CHAPTER 6

Group Policy Control in Microsoft Windows

MICROSOFT PROVIDES MORE EFFECTIVE security controls and countermeasures with each new Windows release. This protects computers from new and improved methods of attacks. It can be difficult and confusing to keep track of all the individual security rules as the number of new features continues to grow. Windows provides administrators with the ability to configure many security rules in a central location. The **Group Policy** feature of Windows organizes collections of security rules that control different aspects of how Windows operates. To make administration easier, collections of Group Policy settings can be stored in named objects called **Group Policy Objects (GPOs)**. GPOs can be associated with one or more users and across multiple computers to enforce settings without having to edit each user's individual settings.

In this chapter, you'll learn about Group Policy and GPOs and how to maintain them in Windows. You'll learn how to use GPOs to control what your users can and cannot do. You'll also learn how to do more than just change settings—you'll learn how to design GPOs that satisfy your organization's security policy.

Chapter 6 Topics

This chapter covers the following topics and concepts:

- What Group Policy and GPOs are
- How to make Group Policy conform to security policy
- Which types of GPOs are in the Registry
- Which types of GPOs are stored in Active Directory
- What designing, deploying, and tracking Group Policy controls are
- How to audit and manage Group Policy
- What best practices for Microsoft Windows Group Policy and processes are

Chapter 6 Goals

When you complete this chapter, you will be able to:

- Explain Group Policy and GPO
- Recognize the relationship between Group Policy and security policy
- Illustrate how to make Group Policy conform to security policy
- Describe GPOs in the Windows Registry
- Describe GPOs in Active Directory
- Design Group Policy controls
- Analyze techniques to deploy and track Group Policy controls
- Examine auditing and managing Group Policy
- Outline best practices for Group Policy and processes
- Discuss business challenges of Group Policy

Group Policy and GPOs

The Windows Group Policy feature provides a centralized set of rules that govern the way Windows operates. It provides the ability to define and apply both general and security configuration changes to one or more computers. You can define both Local Group Policy settings and Group Policies in Active Directory. Local Group Policies control the behavior of a single computer. Active Directory Group Policies can apply to any users on any computers defined in Active Directory. Using Group Policy can make administration tasks easier than having to write scripts or individually secure basic security settings.

When booting a computer or logging on, Windows looks up and applies the GPOs for that computer and user. Group Policy uses a "pull" technology, which means that Windows periodically searches for any updated GPOs. If it finds a new GPO, it downloads and applies the changes to the existing environment. It pulls new or changed GPOs to the local computer and ensures that the settings are current. By default, Windows checks for new or updated GPOs at a random interval from 90 to 120 minutes. This automatic update feature ensures that Windows applies any new or updated GPOs, often without requiring that users log off or reboot computers.

NOTE

Starting with Windows Server 2012, Microsoft included a new feature, called the Remote Group Policy Update, to make applying GPOs easier. Instead of waiting for individual computers to pull GPO changes, Windows Server 2012 and later computers can force GPOs to refresh. All of the selected computers will receive the new or changed GPOs within 10 minutes. You can also use another feature available starting in Windows Server 2012 called GPO caching. If GPO caching is enabled, selected computers will save GPOs locally and use those for the next restart. The advantage is computers using cached GPOs will start faster. The drawback is that any GPO changes that occurred while a computer is offline will be sent to that computer at a regular interval after that computer starts, and not at start time.

Group Policy Settings

GPOs make it easy to enforce standard behavior across multiple users or computers. For example, GPOs can easily set firewall settings on multiple computers, define consistent desktop layouts, run scripts when users log on and log off, and redirect folders to network folders. These are only a few of the uses for GPOs. **TABLE 6-1** lists additional category settings using GPOs.

Group Policy is a central method to customize computer and user settings (**FIGURE 6-1**). Most operating systems, including Windows, provide the ability to create boot and logon scripts that run when a computer boots or a user logs on. Group Policy extends this capability by maintaining the commands from a central location. You don't have to make changes to scripts and copy them to each computer or user's directory. Group Policy changes are automatically distributed to the right locations. Another benefit that bears a closer look is the periodic update feature of Group Policy. Boot and logon scripts take effect only when you reboot the

TABLE 6-1 Categories of Settings in GPOs

CATEGORY	DESCRIPTION
Password Policy	Sets requirements for password strength, age, history, and storage
Account Lockout Policy	Determines how Windows handles accounts locked after failed logon attempts
Kerberos Policy	Sets lifetime limits for Kerberos tickets and clock synchronization
Audit Policy	Defines events Windows should record in audit files
User Rights Assignment	Assigns individual user rights that define what general actions users can perform, such as "Access this computer from the network" or "Change the system time"
Security Options	Offers options granting rights that define what security-related actions users can perform, such as "Allowed to format and eject removable media" or "Require smart card"
Event Log	Defines maximum size, retention settings, and guest access settings for event logs
Restricted Groups	Lists users in security-sensitive groups and to what other groups the restricted group can belong
System Services	Defines startup mode and access permissions for system services
Registry	Defines access permissions and audit settings for Registry keys
File System	Defines access permissions on discretionary access control lists (DACLs) and audit settings for system access control lists (SACLs)

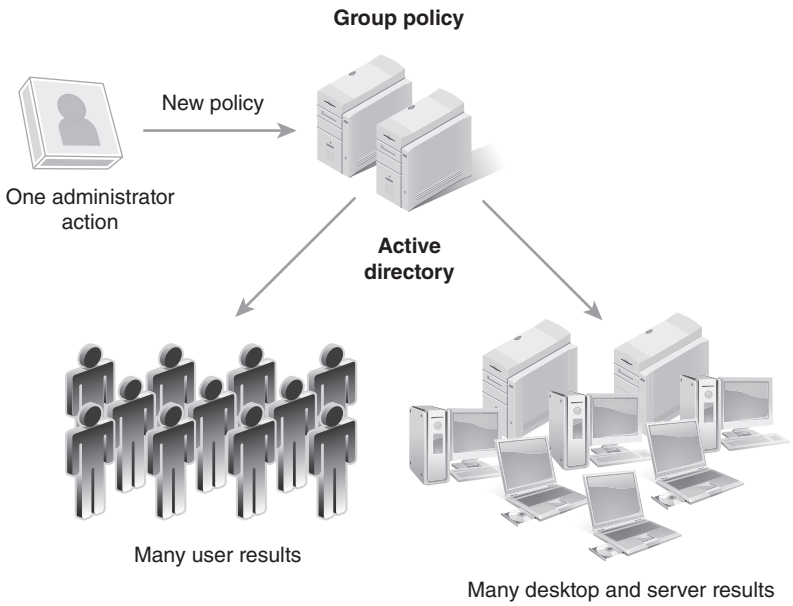


FIGURE 6-1
Group Policy.

computer or log off and log on again. Group Policy applies many settings to the current session. This feature causes changes to take effect faster than with using other configuration options.

Technical TIP

Microsoft publishes a handy spreadsheet listing all of the Group Policy settings included when installing an operating system. Microsoft includes several template files with each Windows version that define many settings. The spreadsheet can be found by visiting the website *http://www.microsoft.com/downloads*, and searching for "Group Policy Settings Reference." Microsoft provides several versions of the spreadsheet to cover different Windows releases. This reference contains descriptive information you can use to create and modify GPOs to meet your organization's security needs.

NOTE

You may define a desktop with icons related to manufacturing applications for the Manufacturing OU. A user who logs on to a computer in the Manufacturing OU will see the desktop specific to manufacturing. Users who log on to a computer that is not in the Manufacturing OU will see a different desktop.

GPO Linking

You can link GPOs to specific users to customize settings for groups of users or even individual users. Users who log on anywhere in the Active Directory domain will get GPOs linked to their user account. You can also link GPOs to **organizational units (OUs)**. In fact, you must link GPOs to at least one computer, domain, or OU for the GPO to be active. GPOs that aren't linked to a computer, domain, or OU are defined but inactive. You can define OUs to logically group computers into functional groups, such as "Accounting," "Manufacturing," and "Distribution." Once you define one or more OUs, you can add computers to each OU to logically group them together. When you link GPOs to OUs, Windows will download and apply only the appropriate GPOs for the computer and the user logging on.

Making Group Policy Conform to Security Policy

Group Policy is a functional feature of Windows that has little meaning by itself. It is a mechanism used to apply controls enforcing your security policy. For example, should you set a maximum password age for all the computers in your environment? The answer is: "It depends." Setting a maximum password age is generally a good idea, but not something you should arbitrarily enforce. Your security policy should direct any settings you add to GPOs. In fact, the GPOs you define and use should conform to your security policy. There are two main reasons for making Group Policy conform to your security policy: to allow management to meet security responsibilities, and to ensure that there are no gaps in your security policy and your policy doesn't contain additional controls.

WARNING

Your organization's culture should provide guidance on interpreting the security policy. A strict security policy interpretation means that no security controls exist unless they are directed by the policy. A less strict interpretation is more common. It allows IT security to exercise some discretion to implement best practices that may not be explicitly defined in the security policy.

Security Responsibility

First, it is management's responsibility to ensure the security of an organization's assets, including information. All actions IT security personnel take to secure information occur within the authority granted by management to do the job. IT security controls that exceed management's security goals also exceed granted authority. Technically, management authorizes IT security to do only what the security policy states. It is important that management include all necessary security goals in your organization's security policy. The policy provides the direction for creating controls to secure information. A strict security policy interpretation means that any control that the security policy does not address is not important to the organization.

Security Policy and Group Policy

Second, your Group Policy definition should satisfy your security policy goals and not add any arbitrary controls. Your primary goal for designing Group Policy should be to ensure your Group Policy does not leave any gaps in your security policy. The GPOs you create and implement should meet all the goals in your security policy. It shouldn't add any controls that are not covered in the policy. When your environment's Group Policy conforms to your security policy, you create a validation method of your security policy. You can record the existence and performance of GPOs as evidence that you are complying with your security policy. You'll learn how to audit how your Group Policy is functioning later in this chapter.

Making Group Policy conform to your security policy is a three-step process. First, examine a list of GPO settings that already exist in the default Windows templates. The Group Policy Settings Reference from Microsoft is an excellent resource for this task. Identify any GPO settings that satisfy parts of your security policy. Activate all settings that are appropriate for your policy.

The second step is to identify any elements in your security policy that do not already exist in default Windows templates. Then, list the elements that new GPO settings can address. For example, suppose you want to hide the Recycle Bin on every user's desktop. You can easily create a new GPO with this setting.

FIGURE 6-2
Group Policy Object order.

The third step in making Group Policy conform to your security policy is to create new GPOs for each of the remaining goals in your security policy that you identified in the second step.

Group Policy Targets

Group Policy allows you to define the specific targets for each rule. Some rules on your security policy apply to all users on all machines while others do not. For example, the rule "All users must create passwords for user accounts that conform to the strong password policy" applies to all users. The rule "Members of the Database Administrator group must change passwords at least every 90 days" applies only to users who are members of the Database Administrator user group. Windows provides you with the ability to specify GPO scope, which defines how Windows enforces security rules.

Active Directory provides the ability to define Group Policy at different levels. Windows looks up all applicable GPOs when a computer boots or a user logs on. Windows applies multiple GPOs in the following order (lower to higher) (**FIGURE 6-2**):

- **Local GPOs**—GPOs defined and stored on the local computer
- **Site GPOs defined in Active Directory (AD)**—GPOs defined in AD for a specific site
- **Domain GPOs**—Domain-wide GPOs defined in AD
- **Organizational unit GPOs**—OU GPOs defined in AD

Any setting in a higher-level GPO will override a lower-level GPO setting. For example, a setting in a domain GPO will override a conflicting setting in a local GPO. This behavior applies only if a GPO setting contains a specific value. If the higher-level GPO setting value is "Not Configured," then Windows applies the value of the lower-level GPO setting.

Creating GPOs that conform to your security policy enables you to validate and evaluate each part of the policy. You'll learn later in this chapter how to list and audit GPOs. Reporting on GPOs makes it easy to evaluate how well your organization is complying with your security policy.

Types of GPOs in the Registry

Windows stores many Group Policy settings in the **Registry**. The Registry is a database on each Windows computer that stores configuration settings for the computer and users. The Group Policy Settings Reference spreadsheet lists the key locations for settings stored in the Registry. The Registry stores Group Policy settings either in HKEY_CURRENT_USER (HKCU) or HKEY_LOCAL_MACHINE (HKLM). HKCU keys define settings that are specific to each user. HKLM keys define settings that apply to the computer, regardless of who is logged on.

Technical TIP

Recall that Microsoft publishes a handy spreadsheet that lists all of the Group Policy settings included when you install your operating system. Microsoft includes several template files with each Windows version that define many settings. You can go to *http://www.microsoft.com/downloads* and search for "Group Policy Settings Reference" to find the spreadsheet. Microsoft provides several versions of the spreadsheet to cover different Windows releases. This reference contains descriptive information you can use to create and modify GPOs to meet your organization's security needs.

Open the spreadsheet, select the "Security" tab at the bottom, and examine the "Policy Path" column to find the key for settings stored in the Windows Registry.

Technical TIP

You can open the Local Group Policy Editor using these steps:

1. Choose the Windows Start button.
2. Type gpedit.msc in the Run box.
3. Press the Enter key.

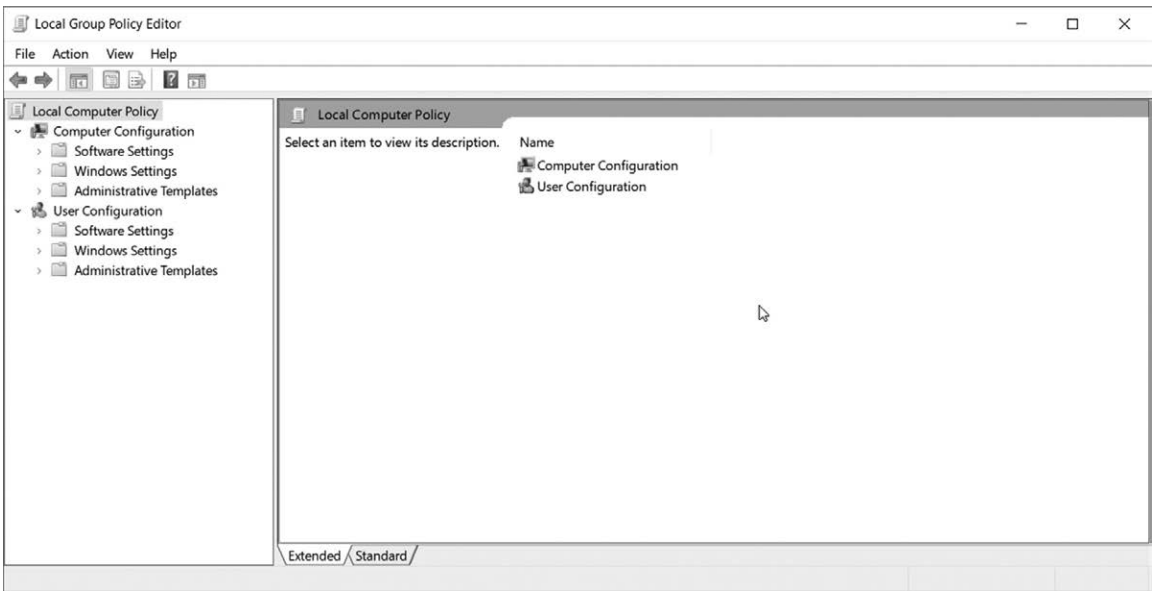
Local Group Policy Editor

It is easy to view and edit Group Policy settings with the Group Policy Editor. There are two main types of Group Policy settings: Local Group Policy settings and Active Directory Group Policy settings, which you'll learn about in the next section. You define local Group Policy settings on each computer and Windows stores the settings on that computer. All of the local Group Policy settings apply to a single computer. When you first open the **Local Group Policy Editor**, you see the two main groups of settings, "Computer Configuration" and "User Configuration" settings. **FIGURE 6-3** shows the Local Group Policy Editor.

FIGURE 6-3

Local Group Policy Editor.

Courtesy of Microsoft Corporation.



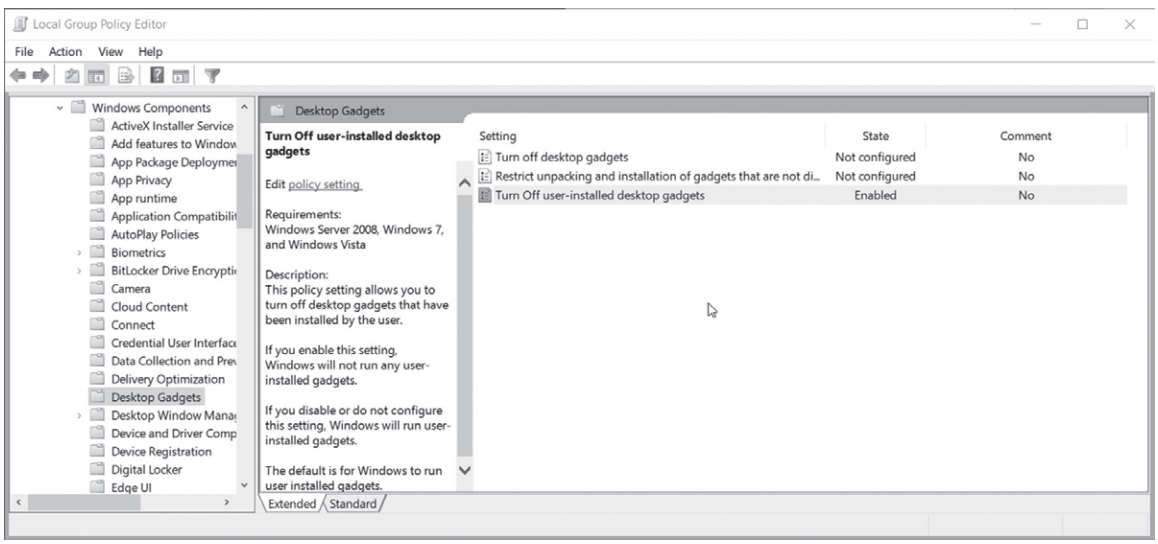
Notice the two main categories of settings in the Local Group Policy Editor. The settings under the Computer Configuration category are stored in the Registry under the HKLM entry. The settings under the User Configuration category are stored under the HKCU entry. Although the Windows Registry Editor can be used to modify Group Policy settings, the Local Group Policy Editor is easier and safer. The Local Group Policy Editor allows you to change only Group Policy settings and ensures the settings are stored properly and in the correct location in the Registry. Changing Group Policy settings in the Local Group Policy

Technical TIP

You can follow these steps to change the same setting you see in Figure 6-4.

1. In the Local Group Policy Editor, expand the Computer Configuration, Administrative Templates, and Windows Components items.
2. Select Desktop Gadgets.
3. On the right side of the window, select Turn Off User-Installed Desktop Gadgets.
4. Right-click to open the context menu and select Edit.
5. Choose the Enabled option button to enable the setting.
6. Choose OK to save the setting and close the Setting Editor dialog box.

FIGURE 6-4
Changing a setting in the Local Group Policy Editor.
Courtesy of Microsoft Corporation.



Editor is easy. Find the setting you want to change, choose Edit, and change the setting to the value you choose. **FIGURE 6-4** shows the modified value for the Turn Off user-installed desktop gadgets setting. When you enable this setting, users will not be able to launch any of their own user-installed gadgets in the sidebar of their desktop.

GPOs in the Registry Editor

Since Group Policy settings are stored in the Registry, they can be edited directly using the **Registry Editor**. Windows stores all currently active GPOs in the Registry under the HKCU entry. When a user logs on, and every 90–120 minutes thereafter, Windows will update the HKCU hive with the most current GPOs that apply to the current user. This updater will also occur within 10 minutes if a Windows Server computer refreshes GPOs with the Remote Group Policy Update. Each GPO has a globally unique identifier (GUID) that uniquely identifies it as a Windows object. The GPO GUID is the key Windows uses to store the GPO in the Registry. Windows stores current GPOs under the key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\. **FIGURE 6-5** shows the GPO setting for "Turn Off User-Installed Desktop Gadgets" from the previous example in the Registry Editor.

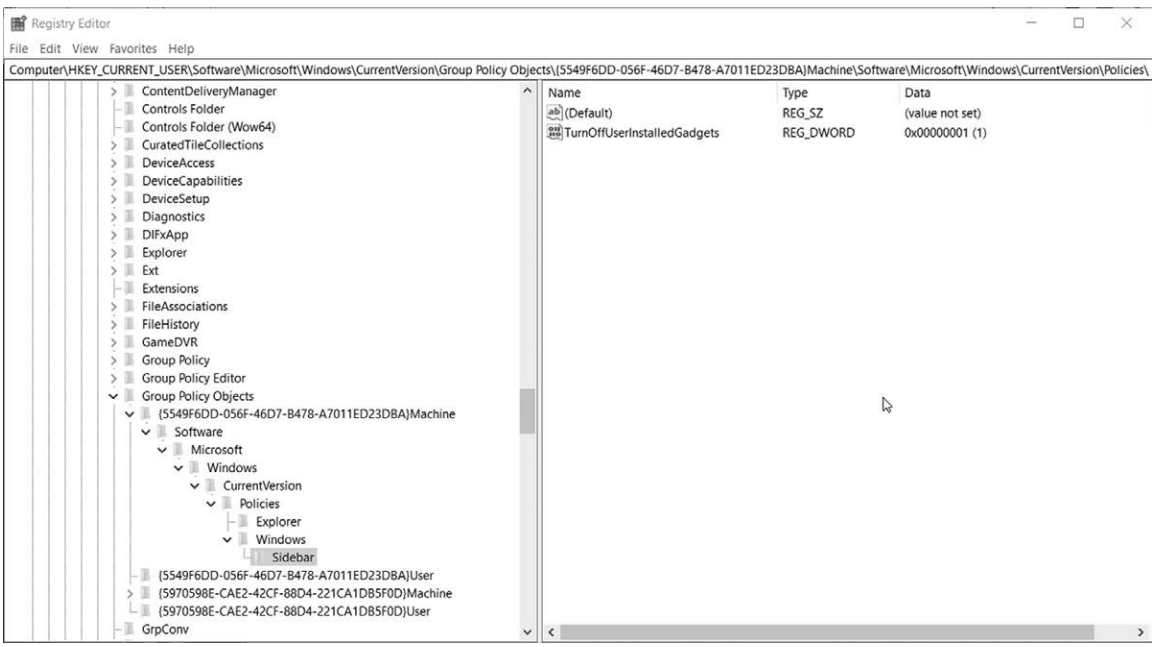
⚠ WARNING

Be very careful when using the Registry Editor. Changing the wrong Registry data in the Registry Editor can make your computer unstable. When another editor is available to edit data, such as the Local Group Policy Editor, use it instead of the Registry Editor.

FIGURE 6-5

Group Policy setting in the Registry Editor.

Courtesy of Microsoft Corporation.



Technical TIP

You can follow these steps to view the same setting you see in Figure 6-5.

1. Select the Windows Start button.
2. Type regedit.exe in the Run box; then, press the Enter key to run the Registry Editor.
3. Select Edit > Find from the menu bar.
4. Type Turn Off User-Installed Gadgets; then, choose Find Next.
5. Examine the full path to the GPO setting in the status area at the bottom of the Registry Editor window.

   If you don't see a path in the status bar, choose View > Status Bar from the menu bar.

Types of GPOs in Active Directory

Although defining local GPOs provides positive control over single computers, the real power of Group Policy is in AD. Defining GPOs in AD gives you the ability to centralize security rules and control how Windows applies each rule. You create AD GPOs on a domain controller. Windows stores GPOs in AD in such a way that the domain controller

automatically replicates the GPOs to other domain controllers. This feature reduces the workload of administrators. Using Group Policy in AD relieves the need to define security rules on multiple computers one at a time.

Group Policy Management Console

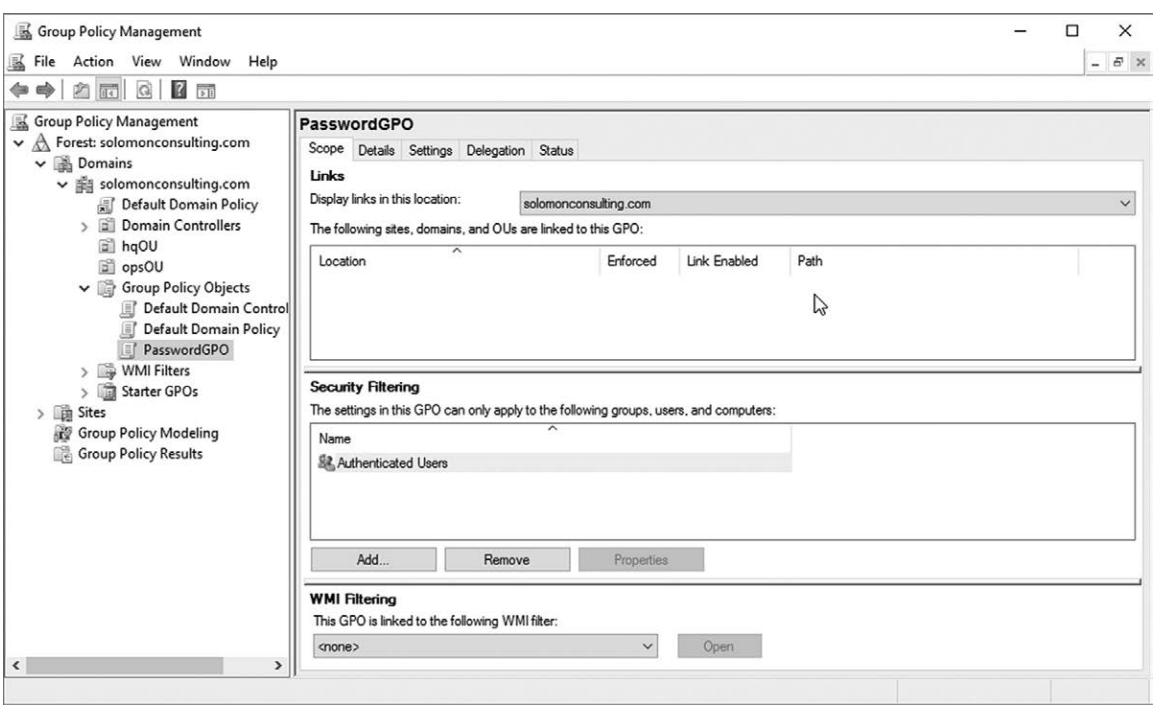
AD GPOs are created on the domain controller using the **Group Policy Management Console (GPMC)** (FIGURE 6-6). Note that the GPMC is only available on domain controllers. The GPMC looks a lot like the Local Group Policy Editor, but it allows you to do far more than just create GPOs and maintain their settings. Here is a list of some of the actions you can perform in the GPMC:

- Create and edit GPOs.
- Import and export GPOs.
- Copy and paste GPOs.
- Back up and restore GPOs.
- Search for GPOs.
- Create reports on GPOs.

FIGURE 6-6

Group Policy Management Console.

Courtesy of Microsoft Corporation.



Although there are multiple ways to create GPOs, the most common method is to create GPOs under the desired domain in the GPMC. New AD GPOs don't actually do anything until you link them with some entity. You'll learn about GPO linking later in this chapter.

Technical TIP

When you promote a server to a domain controller, Windows automatically installs the GPMC on that server. You can follow these steps to open the GPMC:

1. Choose the Windows Start button.
2. Select Windows Administrative Tools > Group Policy Management.

You can also follow these steps to open the GPMC:

3. Choose the Windows Start button.
4. Type gpmc.msc in the Run box.
5. Press the Enter key.

GPOs on the Domain Controller

Windows stores AD GPOs in a folder on the domain controller. Computers that are in a domain retrieve all the GPOs that apply to that computer when a user logs on using a domain account or when a computer connects to the domain. The domain controller searches for the appropriate GPOs and sends them to the computer. Of course, the computer and user must first successfully authenticate to the domain controller. Then, every 90–120 minutes the remote computer asks the domain controller if any GPOs have changed. If they have, the domain controller sends the new or updated GPOs and the remote computer applies them.

WARNING

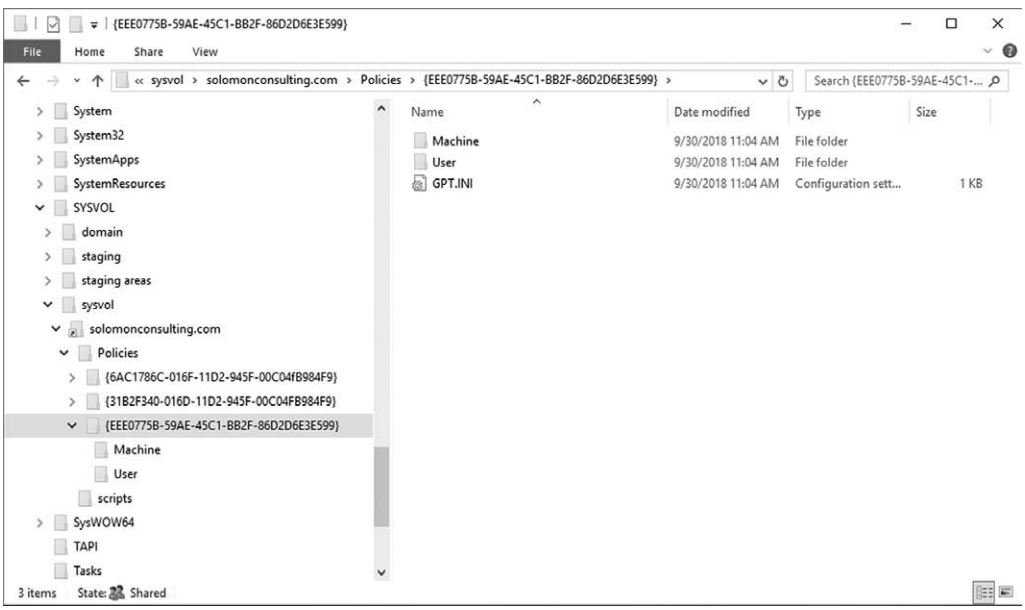
If you installed Windows in a directory other than C:\Windows, then the path to Policies for your computer will be different. Just replace C:\Windows with your Windows install folder to get the correct path to the Policies folder.

The domain controller stores AD GPOs in a folder named Policies (**FIGURE 6-7**). Windows creates a Policies folder for each domain. For example, the full pathname for the Policies folder for a domain named corp.domain.com is: C:\Windows\sysvol\sysvol\corp.domain.com\Policies.

Windows stores each GPO in a subfolder under Policies. The name of each subfolder under Policies is the GUID for the GPO. You can navigate to the GPO in Windows Explorer to see where Windows stores the GPO settings. Each GPO folder, or GPO shell, contains two subfolders named Machine and User. These subfolders contain the GPO settings for both the machine-wide and user-specific settings. Each subfolder contains policy files for defined GPOs that apply to a domain.

Unlike Local GPOs, AD GPOs do nothing until you link them to one or more **containers**. An AD container can be a site, a domain, or an OU. The Group Policy Objects section of the GPMC lists all defined GPOs. You can edit existing GPOs or add new GPOs. You must link GPOs to one or more sites, domains, or OUs to make the GPOs do anything (**FIGURE 6-8** and **6-8A**). A single GPO may be linked to multiple containers, and each container can have

FIGURE 6-7
GPOs in the Policies folder.
Courtesy of Microsoft Corporation.



Technical TIP

Follow these steps to link a GPO to a container:

1. In the GPMC, select a container. For example, select the OU named hqOU.
2. Open the context menu for hqOU by right-clicking on hqOU.
3. Choose Link an Existing GPO.
4. Select the desired GPO from the list of defined GPOs.
5. Choose OK.

multiple GPOs linked to it. The easiest way to link GPOs to containers is from the context menu of the container.

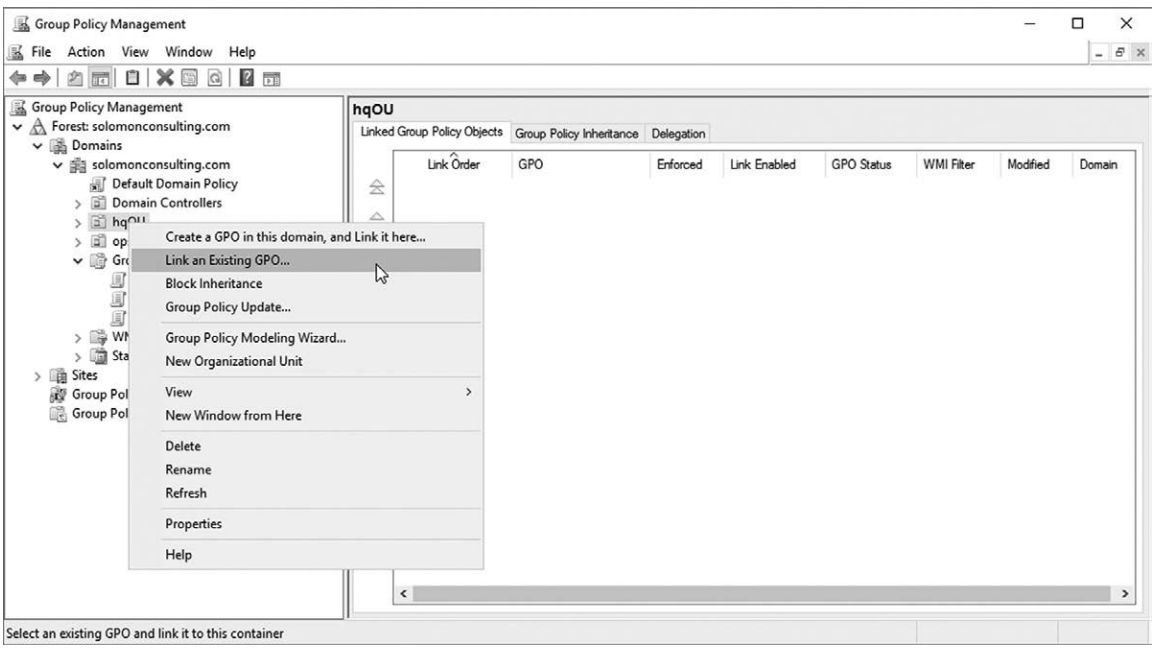
Designing, Deploying, and Tracking Group Policy Controls

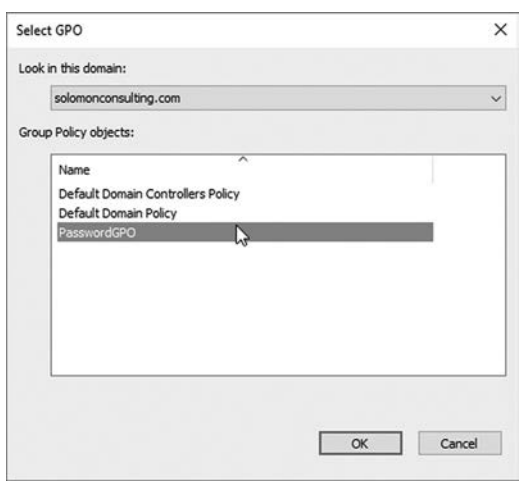
One of the most important considerations when designing GPOs is efficiency. You want to define and link the minimum number of GPOs to satisfy your security policy. Creating too many GPOs will increase the time and effort you'll need to administer and maintain your security policy. Having too many GPOs also increases the possibility of errors and

FIGURE 6-8

Linking AD GPOs in the GPMC.

Courtesy of Microsoft Corporation.





opportunities for attackers to compromise your systems. The simplest environment would be one in which you define one set of GPOs that applies to all computers and all users in all domains. Unfortunately, few environments end up being that simple. Functional demands often require different controls for various computers and users.

GPO Application Order

You can define several layers of GPOs that work together to ensure you enforce your security policy for all computers and all users. Windows gives you the ability to create high-level GPOs that enforce large-scale security settings and more specific GPOs that allow you to fine-tune settings for specific situations. Recall from earlier in this chapter that Windows applies GPOs in a specific order. Knowing this order lets you put more generic settings in GPOs that Windows applies first, and more specific settings in GPOs that Windows applies later in the process.

Recall that Windows applies GPOs in this order:

- **Local GPOs**—GPOs defined and stored on the local computer
- **Site GPOs defined in AD**—GPOs defined in AD for a specific site
- **Domain GPOs**—Domain-wide GPOs defined in AD
- **Organizational unit GPOs**—OU GPOs defined in AD

WARNING

OU GPO settings will override any settings that exist in lower-level GPOs. For example, if a setting exists in both a site GPO and an OU GPO, the OU GPO setting will override the site GPO setting. Don't include settings in OU GPOs that may require local overrides.

Design your GPOs with this order in mind. Since Windows applies OU GPOs last, any global GPO settings should go here. Identify any settings you want to enforce for all computers and users and define GPOs that you link to one or more OUs. Then, you can define GPOs and link them to lower-level containers for settings that do not apply to all computers or users. Since OU GPOs have the largest scope, they are the easiest to implement and maintain. Start by reviewing your OU structure. You should ensure your OU structure realistically represents your functional organizational structure as closely as possible. OU designs that closely represent functional structures make it easier to create appropriate OU-level GPOs that satisfy your security policy. For example, suppose your security policy requires specific application and object access for members of the Human Resources (HR) Department. If you define all users in the HR Department in the HR OU, it is easy to create GPOs for the OU that affect all HR Department users.

All security control design starts with your security policy. Once you validate your OU design and identify the controls you'll need to satisfy your security policy, you can define the control scope. In the context of GPO settings, the scope of any control is the group of computers or users to which each GPO applies. Settings scoped to the OU level should exist in OU GPOs. You can define any settings that apply only to some computers or users in local, site, or domain GPOs. You can also define limited scope GPOs at the OU level and use filters to limit the scope. You'll learn about GPO filters later in this chapter. As a general rule, define GPO settings either at the lowest level that includes all of the desired computers and users or at the OU level using filters when the OU approach meets your needs. For example, you can define any settings that apply to all users for a specific computer in either a local GPO, site GPO, or a filtered OU GPO. The main difference is that Windows stores local GPOs on the affected computer and stores site and OU GPOs in AD. OU GPOs also make administration simpler since you define and link GPOs at a single level.

Security Filters

Windows applies GPOs to all computers and users in a container by default. That means all computers and users in an OU will inherit any OU GPOs defined for that OU by default. You

WARNING

The GPMC creates new GPOs that apply to all authenticated users. If you create filters to limit the scope of a GPO, make sure you delete the default filter of "Authenticated Users."

can change that behavior with **security filters** (FIGURE 6-9) if you want an OU GPO to apply only to some computers or users in the OU. The GPMC allows you to add as many security filters for GPOs as necessary to satisfy your security policy. You can limit a GPO to users, groups, or computers. Once you define a security filter, Windows will apply that GPO only to subjects defined in the filter. This option gives you much more control over how Windows applies GPOs you define at the OU level.

Technical TIP

Follow these steps to define a security filter for an OU GPO:

1. In the GPMC, select and expand a domain.
2. Expand Group Policy Objects and select a GPO.
3. Select the Scope tab in the right panel and then select Add in the Security Filtering section.
4. You have the option to change the type of objects and the location Windows uses to build the filter options. The defaults will allow you to select Users, Groups, or Built-In Security Principles from the domain you selected in Step 1. You can select the Object Types button and select the Computers check box to define a filter for specific computers.
5. Enter the user, group, or computer name for this filter. Choose Check Names to validate the object name you entered.
6. Choose OK to create the new filter and return to the GPMC.

GPO Windows Management Instrumentation Filters

Windows Management Instrumentation (WMI) is the infrastructure Windows uses to maintain and exchange management and operations data. **WMI filters** give you even more control over when and where GPOs apply. You can create multiple WMI filters for each domain and then, link each filter to one or more GPOs. You can link only one WMI filter to each GPO. Windows evaluates the GPO's WMI filter before applying a GPO and proceeds only if the WMI filter expression evaluates to TRUE. WMI filters allow you to query the target environment and apply security settings only in certain situations.

For example, suppose you want to apply a GPO only for computers that are running Microsoft Windows Vista Ultimate. You could define a WMI filter that would restrict the GPO to the desired machines. Windows uses the **WMI Query Language (WQL)** to define the queries for the filters. WQL is a subset of the SQL language many database engines use to query data. The following WQL query will return TRUE when the target computer is running Microsoft Windows 8.1 Pro:

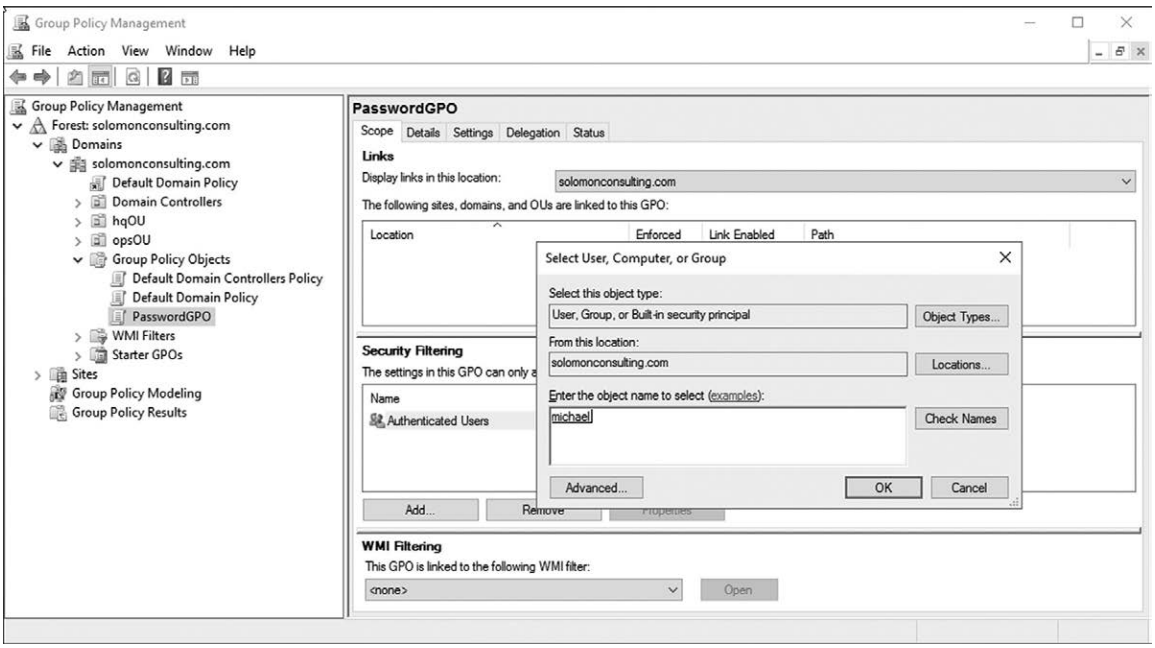
Select * from Win32_OperatingSystem where Caption = Microsoft Windows 8.1 Pro.

If the target computer is running Microsoft Windows 8.1 Pro, Windows will apply the GPO. This additional feature gives administrators the ability to define GPO scope at a very

FIGURE 6-9

GPO security filters.

Courtesy of Microsoft Corporation.



Technical TIP

You can find more information on WQL on Microsoft TechNet at: *http://technet.microsoft.com/en-us/library/ee176998.aspx*.

specific level of detail. Once you define the WMI filter in the GPMC, you can link the filter to any GPO by just selecting the desired WMI filter from the drop-down list in the GPO's WMI Filtering section (**FIGURE 6-10**).

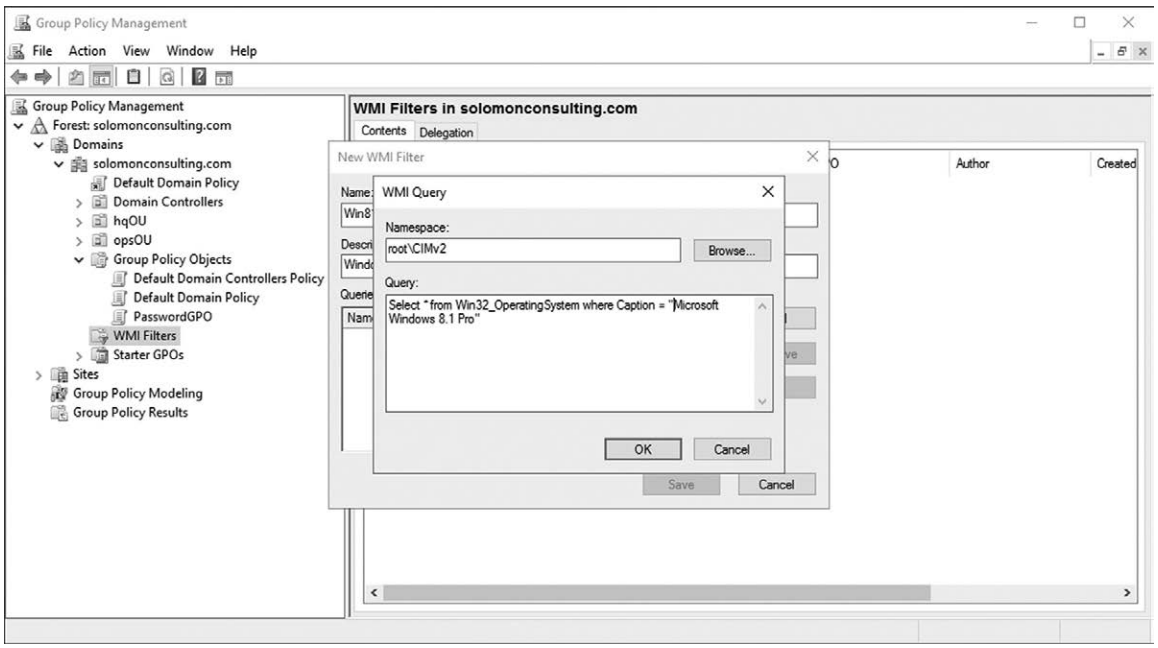
Deploying Group Policy

Windows ensures that new and changed GPOs get distributed and applied every 90–120 minutes. In some cases, you may want to force GPO distribution. In Windows Server 2012 and newer, you can force a GPO refresh from within the GPMC. For all versions of Windows, you can use the **Group Policy Update tool** to accomplish this task. The tool also provides the ability to force user logoff or system boot when setting changes require these actions. You can use the Group Policy Update tool whenever you want to ensure that settings are in place on target computers.

FIGURE 6-10

WMI filters.

Courtesy of Microsoft Corporation.



Technical TIP

Follow these steps to define a WMI filter and link it to an existing GPO:

1. In the GPMC, select and expand a domain.
2. Expand WMI Filters, open the context menu and choose New.
3. Type the desired name and description, then choose Add.
4. Type the following text into the query editor: * from Win32_OperatingSystem where Caption = "Microsoft Windows 8.1 Pro."
5. Choose OK; then, Save to create the new WMI filter and return to the GPMC.
6. Expand Group Policy Objects and select a GPO.
7. Open the drop-down list in the WMI Filters section and select the newly created WMI filter.

Follow these steps to run the Group Policy Update tool:

1. Open a PowerShell window—Choose the Windows Start button > type **powershell.exe**.
2. Enter the following command: gpupdate.exe.

The Group Policy Update tool supports several options that change the scope of targets or additional actions. **TABLE 6-2** lists the most common options for gpupdate.exe.

TABLE 6-2 Gpupdate.exe Options

OPTION	DESCRIPTION
/target:{Computer | User}	Limits the target of the update to only user or computer policy settings.
/force	Reapplies all settings. The default is to apply only new or changed settings.
/wait:value	Sets wait time for the specified number of seconds for the processing to finish. A value of –1 means wait forever.
/logoff	Forces a user logoff after the update processing completes.
/boot	Forces a system reboot after the update processing completes.
/sync	Synchronously applies the next logoff or boot policy setting.

Auditing and Managing Group Policy

Once you design and deploy GPOs to support your security policy, it is important to validate your Group Policy to ensure that you have defined the right GPOs. Auditing Group Policy ensures the GPOs you have in place satisfy your security policy. As you change users and computers in your organization, you may find that your GPOs no longer satisfy your security policy. It is important to audit Group Policy periodically to ensure that any changes in your organization have not reduced your GPO's effectiveness.

Microsoft provides two main tools you will use to audit Group Policy: Group Policy Inventory and Resultant Set of Policy tool. The first tool, Group Policy Inventory, provides an inventory list of GPOs and many other computer and user settings. You must download this program from Microsoft's website and install it on your computer—it isn't included when you install Windows. The second tool is included with Windows. The Resultant Set of Policy tool shows what settings Windows applies to a specific user on a specific computer.

Group Policy Inventory

The first step in using the **Group Policy Inventory tool** (gpinventory.exe) is to download and install it on your computer. You can get the tool from Microsoft's website. Gpinventory queries the computers you select for system and GPO information and then displays the results in a single window. This tool makes it easy to collect information from many computers across a domain to ensure that your Group Policy is deploying the way that you expect. Follow these steps to run Gpinventory:

> **NOTE**
>
> Windows Server 2012 added a new tab to the GPMC. The new Status tab shows the current replication status of the selected GPO. This option makes it easier to see the deployment status of your GPOs.

1. **Open a PowerShell window**—Choose the Windows Start button > type powershell.exe.
2. **Change directories to the install directory for the Gpinventory tool**—Enter: cd C:\program files (x86)\Windows Resource Kits\Tools.
3. **Run Gpinventory**—The command is gpinventory.exe.
4. **Choose the computers to query**—Query > Select Computers to Target using Active Directory.

5. **Choose the information you want to gather**—Query > Select Information to Gather.
6. **Execute the query**—Query > Run Query.

Technical TIP

You must download and install the Group Policy Inventory tool before you can use it. You can get the tool from the Microsoft website. Go to: *http://www.microsoft.com/en-us/download/details.aspx?id=14126* to download the tool.

After Group Policy Inventory gathers the information you requested, it displays the results in the main window. You can view the details and save the information to analyze later. The Group Policy Inventory tool will save the results in an XML file or a text file. Use the Results menu item to save the results in either format. Group Policy Inventory is an important tool to provide validation of Group Policy in your domain. Use it after any GPO change and periodically to ensure computers and users are operating with the settings you define to comply with your security policy.

Analyzing the Effect of GPOs

The other common tool you will use to audit GPOs is the **Resultant Set of Policy (RSOP) tool**. The RSOP tool is included in Windows and shows the specific settings that will result from applying GPOs to a specific user logged on to a specific computer. The Group Policy Inventory tool can include some RSOP results, but the stand-alone RSOP tool provides access to more details. RSOP is a great way to analyze the effect of any GPO changes. RSOP provides two modes of operations—logging mode to show existing GPOs and planning mode that shows the effect of planned GPO changes.

You can run RSOP using two methods. The first method runs RSOP in logging mode that defaults to the currently logged-on user on the current computer. After the initial information displays, you can easily change the user or computer and generate updated GPO information. Follow these steps to run RSOP in logging mode:

1. Choose the Windows Start button.
2. Type rsop.msc in the Run box, and then, press Enter.
3. The Resultant Set of Policy window displays the current settings for the user who is currently logged on. The display looks like the GPMC, but you can't change any settings here.
4. If you want to run RSOP for another user or computer, open the context menu (by right-clicking) on the main item in the left panel. This item will be your username and computer name.
5. On the context menu, select Change Query.
6. Select the desired computer and user on the next two dialog boxes.
7. RSOP will calculate the effective settings using the new user and computer you provided.

RSOP also runs in a powerful planning mode. The planning mode is useful when you want to analyze the effects of a GPO change before deploying the change. Follow these steps to run RSOP in planning mode:

1. Choose the Windows Start button > Windows Administrative Tools > Active Directory Users and Computers.
2. Open the context menu of the desired object by right-clicking the desired computer, user, domain, or OU.
3. Select All Tasks > Resultant Set of Policy (Planning).
4. The next several screens ask you to provide information that describes the planned target environment. RSOP will evaluate the GPOs based on the information you provide here. You can provide the following information:
   a. **User and Container**—Run RSOP for any user for any container.
   b. **Advanced options**—Set advanced simulation conditions.
   c. **Groups**—Analyze the effects of adding or removing group assignments.
   d. **WMI Filters**—See what effects different WMI filters produce.

Group Policy Inventory and RSOP help you validate the Group Policy you have in place and evaluate how changes will affect your environment. Both tools are important components of a complete administrator's toolbox.

Best Practices for Microsoft Windows Group Policy and Processes

Group Policy is an important component of secure Windows environments. Many resources are available to help you follow established best practices for secure systems. You'll learn about a few of the recommended guidelines and available resources in this section.

Group Policy Design Guidelines

While there are many ways to design Group Policy for your organization, a few guidelines can help focus your efforts. Follow these guidelines to design a Group Policy that will minimize administrative effort while satisfying your security policy. Most important, don't make your Group Policy overly complex. Simplicity is always an asset in any policy. Keep your security policy and Group Policy as simple as possible while still fulfilling your goals. Here are a few additional guidelines that should result in simple and effective Group Policy:

- Define OUs that reflect your organization's functional structure.
- Create OU GPOs for controls required in your security policy.
- Use meaningful names for GPOs to make maintenance and administration easier.
- Deploy GPOs in a test environment before deploying to your live environment.
- Use security filtering and WMI filters to restrict settings when necessary.
- Back up your GPOs regularly.
- Do not modify the default policies—instead, create new GPOs.

Ensure your Group Policy is both effective and easily maintainable. Only define and deploy the GPOs you actually need to meet the goals of your security policy. Extra GPOs will only complicate administrative tasks and may get in the way of completing primary business functions. The process of migrating from an environment with few controls to a secure

environment can be frustrating both for end users and administrators. Make sure you test all GPOs before deploying them to a live environment. Conduct tests that will allow you to evaluate how each GPO will affect your users' abilities to do their jobs. New security settings that stop people from doing their jobs are harmful to your business. Be aware of any new policies that may result in a negative business impact. When security requirements conflict with business requirements, it is up to the organization's management to resolve the conflict. The best security solutions always support both security and business concerns.

There are several other resources listed in **TABLE 6-3** that make designing and implementing Group Policy across a domain easier. Use these resources as well as the tools and resources you have already seen. They keep you from reinventing the wheel. They also provide input on solving issues that you may not have encountered yet.

TABLE 6-3 Group Policy Best Practices Resources

RESOURCE	DESCRIPTION	WHERE TO FIND IT
Group Policy Best Practices Analyzer	Helps you identify Group Policy configuration errors or dependency issues that may prevent settings from functioning as you expected.	In Server Manager, select a server role group and select Start BPA Scan in the Best Practices Analyzer.
Group Policy Settings Reference	Spreadsheets that list the policy settings included in the Administrative template files that are delivered with the Windows operating systems.	*http://www.microsoft.com /downloads* (Search for Group Policy Settings Reference)
Windows 8.1 and Windows Server 2012 R2 Security Baseline	Resources for planning, deploying, and monitoring the security baselines of servers running Windows 8.1 and Windows Server 2012 R2.	*https://blogs.technet.microsoft .com/secguide/2014/04/07 /security-baselines-for -windows-8-1-windows-server -2012-r2-and-internet-explorer -11-beta/*
Windows 10 and Windows Server 2016 Security Baseline	Resources for planning, deploying, and monitoring the security baselines of servers running Windows 10 and Windows Server 2016.	*https://docs.microsoft.com /en-us/windows /security/threat-protection /windows-security-baselines*
Windows 10 v1809 and Windows Server 2019 Security Baseline	Resources for planning, deploying, and monitoring the security baselines of servers running Windows 10 v1809 and Windows Server 2019.	*https://blogs.technet.microsoft .com/secguide/2018/11/20 /security-baseline-final-for -windows-10-v1809-and -windows=-server-2019/*
Security Compliance Toolkit (SCT)	A set of tools used to acquire, test, and deploy configuration baselines recommended by Microsoft. The security guides in the toolkit recommend Group Policy configurations and Security Template configurations that are enforced via Active Directory Domain Services.	*https://docs.microsoft.com /en-us/windows /security /threat-protection /security-compliance-toolkit-10*

CHAPTER SUMMARY

Group Policy is one of the most important security and administrative features in Windows. It enables administrators to effectively implement a security policy across a network of computers. Group Policy and Active Directory provide a centrally controlled environment to define and deploy changes to security and other configuration settings. Although Group Policy is most often discussed in security contexts, it is an efficient way to enforce standard settings across a diverse environment. You can use Group Policy to enforce password aging settings and a default screen saver. Group Policy uses are nearly endless. A good Group Policy design can reduce the workload of administrators and greatly enhance their abilities to enforce organizational standards in a consistent manner.

KEY CONCEPTS AND TERMS

Container
Group Policy
Group Policy Inventory tool
Group Policy Management Console (GPMC)
Group Policy Object (GPO)
Group Policy Update tool
Local Group Policy Editor
Organizational unit (OU)
Registry
Registry Editor
Resultant Set of Policy (RSOP) tool
Security filter
Windows Management Instrumentation (WMI)
WMI filter
WMI Query Language (WQL)

CHAPTER 6 ASSESSMENT

1. The Windows Group Policy feature provides a centralized set of rules that govern the way Windows operates.

A. True
B. False

2. Windows checks for new or updates GPOs every _____ minutes.

3. Which of the following statements best describes the relationship between security policy and Group Policy?

A. Security policy should implement Group Policy.
B. Security policy is derived from Group Policy.
C. Group Policy should implement security policy.
D. Group Policy supersedes security policy.

4. Who holds the primary responsibility to ensure the security of an organization's information?

A. IT security
B. Management
C. Information system users
D. Human Resources

5. Which tool would you most likely use to edit Group Policy settings in a stand-alone computer?

A. Local Group Policy Editor
B. Registry Editor
C. Group Policy Management Console
D. Resultant Set of Policy Editor

6. You can only edit user-specific Group Policy settings in the Windows Registry Editor.

A. True
B. False

7. Defining GPOs in _____ gives you the ability to centralize security rules and control how Windows applies each rule.

8. Which folder does Windows use to store AD GPOs on the domain controller?

   A. Windows
   B. Policies
   C. GPO
   D. ADdata

9. Windows stores each GPO in a subfolder with the same name as the _____ of the GPO.

10. Which of the following features allows you to restrict the groups to which a GPO applies?

    A. Security filter
    B. WMI filter
    C. GPO link
    D. OU list

11. Which of the following features allows you to restrict the types of operating systems to which a GPO applies?

    A. Security filter
    B. WMI filter
    C. GPO link
    D. OU list

12. Windows will automatically cause a user logoff or system reboot after applying new or changed GPOs.

    A. True
    B. False

13. Which of the following tools lists information about deployed GPOs and other computer specific attributes?

    A. Gpupdate.exe
    B. RSOP
    C. Gpedit.msc
    D. Gpinventory.exe

14. You can use the _____ tool to view the effective settings after all current GPOs are applied to a specific user.

15. Which of the following resources is installed with Windows?

    A. Group Policy Settings Reference
    B. Security Compliance Management Toolkit
    C. Group Policy Best Practices Analyzer
    D. GPOAccelerator