Microsoft®
Training &
Certification

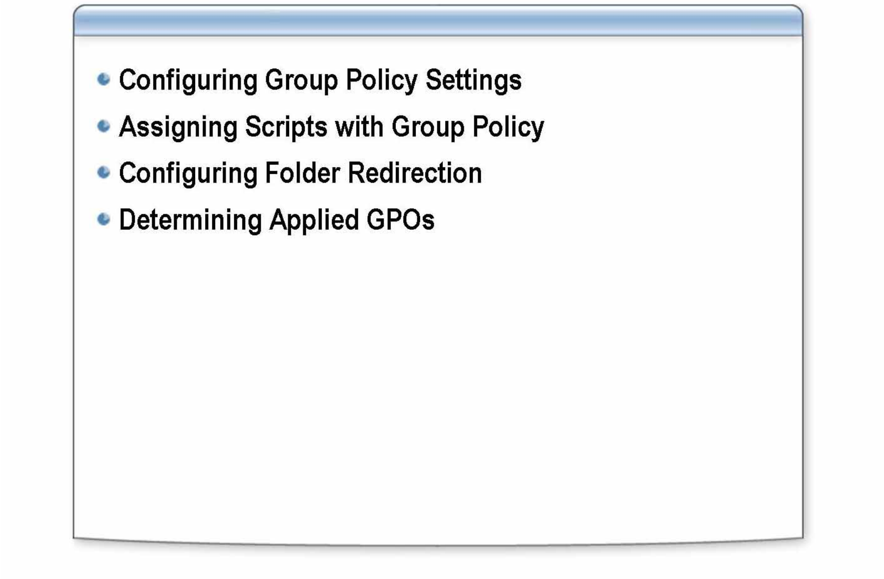
Microsoft® Official
Curriculum

Module 9: Managing the User Environment by Using Group Policy

Contents

Microsoft®

Overview



- Configuring Group Policy Settings
- Assigning Scripts with Group Policy
- Configuring Folder Redirection
- Determining Applied GPOs

Introduction

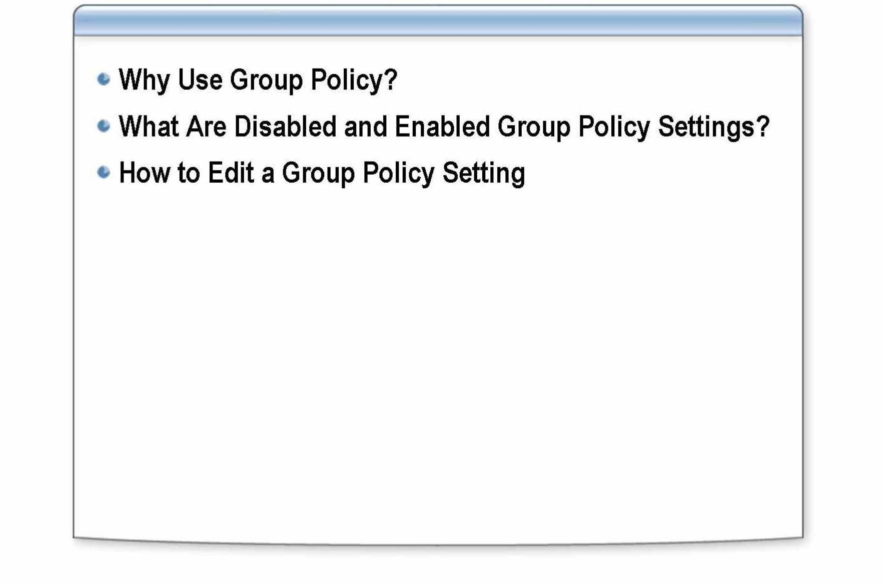
This module introduces the job function of managing the user environment by using Group Policy. Specifically, the module provides the skills and knowledge that you need to use Group Policy to configure Folder Redirection, Microsoft® Internet Explorer connectivity, and the desktop.

Objectives

After completing this module, you will be able to:

- Configure Group Policy settings.
- Assign scripts with Group Policy.
- Configure Folder Redirection.
- Determine Applied Group Policy objects (GPOs).

Lesson: Configuring Group Policy Settings



- Why Use Group Policy?
- What Are Disabled and Enabled Group Policy Settings?
- How to Edit a Group Policy Setting

Introduction

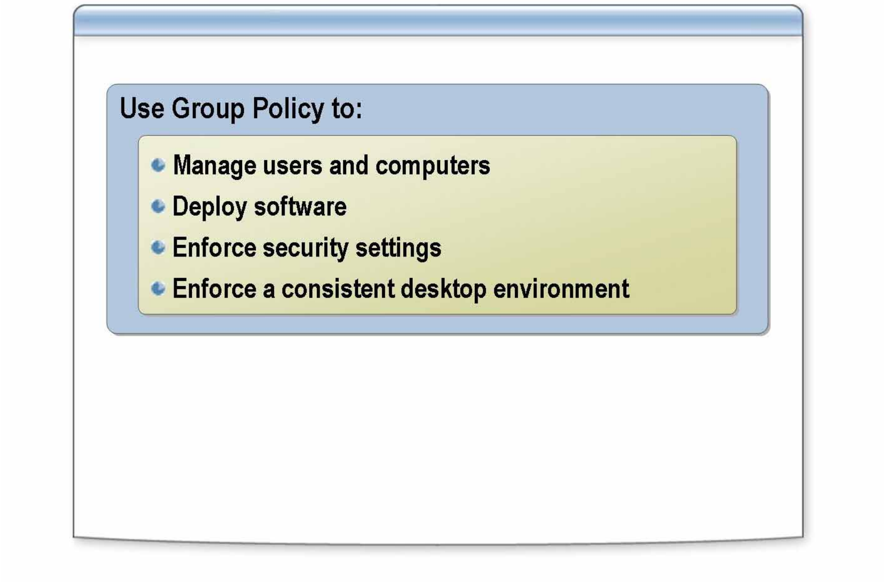
After completing this lesson, you will be able to configure Group Policy settings.

Lesson objectives

After completing this lesson, you will be able to:

- Explain why you use Group Policy.
- Explain what disabled and enabled Group Policy settings are.
- Edit a Group Policy setting.

Why Use Group Policy?



Use Group Policy to:

- Manage users and computers
- Deploy software
- Enforce security settings
- Enforce a consistent desktop environment

Introduction

Managing user environments means controlling what users can do when logged on to the network. You do this by controlling their desktops, network connections, and user interfaces through Group Policy. You manage user environments to ensure that users have what they need to perform their jobs, but that they cannot corrupt or incorrectly configure their environments.

Tasks you can perform with Group Policy

When you centrally configure and manage user environments, you can perform the following tasks:

- Manage users and computers

  By managing user desktop settings with registry-based policies, you ensure that users have the same computing environments even if they log on from different computers. You can control how Microsoft Windows® Server 2003 manages user profiles, which includes how a user's personal data is made available. By redirecting user folders from the user's local hard disks to a central location on a server, you can ensure that the user's data is available to them regardless of the computer they log on to.

- Deploy software

  Software is deployed to computers or users through the Active Directory® directory service. With software deployment, you can ensure that users have their required programs, service packs, and hotfixes.

- Enforce security settings

  By using Group Policy in Active Directory, the systems administrator can centrally apply the security settings required to protect the user environment. In Windows Server 2003, you can use the Security Settings extension in Group Policy to define the security settings for local and domain security policies.

- Enforce a consistent desktop environment

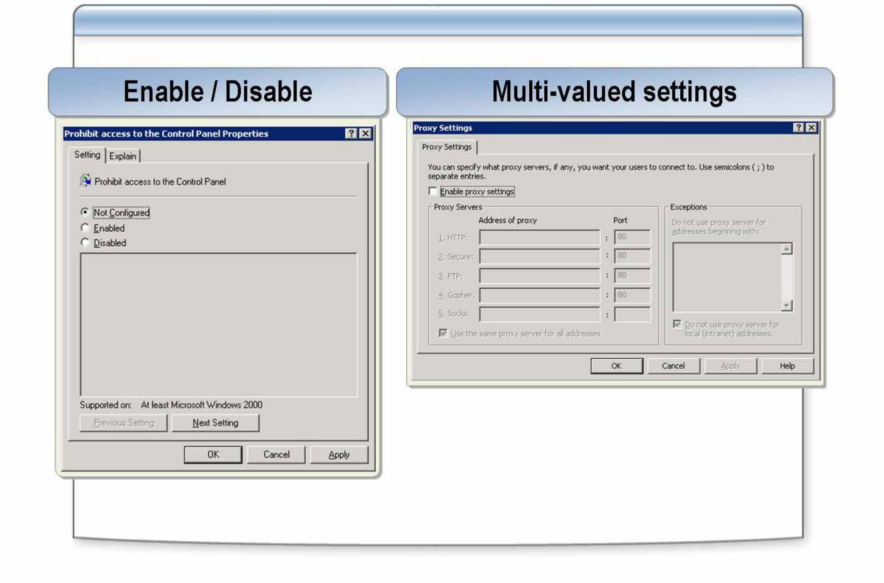
  Group Policy settings provide an efficient way to enforce standards, such as logon scripts and password settings. For example, you can prevent users from making changes to their desktops that may make their user environments more complex than necessary.

Additional reading

For more information about desktop management, see:

- "Windows 2000 Desktop Management Overview" at http://www.microsoft.com/windows2000/techinfo/howitworks/management/ccmintro.asp.
- "Introduction to Windows 2000 Group Policy" at http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp.
- The Group Policy newsgroup at http://www.microsoft.com/windows2000/community/newsgroups/.

What Are Disabled and Enabled Group Policy Settings?



Enable / Disable

Prohibit access to the Control Panel Properties

Prohibit access to the Control Panel

● Not Configured
○ Enabled
○ Disabled

Supported on: At least Microsoft Windows 2000

Multi-valued settings

Proxy Settings

You can specify what proxy servers, if any, you want your users to connect to. Use semicolons (;) to separate entries.

□ Enable proxy settings

Proxy Servers

	Address of proxy	Port
1. HTTP:		80
2. Secure:		80
3. FTP:		80
4. Gopher:		80
5. Socks:		

☑ Use the same proxy server for all addresses

Exceptions

Do not use proxy server for addresses beginning with:

☑ Do not use proxy server for local (intranet) addresses.

Disable a policy setting

If you disable a policy setting, you are disabling the action of the policy setting. For example, users by default can access Control Panel. You do not need to disable the policy setting **Prohibit access to the Control Panel** to allow a user to access Control Panel unless a previously applied policy setting enabled it. In this situation, you set another policy setting that disables the previously applied policy setting.

This is helpful when you have inherited policy settings, and you do not want to use filtering to apply policy settings to one group and not to another group. You can apply a GPO that enables one policy setting on the parent organizational unit and another policy setting that disables the GPO on a child organizational unit.

Enable a policy setting

If you enable a policy setting, you are enabling the action of the policy setting. For example, to revoke someone's access to Control Panel, you enable the policy setting **Prohibit access to the Control Panel**.

Not Configured

A GPO holds the values that change the registry for users and computers that are subject to the GPO. The default configuration for a policy setting is **Not Configured**. If you want to set a computer or user policy setting back to the default value or back to the local policy, select the **Not Configured** option.

For example, you may enable a policy setting for some clients, and when using the not Configured option, the policy will revert to the default, local policy setting.

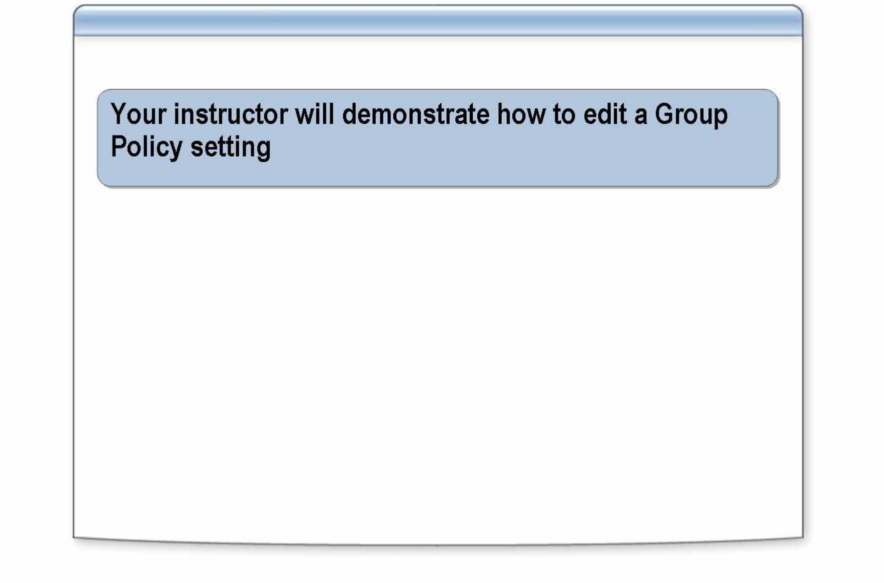
Multi-valued policy settings

Some GPOs require you to provide some additional information after you enable the object. Sometimes you may need to select a group or computer if the policy setting needs to redirect the user to some information. Other times, as the slide shows, to enable proxy settings, you must provide the name or Internet Protocol (IP) address of the proxy server and the port number. If a policy setting is multi-valued and the settings are in conflict with another policy setting, the conflicting multi-valued settings are replaced with the last conflicting policy setting that was applied.

Note The **Settings** tab indicates the operating systems that support the policy setting.

The **Explain** tab has information about the effects of the **Enabled** and **Disabled** options on a user and computer account.

How to Edit a Group Policy Setting



Your instructor will demonstrate how to edit a Group Policy setting

Introduction

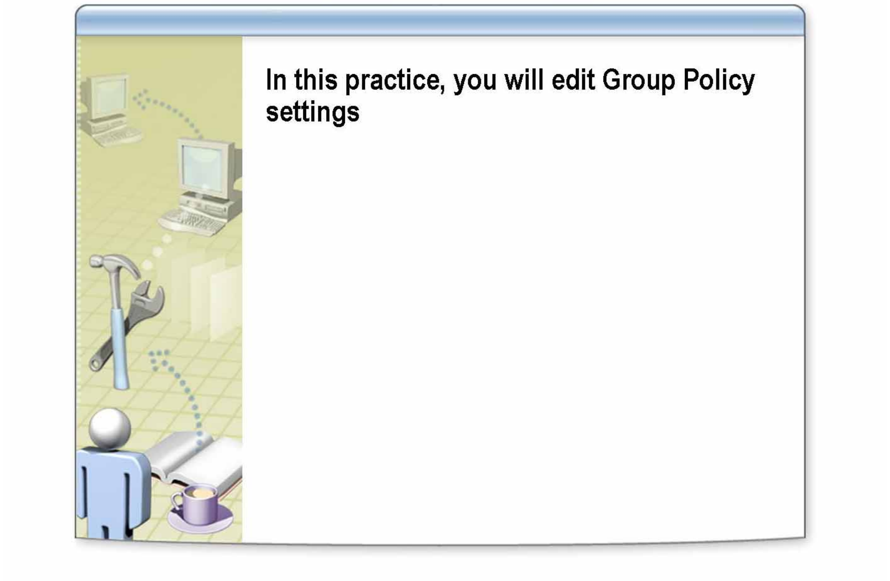
As a systems administrator, you must edit Group Policy settings. Use the following procedure to perform this task.

Procedure

To edit Group Policy settings:

1. In Group Policy Management, in the console tree, navigate to **Group Policy Objects**.
2. Right-click a GPO, and then click **Edit**.
3. In Group Policy Object Editor, navigate to the Group Policy setting that you want to edit, and then double-click the setting.
4. In the **Properties** dialog box, configure the Group Policy setting, and then click **OK**.

Practice: Editing Group Policy Settings



In this practice, you will edit Group Policy settings

Objective

In this practice, you will edit Group Policy settings.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains the following snap-ins:
  - Active Directory Users and Computers
  - Group Policy Management
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Northwind Traders must implement the *ComputerName* Standard Desktop GPO. This GPO is linked to the IT Test/*ComputerName* organizational unit for the test environment and the Locations/*ComputerName* organizational unit for the production environment. You must disable the link for the production environment first. When that is done, Northwind Traders wants to implement the following Group Policy settings in the *ComputerName* Standard Desktop GPO:

- **Remove Run menu from the Start Menu**
- **Prohibit access to the Control Panel**
- **Hide My Network Places icon on desktop**
- **Remove Network Connections from Start Menu**
- **Remove “Map Network Drive” and “Disconnect Network Drive”**

Practice

► **Verify that the GPO links are configured**

- Verify that the *ComputerName* Standard Desktop GPO is linked to the Locations/*ComputerName* organizational unit.

► **Configure security filtering**

- Location: Locations/*ComputerName*
- GPO link: *ComputerName* Standard Desktop
- Security filtering:
  - Remove all security group filtering
  - Add the Everyone group

► **Disable a GPO link**

- Location: Locations/*ComputerName*
- GPO link: *ComputerName* Standard Desktop

► **Edit a GPO**

- GPO: *ComputerName* Standard Desktop

► **Remove Run from the Start menu**

- Location: User Configuration/Administrative Templates/Start Menu and Taskbar
- Group Policy setting: **Remove Run menu from Start Menu Properties**
- Option: **Enabled**

► **Disable access to Control Panel**

- Location: User Configuration/Administrative Templates/Control Panel
- Group Policy setting: **Prohibit access to the Control Panel**
- Option: **Enabled**

► **Hide My Network Places icon on desktop**

- Location: User Configuration/Administrative Templates/Desktop
- Group Policy setting: **Hide My Network Places icon on desktop**
- Option: **Enabled**

► **Remove Network Connections from the Start menu**

- Location: User Configuration/Administrative Templates/Start Menu and Taskbar
- Group Policy setting: **Remove Network Connections from Start Menu**
- Option: **Enabled**

► Enable Remove "Map Network Drive" and "Disconnect Network Drive"

- Location: User Configuration/Administrative Templates/
  Windows Components/Windows Explorer
- Group Policy setting: **Remove "Map Network Drive" and "Disconnect Network Drive"**
- Option: **Enabled**

► Enable a GPO link

- Location: Locations/*ComputerName*
- GPO link: *ComputerName* Standard Desktop

► Create a user account

1. Create a user account (if the user account does not already exist) with the following properties:
   - First name: *ComputerName*
   - Last name: **Test**
   - User logon name: *ComputerName***Test**
   - Password: **P@ssw0rd**
   - Organizational unit: Locations/*ComputerName/*User
2. Log off.

► Log on

1. Log on as *ComputerName***Test** with a password of **P@ssw0rd**.
2. Verify that the following is true:
   - **Run** has been removed menu from the **Start** menu.
   - **Control Panel** has been removed from the **Start** menu.
   - The **My Network Places** icon is hidden on the desktop.
   - **Network Connections** has been removed from the **Start** menu.
   - **Map Network Drive** and **Disconnect Network Drive** have been removed from Windows Explorer.
3. Log off.

Lesson: Assigning Scripts with Group Policy

- What Are Group Policy Script Settings?
- How to Assign Scripts with Group Policy

Introduction

You can use Group Policy to deploy scripts to users and computers. A script is a batch file or a Microsoft Visual Basic® script that can execute code or perform management tasks. You can use Group Policy script settings to automate the process of running scripts.

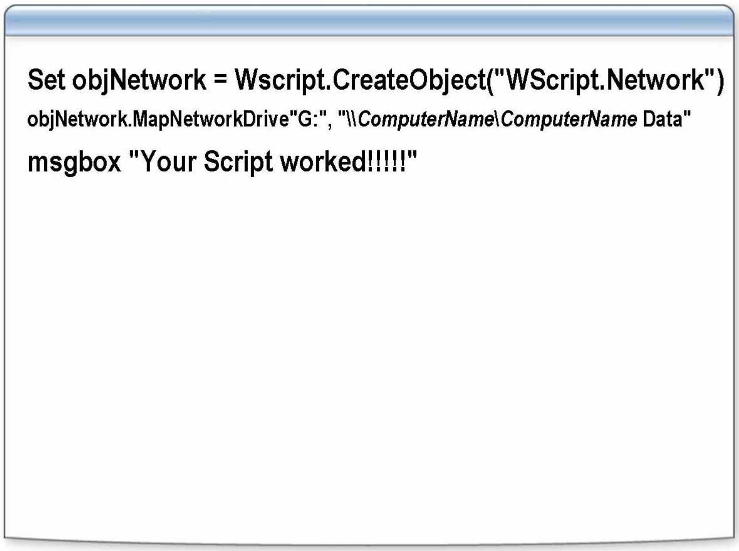
There are script settings under both Computer Configuration and User Configuration in Group Policy. You can use Group Policy to run scripts when a computer starts and shuts down and when a user logs on and logs off. As with all Group Policy settings, you configure a Group Policy script setting once, and Windows Server 2003 continually implements and enforces it throughout your network.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what Group Policy script settings are.
- Assign scripts with Group Policy.

What Are Group Policy Script Settings?



```
Set objNetwork = Wscript.CreateObject("WScript.Network")
objNetwork.MapNetworkDrive"G:", "\\ComputerName\ComputerName Data"
msgbox "Your Script worked!!!!!"
```

Introduction

You can use Group Policy script settings to centrally configure scripts to run automatically when the computer starts and shuts down and when users log on and log off. You can specify any script that runs in Windows Server 2003, including batch files, executable programs, and scripts supported by Windows Script Host (WSH).

Benefits of Group Policy script settings

To help you manage and configure user environments, you can:

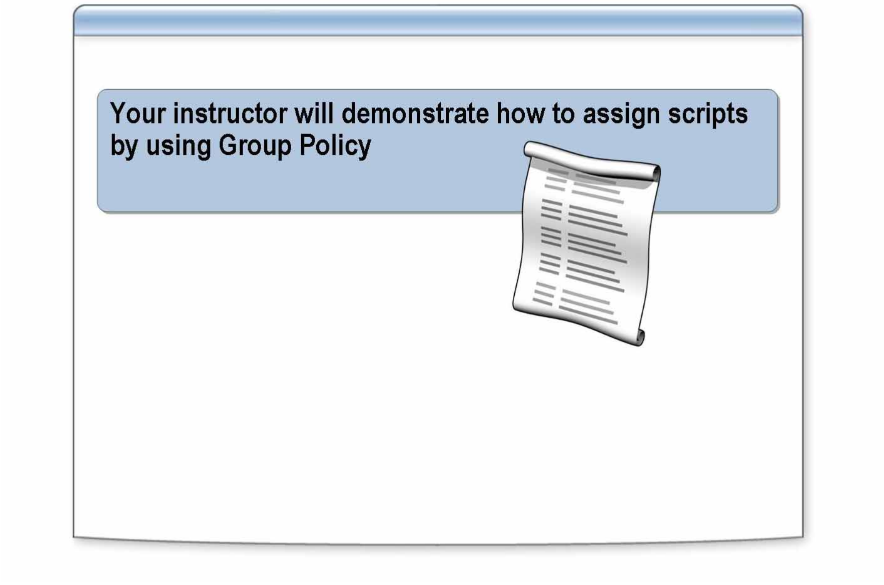
- Run scripts that perform tasks that you cannot perform through other Group Policy settings. For example, you can populate user environments with network connections, printer connections, shortcuts to applications, and corporate documents.
- Clean up desktops when users log off and shut down computers. You can remove connections that you added with logon or startup scripts so that the computer is in the same state as when the user started the computer.
- Run pre-existing scripts already set up to manage user environments until you configure other Group Policy settings to replace these scripts.

Note From Active Directory Users and Computers, you can assign logon scripts individually to user accounts in the **Properties** dialog box for each user account. However, Group Policy is the preferred method for running scripts, because you can manage these scripts centrally, along with startup, shutdown, and logoff scripts.

Additional reading

For more information about scripting, see the TechNet Script Center at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp.

How to Assign Scripts with Group Policy



Your instructor will demonstrate how to assign scripts by using Group Policy

Introduction

To implement a script, you use Group Policy to add that script to the appropriate setting in the Group Policy template. This indicates that the script will run during startup, shutdown, logon, or logoff.

Procedure

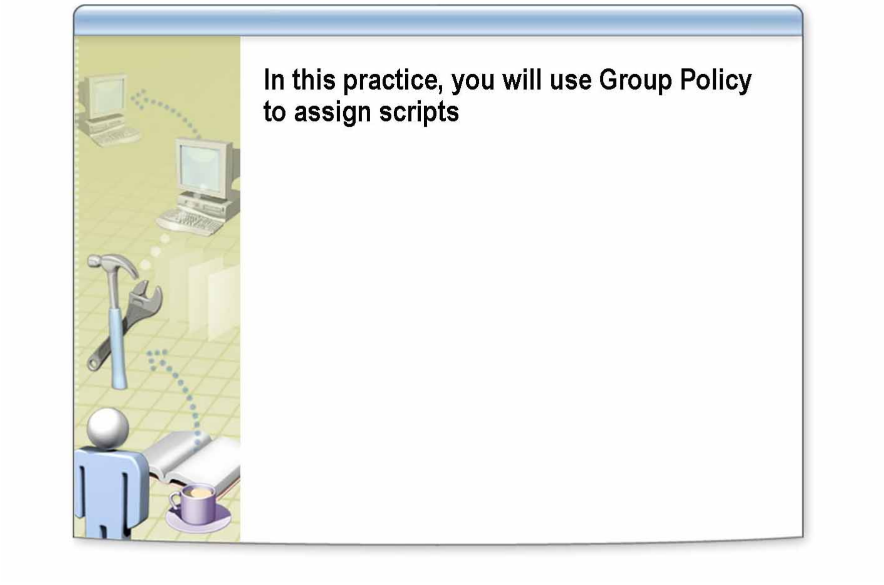
To add a script to a GPO:

1. In Group Policy Management, edit a GPO.
2. In Group Policy Object Editor, in the console tree, navigate to User Configuration/Windows Settings/Scripts (Logon/Logoff).
3. In the details pane, double-click **Logon**.
4. In the **Logon Properties** dialog box, click **Add**.
5. In the **Add a Script** dialog box, configure any of the following settings that you want to use, and then click **OK**:
   - **Script Name**. Type the path to the script or click **Browse** to locate the script file in the Netlogon share of the domain controller.
   - **Script Parameters**. Type any parameters that you want to use in the same way that you type them on the command line.

6. In the **Logon Properties** dialog box, configure any of the following settings that you want to use:
   - **Logon Scripts for**. This box lists all of the scripts that are currently assigned to the selected GPO. If you assign multiple scripts, the scripts are processed in the order that you specify. To move a script in the list, click the script, and then click either **Up** or **Down**.
   - **Add**. Click **Add** to specify any additional scripts that you want to use.
   - **Edit**. Click **Edit** to modify script information such as the name and parameters.
   - **Remove**. Click **Remove** to remove the selected script from the **Logon Scripts** list.
   - **Show Files**. Click **Show Files** to view the script files that are stored in the selected GPO.

Note Logon scripts are run in the context of the user account and not in the context of the administrator account.

Practice: Assigning Scripts with Group Policy



In this practice, you will use Group Policy to assign scripts

Objective

In this practice, you will use Group Policy to assign scripts.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*Admin account.

Note This practice focuses on the concepts in this lesson and as a result may not comply with Microsoft security recommendations. For example, this practice does not comply with the recommendation that users log on with domain user account and use the **Run as** command when performing administrative tasks. When using the Windows Explorer, you cannot use the **Run as** command.

- Open CustomMMC.
- Ensure that CustomMMC contains the following snap-ins:
  - Active Directory Users and Computers
  - Group Policy Management
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Northwind Traders wants drive S on the computers of all personnel to be mapped to a shared folder called *ComputerName* Public on your member server. You must link a GPO named *ComputerName* Logon Scripts to the called IT Test/*ComputerName* organizational unit. You then must test the logon script.

Practice

► Create a shared folder on your computer

- Folder path: D:\ComputerName Public
- Shared folder name: *ComputerName* **Public**
- Permissions: Grant Full Control permission to Administrators and grant Read and Write permissions to other users

► Create and link a GPO

- Location: IT Test/*ComputerName*
- GPO name: **Group** *ComputerName* **Logon Script**

► Edit a GPO

- GPO: *ComputerName* Scripts

► Configure a logon script Group Policy setting

- Location: User Configuration/Windows Settings/Scripts
- Group Policy setting: Logon
- Options:

1. In the **Logon Properties** dialog box, click **Show Files**.
2. In Windows Explorer, on the **Tools** menu, click **Folder Options**.
3. In the **Folder Options** dialog box, on the **View** tab, under **Advanced settings**, clear the **Hide extensions for known file types** check box, and then click **OK**.
4. In Windows Explorer, on the **File** menu, point to **New**, and then click **Text Document**.
5. Change the name of the file called New Text Document.txt to **Logon.vbs**.
6. In the message box, click **Yes**.
7. Right-click **Logon.vbs**, and then click **Edit**.
8. On the **File Download** dialog box, click **Open**.
9. In Microsoft Notepad, type the following:

```
Set objNetwork = Wscript.CreateObject("WScript.Network")
objNetwork.MapNetworkDrive "S:","\\ComputerName\ComputerName Public"
msgbox "Your Script worked!!!!!"
```

10. On the **File** menu, click **Save**.
11. Close Notepad, and then close Windows Explorer.
12. In the **Logon Properties** dialog box, click **Add**.
13. In the **Add a Script** dialog box, click **Browse**.
14. In the **Browse** dialog box, click **logon.vbs**, and then click **Open**.
15. In the **Add a Script** dialog box, click **OK**.
16. In the **Logon Properties** dialog box, click **OK**.
17. Close all windows and log off.

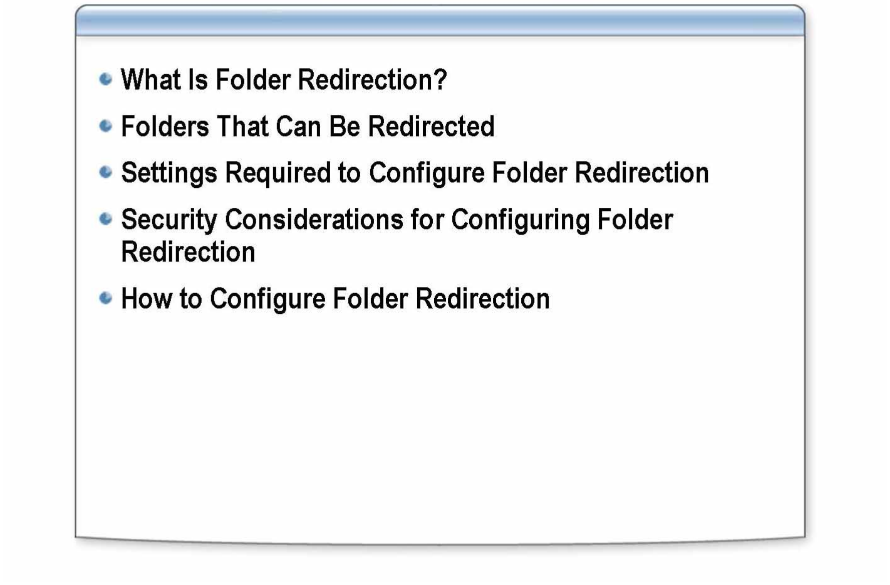
► Test the logon script

1. Log on as *ComputerName***Test** with a password of **P@ssw0rd**.
2. In the **Your Script worked!!!!** box, click **OK**.
3. Close all windows and log off.

► Delete a GPO Link

- Location: Locations/*ComputerName*
- GPO: *ComputerName* Standard Desktop
- Action: Delete the GPO Link

Lesson: Configuring Folder Redirection



- What Is Folder Redirection?
- Folders That Can Be Redirected
- Settings Required to Configure Folder Redirection
- Security Considerations for Configuring Folder Redirection
- How to Configure Folder Redirection

Introduction

Windows Server 2003 enables you to redirect folders that are part of the user profile from users' local hard disks to a central location on a server. By redirecting these folders, you can ensure that users' data is located in a central location and that users' data is available to them regardless of the computers to which they log on.

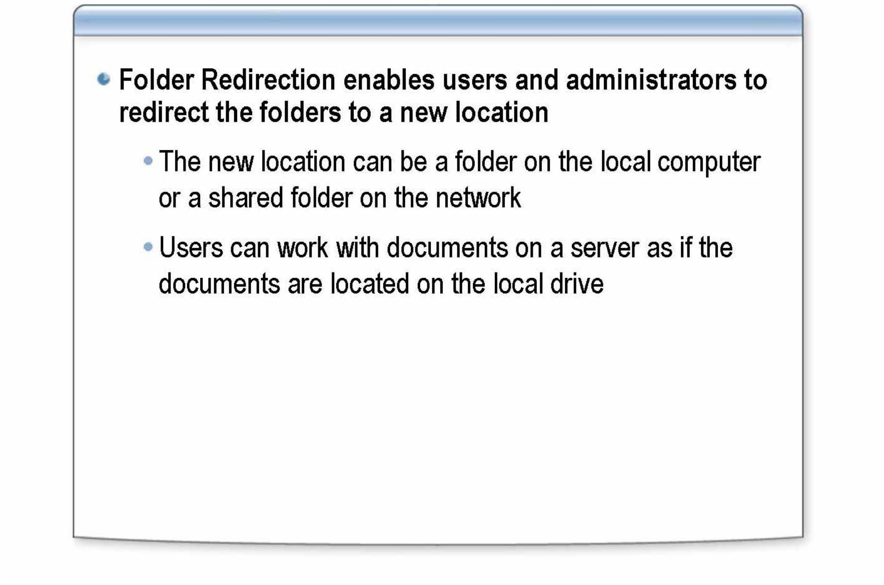
Folder Redirection makes it easier for you to manage and back up centralized data. The folders that you can redirect are My Documents, Application Data, Desktop, and Start Menu. Windows Server 2003 automatically creates these folders and makes them part of the user profile for each user account.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what Folder Redirection is.
- Explain which folders can be redirected.
- Determine which settings are required to configure Folder Redirection.
- Explain security considerations for configuring Folder Redirection.
- Configure Folder Redirection.

What Is Folder Redirection?



- Folder Redirection enables users and administrators to redirect the folders to a new location
  - The new location can be a folder on the local computer or a shared folder on the network
  - Users can work with documents on a server as if the documents are located on the local drive

Introduction

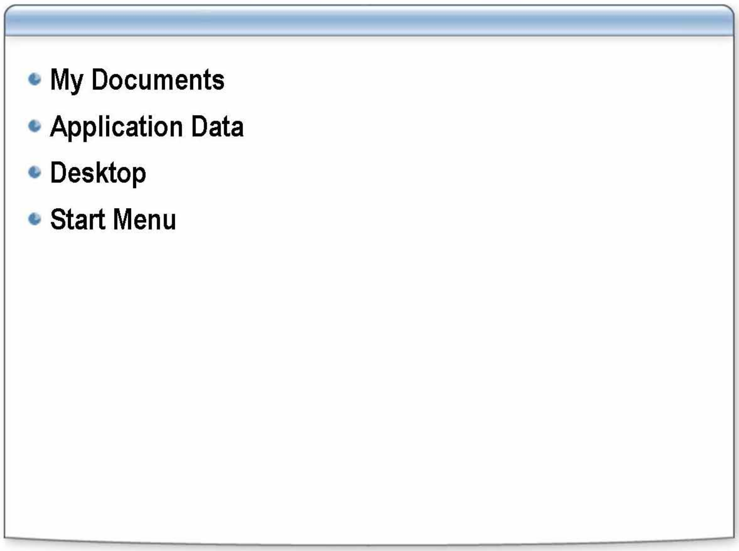
When you redirect folders, you change the storage location of folders from the local hard disk on the user's computer to a shared folder on a network file server. After you redirect a folder to a file server, it still appears to the user as if it is stored on the local hard disk. You can redirect four folders that are part of the user profile: My Documents, Application Data, Desktop, and Start Menu.

Benefits of Folder Redirection

By storing data on the network, users benefit from increased availability and frequent backup of their data. Redirecting folders has the following benefits:

- The data in the folders is available to the user regardless of the client computer that the user logs on to.
- The data in the folders is centrally stored so that the files that they contain are easier to manage and back up.
- Files that are located in redirected folders, unlike files that are part of a roaming user profile, are not copied and saved on the computer that the user logs on to. This means that when a user logs on to a client computer, no storage space is used to store these files, and that data that might be confidential does not remain on a client computer.
- Data that is stored in a shared network folder can be backed up as part of routine system administration. This is safer because it requires no action on the part of the user.
- As an administrator, you can use Group Policy to set disk quotas, limiting the amount of space that is taken by users' special folders.
- Data specific to a user can be redirected to a different hard disk on the user's local computer rather than to the hard disk holding the operating system files. This protects the user's data if the operating system must be reinstalled.

Folders That Can Be Redirected



- My Documents
- Application Data
- Desktop
- Start Menu

Introduction

You can redirect the My Documents, Application Data, Desktop, and Start Menu folders. An organization should redirect these folders to preserve important user data and settings. There are several advantages to redirecting each of these folders. The advantages vary according to your organization's needs.

Redirected folders

You can use Folder Redirection to redirect any of the following folders in a user profile:

- My Documents

  Redirecting My Documents is particularly advantageous because the folder tends to become large over time.

  Offline Files technology gives users access to My Documents even when the users are not connected to the network. This is particularly useful for people who use portable computers.

- Application Data

  A Group Policy setting controls the behavior of Application Data when client-side caching is enabled. This setting synchronizes application data that is centralized on a server with the local computer. As a result, the user can work online or offline. If any changes are made to the application data, synchronization updates the application data on the client and server.

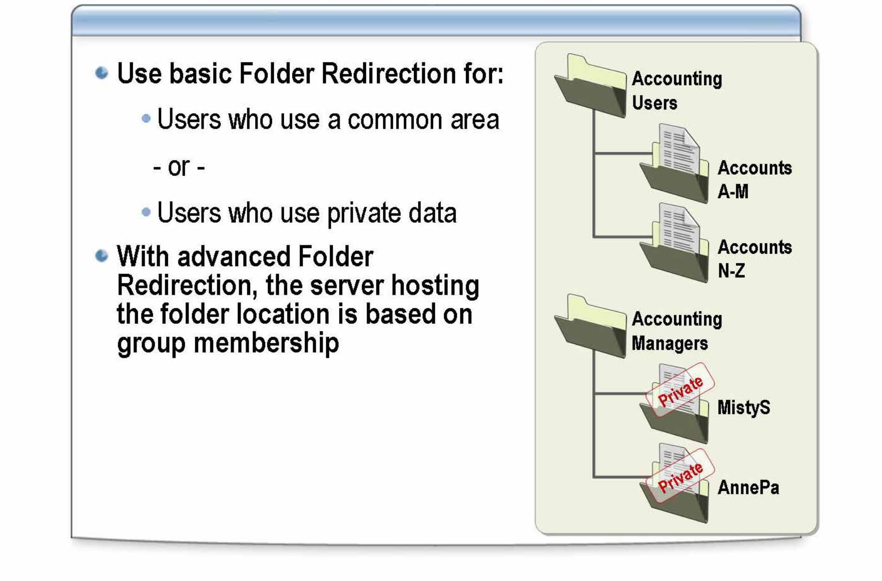
- Desktop

  You can redirect Desktop and all the files, shortcuts, and folders to a centralized server.

- Start Menu

  When you redirect Start Menu, its subfolders are also redirected.

Settings Required to Configure Folder Redirection



- Use basic Folder Redirection for:
  - Users who use a common area

  - or -

  - Users who use private data
- With advanced Folder Redirection, the server hosting the folder location is based on group membership

Introduction

There are three available settings for Folder Redirection: none, basic, and advanced. Basic Folder Redirection is for users who must redirect their folders to a common area or users that need their data to be private.

Basic Folder Redirection

You have the following basic options for Folder Redirection:

- **Redirect folder to the following location**

  All users who redirect their folders to a common area can see or use each other's data in the redirected folder. To do this, choose a **Basic** setting and set **Target folder location** to **Redirect folder to the following location**. Use this option for all redirected folders that contain data that is not private. An example of this is redirecting My Documents for a team of Accounts Receivable personnel who all share the same data.

- **Create a folder for each user under the root path**

  For users who need their redirected folders to be private, choose a **Basic** setting and set **Target folder location** to **Create a folder for each user under the root path**. Use this option for users who need their data to be private, like managers who keep personal data about employees.

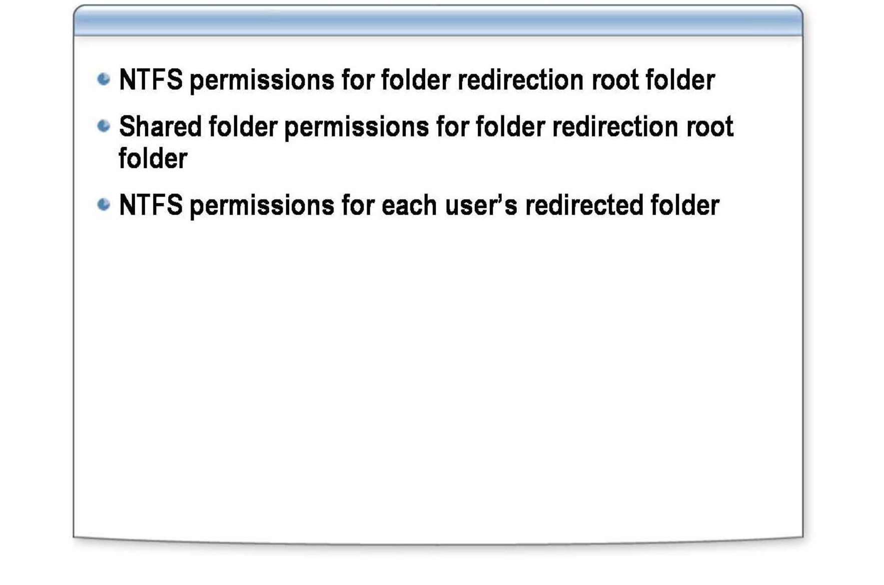
Advanced Folder Redirection

When you select **Advanced – specify locations for various user groups**, folders are redirected to different locations based on the security group membership of the users.

You have the following advanced options for Folder Redirection:

- **Select a group(s)**. This is where you specify who you want to deploy redirection to.
- **Target Folder Location**. You can choose any of the following options:
  - **Create a folder for each user under the root path**. Use this for private data.
  - **Redirect to the following location**. Use this for shared data.
  - **Redirect to the local userprofile location**. Use this for users who use a mixture of legacy client computers that are not Active Directory enabled and computers that are Active Directory enabled.
- **Root Path**. In this box, specify the server and shared folder name that you want to redirect the folders to.

Security Considerations for Configuring Folder Redirection



- NTFS permissions for folder redirection root folder
- Shared folder permissions for folder redirection root folder
- NTFS permissions for each user's redirected folder

Introduction

Folder Redirection can create folders for you, which is the recommended option. When you use this option, the correct permissions are set automatically. Usually, you do need to know what the permissions are. However, if you manually create folders, you will need to know what the permissions are. The following tables show which permissions to set for Folder Redirection.

Note Although it is not recommended, administrators can create the redirected folders before Folder Redirection creates them.

NTFS permissions required for the root folder

Set the following NTFS permissions for the root folder.

User account	Folder Redirection defaults	Minimum permissions needed
Creator/owner	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files
Administrators	No permissions	No permissions
Everyone	No permissions	No permissions
Local System	Full Control, this folder, subfolders, and files	Full Control, this folder, subfolders, and files
Security group of users who need to put data on the shared network server	N/A	List Folder/Read Data, Create Folders/Append Data - This folder only

Shared folder permissions required for the root folder

Set the following shared folder permissions for the root folder.

User account	Folder Redirection defaults	Minimum permissions needed
Everyone	Full Control	No permissions (use security group)
Security group of users who need to put data on the shared network server	N/A	Full Control

NTFS permissions required for each user's redirected folder

Set the following NTFS permissions for each user's redirected folder.

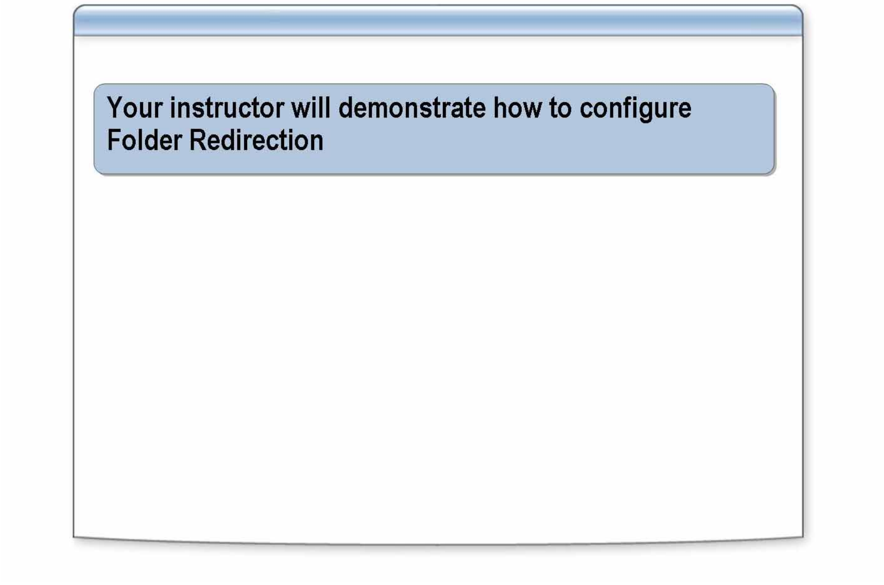
User account	Folder Redirection defaults	Minimum permissions needed
UserName	Full Control, owner of folder	Full Control, owner of folder
Local System	Full Control	Full Control
Administrators	No permissions	No permissions
Everyone	No permissions	No permissions

Note When offline folders are synchronized over the network, the data is transmitted in plain text format. The data is then susceptible to interception by network monitoring tools.

Additional reading

For more information about Folder Redirection, see "Best practices for Folder Redirection," at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_sp_bestprac_foldred.asp

How to Configure Folder Redirection



Your instructor will demonstrate how to configure Folder Redirection

Introduction

You configure Folder Redirection settings by using Group Policy Object Editor.

Procedure

To configure Folder Redirection:

1. In Group Policy Management, edit or create a GPO.
2. In Group Policy Object Editor, in the console tree, expand **User Configuration**, expand **Windows Settings**, and then expand **Folder Redirection**.

   Icons for the four folders that can be redirected are displayed.
3. Right-click the folder that you want to redirect, and then click **Properties**.
4. In the **Properties** dialog box, in the **Setting** tab, click one of the following options:
   - **Basic - Redirect everyone's folder to the same network share point.**

     All folders affected by this GPO are stored in the same shared network folder.
   - **Advanced - Redirect personal folders based on the user's membership in a Windows Server 2003 security group.**

     Folders are redirected to different shared network folders based on security group membership. For example, folders belonging to users in the Accounting group are redirected to the Accounting server, and folders belonging to users in the Marketing group are redirected to the Marketing server.
5. In the **Properties** dialog box, Click **Add**.
6. Under **Target folder location**, in the **Root path** box, type the name of the shared network folder to use, or click **Browse** to locate it.

7. On the **Settings** tab, configure the options you want to use, and then click **OK**.

   The following options for settings are available:

   - **Grant the user exclusive rights to My Documents.**

     Sets the NTFS security descriptor for the usernames unique folder to Full Control for the user and local system *only*. This means that administrators and other users do *not* have access rights to the folder. This option is enabled by default.

   - **Move the contents of My Documents to the new location.**

     Moves any document the user has in the local My Documents folder to the shared network folder. This option is enabled by default.

   - **Leave the folder in the new location when policy is removed.**

     Specifies that files remain in the new location if the GPO no longer applies. This option is enabled by default.

   - **Redirect the folder back to the local user profile location when policy is removed.**

     Specifies that the folder is moved back to the local profile location if the GPO no longer applies.

   The **My Documents Properties** dialog box has the following additional options for the My Pictures folder:

   - **Make My Pictures a subfolder of My Documents.**

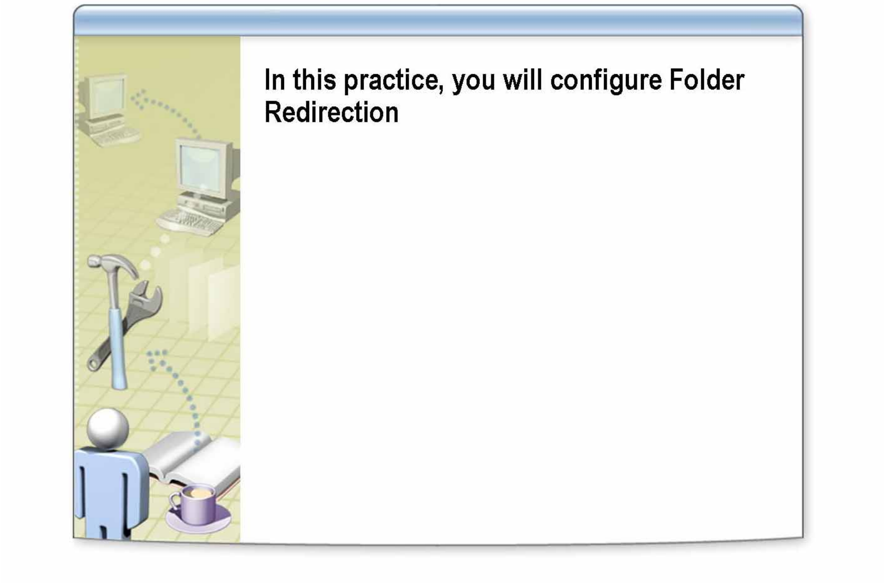
     When the My Documents folder is redirected, My Pictures remains as a subfolder of My Documents. This option is enabled by default.

   - **Do not specify administrative policy for My Pictures.**

     Group Policy does not control the location of My Pictures. The location of My Pictures is determined by the user profile.

Note You should allow the operating system to create the directory and security for Folder Redirection. Do not manually create the directory defined by username. Folder Redirection sets the appropriate permissions on the folder. If you choose to manually create folders for each user, be sure to set the permissions correctly.

Practice: Configuring Folder Redirection



In this practice, you will configure Folder Redirection

Objective

In this practice, you will configure Folder Redirection.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that CustomMMC contains the following snap-ins:
  - Active Directory Users and Computers
  - Group Policy Management
  - Computer Management (Local)
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Northwind Traders is setting up a test environment to test Folder Redirection of the My Documents folder for each city in Northwind Traders. You must create a folder called D:\UserDataTest and share it as UserDataTest$ on your *ComputerName* server.

You also must create a GPO, linked to the IT Test/*ComputerName* organizational unit, called *ComputerName* Folder Redirection Test. This GPO should redirect the My Documents folder to \\ComputerName\UserDataTest$. Do not give users exclusive rights to the redirected folder so that administrators can see if documents are added to it.

Practice

► **Create a shared folder**

- Folder path: D:\
- Name: **UserDataTest**
- Share name: **UserDataTest$**
- Shared folder permissions: Authenticated Users = Full Control
- NTFS permissions: Default

► **Create a user account for the test (If one does not already exist)**

- Organizational unit: Locations/*ComputerName*
- First name: *ComputerName*
- Last name: **Test**
- User logon name: *ComputerName***Test**
- Password: **P@ssw0rd**

► **Link a GPO**

- Organizational unit: Locations/*ComputerName*
- GPO name: *ComputerName* **Folder Redirection**
- Security filtering: Authenticated Users

► **Edit a GPO**

- GPO: *ComputerName* Folder Redirection

► **Configure Folder Redirection**

- Location: /User Configuration/Windows Settings/Folder Redirection
- Group Policy setting: My Documents
- Options:
  - Target folder setting: **Basic – Redirect everyone's folder to the same location**
  - Target folder location: **Create a folder for each user under the root path**
  - Root path: \\ComputerName\UserDataTest$
  - Redirect settings: Clear the **Grant the user exclusive rights to My Documents** check box
  - Policy Removal: **Redirect the folder back to the local userprofile location when policy is removed**
  - My Pictures Preferences: **Make My Pictures a subfolder of My Documents**

► Test the Folder Redirection of My Documents

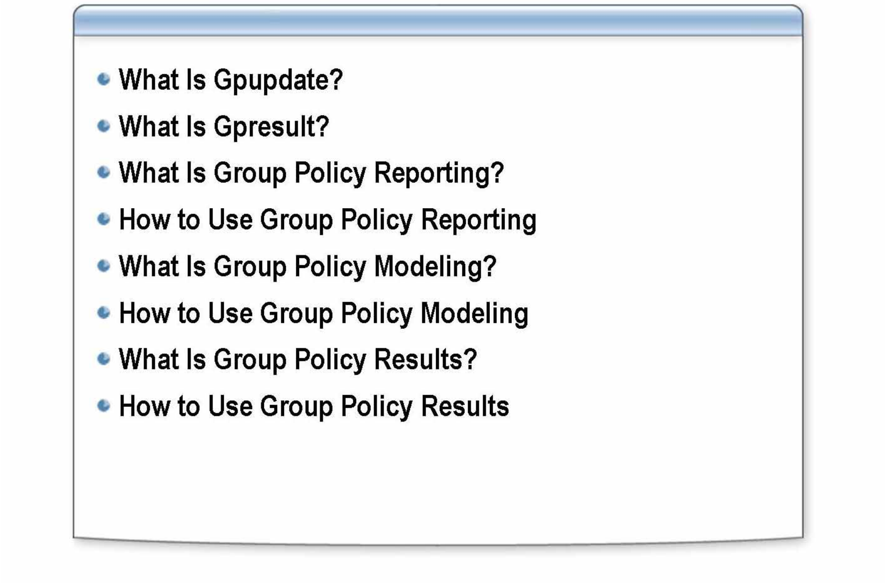
1. Log off.
2. Log on as *ComputerName***Test** with a password of **P@ssw0rd**.
3. In the message box, click **OK**.
4. Click **Start**.
5. Right-click **My Documents**, and then click **Properties**.
6. In the **My Document Properties** dialog box, verify that the following is in the **Target** box:

   \\*ComputerName***\userdatatest$\\***ComputerName*test\My Documents
7. Click **OK**.
8. Click **Start**, and then click **My Documents**.
9. In My Documents, on the **File** menu, point to **New**, and then click **Text Document**.
10. Close all windows and log off.

► Test the permissions of redirected folders

1. Log on as *ComputerName***Admin** with a password of **P@ssw0rd**.
2. Go to: **D:\UserDataTest**.
3. In D:\UserDataTest\ComputerNameTest, double-click *ComputerName***Test's Documents**.
4. In D:\UserDataTest\ComputerNameTest\ComputerNameTest's Documents, verify that the file called New Text Document.txt was created.
5. Close all windows and log off.

Lesson: Determining Applied GPOs



- What Is Gpupdate?
- What Is Gpresult?
- What Is Group Policy Reporting?
- How to Use Group Policy Reporting
- What Is Group Policy Modeling?
- How to Use Group Policy Modeling
- What Is Group Policy Results?
- How to Use Group Policy Results

Introduction

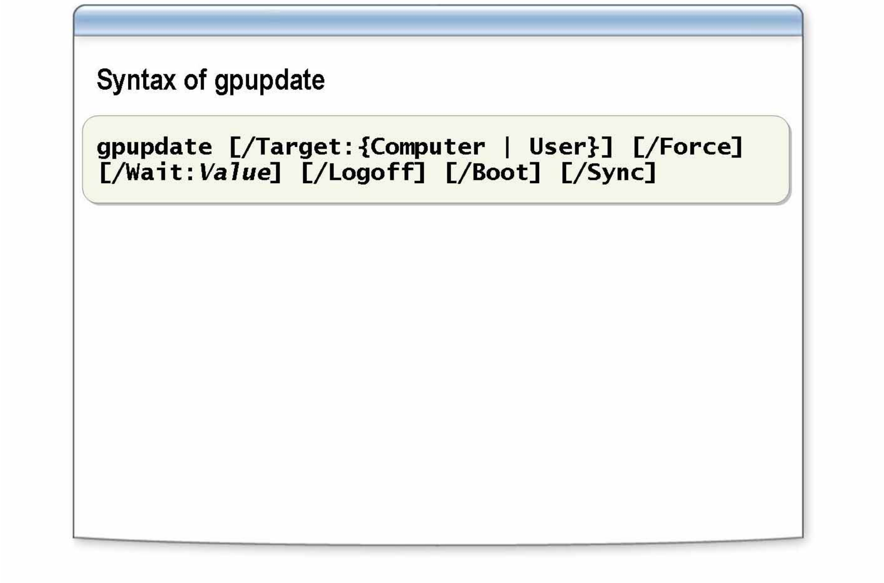
Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an Active Directory environment, Group Policy is applied to users or computers on the basis of their membership in sites, domains, or organizational units.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what **gpupdate** is.
- Explain what **gpresult** is.
- Explain what is group policy reporting.
- Use group policy reporting.
- Explain what is group policy modeling.
- Use group policy modeling.
- Explain what is group policy results.
- Use group policy results.

What Is Gpupdate?



Syntax of gpupdate

```
gpupdate [/Target:{Computer | User}] [/Force]
[/Wait:Value] [/Logoff] [/Boot] [/Sync]
```

Introduction

Gpupdate is a command-line tool that refreshes local Group Policy settings and Group Policy settings that are stored in Active Directory, including security settings. By default, security settings are refreshed every 90 minutes on a workstation or server and every five minutes on a domain controller. You can run **gpupdate** to test a Group Policy setting or to force a Group Policy setting.

Examples of gpupdate

The following examples show how you can use the **gpupdate** command:

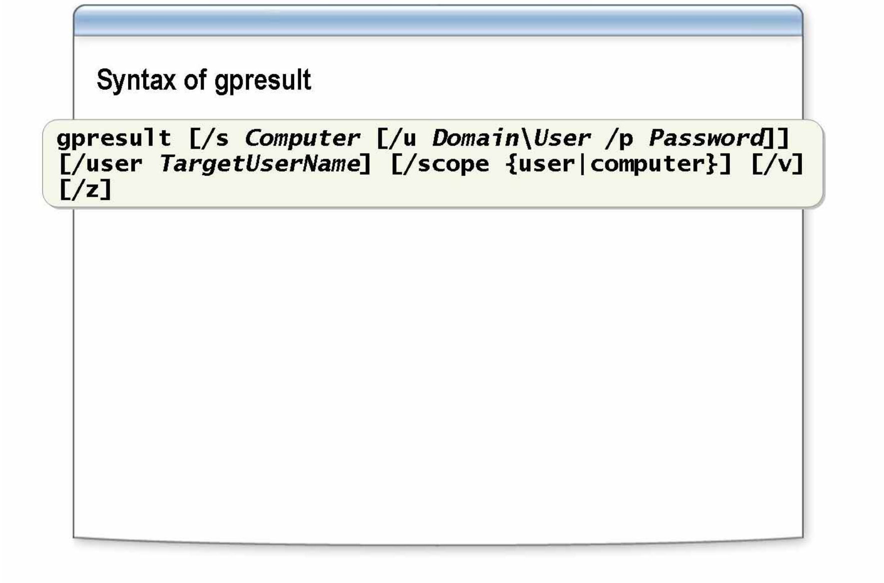
- C:\gpupdate
- C:\gpupdate /target:computer
- C:\gpupdate /force /wait:100
- C:\gpupdate /boot

Parameters of gpupdate

Gpupdate has the following parameters.

Value	Description
/**Target**:{**Computer** | **User**}	Specifies that only user or only computer policy settings are refreshed. By default, both user and computer policy settings are refreshed.
/**Force**	Reapplies all policy settings. By default, only policy settings that have changed are reapplied.
/**Wait**:{*Value*}	Sets the number of seconds to wait for policy processing to finish. The default is 600 seconds. The value '0' means not to wait. The value '-1' means to wait indefinitely.
/**Logoff**	Causes a logoff after the Group Policy settings are refreshed. This is required for those Group Policy client-side extensions that do not process policy settings during a background refresh cycle but do process policy settings when a user logs on. Examples include user-targeted Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require a logoff.
/**Boot**	Causes the computer to restart after the Group Policy settings are refreshed. This is required for those Group Policy client-side extensions that do not process policy during a background refresh cycle but do process policy when the computer starts. Examples include computer-targeted Software Installation. This option has no effect if there are no extensions called that require the computer to restart.
/**Sync**	Causes the next foreground policy setting to be applied synchronously. Foreground policy settings are applied when the computer starts and when the user logs on. You can specify this for the user, computer, or both by using the /**Target** parameter. The /**Force** and /**Wait** parameters are ignored.

What Is Gpresult?



Syntax of gpresult

```
gpresult [/s Computer [/u Domain\User /p Password]]
[/user TargetUserName] [/scope {user|computer}] [/v]
[/z]
```

Introduction

Because you can apply overlapping levels of policy settings to any computer or user, Group Policy generates a resulting set of policies at logon. **Gpresult** displays the resulting set of policies that are enforced on the computer for the specified user at logon.

The **gpresult** command displays Group Policy settings and Resultant Set of Policy (RSoP) data for a user or a computer. You can use **gpresult** to see what policy setting is in effect and to troubleshoot problems.

Examples of gpresult

The following examples show how you can use the **gpresult** command:

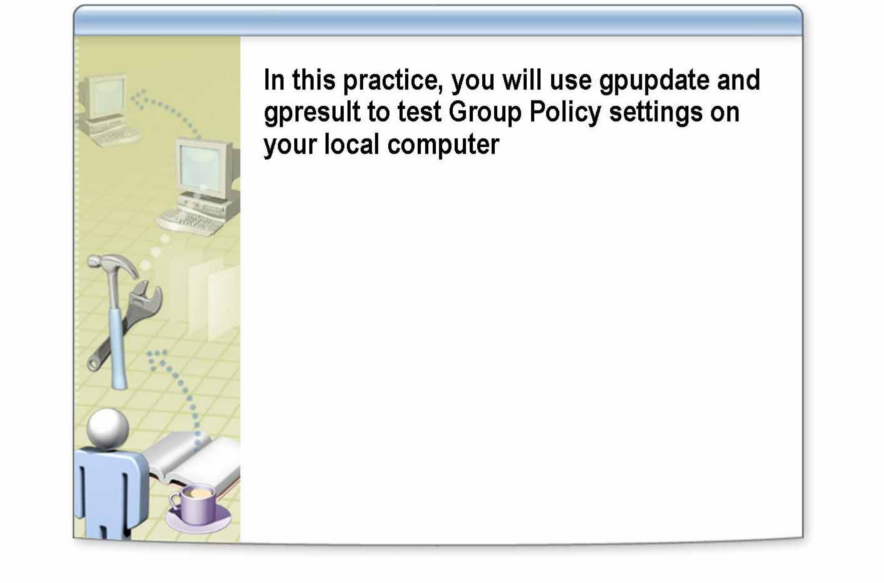
- C:\gpresult /user targetusername /scope computer
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /scope USER
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /z >policy.txt
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23

Parameters of gpresult

Gpresult has the following parameters.

Value	Description
/**s** *Computer*	Specifies the name or IP address of a remote computer. Do not use backslashes. The default is the local computer.
/**u** *Domain*/*User*	Runs the command with the account permissions of the user that is specified by *User* or *Domain*/*User*. The default is the permissions of the user who is currently logged on to the computer that issues the command.
/**p** *Password*	Specifies the password of the user account that is specified in the /**u** parameter.
/**user** *TargetUserName*	Specifies the user name of the user whose RSoP data is to be displayed.
/**scope** {**user**|**computer**}	Displays either user or computer policy settings. Valid values for the /**scope** parameter are **user** or **computer**. If you omit the /**scope** parameter, **gpresult** displays both user and computer policy settings.
/**v**	Specifies that the output will display verbose policy information.
/**z**	Specifies that the output will display all available information about Group Policy. Because this parameter produces more information than the /**v** parameter, redirect output to a text file when you use this parameter (for example, you can type **gpresult /z >policy.txt**).
/**?**	Displays help in the command prompt window.

Practice: Using Gpupdate and Gpresult



In this practice, you will use gpupdate and gpresult to test Group Policy settings on your local computer

Objective

In this practice, you will use **gpupdate** and **gpresult** to test policy settings on your local computer.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (example: LondonAdmin).
- Ensure that CustomMMC contains Group Policy Management.
- Open a command prompt with the Run as command.

  From Run type **runas /user:nwtraders\***ComputerName***Admin cmd** and click **OK**. When prompted for a password type **P@ssw0rd**, and press **ENTER**.
- Ensure that you have a user account created named *ComputerName*Test.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

You are testing some Group Policy settings on your local computer. You do not want to wait for the refresh interval to see the Group Policy update, so you must run the **gpupdate** command.

Gpupdate with no switches

► **Use gpupdate with no switches**

- From a command prompt, type **gpupdate**

► **Use gpupdate with the /force switch**

- From a command prompt, type **gpupdate /force**. If prompted to logoff, type **N** and press **ENTER**.

Scenario

You must use **gpresult** to see which Group Policy settings are in effect on your server so that you can help troubleshoot remote computers.

Gpresult with no switches

► Use gpresult with no switches

1. From a command prompt, type **gpresult**
2. Scroll up the command prompt window to see the results of the Group Policy settings that have been applied to your computer.

► Use gpresult with the /scope switch

1. From a command prompt, type **gpresult /scope computer**
2. Scroll up the command prompt window to see the results of the Group Policy settings that have been applied to your computer.
3. From a command prompt, type **gpresult /scope user**
4. Scroll up the command prompt window to see the results of the Group Policy settings that have been applied to your computer.

► Send the gpresult data to a text file with the /z switch

1. From a command prompt, type **gpresult /z >gp.txt**
2. From a command prompt, type **notepad gp.txt**
3. In Notepad, scroll through the results, and then close Notepad.

Scenario

Your boss wants you to test a Group Policy setting. The Group Policy setting removes the **Search** option from the **Start** menu and only affects your local computer. When you are done, your boss needs a report to see that the changes were applied correctly.

Testing group policy settings

► Log on as *ComputerName*Test and run CustomMMC

1. Log on as *ComputerName***Test** with a password of **P@ssw0rd**.
2. Open C:\MOC\CustomMMC with the **Run as** command by using the user account nwtraders*ComputerName*Admin.
3. Type your password, and then click **OK**.

► Create and link a GPO

- Location: Locations/*ComputerName*
- GPO name: *ComputerName* **gpresult**

► Edit a GPO

- GPO: *ComputerName* gpresult

► Remove Search menu from Start Menu Properties

- Location: User Configuration/Administrative Templates/Start Menu and Taskbar
- Group Policy setting: **Remove Search menu from Start Menu Properties**
- Option: **Enabled**

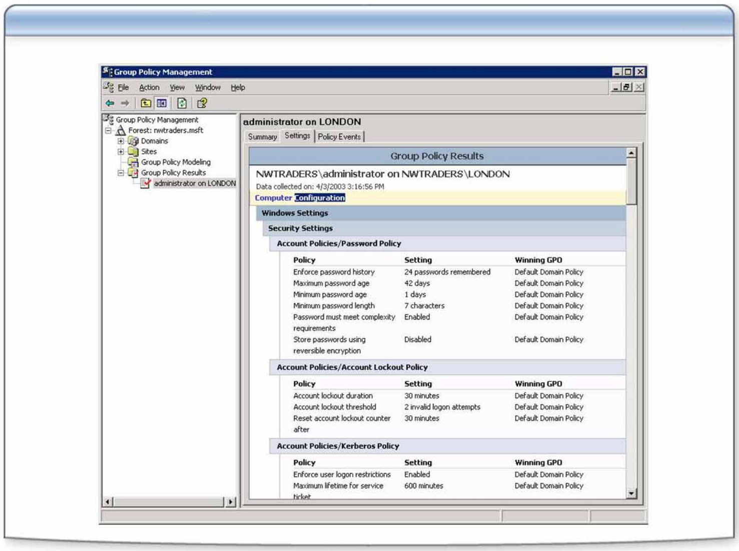
► Test to see if the Group Policy setting has been applied

1. From a command prompt, type **gpresult /z >1.txt**
2. From a command prompt, type **notepad 1.txt**
3. In Notepad, on the **Edit** menu, click **Find**.
4. In the **Find** dialog box, in the **Find what** box, type *ComputerName* **gpresult** and then click **Find Now**.
5. In Notepad, verify that the message says **Cannot find "*ComputerName* gpresult"** and then click **OK**.
6. In the **Find** dialog box, click **Cancel**, and then close Notepad.
7. From a command prompt, type **gpupdate**

► Test again to see if the Group Policy setting has been applied

1. From a command prompt, type **gpresult /z >2.txt**
2. From a command prompt, type **notepad 2.txt**
3. In Notepad, on the **Edit** menu, click **Find**.
4. In the **Find** dialog box, in the **Find what** box, type *ComputerName* **gpresult** and then click **Find Now**.
5. In Notepad, verify that ***ComputerName*** **gpresult** is highlighted under **Applied Group Policy Object**.
6. In the **Find** dialog box, click **Find Next**.
7. In Notepad, verify that ***ComputerName*** **gpresult** is highlighted under **Administrative Templates**.
8. In the **Find** dialog box, click **Cancel**, and then close Notepad.
9. Close all windows and log off.

What Is Group Policy Reporting?



administrator on LONDON

Group Policy Results

NWTRADERS\administrator on NWTRADERS\LONDON

Data collected on: 4/3/2003 3:16:56 PM

Computer Configuration

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout duration	30 minutes	Default Domain Policy
Account lockout threshold	2 invalid logon attempts	Default Domain Policy
Reset account lockout counter after	30 minutes	Default Domain Policy

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy

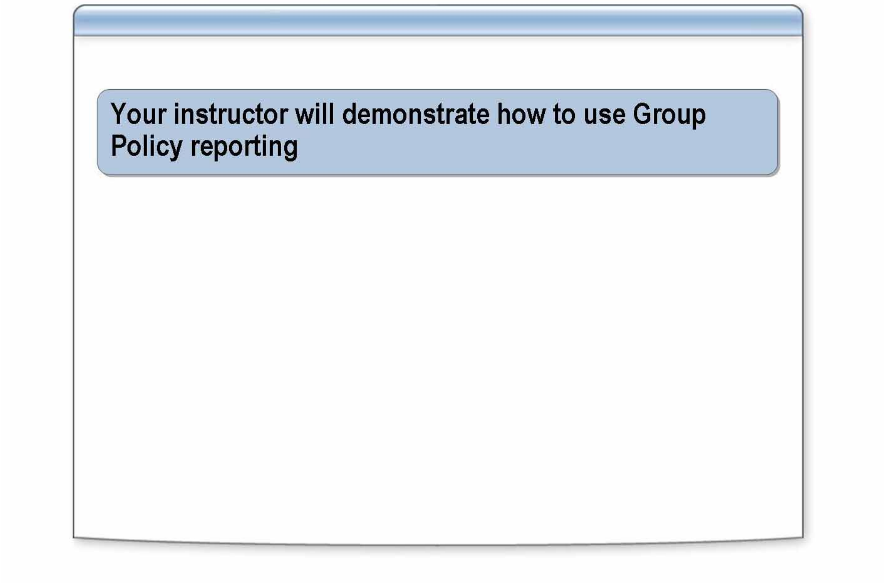
Definition

A systems administrator can make hundreds of changes to a GPO. To verify changes made to a GPO without actually opening the GPO and expanding every folder, you can generate a Hypertext Markup Language (HTML) report that lists the items in the GPO that are configured.

Settings tab

The **Settings** tab of the details pane for a GPO or GPO link in Group Policy Management shows an HTML report that displays all the defined settings in the GPO. Any user with read access to the GPO can generate this report. If you click **show all** at the top of the report, the report is fully expanded, and all settings are shown. Also, using a context menu, you can print the reports or save them to a file as either HTML or Extensible Markup Language (XML).

How to Use Group Policy Reporting



Your instructor will demonstrate how to use Group Policy reporting

Introduction

Use the following procedure to determine applied Group Policy settings by using Group Policy reporting.

Procedure

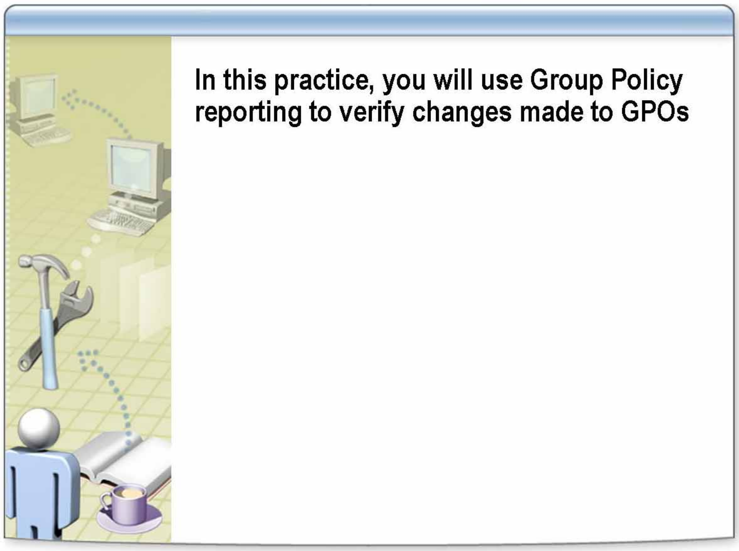
To use Group Policy reporting:

1. In Group Policy Management, in the console tree, click the GPO that you want to generate a report for.

   You must expand the forest, domain, and domain name to locate the GPO that you want to generate a report for.

2. In the details pane, click the **Settings** tab.

Practice: Using Group Policy Reporting



In this practice, you will use Group Policy reporting to verify changes made to GPOs

Objective

In this practice, you will use Group Policy reporting to verify changes made to GPOs.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (example: LondonAdmin).
- Ensure that CustomMMC contains Group Policy Management.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

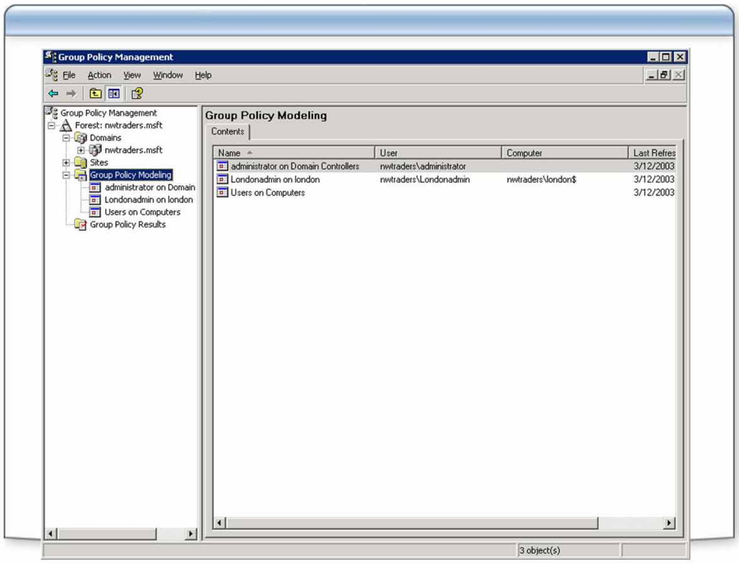
You have been asked to document the Group Policy settings for the Default Domain Policy GPO.

Practice

► **View the report for Default Domain Policy**

1. In Group Policy Management, in the console tree, expand **Group Policy Objects**.
2. Click **Default Domain Policy**.
3. In the details pane, click the **Settings** tab.
4. From the **Internet Explorer** box, click **Close**.
5. Review the Group Policy settings for Default Domain Policy.
6. Right-click anywhere in the report, and then click **Save Report**.
7. In the **Save GPO Report** dialog box, click **Save**.

What Is Group Policy Modeling?



Group Policy Modeling

Name	User	Computer	Last Refres
administrator on Domain Controllers	nwtraders\administrator		3/12/2003
Londonadmin on london	nwtraders\Londonadmin	nwtraders\london$	3/12/2003
Users on Computers			3/12/2003

Introduction

Windows Server 2003 enables you to simulate a GPO deployment that is applied to users and computers before you actually deploy the GPO. The simulation creates a report that takes into account the user's organizational unit, the computer's organizational unit, and any group membership or Windows Management Instrumentation (WMI) filtering. It also takes into account any Group Policy inheritance issues or conflicts.

Requirements

If you want to use Group Policy modeling, there must be a Windows Server 2003 domain controller in the forest. This is because the simulation is performed by a service that is only present on Windows Server 2003 domain controllers.

Results of Group Policy Modeling

To perform a Group Policy Modeling query, the user uses the Group Policy Modeling Wizard. After the user completes the Group Policy Modeling Wizard, a new node in the console tree of Group Policy Management appears under **Group Policy Modeling** to display the results. The **Contents** tab in the details pane for Group Policy Modeling displays a summary of all Group Policy Modeling queries that the user has performed.

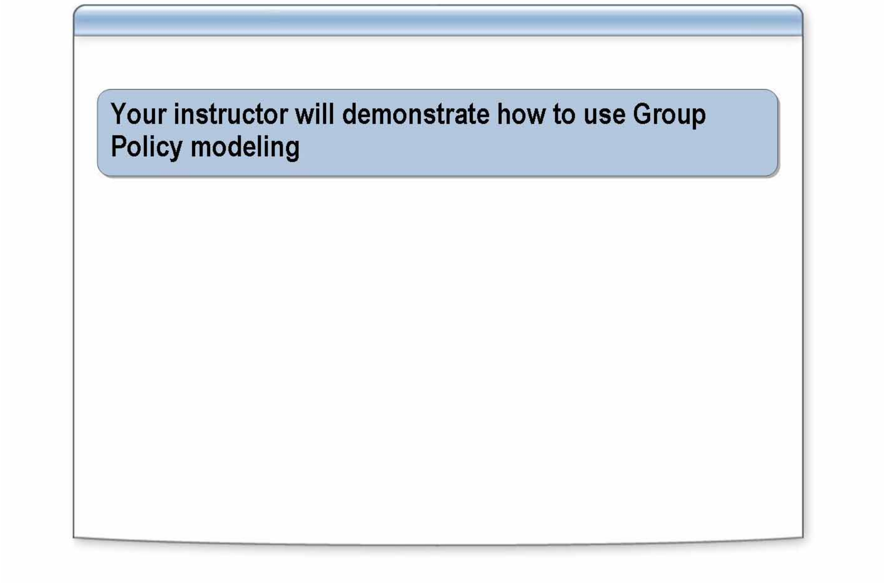
For each query, Group Policy Management shows the following data:

- **Name**. This is the user-supplied name of the modeling results.
- **User**. This is the user object (or the organizational unit where the user object is located) that the modeling query is based on.
- **Computer**. This is the computer object (or the organizational unit where the computer object is located) that the modeling query is based on.
- **Last refresh time**. This is the last time the modeling query was refreshed.

For each query, the details pane for the node contains the following three tabs:

- **Summary**. This contains an HTML report of the summary information, including the list of GPOs, security group membership, and WMI filters.
- **Settings**. This contains an HTML report of the policy settings that were applied in this simulation.
- **Query**. This lists the parameters that were used to generate the query.

How to Use Group Policy Modeling



Your instructor will demonstrate how to use Group Policy modeling

Introduction

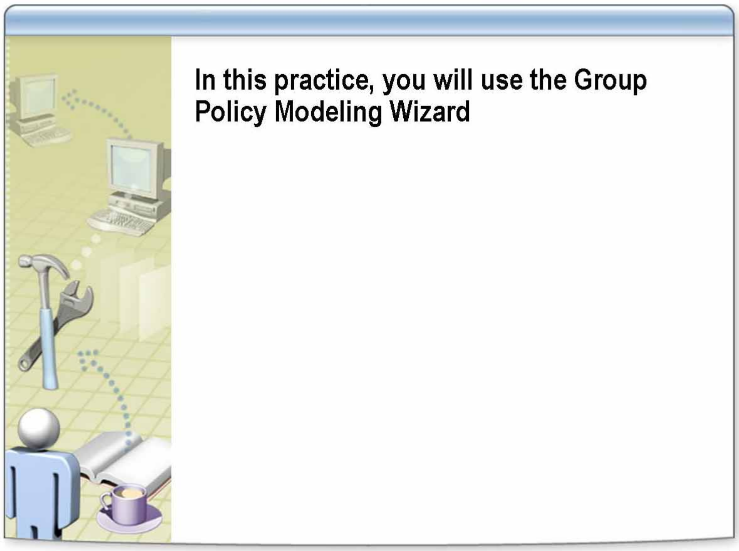
To determine the applied Group Policy settings, you use the Group Policy Modeling Wizard. This enables you to simulate the results of applying a new GPO before actually applying it.

Procedure

To use Group Policy Modeling:

1. In Group Policy Management, in the console tree, double-click the forest in which you want to create a Group Policy Modeling query, right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
2. In the Group Policy Modeling Wizard, click **Next** and then enter the following information:
   - If you want to model what the effect of a new GPO is for a user or computer, enter the name of the container for the user or computer.
   - If you want to model what the effect of a new GPO is for a specific user or computer account that will be migrated to a different organizational unit, enter the user or computer name. The wizard then prompts you for the destination of that user or computer.
3. When finished, click **Finish**.

Practice: Using Group Policy Modeling Wizard



In this practice, you will use the Group Policy Modeling Wizard

Objective

In this practice, you will use the Group Policy Modeling Wizard.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (example: LondonAdmin).
- Ensure that CustomMMC contains Group Policy Management.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Your manager needs to know how Group Policy will be applied if your *ComputerName* computer account is moved to the IT Test/*ComputerName* organizational unit.

Practice

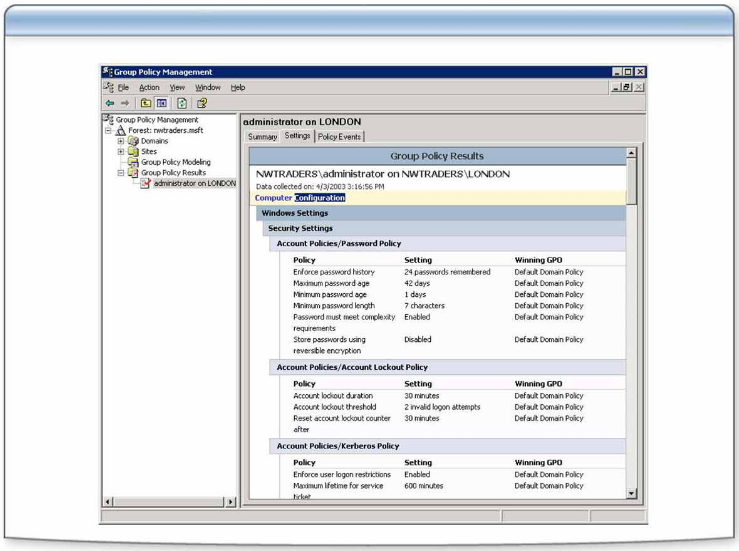
► Generate a Group Policy Modeling report

1. In Group Policy Management, in the console tree, right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
2. In the Group Policy Modeling Wizard, on the **Welcome** page, click **Next**.
3. On the **Domain Controller Selection** page, click **Next**.
4. On the **User and Computer Selection** page, under **Computer information**, click **Computer**, type **nwtraders\**_ComputerName_ and then click **Next**.
5. On the **Advanced Simulation Options** page, click **Next**.
6. On the **Alternative Active Directory Paths** page, in the **Computer location** box, type **OU=**_ComputerName_**,OU=IT Test,DC=nwtraders, DC=msft** and then click **Next**.
7. On the **Computer Security Groups** page, click **Next**.
8. On the **WMI Filters for Computers** page, click **Next**.
9. On the **Summary of Selections** page, click **Next**.
10. Click **Finish**.
11. From the **Internet Explorer** box, click **Close**.

► View the Group Policy Modeling report

1. On the **Summary** tab, look through the report.
2. From the ***ComputerName*** details pane, click the **Settings** tab.
3. From the **Internet Explorer** box, click **Close**.
4. Look through the report.
5. Click the **Query** tab.
6. Look through the report.

What Is Group Policy Results?



administrator on LONDON

Group Policy Results

NWTRADERS\administrator on NWTRADERS\LONDON

Data collected on: 4/3/2003 3:16:56 PM

Computer Configuration

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout duration	30 minutes	Default Domain Policy
Account lockout threshold	2 invalid logon attempts	Default Domain Policy
Reset account lockout counter after	30 minutes	Default Domain Policy

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy

Introduction

The data that is presented in Group Policy Results is similar to Group Policy Modeling data. However, unlike Group Policy Modeling data, this data is not a simulation. It is the actual RSoP data obtained from the target computer. By default, this access is granted to all users on Microsoft Windows XP, but not on Windows Server 2003.

Requirements

Unlike Group Policy Modeling, the data in Group Policy Results is obtained from the client and is not simulated on the domain controller. Technically, a Windows Server 2003 domain controller is not required to be in the forest if you want to access Group Policy Results. However, the client must be running Windows XP or Windows Server 2003. It is not possible to get Group Policy Results data for a client running Microsoft Windows 2000.

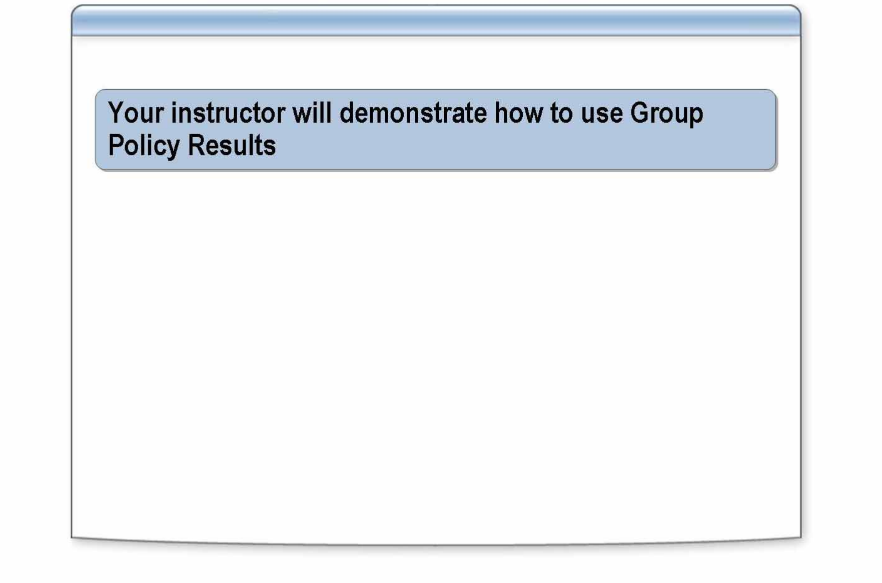
Note By default, only users with local administrator privileges on the target computer can remotely access Group Policy Results data. To gather this data, the user performing the query must have access to remotely view the event log.

Results of Group Policy Results

Each Group Policy Results query is represented by a node under the Group Policy Results container in the console tree of Group Policy Management. The details pane for each node has the following three tabs:

- **Summary**. This contains an HTML report of the summary information including the list of GPOs, security group membership, and WMI filters.
- **Settings**. This contains an HTML report of the policy settings that were applied.
- **Events**. This shows all policy-related events from the target computer.

How to Use Group Policy Results



Your instructor will demonstrate how to use Group Policy Results

Introduction

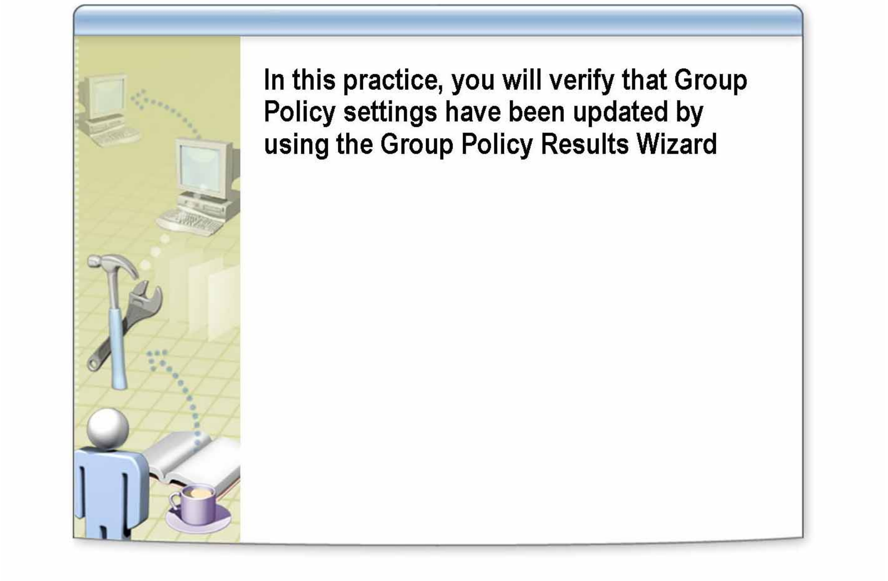
Use the following procedure to use Group Policy Results.

Procedure

To use Group Policy Results:

1. In Group Policy Management, in the console tree, double-click the forest in which you want to create a Group Policy Results query, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
2. In the Group Policy Results Wizard, click **Next** and then enter the appropriate information.
3. After completing the wizard, click **Finish**.

Practice: Using Group Policy Results Wizard



In this practice, you will verify that Group Policy settings have been updated by using the Group Policy Results Wizard

Introduction

In this practice, you will verify that policy settings have been updated by using the Group Policy Results Wizard.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (example: LondonAdmin).
- Ensure that CustomMMC contains Group Policy Management.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

You want to verify that policy settings are being updated on your student computer. You want to look at the computer policy setting being applied to your computer with the *ComputerName*Admin account.

Practice

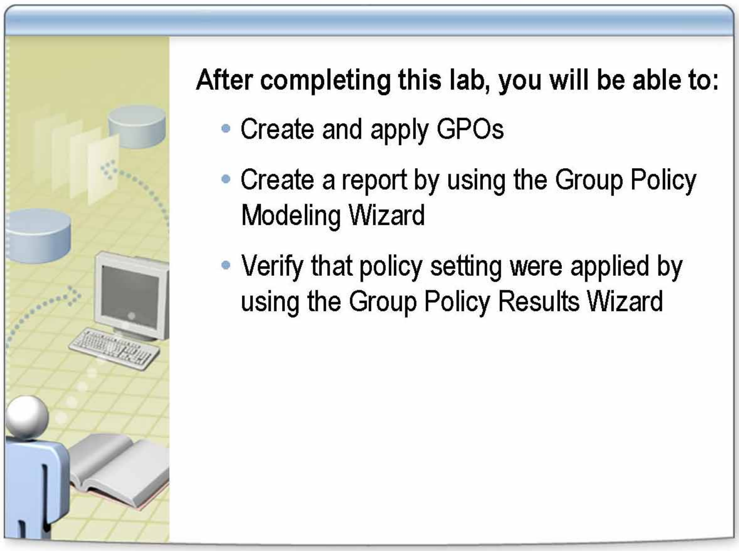
► Generate a Group Policy Results report

1. In Group Policy Management, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
2. In the Group Policy Results Wizard, on the **Welcome** page, click **Next**.
3. On the **Computer Selection** page, click **Next**.
4. On the **User Selection** page, click **Select a specific user**, click **NWTRADERS\***ComputerName***Admin**, and then click **Next**.
5. On the **Summary of Selections** page, click **Next**.
6. On the **Completing the Group Policy Results Wizard** page, click **Finish**.
7. From the **Internet Explorer** dialog box, click **Close**.

► View a Group Policy Results report

1. On the **Summary** tab look through the report.
2. On the **Policy Events** tab, double-click **Source**.
3. Scroll down to see the source labeled SceCli.
4. Double-click the first event with the source labeled SceCli.
5. In the **Event Properties** dialog box, notice the date and time the security policy setting was applied successfully.
6. Click the down arrow to see the next event, notice the date and time the security policy setting was applied successfully, and then click **OK**.

Lab A: Using Group Policies Reports



After completing this lab, you will be able to:

- Create and apply GPOs
- Create a report by using the Group Policy Modeling Wizard
- Verify that policy setting were applied by using the Group Policy Results Wizard

Objectives

After completing this lab, you will be able to:

- Create and apply GPOs.
- Create a report by using the Group Policy Modeling Wizard.
- Verify that policy settings were applied by using the Group Policy Results Wizard.

Instructions

Before you begin this lab:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (example: LondonAdmin).
- Ensure that CustomMMC contains the following snap-ins:
  - Active Directory Users and Computers
  - Computer Management (Local)
  - Group Policy Management
- Ensure that you have organizational units named Laptops and Desktops in the Locations/*ComputerName*/Computers organizational unit.

Scenario

Northwind Traders has finished testing GPOs and must configure multiple GPOs that will affect many users and computers in your city. You must create and apply GPOs by using all of the properties in the following tables. After you configure all of the GPOs, you must create reports to show that the appropriate groups are not affected by certain policy settings and that the proper policy settings are applied.

Estimated time to complete this lab: 50 minutes

Exercise 1
Creating a GPO for Standard Desktop Computers

In this exercise, you will create a GPO.

Scenario

Northwind Traders has finished testing a GPO that enables the Marketing personnel to use a standard desktop computer. Create a GPO with the following properties.

Properties	Special Instructions
1. Create a GPO.	▪ GPO name: *ComputerName* **Standard Desktop 2**
2. Create a GPO link.	▪ Location: Locations/*ComputerName* ▪ GPO name: *ComputerName* Standard Desktop 2
3. Configure security filtering.	▪ Location: Locations/*ComputerName* ▪ GPO: *ComputerName* Standard Desktop 2 ▪ Security Filtering: • Remove Authenticated Users • Add G NWTraders Marketing Personnel • Deny the Apply Group Policy permission to G NWTraders Marketing Managers
4. Set the following Group Policy settings to **Enabled**.	▪ GPO: *ComputerName* Standard Desktop 2 ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Windows Components/Application Compatibility/Prevent access to 16-bit applications ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Windows Components/Windows Explorer/Remove Search button from Windows Explorer ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Windows Components/ Windows Explorer/Remove Hardware tab ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Start Menu and Taskbar/Remove links and access to Windows Update ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Start Menu and Taskbar/Remove Network Connections from Start Menu ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Start Menu and Taskbar/Remove Run from Start Menu

Exercise 2
Creating a GPO for Folder Redirection

In this exercise, you will set Deny permissions for all temporary employees of Northwind Traders so that they do not receive the *ComputerName* Folder Redirection GPO.

Scenario

Northwind Traders has finished testing a GPO for Folder Redirection. You must create a GPO that redirects folders of Accounting personnel only.

Tasks	Special instructions
1. Create a GPO.	▪ GPO name: *ComputerName* **Accounting Folder Redirection**
2. Create a GPO link.	▪ Location: Locations/*ComputerName*/Users ▪ GPO name: *ComputerName* Accounting Folder Redirection
3. Configure security filtering.	▪ Location: Locations/*ComputerName* ▪ GPO: *ComputerName* Accounting Folder Redirection ▪ Security Filtering: • Remove Everyone • Add DL NWTraders Accounting Personnel Full Control
4. Create a shared folder.	▪ Folder Path: D:\Accounting Data ▪ Share Name: \\ComputerName\Accounting Data$ ▪ Permissions: Grant Full Control permission to DL NWTraders Accounting Personnel Full Control
5. Configure Group Policy settings.	▪ Location: Locations/*ComputerName*/Users ▪ GPO: *ComputerName* Accounting Folder Redirection ▪ Location of Group Policy setting: User Configuration/Windows Settings/Folder Redirection/My Documents ▪ Options: • Target folder setting: **Basic – Redirect everyone's folder to the same location** • Target folder location: **Create a folder for each user under the root path** • Root Path: \\***ComputerName*\\Accounting Data$** • Redirection settings: • **Grant the user exclusive user rights to My Documents** • **Redirect the folder back to the local userprofile when the policy is removed**

Exercise 3
Creating a GPO for Laptop Computers

In this exercise, you will configure a GPO for laptop computers.

Scenario

Northwind Traders has finished testing a GPO for laptop computers. Create a GPO with the following properties that will be enforced on all laptop computers.

Tasks	Special instructions
1. Create a GPO	▪ GPO name: *ComputerName* **Laptop Settings**
2. Create a GPO link.	▪ Location: Locations/*ComputerName*/Computers/Laptops ▪ GPO name: *ComputerName* Laptop Settings
3. Set the following Group Policy settings to **Enabled**.	▪ GPO: *ComputerName* Laptop Settings ▪ Location of Group Policy setting: User Configuration/ Administrative Templates/System/Power Management/Prompt for password on resume from hibernation / suspend ▪ Location of Group Policy setting: User Configuration/ Administrative Templates/Network/Offline Files/Synchronize all offline files when logging on ▪ Location of Group Policy setting: User Configuration/ Administrative Templates/Network/Offline Files/Synchronize all offline files before logging off

Exercise 4
Creating a GPO for Desktop Computers

In this exercise, you will configure a GPO for desktop computers.

Scenario

Northwind Traders has finished testing a GPO for desktop computers. Create a GPO with the following properties that will be enforced on all desktop computers.

Tasks	Special instructions
1. Create a GPO.	▪ GPO name: *ComputerName* **Desktop Settings**
2. Create a GPO link.	▪ Location: Locations/*ComputerName*/Computers/Desktop ▪ GPO name: *ComputerName* Desktop Settings
3. Set the following Group Policy settings to **Enabled**.	▪ GPO: *ComputerName* Desktop Settings ▪ Location of Group Policy setting: User Configuration/Administrative Templates/Network/Offline Files/Prevent use of offline folders

Exercise 5
Generating a Group Policy Modeling Report

In this exercise, you will generate two Group Policy Modeling reports. You will generate one report for Accounting managers with laptop computers and another report for Accounting personnel with desktop computers.

Report name	Special instructions
1. Create a Group Policy Modeling report for laptop computers.	▪ User Container: OU=Users,OU=*ComputerName*,OU=Locations,DC=nwtraders, DC=msft ▪ Computer Container: OU=Laptops,OU=Computers,OU=*ComputerName*,OU=Locations, DC=nwtraders,DC=msft ▪ User Security Groups: Authenticated Users, Everyone, NWTRADERS\G NWTraders Accounting Managers
2. Create a Group Policy Modeling report for desktop computers.	▪ User Container: OU=Users,OU=*ComputerName*,OU=Locations,DC=nwtraders, DC=msft ▪ Computer Container: OU=Desktops,OU=Computers,OU=*ComputerName*,OU=Locations, DC=nwtraders,DC=msft ▪ User Security Groups: Authenticated Users, Everyone, NWTRADES\G NWTraders Accounting Personnel

Exercise 6
Generating a Group Policy Results Report

In this exercise, you will generate a Group Policy Results report to see what policy settings have been applied to the nwtraders\administrator account on the server named Glasgow.

Task	Special instructions
1. Create a Group Policy Results report.	▪ Computer Selection: Glasgow ▪ User Selection: NWTRADERS\administrator
2. View a Group Policy Results report.	▪ Determine when policy settings were last refreshed