

# Module 8: Using Group Policy to Manage User Environments

## Contents

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Overview                                                                    | 1  |
| Introduction to Managing User Environments                                  | 2  |
| Introduction to Administrative Templates                                    | 4  |
| Using Administrative Templates in Group Policy                              | 8  |
| Lab A: Using Administrative Templates to Assign Registry-Based Group Policy | 19 |
| Assigning Scripts with Group Policy                                         | 25 |
| Lab B: Using Group Policy to Assign Scripts to Users and Computers          | 29 |
| Using Group Policy to Redirect Folders                                      | 34 |
| Lab C: Implementing Folder Redirection Policy                               | 39 |
| Using Group Policy to Secure the User Environment                           | 44 |
| Lab D: Implementing Security Settings by Using Group Policy                 | 46 |
| Troubleshooting User Environment Management                                 | 50 |
| Best Practices                                                              | 52 |
| Review                                                                      | 53 |



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Instructor Notes

**Presentation:**  
**75 Minutes**

**Labs:**  
**75 Minutes**

This module provides students with knowledge and skills to manage user environments by using Group Policy. Students will learn to manage user environments by configuring the administrative template settings, using Group Policy to run scripts at designated times, redirecting folders to a central location, and applying security settings.

At the end of this module, students will be able to:

- Identify how Group Policy simplifies user environment management.
- Identify the purpose and the process of applying Administrative Templates.
- Use Administrative Templates in Group Policy to assign registry-based policies to control and configure user and computer environments.
- Assign scripts, such as startup, shutdown, logon, and logoff with Group Policy to control user environments.
- Use Group Policy to redirect user folders to a central network location.
- Use Group Policy to apply security policies to secure the user environment.
- Troubleshoot managing user environments by using Group Policy.
- Apply best practices for using Group Policy to manage user environments.

In the four hands-on labs in this module, students will have a chance to configure, apply, and test the settings in Group Policy. In the first lab, students will configure administrative template settings for users and computers, and then test the configuration. In the second lab, students will configure script settings for logon and logoff scripts, and then test the configuration. In the third lab, students will redirect a folder to a new location on the network by using Group Policy. In the final lab, they will implement the required security settings.

## Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

### Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2154A\_08.ppt

### Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read the white paper, *Windows 2000 Desktop Management*, on the Student Materials compact disc.
- Read the white paper, *Introduction to IntelliMirror® Management Technologies*, on the Student Materials compact disc.
- Read the white paper, *Windows Script Host: A Universal Scripting Host for Scripting Languages*, on the Student Materials compact disc.
- Read the white paper, *Using Group Policy Scenarios*, on the Student Materials compact disc.
- Read the white paper, *Security Configuration Tool Set*, on the Student Materials compact disc.
- Review the Microsoft Windows® Script Host information at: <http://msdn.microsoft.com/scripting>.

## Module Strategy

Use the following strategy to present this module:

- Introduction to Managing User Environments

In this topic, you will introduce managing user environments by configuring the Administrative Templates, Scripts Group Policy extensions, and security settings in Group Policy, and by redirecting folders. Emphasize that configuring user environments by using Group Policy allows you to immediately apply the environments to users or computers by adding the user or computer to the organizational unit (OU) affected by the settings.

- Introduction to Administrative Templates

In this topic, you will explain how to use administrative template settings to manage user environments. Describe Administrative Templates. Emphasize that although they are registry-based settings, they do not permanently change the registry. Then explain how computers apply Group Policy registry settings. Use the animated slide. Emphasize that settings and values are located in the Registry.pol file.

- Using Administrative Templates in Group Policy

In this topic, you will introduce the different types of settings in Administrative Templates. Illustrate the type of settings to use if an administrator wants to lockdown users' access to the desktop, to network resources, or to administrative tools and applications. Emphasize that the settings being presented are only examples and not recommendations. Next, present information on the loopback Group Policy settings. Show students the loopback settings in Administrative Templates. Finally, demonstrate how to implement administrative template settings.

- Lab A: Using Administrative Templates to Assign Registry-Based Group Policy

Prepare students for the lab in which they students will create a Group Policy object (GPO) linked to the Domain Controllers OU, and configure the GPO with Group Policy settings that satisfy the scenario requirements. After the GPO is configured, they will test the settings that they configured. Make sure that students run the command file for the lab and tell them that they will have to initiate replications between their domain controllers and their partner's domain controllers. After students have completed the lab, ask them if they have any questions.

- Assigning Scripts with Group Policy

In this topic, you will introduce how to use Group Policy to run scripts. Present how Group Policy handles scripts. Emphasize that script settings allow an administrator to automate the running of scripts at specific times (startup, shutdown, and when a user logs on or logs off). Then present the order in which Microsoft Windows 2000 processes scripts. Emphasize that startup scripts run synchronously, and define the term if needed. Finally, demonstrate how to implement scripts.

- Lab B: Using Group Policy to Assign Scripts to Users and Computers

Prepare students for the lab in which they will create a GPO for the Sales OU and a second GPO for the Retail OU. They will configure the settings in the two GPOs to run the required scripts. After students have completed the lab, ask them if they have any questions.

- Using Group Policy to Redirect Folders

In this topic, introduce how to redirect four default user folders to a network server by using Group Policy. Explain what folder redirection is. Emphasize that although the folder appears to be stored locally, it is actually stored on a server. Mention that the information in a redirected folder is always present for the user, regardless of the computer from which the user logs on. Present information on the four types of folders that an administrator can redirect and why an administrator would choose to redirect these folders. Emphasize that an administrator should always redirect users' My Documents folders. Finally, demonstrate how to redirect folders by using Group Policy.

- Lab C: Implementing Folder Redirection Policy

Prepare students for the lab in which they will redirect the My Documents folder to a new location on the network by using Group Policy. After students have completed the lab, ask them if they have any questions.

- Using Group Policy to Secure the User Environment

In this topic, you will introduce the procedure for implementing security policies. Emphasize that a preconfigured security template ensures duplication of desired settings that already exist for a computer, and can be tested before security settings are applied to multiple computers. Demonstrate how to use Group Policy to apply security policies. Emphasize that you can define a security setting once and apply it in many places.

- Lab D: Implementing Security Settings by Using Group Policy

Prepare students for the lab in which they will create a new GPO, which is linked to the Domain Controllers OU and named Additional Security Settings Policy, to implement the required security settings. After students have completed the lab, ask them if they have any questions.

- Troubleshooting User Environment Management

In this topic, you will introduce troubleshooting options for configuring and managing user environments through Group Policy. Explain some of the more common problems that they may encounter during user environment management, along with suggested strategies for resolving these problems.

- Best Practices

Present best practices for managing user environments through Group Policy. Emphasize the reason for each best practice.

## Customization Information

This section identifies the lab setup requirements for the module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

---

**Important** The labs in this module are also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

---

The labs in this module require that the student computers be configured as domain controllers. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete Module 3, “Creating a Windows 2000 Domain,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Autode.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autode folder.
- Run Dcpromo.exe on the student computers by using the following parameters:
  - A domain controller for a new domain.
  - A new domain tree.
  - A new forest of domain trees.
  - Full DNS domain name, which is *computerdom.nwtraders.msft* (where *computer* is the assigned computer name).
  - NetBIOS domain name, which is *COMPUTERDOM*.
  - Default location for the database, log files, and SYSVOL.
  - Permission compatible only with Windows 2000–based servers.
  - Directory Services Restore Mode Administrator password, which is **password**.

---

**Note** Before you use Module 3, “Creating a Windows 2000 Domain,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*, you must successfully complete Module 2, “Implementing DNS to Support Active Directory,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

---

## Lab Results

Performing the labs in this module introduces no configuration changes.



# Overview

**Topic Objective**

To provide an overview of the module topics and objectives.

**Lead-in**

In this module, you will learn to configure and manage the user desktop environment by using Group Policy.

- Introduction to Managing User Environments
- Introduction to Administrative Templates
- Using Administrative Templates in Group Policy
- Assigning Scripts with Group Policy
- Using Group Policy to Redirect Folders
- Using Group Policy to Secure the User Environment
- Troubleshooting User Environment Management
- Best Practices

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Group Policy in Microsoft® Windows® 2000 allows an organization to reduce total cost of ownership (TCO) by allowing administrators to enhance and control users' desktops. Administrators can enhance and control users' desktops by creating a managed desktop environment that is tailored to the user's job responsibilities and experience level. TCO is the cost that is involved in administering distributed personal computer networks.

Microsoft Windows 2000 Advanced Server includes many Group Policy settings that provide administrators with greater control over computer configurations. Group Policy allows administrators to specify Group Policy settings to manage desktop configurations for groups of computers and users. Group Policy is flexible and includes settings for registry-based Group Policy, security, software installation, scripts, computer startup and shutdown, user logon and logoff, and folder redirection.

At the end of this module, you will be able to:

- Identify how Group Policy simplifies user environment management.
- Identify the purpose and the process of applying Administrative Templates.
- Use Administrative Templates in Group Policy to assign registry-based policies to control and configure user and computer environments.
- Assign scripts, such as startup, shutdown, logon, and logoff, with Group Policy to control user environments.
- Use Group Policy to redirect folders to a central network location.
- Use Group Policy to apply security policies to secure the user environment.
- Troubleshoot managing user environments by using Group Policy.
- Apply best practices for using Group Policy to manage user environments.

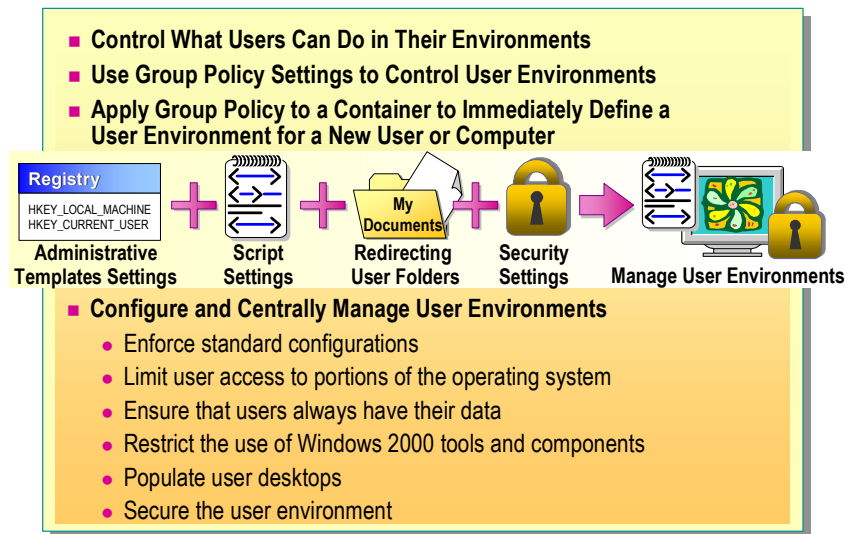
# Introduction to Managing User Environments

## Topic Objective

To identify the benefits of using Group Policy to centrally configure and manage the user desktop environment.

## Lead-in

Managing user environments means controlling what users can do when logged on to the network, as well as what appears on their desktops.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Describe the tasks involved in centrally managing user environments with Group Policy.

Remind students that they can set up Group Policy once, and then Windows 2000 will continually enforce it.

## Key Points

If Group Policy settings that control user environments are set up for an OU, when an administrator adds a new user or computer to that OU, the Group Policy settings immediately apply. This means that the user environment is immediately set up for that user or computer.

Administrators can use Group Policy to provide users with what they need to do their jobs while curtailing user actions that could accidentally corrupt the user environments.

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. You control user environments to ensure that users have what they need to perform their jobs, but do not have the ability to corrupt or incorrectly configure their environments.

The types of Group Policy settings that you typically use to manage user environments are administrative template settings, script settings, folder redirection, and security settings. You configure these settings in Group Policy in the Administrative Templates and Script extensions.

If you have used Group Policy to set up user environments for an Active Directory® directory service container, such as an organizational unit (OU), any computer or user who you add to that OU has the Group Policy settings applied automatically.

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

- Enforce standard configurations. 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 could make their user environments more complex than necessary.
- Limit user access to selected portions of the operating system. You can prevent users from opening Control Panel and shutting down their computers. By preventing users from accessing critical operating system components and configuration options, you reduce the possibility of users corrupting their systems, and therefore, the number of technical support calls required.

- Ensure that users always have their desktops and personal data. 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 Windows 2000 manages user profiles, which includes how users' personal data is made available. By redirecting user folders from users' local hard disks to a central location on a server, you can ensure that users' data is available to them regardless of the computers to which they log on.
- Restrict the use of tools and components in Windows 2000. These tools and components include Microsoft Internet Explorer, Windows Explorer, and the Microsoft Management Console (MMC). You can ensure that users never see these tools unless they have a genuine need for them.
- Populate user desktops. You can ensure that users have their required files, shortcuts, and network connections.
- Secure the user environment. Through the use of Group Policy in Active Directory, administrators can centrally apply the security settings required to protect the user environment. In Windows 2000, you can use the Security Settings extension in Group Policy to define the security settings for local and domain security policies.

## ◆ Introduction to Administrative Templates

**Topic Objective**

To introduce Administrative Templates.

**Lead-in**

Administrative Templates provide you with the capability to effectively configure and manage user environments.

- What Are Administrative Templates?
- How Computers Apply Administrative Template Settings

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

To effectively configure and manage user environments, ensure that users can gain access to only the resources that they require to do their jobs. You can use Administrative Templates to simplify user environments and prevent users from corrupting their environments or spending time on unnecessary applications, software, or files.

By using the Administrative Templates extensions in Group Policy, you can set up the environments for multiple users and computers once, and then rely on Windows 2000 to continually implement and apply those settings.

## What Are Administrative Templates?

### Topic Objective

To identify the purposes of administrative template settings.

### Lead-in

Group Policy administrative template settings are registry-based settings that you can use to manage user environments.

- **Administrative Template Settings Modify Registry Settings That Control User Environments**
- **Settings Modify Registry Settings in the Registry Subtrees**
  - **HKEY\_LOCAL\_MACHINE** for computer settings
  - **HKEY\_CURRENT\_USER** for user settings
- **If a GPO No Longer Applies, Policy Settings Are Removed**
- **Windows 2000 Applies Both Group Policy and Local Default-Registry Settings Unless There Is a Conflict**

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Key Points

Administrative template settings modify the settings stored in the two registry subtrees. The subtrees are **HKEY\_LOCAL\_MACHINE** for computer settings, and **HKEY\_CURRENT\_USER** for user settings.

Registry settings specified by Group Policy write to special locations in the registry. They do not permanently change the local registry settings.

If you remove the Group Policy settings, only the local registry settings apply.

Administrative Templates are a collection of Group Policy settings that modify registry settings. You use Administrative Templates in Group Policy to configure user and computer registry-based settings that control the user's working environment. This includes controlling users' desktops, interface options, operating system components, and the default values for application settings.

Administrative template settings modify the values located in the following registry locations:

- **HKEY\_LOCAL\_MACHINE (HKLM).** When a computer starts, the Group Policy settings contained within the Computer Configuration portion of the Group Policy objects (GPOs) that apply to the computer are written to either the SOFTWARE\Policies key or to the \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies key below HKLM.
- **HKEY\_CURRENT\_USER (HKCU).** When a user logs on to a computer, Group Policy settings contained within the User Configuration portion of the GPOs that apply to the user are written to either the SOFTWARE\Policies key or to the \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies key below HKCU.

Windows 2000 applies both the Group Policy settings and any default registry settings to users and computers. If there are conflicts, the Group Policy settings prevail. If the GPO containing the settings that affect the user or computer account no longer applies (for example if it is removed or if the account is moved to a location that is not affected by the GPO) the settings are removed from the registry the next time that Group Policy is refreshed, and the local default registry settings apply.

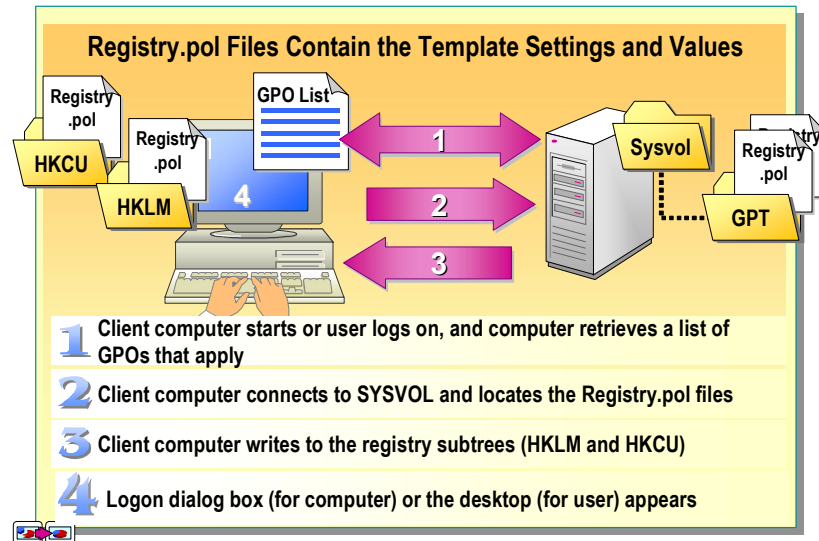
## How Computers Apply Administrative Template Settings

### Topic Objective

To identify the process of applying administrative template settings.

### Lead-in

Now let us look at the process in which Group Policy registry settings are applied.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

The slide for this topic is animated. Display a new step on the slide as you talk about it.

### Delivery Tip

Open Windows Explorer and show students the Registry.pol files in the path provided in the Note in the student text.

### Key Points

The administrative template settings that Windows 2000 applies are stored in the Registry.pol file in the GPT on domain controllers.

The values for the registry settings are contained in the Registry.pol file.

The administrative template settings and the values for the settings that Windows 2000 applies are stored in a Registry.pol file in the Group Policy template (GPT) on domain controllers. There are two files: one for computer settings, and one for user settings.

**Note** The path for the Registry.pol file is `systemroot\SYSVOL\Sysvol\domain_name\Policies\GPO_GUID_identifier\Machine` or `\User`.

The process that a computer running Windows 2000 uses to apply administrative template settings during the start up process is as follows:

1. When the client computer starts, it retrieves the list of GPOs that contain computer configuration settings and determines the order in which to apply them.
2. The client computer connects to the SYSVOL folder on the authenticating domain controller, and then locates the Registry.pol files in the Machine folder in the GPT for each GPO that contains administrative template settings that apply to the computer.
3. The client computer writes the registry settings and their values in the Registry.pol file to the appropriate registry subtree. The computer continues initializing the operating system and enforces the registry settings.
4. When the registry settings have been enforced, the logon dialog box appears.

The following process is repeated during the user logon process:

1. After the user has initiated the logon process, the client computer retrieves the list of GPOs that contain user configuration settings, and determines the order in which to apply them.
2. The client computer connects to the SYSVOL folder on the authenticating domain controller, and then locates the Registry.pol files in the User folder in the GPT for each GPO that contains administrative template settings that apply to the user.
3. The client computer writes the registry settings and their values in the Registry.pol file to the appropriate registry subtree. The computer continues the logon process and enforces the registry settings.
4. When the registry settings have been enforced, the desktop is displayed.

The settings in the Group Policy section of the registry apply even when there is a conflict with settings in the local default registry settings.

## ◆ Using Administrative Templates in Group Policy

**Topic Objective**

To introduce the topics related to using Administrative Templates in Group Policy.

**Lead-in**

There are administrative template settings available for both computers and user accounts that you can use to control the user environment.

- **Types of Administrative Template Settings**
- **Settings for Locking Down the Desktop**
- **Settings for Locking Down User Access to Network Resources**
- **Settings for Locking Down User Access to Administrative Tools and Applications**
- **The Loopback Processing Mode Setting in Group Policy**
- **Implementing Administrative Templates**

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Administrative template settings are registry-based Group Policy settings that you can use to mandate registry settings that control the behavior and appearance of the desktop, including the operating system components and applications. There are administrative template settings available for both computers and user accounts.

You can control the user environment by configuring specific administrative settings to lock down user environments. You should only lock down the desktops of users who perform defined and specific tasks, for example, users who perform telemarketing, data entry, or training.

## Types of Administrative Template Settings

### Topic Objective

To identify the different types of administrative template settings used to control user environments.

### Lead-in

You can configure several administrative template settings that apply to both user and computer settings.

| Setting types                   | Controls                                                                                                    | Available for                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Windows Components</b>       | The parts of Windows 2000 and its tools and components to which users can gain access, including MMC        |   |
| <b>System</b>                   | Logon and logoff, Group Policy, disk quotas, and loopback policy                                            |   |
| <b>Network</b>                  | The properties of network connections and dial-in connections                                               |   |
| <b>Printers</b>                 | Printer settings that can force printers to be published in Active Directory and disable Web-based printing |                                                                                      |
| <b>Start Menu &amp; Taskbar</b> | What users can gain access to from the <b>Start</b> menu and what makes the <b>Start</b> menu read-only     |                                                                                      |
| <b>Desktop</b>                  | The Active Desktop, including what appears on desktops, and what users can do with the My Documents folder  |                                                                                      |
| <b>Control Panel</b>            | The use of Add/Remove Programs, Printers, and Display in Control Panel                                      |                                                                                      |

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Because of the large number of administrative template settings, encourage users to explore the Administrative Templates extension in Group Policy.

### Delivery Tip

Show students the different types of administrative template settings in Group Policy. Mention that some types apply to both computers and users.

### Key Point

Computer settings focus more on the management of Windows 2000, whereas user settings focus more on controlling how users can affect their desktop environments.

Administrative template settings are organized into seven types, for which there are both user and computer settings. The computer settings focus more on the management of Windows 2000, whereas user settings focus more on controlling how users can affect their desktop environments.

The following table provides the types of settings in the Administrative Templates extension.

| Setting type       | Controls                                                                                                                                                     | Available for       |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Windows Components | The parts of Windows 2000 and its tools and components to which users can gain access. This includes controlling user access to MMC.                         | Computers and users |
| System             | Logon and logoff procedures. With System settings, you can manage Group Policy and refresh intervals, enable disk quotas, and implement loopback processing. | Computers and users |
| Network            | The properties of network connections and dial-in connections, which include shared network access.                                                          | Computers and users |
| Printers           | Printer settings that can force printers to be automatically published in Active Directory and can disable Web-based printing.                               | Computers           |

*(continued)*

| Setting type         | Controls                                                                                                                                                                                                                                                                                             | Available for |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Start Menu & Taskbar | Which features users can access from the <b>Start</b> menu. For example, by removing the <b>Run</b> command, users are prevented from running applications for which there is no icon or shortcut. You can also make the <b>Start</b> menu read-only and disable the user's ability to make changes. | Users         |
| Desktop              | The Active Desktop. You can control users' ability to gain access to the network and the Internet by hiding the appropriate desktop icons and controlling what they can do with their My Documents folder.                                                                                           | Users         |
| Control Panel        | Several applications in Control Panel. This includes restricting the use of Add/Remove Programs, Display, and Printers.                                                                                                                                                                              | Users         |

---

**Note** Windows 2000 provides you with the ability to add additional templates to Administrative Templates in Group Policy if the preconfigured templates do not provide you with the settings that you require.

---

## Settings for Locking Down the Desktop

### Topic Objective

To identify how to use the administrative template settings to lock down users' desktops.

### Lead-in

You can use some of these administrative template settings to lock down users' desktop environment.

**Group Policy Settings to Lock Down the Desktop**

- Hide all icons on desktop
- Don't save settings at exit
- Hide these specified drives in My Computer
- Remove Run menu from Start menu
- Prohibit user from running Display control panel
- Disable and remove links to Windows Update
- Disable changes to Taskbar and Start Menu settings
- Disable/Remove the Shut Down command



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Emphasize that this table provides examples (not recommendations) for the type of administrative settings to configure to lockdown user desktop environment. These examples show a very restrictive application of the settings, but students may want to use these in their networks.

Tell students that the different sections of the Administrative Templates extensions contain a multitude of settings.

There are several Group Policy settings that you can use to customize a user's desktop environment. Securing the desktop involves setting up a computer so that it can perform only a limited number of functions that users cannot modify. For example, a computer in a public information kiosk can be configured to run only a Web browser.

The following table describes common Group Policy settings to configure when locking down user desktops, and examples of the possible effect of these configurations.

| Group Policy setting and location                                                                                                           | Action                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hide all icons on desktop<br>(User Configuration\<br>Administrative Templates\Desktop)                                                      | Hides all desktop items, including menus, folders, and shortcuts. This provides users with a simpler user interface.                                                                                                                                                                                 |
| Don't save settings at exit<br>(User Configuration\<br>Administrative Templates\Desktop)                                                    | Disables the ability to save any configuration changes made during the logon session. The original settings are restored each time users log off and then log back on.                                                                                                                               |
| Hide these specified drives in My Computer<br>(User Configuration\<br>Administrative Templates\<br>Windows Components\<br>Windows Explorer) | Removes icons representing the selected drives from My Computer, Windows Explorer, and My Network Places. Drive letters will not appear in the <b>Open</b> dialog box of any application. By hiding drives, you help limit users to running only the applications that are on the <b>Start</b> menu. |

*(continued)*

| Group Policy setting and location                                                                                                  | Action                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remove Run menu from Start menu<br>(User Configuration\<br>Administrative Templates\ Start Menu &<br>Taskbar)                      | Removes the <b>Run</b> command from the <b>Start</b> menu. However, users can still access this command through Task Manager.                                                                                                                                    |
| Prohibit user from running Display in Control Panel<br>(User Configuration\<br>Administrative Templates\<br>Control Panel\Display) | Prevents users from changing display settings such as the wallpaper, screen saver, or color schemes. This setting also reduces problems that can arise when users change their desktop settings.                                                                 |
| Disable and remove links to Windows Update<br>(User Configuration\<br>Administrative Templates\ Start Menu &<br>Taskbar)           | Removes the <b>Windows Update</b> command from the <b>Settings</b> menu. However, this command will still be available in Internet Explorer. Removing this command helps prevent users from applying unauthorized updates or changes to their operating systems. |
| Disable changes to Taskbar and Start Menu settings<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar)   | Removes the <b>Taskbar &amp; Start Menu</b> command from the <b>Settings</b> menu. This helps prevent users from overriding any changes that you make to the <b>Start</b> menu.                                                                                  |
| Disable/Remove the Shut Down command<br>(User Configuration\<br>Administrative Templates\Desktop)                                  | Prevents users from shutting down and restarting Windows 2000. This is useful on computers that need to run continually, such as a computer in a public library.                                                                                                 |

## Settings for Locking Down User Access to Network Resources

### Topic Objective

To identify how to use the administrative template settings to lock down users' access to network resources.

### Lead-in

You can use some of these administrative template settings to lock down user access to network resources.

**Group Policy Settings to Lock Down User Access to Network Resources**

- Hide My Network Places icon on desktop
- Remove the "Map Network Drive" and "Disconnect Network Drive"
- Tools menu: Disable Internet Options... menu option



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Emphasize that this table provides examples (not recommendations) for the type of administrative settings to configure to lockdown users' network access. These examples show a very restrictive application of the settings, but students may want to use these in their networks.

You can restrict the network resources to which users can gain access. The following table provides types of Group Policy that contain settings to configure when locking down user access to network resources, and examples of the possible effect of these configurations.

| Group Policy setting and location                                                                                                                                   | Action                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hide My Network Places icon on desktop<br>(User Configuration\<br>Administrative Templates\Desktop)                                                                 | Removes <b>My Network Places</b> from the desktop and disables support for universal naming convention (UNC) file names. By using logon scripts to map network drives, you can control the network resources to which users have access.                                                                                                                      |
| Remove the "Map Network Drive" and "Disconnect Network Drive"<br>(User Configuration\<br>Administrative Templates\<br>Windows Components\<br>Windows Explorer)      | Removes the Map Network Drive and Disconnect Network Drive options from Windows Explorer. This setting also removes the Add Network Places wizard from My Network Places. However, users can still connect to computers by using the <b>Run</b> command on the <b>Start</b> menu.                                                                             |
| Tools menu: Disable Internet Options... menu option<br>(User Configuration\<br>Administrative Templates\<br>Windows Components\<br>Internet Explorer\Browser Menus) | Removes the <b>Internet Options</b> command from Internet Explorer. This prevents users from modifying their Internet Explorer configurations.<br><br>You can also disable individual pages by using Group Policy settings located under User Configuration\<br>Administrative Templates\<br>Windows Components\Internet Explorer\<br>Internet Control Panel. |

## Settings for Locking Down User Access to Administrative Tools and Applications

### Topic Objective

To identify how to use the administrative template settings to lock down users' access to administrative tools and applications.

### Lead-in

You can use some of these administrative template settings to lock down user access to administrative tools and applications.

**Group Policy Settings to Lock Down User Access to Administrative Tools and Applications**

- Remove Search menu from Start menu
- Remove Run menu from Start menu
- Disable Task Manager
- Run only allowed Windows applications
- Remove the Documents menu from the Start menu
- Disable changes to Taskbar and Start Menu settings
- Hide common program groups in Start menu



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Emphasize that this table provides examples (not recommendations) for the type of administrative settings to configure user access to administrative tools and applications. These examples show a very restrictive application of the settings, but students may want to use these in their networks.

The following table provides the setting types that contain settings to configure when locking down user access to administrative tools and applications, and examples of the possible effect of these configurations.

| Group Policy setting and location                                                                                | Action                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remove Search menu from Start menu<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar) | Removes the <b>Search</b> menu from the <b>Start</b> menu. However, the <b>Search</b> menu will still appear in Windows Explorer and Internet Explorer. Removing the <b>Search</b> command helps prevent users from conducting bandwidth-intensive searches across the network. |
| Remove Run menu from Start menu<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar)    | Removes the <b>Run</b> command from the <b>Start</b> menu. This makes it more difficult for users to run unauthorized applications.                                                                                                                                             |
| Disable Task Manager<br>(User Configuration\<br>Administrative Templates\System\<br>Logon/Logoff)                | Prevents the user from starting applications by using Task Manager.                                                                                                                                                                                                             |

*(continued)*

| Group Policy setting and location                                                                                                | Action                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Run only allowed Windows applications<br>(User Configuration\<br>Administrative Templates\System)                                | Prevents users from running applications other than those you specify in this Group Policy setting. This restriction applies only to applications that are started through Windows Explorer. |
| Remove the Documents menu from the Start menu<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar)      | Removes the <b>Documents</b> command from the <b>Start</b> menu.                                                                                                                             |
| Disable changes to Taskbar and Start Menu settings<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar) | Removes the <b>Taskbar &amp; Start Menu</b> command from the <b>Settings</b> menu. This helps prevent users from overriding any changes that you make to the <b>Start</b> menu.              |
| Hide common program groups in Start menu<br>(User Configuration\<br>Administrative Templates\<br>Start Menu & Taskbar)           | Removes common program groups from the <b>Start</b> menu. This means that users receive only the <b>Start</b> menu items specified in their user profiles.                                   |

## The Loopback Processing Mode Setting in Group Policy

### Topic Objective

To identify how the loopback processing mode in Group Policy enables administrative template settings to enforce User Configuration settings.

### Lead-in

Windows 2000 allows you to alter the typical method in which Group Policy settings are applied by enabling a loopback setting.

### The Loopback Processing Mode Setting:

- **Applies Configuration Settings to Computers**
- **Is Used for Computers Dedicated to Specific Tasks**
- **Can Either Be Set to Either Replace Mode or Merge Mode**

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Delivery Tip

Demonstrate configuring the User Group Policy loopback processing mode setting that is located in Group Policy. Define the Replace and Merge modes.

### Key Points

The Group Policy loopback processing mode setting causes administrative template settings for users to apply to computers.

Loopback processing mode is most useful for computers that are dedicated to specific tasks or that have special software installed on them.

Loopback processing mode is a Group Policy setting that enforces the User Configuration settings in the GPOs that apply to the computer, rather than enforcing the User Configuration settings in the GPOs that apply to the user object.

Group Policy is normally applied to a user or computer based on where the user object or the computer object is located in Active Directory. For example, the user whose user object is located in the Sales OU logs on to a computer. The computer object is located in the Servers OU. The Group Policy settings that are applied to the user are based on any GPOs that are linked to the Sales OU, and GPOs linked to any parent containers. The settings that are applied to the computer are based on any GPOs that are linked to the Servers OU, and GPOs linked to any parent containers. However, this default behavior may not be appropriate for certain computers, such as servers or computers that are dedicated to a certain task. For example, applications that are assigned to a user should not be automatically available on a server.

There are two possible modes for loopback processing:

- *Replace mode.* Processes only the GPOs that apply to the computer.
- *Merge mode.* First processes the GPOs that apply to the user object, and then the GPOs that apply to the computer object. If settings conflict, the computer object settings in the GPO are enforced, because those GPO settings are applied last.

To enable the loopback processing mode, perform the following steps:

1. Open Group Policy, expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and then click **Group Policy**.
2. Double-click **User Group Policy loopback processing mode**.
3. Click **Enabled** if it is not already selected, and then in the **Mode** list, click either **Replace** or **Merge**.

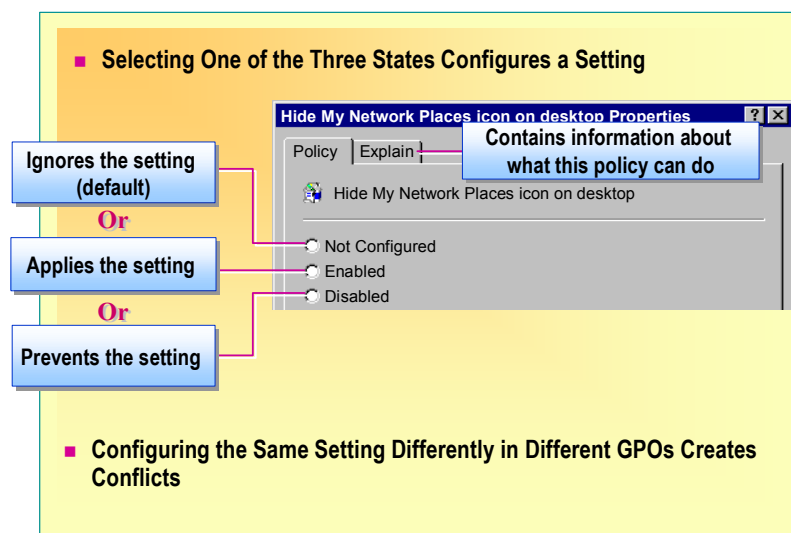
## Implementing Administrative Templates

### Topic Objective

To illustrate the procedure to implement the administrative template settings to control user environments.

### Lead-in

You implement administrative template settings by configuring the settings in the Administrative Templates extension in Group Policy.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Delivery Tip

Demonstrate configuring a setting by selecting a state for an administrative template setting. The example in the slide is in Group Policy\ User Configuration\ Administrative Templates\ Desktop.

### Key Points

The Not Configured state makes no change to the Registry.pol file.

Conflicts can arise from configuring the same settings differently in different GPOs. When these conflicts arise, the last setting applied prevails, unless Group Policy inheritance is modified.

Implement administrative template settings by configuring the settings in the Administrative Templates extension in Group Policy. In most instances, you configure a setting by selecting one of three states for the setting. You select the state on the **Policy** tab of the **Properties** dialog box for the Group Policy setting.

The following list provides descriptions of the three states:

- *Not configured.* Windows 2000 ignores the setting and makes no changes to the computer. This state does not specify a value change in the registry.
- *Enabled.* Windows 2000 applies the setting and adds the change to the appropriate Registry.pol file.
- *Disabled.* Windows 2000 prevents the setting from being applied and adds the change to the appropriate Registry.pol file.

Besides selecting a state for a setting, you may need to provide additional information, such as the mode for Loopback processing, or the size for a disk quota.

The enabled and disabled states can create conflicting GPOs. This occurs, for example, when a setting is enabled in one GPO and the same setting is disabled in another GPO—but both GPOs apply to the same users or computers. Unless Group Policy inheritance is modified, the last setting applied prevails.

To gain access to the **Policy** tab for an administrative template setting, perform the following steps:

1. Right-click the appropriate site, domain, or OU, and then click **Properties**.
2. On the **Group Policy** tab, create or select an existing GPO, and then click **Edit**.
3. In Group Policy, expand **Computer Settings** or **User Settings**, and then expand **Administrative Templates** until you locate the setting that you want to modify, for example, User Configuration\Administrative Templates\Desktop.
4. In the details pane of Group Policy, double-click the Group Policy setting that you want to modify.

---

**Note** When you create a GPO that contains only settings for users or computers, you can disable the other type of settings (user or computer) to speed up processing of the Group Policy settings. You can disable the settings on the **General** tab of the **Properties** dialog box for the GPO.

---

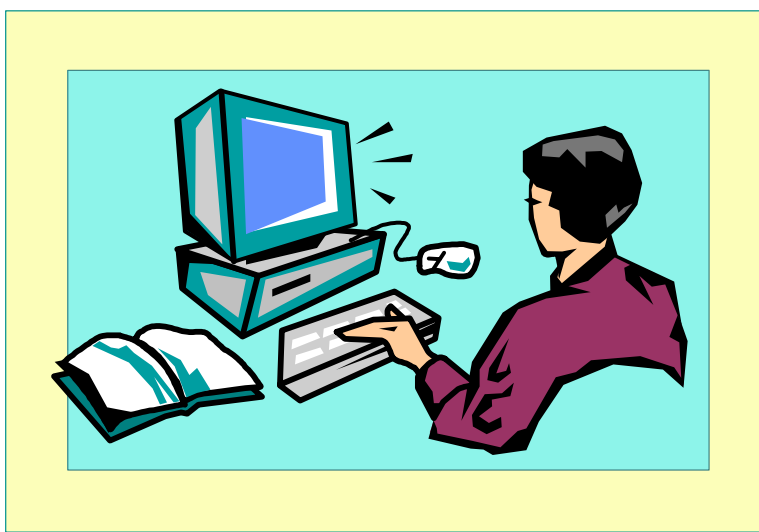
## Lab A: Using Administrative Templates to Assign Registry-Based Group Policy

### Topic Objective

To introduce the lab.

### Lead-in

In this lab, you will create a Group Policy object (GPO), configure the administrative template settings that satisfy the scenario requirements, and then link the new GPO to an OU.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Explain the lab objectives.

### Objectives

After completing this lab, you will be able to configure, apply, and test registry-based Group Policy by using Administrative Templates.

### Prerequisites

Before working on this lab, you must have experience:

- Working with Active Directory Users and Computers.
- Managing disk quotas and scheduled tasks.

### Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a domain controller.
- An OU structure. To create the required OUs and users, run the Sales.vbs script file from C:\Moc\Win2154A\Labfiles.

### Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

---

**Important** The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

---



---

**Important** Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

---

**Estimated time to complete this lab: 30 minutes**

## Exercise 1

### Implementing an Administrative Templates Policy for Computers

#### Scenario

You need to assign additional Group Policy settings for a domain controller in your domain. The Group Policy settings that you need to apply to enhance the settings in the default domain controller Group Policy need to satisfy the following management requirements:

- Disk quotas must be enabled for all volumes so that disk space usage can be easily tracked.
- Disk quota limits should not be enforced. No limits will be enforced until you can determine the average disk utilization for the server and install additional disk capacity, if required.
- Users must not be able to run the New Task wizard so that server performance is not impacted.

#### Goal

Create a Group Policy object (GPO) linked to the Domain Controllers OU, and configure the GPO with Group Policy settings that satisfy the scenario requirements. After the GPO is configured, restart your computer to ensure that the Group Policy settings have been applied.

| Tasks                                                                                                                                                                                                                                                         | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a new GPO linked to the Domain Controllers OU. Name the new GPO Admin Template Policy.                                                                                                                                                              | <ol style="list-style-type: none"> <li>a. Log on as Administrator with a password of <b>password</b>.</li> <li>b. Open Active Directory Users and Computers from the <b>Administrative Tools</b> menu.</li> <li>c. In the console tree, expand your domain, right-click <b>Domain Controllers</b>, and then click <b>Properties</b>.</li> <li>d. On the <b>Group Policy</b> tab, click <b>New</b>, type <b>Admin Template Policy</b> and then press ENTER.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2. Edit the administrative template settings for the new GPO to: <ul style="list-style-type: none"> <li>• Enable disk quotas.</li> <li>• Prevent disk quota limits from being enforced.</li> <li>• Prevent users from running the New Task wizard.</li> </ul> | <ol style="list-style-type: none"> <li>a. Select the new Group Policy, and then click <b>Edit</b>.</li> <li>b. In the Group Policy console tree, under <b>Computer Configuration</b>, expand <b>Administrative Templates</b>.</li> <li>c. In the console tree, expand <b>System</b>, click <b>Disk Quotas</b>, and then in the details pane, double-click <b>Enable disk quotas</b>.</li> <li>d. In the <b>Enable disk quotas Properties</b> dialog box, on the <b>Policy</b> tab, click <b>Enabled</b>, and then click <b>OK</b>.</li> <li>e. In the details pane, double-click <b>Enforce disk quota limit</b>.</li> <li>f. In the <b>Enforce disk quota limit Properties</b> box, click <b>Disabled</b>, and then click <b>OK</b>.</li> <li>g. In the console tree, expand <b>Windows Components</b>, click <b>Task Scheduler</b>, and then in the details pane, double-click <b>Disable New Task Creation</b>.</li> <li>h. In the <b>Disable New Task Creation Properties</b> dialog box, on the <b>Policy</b> tab, click <b>Enabled</b>, and then click <b>OK</b>.</li> <li>i. Close Group Policy, and then click <b>Close</b> to close the <b>Domain Controllers Properties</b> dialog box.</li> <li>j. Leave Active Directory Users and Computers open.</li> </ol> |

## Exercise 2

### Implementing an Administrative Templates Policy for Users

#### Scenario

Telemarketing users are typically temporary workers who accept orders by telephone and enter the customer's data into a database by using in-house software installed on preconfigured computers. You need to implement Group Policy settings that enforce the following restrictions for telemarketing users:

- Prevent users from mapping network drives.
- Prevent users from using My Network Places to browse the corporate network.
- Prevent users from making changes to Taskbar & Start Menu settings.
- Prevent users from accessing the Windows Update icon. The Information Services department should install all software updates for corporate computers.
- Enable users to run the New Task wizard to schedule an in-house tool to perform maintenance tasks on the order database.

#### Goal

Create a GPO linked to the Telemarketing OU, and configure the GPO with Group Policy settings that satisfy the restrictions described in the scenario.

| Tasks                                                                                                                       | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a GPO for the Telemarketing OU. Name this new GPO Telemarketing Policy.                                           | <ul style="list-style-type: none"><li>a. In the console tree, expand your domain, expand <b>Sales</b>, right-click <b>Telemarketing</b>, and then click <b>Properties</b>.</li><li>b. On the <b>Group Policy</b> tab, click <b>New</b>, type <b>Telemarketing Policy</b> and then press ENTER.</li></ul>                                                                                                                                                                                                                                                                                                                        |
| 2. Edit the administrative template settings for the Telemarketing Policy GPO to prevent users from mapping network drives. | <ul style="list-style-type: none"><li>a. With <b>Telemarketing Policy</b> selected, click <b>Edit</b>.</li><li>b. In the console tree, under <b>User Configuration</b>, expand <b>Administrative Templates</b>.</li><li>c. In the console tree, expand <b>Windows Components</b>, click <b>Windows Explorer</b>, and then in the details pane, double-click <b>Remove the "Map Network Drive" and "Disconnect Network Drive."</b></li><li>d. In the <b>Remove "Map Network Drive" and "Disconnect Network Drive" Properties</b> dialog box, on the <b>Policy</b> tab, click <b>Enabled</b>, and then click <b>OK</b>.</li></ul> |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                        | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>3.</b> Edit the remaining administrative template settings for the Telemarketing GPO to:</p> <ul style="list-style-type: none"><li>• Prevent users from using My Network Places to browse the corporate network.</li><li>• Prevent users from making changes to Taskbar &amp; Start Menu settings.</li><li>• Prevent users from accessing Windows Update.</li><li>• Enable users to run the New Task wizard.</li></ul> | <p><b>a.</b> Using the following information, configure the remaining required restrictions:</p> <ul style="list-style-type: none"><li>• Enable the Hide My Network Places icon on Desktop policy, which is located in the Desktop folder.</li><li>• Enable the Disable changes to Taskbar and Start Menu Settings policy, which is located in the Start Menu &amp; Taskbar folder.</li><li>• Enable the Disable and Remove links to Windows Update policy, which is located in the Start Menu &amp; Taskbar folder.</li><li>• Disable the Disable New Task Creation policy, which is located in the Windows Components\Task Scheduler folder.</li></ul> <p><b>b.</b> Close all open windows, and then restart your computer.</p> |

## Exercise 3

### Verifying Administrative Templates Policies

#### Scenario

Now that the required GPOs are in place and configured, you need to confirm that the Group Policy settings are being applied as expected.

#### Goal

Log on as Administrator to verify which computer Group Policy settings are in effect. Then log on as a Telemarketing user to verify which user Group Policy settings are in effect for members of the Telemarketing OU.

| Tasks                                                                                                                                                                                                                                                                     | Detailed Steps                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Verify that the Group Policy settings contained in the Admin Template GPO are being properly applied.                                                                                                                                                                  | <ol style="list-style-type: none"> <li>Log on as Administrator with a password of <b>password</b>.</li> <li>On the desktop, double-click <b>My Computer</b>, right-click the icon for drive C, and then click <b>Properties</b>.</li> <li>Click the <b>Quota</b> tab.</li> </ol> |
| <p> Are disk quotas enabled? Why or why not?</p> <p><b>Yes, because disk quotas were enabled in the Admin Template GPO.</b></p> <hr/> <hr/> <hr/> <hr/>                                 |                                                                                                                                                                                                                                                                                  |
| <p> Are disk quota limits enforced? Why or why not?</p> <p><b>No, because the enforcement of disk quota limits was disabled in the Admin Template GPO.</b></p> <hr/> <hr/> <hr/> <hr/> |                                                                                                                                                                                                                                                                                  |
| 1. (continued)                                                                                                                                                                                                                                                            | <ol style="list-style-type: none"> <li>Click <b>Cancel</b> to close the <b>Local Disk (C:) Properties</b> dialog box.</li> <li>In the My Computer window, double-click <b>Control Panel</b>.</li> <li>In Control Panel, double-click <b>Scheduled Tasks</b>.</li> </ol>          |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Detailed Steps                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <p> Are you able to run the Add Task wizard?</p> <p>No.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                          |
| <p> Were all of the Group Policy settings in the Admin Template Policy GPO applied?</p> <p>Yes.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                          |
| 1. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | g. Close all open windows, and then log off.             |
| 2. Log on as TMUser and verify that the Group Policy settings contained in the Telemarketing GPO are being properly applied.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | a. Log on as TMUser with a password of <b>password</b> . |
| <p> Are the following settings contained in the Telemarketing Policy GPO enforced? Why or why not?</p> <ul style="list-style-type: none"> <li>▪ The <b>My Network Places</b> icon does not appear on the desktop.</li> <li>▪ Unable to map a network drive.</li> <li>▪ Unable to modify Taskbar &amp; Start Menu settings.</li> <li>▪ The <b>Windows Update</b> icon does not appear on the <b>Start</b> menu.</li> <li>▪ Able to schedule a new task using the Add a New Task wizard.</li> </ul> <p><b>All of the Group Policy settings are enforced, with the exception of being able to schedule a new task by using the Add a New Task wizard. Because the user is logging on to a domain controller, the Admin Template Policy GPO, which is linked to the Domain Controllers OU, is also being applied. The Admin Template Policy GPO contains a setting, which restricts the right to use the Add a New Task wizard, and computer Group Policy overrides user Group Policy.</b></p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> |                                                          |
| 2. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | b. Close all open windows, and then log off.             |

## ◆ Assigning Scripts with Group Policy

**Topic Objective**

To introduce the topics related to assigning scripts in Group Policy.

**Lead-in**

You can use Group Policy to automate the running of scripts.

- What Are Group Policy Script Settings?
- The Process of Applying Script Settings with Group Policy
- Assigning Group Policy Script Settings

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

You can use Group Policy script settings to automate the running of 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 setting once, and Windows 2000 continually implements and enforces it throughout your network.

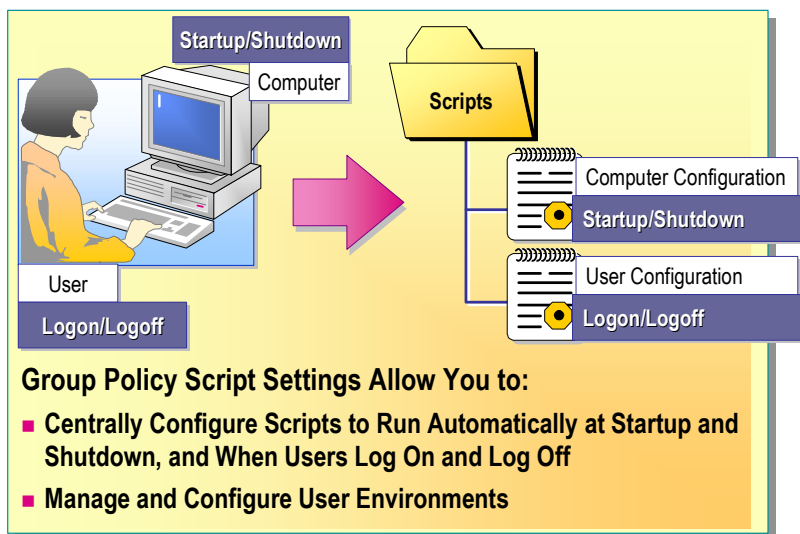
## What Are Group Policy Script Settings?

### Topic Objective

To identify the purpose of Group Policy script settings.

### Lead-in

Using Group Policy script settings, you can set up scripts to run automatically at specific times.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Point students to the Windows Script Technologies Web site for Windows Script Host at: <http://msdn.microsoft.com/scripting/>.

### Key Points

Administrators can use the Scripts extension in Group Policy to run batch files, executable programs, and Windows Script Host supported scripts.

If an administrator needs a Group Policy that cannot be implemented by any existing Group Policy setting, that administrator can set up a script to accomplish the desired result and then run the script through Group Policy.

Group Policy script settings allow you to centrally configure scripts to run automatically at startup and shutdown, and when users log on and log off. You can specify any script that runs in Windows 2000, including batch files, executable programs, and Windows Script Host supported scripts. For more information about Windows Script Host, see the Windows Script Technologies Web site at: <http://msdn.microsoft.com/scripting/>.

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

- Run scripts that perform tasks that you cannot configure through other Group Policy settings. For example, you can populate user environments with network connections, printer connections, shortcuts to applications, and corporate documents.

You can also use scripts to 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 left in the same state as when the user started the computer.

- Run pre-existing scripts already set up to manage user environments until you have set up other Group Policy settings to replace the tasks that these scripts perform.

**Note** 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 of running scripts because you can manage these scripts centrally, along with startup, shutdown, and logoff scripts.

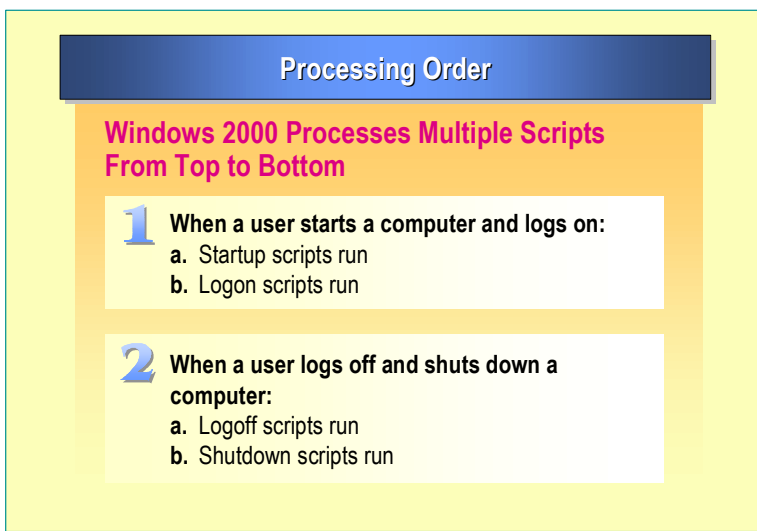
## The Process of Applying Script Settings with Group Policy

### Topic Objective

To identify the process of applying script settings in Group Policy.

### Lead-in

Windows 2000 processes Group Policy scripts in a particular order, which is from top to bottom.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Delivery Tip

On the **Script** tab of the **Startup Properties** dialog box, demonstrate the order in which startup scripts run. To open the dialog box, double-click **Startup** in Computer Configuration\Windows Settings\Scripts.

### Key Points

By default, startup scripts run hidden and synchronously. Running synchronously means that each script must complete or timeout before the next script starts to run.

By default, logon scripts run hidden and asynchronously. Running asynchronously means that the scripts can run simultaneously.

Windows 2000 executes multiple scripts from top to bottom as listed on the **Script** tab of the **Script Properties** dialog box. If there is a conflict between different scripts, the script processed last prevails. Windows 2000 processes and runs Group Policy assigned scripts in the following order:

1. When a user starts a computer and logs on, the following occurs:
  - a. Startup scripts are hidden and run synchronously by default.  
When scripts run synchronously, each script must complete or timeout before the next one starts.
  - b. Logon scripts are hidden and run asynchronously by default.  
When scripts run asynchronously, a script can start running, even while a previous script is running. Multiple scripts can run at the same time.  
Non-Group Policy logon scripts associated with a specific user account run after the Group Policy logon scripts run for the user account.
2. When a user logs off and shuts down a computer, the following occurs:
  - a. Logoff scripts run.
  - b. Shutdown scripts run.

**Note** The default timeout value for processing scripts is 10 minutes. If a script requires more than 10 minutes to process, you must adjust the timeout value by configuring the wait time in Computer Configuration\Administrative Templates\System\Logon\Maximum wait time for Group Policy scripts. This setting affects all scripts that run, not just logon scripts.

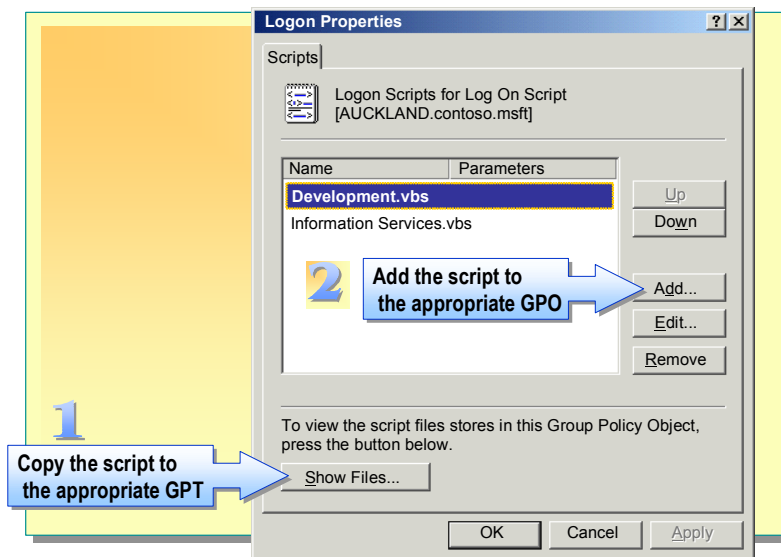
## Assigning Group Policy Script Settings

### Topic Objective

To illustrate the procedure to assign Group Policy scripts settings to users and computers.

### Lead-in

To implement scripts by using Group Policy, you add the script to the appropriate script setting.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Delivery Tip

Demonstrate adding a startup script by using Group Policy. Then show students where the script resides in the GPT.

The path to the location in the GPT is `systemroot\SYSTEMROOT\sysvol\domain_name\policies\GPO_GUID_identifier\machine\scripts\Startup`.

### Key Point

A script must reside in the GPT to run as a Group Policy script.

By adding a script to one of the Group Policy script settings, you can determine when it runs.

Implementing a script means using Group Policy to add that script to the appropriate setting in the GPT. This designates that the script runs during startup, shutdown, logon, or logoff.

1. To copy a script into the appropriate GPT, perform the following steps:
  - a. Locate the script on your hard disk by using Windows Explorer.
  - b. Open the appropriate GPO in Group Policy, expand either **Computer Configuration** (for startup and shutdown scripts) or **User Configuration** (for logon and logoff scripts), expand **Windows Settings**, and then click **Scripts**.
  - c. Double-click the appropriate script type (**Startup**, **Shutdown**, **Logon**, or **Logoff**), and then click **Show Files**.
  - d. Copy the script file from Windows Explorer to the window that appears, and then close the window.
2. To add a script to a GPO, perform the following steps:
  - a. In the **Properties** dialog box for the script type, click **Add**, click **Browse**, select a script, and then click **Open**.
  - b. Add any necessary script parameters, and then click **OK**.

For more information about creating a script in the Microsoft Visual Basic®, Scripting Edition (VBScript) language, see Course 1080, *Essentials of Microsoft® Visual Basic® Scripting Edition 3.0* under the Student Materials Web page on the Student Materials compact disc.

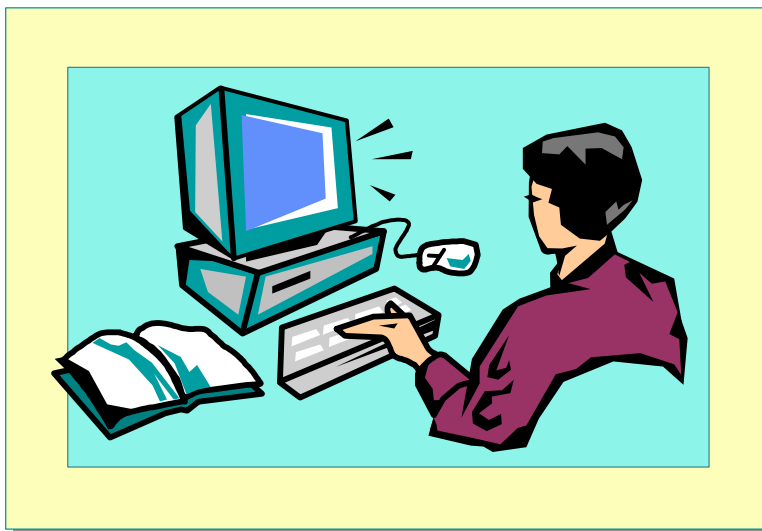
## Lab B: Using Group Policy to Assign Scripts to Users and Computers

**Topic Objective**

To introduce the lab.

**Lead-in**

In this lab, you will create a Group Policy object (GPO), configure the Script settings that satisfy the scenario requirements, and then link the new GPO to an OU.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Explain the lab objectives.

### Objectives

After completing this lab, you will be able to assign scripts to users and computers by using Group Policy.

### Prerequisites

Before working on this lab, you must have a working knowledge of Active Directory Users and Computers.

### Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a domain controller.

**Estimated time to complete this lab: 15 minutes**

## Exercise 1

### Using Group Policy to Assign Scripts

#### Scenario

All Sales users in your organization need to run scripts to configure their desktop environments at logon and perform cleanup tasks at logoff. Retail users must run additional scripts to configure their computers to use proprietary software. You need to assign the following script Group Policy for users in the Sales organizational unit (OU) and its child OUs:

- All users in the Sales OU and the child OUs must run the Sales Logon.vbs script at logon.
- All users in the Sales OU and the child OUs must run the Sales Logoff.vbs script at logoff.
- All users in the Retail OU must run the Retail Logon.vbs script and the Retail Config.vbs script at logon.

#### Goal

In this exercise, you will create a GPO for the Sales OU and a second GPO for the Retail OU. You will configure the settings in the two GPOs to run the required scripts.

| Tasks                                                                                                                           | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a GPO linked to the Sales OU. Name this GPO Sales Script Policy.                                                      | <ol style="list-style-type: none"> <li>a. Log on as Administrator with a password of <b>password</b>.</li> <li>b. Open Active Directory Users and Computers from the <b>Administrative Tools</b> menu.</li> <li>c. In the console tree, expand your domain, right-click <b>Sales</b>, and then click <b>Properties</b>.</li> <li>d. On the <b>Group Policy</b> tab, click <b>New</b>, type <b>Sales Script Policy</b> and then press ENTER.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 2. Copy the Sales Logon script from C:\MOC\Win2154A\Labfiles\Scripts to the Logon folder in the Sales Script Policy GPT folder. | <ol style="list-style-type: none"> <li>a. With <b>Sales Script Policy</b> selected, click <b>Edit</b>.</li> <li>b. In the console tree, under <b>User Configuration</b>, expand <b>Windows Settings</b>, and then click <b>Scripts (Logon/Logoff)</b>.</li> <li>c. In the details pane, double-click <b>Logon</b>, and then in the <b>Logon Properties</b> box, click <b>Show Files</b>. <div style="margin-top: 10px;">  <p><i>A window appears showing the contents of the Logon folder in the Group Policy Template (GPT) for this GPO. Before you can assign a script with this GPO, you must copy the script file to this folder.</i></p> </div> </li> <li>d. Open the C:\MOC\Win2154A\Labfiles\Scripts folder.</li> <li>e. Copy the Sales Logon script file from the Scripts folder to the Logon folder.</li> <li>f. Minimize the Scripts folder, and then close the Logon folder.</li> <li>g. Leave the <b>Logon Properties</b> dialog box open.</li> </ol> |

| Tasks                                                                                                                                                | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Add the Sales Logon script to the list of Logon scripts for the Sales Script Policy GPO.                                                          | <ol style="list-style-type: none"> <li>In the <b>Logon Properties</b> dialog box, click <b>Add</b>.</li> <li>In the <b>Add a Script</b> dialog box, click <b>Browse</b>, click the <b>Sales Logon</b> script, click <b>Open</b>, and then click <b>OK</b>.</li> <li>Click <b>OK</b> to close the <b>Logon Properties</b> dialog box.</li> <li>Leave Group Policy open.</li> </ol>                                                                                                                                                                                                                                                                                                                                                  |
| 4. Copy the Sales Logoff script from C:\MOC\Win2154A\Labfiles\Scripts to the Logoff folder in the Sales Script Policy GPT folder.                    | <ol style="list-style-type: none"> <li>In the details pane, double-click <b>Logoff</b>, and then in the <b>Logoff Properties</b> dialog box, click <b>Show Files</b>.</li> <li>Restore the Scripts window and copy the Sales Logoff script to the Logoff folder.</li> <li>Minimize the Scripts window, and then close the Logoff window.</li> <li>Leave the <b>Logoff Properties</b> dialog box open.</li> </ol>                                                                                                                                                                                                                                                                                                                   |
| 5. Add the Sales Logoff script to the list of Logoff scripts for the Sales Script Policy GPO.                                                        | <ol style="list-style-type: none"> <li>In the <b>Logoff Properties</b> dialog box, click <b>Add</b>.</li> <li>In the <b>Add a Script</b> dialog box, click <b>Browse</b>, click the <b>Sales Logoff</b> script, click <b>Open</b>, and then click <b>OK</b>.</li> <li>Click <b>OK</b> to close the <b>Logoff Properties</b> dialog box, and then close <b>Group Policy</b>.</li> <li>Click <b>Close</b> to close the <b>Sales Properties</b> dialog box.</li> <li>Leave Active Directory Users and Computers open.</li> </ol>                                                                                                                                                                                                      |
| 6. Create a GPO linked to the Retail OU. Name this GPO Retail Script Policy.                                                                         | <ol style="list-style-type: none"> <li>In the details pane, expand <b>Sales</b>, right-click <b>Retail</b>, and then click <b>Properties</b>.</li> <li>On the <b>Group Policy</b> tab, click <b>New</b>, type <b>Retail Script Policy</b> and then press ENTER.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 7. Copy the Retail Logon and Retail Config scripts from C:\MOC\Win2154A\Labfiles\Scripts to the Logon folder in the Retail Script Policy GPT folder. | <ol style="list-style-type: none"> <li>With Retail Script Policy selected, click <b>Edit</b>.</li> <li>In the console tree, under <b>User Configuration</b>, expand <b>Windows Settings</b>, and then click <b>Scripts (Logon/Logoff)</b>.</li> <li>In the details pane, double-click <b>Logon</b>, and then in the <b>Logon Properties</b> dialog box, click <b>Show Files</b>.</li> <li>Restore the Scripts window and copy the Retail Logon and Retail Config scripts from the Scripts folder to the Logon folder.</li> <li>Close the Scripts window and the Logon window.</li> </ol>                                                                                                                                           |
| 8. Add the Retail Logon and the Retail Config scripts to the list of Logon Scripts for the Retail Script Policy GPO.                                 | <ol style="list-style-type: none"> <li>In the <b>Logon Properties</b> dialog box, click <b>Add</b>.</li> <li>In the <b>Add a Script</b> dialog box, click <b>Browse</b>, click the <b>Retail Logon</b> script, click <b>Open</b>, and then click <b>OK</b>.</li> <li>In the <b>Logon Properties</b> dialog box, click <b>Add</b>.</li> <li>In the <b>Add a Script</b> dialog box, click <b>Browse</b>, click the <b>Retail Config</b> script, click <b>Open</b>, and then click <b>OK</b>.</li> <li>Click <b>OK</b> to close the <b>Logon Properties</b> dialog box, and then close Group Policy.</li> <li>Close the <b>Retail Properties</b> dialog box, close Active Directory Users and Computers, and then log off.</li> </ol> |

## Exercise 2

### Verifying Script Assignment

#### Scenario

Now that the required GPOs are setup and configured, you need to confirm that the Group Policy settings are being applied as expected.

#### Goal

Log on using a user account in the Sales OU to verify that the proper scripts are executed. Log on as a user in the Retail OU to verify that the proper scripts are executed.

| Tasks                                                                                                                                                                                                                                                                                                                                      | Detailed Steps                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1. Log on as salesuser to verify that the Sales Logon script executes.                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"><li>Log on as Salesuser with a password of <b>password</b>.</li></ul> |
| <p> Did the Sales Logon script execute? Why or why not?</p> <p><b>Yes, the Sales Logon script was executed. This script was assigned to the Sales OU and will be executed for users in the Sales OU and in all child OUs.</b></p> <hr/> <hr/> <hr/> <hr/> |                                                                                                         |
| 2. Log off to verify that the Sales Logoff script executes.                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"><li>Log off.</li></ul>                                                |
| <p> Did the Sales Logoff script execute?</p> <p><b>Yes.</b></p> <hr/> <hr/> <hr/> <hr/>                                                                                                                                                                 |                                                                                                         |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Detailed Steps                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>3.</b> Log on as retailuser to verify that the Sales Logon, Retail Logon and Retail Config scripts execute.                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"><li>▪ Log on as Retailuser with a password of <b>password</b>.</li></ul> |
| <div data-bbox="321 449 370 499"></div> <div data-bbox="396 436 800 466">Which logon scripts executed and why?</div> <div data-bbox="396 518 1474 611"><b>The Sales Logon, Retail Logon, and Retail Config scripts were executed. The Sales Logon script will be executed for all user accounts in the Sales OU and all child OUs. The Retail Logon and Retail Config scripts will be executed for all user accounts in the Retail OU.</b></div> <div data-bbox="396 657 1490 800"><hr/><hr/><hr/><hr/></div> |                                                                                                            |
| <b>4.</b> Log off to verify that the Sales Logoff script executes.                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"><li>▪ Log off.</li></ul>                                                 |
| <div data-bbox="321 921 370 972"></div> <div data-bbox="396 909 764 938">Did the Sales Logoff script execute?</div> <div data-bbox="396 991 444 1020"><b>Yes.</b></div> <div data-bbox="396 1066 1490 1209"><hr/><hr/><hr/><hr/></div>                                                                                                                                                                                                                                                                        |                                                                                                            |

## ◆ Using Group Policy to Redirect Folders

**Topic Objective**

To introduce the topics related to using Group Policy to redirect user folders.

**Lead-in**

By redirecting folders, you can ensure that users' data is available to them regardless of the computers to which they log on.

- What Is Folder Redirection?
- Selecting the Folders to Redirect
- Redirecting Folders to a Server Location

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Windows 2000 allows you to redirect folders, which 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 at a central location, and that users' data is available to them regardless of the computers to which they log on. It is easier to manage and back up centralized data. The folders that you can redirect are My Documents, Application Data, Desktop, and Start Menu. Windows 2000 automatically creates these folders and makes them part of the user profile for each user account.

## What Is Folder Redirection?

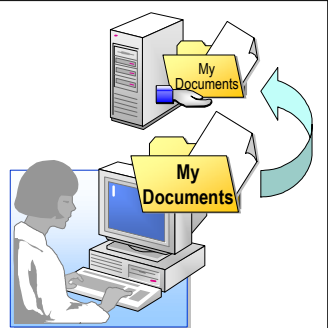
### Topic Objective

To identify the purposes of redirecting folders.

### Lead-in

You can redirect folders so that users can locate and access their data regardless of the computer from which they log on.

### Redirected Personal Folders



Documents Are Stored on the  
Server but Appear to Be  
Stored Locally

### Advantages of Folder Redirection:

- Data Is Always Available to Users Regardless of the Computer Logged on to
- Data Is Centrally Stored for Ease of Management and Backup
- Network Traffic Is Generated Only When Users Gain Access to Files
- Files Are Not Saved on the Client Computer

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Do not go into detail on the four folders, as they are covered in the next topic. Be sure to mention the advantages of folder redirection.

### Key Points

The four folders are part of the user profile.

The data stored on the server appears local to the user.

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 were 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.

The following list describes the advantages of redirecting folders:

- The data in the folders is available to the user regardless of the client computer to which the user logs on.
- The data in the folders is centrally stored, so the files that they contain are easier to manage and back up.
- Network traffic is reduced. When users have roaming user profiles and folders are not redirected, changes to the data in the folders are copied between the local computer and the server each time that the user logs on and logs off. Network traffic is generated only when a user accesses a file.
- Files in redirected folders, unlike files that are part of a roaming user profile, are not copied and saved on the computers where the user logs on. This means that when a user logs on to a client computer, no storage space is used to store these files, and data that might be confidential does not remain on a client computer.

## Selecting the Folders to Redirect

### Topic Objective

To introduce the different types of folders, and the reasons to redirect these folders.

### Lead-in

Depending on the needs of users and your network, you may redirect My Documents, Application Data, Desktop, and Start Menu folders.

| Folder           | Contains                                                | Redirect to a server so that                                                                                 |
|------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| My Documents     | A user's personal data                                  | Users can access their data from any computer, and this data can be backed up and managed centrally          |
| Start Menu       | Folders and shortcuts on the <b>Start</b> menu          | Users' <b>Start</b> menus are standardized                                                                   |
| Desktop          | All files and folders that a user places on the desktop | Users have the same desktop regardless of the computer to which they log on                                  |
| Application Data | User-specific data stored by applications               | Applications use the same user-specific data for a user regardless of the computer to which the user logs on |

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Emphasize that administrators should always redirect the My Documents folder.

### Key Point

You can standardize user **Start** menus by redirecting their Start Menu folders to the same folder and then assigning only the NTFS Read permission so that users cannot change the contents of their **Start** menus.

Depending on the needs of users and your network, you may redirect all or some of the folders that can be redirected. The following table describes what each folder contains and provides specific reasons for redirecting the folder.

| Folder           | Contains                                                                                                                                                                                                                                                                                                                   | Redirect to a server so that                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| My Documents     | The default location where users store their personal work data. It is the default location for the <b>Open</b> and <b>Save As</b> commands on the <b>File</b> menu. Windows 2000 places a <b>My Documents</b> shortcut icon on the desktop. It also includes the My Pictures folder, where users can save their graphics. | User can access data from any computer, and this data can be backed up and managed centrally, and the amount of data saved in the user profile is reduced.<br><br>Always redirect the My Documents folder, because it is important that users are always able to gain access to their data. |
| Start Menu       | Folders and shortcuts on the <b>Start</b> menu.                                                                                                                                                                                                                                                                            | Users' <b>Start</b> menus are standardized. Redirect multiple users' Start Menu folders to the same network location and then assign only the NTFS file system Read permission so that users cannot change their <b>Start</b> menu content.                                                 |
| Desktop          | The folder that contains all files, folders, and shortcuts that a user places on his or her desktop.                                                                                                                                                                                                                       | Users' desktops are standardized. Use the same strategy that you use for the <b>Start</b> menu.                                                                                                                                                                                             |
| Application Data | User-specific data stored by applications, such as configuration files and personal dictionaries for spell checking.                                                                                                                                                                                                       | Applications use the same user-specific data for a user, regardless of the computer to which the user logs on.                                                                                                                                                                              |

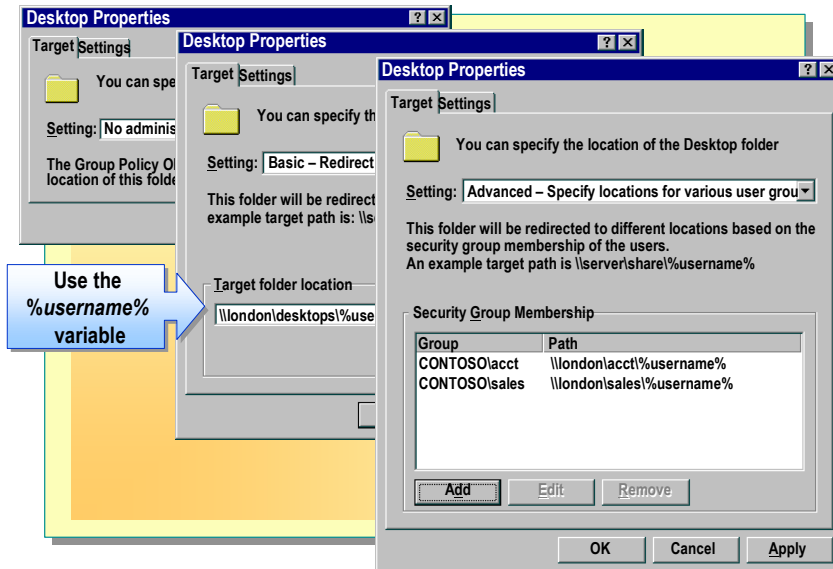
## Redirecting Folders to a Server Location

### Topic Objective

To illustrate how to redirect folders to a server location by using Group Policy.

### Lead-in

You use the Folder Redirection extension in Group Policy to redirect folders.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

### Delivery Tip

Demonstrate, at an OU level, configuring the Group Policy settings to redirect My Documents to a shared folder on a server.

Demonstrate the three other settings related to folder redirection.

### Key Points

An administrator redirects the four folders by using the Folder Redirection extension in Group Policy.

If an administrator uses the `%username%` variable when redirecting a folder, then Windows 2000 creates a unique personal folder on the server for each user to which it applies the Group Policy setting.

To store the My Documents, Application Data, Desktop, and Start Menu folders on a server, use the Folder Redirection extension in Group Policy.

To redirect a folder, perform the following steps:

1. Create a new GPO or select an existing GPO, and then click **Edit**.
2. Expand **User Configuration**, expand **Windows Settings**, and then expand **Folder Redirection**.
3. Right-click the name of the folder that you want to redirect, click **Properties**, and then provide the target location and path to the location.

The options on the **Target** tab are described in the following table.

| Options                          | Description                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Setting</b>                   | <p><b>No administrative policy specified.</b> Selected by default.</p> <p><b>Basic.</b> Redirects all folders to the same location.</p> <p><b>Advanced.</b> Specifies locations for various security groups. This option allows you to redirect the folders of users to whom this GPO applies and to specify different locations, depending on group membership.</p> |
| <b>Target folder location</b>    | <p>This option appears when you select <b>Basic</b>. This option redirects all folders to the same location and allows you to specify a universal naming convention (UNC) path name to the new location. You can use the following syntax to create target folders named after a user's logon name:</p> <p><code>\\server_name\share_name%\%username%</code></p>     |
| <b>Security Group Membership</b> | <p>This option appears when you select <b>Advanced</b>. This option specifies locations for various security groups. The security groups and the path to the redirected folders appear here. As with the previous option, you can use <code>\\server_name\share_name%\%username%</code> to create folders named after a user's logon name.</p>                       |

The options on the **Setting** tab control the behavior of folder redirection. You should be aware of the defaults for these settings, as they have implications for server disk space and security. The settings for folder redirection are explained in the following table:

| Setting                                                        | Effect                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Grant the user exclusive rights to <i>folder</i>.</b>       | <p>Enabled by default, this setting ensures that only the user and the system have rights to the folder. Administrators do not have access to the folder.</p> <p>If this check box is cleared, the new folder location will retain the rights of the previous location.</p> |
| <b>Move the contents of <i>folder</i> to the new location.</b> | <p>Enabled by default, this setting moves the contents of the folder to the new location the next time Group Policy is applied.</p> <p>If this check box is cleared, the folder will be redirected, but the contents will remain in the previous location.</p>              |
| <b>Policy Removal.</b>                                         | <p>By default, when a folder redirection Group Policy is removed, the folder remains in the redirected location.</p> <p>You can also choose to return redirected folders to the local user profile location when Group Policy is removed.</p>                               |

## Lab C: Implementing Folder Redirection Policy

**Topic Objective**

To introduce the lab.

**Lead-in**

In this lab, you will use Group Policy to redirect the My Documents folder to a shared folder, and verify that My Documents is redirected.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Explain the lab objectives.

### Objective

After completing this lab, you will be able to implement folder redirection by using Group Policy.

### Prerequisites

Before working on this lab, you must have an understanding of Group Policy.

### Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller.

**Estimated time to complete this lab: 15 minutes**

## Exercise 1

### Implementing Folder Redirection Policy

#### Scenario

Northwind Traders has a policy that only data on the servers will be backed up. To address fault tolerance concerns, you do not want the contents of the My Documents folder to be stored locally. You want to redirect the folder to the user's home directory on the server because the servers get backed up every evening.

#### Goal

In this exercise, you will redirect the My Documents folder to a new location on the network by using Group Policy.

| Tasks                                                                                                                                                                                                               | Detailed Steps                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Confirm the current location of My Documents for the salesuser account and create a text file in the My Documents folder.                                                                                        | a. Log on as Salesuser with a password of <b>password</b> .<br>b. Open the <b>Properties</b> dialog box for My Documents.                                                                       |
|  What is the current location of My Documents?<br><br><b>C:\Documents and Settings\Salesuser.</b><br><br><hr/> <hr/> <hr/> <hr/> |                                                                                                                                                                                                 |
|  Can the user change this location?<br><br><b>Yes.</b><br><br><hr/> <hr/> <hr/> <hr/>                                            |                                                                                                                                                                                                 |
| 1. (continued)                                                                                                                                                                                                      | c. Close the <b>My Documents Properties</b> dialog box, and then open the My Documents folder.<br>d. Create a text file in the My Documents folder.<br>e. Close My Documents, and then log off. |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2. Redirect the My Documents folder for a user in the Sales OU. Use the following settings for the redirected folder:</p> <ul style="list-style-type: none"> <li>Setting: Basic – Redirect everyone's folder to the same location.</li> <li>Target:<br/>\\computer\redirect\%username% (where <i>computer</i> is your computer name).</li> <li>Policy Removal: Redirect the folder back to the local user profile location when Group Policy is removed.</li> </ul>                                                                                                   | <ol style="list-style-type: none"> <li>Log on as Administrator with a password of <b>password</b>.</li> <li>At the root of drive C, create a folder named Redirect, and then share it with the default permissions.</li> <li>Open Active Directory Users and Computers from the <b>Administrative Tools</b> menu.</li> <li>In the console tree, expand your domain, right-click <b>Sales</b>, and then click <b>Properties</b>.</li> <li>On the <b>Group Policy</b> tab, create a new GPO named <b>Folder Redirect Policy</b>, and then click <b>Edit</b>.</li> <li>Under <b>User Configuration</b>, expand <b>Windows Settings</b>, expand <b>Folder Redirection</b>, right-click <b>My Documents</b>, and then click <b>Properties</b>.</li> <li>In the <b>Setting</b> list, click <b>Basic – Redirect everyone's folder to the same location</b>.</li> <li>Under <b>Target folder location</b>, type \\computer\redirect\%username% (where <i>computer</i> is your computer name), and then click the <b>Settings</b> tab.</li> </ol> |
| <p> Record the default settings for folder redirection in the following space.</p> <p><b>Grant the user exclusive rights to My Documents is enabled.</b></p> <p><b>Move the contents of My Documents to the new location is enabled.</b></p> <p><b>Policy Removal defaults to leave the folder in the new location when the Group Policy is removed.</b></p> <p><b>My Pictures Preferences defaults to making My Pictures a subfolder of My Documents.</b></p> <hr/> <hr/> <hr/> <hr/> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ol style="list-style-type: none"> <li>Click <b>Redirect the folder back to the local user profile location when policy is removed</b>, and then click <b>OK</b>.</li> <li>Close all open windows, and then log off.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 3. Verify that the Folder Redirection Group Policy is being applied properly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ol style="list-style-type: none"> <li>Log on as Salesuser with a password of password.</li> <li>Open the Properties dialog box for My Documents.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Tasks                                                                                                                                                                                                                                                                                            | Detailed Steps                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <p><b>?</b> What is the current location of My Documents?</p> <p>\\computer\redirect\SalesUser (where <i>computer</i> is your assigned computer name).</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>                                                                                   |                                                                                                   |
| <p><b>?</b> Can the user change the location of My Documents? Why or why not?</p> <p>No because the folder was redirected by using Group Policy.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>                                                                                         |                                                                                                   |
| <p><b>?</b> What permissions are set on My Documents? Why?</p> <p>The permissions are SYSTEM– Full Control and SalesUser – Full Control. The default setting for folder redirection is to grant the user exclusive access to the folder.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> |                                                                                                   |
| <p><b>3.</b> (continued)</p>                                                                                                                                                                                                                                                                     | <p><b>c.</b> Close the <b>My Documents Properties</b> dialog box, and then open My Documents.</p> |
| <p><b>?</b> Does the My Documents folder contain the text file that you created earlier? Why or why not?</p> <p>Yes. The default setting for folder redirection moves the contents of the redirected folder to the new location.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p>         |                                                                                                   |
| <p><b>3.</b> (continued)</p>                                                                                                                                                                                                                                                                     | <p><b>d.</b> Close My Documents, and then log off.</p>                                            |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Remove the Folder Redirection Policy GPO.                                                                                                                                                                                                                                                                                                                                                                                                             | <ol style="list-style-type: none"> <li>Log on as Administrator with a password of <b>password</b>.</li> <li>Open Active Directory Users and Computers from the <b>Administrative Tools</b> menu.</li> <li>In the console tree, expand your domain, right-click <b>Sales</b>, and then click <b>Properties</b>.</li> <li>On the <b>Group Policy</b> tab, select the <b>Folder Redirect Policy</b> GPO, and then click <b>Delete</b>.</li> <li>In the <b>Delete</b> dialog box, click <b>Remove the link and delete the Group Policy Object permanently</b>, and then click <b>OK</b>.</li> <li>In the <b>Delete Group Policy Object</b> dialog box, click <b>Yes</b>, and then click <b>Close</b> to close the <b>Sales Properties</b> box.</li> <li>Close all open windows, and then log off.</li> </ol> |
| 5. Test the results of deleting the Folder Redirect Policy GPO.                                                                                                                                                                                                                                                                                                                                                                                          | <ol style="list-style-type: none"> <li>Log on as Salesuser with a password of <b>password</b>.</li> <li>Right-click <b>My Documents</b>, and then click <b>Properties</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p> What is the current location of My Documents? Is this the default behavior when folder redirection Group Policy is removed?</p> <p><b>C:\Documents and Settings\Salesuser. No, the default behavior when folder redirection Group Policy is removed is to leave the redirected folder on the network share where it was redirected.</b></p> <hr/> <hr/> <hr/> <hr/> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 5. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ol style="list-style-type: none"> <li>Close all open windows, and then log off.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

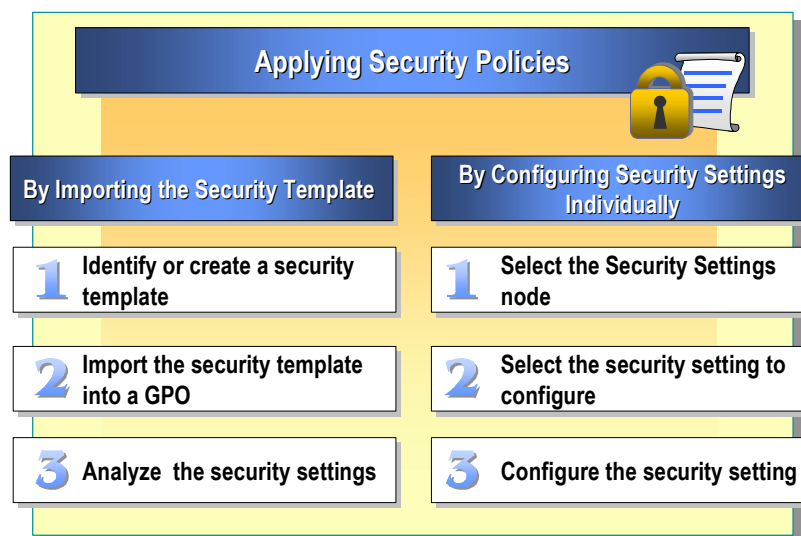
# Using Group Policy to Secure the User Environment

## Topic Objective

To illustrate how to apply security Group Policy to secure the user environment by using Group Policy.

## Lead-in

Security policies can be implemented on a per-computer basis or on the site, domain, or OU level by using Group Policy.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

## Delivery Tip

Demonstrate how to import a security template by using Group Policy.

Demonstrate how to apply security policies by individually configuring each security setting.

## Key Points

Use Group Policy to standardize security settings.

Import security templates into Security Settings in Group Policy to apply consistent and tested security policies to computers in an Active Directory container.

Group Policy also includes security settings to ensure that the user environment is secured against unauthorized access and define an organization's prevention and response to security infractions. Group Policy allows you to standardize security settings by applying the same security template to multiple computers in one step. Security templates are groups of security settings that can be imported into GPOs or used for analysis.

## Setting Account Policies

When you set account policies in Active Directory, keep in mind that Windows 2000 allows only one domain account policy for each domain. The domain account policy becomes the default account policy of any Windows 2000-based workstation or server that is a member of the domain. The only exception to this rule is when another account policy is defined for an organizational unit. The account policy settings for the organizational unit affect the local policy on any computers contained in the organizational unit. This means that the account policies set at the domain level always apply when logging on using an account that exists in the domain. The local policy settings apply only when logging on using an account that is local to the computer to which you are logging on.

## Applying Security Policies

To apply security policies for a local computer or an Active Directory container, you import one or more security templates, which contain security settings for all security areas, into Security Settings in Group Policy. Importing a security template into Group Policy ensures that all members of the container automatically receive the security template when Group Policy propagates. When you apply a template to existing security settings, the settings in the template are merged into the computer's security settings database.

To import a security template into a GPO, perform the following tasks:

1. Identify an existing Windows 2000 security template that contains the required security configuration, or create a new security template.
2. Import the security template into the GPO:
  - a. Expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
  - b. Right-click **Security Settings**, and then click **Import Policy**.
  - c. Select the security template that you want to import, and then click **OK**.
3. Analyze the security settings for each computer to determine if the current security settings should be modified to meet your organization's security requirements.

---

**Note** Before deploying a security template to large groups of computers, it is important to analyze the results of applying a configuration to ensure there are no adverse effects on applications, connectivity, or security. A thorough analysis can also help you identify security breaches and deviations from standard configurations. The Security Configuration and Analysis snap-in allows you to create and review hypothetical scenarios and make adjustments to a configuration.

---

An alternative method of applying security policies is to individually configure the security settings for each computer. You can edit the security settings in a Group Policy object (GPO) for any site, domain, or OU.

To configure a security setting, perform the following tasks:

1. Expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
2. In the Policy details pane, double-click the security setting that you want to configure.
3. On the Policy tab, configure the security setting by selecting one of three states, Enabled, Disabled, or Not Configured, for the setting.

For more information about the different types of security policies, and the utilities used to configure and analyze security settings, see Course 2152, *Implementing Microsoft Windows 2000 Professional and Server*.

---

**Note** Security settings, unlike other Group Policy settings, are persistent. That is, security settings remain in the registry even when the GPO that contains the security settings has been removed.

---

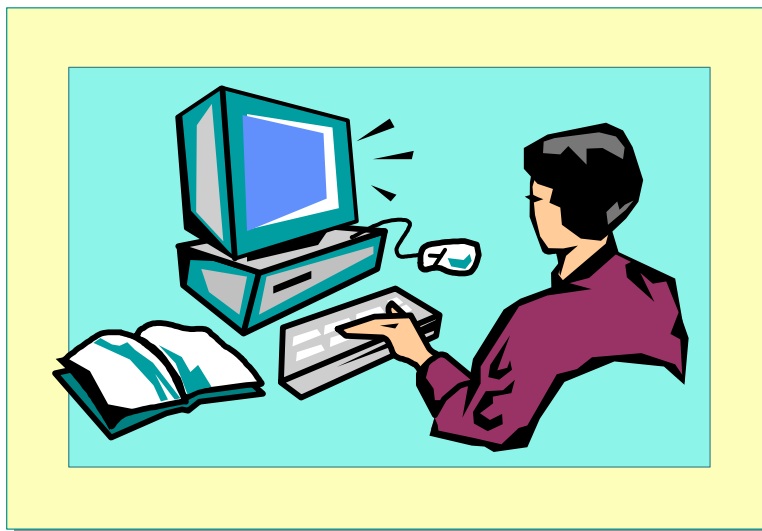
## Lab D: Implementing Security Settings by Using Group Policy

**Topic Objective**

To introduce the lab.

**Lead-in**

In this lab, you will create a Group Policy object (GPO) linked to the OU that contains your domain controller, import the security template to the GPO, and then manually configure the Audit Group Policy settings.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Explain the lab objectives.

### Objectives

After completing this lab, you will be able to implement security settings by using Group Policy.

### Prerequisites

Before working on this lab, you must have an understanding of Group Policy.

### Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server configured as a domain controller.

**Estimated time to complete this lab: 15 minutes**

## Exercise 1

### Implementing Security Policy

#### Scenario

You are a domain administrator for a domain in the Northwind Traders organization, and are required to implement the following security settings on your domain controllers:

- Passwords must be at least six characters.
- A dialog box should appear during the logon process, informing users that unauthorized access is not allowed.
- Domain Admins should have only the Administrator account as a member.
- Telnet, which is set to start manually, should be disabled.

#### Goal

In this exercise, you will create a new GPO, which is linked to the Domain Controllers OU and named Additional Security Settings Policy, to implement the required security settings.

| Tasks                                                                                                                                                                                                                                          | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Create a new GPO linked to the Domain Controllers OU. Name this new GPO Additional Security Settings Policy.                                                                                                                                | <ol style="list-style-type: none"> <li>a. Log on as Administrator with a password of <b>password</b>.</li> <li>b. Open Active Directory Users and Computers from the <b>Administrative Tools</b> menu.</li> <li>c. In the console tree, expand your domain, right-click <b>Domain Controllers</b>, and then click <b>Properties</b>.</li> <li>d. On the <b>Group Policy</b> tab, click <b>New</b>, type <b>Additional Security Settings Policy</b> and then press ENTER.</li> </ol>                                                                                                                                                                                         |
| 2. Modify the Additional Security Settings Policy GPO to implement the following security setting: <ul style="list-style-type: none"> <li>• Passwords must be at least six characters.</li> </ul>                                              | <ol style="list-style-type: none"> <li>a. With the Additional Security Settings Policy GPO selected, click <b>Edit</b>.</li> <li>b. Under <b>Computer Configuration</b>, expand <b>Windows Settings</b>, expand <b>Security Settings</b>, expand <b>Account Policies</b>, and then click <b>Password Policy</b>.</li> <li>c. In the details pane, double-click <b>Minimum password length</b>.</li> <li>d. In the <b>Security Policy Setting</b> dialog box, click <b>Define this policy setting</b>, change the value for the minimum password length to <b>6</b>, and then click <b>OK</b>.</li> </ol>                                                                    |
| 3. Modify the Additional Security Settings Policy GPO to implement the following security setting: <ul style="list-style-type: none"> <li>• Display a dialog box at logon that warns users that unauthorized access is not allowed.</li> </ul> | <ol style="list-style-type: none"> <li>a. In the console tree, expand <b>Local Policies</b>, and then click <b>Security Options</b>.</li> <li>b. In the details pane, double-click <b>Message text for users attempting to logon</b>.</li> <li>c. In the <b>Security Policy Setting</b> dialog box, click <b>Define this policy setting</b>, type <b>Authorized access only</b> and then click <b>OK</b>.</li> <li>d. In the details pane, double-click <b>Message title for users attempting to logon</b>.</li> <li>e. In the <b>Security Policy Setting</b> dialog box, click <b>Define this policy setting</b>, type <b>Warning</b> and then click <b>OK</b>.</li> </ol> |

| Tasks                                                                                                                                                                                                                             | Detailed Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>4. Modify the Additional Security Settings Policy GPO to implement the following security setting:</p> <ul style="list-style-type: none"> <li>Domain Admins should have only the Administrator account as a member.</li> </ul> | <ol style="list-style-type: none"> <li>In the console tree, click <b>Restricted Groups</b>.</li> <li>Right-click <b>Restricted Groups</b>, and then click <b>Add Group</b>.</li> <li>In the <b>Add Group</b> dialog box, click <b>Browse</b>, type <b>Domain Admins</b> click <b>OK</b>, and then click <b>OK</b> again to close the <b>Add Group</b> dialog box.</li> <li>In the details pane, double-click <i>Domain\</i><b>Domain Admins</b>.</li> <li>In the <b>Configure Membership for Domain\Domain Admins</b> dialog box, click <b>Add</b> to the right of <b>Members of this group</b>.</li> <li>In the <b>Add Member</b> dialog box, click <b>Browse</b>, type <b>Administrator</b> click <b>OK</b>, and then click <b>OK</b> again to close the <b>Add Member</b> dialog box.</li> <li>Click <b>OK</b> to close the <b>Configure Membership for Domain\Domain Admins</b> dialog box.</li> </ol>                                                                               |
| <p>5. Modify the Additional Security Settings Policy GPO to implement the following security setting:</p> <ul style="list-style-type: none"> <li>The Telnet service should be disabled.</li> </ul>                                | <ol style="list-style-type: none"> <li>In the console tree, click <b>System Services</b>.</li> <li>In the details pane, double-click <b>Telnet</b>.</li> <li>In the <b>Security Policy Setting</b> dialog box, click <b>Define this policy setting</b>.<br/>  <i>Notice that the <b>Security for Telnet</b> security editor appears. System services need to be properly secured, so this dialog box appears for any service in the list.</i> </li> <li>Select <b>Everyone</b>, and then click <b>Remove</b>.</li> <li>Click <b>Add</b>, type <b>Domain Admins</b> and then click <b>OK</b>.</li> <li>Select the <b>Allow</b> check box beside <b>Full Control</b>, and then click <b>OK</b>.</li> <li>In the <b>Security Policy Setting</b> dialog box, ensure that <b>Disabled</b> is selected, and then click <b>OK</b>.</li> <li>Close all open windows, and then restart the computer.</li> </ol> |
| <p>6. Verify that the modifications to the Additional Security Settings Policy GPO are being applied correctly.</p>                                                                                                               | <ol style="list-style-type: none"> <li>Log on as Administrator with a password of <b>password</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p> Did the warning message appear when you tried to log on?</p> <p>Yes.</p> <hr/> <hr/> <hr/> <hr/>                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Tasks                                                                                                                                                                                                                                                                                                                                                                                                                            | Detailed Steps                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                   | b. Change your password from <b>password</b> to <b>123</b> .                                                                                                                                                                                                                                 |
| <p> Did the minimum password length Group Policy setting of six characters prevent you from changing your password to one that contained only three characters? Why or why not?</p> <p><b>No, the password was changed successfully. Password Group Policy is only enforced when it is set at the domain level.</b></p> <hr/> <hr/> <hr/> <hr/> |                                                                                                                                                                                                                                                                                              |
| 6. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>c. If necessary, change your password back to password.</p> <p>d. Add the Guest user account to the Domain Admins group.</p> <p>e. Force a refresh of Group Policy by opening a command prompt, typing <b>secedit /refreshpolicy machine_policy /enforce</b> and then pressing ENTER.</p> |
| <p> Is the Guest user account still listed as a member of the Domain Admins group? Why or why not?</p> <p><b>No. The membership of Domain Admins is restricted to the Administrator account. When Group Policy was refreshed, the Guest account was removed.</b></p> <hr/> <hr/> <hr/> <hr/>                                                   |                                                                                                                                                                                                                                                                                              |
| 6. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                   | f. Open Services from the Administrative Tools menu.                                                                                                                                                                                                                                         |
| <p> What is the value in the <b>Startup Type</b> column for the Telnet service?</p> <p><b>Disabled.</b></p> <hr/> <hr/> <hr/> <hr/>                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                              |
| 6. (continued)                                                                                                                                                                                                                                                                                                                                                                                                                   | g. Close all open windows.                                                                                                                                                                                                                                                                   |
| 7. Run the Delpol.cmd batch file in the C:\Moc\Win2154A\Labfiles folder. This batch file removes all GPOs created in the labs in this module.                                                                                                                                                                                                                                                                                    | <p>a. Open the C:\Moc\Win2154A\Labfiles folder.</p> <p>b. Double-click <b>Delpol.cmd</b> to remove all of the GPOs created during the labs in this module.</p> <p>c. Restart your computer.</p>                                                                                              |

# Troubleshooting User Environment Management

**Topic Objective**

To introduce troubleshooting options for resolving problems that may occur when using Group Policy to manage user environments.

**Lead-in**

You may encounter problems when managing the user environment through Group Policy.



\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

You may encounter problems when using Group Policy to manage user environments. Here are some of the more common problems that you may encounter, along with suggested strategies for resolving them:

- Registry settings using Administrative Templates are not applied. The possible problem could be that the administrative template settings are not applied to the user or computer affected by Group Policy. Another possible problem could be that Active Directory replication had not yet completed on the Domain Controller. Run Gpresult.exe in verbose mode on the client computer to confirm that Administrative Templates Group Policy settings are not applied.
  - If the text “The user (or computer) received "Registry" settings from these GPOs.” does not appear in the output, no administrative template settings were applied. If this text does not appear, verify to make sure that the user or computer account has at least Read and Apply Group Policy permissions on all GPOs that should be processed.
  - Also, verify the relevant GPOs to see if either the User Configuration or Computer Configuration nodes are disabled.
  - Finally, verify to see if the *Loopback processing* mode is enabled.
- Scripts do not execute.
  - Confirm that the Group Policy Scripts client-side extension is executing. Run Gpresult.exe in verbose mode, and examine the output under the User received Scripts settings from these GPOs heading. If the text is missing from the output, verify permissions on the relevant GPOs and check for inheritance issues.
  - If the text appears in the output, but certain scripts are not executing, verify to insure that SYSVOL is being properly replicated to all domain controllers.

- Folders are not being redirected.
  - If you are using redirected folders and they are not being redirected, verify the discretionary access control list (DACL) on the network share where the folders are being redirected. Ensure that the user has sufficient permissions.
  - If the volume that contains the redirected folders has disk quotas enabled, verify that the user has not exceeded his or her quota limit.
  - If the folder on the network share existed before you implemented redirection, ensure that the DACL for the folder allows the user Full Control.

---

**Note** For additional strategies for troubleshooting Group Policy to manage user environments, see Module 7, “Implementing Group Policy,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

---

## Best Practices

### Topic Objective

To identify best practices for managing user environments.

### Lead-in

Review this checklist before you use Group Policy to manage user environments.



**Create a Minimal Number of GPOs Required**



**Place All Computers Affected by Loopback in the Same OU**



**Always Test the Effects of Administrative Template Settings**



**Make Sure That Scripts Run in the Preferred Order**



**Always Redirect the My Documents Folders**

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Emphasize the reason for each best practice.

The following list provides best practices for managing user environments:

- Create a minimal number of GPOs containing administrative template settings. It can be difficult to manage user environments properly if you create too many GPOs containing these settings.
- Place all computers to which you want to apply the loopback processing mode in their own OU. There should not be any user accounts in that OU. Then you can create and link a GPO with configured settings that specifically set up the user environment on these computers.
- Always test the effects of administrative template settings. Create a test environment that is parallel to your production environment. Give selected users an additional user account that resides in a test OU and have them perform their normal tasks to ensure that there are no problems. If you are going to lock down user desktops, ensure that you have the correct settings configured so that you do not inadvertently disrupt users' work.
- Make sure that scripts run in the preferred order so that you get the proper results. Windows 2000 processes Group Policy settings in a particular order. This process determines the order in which scripts run and the effects they have on computers and users.
- Always redirect the My Documents folders so users can access their personal data from any computer. It reduces logon and logoff times for roaming users, because files in the My Documents folder are only copied between the client computer and the server when users gain access to files. Redirecting My Documents allows you to back up users' data centrally.

# Review

## Topic Objective

To reinforce module objectives by reviewing key points.

## Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Managing User Environments
- Introduction to Administrative Templates
- Using Administrative Templates in Group Policy
- Assigning Scripts with Group Policy
- Using Group Policy to Redirect Folders
- Using Group Policy to Secure the User Environment
- Troubleshooting User Environment Management
- Best Practices

\*\*\*\*\*ILLEGAL FOR NON-TRAINER USE\*\*\*\*\*

Give the students time to read and answer the review questions on their own, and then go over the answers as a group.

1. You do not want users to be able to open Control Panel and gain access to Display or any of the other applications. What do you do?

**Configure an administrative template setting (Start Menu & Taskbar\Disable Changes to Control Panel) that prevents users from modifying the Start menu and taskbar. Control Panel will not appear on the Start menu, and users will not be able to gain access to it.**

2. Your network no longer needs a user administrative template setting that you configured. What do you do to change the registry back to the way it was before you configured the settings?

**You select the not configured state for the setting. Then the setting is not present in the Registry.pol file. The next time that the user starts the computer and logs on, the Registry.pol file does not contain this setting or its value, and it is not applied.**

3. The Research department employees need a shortcut on their desktops to a special third-party application that resides on a network server. There are no existing Group Policy settings that can provide this shortcut. There is a Research Department OU. What can you do?

**Write a script to create shortcuts on users' desktops that connect to the applications and documents. Use Group Policy script settings to automate the running of the script at logon and link the GPO that contains the settings to the Research Department OU.**

4. Employees in the Production Department log on at different client computers. All users need to have their work data available to them at all times. What do you need to do?

**Redirect the My Documents folder to a shared folder on a network server. Regardless of where users log on, they can gain access to their documents.**

5. You need to configure identical security settings for six domain servers that are in the same OU. What is the simplest method for doing this?

**Create and test a security template with the settings that you require. Import the template into a GPO and link the GPO to the OU that contains the domain servers.**