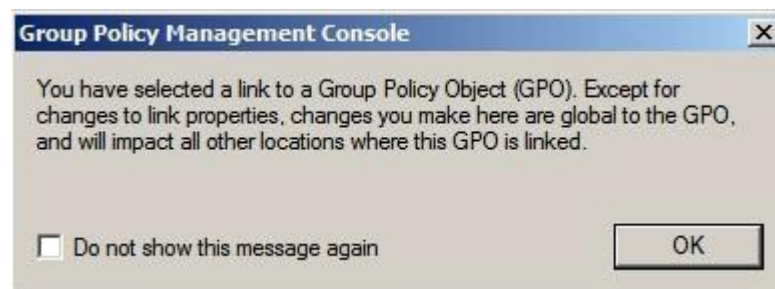


Figure 0128 : Group Policy Management Console Warning

23. Right click **Default Domain Policy** and select **Edit** (Figure 0129).

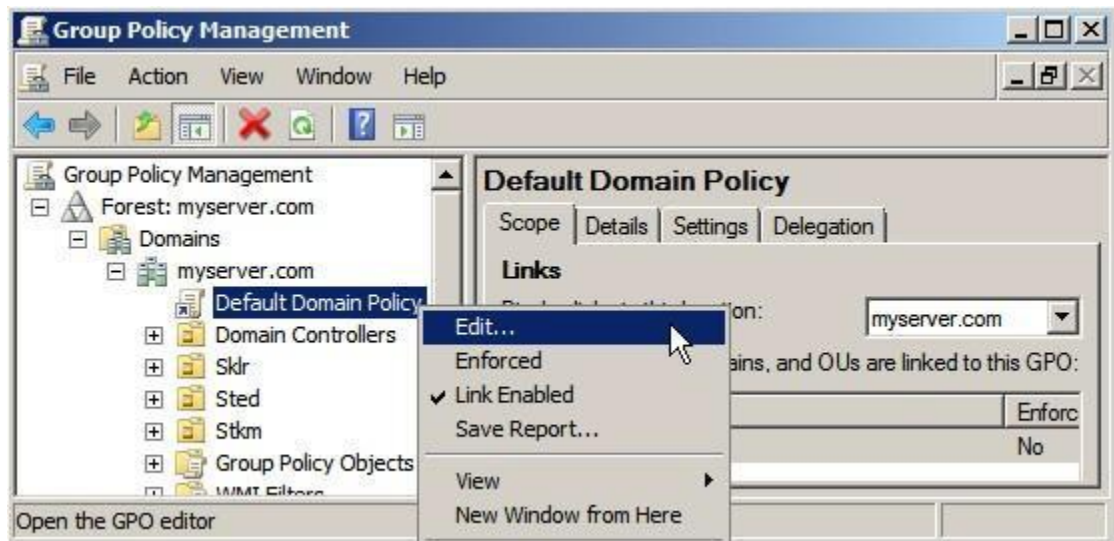


Figure 0129 : Group Policy Management – Default Domain Policy

24. Double click to expand **Policies** (Figure 0130).

25. Expand **Windows Settings**.

26. Expand **Security Settings** (Figure 0130).

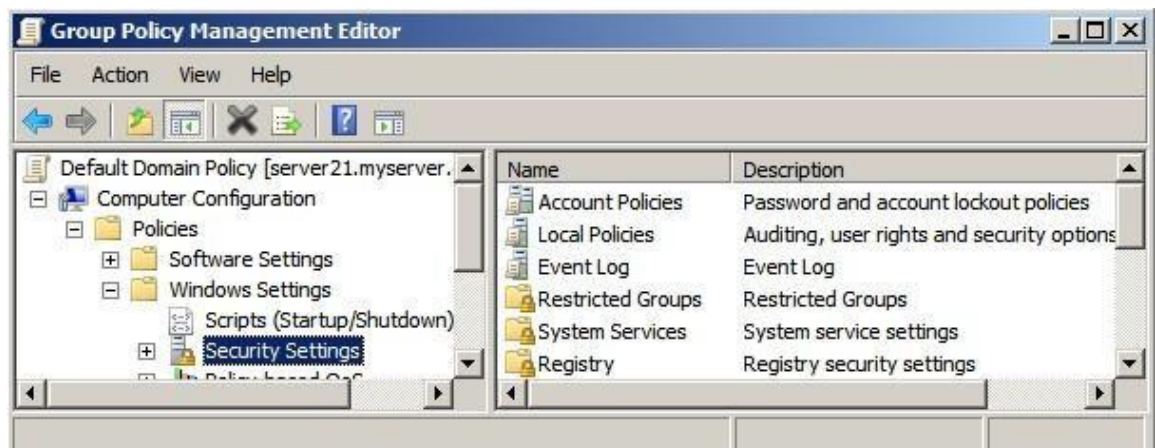


Figure 0130 : Group Policy Management – Security Settings

27. Double click to expand **Account Policies** (Figure 0131).

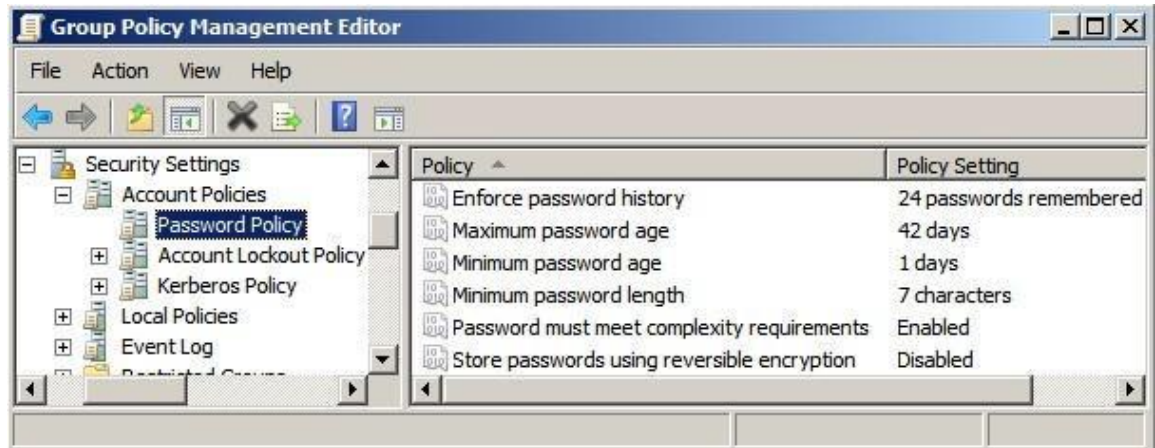


Figure 0131 : Group Policy Management – Password Policy

28. Click **Password Policy** (Figure 0132).

29. Double click **Password must meet complexity requirements** under Password Policy to open **Password must meet complexity requirements Properties**.

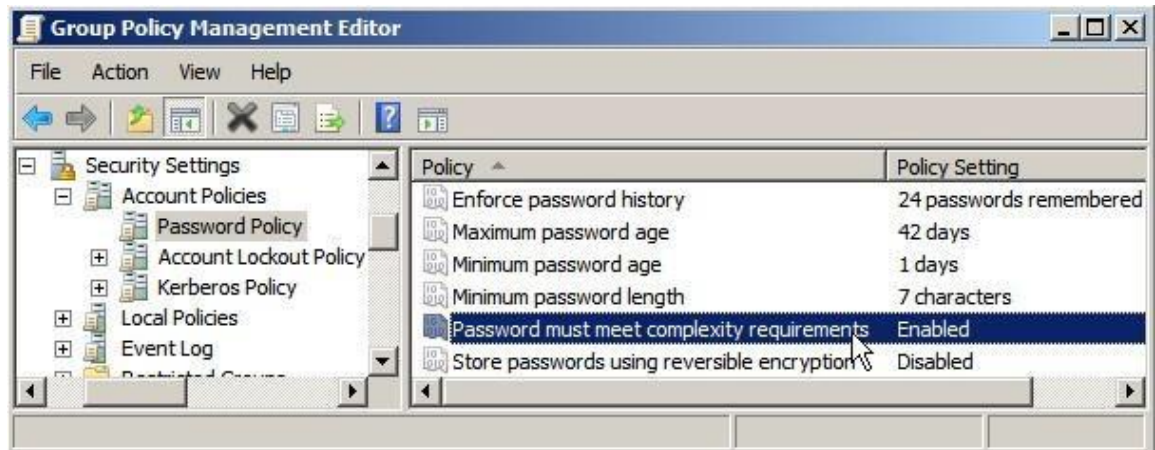


Figure 0132 : Group Policy Management - Password Must Meet Complexity Requirements

30. Select **Disabled** under Security Policy Setting tab (Figure 0133).



Figure 0133 : Password Must Meet Complexity Requirements Properties

31. Click **OK**.

32. Double click **Minimum password length** under Password Policy to open **Minimum password length Properties** (Figure 0134).



Figure 0134 : Group Policy Management - Minimum Password Length

33. Set **No password required** to **0** characters (Figure 0135).

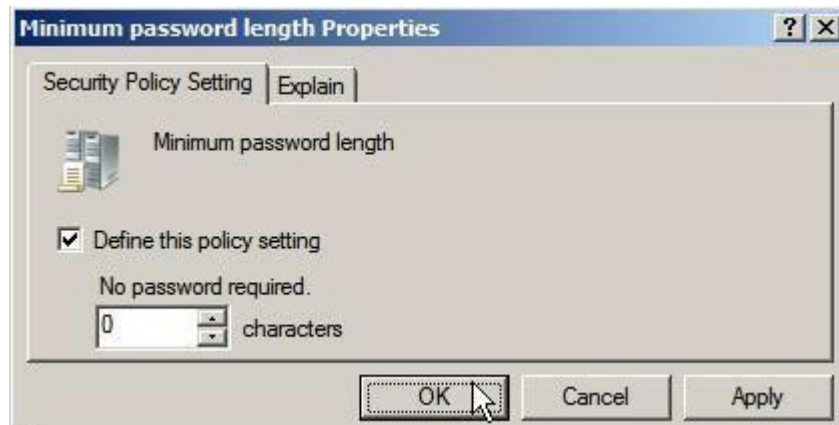


Figure 0135 : Minimum Password Length Properties

34. Click **OK**.

35. Recheck your configuration. Your configuration should be same as figure below (Figure 0136).



Figure 0136 : Group Policy Management - Password Policy

36. **Close** all windows and **RESTART** your server.

After restarting server, login as Administrator and start **create** user **Zul Zcomby** again (follow step 10 to 14). There should be no problem anymore.



### Creating Users within Organizational Units (EXERCISE 5.2 - Continue)

37. Now create the new user **Ocah** in the **Stkm** OU using the following properties (Figure 0137).

First Name	Ocah
Last Name	Blue
Full Name	Ocah Blue
User logon name	ocah.blue
Password	ocah
User cannot change password	
Password never expires	

Figure 0137 : Ocah Blue Properties

38. Create the following user account in the **Sted** OU (Figure 0138).

First Name	Ahmad
Last Name	Akmal
Full Name	Ahmad Akmal
User logon name	zul.akmal
Password	akmal
User cannot change password	
Password never expires	

Figure 0138 : Ahmad Akmal Properties

39. Create the following user account in the **Sklr** OU.

First Name	Ain
Last Name	Syahmi
Full Name	Ain Syahmi
User logon name	ain.syahmi
Password	ain
User cannot change password	
Password never expires	

Figure 0139 : Ain Syahmi Properties



First Name	Ali
Last Name	Uddin
Full Name	Aliuddin
User logon name	ali.zul
Password	ali
User cannot change password	
Password never expires	

Figure 0140 : Aliuddin Properties

First Name	Wan
Last Name	Saad
Full Name	Md Saad
User logon name	wan.saad
Password	masuri
User must change password at next logon	
Account is disabled	

Figure 0141 : Md Saad Properties



40. Note the down arrow that appears on the icon for the user *Md Saad*, indicating this account has been disabled (Figure 0142).

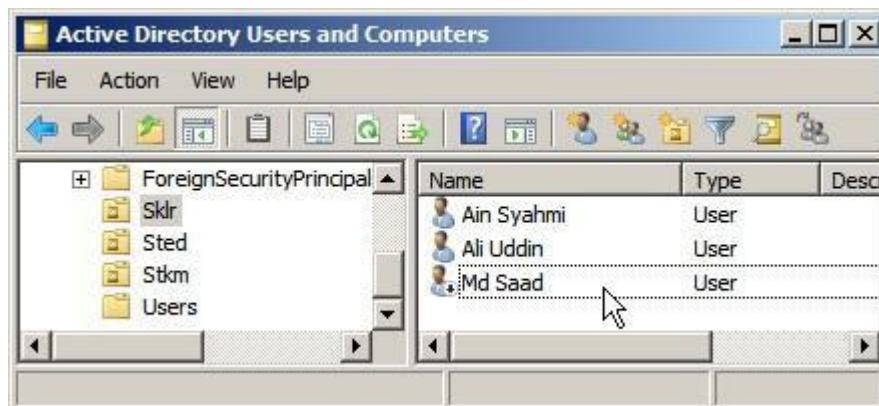


Figure 0142 : AD Users and Computers – User Disabled

### **EXERCISE 5.3**

#### **Moving Users within Organizational Units**

41. It is easy to delete, rename or move a user from an organization unit. In the above exercise the user *Md Saad* was inadvertently placed in the wrong OU. **Right-click** the user *Md Saad* and select **move** from the list (Figure 0143).



Figure 0143 : Move Users

42. Click **Stkm** as the destination OU (Figure 0144).



Figure 0144 : Move Users – Stkm OU

43. Click **OK**

44. Expand the **Stkm** OU to confirm that the user *Md Saad* is now a member of Stkm OU (Figure 0145).



Figure 0145 : Stkm OU Members

You have now created a number of users within the organizational units created earlier. At this stage, you cannot see the benefits of doing this. However, the later exercises will start to illustrate why this has been done, by allocating resources to organizational units.

Thus, a user will get access to a resource based on their OU membership properties. If a user moves from one organizational unit to another, they will inherit all the resources associated with the new OU.

## EXERCISE 5.4

### Updating User Information

In this exercise we will look at default user properties such as logon times and how often they need to change their passwords.

Active Directory allows organizations to store significantly more information than in previous versions of Windows. For example, you can store telephone and office information in the Active Directory with the user information.

45. Double click the user *Md Saad* in the **Stkm** OU (Figure 0146).

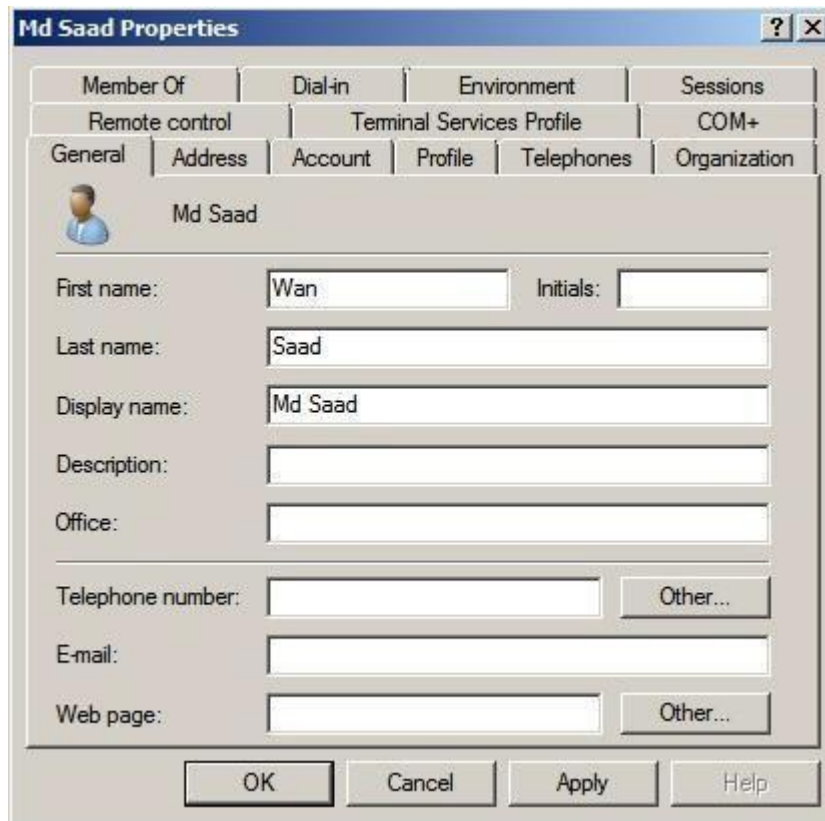


Figure 0146 : User Properties

46. Enter the following details (Figure 0147).

Office	Integration
Telephone Number	012-5740157
E-Mail	md.saad@myserver.com
Job Title (Organization)	Senior Instructor
Department	Computer Technology
Company	IKM

Figure 0147 : User Details

**Md Saad Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

**Md Saad**

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

Figure 0148 : Md Saad Properties - General

**Md Saad Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

Job Title:

Department:

Company:

Manager

Name:

Direct reports:

Figure 0149 : Md Saad Properties - Organization

47. Click **OK** to apply the changes.

## EXERCISE 5.5

### Restrict User Logon Hours

48. Double click the user *Md Saad* in the **Stkm** OU (Figure 0150).

The 'Md Saad Properties' dialog box is shown with the 'General' tab selected. It contains the following fields:

- Member Of: [Empty]
- Dial-in: [Empty]
- Environment: [Empty]
- Sessions: [Empty]
- Remote control: [Empty]
- Terminal Services Profile: [Empty]
- COM+: [Empty]
- General: [Selected]
- Address: [Empty]
- Account: [Empty]
- Profile: [Empty]
- Telephones: [Empty]
- Organization: [Empty]

Below the tabs, there is a user icon and the name 'Md Saad'. The fields are:

- First name: Wan
- Initials: [Empty]
- Last name: Saad
- Display name: Md Saad
- Description: [Empty]
- Office: Integration
- Telephone number: 012-5740157
- Other...: [Button]
- E-mail: md.saad@myserver.com
- Web page: [Empty]
- Other...: [Button]

At the bottom are buttons for OK, Cancel, Apply, and Help.

Figure 0150 : Md Saad Properties

49. Click **Account** tab (Figure 0151).

The 'Md Saad Properties' dialog box is shown with the 'Account' tab selected. It contains the following fields and options:

- User logon name: wan.saad@myserver.com
- User logon name (pre-Windows 2000): MYSERVER\wan.saad
- Logon Hours...: [Button]
- Log On To...: [Button]
- Unlock account: ☐
- Account options:
  - ☒ User must change password at next logon
  - ☐ User cannot change password
  - ☐ Password never expires
  - ☐ Store password using reversible encryption
- Account expires:
  - ☒ Never
  - ☐ End of: Sunday, September 27, 2009

At the bottom are buttons for OK, Cancel, Apply, and Help.

Figure 0151 : Md Saad Properties - Account



50. Click the **Logon Hours** button (Figure 0152).

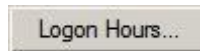


Figure 0152 : Logon Hours

51. Select all areas and click **Logon Denied** (Figure 0153).

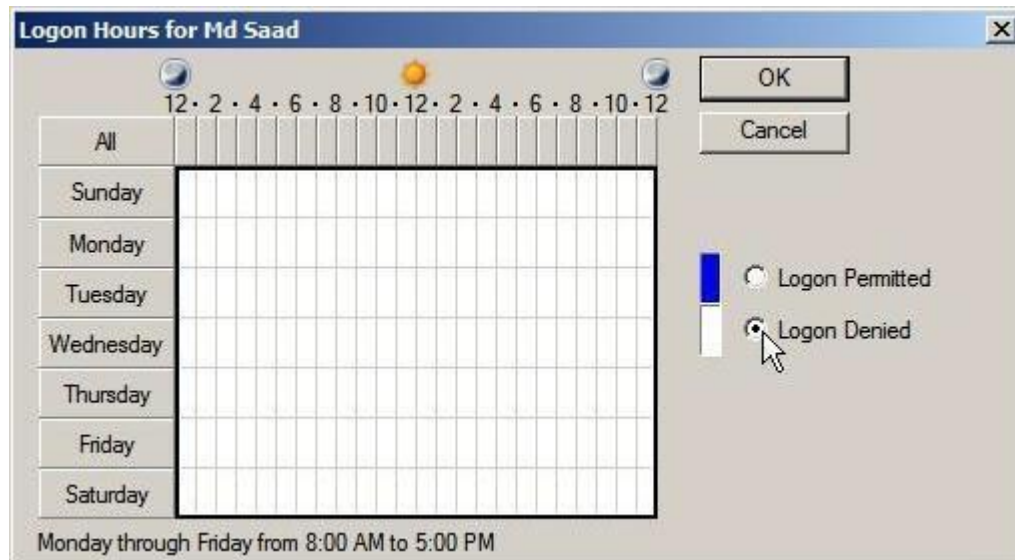


Figure 0153 : Logon Hours for Md Saad – Logon Denied

Restrict the logon hours (under Account Tab) to Monday-Friday, 8am-5pm.

52. Select the areas Monday to Friday and 8am to 5pm (Figure 0154).

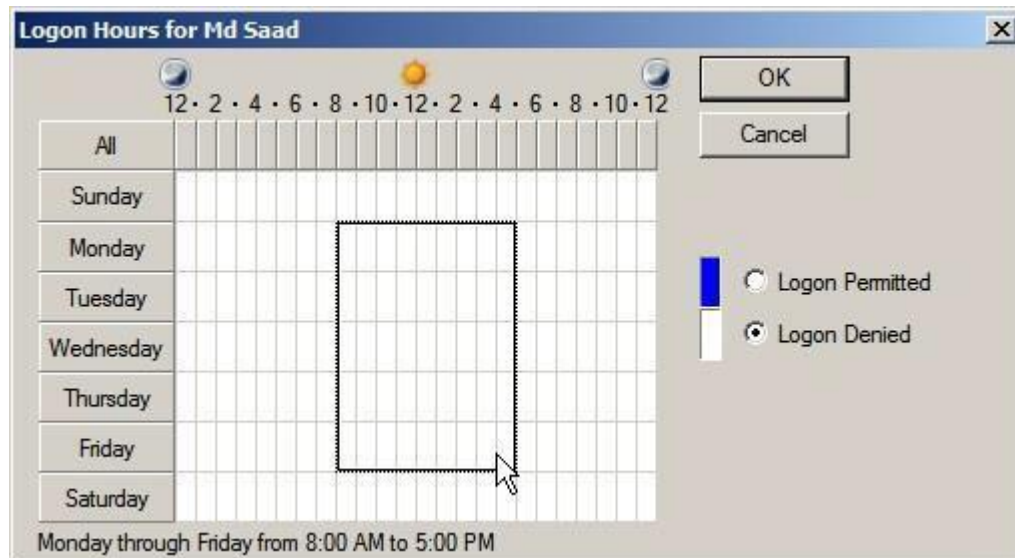


Figure 0154 : Logon Hours for Md Saad – Select Areas

53. Select **Logon Permitted** (Figure 0155).

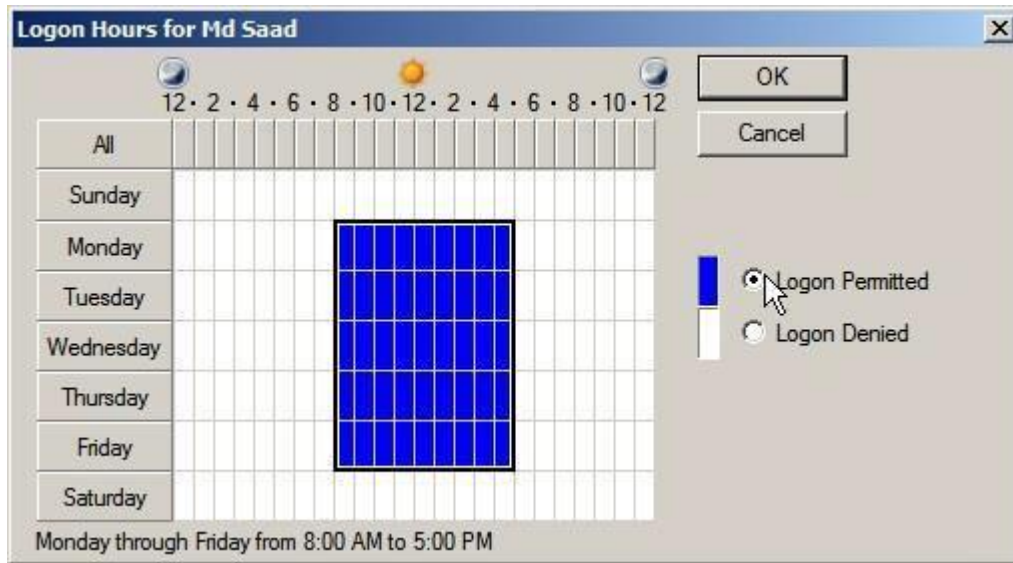


Figure 0155 : Logon Hours for Md Saad – Set Logon Permitted

54. Click the **OK** button.

55. Click the **OK** button again.

In the above exercise you assigned some organizational information to a user. You also explored some of the properties that can be applied.