

# Group Policy for Beginners

139 out of 151 rated this helpful

Updated: April 27, 2011

Applies To: Windows 7

If you are an IT pro who has never used Group Policy to control computer configurations, this white paper is for you. Group Policy is the essential way that most organizations enforce settings on their computers. It is flexible enough for even the most complex scenarios; however, the essential features are easy to use in simple scenarios, which are more common.

This white paper is an introduction to Group Policy. It first provides an overview of what you can do with Group Policy, and then it describes essential concepts that you must know. For example, what is a Group Policy object (GPO)? What does inheritance mean? With the fundamentals out of the way, this white paper provides step-by-step instructions, with plenty of screenshots, for the most common Group Policy tasks.

## Note

This guide is for Group Policy novices. As much as possible, it uses plain English to describe Group Policy concepts in simple ways. Group Policy pros should see [Group Policy Planning and Deployment Guide](#) on TechNet for more technically detailed information.

For a downloadable version of this document, see [Group Policy for Beginners](#) in the Microsoft Download Center.

## Overview of Group Policy

Group Policy is simply the easiest way to reach out and configure computer and user settings on networks based on Active Directory Domain Services (AD DS). If your business is not using Group Policy, you are missing a huge opportunity to reduce costs, control configurations, keep users productive and happy, and harden security. Think of Group Policy as “touch once, configure many.”

The requirements for using Group Policy and following the instructions that this white paper provides are straightforward:

- The network must be based on AD DS (that is, at least one server must have the AD DS role installed). To learn more about AD DS, see [Active Directory Domain Services Overview](#) on TechNet.
- Computers that you want to manage must be joined to the domain, and users that you want to manage must use domain credentials to log on to their computers.
- You must have permission to edit Group Policy in the domain.

Although this white paper focuses on using Group Policy in AD DS, you can also configure Group Policy settings locally on each computer. This capability is great for one-off scenarios or workgroup computers, but using local Group Policy is not recommended for business networks based on AD DS. The reason is simple: Domain-based Group Policy centralizes management, so you can touch many computers from one place. Local Group Policy requires that you touch each computer—not an ideal scenario in a large environment. For more information about configuring local Group Policy, see [Local Group Policy Editor](#) on TechNet.

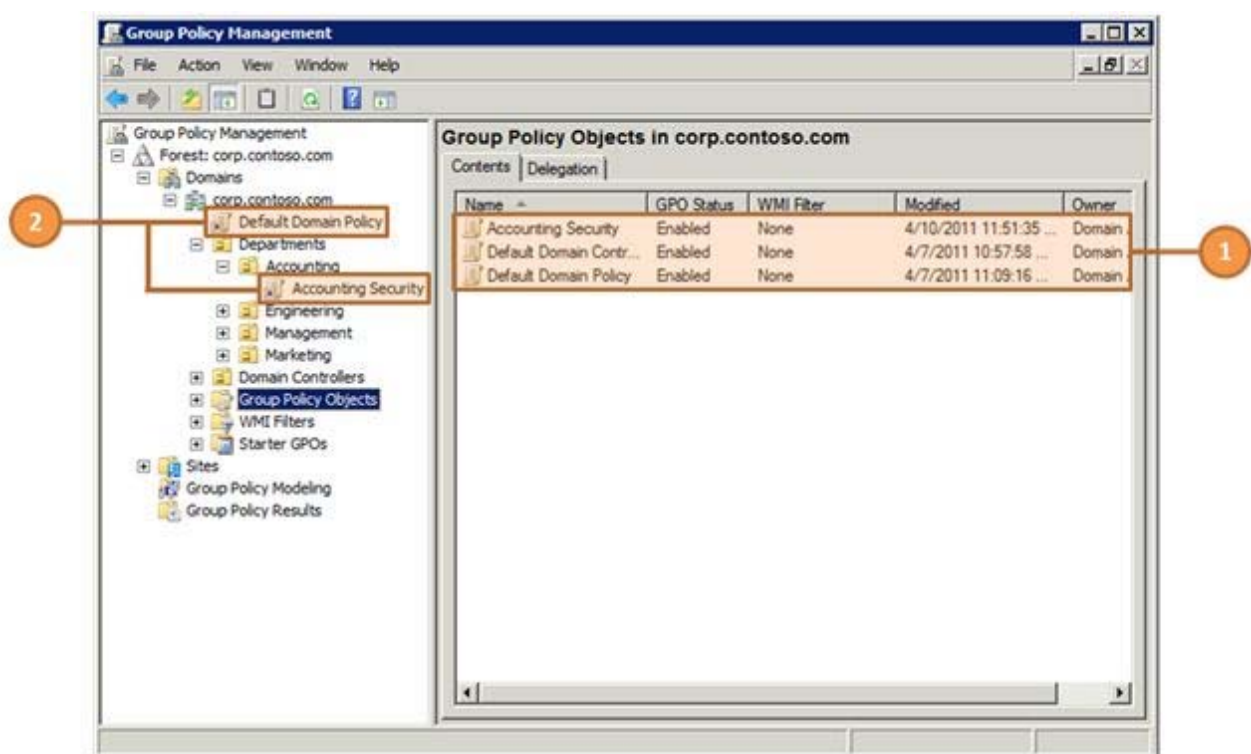
Windows 7 enforces the policy settings that you define by using Group Policy. In most cases, it disables the user interface for those settings. Additionally, because Windows 7 stores Group Policy settings in secure locations in the registry, standard user accounts cannot change those settings. So, by touching a setting one time, you can configure and enforce that setting on many computers. When a setting no longer applies to a computer or user, Group Policy removes the policy setting, restoring the original setting and enabling its user interface. The functionality is all quite amazing and extremely powerful.

#### Note

Standard user accounts are user accounts that are members of the local Users group and not the local Administrators group. They have a restricted ability to configure system settings. Windows 7 better supports standard user accounts than earlier Windows versions, allowing these accounts to change the time zone, install printers, repair network connections, and so on. Deploying standard user accounts is a best practice, and you do so by simply not adding user accounts to the local Administrators group. Windows 7 automatically adds the Domain Users group to the local Users group when you join the computer to the domain.

## Essential Group Policy Concepts

You can manage all aspects of Group Policy by using the Group Policy Management Console (GPMC). Figure 1 shows the GPMC, and this white paper will refer to this figure many times as you learn about important Group Policy concepts.



**Figure 1.** Group Policy Management Console

You start the GPMC from the Start menu: Click **Start, All Programs, Administrative Tools, Group Policy Management**. You can also click **Start**, type **Group Policy Management**, and then click **Group Policy Management** in the **Programs** section of the Start menu. Windows Server 2008 and Windows Server 2008 R2 include the GPMC when they are running the AD DS role. Otherwise, you can install the GPMC on Windows Server 2008, Windows Server 2008 R2, or Windows 7 as described in the section "Installing the GPMC in Windows 7," later in this white paper.

### Group Policy objects

GPOs contain policy settings. You can think of GPOs as policy documents that apply their settings to the computers and users within their control. If GPOs are policy documents, then the GPMC is like

Windows Explorer. You use the GPMC to create, move, and delete GPOs just as you use Windows Explorer to create, move, and delete files.

In the GPMC, you see all the domain's GPOs in the Group Policy objects folder. In Figure 1, the callout number 1 shows three GPOs for the domain corp.contoso.com domain. These GPOs are:

- **Accounting Security.** This is a custom GPO created specifically for Contoso, Ltd.
- **Default Domain Controller Policy.** Installing the AD DS server role creates this policy by default. It contains policy settings that apply specifically to domain controllers.
- **Default Domain Policy.** Installing the AD DS server role creates this policy by default. It contains policy settings that apply to all computers and users in the domain.

## Group Policy Links

At the top level of AD DS are sites and domains. Simple implementations will have a single site and a single domain. Within a domain, you can create organizational units (OUs). OUs are like folders in Windows Explorer. Instead of containing files and subfolders, however, they can contain computers, users, and other objects.

For example, in Figure 1 you see an OU named Departments. Below the Departments OU, you see four subfolders: Accounting, Engineering, Management, and Marketing. These are child OUs. Other than the Domain Controllers OU that you see in Figure 1, nothing else in the figure is an OU.

What does this have to do with Group Policy links? Well, GPOs in the Group Policy objects folder have no impact unless you link them to a site, domain, or OU. When you link a GPO to a container, Group Policy applies the GPO's settings to the computers and users in that container. In Figure 1, the callout number 1 points to two GPOs linked to OUs:

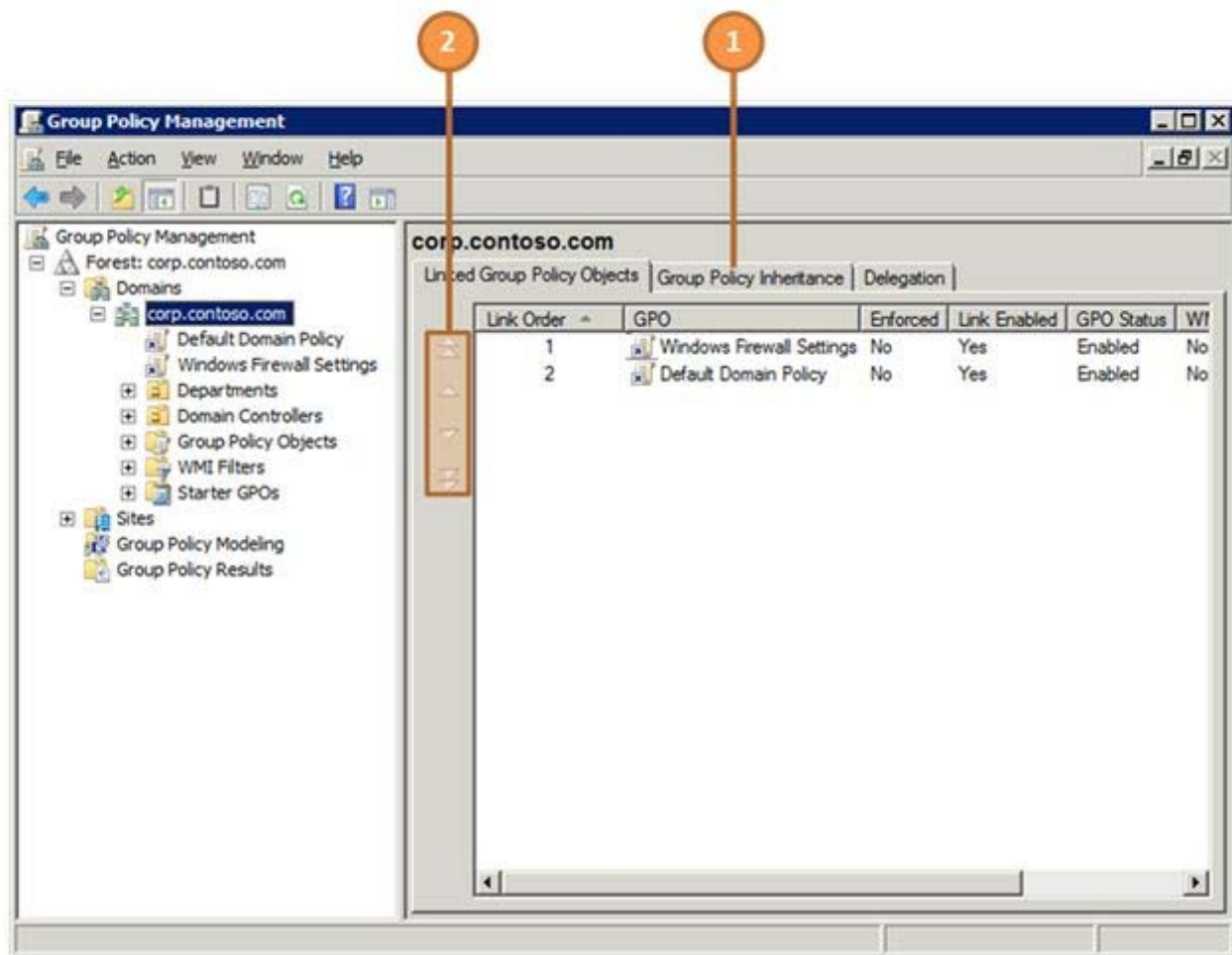
- The first GPO is named Default Domain Policy, and this GPO is linked to the domain corp.contoso.com. This GPO applies to every computer and user in the domain.
- The second GPO is named Accounting Security, and this GPO is linked to the OU named Accounting. This GPO applies to every computer and user in the Accounting OU.

In the GPMC, you can create GPOs in the Group Policy objects folder and then link them—two steps. You can also create and link a GPO in one step. Most of the time, you will simply create and link a GPO in a single step, which the section “Creating a GPO,” later in this white paper, describes.

## Group Policy Inheritance

As the previous section hinted, when you link a GPO to the domain, the GPO applies to the computers and users in every OU and child OU in the domain. Likewise, when you link a GPO to an OU, the GPO applies to the computers and users in every child OU. This concept is called inheritance.

For example, if you create a GPO named Windows Firewall Settings and link it to the corp.contoso.com domain in Figure 1, the settings in that GPO apply to all of the OUs you see in the figure: Departments, Accounting, Engineering, Management, Marketing, and Domain Controllers. If instead you link the GPO to the Departments OU, the settings in the GPO apply only to the Departments, Accounting, Engineering, Management, and Marketing OUs. It does not apply to the entire domain or the Domain Controllers OU. Moving down one level, if you link the same GPO to the Accounting OU in Figure 1, the settings in the GPO apply only to the Accounting OU, as it has no child OUs. In the GPMC, you can see what GPOs a container is inheriting by clicking the Group Policy Inheritance tab (callout number 1 in Figure 2).



**Figure 2.** Group Policy inheritance and precedence

So, what happens if multiple GPOs contain the same setting? This is where order of precedence comes into play. In general, the order in which Group Policy applies GPOs determines precedence. The order is site, domain, OU, and child OUs. As a result, GPOs in child OUs have a higher precedence than GPOs linked to parent OUs, which have a higher precedence than GPOs linked to the domain, which have a higher precedence than GPOs linked to the site. An easy way to think of this is that Group Policy applies GPOs from the top down, overwriting settings along the way. In more advanced scenarios, however, you can override the order of precedence.

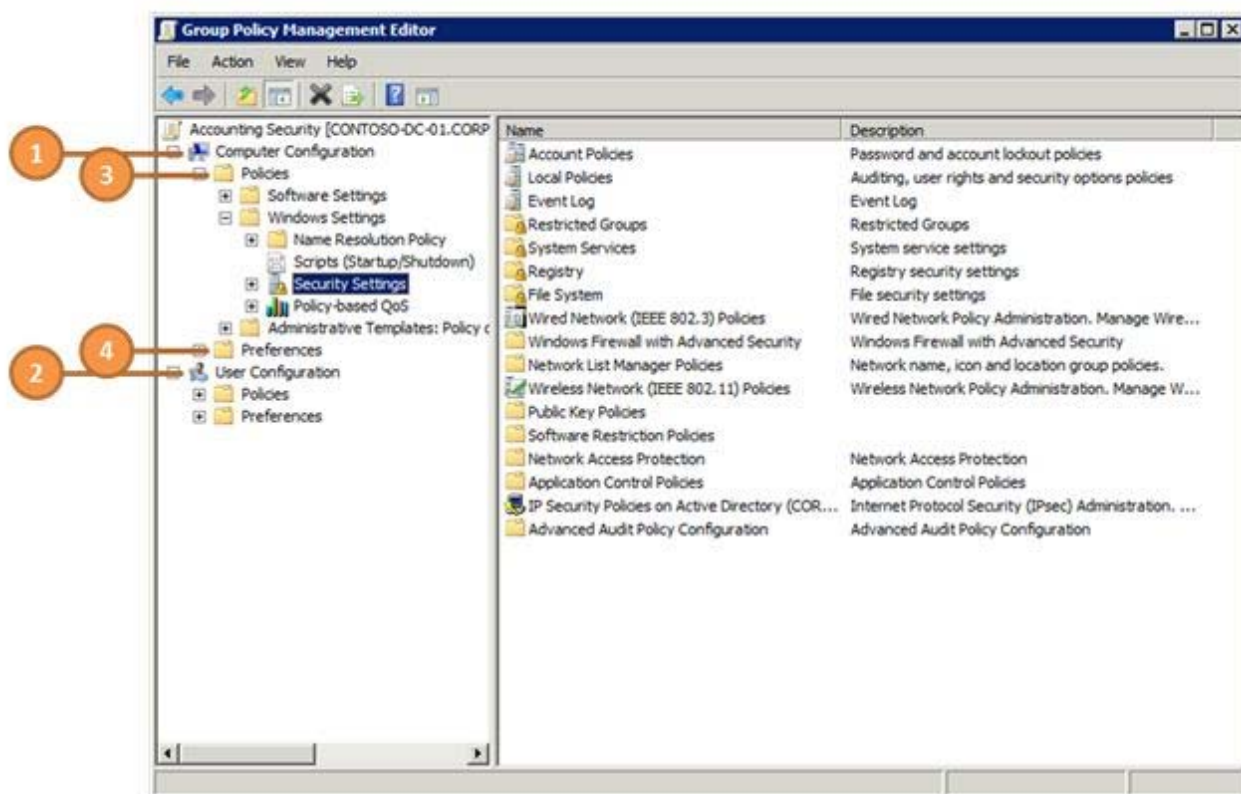
You can also have—within a single OU—multiple GPOs that contain the same setting. Like before, the order in which Group Policy applies GPOs determines the order of precedence. In Figure 2, you see two GPOs linked to the domain corp.contoso.com: Windows Firewall Settings and Default Domain Policy. Group Policy applies GPOs with a lower link order after applying GPOs with a higher link order. In this case, it will apply Windows Firewall Settings after Default Domain Policy. Just remember that a link order of 1 is first priority, and a link order of 2 is second priority. You can change the link order for a container by clicking the up and down arrows as shown by callout number 2 in Figure 2.

#### Note

As you are probably realizing by now, Group Policy is a remarkably versatile tool. However, Group Policy provides the opportunity to make things overly complicated. In simple environments, such as labs and small businesses, there is nothing wrong with linking all of your GPOs to the domain. Keep it simple. There should be a justification for complication. In Figure 1, if you wanted to create a GPO and link it only to the Engineering and Marketing OUs, the justification should be that the GPO contains settings that apply only to those two departments and should not be applied to any other department. If you cannot make this justification, then keep things simple by linking the GPO one time to the domain.

## Group Policy Settings

To this point, you have learned about GPOs. You have learned that GPMC is to GPOs and OUs as Windows Explorer is to files and folders. GPOs are the policy documents. At some point, you are going to have to edit one of those documents, though, and the editor you use is the Group Policy Management Editor (GPME), which Figure 3 shows. You open a GPO in the GPME by right-clicking it in the GPMC and clicking **Edit**. Once you are finished, you simply close the window. The GPME saves your changes automatically, so you do not have to save.



**Figure 3.** Group Policy Management Editor

In Figure 3, callout numbers 1 and 2 point to Computer Configuration and User Configuration, respectively. The Computer Configuration folder contains settings that apply to computers, regardless of which users log on to them. These tend to be system and security settings that configure and control the computer. The User Configuration folder contains settings that apply to users, regardless of which computer they use. These tend to affect the user experience.

Within the Computer Configuration and User Configuration folders, you see two subfolders (callout numbers 3 and 4 in Figure 3):

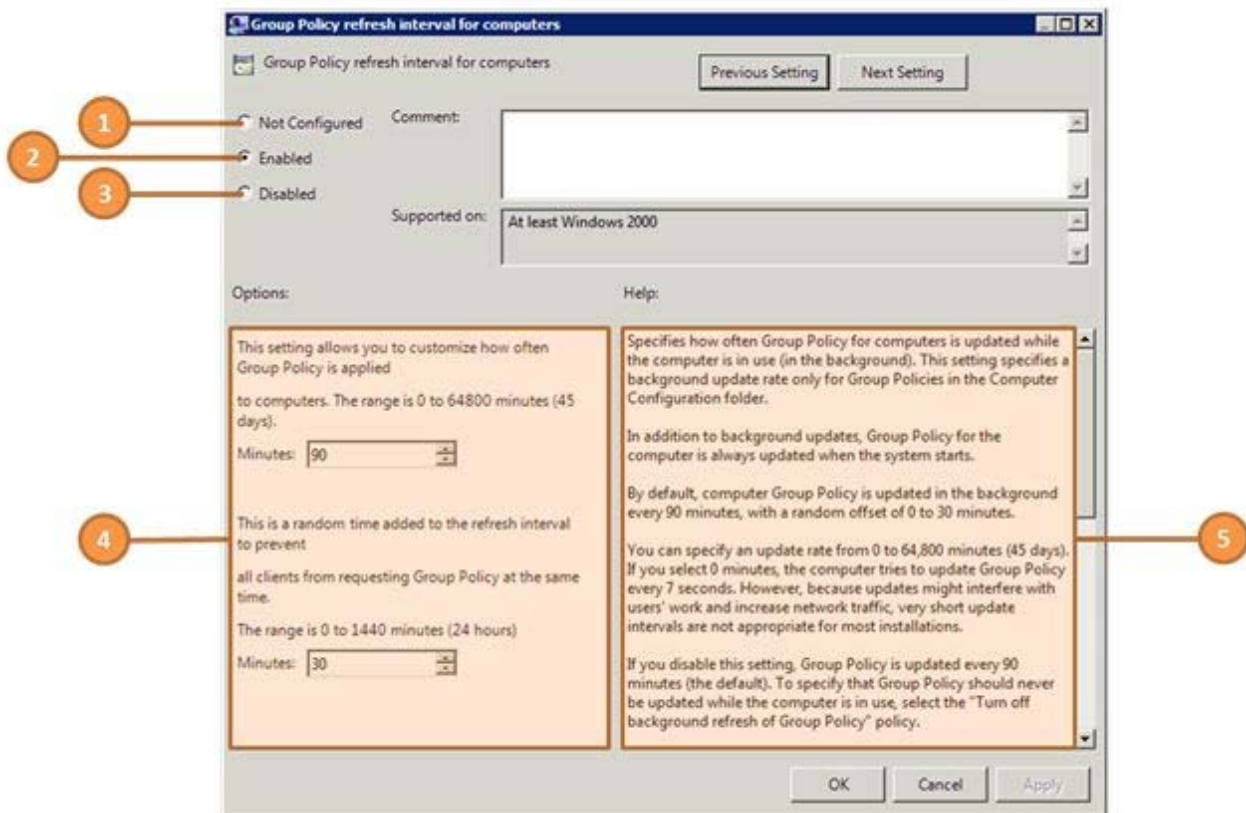
- **Policies.** Policies contains policy settings that Group Policy enforces.
- **Preferences.** Preferences contains preference settings that you can use to change almost any registry setting, file, folder, or other item. By using preference settings, you can configure applications and Windows features that are not Group Policy–aware. For example, you can create a preference setting that configures a registry value for a third-party application, deletes the Sample Pictures folder from user profiles, or configures an .ini file. You can also choose whether Group Policy enforces each preference setting or not. However, standard user accounts can change most preference settings that you define in the User Configuration folder between Group Policy refreshes. You can learn more about preference settings by reading the [Group Policy Preferences Overview](#).

When you are first learning Group Policy, most of the settings that you will configure will be in the Administrative Templates folders. These are registry-based policy settings that Group Policy enforces. They are different from other policy settings for two reasons. First, Group Policy stores these settings in specific registry locations, called the Policies branches, which standard user accounts cannot change. Group Policy–aware Windows features and applications look for these settings in the registry.



If they find these policy settings, they use the policy settings instead of the regular settings. They often disable the user interface for those settings as well.

Second, administrative template files, which have the .admx extension, define templates for these settings. These templates not only define where policy settings go in the registry but also describe how to prompt for them in the GPME. In the Group Policy setting that Figure 4 shows, for example, an administrative template file defines help text, available options, supported operating systems, and so on.



**Figure 4.** Group Policy setting

When you edit a policy setting, you are usually confronted with the choices that callout numbers 1 to 3 indicate in Figure 4. In general, clicking:

- **Enabled** writes the policy setting to the registry with a value that enables it.
- **Disabled** writes the policy setting to the registry with a value that disables it.
- **Not Configured** leaves the policy setting undefined. Group Policy does not write the policy setting to the registry, and so it has no impact on computers or users.

Generalizing what enabled and disabled means for every policy setting is not possible. You can usually read the help text, shown in callout number 5, to determine exactly what these choices mean. You must also be careful to read the name of the policy setting. For example, some policy settings say, "Turn on feature X," whereas other policy settings say, "Turn off feature Y." Enabled and disabled have different meanings in each case. Until you are comfortable, make sure you read the help text for policy settings you configure.

Some policy settings have additional options that you can configure. Callout number 4 in Figure 4 shows the options that are available for the Group Policy refresh interval policy setting. In most cases, the default values match the default values for Windows. As well, the help text usually gives detailed information about the options you can configure.

## Group Policy Refresh

As you learned in the previous section, GPOs contain both computer and user settings. Group Policy applies:

- Computer settings when Windows starts.
- User settings after the user logs on to the computer.

Group Policy also refreshes GPOs on a regular basis, ensuring that Group Policy applies new and changed GPOs without waiting for the computer to restart or the user to log off. The period of time between these refreshes is called the Group Policy refresh interval, and the default is 90 minutes with a bit of randomness built in to prevent all computers from refreshing at the same time. If you change a GPO in the middle of the day, Group Policy will apply your changes within about 90 minutes. You don't have to wait until the end of the day, when users have logged off of or restarted their computers. In advanced scenarios, you can change the default refresh interval.

#### Note

You can manually update Group Policy any time by using the command `Gpupdate.exe`. For example, after updating a GPO, you might want to refresh Group Policy on a computer in order to test your changes without waiting for the Group Policy refresh interval. For step-by-step instructions, see the section titled “Updating Clients” later in this white paper.

## Essential Group Policy Tasks

You have now learned the essential Group Policy concepts. You know that a GPO is like a document that contains policy settings. You manage GPOs by using the GPMC and you edit them by using the GPME.

You also know that you link GPOs to AD DS sites, domains, and OUs to apply the GPOs' settings to those containers. Domains, OUs, and child OUs inherit settings from their parents, but duplicate settings in GPOs linked to child OUs have precedence over the same settings in GPOs linked to parent OUs, which have precedence over GPOs linked to the domain, and so on.

You also know that within a site, domain, or OU, the link order determines the order of precedence (the smaller the number, the higher the precedence). Last, you have an essential understanding of how to edit GPOs and what types of settings they contain.

Now that you know the essential concepts, you are ready to learn the essential tasks. This section describes how to create, edit, and delete GPOs. It describes many other tasks, as well. For each task, you'll find an explanation of its purpose and step-by-step instructions with screenshots at each step.

#### Note

A feature of the Microsoft Desktop Optimization Pack (MDOP) called Advanced Group Policy Management (AGPM) extends Group Policy with new capabilities such as offline editing, version control, and role-based delegation. Any organization can benefit from using AGPM to manage Group Policy. For more information about AGPM, see [Enhancing Group Policy through change management](#).

## Creating a GPO

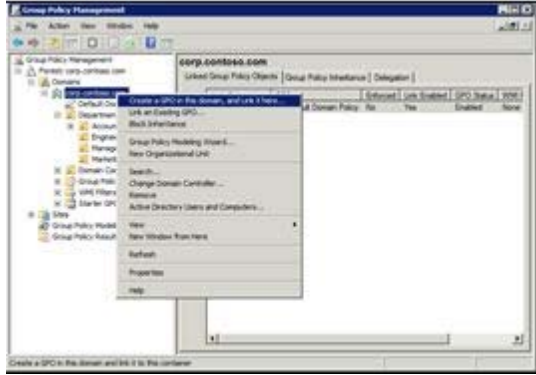

You create a GPO by using the GPMC. There are two ways to create a GPO:

- Create and link a GPO in one step.
- Create a GPO in the Group Policy objects folder, and then link it to the domain or OU.

The instructions in this section describe how to create and link a GPO in one step.

You can start with a blank GPO, which the instructions describe, or you can use a starter GPO. Starter GPOs are an advanced topic that you can learn about in [Working with Starter GPOs](#).

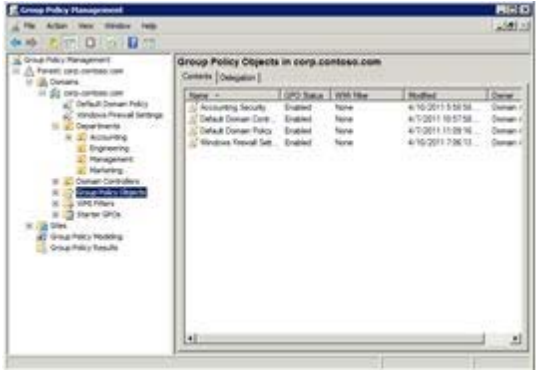
**To create and link a GPO in the domain or an OU**

|  |   |
|--|---|
| <p>1 In the GPMC, right-click the domain or OU in which you want to create and link a GPO, and click <b>Create a GPO in this domain, and Link it here</b>.</p> |   |
| <p>2 In the <b>Name</b> box on the <b>New GPO</b> dialog box, type a descriptive name for the GPO, and then click <b>OK</b>.</p>                               |  |

**Editing a GPO**

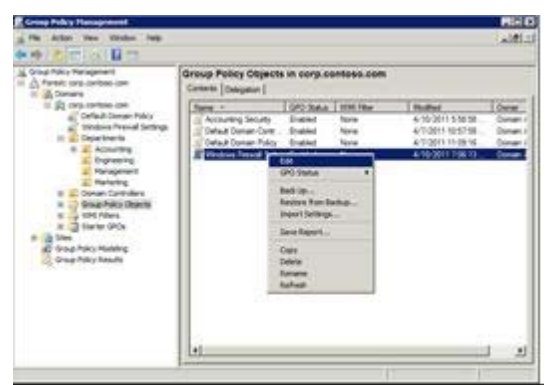
In the GPMC, you can open GPOs in the GPME to edit them within any container. To see all of your GPOs, regardless of where you link them, use the Group Policy objects folder to edit them.

**To edit a GPO in the domain, an OU, or the Group Policy objects folder**

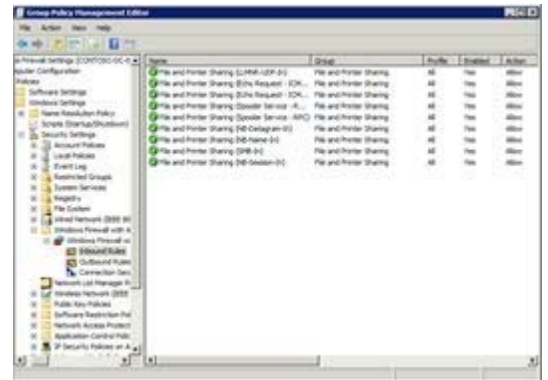
|  |  |
|--|--|
| <p>1 In the left pane of the GPMC, click <b>Group Policy objects</b> to display all the domain's GPOs in the right pane. Alternatively, you can click the domain or any OU to display that container's GPOs in the right pane.</p> |  |
|--|--|



- In the right pane of the GPMC, right-click the GPO that you want to edit, and click **Edit** to open the GPME in the GPME.



- In the GPME, edit the Group Policy settings that you want to change, and close the GPME window when finished. You do not have to save your changes, because the GPME saves your changes automatically.

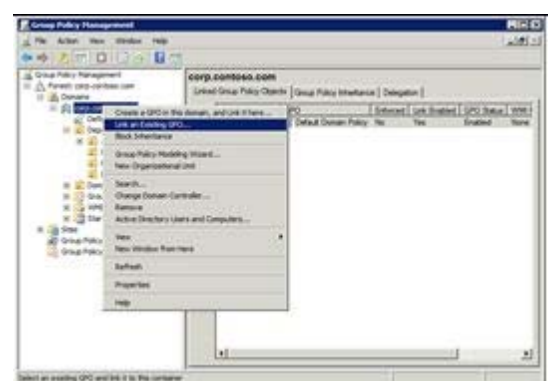


## Linking a GPO

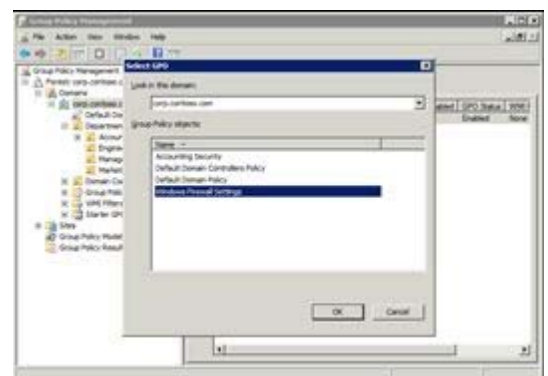
If you create and link GPOs in one step, you do not have to manually link GPOs to the domain or OUs. However, if you create a GPO in the Group Policy objects folder or unlink a GPO and want to restore it, you will need to manually link the GPO. The easy way to link a GPO is to simply drag the GPO from the Group Policy objects folder and drop it onto the domain or OU to which you want to link it.

### To link a GPO to a domain or OU

- In the GPMC, right-click the domain or OU to which you want to link the GPO, and then click **Link an Existing GPO**.



- In the **Select GPO** dialog box, click the GPO that you want to link to the domain or OU, and then click **OK**.

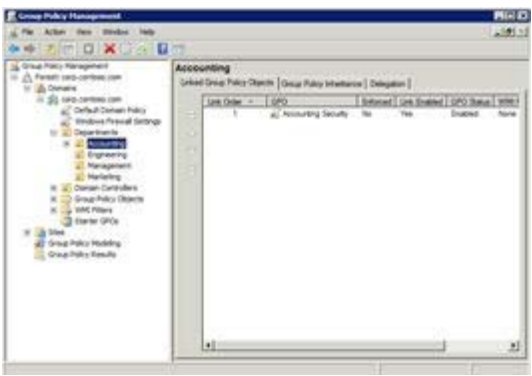
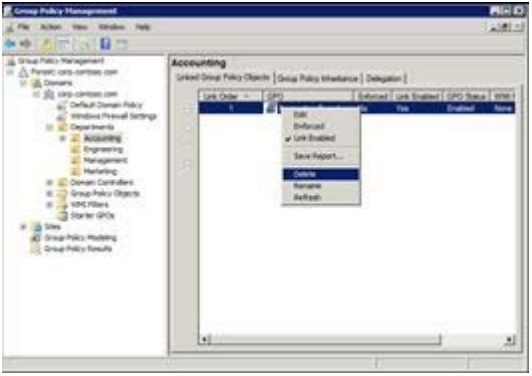
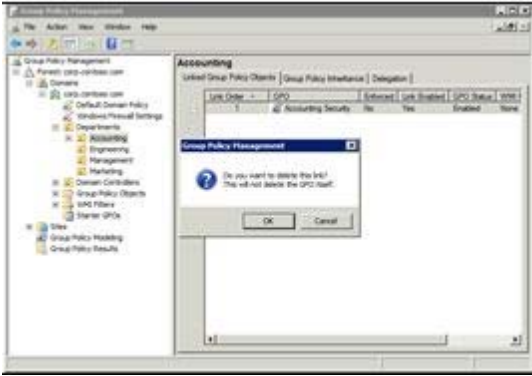


# Unlinking a GPO

You unlink a GPO when you no longer want to apply it to the domain or OU (or its child OUs). You can later restore the link, as the section titled “Linking a GPO” described.


Unlinking a GPO from a domain or OU does not delete the GPO. It only deletes the link. After unlinking a GPO, you can still find it in the Group Policy objects folder in the GPMC.

## To unlink a GPO from a domain or OU

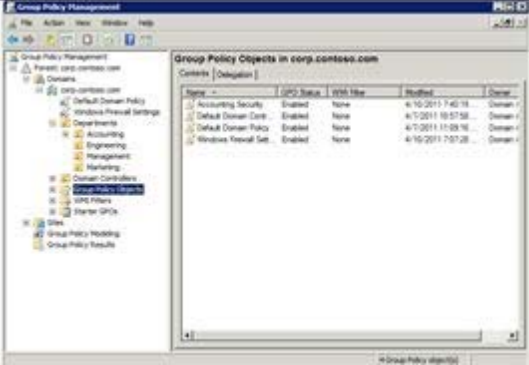
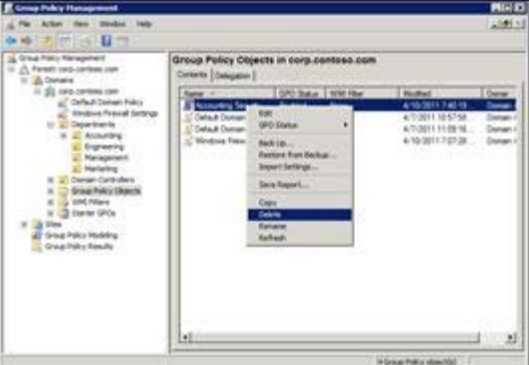
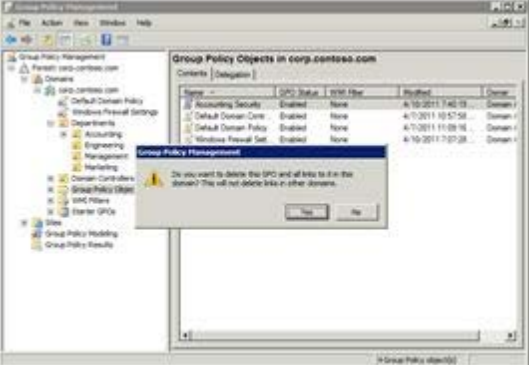
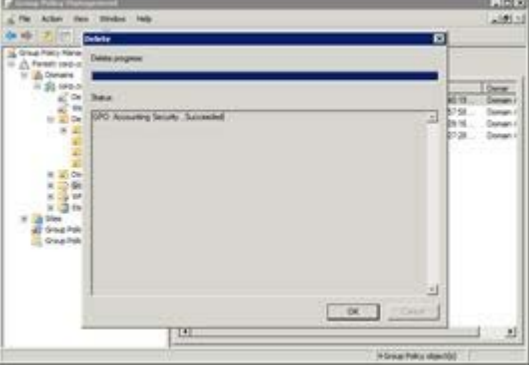
|   |  |  |
|---|--|--|
| 1 | In the GPMC, click the domain or OU containing the GPO that you want to unlink.              |    |
| 2 | Right-click the GPO that you want to unlink from the domain or OU, and click <b>Delete</b> . |   |
| 3 | In the <b>Group Policy Management</b> dialog box, click <b>OK</b> .                          |  |

# Deleting a GPO

Deleting a GPO is not the same as unlinking a GPO from a domain or OU. You delete GPOs within the Group Policy objects folder. Doing so removes not only the links but also the GPO itself.

|  |
|--|
|  <b>Note</b>  |
| Consider backing up the GPO before deleting it. The section titled “Backing Up GPOs” describes how to back up GPOs. The section titled “Restoring GPOs” describes how to restore them from a backup. |


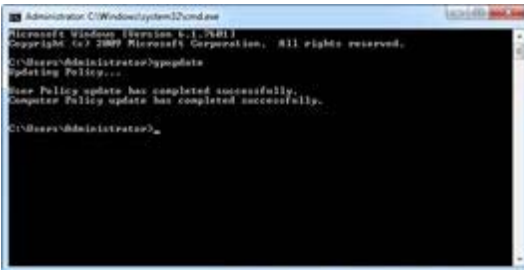
## To delete a GPO from the Group Policy objects folder

|   |  |  |
|---|--|--|
| 1 | In the GPMC, click the <b>Group Policy objects</b> folder.   |    |
| 2 | In the right pane of the GPMC, right-click the GPO that you want to delete, and click <b>Delete</b> .                        |    |
| 3 | In the <b>Group Policy Management</b> dialog box, click <b>Yes</b> to confirm that you want to delete the GPO and its links. |   |
| 4 | In the <b>Delete</b> dialog box, confirm that the deletion was successful, and click <b>OK</b> .                             |  |

## Updating Clients

While editing, testing, or troubleshooting GPOs, you do not need to wait for the Group Policy refresh interval (90 minutes, by default). You can manually update Group Policy on any client computer by running Gpupdate.exe. Gpupdate.exe supports many command-line options, which you can learn about by typing gpupdate.exe /? in a Command Prompt windows In most cases, however, you can follow the instructions in this section to update Group Policy.

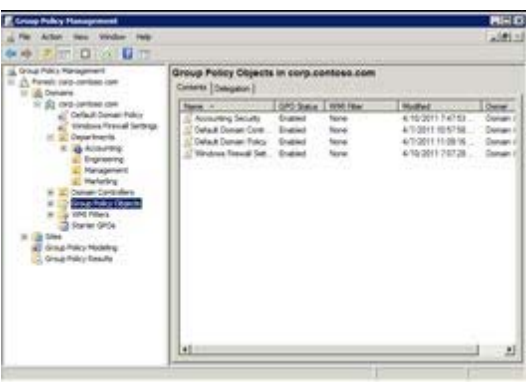
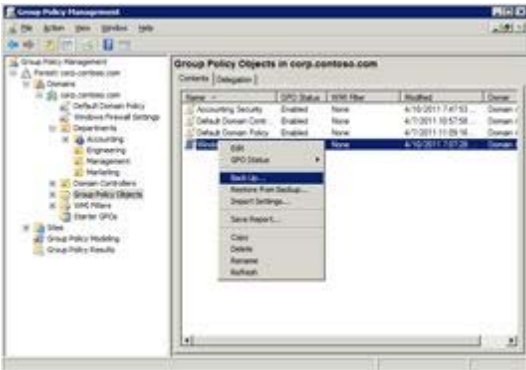
### To manually update Group Policy by using Gpupdate.exe

|   |  |  |
|---|--|--|
| 1 | Click <b>Start</b> , type <b>cmd</b> , and press <b>Enter</b> to open a Command Prompt window.   |  |
| 2 | At the Command Prompt, type <b>gpupdate</b> and press <b>Enter</b> . Gpupdate.exe will update any changed settings. You can force Gpupdate.exe to update all settings, whether or not they have changed recently, by typing <b>gpupdate /force</b> and pressing <b>Enter</b> . |  |

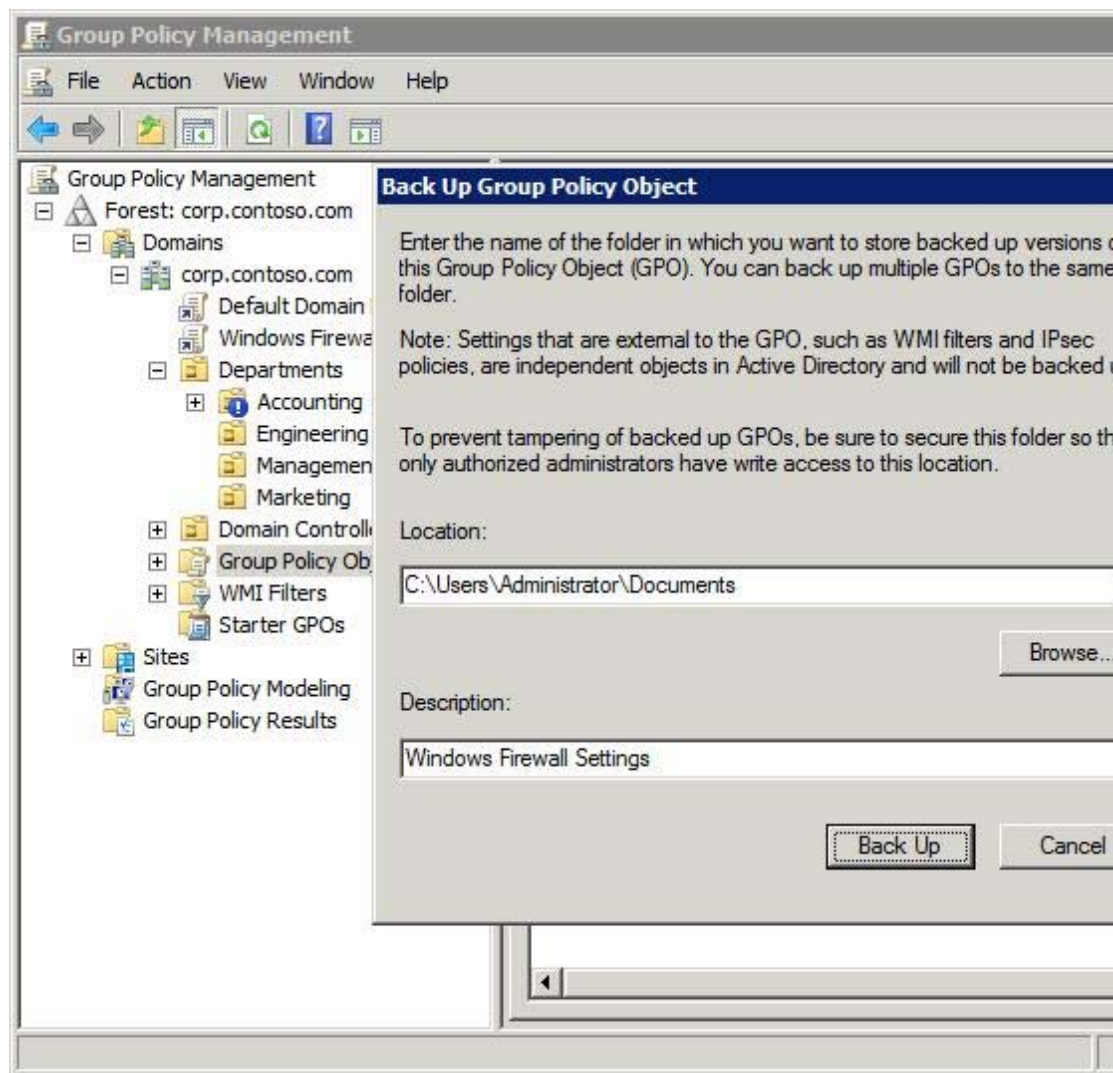
## Backing Up GPOs

Backing up important files is an important practice, and GPOs are no exception. If you erroneously change or accidentally delete a GPO, you can quickly restore it from a backup. By using the GPMC, you can back up GPOs to any location.

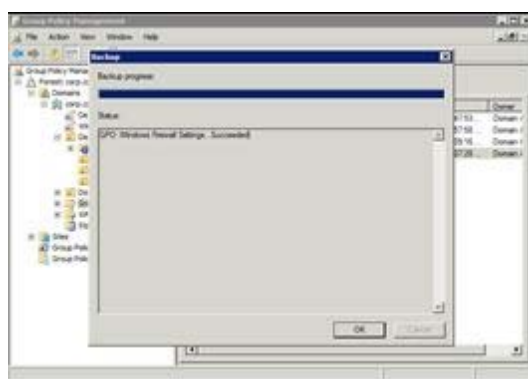
### To back up a GPO to a folder

|   |  |   |
|---|--|---|
| 1 | In the GPMC, click the <b>Group Policy objects</b> folder.               |  |
| 2 | Right-click the GPO that you want to back up, and click <b>Back Up</b> . |  |

- 3 In the **Location** box of the **Back Up Group Policy object** dialog box, type the path of the folder to which you want to back up the GPO. You can also click **Browse** to choose a folder. Also, in the **Description** box, type a brief description of the GPO, and then click **Back Up**.



- 4 In the **Backup** dialog box, confirm the results and click **OK**.

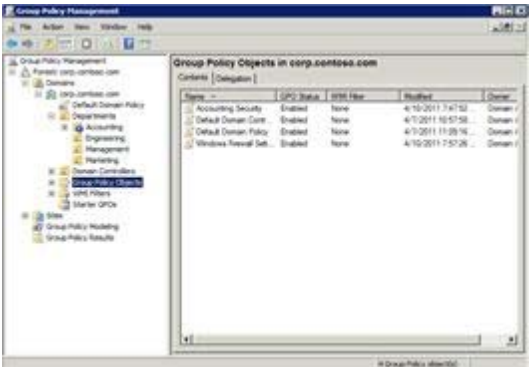
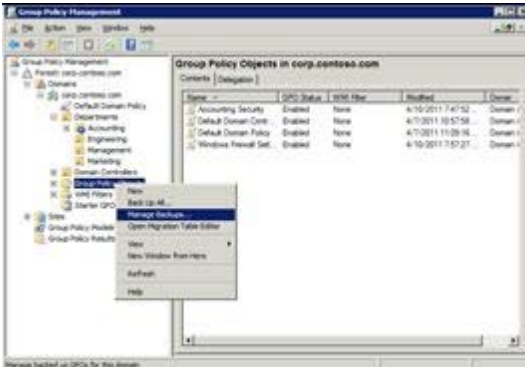
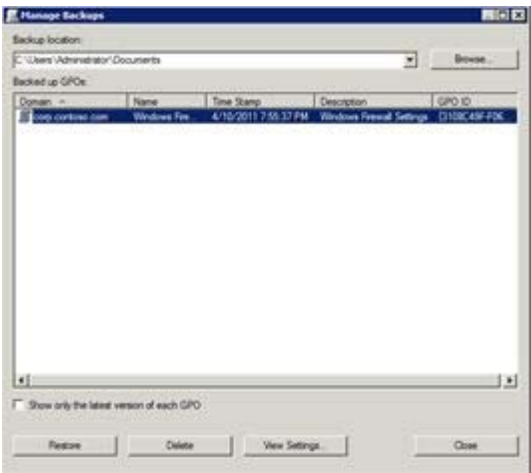
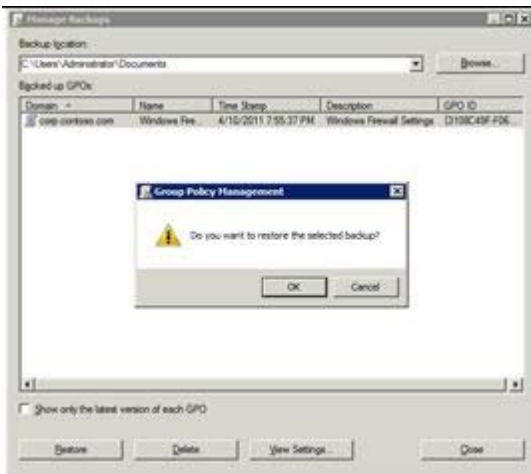


## Restoring GPOs

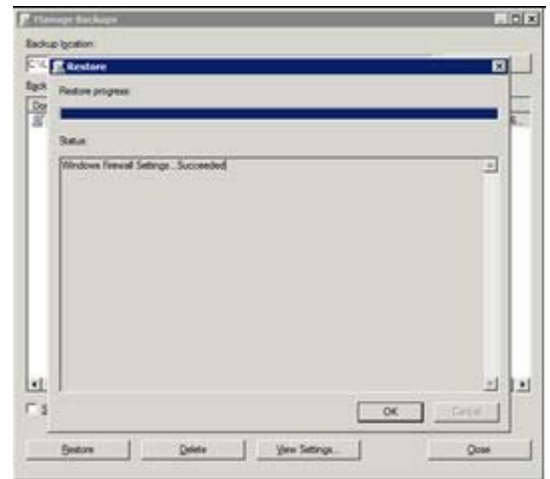
By using the GPMC, you can restore any previous version of a GPO that you have backed up. The instructions in this section describe how to restore one or more GPOs from a backup folder.

### To restore a previously backed-up GPO



|   |  |  |
|---|--|--|
| 1 | In the GPMC, click the <b>Group Policy objects</b> folder to see the GPOs in the domain.   |     |
| 2 | Right-click the <b>Group Policy objects</b> folder, and click <b>Manage Backups</b> .  |    |
| 3 | In the <b>Backup location</b> list of the <b>Manage Backups</b> dialog box, click a backup location that you've previously used. You can also click <b>Browse</b> to choose a folder containing GPO backups.   |   |
| 4 | In the <b>Backed up GPOs</b> list, choose one or more GPOs that you want to restore, and click <b>Restore</b> . If you see multiple versions of each GPO and want to see only the most recently backed-up version of each GPO, select the <b>Show only the latest version of each GPO</b> check box. |  |

- 5 In the **Restore** dialog box, confirm that the operation was successful, and click **OK**.



## Installing the GPMC in Windows 7

Windows Server 2008 and Windows Server 2008 R2 include the GPMC when they are running the AD DS role. Otherwise, you can install the GPMC on Windows Server 2008, Windows Server 2008 R2, or Windows 7. You install the GPMC by downloading the [Remote Server Administration Tools for Windows 7 with Service Pack 1 \(SP1\)](#) and installing either of the following files on the computer:

1. **Windows6.1-KB958830-x64-RefreshPkg.msu**. Install this package on x64 computers, including those running Windows Server 2008 R2.
2. **Windows6.1-KB958830-x86-RefreshPkg.msu**. Install this package on x86 computers.

Installing the update only adds the feature to Windows. You must also turn on the Group Policy Management Tools feature using Programs and Features in the Control Panel. The instructions in this section describe how to install the update as well as how to enable the Group Policy Management Tools.

### To install the Remote Server Administration Tools for Windows 7 with SP1

- 1 Run either of the following files that you previously downloaded:
  1. Windows6.1-KB958830-x64-RefreshPkg.msu
  2. Windows6.1-KB958830-x86-RefreshPkg.msu

Then, click **Yes** to install the update.



- 2 On the **Read these license terms (1 of 1)** page, review the license terms, and if you accept, click **I Accept**.

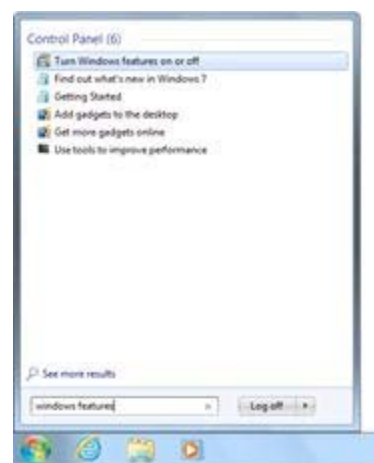


- 3 On the **Installation complete** page, click **Close**.



### To turn on the Group Policy Management Tools feature

- 1 Click **Start**, type **windows features**, and click **Turn Windows features on or off** in the **Control Panel** section of the Start menu.



- 2 In the **Windows Features** dialog box, select the **Group Policy Management Tools** check box, and click **OK**. **Group Policy Management Tools** is under **Remote Service Administration Tools, Feature Administration Tools**.



## Conclusion

You have come a long way. You have learned important Group Policy concepts such as GPOs, links, inheritance, and so on. You have also learned how to use the GPMC and the GPME to perform essential tasks such as creating, editing, and deleting GPOs.

When you are ready to learn more about Group Policy and broaden your skills, Microsoft has numerous resources available for you. First, the [Group Policy resource page](#) on the Windows Server TechCenter is a one-stop shop for any technical content related to Group Policy. It provides numerous getting-started guides as well as videos. For Group Policy guidance specific to Windows 7, visit the [Windows Client Security and Control zone](#).

Did you find this helpful? ☐ Yes ☐ No