

Module 8: Implementing Group Policy

Contents

Overview	1
Multimedia: Introduction to Group Policy	2
Lesson: Implementing Group Policy Objects	3
Lesson: Implementing GPOs on a Domain	10
Lesson: Managing the Deployment of Group Policy	21
Lab A: Implementing Group Policy	33
Course Evaluation	38



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, place or event 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.

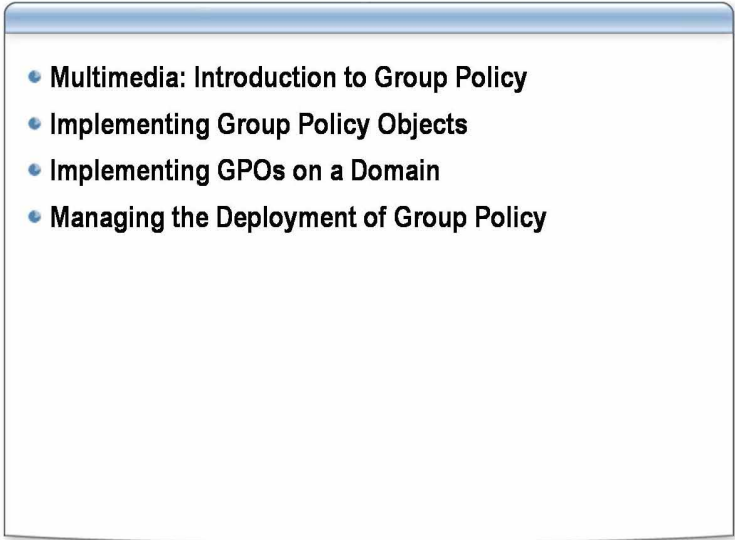
Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these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

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, IntelliMirror, MSDN, PowerPoint, Visual Basic, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Overview

- 
- **Multimedia: Introduction to Group Policy**
 - **Implementing Group Policy Objects**
 - **Implementing GPOs on a Domain**
 - **Managing the Deployment of Group Policy**

Introduction

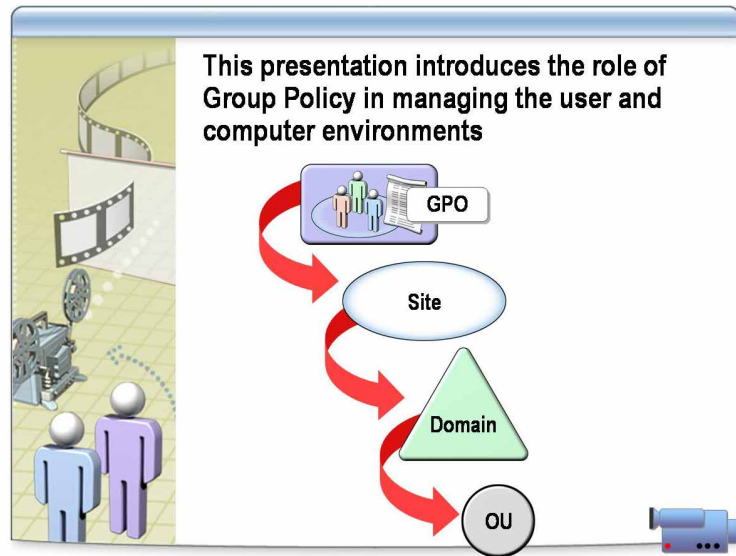
The information in this module introduces the job function of implementing Group Policy. Specifically, the module provides the skills and knowledge that you need to explain the purpose and function of Group Policy in a Microsoft® Windows® Server 2003 environment, implement Group Policy objects (GPOs), and manage GPOs.

Objectives

After completing this module, you will be able to:

- Implement a Group Policy objects.
- Implement GPOs on a domain.
- Manage the deployment of Group Policy.

Multimedia: Introduction to Group Policy



File location

To view the *Introduction to Group Policy* presentation, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objectives

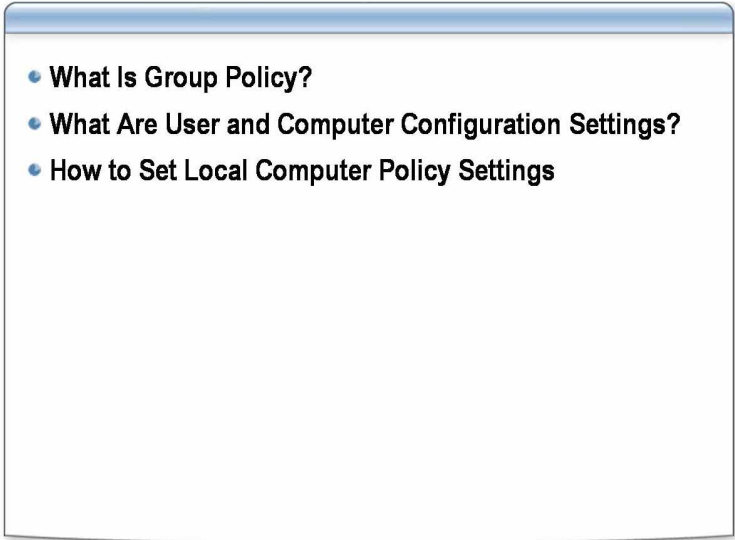
After completing this lesson, you will be able to:

- Describe the types of settings that you can define in Group Policy.
- Describe how Group Policy is applied.

Additional reading

For more information about how clients apply Group Policy, see "Order of events in startup and logon" at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxp/proddocs/orderofevents.asp>.

Lesson: Implementing Group Policy Objects

- 
- What Is Group Policy?
 - What Are User and Computer Configuration Settings?
 - How to Set Local Computer Policy Settings

Introduction

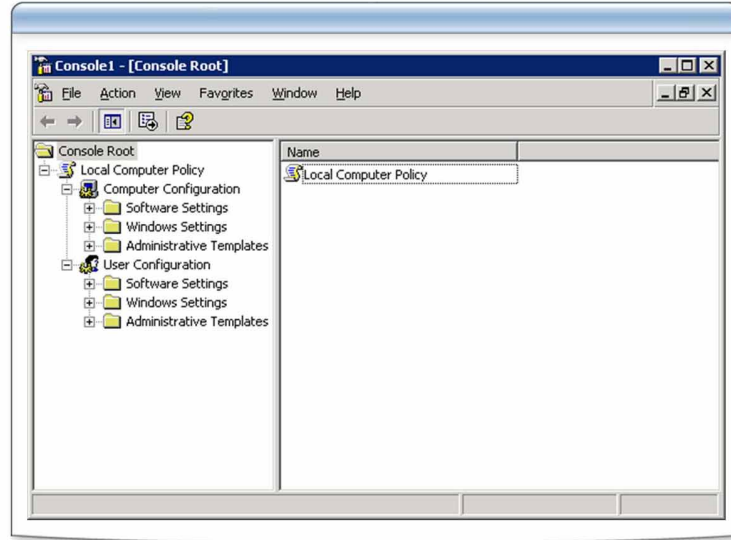
After completing this lesson, students will be able to implement GPOs.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what Group Policy is.
- Describe users and computer configuration settings.
- Set local computer policy settings.

What Is Group Policy?



Definition

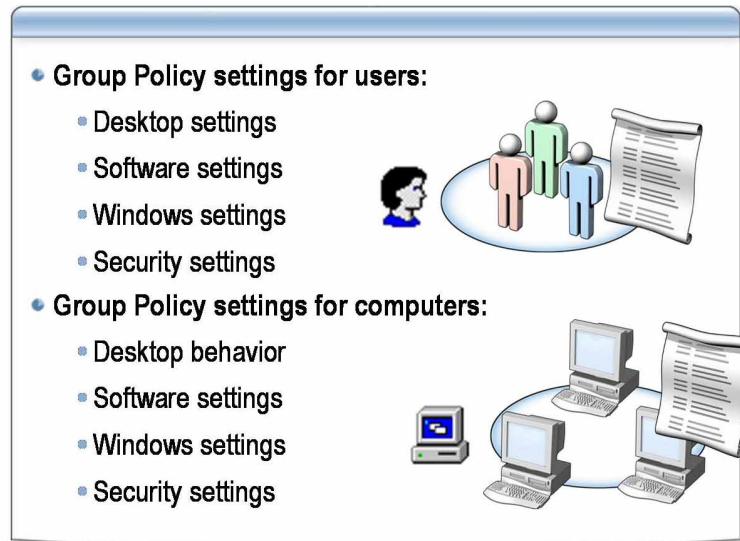
The Active Directory® directory service uses Group Policy to manage users and computers in your network. When using Group Policy, you can define the state of a user's work environment once, and then rely on the Windows Server 2003 family to continually enforce the Group Policy settings that you defined. You can apply Group Policy settings across an entire organization, or you can apply Group Policy settings to specific groups of users and computers.

Additional reading

For more information about Group Policy, see:

- "Microsoft IntelliMirror®" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_IMirror_top_node.asp.
- "Group Policy settings overview" at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/gpsettings.asp>.

What Are User and Computer Configuration Settings?



Introduction

You can enforce Group Policy settings for computers and users by using the Computer Configuration and User Configuration features in Group Policy.

User configuration

Group Policy settings for users include specific operating system behavior, desktop settings, security settings, assigned and published application options, application settings, folder redirection options, and user logon and logoff scripts. User-related Group Policy settings are applied when users log on to the computer and during the periodic refresh cycle.

Group Policy settings that customize the user's desktop environment, or enforce lockdown policies on users, are contained under User Configuration in Group Policy Object Editor.

Software settings for user configuration

The Software Settings folder under User Configuration contains software settings that apply to users regardless of which computer they log on to. This folder also contains software installation settings, and it might contain other settings that are placed there by independent software vendors (ISVs).

Windows settings for user configuration

The Windows Settings folder under User Configuration contains Windows settings that apply to users regardless of which computer they log on to. This folder also contains the following items: Folder Redirection, Security Settings, and Scripts.

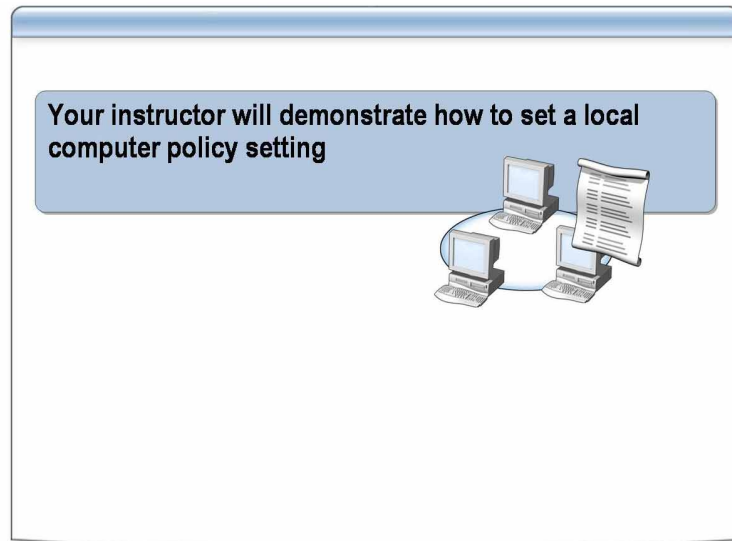
Computer configuration

Group Policy settings for computers include how the operating system behaves, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned application options, and application settings. Computer-related Group Policy settings are applied when the operating system initializes and during the periodic refresh cycle. In general, computer-related Group Policy settings takes precedence over conflicting user-related Group Policy settings.

Group Policy settings that customize the desktop environment for all users of a computer, or enforce security policies on a network's computers, are contained under Computer Configuration in Group Policy Object Editor.

Software Settings for computer configuration	The Software Settings folder under Computer Configuration contains software settings that apply to all users who log on to the computer. This folder contains software installation settings, and it may contain other settings that are placed there by ISVs.
Windows settings for computer configuration	The Windows Settings folder under Computer Configuration contains Windows settings that apply to all users who log on to the computer. This folder also contains the following items: Security Settings and Scripts.
Security settings for user and computer configuration	Security settings are available under the Windows Settings folder under Computer Configuration and User Configuration in Group Policy Object Editor. Security settings or security policies are rules that you configure on a computer or multiple computers that protect resources on a computer or network. With security settings, you can specify the security policy of an organizational unit, domain, or site.
Additional reading	For more information about extending Group Policy, see “Advanced methods of extending Group Policy” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SPconcepts_30.asp .

How to Set Local Computer Policy Settings



Introduction

To edit a local GPO, you must be logged on as a member of the Domain Admins group, the Enterprise Admins group, or the Group Policy Creator Owners group.

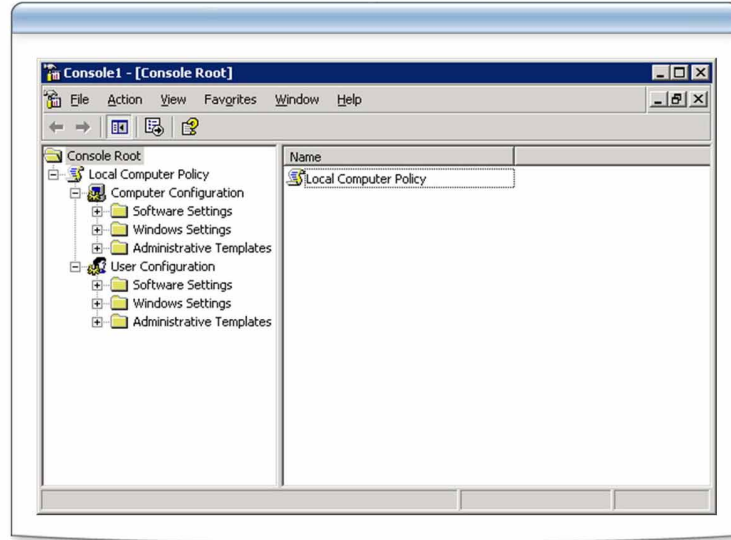
Note You can access Group Policy Object Editor from Administrative Tools or through a Microsoft Management Console (MMC) snap-in.

Procedure

To set local computer policy settings:

1. Open Group Policy Object Editor.
2. In the console tree, double-click the folders to view the policy settings in the details pane.
3. In the details pane, double-click a policy setting to open the **Properties** dialog box, and then change the policy setting.

Practice: Setting Local Computer Policy Settings



Objective	In this exercise, you will set a local computer policy setting by using Group Policy Object Editor.
Instruction	<p>Before you begin this practice:</p> <ul style="list-style-type: none">■ Log on to the domain by using the <i>ComputerNameUser</i> account.■ Open CustomMMC with the Run as command. Use the user account <i>Nwtraders\ComputerNameAdmin</i> (Example: <i>LondonAdmin</i>).■ Review the procedures in this lesson that describe how to perform this task.
Scenario	The systems administrators team has asked you to test some local policy settings before they deploy the policy settings to production servers. You will set some local computer policy settings on your server and test the policy settings to make sure they work.
Practice	<p>► Add Group Policy Object Editor to CustomMMC</p> <ol style="list-style-type: none">1. Open CustomMMC.2. Add the snap-in Group Policy Object Editor.3. Save CustomMMC.

► **Prevent users from shutting down the server by using a local policy setting**

1. In CustomMMC, expand the snap-in, **Local Computer Policy**.
2. In the console tree, expand **User Configuration**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
3. In the details pane, double-click **Remove and prevent access to the Shut Down command**.
4. In the **Remove and prevent access to the Shut Down command Properties** dialog box, click **Enabled**, and then click **OK**.
5. Close and save all programs and log off.

► **Test the policy setting that prevents users from shutting down the server**

1. Log on as *ComputerNameUser* with a password of **P@ssw0rd** in the NWTraders domain.
2. Click **Start** and verify that the **Shut Down** button has been removed from the **Start** menu.
3. Close and save all programs and log off.

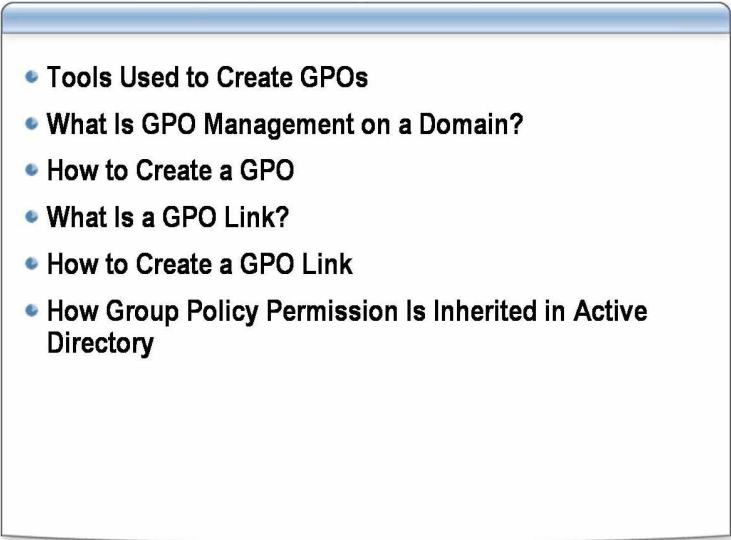
► **Enable the Shut Down button on the server by using a local policy setting**

1. Log on as *ComputerNameUser* with a password of **P@ssw0rd** in the NWTraders domain.
2. Open CustomMMC with the **Run as** command with the *Nwtraders\ComputerNameAdmin* user account.
3. In CustomMMC, expand the snap-in, **Local Computer Policy**.
4. In the console tree, expand **User Configuration**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
5. In the details pane, double-click **Remove and prevent access to the Shut Down command**.
6. In the **Remove and prevent access to the Shut Down command Properties** dialog box, click **Not configured**, and then click **OK**.
7. Close and save all programs and log off.

► **Test the local policy that enables the shut down option on the server**

1. Log on as *ComputerNameUser* with a password of **P@ssw0rd** in the NWTraders domain.
2. Click **Start** and verify that the **Shut Down** button on the **Start** menu had been enabled.
3. Close all programs and log off.

Lesson: Implementing GPOs on a Domain

- 
- Tools Used to Create GPOs
 - What Is GPO Management on a Domain?
 - How to Create a GPO
 - What Is a GPO Link?
 - How to Create a GPO Link
 - How Group Policy Permission Is Inherited in Active Directory

Introduction

Implementing Group Policy on a domain provides the network administrator with greater control over computer configurations throughout the network structure. Also, by using Group Policy in Windows Server 2003, you can create a managed desktop environment that is tailored to the user's job responsibilities and experience level, which can decrease the amount of network support needed.

Lesson objectives

After completing this lesson, you will be able to:

- Understand the tools used to create GPOs.
- Explain what GPO management on a domain is.
- Create a GPO.
- Explain what a GPO link is.
- Explain how to configure attributes of GPO links.
- Explain how Group Policy permission is inherited in Active Directory.

Tools Used to Create GPOs



Introduction

You can open Group Policy Object Editor from other tools to edit GPOs.

Active Directory Users and Computers

You can open Group Policy Object Editor from Active Directory Users and Computers to manage GPOs for domains and organizational units. In the **Properties** dialog box for a domain or an organizational unit, there is a **Group Policy** tab. On this tab, you can manage GPOs for the domain or organizational units.

Active Directory Sites and Services

You can open Group Policy Object Editor from Active Directory Sites and Services to manage GPOs for sites. In the **Properties** dialog box for a site, there is a **Group Policy** tab. On this tab, you can manage GPOs for the site.

Note If the Group Policy Management console is installed, the ADUC and ADSS are replaced by a button to launch the Group Policy Management console.

Group Policy Management console

The Group Policy Management console is a set of programmable interfaces for managing Group Policy, as well as an MMC snap-in that is built on those programmable interfaces. Together, the components of Group Policy Management consolidate the management of Group Policy across the enterprise.

The Group Policy Management console combines the functionality of multiple components in a single user interface (UI). The UI is structured to match the way you use and manage Group Policy. It incorporates functionality related to Group Policy from the following tools into a single MMC snap-in:

- Active Directory Users and Computers
- Active Directory Sites and Services
- Resultant Set of Policy (RSOP)

Group Policy Management also provides the following extended capabilities that were not available in previous Group Policy tools. With Group Policy Management, you can:

- Back up and restore GPOs.
- Copy and import GPOs.
- Use Windows Management Instrumentation (WMI) filters.
- Report GPO and RSoP data.
- Search for GPOs.

Group Policy Management vs. default Group Policy tools

Prior to Group Policy Management, you managed Group Policy by using a variety of Windows-based tools, including Active Directory Users and Computers, Active Directory Sites and Services, and RSoP. Group Policy Management consolidates management of all core Group Policy tasks into a single tool. Because of this consolidated management, Group Policy functionality is no longer required in these other tools.

After installing Group Policy Management, you still use each of the Active Directory tools for their intended directory management purposes, such as creating user, computer, and group objects. However, you can use Group Policy Management to perform all tasks related to Group Policy. Group Policy functionality is no longer available through the Active Directory tools when Group Policy Management is installed.

Group Policy Management does not replace Group Policy Object Editor. You still must edit GPOs by using Group Policy Object Editor. Group Policy Management integrates editing functionality by providing direct access to Group Policy Object Editor.

Note The Group Policy Management console does not come with Windows Server 2003. You must download it from <http://www.microsoft.com>.

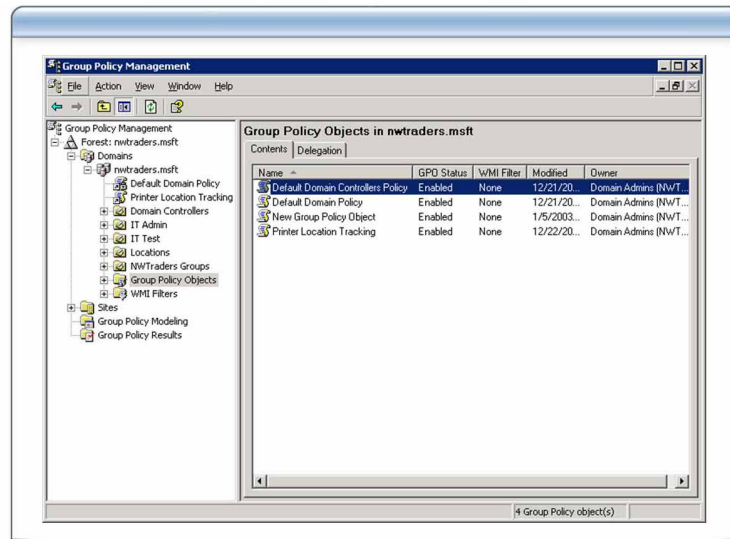
Administrative Templates

There are several template files with an .adm extension that are included with Windows. These files, called Administrative Templates, provide policy information for the items that are under the Administrative Templates folder in the console tree of Group Policy Object Editor. Administrative Templates include Registry-based settings, which are available under Computer Configuration and User Configuration in Group Policy Object Editor.

An .adm file consists of a hierarchy of categories and subcategories that define how the policy settings appear. It also contains the following information:

- Registry locations that correspond to each setting
- Options or restrictions in values that are associated with each setting
- For many settings, a default value
- Explanation of what each setting does
- The versions of Windows that support each setting

What Is GPO Management on a Domain?



Introduction

After you create a GPO, you then configure the settings for that specific GPO. By grouping collections of settings into separate GPOs, you can specify different configurations for each GPO so that each GPO affects only the computers and users that you specify. When you place GPOs on a domain, you can manage the configuration settings on a domain-wide basis.

Group Policy container

The Group Policy container is an Active Directory object that contains GPO attributes. It includes subcontainers for Group Policy information about computers and users. The Group Policy container includes the following information:

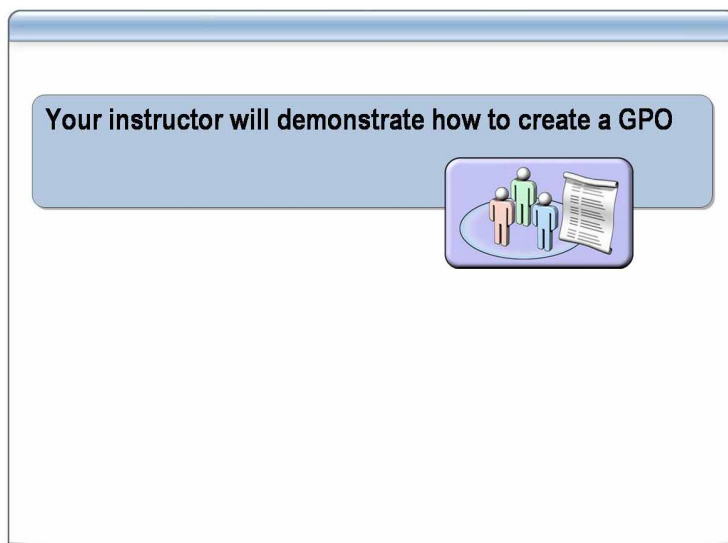
- *Version information.* Ensures that the information in the Group Policy container is synchronized across all domain controllers.
- *Status information.* Indicates whether the GPO is enabled or disabled.
- *List of extensions.* Lists any of the Group Policy extensions that are used in the GPO.

Additional reading

For more information about Group Policy Management, see:

- “Introducing the Group Policy Management Console” at <http://www.microsoft.com/windowsserver2003/gpmc/gpmcintro.mspx>.
- “Enterprise Management with the Group Policy Management Console” at <http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>.

How to Create a GPO



Introduction

Use the following procedures to create a new GPO or link an existing GPO by using Active Directory Users and Computers and to create a GPO in a site, domain, or organizational unit.

Procedure using Active Directory Users and Computers

To create a new GPO or link an existing GPO by using Active Directory Users and Computers:

1. In Active Directory Users and Computers, right-click the Active Directory container (domain or organizational unit) for which you want to create a GPO, and then click **Properties**.
2. In the **Properties** dialog box, on the **Group Policy** tab, choose one of the following options:
 - To create a new GPO, click **New**, type a name for the new GPO, and then press ENTER.
 - To link an existing GPO, click **Add**, and then select the GPO from the list.

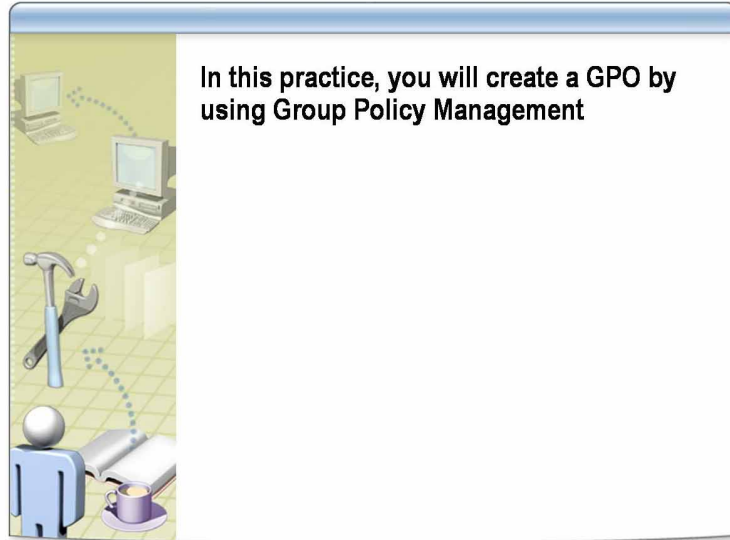
The GPO that you create or link is displayed in the list of GPOs that are linked to the Active Directory container.

Procedure using Group Policy Management

To create a GPO for a site, a domain, or an organizational unit:

1. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to create a new GPO, expand **Domains**, and then expand the domain.
3. Right-click **Group Policy Objects**, and then click **New**.
4. In the **New GPO** dialog box, type a name for the new Group Policy object, and then click **OK**.

Practice: Creating a GPO



Objective

In this practice, you will create a GPO by using Group Policy Management.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that Custom MMC contains Group Policy Management.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

The systems engineers at Northwind Traders are going to test Group Policy settings in a test environment. These Group Policy settings will be used later for scalability testing. The systems engineers need your team of systems administrators to create a GPO called *ComputerNameGP* in the Group Policy Objects container.

Practice

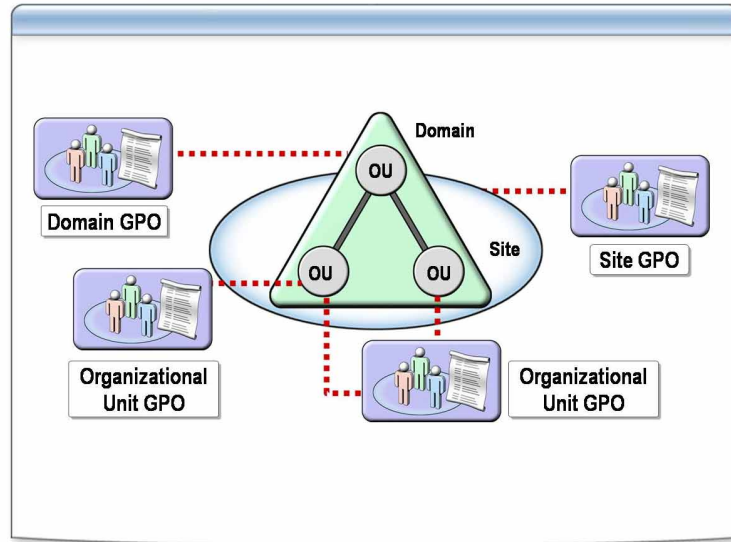
► Create a GPO by using Group Policy Management

1. In Group Policy Management, expand **nwtraders.msft**.
2. Create a GPO called *ComputerNameGP* in the Group Policy Objects container.

Additional reading

For more information about migrating GPOs, see “Migrating GPOs Across Domains with GPMC” at <http://www.microsoft.com/windowsserver2003/gpmc/migrppo.mspx>.

What Is a GPO Link?



Introduction

All GPOs are stored in a container in Active Directory called Group Policy Objects. When a GPO is used by a site, domain, or organizational unit, the GPO is linked to the Group Policy Objects container. As a result, you can centrally administer and deploy the GPOs to many domains or organizational units.

Creating a linked GPO

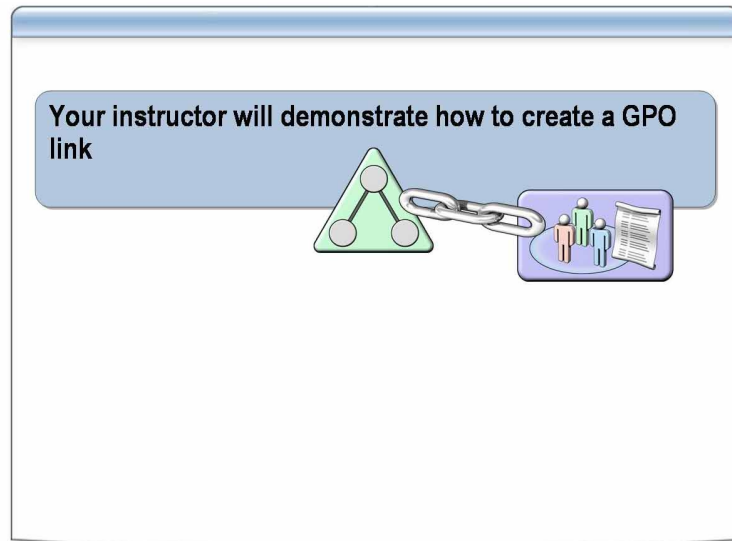
When you create a GPO linked to a site, domain, or organizational unit, you actually perform two separate operations: creating the new GPO, and then linking it to the site, domain, or organizational unit. When delegating permissions to link a GPO to a domain, organizational unit, or site, you must have Modify permission for the domain, organizational unit, or site that you want to delegate.

By default, only members of the Domain Admins and Enterprise Admins groups have the necessary permissions to link GPOs to domains and organizational units. Only members of the Enterprise Admins group have the permissions to link GPOs to sites. Members of the Group Policy Creator Owners group can create GPOs but cannot link them.

Creating an unlinked GPO

When you create a GPO in the Group Policy Objects container, the GPO is not deployed to any users or computers until a GPO link is created. You can create an unlinked GPO by using Group Policy Management. You might create unlinked GPOs in a large organization where one group creates GPOs, and another group links the GPOs to the required site, domain, or organizational unit.

How to Create a GPO Link



Introduction

Use the following procedures to create and link GPOs, link existing GPOs, unlink a GPO, delete a GPO link, delete a GPO, and disable a GPO.

Procedure for creating and linking a GPO

To link a GPO when you create it:

1. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to create and link a GPO, expand **Domains**, and then do one of the following:
 - To create a GPO and link it to a domain, right-click the domain, and then click **Create and Link a GPO Here**.
 - To create a GPO and link it to an organizational unit, expand the domain containing the organizational unit, right-click the organizational unit, and then click **Create and Link a GPO Here**.
2. In the **New GPO** dialog box, type a name for the new GPO, and then click **OK**.

Procedure for linking an existing GPO

To link an existing GPO to a site, domain, or organizational unit:

1. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to link an existing GPO, expand **Domains**, and then expand the domain.
2. Right-click the domain, site, or organizational unit, and then click **Link an Existing GPO**.
3. In the **Select GPO** dialog box, click the GPO that you want to link, and then click **OK**.

Important You cannot link a GPO to containers in Active Directory like the Users and Computers containers. However, any GPO linked to the domain applies to users and computers in these containers.

Procedure for unlinking a GPO

To unlink a GPO from a site, domain, or organizational unit:

1. In Group Policy Management, in the console tree, expand the forest containing the domain from which you want to unlink an existing GPO, expand **Domains**, and then expand the domain.
2. Right-click a linked GPO, and then clear the **Link Enabled** option.

Note Unlinking a GPO and deleting a GPO have the same effect. However, if you want to temporarily remove the GPO, you unlink it, which disables it. If you want to completely remove the GPO, then delete the link.

Procedure for deleting a GPO link

To delete a GPO link to a site, domain, or organizational unit:

1. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to delete an existing GPO link, expand **Domains**, and then expand the domain.
2. Right-click a linked GPO, and then click **Delete**.
This deletes only the GPO link and not the GPO.
3. In the message box, click **OK**.

Procedure for deleting a GPO

To delete a GPO:

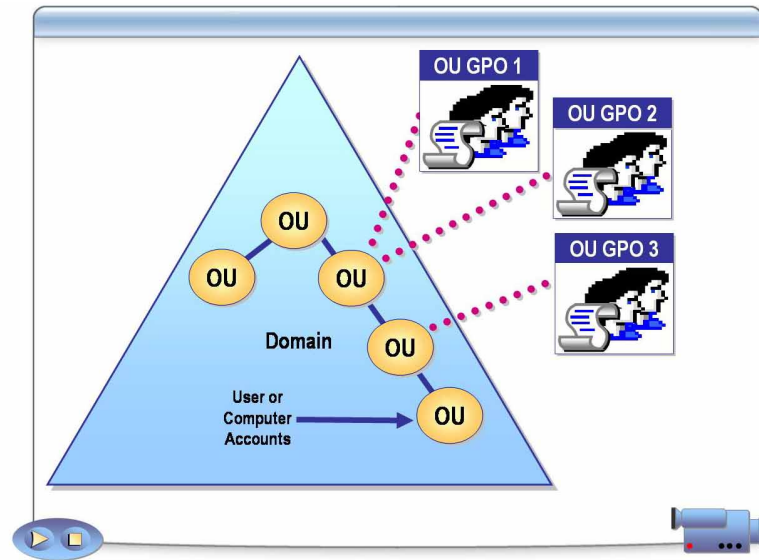
1. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to delete a GPO, expand **Domains**, expand the domain, and then expand **Group Policy Objects**.
2. Right-click the GPO that you want to delete, and then click **Delete**.
This does not delete the link to the GPO from other domains.
3. In the message box, click **OK**.

Procedure for disabling a GPO

To disable a GPO:

1. In Group Policy Management, in the console tree, expand the forest containing the domain in which you want to disable a GPO, expand **Domains**, expand the domain, and then expand **Group Policy Objects**.
2. Click the GPO that you want to disable.
3. In the details pane, on the **Details** tab, in the **GPO status** box, click one of the following:
 - **All settings disabled**
 - **Computer configuration settings disabled**
 - **Users configuration settings disabled**

How Group Policy Permission Is Inherited in Active Directory



Introduction

The order in which Windows Server 2003 applies GPOs depends on the Active Directory container to which the GPOs are linked. The GPOs are applied first to the site, then to domains, and then to organizational units in the domains.

Flow of inheritance

A child container inherits GPOs from the parent container. This means that the child container can have many Group Policy settings applied to its users and computers without having a GPO linked to it. However, there is no hierarchy of domains like there is for organizational units, such as parent organizational units and child organizational units.

Order of inheritance

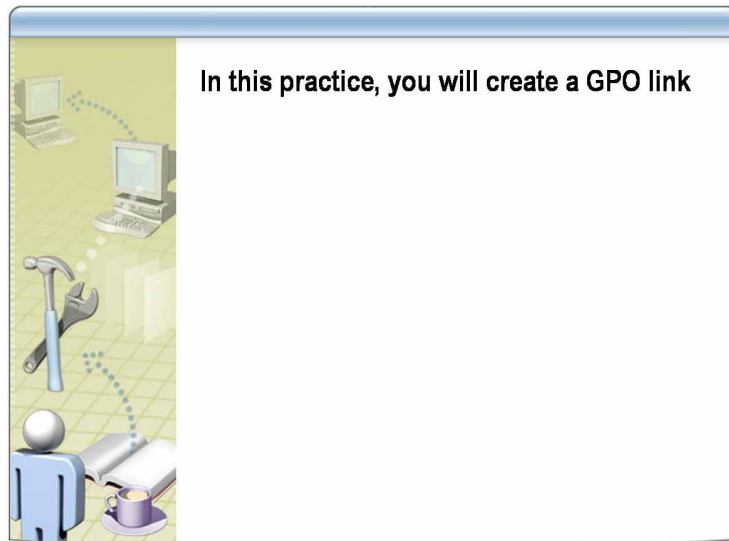
GPOs are cumulative, meaning that they are inherited. Group Policy inheritance is the order in which Windows Server 2003 applies GPOs. The order in which GPOs are applied and how GPOs are inherited ultimately determines which settings affect users and computers. If there are multiple GPOs that are set at the same value, by default the GPO applied last takes precedence.

You can also have multiple GPOs linked to the same containers. For example, you can have three GPOs linked to a single domain. Because the order in which the GPOs are applied may affect the resultant Group Policy settings, there is also an order, or priority of Group Policy settings, of GPOs for each container.

Multimedia activity

The *Implementing Group Policy* activity includes multiple choice and drag-and-drop exercises that test your knowledge. To start the activity, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click **Implementing Group Policy**. Read the instructions, and then click the **Effects of Group Policy Settings** tab to begin the activity.

Practice: Creating a GPO Link



Objective

In this practice, you will create a GPO link.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains Group Policy Management and Active Directory Users and Computers.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

The systems engineers at Northwind Traders are going test Group Policy settings in a test environment. These Group Policy settings will be used later for scalability testing. The systems engineers need your team of systems administrators to create GPOs for these tests.

Practice

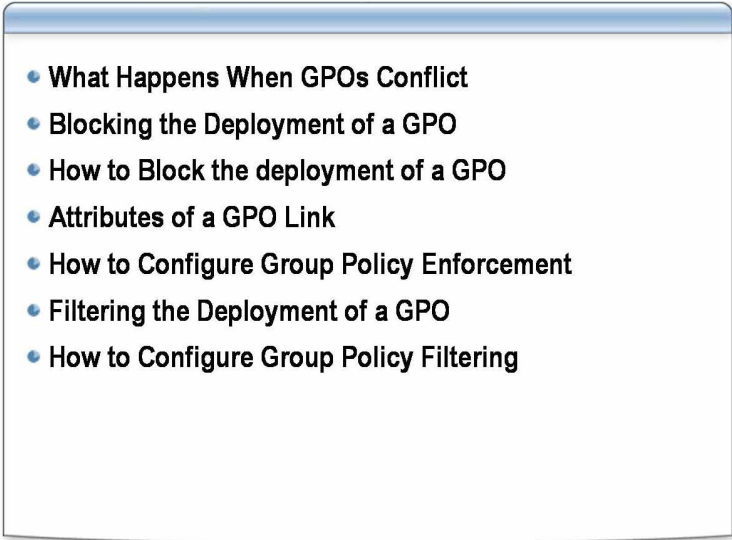
► **Create an organizational unit in the IT Test organizational unit**

1. In Active Directory Users and Computers, expand **nwtraders.msft**, and then expand the **IT Test** organizational unit.
2. Create an organizational unit called *ComputerName*.

► **Create a GPO link to the IT Test/*ComputerName* organizational unit**

- In Group Policy Management, create a GPO called *ComputerName GP* and link it to the IT Test/*ComputerName* organizational unit.

Lesson: Managing the Deployment of Group Policy

- 
- What Happens When GPOs Conflict
 - Blocking the Deployment of a GPO
 - How to Block the deployment of a GPO
 - Attributes of a GPO Link
 - How to Configure Group Policy Enforcement
 - Filtering the Deployment of a GPO
 - How to Configure Group Policy Filtering

Introduction

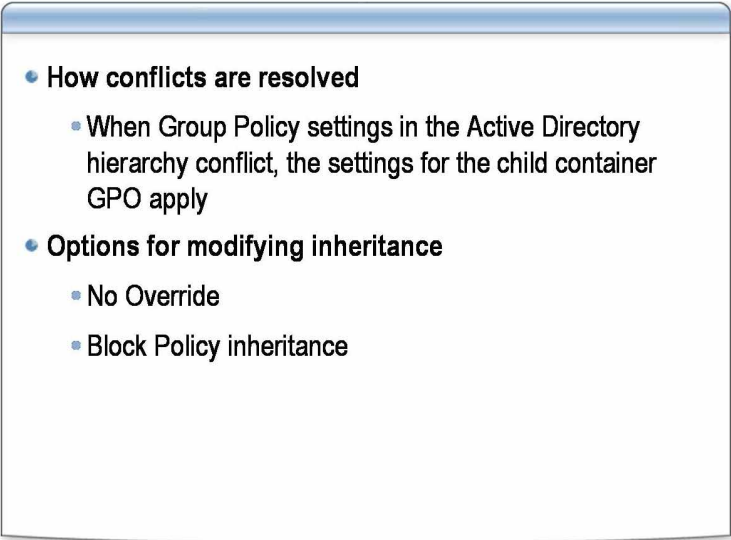
After completing this lesson, students will be able to manage the deployment of Group Policy.

Lesson objectives

After completing this lesson, you will be able to:

- Explain what happens when GPOs conflict.
- Explain what it means to block the deployment of a GPO.
- Block the deployment of a GPO.
- Describe attributes of a GPO link.
- Configure Group Policy enforcement.
- Explain what it means to filter the deployment of a GPO.
- Configure Group Policy filtering.

What Happens When GPOs Conflict

- 
- **How conflicts are resolved**
 - When Group Policy settings in the Active Directory hierarchy conflict, the settings for the child container GPO apply
 - **Options for modifying inheritance**
 - No Override
 - Block Policy inheritance

Introduction

Complex combinations of GPOs may create conflicts, which may require you to modify default inheritance behavior. When a Group Policy setting is configured for a parent organizational unit, and the same Group Policy setting is not configured for a child organizational unit, the objects in the child organizational unit inherit the Group Policy setting from the parent organizational unit.

How conflicts are resolved

When Group Policy settings are configured for both the parent organizational unit and the child organizational units, the settings for both organizational units apply. If the settings are incompatible, the child organizational unit retains its own Group Policy setting. For example, a Group Policy setting for the organizational unit that was last applied to the computer or user overwrites a conflicting Group Policy setting for a container that is higher up in the Active Directory hierarchy.

Options for modifying inheritance

If the default inheritance order does not meet your organization's needs, you can modify the inheritance rules for specific GPOs. Windows Server 2003 provides the following two options for changing the default inheritance order:

■ No Override

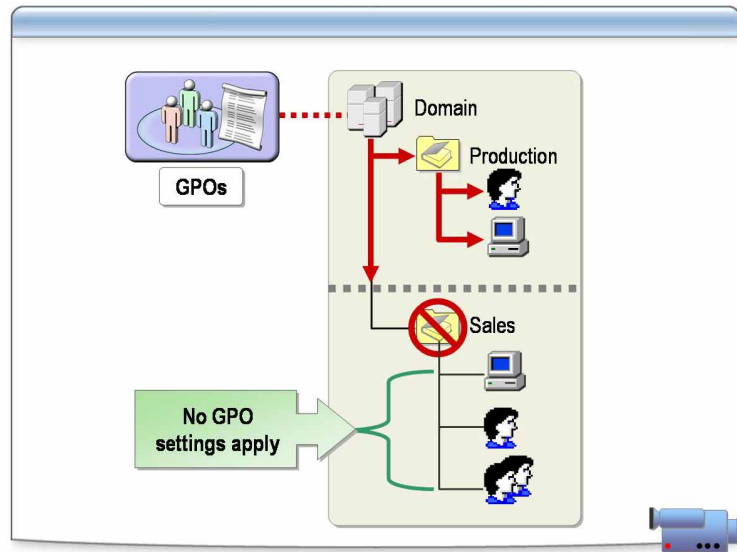
Use this option to prevent child containers from overriding a GPO with a higher priority setting. This option is useful for enforcing GPOs that represent organization-wide business rules. The **No Override** option is set on an individual GPO basis.

You can set this option on one or more GPOs as required. When more than one GPO is set to **No Override**, the GPO set to **No Override** that is highest in the Active Directory hierarchy takes precedence.

■ Block Policy inheritance

Use this option to force a child container to block inheritance from all parent containers. This option is useful when an organizational unit requires unique Group Policy settings. **Block Policy inheritance** is set on a per-container basis. In the case of a conflict, the **No Override** option always takes precedence over the **Block Policy inheritance** option.

Blocking the Deployment of a GPO



Introduction

You can prevent a child container from inheriting any GPOs from parent containers by enabling **Block Policy inheritance** on the child container.

Why use Block Policy inheritance?

Enabling **Block Policy inheritance** on a child container prevents the container from inheriting all Group Policy settings, not just selected Group Policy settings. This is useful when an Active Directory container requires unique Group Policy settings, and you want to ensure that Group Policy settings are not inherited. For example, you can use **Block Policy inheritance** when the administrator of an organizational unit must control all GPOs for that container.

Considerations

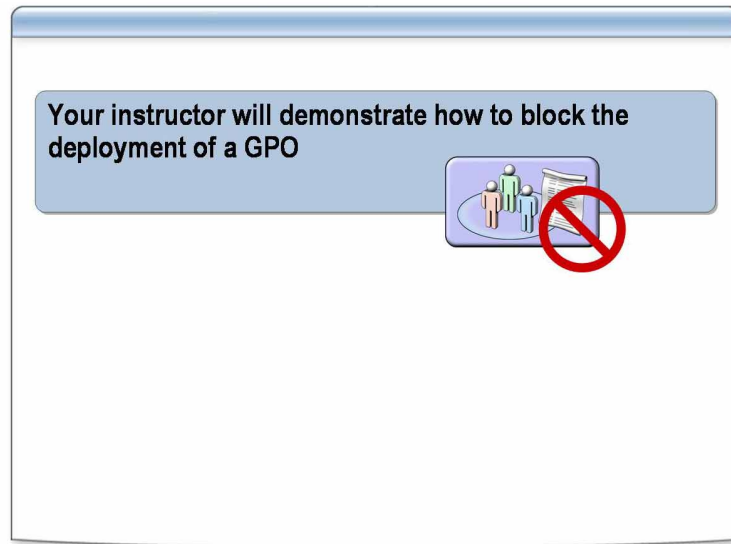
Consider the following when using **Block Policy inheritance**:

- You cannot selectively choose which GPOs are blocked. **Block Policy inheritance** affects all GPOs from all parent containers, except GPOs configured with the **No Override** option with out GPMC installed and **Enforced** with GPMC installed.
- **Block Policy inheritance** does not block the inheritance of a GPO linked to a parent container if the link is configured with the **No Override** option.

Multimedia activity

The *Implementing Group Policy* activity includes multiple choice and drag-and-drop exercises that test your knowledge. To start the activity, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click **Implementing Group Policy**. Read the instructions, and then click the **Managing the Deployment of Group Policy** tab to begin the activity.

How to Block the Deployment of a GPO



Introduction

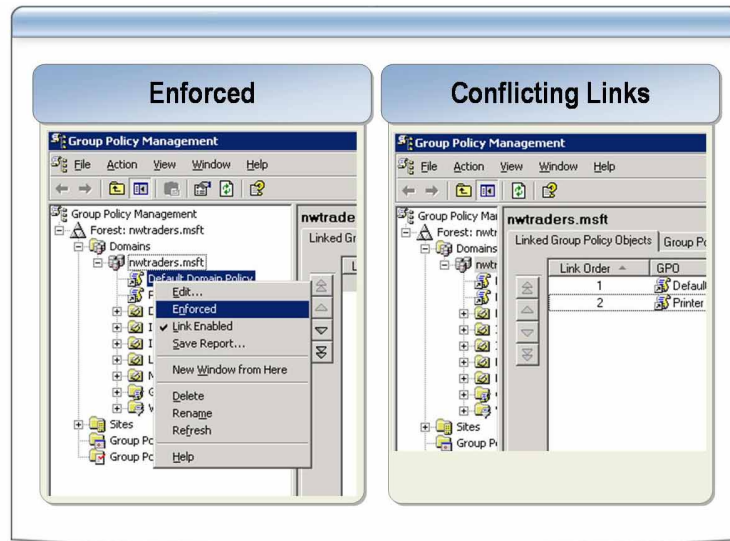
Use the following procedure to enable **Block Policy inheritance**.

Procedure

To enable **Block Policy inheritance**:

1. In Group Policy Management, in the console tree, expand the forest in which you want to block inheritance, and then do one of the following:
 - To block inheritance of the GPO links for an entire domain, expand **Domains**, and then right-click the domain.
 - To block inheritance of the GPO links for an organizational unit, expand **Domains**, expand the domain containing the organizational unit, and then right-click the organizational unit.
2. Click **Block Inheritance**.

Attributes of a GPO Link



Introduction

You can enable, disable, enforce, and group GPO links. These options significantly affect the user and computer accounts in the organizational unit that the GPO is linked to.

The Enforced option

The **Enforced** option is an attribute of the GPO link, *not* the GPO itself. If you have a GPO that is linked to multiple containers, you configure the **Enforced** option on each individual container. Furthermore, if the same GPO is linked elsewhere, the **Enforced** option does not apply to that link unless you also modify that link.

All Group Policy settings contained in the GPO whose link is configured with **Enforced** apply, even if they conflict with Group Policy settings processed after them or if inheritance is blocked lower in the Active Directory tree. You should enable the **Enforced** option only for the links to the GPO that represents critical organization-wide rules. Link the GPO high in the Active Directory tree so that it affects multiple organizational units. For example, you will want to link a GPO with network security settings to a domain or site.

Important The **Enforced** option is called **No Override** in Active Directory Users and Computers before Group Policy Management is installed.

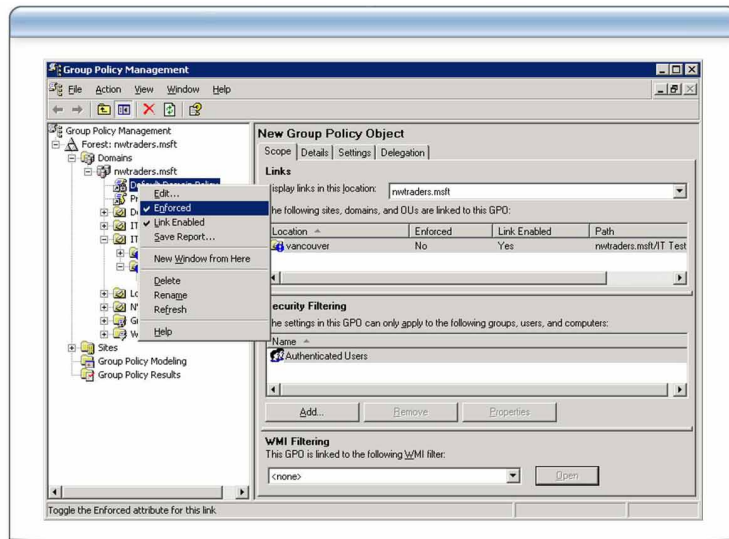
Enabling and disabling a link

Link Enabled is another attribute that you may use when you are troubleshooting a GPO. You can disable the GPO link by clearing the **Link Enabled** option, instead of deleting the GPO link. By disabling the link, you only change the effect on the user and computer accounts in the organizational unit and all child organizational units. You do not affect other links to the GPO may have.

Conflicting links

When multiple GPOs are linked to an organizational unit, the GPO with the highest link order is applied last. If Group Policy settings in the GPO conflict, the last one applied takes precedence.

How to Configure Group Policy Enforcement



Introduction

Use the following procedure to configure the enforcement of a GPO link.

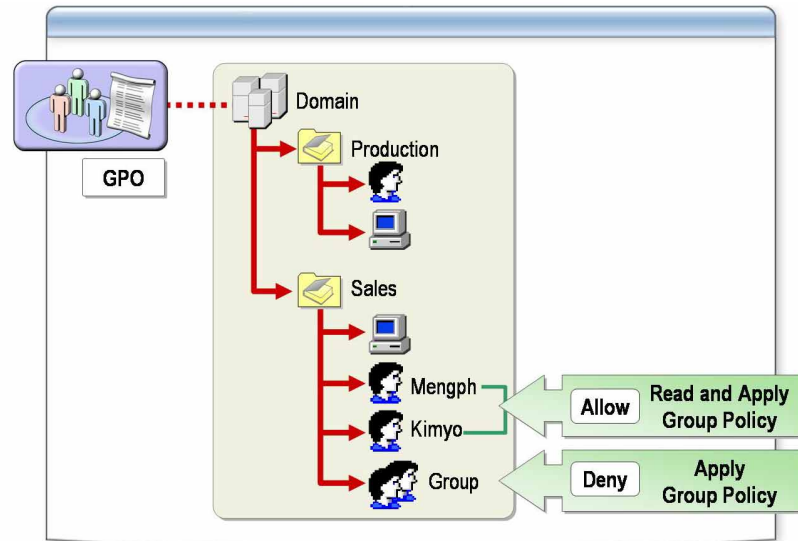
Procedure

To configure the enforcement of a GPO link:

1. In Group Policy Management, in the console tree, expand the forest with the link for which you want to configure enforcement, and then do one of the following:
 - To configure enforcement for a GPO link to a domain, expand **Domains**, and then expand the domain containing the GPO link.
 - To configure enforcement for a GPO link to an organizational unit, expand **Domains**, expand the domain containing the organizational unit, and then expand the organizational unit, which may include any parent or child organizational unit containing the GPO link.
 - To configure enforcement for a GPO link to a site, expand **Sites**, and then expand the site containing the GPO link.
2. Right-click the GPO link, and then click **Enforced** to enable or disable enforcement.

Note Include only critical Group Policy settings in linked GPOs that are set to **Enforced**, because they take effect regardless of how other GPOs are configured. You want to be sure that you are not overriding important GPOs.

Filtering the Deployment of a GPO



Introduction

By default, all Group Policy settings contained in the GPOs that affect the container are applied to all users and computers in that container, which may not produce the results that you desire. By using the filtering feature, you can determine which settings are applied to the users and computers in the specific container.

Permissions for GPOs

You can filter the deployment of a GPO by setting permissions on the GPO Link to determine the access of the read or deny permission on the GPO. For Group Policy settings to apply to a user or computer account, the account must have at least Read permission for a GPO. The default permissions for a new GPO have the following access control entries (ACEs):

- Authenticated Users—Allow Read and Allow Apply Group Policy
- Domain Admins, Enterprise Admins and SYSTEM—Allow Read, Allow Write, Allow Create All Child objects, Allow Delete All Child objects

Filtering methods

You can use the following filtering methods:

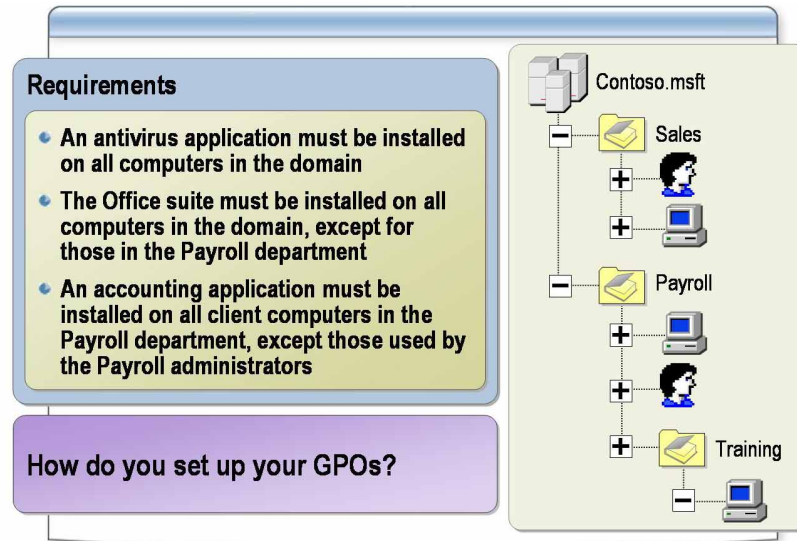
- Explicitly deny

This method is used when denying access to the Group Policy. For example, you could explicitly deny permission to the administrators security group, which would prevent administrators in the organizational unit from receiving the GPO settings.

- Remove Authenticated Users

You can omit the organizational unit administrators from the security group, which means that they have no explicit permissions for the GPO.

Class Discussion: Modifying Group Policy Inheritance



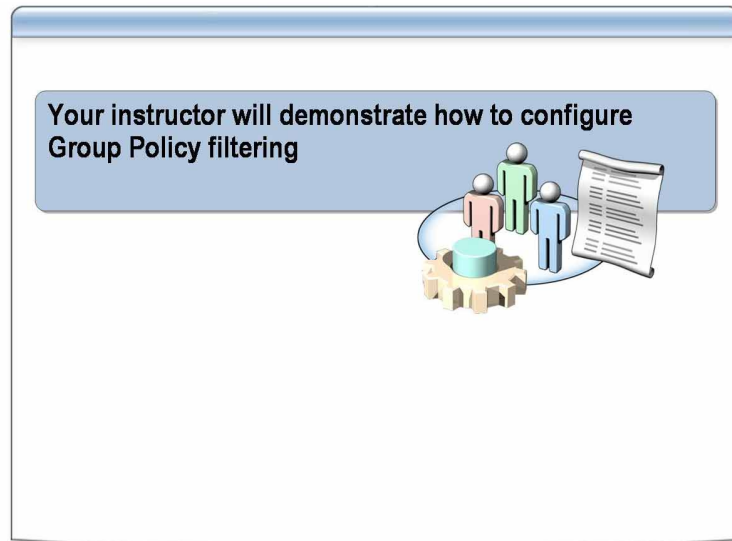
Class discussion

You have determined that the following conditions must exist in your network:

- An antivirus application must be installed on all computers in the domain.
- The Microsoft Office suite must be installed on computers in the domain, except those in the Payroll department.
- A line-of-business accounting application must be installed on all computers in the Payroll department, except those that are used by administrators of the Payroll organizational unit.

How do you set up GPOs so that the above conditions are met?

How to Configure Group Policy Filtering



Introduction

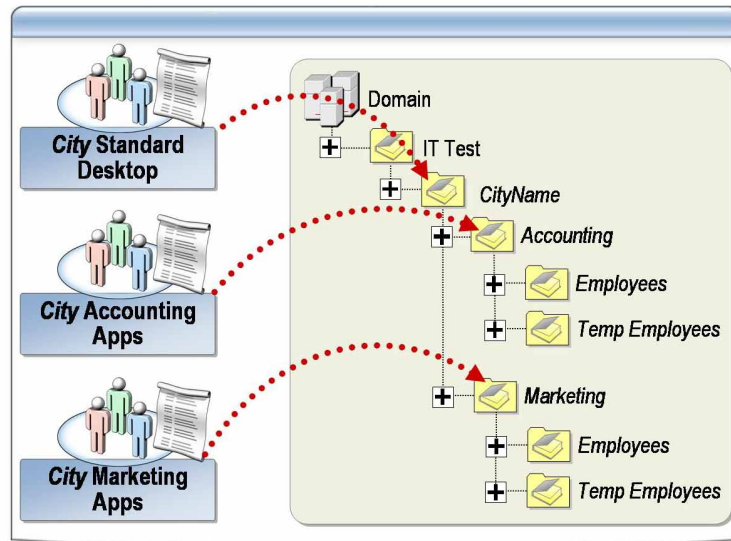
Use the following procedure to configure Group Policy filtering.

Procedure

To filter the scope of a GPO by using security groups:

1. In Group Policy Management, in the console tree, expand the forest and domain with the GPO, expand **Group Policy objects**, and then click the GPO.
2. In the details pane, on the **Scope** tab, click **Add**.
3. In the **Select User, Computer, or Group** dialog box, in the **Enter the object name to select** box, enter the name of the security principal, and then click **OK**.

Practice: Managing the Deployment of Group Policy



Objective

In this practice, you will manage the deployment of Group Policy.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains the following snap-ins:
 - Active Directory Users and Computers
 - Group Policy Management
- Review the procedures in this lesson that describe how to perform this task.

Scenario

Northwind Traders is testing the effect of multiple Group Policy settings on users and computers. Northwind Traders wants to implement an organizational unit that gives all users a standard desktop, except managers whose accounts are in the Employees organizational unit.

Management has asked the systems administrators team to create an organizational unit hierarchy in the IT Test organizational unit. The organizational unit hierarchy must contain an Accounting organizational unit and a Marketing organizational unit like in the diagram on the slide.

Management has also asked you to create a GPO to be used to install an Accounting and a separate Marketing application. The Accounting and Marketing applications are to be eventually installed to all Accounting and Marketing personnel; however, management wants to wait to deploy the application for the temporary employees. Management wants to maintain flexibility so when the temporary employees are ready for the applications, it can easily be enabled for them.

Practice**► Create three GPOs for testing purposes**

- In Group Policy Management, create three GPOs in the Group Policy Objects container with the following names:
 - *ComputerName* Standard Desktop
 - *ComputerName* Accounting Apps
 - *ComputerName* Marketing Apps

► Create an organizational unit structure that matches the slide

- In Active Directory Users and Computers, create the organizational unit structure that appears on the slide.

► Create an enforced GPO link

1. Link the *ComputerName* Standard Desktop GPO to the IT Test/*ComputerName* organizational unit.
2. In the IT Test/*ComputerName* organizational unit, right-click the *ComputerName* **Standard Desktop** link, and click **Enforced**.

► Configure a GPO security filter

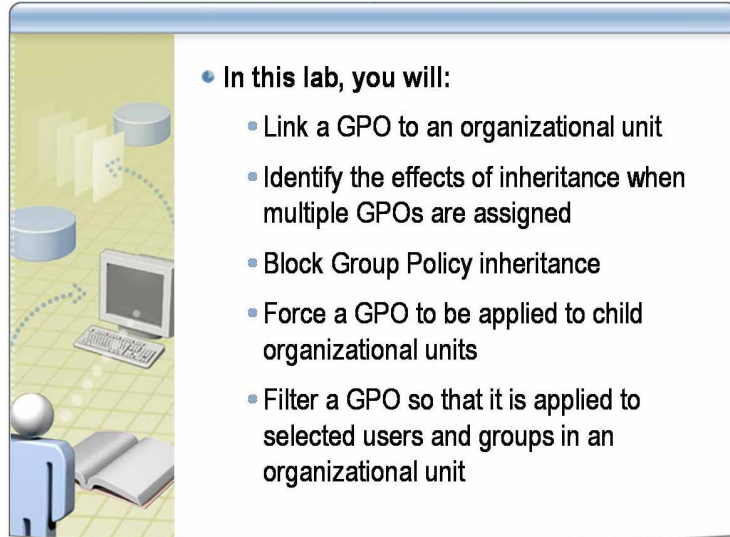
1. In Group Policy Management, in the **Group Policy Objects** container, double-click the *ComputerName* **Standard Desktop** GPO link.
2. In the details pane, on the **Scope** tab, add the following groups:
 - G NWTraders Accounting Managers
 - G NWTraders Accounting Personnel
 - G NWTraders Marketing Managers
 - G NWTraders Marketing Personnel
3. Remove Authenticated Users.
4. On the **Delegation** tab, click **Advanced**.
5. In the **Security Settings** dialog box, configure the following advanced security settings:
 - For the G NWTraders Accounting Managers group, set the Apply Group Policy permissions to Deny.
 - For the G NWTraders Marketing Managers group, set the Apply Group Policy permissions to Deny.

► Configure GPOs to block inheritance

1. Link the *ComputerName* Accounting Apps GPO to the IT Test/*ComputerName*/Accounting organizational unit.
2. Click the **Temp Employees** organizational unit in the IT Test/*ComputerName*/Accounting organizational unit.
3. List the GPOs that the IT Test/*ComputerName*/Accounting organizational unit inherits.

4. Right-click the **Temp Employees** organizational unit in the IT Test/*ComputerName*/Accounting organizational unit, and then click **Block Inheritance**.
5. List the GPOs that the IT Test/*ComputerName*/Accounting organizational unit inherits.

Lab A: Implementing Group Policy



Objectives

After completing this lab, you will be able to:

- Link a GPO to an organizational unit.
- Identify the effects of inheritance when multiple GPOs are assigned.
- Block Group Policy inheritance.
- Force a GPO to be applied to child organizational units.
- Filter a GPO so that it is applied to selected users and groups in an organizational unit.

Instructions

Before you begin this lab:

- Log on to the domain by using the *ComputerNameUser* account.
- Open CustomMMC with the **Run as** command.
Use the user account *Nwtraders\ComputerNameAdmin* (Example: *LondonAdmin*).
- Ensure that CustomMMC contains the following snap-ins:
 - Active Directory Users and Computers
 - Group Policy Management

Estimated time to
complete this lab:
25 minutes

Scenario

Northwind Traders is preparing to implement GPOs to the users and computers throughout all cities on their network. The systems engineers want the systems administrators team to create all the necessary GPOs and then link the GPOs to the appropriate organizational units. After the GPOs are created and deployed to the workstations, you must then configure the GPOs to perform the intended functions.

The systems administrators have provided you with a list of GPOs, along with their properties, that need to be created and configured. You should reuse GPOs that have already been created if you can. You also must make sure that no computer-related Group Policy settings affect laptops in your city, so you must block any GPOs from affecting the Laptops organizational unit.

GPO name	Location	Filtering	Enforcement
<i>ComputerName</i> Standard Desktop	Location/ <i>ComputerName</i>	Default	Enforced
<i>ComputerName</i> Folder Redirection	Location/ <i>ComputerName</i> /Users	DL Temp Employees = Deny	
<i>ComputerName</i> Scripts	Location/ <i>ComputerName</i> /Users	Default	
<i>ComputerName</i> Proxy Settings	Location/ <i>ComputerName</i> /Computers/Desktops	Default	Enforced

Exercise 1

Creating and Linking GPOs

In this exercise, you will create and link GPOs to your *ComputerName* organizational unit.

Tasks	Detailed Steps
1. Link a Standard Desktop GPO.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>b. GPO Name: <i>ComputerName</i> Standard Desktop
2. Create and link a Folder Redirection GPO.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Usersb. GPO Name: <i>ComputerName</i> Folder Redirection
3. Create and link a Scripts GPO.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Usersb. GPO Name: <i>ComputerName</i> Scripts
4. Create and link a Proxy Settings GPO.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Computers/Desktopsb. GPO Name: <i>ComputerName</i> Proxy Settings

Exercise 2

Filtering the Deployment of a GPO

In this exercise, you will set Deny permissions for all temporary employees of Northwind Traders so that the *ComputerName* Folder Redirection GPO is not applied to them.

Tasks	Detailed Steps
1. Configure filtering of a GPO for a group.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Usersb. GPO: <i>ComputerName</i> Folder Redirectionc. Group: DL Temp Employeesd. Permissions: Set the Apply Group Policy permission to Deny

Exercise 3

Configuring the Enforcement of GPOs

In this exercise, you will configure GPOs to be enforced throughout your organizational unit hierarchy.

Tasks	Detailed Steps
1. Set the Enforced option on a GPO link.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>.b. GPO: <i>ComputerName</i> Standard Desktop linkc. Option: Enforced
2. Set the Enforced option on a GPO link.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Computers/Desktopsb. GPO: <i>ComputerName</i> Proxy Settingsc. Option: Enforced

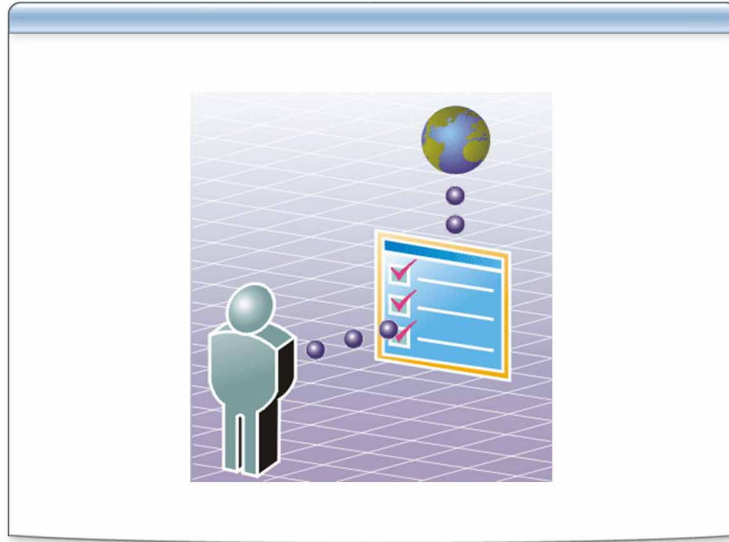
Exercise 4

Configuring the Blocking of GPOs

In this exercise, you will block inheritance of GPOs throughout your organizational unit hierarchy.

Tasks	Detailed Steps
1. Set the Block Policy inheritance option on an organizational unit.	<ul style="list-style-type: none">a. Location: nwtraders.msft/Locations/<i>ComputerName</i>/Computers/Laptopsb. Option: Block Policy inheritance

Course Evaluation



Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time before the end of the course, please complete a course evaluation, which is available at <http://www.CourseSurvey.com>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.