Chapter 9

Managing Security

Windows 7 offers a wide variety of security options. If the Windows 7 computer is part of a domain, you can apply security through a Group Policy Object using the Group Policy Management Console. If the Windows 7 computer is not part of a domain, you use Local Group Policy Objects to manage local security.

In the first part of this chapter, you will learn about the different Windows 7 environments and the utilities that you can use to manage security.

You can use policies to help manage user accounts. Account policies control the logon environment for the computer, such as password and logon restrictions. Local policies specify what users can do after they log on and include auditing, user rights, and security options. You can also manage critical security features through the Windows Security Center.

We continue the chapter with NTFS security and shared permissions and how they work independently and how they work together.

In this chapter, you'll learn how to:

- Understand Local Group Policy Objects
- Understand User Account Control (UAC)
- Configure NTFS security
- Manage shared permissions

Managing Security Configurations

The tools you use to manage Windows 7 computer security configurations depend on whether the Windows 7 computer is part of a Windows 2000, Windows 2003, or Windows 2008 domain environment.

If the Windows 7 client is not part of a domain, you apply security settings through Local Group Policy Objects (LGPOs). LGPOs are a set of security configuration settings that are applied to users and computers. LGPOs are created and stored on the Windows 7 computer.

If your Windows 7 computer is part of a domain, which uses the services of Active Directory, you typically manage and configure security through Group Policy Objects (GPOs). Active Directory is the database that contains all your domain user and group accounts together with all other domain objects.

GPOs are policies that can be placed on either users or computers in the domain. The Group Policy Management Console (GPMC) is a Microsoft Management Console (MMC) snap-in that is used to configure and manage GPOs for users and computers via Active Directory.

Windows 7 computers that are part of a domain still have LGPOs, and you can use LGPOs in conjunction with the Active Directory group policies.

> **GROUP POLICY OBJECTS**
>
> Use of GPOs is covered in detail in *MCTS: Windows Server 2008 Active Directory Configuration*, by William Panek and James Chellis (Sybex, 2008).

The settings you can apply through the Group Policy Management Console (GPMC) utility are more comprehensive than the settings you can apply through LGPOs.

By default, LGPOs are stored in `%systemroot% System32\GroupPolicyUsers`. Table 9.1 lists some of the options that you can set for GPOs within Active Directory and which of those options you can apply through LGPOs.

TABLE 9.1: Group Policy and LGPO Setting Options

GROUP POLICY SETTING	AVAILABLE FOR LGPO?
Software Installation	No
Remote Installation Services	Yes
Scripts	Yes
Printers	Yes
Security Settings	Yes
Policy-Based QOS	Yes
Administrative Templates	Yes
Folder Redirection	No
Internet Explorer Configuration	Yes

In the next section, we look at how GPOs work within an Active Directory domain.

Understanding Group Policy Objects and Active Directory

Most Windows 7 computers reside within a Windows Server 2000, Windows Server 2003, or Windows Server 2008 domain. GPOs are applied through Active Directory by using the Group Policy Management Console (GPMC). It is much easier to globally manage GPOs through the GPMC than applying LGPOs at local levels of each Windows 7 machine.

To help you understand how GPOs and LGPOs work together, the following sections first provide an overview of Active Directory and then show you how GPOs and LGPOs are applied based on predefined inheritance rules.

Active Directory Overview

First, the easiest way to explain Active Directory is to state that Active Directory is a database. That's it. Active Directory is just a database — but it's the most important database in your domain because the Active Directory database contains all your usernames and passwords, groups, and other objects within the domain.

Within that Active Directory database, you have several levels of a hierarchical structure. A typical structure consists of domains and Organizational Units (OUs). Other levels exist within Active Directory, but this overview focuses on domains and OUs in the context of using GPOs.

The domain (for example, Panek.com) is the main unit of organization within Active Directory, as shown in Figure 9.1. Within a domain are many domain objects, including security objects such as user and group accounts. Each domain security object can then have permissions applied that specify what rights that security object can have when it accesses resources within the domain.

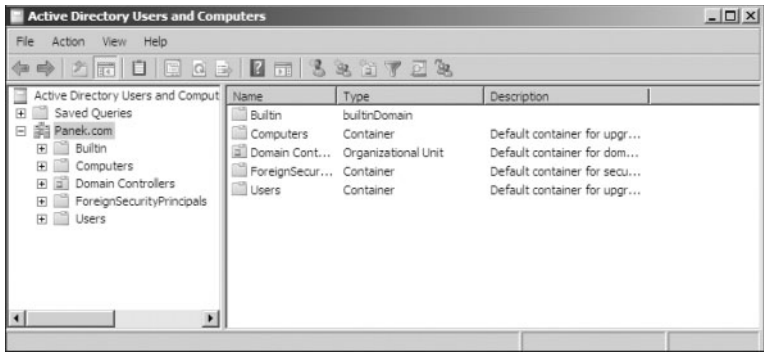


FIGURE 9.1
Active Directory hierarchical structure

Within a domain, you can further subdivide and organize domain objects through the use of Organizational Units (OUs). This is one of the key differences between Windows NT 4 domains and Windows 2000, 2003, and 2008 domains. The NT domains were not able to store information hierarchically. Windows 2000, 2003, and 2008 domains, through the use of OUs, allow you to store objects hierarchically, typically based on function or geography.

For example, assume that your company is called Stellacon. You have locations in New York, San Jose, and Belfast. You might create a domain called Stellacon.Com with OUs called NY, SJ, and Belfast. In a large corporation, you might also organize the OUs based on function. For example, the domain could be Stellacon.Com and the OUs might be Sales, Accounting, and R&D. Based on the size and security needs of your organization, you might also have OUs nested within OUs. As a general rule, however, you want to keep your Active Directory structure as simple as possible.

Domains are logical grouping of objects. If we had the Stellacon.com domain, we would expect that everyone in the domain would belong to the company named Stellacon.

A domain does not have to be in one geographical location. Microsoft is a worldwide company and the Microsoft.com domain has locations all over the world.

If you need to set up physical locations, you would set up *sites*. Sites are physical representations of the domain. For example, let's say that we have a company with two buildings next to each other. You might want all the users in one building to access resources within that building and the same for the other building.

You can set up two sites, one for each building. Then users will always try to find resources in their own site first. If the resource in the site is not available, the user will automatically leave the site and try to find the resource in another site. Sites are an excellent way to keep your users local to their location.

SITES

Usage of sites is covered in detail in *MCTS: Windows Server 2008 Active Directory Configuration*, by William Panek and James Chellis (Sybex, 2008).

Now we'll explain how GPO inheritance works and what happens when multiple GPOs conflict with each other.

Understanding GPO Inheritance

When GPOs are created within Active Directory using the GPMC, there is a specific order of inheritance. That is, the policies are applied in a specific order within the hierarchical structure of Active Directory. When a user logs onto Active Directory, depending on where within the hierarchy GPOs have been applied, the order of application is as follows:

1. Local
2. Site
3. Domain
4. OU

Each level of the hierarchy is called a container. Containers higher in the hierarchy are called parent containers; containers lower in the hierarchy are called child containers. Settings from these containers are inherited from parent container to child container. By default, child container policy settings override any conflicting settings applied by parent containers.

For example, if you set the wallpaper at the site level to be red and set the wallpaper at the OU level to be blue, if a user who belongs to both the site and the OU logs on, their wallpaper would be blue.

The local policy is, by default, applied first when a user logs on. Then the site policies are applied, and if the site policy contains settings that the local policy doesn't have, they are added to the local policy. If any conflicts exist, the site policy overrides the local policy. Then the domain policies are defined.

Again, if the domain policy contains additional settings, they are incorporated. The domain policy overrides the site policy or the local policy when settings conflict. Finally, the OU policies are applied. Any additional settings are incorporated; for conflicts, the OU policy overrides the domain, site, and local policies. If any child OUs exist, their GPOs are applied after the parent OU GPOs.

So as we have just stated, the child policy overrides the parent policy by default, but this can be changed. As with any child/parent relationship, the parent can force the child to accept the policy that is being issued. The Enforce option allows you to override a child option. There is also the ability to block inheritance. Let's look at these two options:

Enforce (No Override) The Enforce option is used to specify that child containers can't override the policy settings of higher-level containers. For example, if a site policy is marked as

Enforce, it will not be overridden by conflicting domain or OU policies. If multiple Enforced policies are set, the one from the highest container would take precedence.

The Enforce option would be used if you wanted to set corporate-wide policies without allowing administrators of lower-level containers to override your settings. This option can be set per container, as needed.

The Enforce option used to be known as the No Override option. When you created a GPO in Active Directory Users and Computers, this option was called No Override. Now that we use the Group Policy Management Console (GPMC), it's called Enforce.

Block Inheritance The Block Inheritance option is used to allow a child container to block GPO inheritance from parent containers. Use this option if you do not want to inherit GPO settings from parent containers and want only the GPO you have set for your container to be applied. For example, if you set Block Inheritance on an OU policy, only the OU policy would be applied; no parent container policies would be inherited.

If a conflict exists between the Enforce and the Block Inheritance settings, the Enforce option is applied.

Real World Scenario

APPLYING GPOS

You manage a network that consists of 500 computers all running Windows 7. You are already using Active Directory and have logically defined your OUs based on function. One OU, called Sales, has 50 users. Your task is to configure the Sales computers so they all have a consistent Desktop that can't be modified. You also need to add the new Sales Management software to each computer.

It would take days for you to manually configure each computer with a Local Group Policy and then add the software. In this case, GPOs are a real benefit. As the administrator of the Sales OU, you can create a single GPO that will be applied to all users of the container. You can specify the Desktop settings and publish any applications that you want to install. Next time the Sales users log on, the Group Policies are applied, and the users' Registries are updated to reflect the changes. In addition, through the automated publishing applications, the GPO can be configured to be automatically loaded on each of the Sales users' computers.

By using GPOs, you can add new software, configure computers, and accomplish other tasks from your computer that would normally require you to physically visit each machine.

Now that we have looked at GPOs, let's explore some of the tools available for creating and managing GPOs.

Using the Group Policy Result Tool

When a user logs on to a computer or domain, a resulting set of policies to be applied is generated based on the LGPOs, site GPOs, domain GPOs, and OU GPOs. The overlapping nature of Group Policies can make it difficult to determine what Group Policies will be applied to a computer or user.

To help determine what policies will actually be applied, Windows 7 includes a tool called the Group Policy Result Tool, also known as the Resultant Set of Policy (RSoP). You can access this tool through the GPResult command-line utility. The `gpresult` command displays the resulting set of policies that were enforced on the computer and the specified user during the logon process.

The `gpresult` command displays the RSoP for the computer and the user who is currently logged in. You can use several options with this command. Table 9.2 shows the different switches that you can use for the `gpresult` command.

TABLE 9.2: `gpresult` Switches

SWITCH	EXPLANATION
/F	Forces `gpresult` to override the filename specified in the /X or /H command
/H	Saves the report in an HTML format
/P	Specifies the password for a given user context
/R	Displays RSoP summary data
/S	Specifies the remote system to connect to
/U	Specifies which user context under which the command should be executed
/V	Specifies that verbose information should be displayed
/X	Saves the report in XML format
/Z	Specifies that the super verbose information should be displayed
/?	Shows all the `gpresult` command switches
/scope	Specifies whether the user or the computer settings need to be displayed
/User	Specifies the username for which the RSoP data is to be displayed

In the next section, you'll learn how to create and apply LGPOs to the Windows 7 machine.

Creating and Applying LGPOs

As we discussed previously, policies that have been linked through Active Directory will, by default, take precedence over any established Local Group Policies. Local Group Policies are typically applied to computers that are not part of a network or are in a network that does not have a domain controller, and thus do not use Active Directory.

Previous versions of Windows (before Vista) only contained one LGPO that applied to all the computer's users unless NTFS permissions were applied to the LGPO. However, Windows 7 and Windows Vista changed that with the addition of Multiple Local Group Policy

Objects (MLGPOs). Like Active Directory GPOs, MLGPOs are applied in a certain hierarchical order, as follows:

1. Local Computer Policy
2. Administrators and Non-Administrators Local Group Policy
3. User-Specific Group Policy

The Local Computer Policy is the only LGPO that includes computer and user settings; the other LGPOs only contain user settings. Settings applied here apply to all users of the computer.

The Administrators and Non-Administrators LGPOs were new to Windows Vista and are still included with Windows 7. The Administrators LGPO is applied to users who are members of the built-in local Administrators group. As you might guess, the Non-Administrators LGPO is applied to users who are not members of the local Administrators group. Because each user of a computer can be classified as an administrator or a non-administrator, either one policy or the other will apply.

User-Specific LGPOs are also included with Windows 7. These LGPOs make it possible for specific policy settings to apply to a single user.

Like Active Directory GPOs, any GPO settings applied lower in the hierarchy will override GPO settings applied higher in the hierarchy by default. For example, any user-specific GPO settings will override any conflicting administrator/non-administrator GPO settings or Local Computer Policy settings. And, of course, any AD GPO settings will still override any conflicting LGPO settings.

Disabling the Local Group Policy Object

Domain administrators can disable LGPOs on Windows 7 computers by enabling the Turn Off LGPOs Processing domain GPO setting, which you can find under `Computer Configuration\Administrative Templates\System\Group Policy`.

You apply an LGPO to a Windows 7 computer through the GPO Editor snap-in within the MMC. Figure 9.2 shows the Local Computer Policy dialog box for a Windows 7 computer.

Perform the following steps to add the Local Computer Policy snap-in to the MMC:

1. Open the Admin Console MMC shortcut by typing **MMC** in the Search Programs And Files box.
2. A User Account Control dialog box appears. Click Yes.
3. Select File ➢ Add/Remove Snap-in.
4. Highlight the Group Policy Object Editor Snap-in and click the Add button.
5. The Group Policy Object specifies Local Computer by default. Click the Finish button.
6. In the Add Or Remove Snap-ins dialog box, click OK.
7. In the left-hand pane, right-click the Local Computer Policy and choose New Windows From Here.

8. Choose File ➢ Save As and name the console **LGPO**. Make sure you save it to the Desktop. Click Save.
9. Close the MMC Admin console.

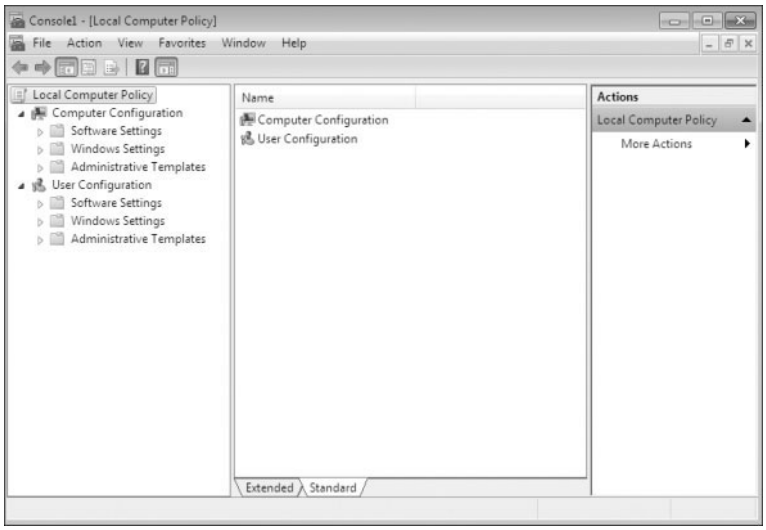


FIGURE 9.2
Local Computer Policy dialog box

Now let's see how to open an LGPO for a specific user account on a Windows 7 machine.

Perform the following steps to access the Administrators, Non-Administrators, and User-Specific LGPOs. The previous steps must be completed to use this procedure.

1. Open the Admin Console MMC shortcut by typing **MMC** in the Search Programs And Files box.
2. Select File ➢ Add/Remove Snap-in.
3. Highlight the Group Policy Object Editor Snap-in and click Add.
4. Click Browse to look for a different GPO.
5. Click the Users tab.
6. Select the user that you want to access and click OK.
7. In the Select Group Policy Object dialog box, click Finish.
8. In the Add Or Remove Snap-ins dialog box, click OK. You can close the console when you are finished looking at the LGPO settings for the user you chose.

USER CONFIGURATION SETTINGS ONLY

Notice that the Administrators, Non-Administrators, and User-Specific LGPOs contain only User Configuration settings, not Computer Configuration settings.

Now let's examine the various security settings that you can configure in the LGPO.

Configuring Local Security Policies

Through the use of the Local Computer Policy, you can set a wide range of security options under Computer Configuration\Windows Settings\Security Settings.

This portion of the Local Computer Policy is also known as the Local Security Policy. The following list describes in detail how to apply security settings through LGPOs, as shown in Figure 9.3.

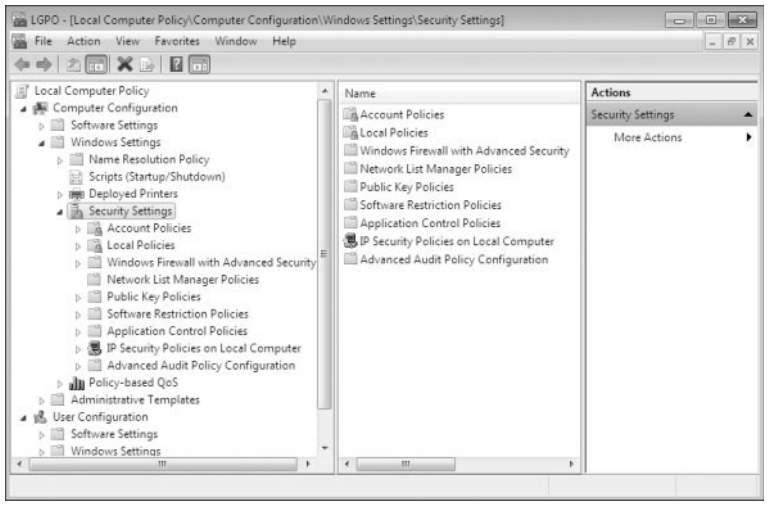


FIGURE 9.3 Security settings of the LGPO

The main areas of security configuration of the LGPO are as follows:

Account Policies You can use Account policies to configure password and account lockout features. Some of these settings include Password History, Maximum Password Age, Minimum Password Age, Minimum Password Length, Password Complexity, Account Lockout Duration, Account Lockout Threshold, and Reset Account Lockout Counter After.

Local Policies You can use Local Policies to configure auditing, user rights, and security options.

Windows Firewall with Advanced Security Windows Firewall with Advanced Security provides network security for Windows computers. Through this LGPO, you can set Domain, Private, and Public Profiles. You can also set this LGPO to authenticate communications between computers and inbound/outbound rules.

Network List Manager Policies This section allows you to set the network name, icon, and location Group Policies. Administrators can set Unidentified Networks, Identifying Networks, and All Networks.

Public Key Policies You can use the Public Key Policies settings to specify how to manage certificates and certificate life cycles.

Software Restriction Policies Software Restriction Policies allow you to identify malicious software and control that software's ability to run on the Windows 7 machine. These policies allow an administrator to protect the Windows 7 operating system against security threats such as viruses and Trojan horse programs.

Application Control Policies You can use these policies to set up AppLocker. AppLocker allows you to configure a Denied list and an Accepted list for applications. Applications that are configured on the Denied list will not run on the system, and applications on the Accepted list will operate properly.

IP Security Policies on Local Computer You can use these policies to configure the IPSec policies. IPSec is a way to secure data packets at the IP level of the message.

Advanced Audit Policy Configuration You can use Advanced Audit Policy configuration settings to provide detailed control over audit policies. This section also allows you to configure auditing to help show administrators either successful or unsuccessful attacks on their network.

Accessing the Local Security Policy

You can also access the Local Security Policy by running `secpol.msc` or by opening Control Panel and selecting Administrative Tools ➢ Local Security Policy.

Now that we have seen all the options in the security section of the LGPO, let's look at account policies and local policies in more detail in the following sections.

Using Account Policies

You use account policies to specify the user account properties that relate to the logon process. They allow you to configure computer security settings for passwords and account lockout specifications.

If security is not an issue — perhaps because you are using your Windows 7 computer at home — you don't need to bother with account policies. If, on the other hand, security is important — for example, because your computer provides access to payroll information — you should set very restrictive account policies.

Account Policies

Account policies at the LGPO level apply only to local user accounts, not domain accounts. To ensure that user account security is configured for domain user accounts, you need to configure these policies at the Domain GPO level.

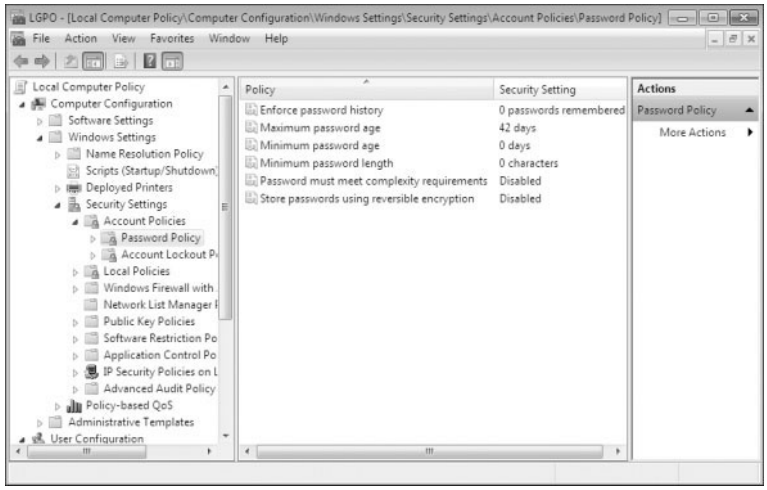
To access the Account Policies folder from the MMC, follow this path: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies. We look at all these folders and how to use them throughout the rest of this chapter.

In the following sections you will learn about the password policies and account lockout policies that define how security is applied to account policies.

Setting Password Policies

Password policies ensure that security requirements are enforced on the computer. It is important to understand that the password policy is set on a per-computer basis; it cannot be configured for specific users. Figure 9.4 shows the password policies that Table 9.3 describes.

FIGURE 9.4
The password policies



You can use the password policies shown in Table 9.3 as follows:

Enforce Password History Prevents users from repeatedly using the same passwords. Users must create a new password when their password expires or is changed.

Maximum Password Age Forces users to change their password after the maximum password age is exceeded. Setting this value to 0 will specify that the password will never expire.

Minimum Password Age Prevents users from changing their password several times in rapid succession in order to defeat the purpose of the Enforce Password History policy.

Minimum Password Length Ensures that users create a password and specifies the length requirement for that password. If this option isn't set, users are not required to create a password at all.

Password Must Meet Complexity Requirements Passwords must be six characters or longer and cannot contain the user's account name or any part of the user's full name. In addition, passwords must contain three of the following character types:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Decimal digits (0 through 9)
- Symbols (such as !, @, #, $, and %)

Store Passwords Using Reversible Encryption Provides a higher level of security for user passwords. This is required for Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS) and for Digest Authentication with Internet Information Services (IIS).

TABLE 9.3: Password Policy Options

POLICY	DESCRIPTION	DEFAULT	MINIMUM	MAXIMUM
Enforce Password History	Keeps track of user's password history	Remember 0 passwords	Same as default	Remember 24 passwords
Maximum Password Age	Determines maximum number of days user can keep valid password	Keep password for 42 days	Keep password for 1 day	Keep password for up to 999 days
Minimum Password Age	Specifies how long password must be kept before it can be changed	0 days (password can be changed immediately)	Same as default	998 days
Minimum Password Length	Specifies minimum number of characters password must contain	0 characters (no password required)	Same as default	14 characters
Password Must Meet Complexity Requirements	Requires that passwords meet minimum levels of complexity	Disabled		
Store Passwords Using Reversible Encryption	Specifies higher level of encryption for stored user passwords	Disabled		

Perform the following steps to configure password policies for your computer. These steps assume that you have added the Local Computer Policy snap-in to the MMC completed in earlier steps.

1. Open the LGPO MMC shortcut that you created earlier.
2. Expand the Local Computer Policy snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies ➢ Password Policy.
4. Open the Enforce Password History policy. On the Local Security Setting tab, specify that 5 passwords will be remembered. Click OK.
5. Open the Maximum Password Age policy. On the Local Security Setting tab, specify that the password expires in 60 days. Click OK.

Let's look at how to set and manage the Account Lockout Policies section.

Setting Account Lockout Policies

The account lockout policies specify how many invalid logon attempts should be tolerated. You configure the account lockout policies so that after *x* number of unsuccessful logon attempts within *y* number of minutes, the account will be locked for a specified amount of time or until the administrator unlocks the account.

Account lockout policies are similar to a bank's arrangements for ATM access code security. You have a certain number of chances to enter the correct PIN. That way, anyone who steals your card can't just keep guessing your access code until they get it right. Typically, after three unsuccessful attempts, the ATM takes the card. Then you need to request a new card from the bank. Figure 9.5 shows the account lockout policies that Table 9.4 describes.

Figure 9.5
The account lockout policies

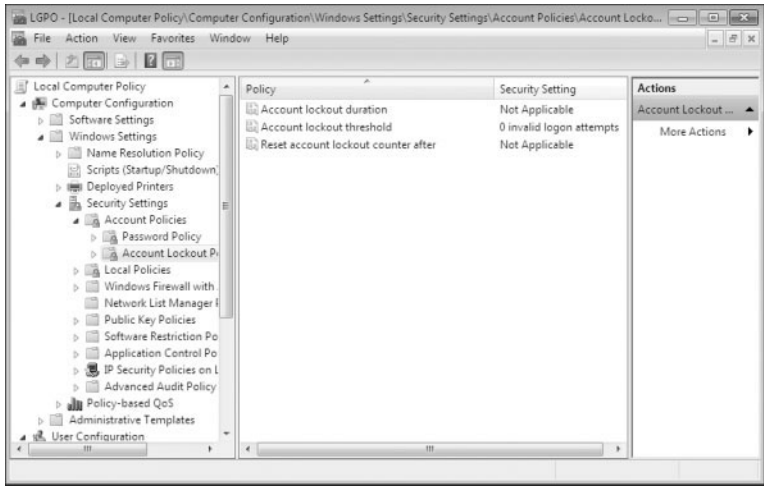


Table 9.4: Account Lockout Policy Options

Policy	Description	Default	Minimum	Maximum
Account Lockout Duration	Specifies how long account will remain locked if Account Lockout Threshold is reached	Disabled, but if Account Lockout Threshold is enabled, 30 minutes	Same as default	99,999 minutes
Account Lockout Threshold	Specifies number of invalid attempts allowed before account is locked out	0 (disabled; account will not be locked out)	Same as default	999 attempts
Reset Account Lockout Counter After	Specifies how long counter will remember unsuccessful logon attempts	Disabled, but if Account Lockout Threshold is enabled, 30 minutes	Same as default	99,999 minutes

The Account Lockout Duration and Reset Account Lockout Counter After policies will be disabled until a value is specified for the Account Lockout Threshold. After the Account Lockout Threshold is set, the Account Lockout Duration and Reset Account Lockout Counter After policies will be set to 30 minutes. If you set the Account Lockout Duration to 0, the account will remain locked out until an administrator unlocks it.

RESET ACCOUNT LOCKOUT COUNTER

The Reset Account Lockout Counter After value must be equal to or less than the Account Lockout Duration value.

Perform the following steps to configure account lockout policies and test their effects. Make sure that you completed all previous procedures before you perform these steps.

1. Open the LGPO MMC shortcut.
2. Expand the Local Computer Policy snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Account Policies ➢ Account Lockout Policy.
4. Open the Account Lockout Threshold policy. On the Local Security Setting tab, specify that the account will lock after three invalid logon attempts. Click OK.
5. Accept the ''Suggested Value Changes for the Account Lockout Duration and Reset Account Lockout Counter After'' policies by clicking OK.
6. Open the Account Lockout Duration policy. On the Local Security Setting tab, specify that the account will remain locked for 5 minutes. Click OK.
7. Accept the ''Suggested Value Changes for the Reset Account Lockout Counter After'' policy by clicking OK.
8. Log off your administrator account. Try to log on as one of the accounts that were created on this Windows 7 machine and enter an incorrect password four times.
9. After you see the error message that states that the referenced account has been locked out, log on as an administrator.
10. To unlock the account, open the Local Users and Groups snap-in in the MMC, expand the Users folder, and double-click the user.
11. On the General tab of the users Properties dialog box, click to remove the check from the Account Is Locked Out check box. Then click OK.

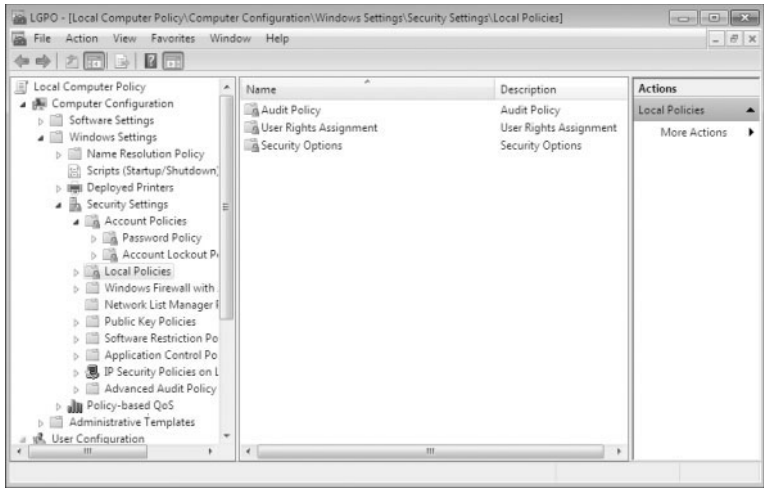
In the next section we discuss how to control a user or computer after the user has logged into the Windows 7 machine.

Using Local Policies

As you learned in the preceding section, account policies are used to control logon procedures. When you want to control what a user can do after logging on, you use local policies. With local policies, you can implement auditing, specify user rights, and set security options.

To use local policies, first add the Local Computer Policy snap-in to the MMC. Then, from the MMC, follow this path to access the Local Policies folders: Local Computer Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies. Figure 9.6 shows the three Local Policies folders: Audit Policy, User Rights Assignment, and Security Options. We look at each of these in the following sections.

FIGURE 9.6
Accessing the Local Policies folders



Setting Audit Policies

You can implement audit policies to track success or failure of specified user actions. You audit events that pertain to user management through the audit policies. By tracking certain events, you can create a history of specific tasks, such as user creation and successful or unsuccessful logon attempts. You can also identify security violations that arise when users attempt to access system management tasks for which they do not have permissions.

Real World Scenario

Auditing Failed Attempts

As an IT manager, you have to make sure that you monitor failed attempts to resources. A failed attempt to a resource usually means that someone tried to access a resource and they were denied due to insufficient privileges.

Users who try to go to areas for which they do not have permissions usually fall into two categories: hackers and people who are just curious to see what they can get away with. Both are very dangerous.

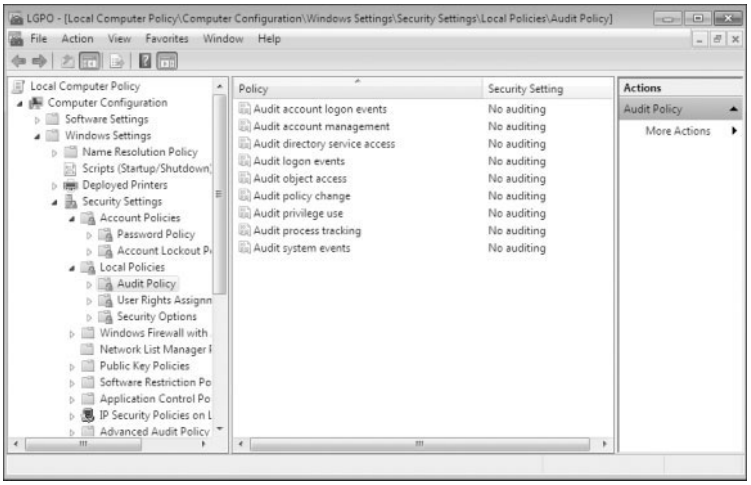
If a user is trying to access an area that they do not belong to, be sure to warn the user about the attacks. This is very common on a network and needs to be nipped in the bud immediately.

When you define an audit policy, you can choose to audit success or failure of specific events. The success of an event means that the task was successfully accomplished. The failure of an event means that the task was not successfully accomplished.

By default, auditing is not enabled, and it must be manually configured. After you have configured auditing, you can see the results of the audit in the Security log by using the Event Viewer utility.

Figure 9.7 shows the audit policies that Table 9.5 describes.

FIGURE 9.7
The audit policies



After you set the Audit Object Access policy to enable auditing of object access, you must enable file auditing through NTFS security or print auditing through printer security.

Perform the following steps to configure audit policies and view their results. These steps assume that you have added the Local Group Object Policy snap-in to the MMC completed in earlier steps.

1. Open the LGOP MMC shortcut.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Audit Policy.
4. Open the Audit Account Logon Events policy. Check the boxes for Success and Failure. Click OK.
5. Open the Audit Account Management policy. Check the boxes for Success and Failure. Click OK.
6. Log off your administrator account. Attempt to log back on as your administrator account with an incorrect password. The logon should fail (because the password is incorrect).
7. Log on as an administrator.
8. Select Start, right-click Computer, and select Manage to open Computer Management. Click Event Viewer.
9. From Event Viewer, open the Security log by selecting Windows Logs ➢ Security. You should see the audited events listed with a Task Category of Credential Validation.

TABLE 9.5: Audit Policy Options

POLICY	DESCRIPTION
Audit Account Logon Events	Tracks when a user logs on or logs off either their local machine or the domain (if domain auditing is enabled)
Audit Account Management	Tracks user and group account creation, deletion, and management actions, such as password changes
Audit Directory Service Access	Tracks directory service accesses
Audit Logon Events	Audits events related to logon, such as running a logon script or accessing a roaming profile or accessing a server
Audit Object Access	Enables auditing of access to files, folders, and printers
Audit Policy Change	Tracks any changes to the audit policies, trust policies, or user rights assignment policies
Audit Privilege Use	Tracks users exercising a user right
Audit Process Tracking	Tracks events such as activating a program, accessing an object, and exiting a process
Audit System Events	Tracks system events such as shutting down or restarting the computer, as well as events that relate to the Security log in Event Viewer

AUDITING

You might want to limit the number of events that are audited. If you audit excessive events on a busy computer, the log file can grow quickly. In the event that the log file becomes full, you can configure the computer to shut down through a security option policy, Audit: Shut Down System Immediately If Unable To Log Security Audits. If this option is triggered, the only user who will be able to log on to the computer will be an administrator until the log is cleared. If this option is not enabled and the log file becomes full, you have the option of overwriting older log events.

In the next section, we look at how to configure the user rights on the Windows 7 machine.

ASSIGNING USER RIGHTS

The user right policies determine what rights a user or group has on the computer. User rights apply to the system. They are not the same as permissions, which apply to a specific object (permissions are discussed later in this chapter, in the section ''Managing File and Folder Security'').

An example of a user right is the Back Up Files And Directories right. This right allows a user to back up files and folders, even if the user does not have permissions that have been defined through NTFS file system permissions. The other user rights are similar because they deal with system access as opposed to resource access.

Figure 9.8 shows the user right policies that Table 9.6 describes.

FIGURE 9.8
The user right policies

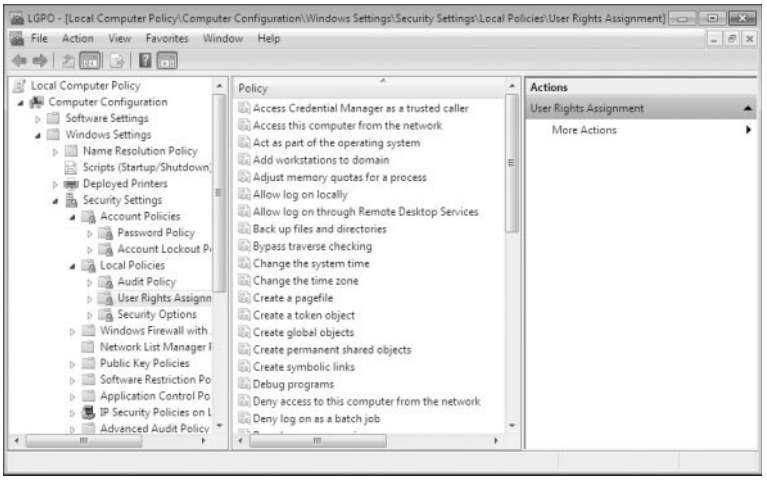


TABLE 9.6: User Rights Assignment Policy Options

RIGHT	DESCRIPTION
Access Credential Manager As A Trusted Caller	Used to back up and restore Credential Manager.
Access This Computer From The Network	Allows a user to access the computer from the network.
Act As Part Of The Operating System	Allows low-level authentication services to authenticate as any user.
Add Workstations To Domain	Allows a user to create a computer account on the domain.
Adjust Memory Quotas For A Process	Allows you to configure how much memory can be used by a specific process.
Allow Log On Locally	Allows a user to log on at the physical computer.
Allow Log On Through Terminal Services	Gives a user permission to log on through Terminal Services. Does not affect Windows 2000 computers prior to SP2.
Back Up Files And Directories	Allows a user to back up all files and directories, regardless of how the file and directory permissions have been set.
Bypass Traverse Checking	Allows a user to pass through and traverse the directory structure, even if that user does not have permissions to list the contents of the directory.
Change The System Time	Allows a user to change the internal time and date on the computer.
Change The Time Zone	Allows a user to change the time zone.

TABLE 9.6: User Rights Assignment Policy Options (*CONTINUED*)

RIGHT	DESCRIPTION
Create A Pagefile	Allows a user to create or change the size of a page file.
Create A Token Object	Allows a process to create a token if the process uses an internal API to create the token.
Create Global Objects	Allows a user to create global objects when connected using Terminal Server.
Create Permanent Shared Objects	Allows a process to create directory objects through the Object Manager.
Create Symbolic Links	Allows a user to create a symbolic link.
Debug Programs	Allows a user to attach a debugging program to any process.
Deny Access To This Computer From The Network	Allows you to deny specific users or groups access to this computer from the network. Overrides the Access This Computer from the Network policy for accounts present in both policies.
Deny Log On As A Batch Job	Allows you to prevent specific users or groups from logging on as a batch file. Overrides the Log On as a Batch Job policy for accounts present in both policies.
Deny Log On As A Service	Allows you to prevent specific users or groups from logging on as a service. Overrides the Log On as a Service policy for accounts present in both policies.
Deny Log On Locally	Allows you to deny specific users or groups access to the computer locally. Overrides the Log On Locally policy for accounts present in both policies.
Deny Log On Through Terminal Services	Specifies that a user is not able to log on through Terminal Services. Does not affect Windows 2000 computers prior to SP2.
Enable Computer And User Accounts To Be Trusted For Delegation	Allows a user or group to set the Trusted For Delegation setting for a user or computer object.
Force Shutdown From A Remote System	Allows the system to be shut down by a user at a remote location on the network.
Generate Security Audits	Allows a user, group, or process to make entries in the Security log.
Impersonate A Client After Authentication	Enables programs running on behalf of a user to impersonate a client.
Increase A Process Working Set	Allows the size of a process working set to be increased.
Increase Scheduling Priority	Specifies that a process can increase or decrease the priority that is assigned to another process.

TABLE 9.6: User Rights Assignment Policy Options (*CONTINUED*)

RIGHT	DESCRIPTION
Load And Unload Device Drivers	Allows a user to dynamically unload and load device drivers. This right does not apply to Plug and Play drivers.
Lock Pages In Memory	Allows an account to create a process that runs only in physical RAM, preventing it from being paged.
Log On As A Batch Job	Allows a process to log on to the system and run a file that contains one or more operating system commands.
Log On As A Service	Allows a service to log on in order to run the specific service.
Manage Auditing And Security Log	Allows a user to enable object access auditing for files and other Active Directory objects. This right does not allow a user to enable general object access auditing in the Local Security Policy.
Modify An Object Label	Allows a user to change the integrity level of files, folders, or other objects.
Modify Firmware Environment Variables	Allows a user to install or upgrade Windows. It also allows a user or process to modify the firmware environment variables stored in NVRAM of non-x86-based computers. This right does *not* affect the modification of system environment variables or user environment variables.
Perform Volume Maintenance Tasks	Allows a user to perform volume maintenance tasks such as defragmentation and error checking.
Profile Single Process	Allows a user to monitor nonsystem processes through performance-monitoring tools.
Profile System Performance	Allows a user to monitor system processes through performance-monitoring tools.
Remove Computer From Docking Station	Allows a user to undock a laptop through the Windows 7 user interface.
Replace A Process Level Token	Allows a process, such as Task Scheduler, to call an API to start another service.
Restore Files And Directories	Allows a user to restore files and directories, regardless of file and directory permissions.
Shut Down The System	Allows a user to shut down the Windows 7 computer locally.
Synchronize Directory Service Data	Allows a user to synchronize Active Directory data.
Take Ownership Of Files Or Other Objects	Allows a user to take ownership of system objects, such as files, folders, printers, and processes.

Perform the following steps to apply a user right policy. These steps assume that you added the Local Group Object Policy snap-in to the MMC completed in earlier steps.

1. Open the LGPO MMC shortcut.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ User Rights Assignment.
4. Open the Log On As A Service user right.
5. Click the Add User Or Group button. The Select Users Or Groups dialog box appears.
6. Click the Advanced button and then select Find Now.
7. Select a user. Click OK.
8. Click OK in the Select Users Or Groups dialog box.
9. In the Log On As A Service Properties dialog box, click OK.

Now we look at how to define security options within the LGPO.

Defining Security Options

You can use security option policies to configure security for the computer. Unlike user right policies, which are applied to a user, security option policies apply to the computer. Figure 9.9 shows the security option policies that Table 9.7 describes.

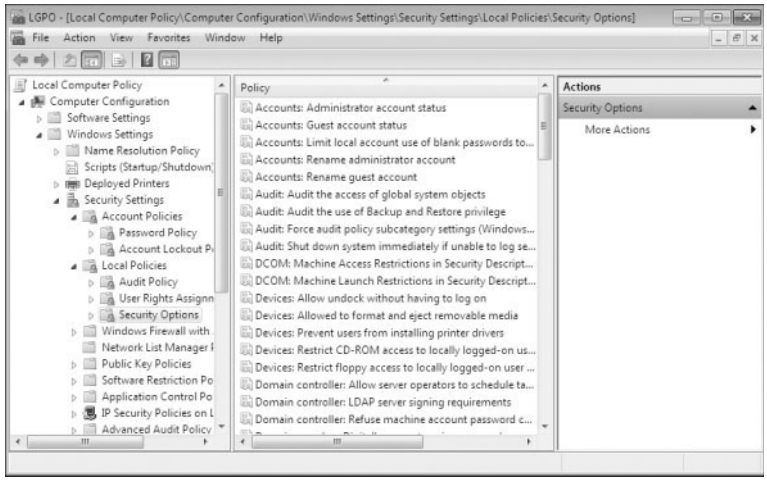


Figure 9.9
The security option policies

TABLE 9.7: Security Options

OPTION	DESCRIPTION	DEFAULT
Accounts: Administrator Account Status	Specifies whether the Administrator account is enabled or disabled under normal operation. Booting under Safe Mode, the Administrator account is enabled, regardless of this setting.	Disabled
Accounts: Guest Account Status	Determines whether the Guest account is enabled or disabled.	Disabled
Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only	Determines whether a local user with a blank password will be able to log on remotely. If this policy is enabled, users with blank passwords will only be able to log on locally. This setting does not apply to domain logon accounts.	Enabled
Accounts: Rename Administrator Account	Allows the Administrator account to be renamed.	Administrator account is named Administrator.
Accounts: Rename Guest Account	Allows the Guest account to be renamed.	Guest account is named Guest.
Audit: Audit The Access Of Global System Objects	Allows access of global system objects to be audited.	Disabled
Audit: Audit The Use Of Backup And Restore Privilege	Allows the use of backup and restore privileges to be audited.	Disabled
Audit: Force Audit Policy Subcategory Settings (Windows 7 Or Later) To Override Audit Policy Category Settings	Allows audit policy subcategory settings to override audit policy category settings at the category level.	Not defined
Audit: Shut Down System Immediately If Unable To Log Security Audits	Specifies that the system shuts down immediately if it is unable to log security audits.	Disabled
DCOM: Machine Access Restrictions In Security Descriptor Definition Language (SDDL) Syntax	Specifies the users who can access DCOM applications.	Not defined
DCOM: Machine Launch Restrictions In Security Descriptor Definition Language (SDDL) Syntax	Specifies the users who can launch DCOM applications.	Not defined

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
Devices: Allow Undock Without Having To Log On	Allows a user to undock a laptop computer from a docking station by pushing the computer's eject button without first having to log on.	Enabled
Devices: Allowed to Format and Eject Removable Media	Specifies which users can format and eject removable NTFS media.	Not defined
Devices: Prevent Users From Installing Printer Drivers	If enabled, allows only Administrators to install print drivers for a network printer.	Disabled
Devices: Restrict CD-ROM Access To Locally Logged-On User Only	Specifies whether the CD-ROM is accessible to local users and network users. If enabled, only the local user can access the CD-ROM, but if no local user is logged in, then the CD-ROM can be accessed over the network. If disabled or not defined, access is not restricted.	Not defined
Devices: Restrict Floppy Access To Locally Logged-On User Only	Specifies whether the floppy drive is accessible to local users and network users. If enabled, only the local user can access the floppy, but if no local user is logged in, then the floppy can be accessed over the network. If disabled or not defined, access is not restricted.	Not defined
Domain Controller: Allow Server Operators To Schedule Tasks	Allows server operators to schedule specific tasks to occur at specific times or intervals. Applies only to tasks scheduled through the AT command and does not affect tasks scheduled through Task Scheduler.	Not defined
Domain Controller: LDAP Server Signing Requirements	Specifies whether a Lightweight Directory Access Protocol server requires server signing with an LDAP client.	Not defined
Domain Controller: Refuse Machine Account Password Changes	Specifies whether a domain controller will accept password changes for computer accounts.	Not defined
Domain Member: Digitally Encrypt Or Sign Secure Channel Data (Always)	Specifies whether a secure channel must be created with the domain controller before secure channel traffic is generated.	Enabled
Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Specifies that if a secure channel can be created between the domain controller and the domain controller partner, it will be.	Enabled

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
Domain Member: Digitally Sign Secure Channel Data (When Possible)	Specifies that all secure channel traffic be signed if both domain controller partners who are transferring data are capable of signing secure data.	Enabled
Domain Member: Disable Machine Account Password Changes	Specifies whether a domain member must periodically change its computer account password as defined in the Domain Member: Maximum Machine Account Password Age setting.	Disabled
Domain Member: Maximum Machine Account Password Age	Specifies the maximum age of a computer account password.	30 days
Domain Member: Require Strong (Windows 2000 Or Later) Session Key	If enabled, the domain controller must encrypt data with a 128-bit session key; if not enabled, 64-bit session keys can be used.	Disabled
Interactive Logon: Do Not Display Last User Name	Prevents the last username in the logon screen from being displayed.	Disabled
Interactive Logon: Do Not Require Ctrl+Alt+Del	Allows the Ctrl+Alt+Del requirement for logon to be disabled.	Not defined, but it is automatically used on standalone workstations, meaning users who log on to the workstation see a start screen with icons for all users who have been created on the computer.
Interactive Logon: Message Text For Users Attempting To Log On	Displays message text for users trying to log on, usually configured for displaying legal text messages.	Not defined
Interactive Logon: Message Title For Users Attempting to Log On	Displays a message title for users trying to log on.	Not defined
Interactive Logon: Number Of Previous Logon Attempts To Cache (In Case Domain Controller Is Not Available)	Specifies the number of previous logon attempts stored in the cache. This option is useful if a domain controller is not available.	10

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
Interactive Logon: Prompt User To Change Password Before Expiration	Prompts the user to change the password before expiration.	14 days before password expiration
Interactive Logon: Require Domain Controller Authentication To Unlock	Specifies that a user name and password be required to unlock a locked computer. When this is disabled, a user can unlock a computer with cached credentials. When this is enabled, a user is required to authenticate to a domain controller to unlock the computer.	Disabled
Interactive Logon: Require Smart Card	Specifies that a smart card is required to log on to the computer.	Disabled
Interactive Logon: Smart Card Removal Behavior	Specifies what happens if a user who is logged on with a smart card removes the smart card.	No action
Microsoft Network Client: Digitally Sign Communications (Always)	Specifies that the server should always digitally sign client communication.	Disabled
Microsoft Network Client: Digitally Sign Communications (If Server Agrees)	Specifies that the server should digitally sign client communication when possible.	Enabled
Microsoft Network Client: Send Unencrypted Password To Third-Party SMB Servers	Allows third-party Server Message Block servers to use unencrypted passwords for authentication.	Disabled
Microsoft Network Client: Amount Of Idle Time Required: Before Suspending Session	Allows sessions to be disconnected when they are idle.	15 minutes
Microsoft Network Server: Digitally Sign Communications (Always)	Ensures that server communications will always be digitally signed.	Disabled
Microsoft Network Server: Digitally Sign Communications (If Client Agrees)	Specifies that server communications should be signed when possible.	Disabled
Microsoft Network Server: Disconnect Clients When Logon Hours Expire	If a user logs on and then their logon hours expire, specifies whether an existing connection will remain connected or be disconnected.	Enabled

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
Network Access: Allow Anonymous SID/Name Translation	Specifies whether an anonymous user can request the security identifier (SID) attributes for another user.	Disabled
Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts.	Enabled
Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts And Shares	If enabled, prevents an anonymous connection from enumerating Security Account Manager (SAM) accounts and network shares.	Disabled
Network Access: Do Not Allow Storage Of Credentials Or .NET Passports for Network Authentication	Specifies whether passwords, credentials, and .NET Passports are stored and available for use after a user is authenticated to a domain.	Disabled
Network Access: Let Everyone Permissions Apply To Anonymous Users	Specifies whether Everyone permission will apply to anonymous users.	Disabled
Network Access: Named Pipes That Can Be Accessed Anonymously	Specifies which communication sessions are allowed to anonymous users.	Defined
Network Access: Remotely Accessible Registry Paths	Determines which Registry paths will be accessible when the `winreg` key is accessed for remote Registry access, regardless of the ACL setting.	Defined
Network Access: Remotely Accessible Registry Paths And Sub-Paths	Determines which Registry paths and subpaths will be accessible when the `winreg` key is accessed for remote Registry access, regardless of the ACL setting.	Defined
Network Access: Restrict Anonymous Access To Named Pipes And Shares	Specifies whether anonymous access is allowed to shares and pipes for the Network Access: Named Pipes That Can Be Accessed Anonymously and Network Access: Shares That Can Be Accessed Anonymously policies	Enabled
Network Access: Shares That Can Be Accessed Anonymously	Specifies which network shares can be accessed by anonymous users.	Not defined
Network Access: Sharing And Security Model For Local Accounts	Specifies how local accounts will be authenticated over the network.	Classic – Local Users Authenticate As Themselves

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
Network Security: Do Not Store LAN Manager Hash Value On Next Password Change	Specifies whether LAN Manager will store hash values from password changes.	Enabled
Network Security: Force Logoff When Logon Hours Expire	Specifies whether a user with a current connection will be automatically logged off when the user's logon hours expire.	Disabled
Network Security: LAN Manager Authentication Level	Specifies the LAN Manager Authentication Level.	Send NTLMv2 Response Only
Network Security: LDAP Client Signing Requirements	Specifies the client signing requirements that will be enforced for LDAP clients.	Negotiate Signing
Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Clients	Specifies the minimum security standards for application-to-application client communications.	No minimum
Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Servers	Specifies the minimum security standards for application-to-application server communications.	No minimum
Recovery Console: Allow Automatic Administrative Logon	Specifies whether a password is required for Administrative logon when the Recovery Console is loaded. If Enabled, the password is not required.	Disabled
Recovery Console: Allow Floppy Copy and Access To All Drives And All Folders	Allows you to copy files from all drives and folders when the Recovery Console is loaded.	Disabled
Shutdown: Allow System To Be Shut Down Without Having To Log On	Allows the user to shut down the system without logging on.	Enabled
Shutdown: Clear Virtual Memory Pagefile	Specifies whether the virtual memory pagefile will be cleared when the system is shut down.	Disabled
System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer	Specifies whether a password is required to use a private key.	Not defined
System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing and Signing	Specifies which encryption algorithms should be supported for encrypting, hashing, and signing file data.	Disabled

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
System Objects: Default Owner For Objects Created By Members Of The Administrators Group	Determines whether, when an object is created by a member of the Administrators group, the owner will be the Administrators group or the user who created the object.	Object Creator
System Objects: Require Case Insensitivity For Non-Windows Subsystems	By default, Windows 7 does not specify case insensitivity for file subsystems. However, subsystems such as POSIX use case-sensitive file systems, so this option allows you to configure case sensitivity.	Enabled
System Objects: Strengthen Default Permissions Of Internal System Objects (for example, Symbolic Links)	Specifies the default discretionary access control list for objects.	Enabled
System Settings: Optional Subsystems	Specifies the subsystems that are used to support applications in your environment.	POSIX
System Settings: Use Certificate Rules On Windows Executables For Software Restriction Policies	Specifies whether digital certificates are required when a user or process runs an EXE file.	Disabled
User Account Control: Admin Approval Mode For The Built-in Administrator Account	If Enabled, the built-in Administrator account will require approval for any operation that requires privilege elevation. If Disabled, the built-in Administrator account will use XP-compatible mode with full administrative privileges.	Disabled
User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode	Specifies the method for approval of privilege elevation for administrators.	Prompt For Consent
User Account Control: Behavior Of The Elevation Prompt For Standard Users	Specifies the method for approval of privilege elevation for standard users.	Prompt For Credentials
User Account Control: Detect Application Installations And Prompt For Elevation	Specifies how applications are installed and whether approval is required.	Enabled
User Account Control: Only Elevate Executables That Are Signed And Validated	Specifies whether PKI signature checks are required for applications that request privilege elevation.	Disabled

TABLE 9.7: Security Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT
User Account Control: Only Elevate UIAccess Applications That Are Installed In Secure Locations	Requires that applications executing with a UIAccess integrity level reside in a secure file system location.	Enabled
User Account Control: Run All Administrators In Admin Approval Mode	Enforces UAC policy for all users, including administrators.	Enabled
User Account Control: Switch To The Secure Desktop When Prompting For Elevation	If Enabled, elevation requests will go to the Secure Desktop. If Disabled, elevation requests will appear on the users' desktop.	Enabled
User Account Control: Virtualize File And Registry Write Failures To Per-User Locations	Allows standard users to run pre-Windows 7 applications that formerly required administrator-level access to write to protected locations.	Enabled

Perform the following steps to define some security option policies and see how they work. These steps assume that you added the Local Group Object Policy snap-in to the MMC completed in earlier steps.

1. Open the LGPO MMC shortcut.
2. Expand the Local Computer Policy Snap-in.
3. Expand the folders as follows: Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options.
4. Open the policy Interactive Logon: Message Text For Users Attempting To Log On. On the Local Policy Setting tab, type **Welcome to all authorized users**. Click OK.
5. Open the policy Interactive Logon: Message Title For Users Attempting To Log On. On the Local Security Setting tab, type **Welcome Message**. Click OK.
6. Open the policy Interactive Logon: Prompt User To Change Password Before Expiration. On the Local Security Setting tab, type **3 days**. Click OK.
7. Log off your administrator account and see the Welcome Message text appear. Click OK.
8. Log on as an administrator.

In the next section we look at how users can install resources on Windows 7 without being an administrator by using the User Account Control.

Configuring User Account Control

Most administrators have had to wrestle with the balance between security and enabling applications to run correctly. In the past, some applications simply would not run correctly under Windows unless the user running the application was a local administrator.

Unfortunately, granting local administrator permissions to a user also allows the user to install software and hardware, change configuration settings, modify local user accounts, and delete critical files. Even more troubling is the fact that malware that infects a computer while an administrator is logged in is also able to perform those same functions.

Limited user accounts in Windows XP were supposed to allow applications to run correctly and allow users to perform necessary tasks. However, in practical application, it did not work as advertised. Many applications require that users have permissions to write to protected folders and to the Registry, and limited user accounts did not allow users to do so.

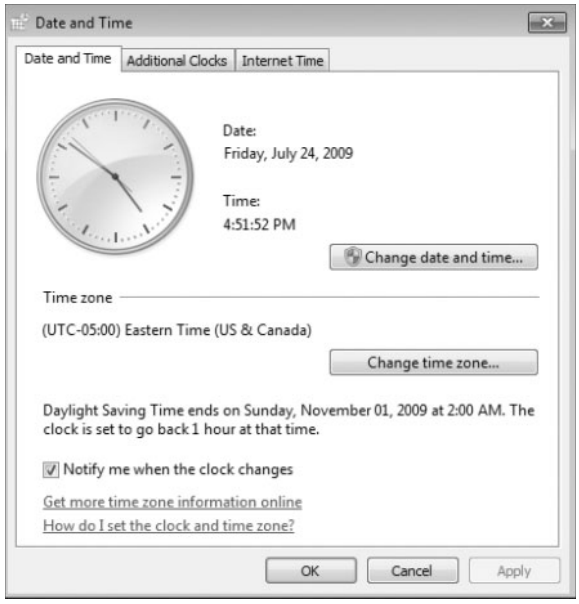
Windows 7's answer to the problem is User Account Control (UAC). UAC enables nonadministrator users to perform standard tasks, such as install a printer, configure a VPN or wireless connection, and install updates, while preventing them from performing tasks that require administrative privileges, such as installing applications.

Managing Privilege Elevation

UAC protects computers by requiring privilege elevation for all users, even users who are members of the local Administrators group. As you have no doubt seen by now, UAC prompts you for permission when you perform a task that requires privilege elevation. This prevents malware from silently launching processes without your knowledge.

Privilege elevation is required for any feature that contains the four-color security shield. For example, the small shield shown on the Change Date And Time button in the Date And Time dialog box in Figure 9.10 indicates an action that requires privilege elevation.

FIGURE 9.10
Date And Time dialog box



Now let's look at how to elevate privileges for users.

Elevated Privileges for Users

By default, local administrators are logged on as standard users. When administrators attempt to perform a task that requires privilege escalation, they are prompted for confirmation by

default. You can require administrators to authenticate when performing a task that requires privilege escalation by changing the User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode policy setting to Prompt For Credentials. On the other hand, if you don't want UAC to prompt administrators for confirmation when elevating privileges, you can change the policy setting to Elevate Without Prompting.

Nonadministrator accounts are called standard users. When standard users attempt to perform a task that requires privilege elevation, they are prompted for a password of a user account that has administrative privileges. You cannot configure UAC to automatically allow standard users to perform administrative tasks, nor can you configure UAC to prompt a standard user for confirmation before performing administrative tasks. If you do not want standard users to be prompted for credentials when attempting to perform administrative tasks, you can automatically deny elevation requests by changing the User Account Control: Behavior Of The Elevation Prompt For Standard Users policy setting to Automatically Deny Elevation Requests.

The built-in Administrator account, though disabled by default, is not affected by UAC. UAC will not prompt the Administrator account for elevation of privileges. Thus, it is important to use a normal user account whenever possible and use the built-in Administrator account only when absolutely necessary.

Perform the following steps to see how UAC affects administrator and nonadministrator accounts differently:

1. Log on to Windows 7 as a nonadministrator account.
2. Select Start ➢ Control Panel ➢ Large Icons View ➢ Windows Firewall.
3. Click the Turn Windows Firewall On Or Off link on the left side. The UAC box should prompt you for permission to continue, as shown in Figure 9.11. Click Yes. You should not be allowed access to the Windows Firewall Settings dialog box.

FIGURE 9.11
UAC dialog box

4. Log off and log on as the administrator account.
5. Select Start ➢ Control Panel ➢ Large Icons View ➢ Windows Firewall.

6. Click the Turn Windows Firewall On Or Off link.
7. You should automatically go to the Windows Firewall screen. Close the Windows Firewall screen

Now instead of just elevating privileges for users, let's look at elevating privileges for executable applications.

Elevated Privileges for Executables

You can also enable an executable file to run with elevated privileges. To do so on a one-time basis, you can right-click a shortcut or executable and select Run As Administrator.

But what if you need to configure an application to always run with elevated privileges for a user? To do so, log in as an administrator, right-click a shortcut or executable, and select Properties. On the Compatibility tab, click the Run This Program As An Administrator check box. If the Run This Program As An Administrator check box is unavailable, the program is blocked from permanently running as an administrator, the program doesn't need administrative privileges, or you are not logged on as an administrator.

Many applications that are installed on a Windows 7 machine need to have access to the Registry. Windows 7 protects the Registry from nonadministrator accounts. Let's look at how this works.

Registry and File Virtualization

Windows 7 uses a feature called Registry and file virtualization to enable nonadministrator users to run applications that previously required administrative privileges to run correctly. As discussed previously, some applications write to the Registry and to protected folders, such as `C:\Windows` and `C:\Program Files`. For nonadministrator users, Windows 7 redirects any attempts to write to protected locations to a per-user location. By doing so, Windows 7 enables users to use the application successfully while it protects critical areas of the system.

In the next section, we look at other areas of security such as Windows Firewall and the Action Center.

Using Advanced Security Options

In this section, we look at some of the advanced security options that you can configure to protect a Windows 7 machine. The first section discusses Windows Firewall and how to use the firewall to protect against intruders.

We then look at the Action Center, shown in Figure 9.12. The Action Center is designed to allow you to monitor and configure critical settings through a centralized dialog box. Critical settings include Automatic Updating, Malware Protection, and Other Security Settings. Malware Protection includes virus protection and spyware protection (included through Windows Defender).

Let's start by looking at how to configure and maintain Windows Firewall.

Configuring Windows Firewall

Windows Firewall, which is included with Windows 7, helps to prevent unauthorized users or malicious software from accessing your computer. Windows Firewall does not allow unsolicited traffic (traffic that was not sent in response to a request) to pass through the firewall.

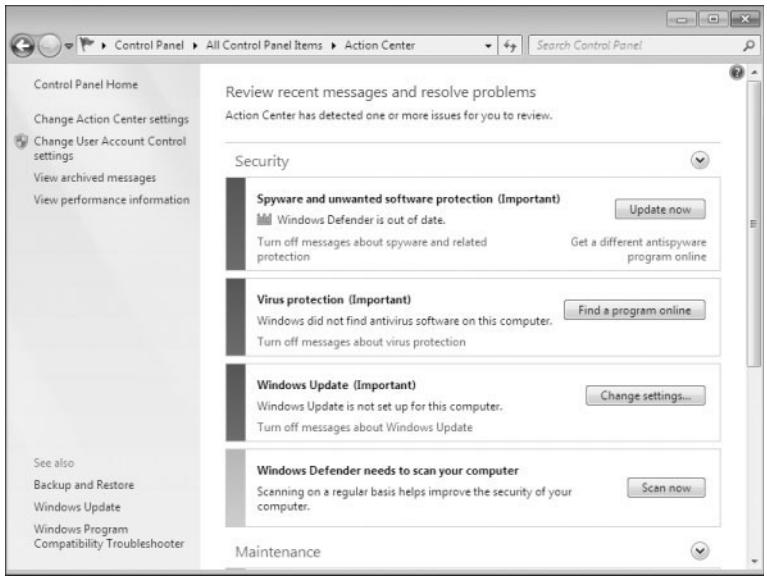


FIGURE 9.12
Windows Security Center dialog box

To configure Windows Firewall, select Start ➢ Control Panel ➢ Large Icons View ➢ Windows Firewall, then click Turn Windows Firewall On Or Off. The Windows Firewall Settings dialog box appears, as shown in Figure 9.13.

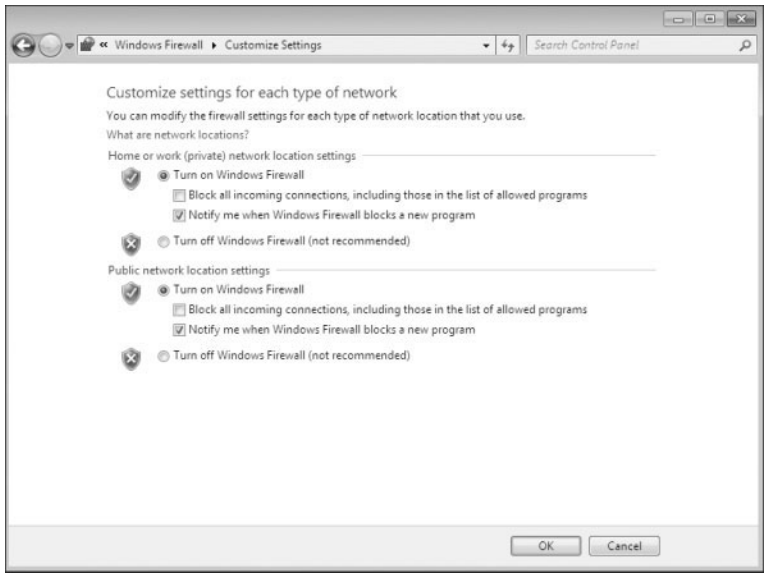


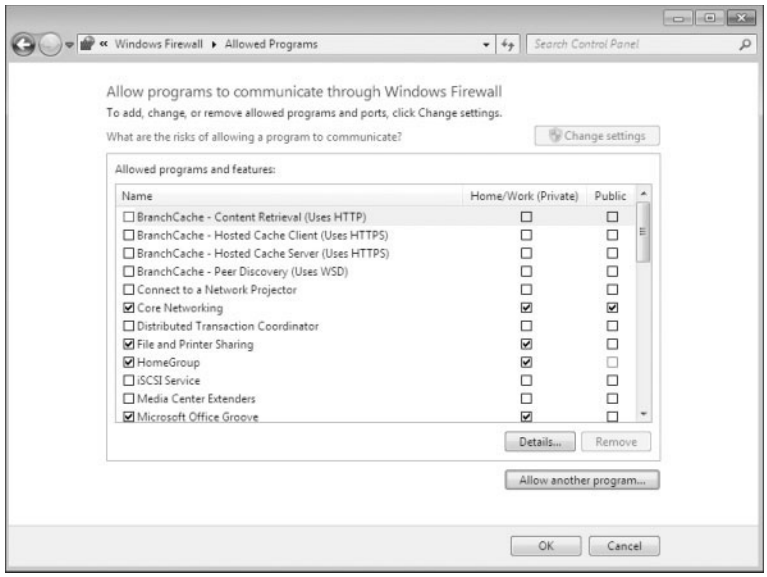
FIGURE 9.13
Windows Firewall Settings dialog box

The Windows Firewall Settings dialog box allows you to turn Windows Firewall on or off for both private and public networks. The On setting blocks external sources except those that are specified on the Exceptions tab. The Off setting allows external sources to connect.

There is also a check box for Block All Incoming Connections. This feature allows you to connect to networks that are not secure. When Block All Incoming Connections is enabled, exceptions are ignored and no notification is given when an application is blocked by Windows Firewall.

The exceptions section of the Windows Firewall Settings dialog box, shown in Figure 9.14, allows you to define which programs and services should be allowed to pass through Windows Firewall. You can select from a defined list of programs and services, or you can use the Add Another Program button to customize your exceptions.

FIGURE 9.14
Windows Firewall Allowed Programs dialog box



Take great care in enabling exceptions. Exceptions allow traffic to pass through the firewall, which could expose your computer to risk. Remember that the Block All Incoming Connections setting ignores all exceptions.

Now that we have looked at the basic Windows Firewall settings, let's discuss Windows Firewall with Advanced Security.

Windows Firewall with Advanced Security

You can configure more advanced settings by configuring Windows Firewall with Advanced Security (WFAS). To access Windows Firewall with Advanced Security, click Start ➢ Control Panel ➢ Large Icons View ➢ Windows Firewall and then click the Advanced Settings link. The Windows Firewall With Advanced Security On Local Computer dialog box appears, as shown in Figure 9.15.

The scope pane to the left shows that you can set up specific inbound and outbound rules, connection security rules, and monitoring rules. The central area shows an overview of the firewall's status, as well as the current profile settings. Let's look at these in detail.

Inbound and Outbound Rules

Inbound and outbound rules consist of many preconfigured rules that can be enabled or disabled. Obviously, inbound rules monitor inbound traffic, and outbound rules monitor

outbound traffic, as shown in Figure 9.16. By default, many are disabled. Double-clicking a rule brings up its Properties dialog box, as shown in Figure 9.17.

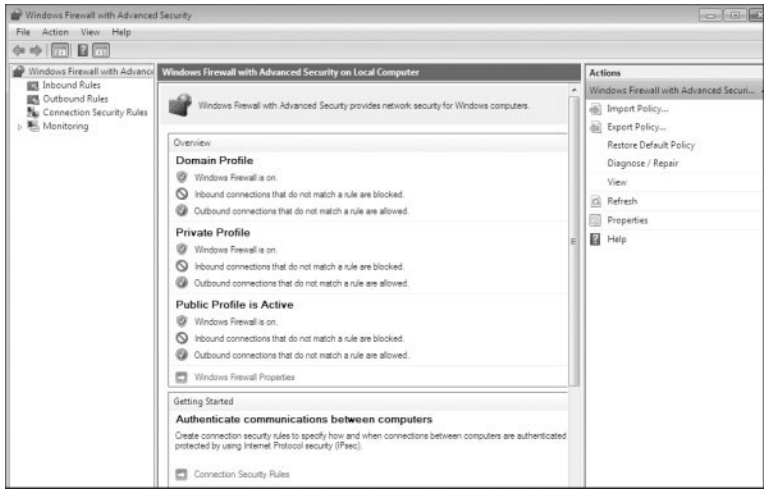


FIGURE 9.15
Windows Firewall With Advanced Security On Local Computer dialog box

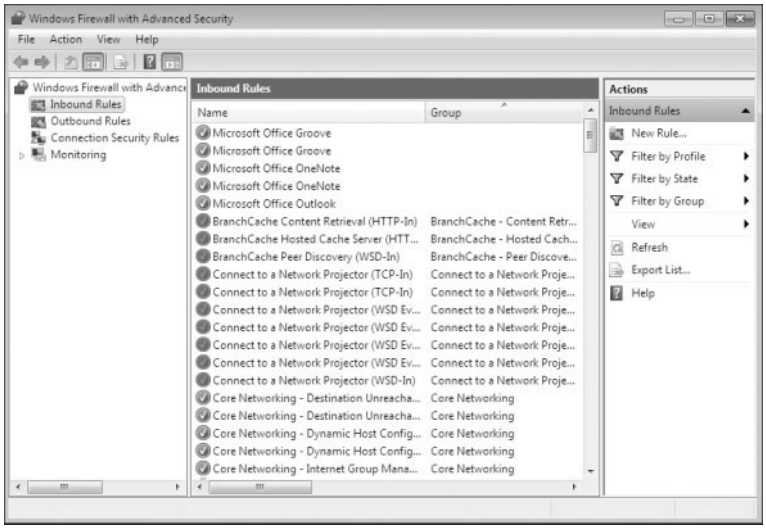


FIGURE 9.16
Inbound Rules dialog box

You can filter the rules to make them easier to view. Filtering can be performed based on the profile the rule affects, whether the rule is enabled or disabled, or based on the rule group.

If you can't find a rule that is appropriate for your needs, you can create a new rule by right-clicking Inbound Rules or Outbound Rules in the scope pane and then selecting New Rule. The New Inbound (or Outbound) Rule Wizard launches, and you are asked whether you want to create a rule based on a particular program, protocol or port, predefined category, or custom settings.

FIGURE 9.17
An inbound rule's Properties dialog box

Perform the following steps to create a new inbound rule that will allow only encrypted TCP traffic:

1. Select Start ➢ Control Panel ➢ Large Icon View ➢ Windows Firewall.
2. Click Advanced Settings on the left-hand side.
3. Right-click Inbound Rules and select New Rule.
4. Choose a Rule Type. For this exercise, let's choose Custom so that we can see all the options available to us; then click Next.
5. Choose the programs or services that are affected by this rule. For this exercise, let's choose All Programs; then click Next.
6. Choose the protocol type, as well as the local and remote port numbers that are affected by this rule. For this exercise, let's choose TCP, and ensure that All Ports is selected for both Local Port and Remote Port. Click Next to continue.
7. Choose the local and remote IP addresses that are affected by this rule. Let's choose Any IP Address for both local and remote, and then click Next.
8. Specify whether this rule will allow the connection, allow the connection only if it is secure, or block the connection. Let's select the option Allow The Connection If It Is Secure and then click Next.

9. Specify whether connections should be allowed only from certain users. You can experiment with these options if you want; then click Next to continue.
10. Specify whether connections should be allowed only from certain computers. Again you can experiment with these options if you want; then click Next to continue
11. Choose which profiles will be affected by this rule. Select one or more profiles and click Next to continue.
12. Give your profile a name and description and then click Finish. Your custom rule appears in the list of Inbound Rules and the rule is enabled.
13. Double-click your newly created rule. Notice that you can change the options that you previously configured.
14. Disable the rule by deselecting the Enabled check box. Click OK.

Now let's look at setting up Connection Security Rules through Windows Firewall with Advanced Security.

Connection Security Rules

You can use Connection Security Rules to configure how and when authentication occurs. These rules do not specifically allow connections; that's the job of inbound and outbound rules. You can configure the following connection security rules, as shown in Figure 9.18:

Isolation To restrict a connection based on authentication criteria

Authentication Exemption To specify computers that are exempt from authentication requirements

Server-to-Server To authenticate connections between computers

Tunnel To authenticate connections between gateway computers

Custom Allows you to provide a custom connection security rule.

The final section of Windows Firewall with Advanced Security we'll discuss is the Monitoring section.

Monitoring

The Monitoring section shows detailed information about the firewall configurations for the Domain Profile, Private Profile, and Public Profile settings, as shown in Figure 9.19. These network location profiles determine what settings are enforced for private networks, public networks, and networks connected to a domain.

Real World Scenario

Firewalls

When doing consulting, it always make me laugh when I see small to mid-size companies using Microsoft Windows Firewalls and no other protection.

Microsoft Windows Firewalls should be your *last* line of defense. You need to make sure that you have good hardware firewalls that separate your network from the world.

Also watch Windows Firewalls when it comes to printing. I have run into many situations where a printer that needs to talk to the operating system has issues when the Windows Firewall is enabled. If this happens, make sure that the printer is allowed in the allowed programs section.

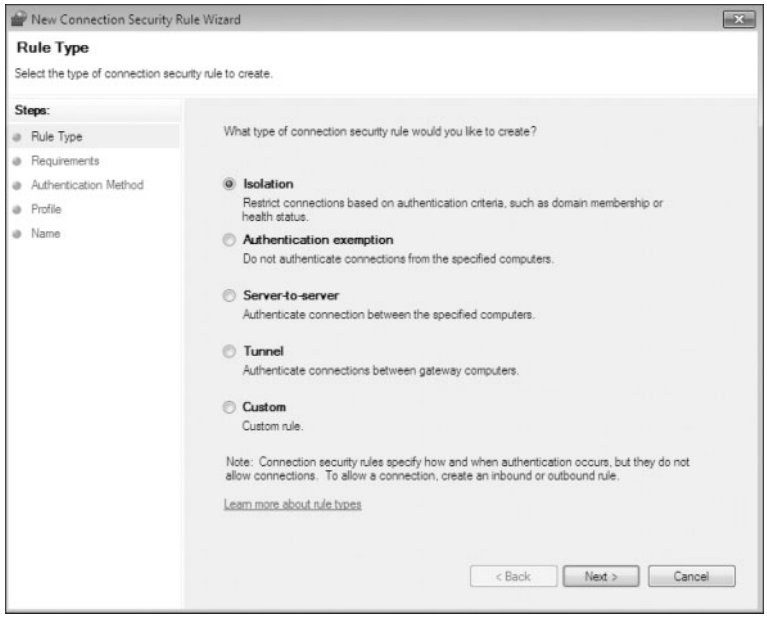


FIGURE 9.18
Connection security rules

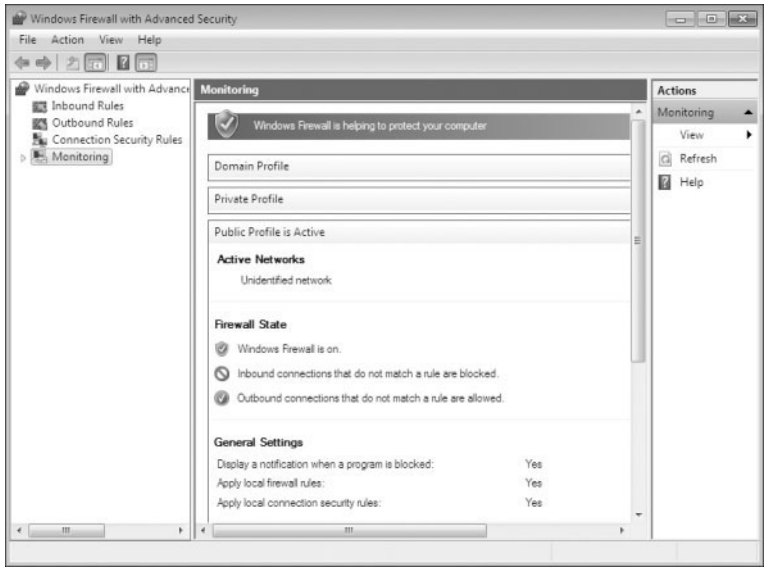


FIGURE 9.19
Monitoring section

In the next section we look at the Action Center and some of the functions that you can perform from the Action Center.

Configuring the Action Center

These days, having a firewall just isn't enough. Spyware and viruses are becoming more widespread, more sophisticated, and more dangerous. Users can unintentionally pick up spyware and viruses by visiting websites, or by installing an application in which spyware and viruses are bundled.

Even worse, malicious software cannot typically be uninstalled. Thus, antispyware and virus protection applications are also required to ensure that your computer remains protected. Let's take a look at some of the ways you can protect your Windows 7 computers using the Action Center.

Using Windows Defender

Windows 7 comes with an antispyware application called Windows Defender. Windows Defender offers real-time protection from spyware and other unwanted software. You can also configure Windows Defender to scan for spyware on a regular basis.

Like antivirus programs, Windows Defender relies on definitions, which are used to determine whether a file contains spyware. Out-of-date definitions can cause Windows Defender to fail to detect some spyware. Windows Update is used to regularly update the definitions used by Windows Defender so that the latest spyware can be detected. You can also configure Windows Defender to manually check for updates using Windows Update.

To access Windows Defender, as shown in Figure 9.20, click Start ➢ Control Panel ➢ Large Icons View ➢ Action Center ➢ Windows Defender. status appears at the bottom of the screen, which includes time of the last scan, the scan schedule, the real-time protection status, and the definition version.

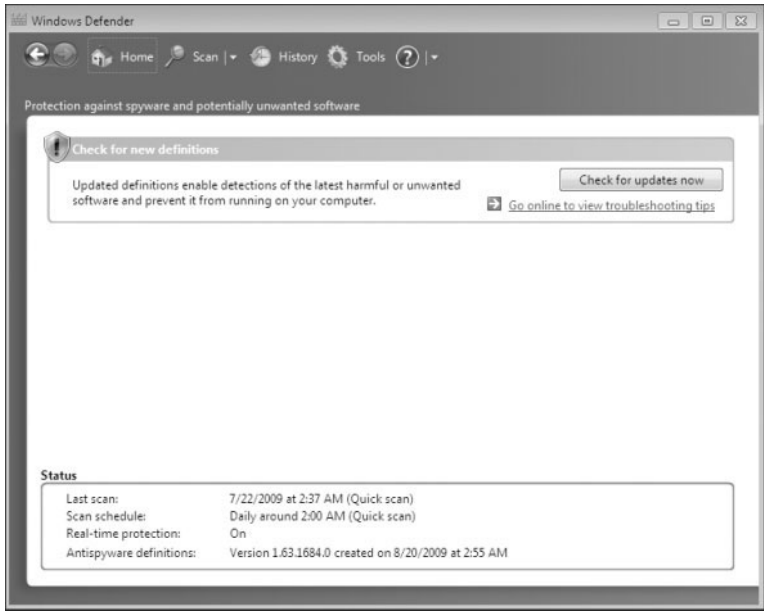


FIGURE 9.20
Windows Defender dialog box

Let's look at how we can scan the system for spyware using Windows Defender.

Performing a Manual Scan

You can configure Windows Defender to perform a manual scan of your computer at any time. You can perform the following three types of scans:

- Quick Scan checks only where spyware is most likely to be found.
- Full Scan checks all memory, running processes, and folders.
- Custom Scan checks only the drives and folders that you select.

By default, Windows Defender performs a Quick Scan daily at 2 a.m. You can change this setting by using the Tools menu option, as shown in Figure 9.21.

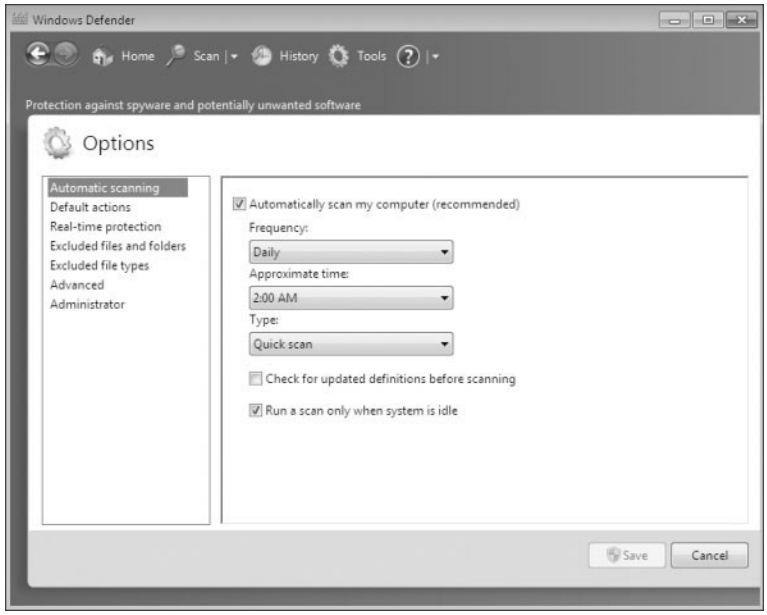


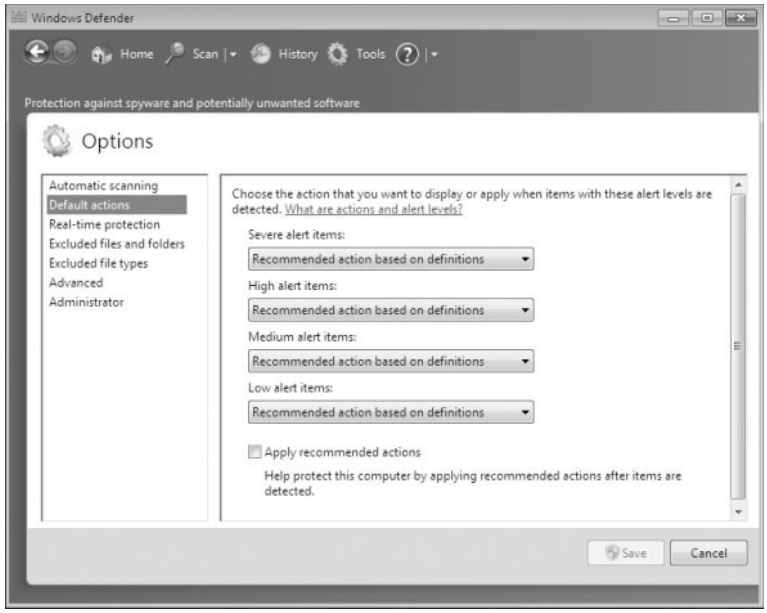
FIGURE 9.21
Windows Defender Tools menu dialog box

Programs are classified into four spyware alert levels, as shown in Figure 9.22:

- Severe
- High
- Medium
- Low

Depending on the alert level, you can choose to have Windows Defender ignore, quarantine, remove, or always allow software.

FIGURE 9.22
Spyware alert levels



In the next section, you will learn how to configure the many options of Windows Defender.

Configuring Windows Defender

Use the Tools and Settings menu to configure Windows Defender. As shown in Figure 9.23, you can access the following items through this menu:

- Options
- Microsoft SpyNet
- Quarantined Items
- Allowed Items
- Windows Defender Website
- Microsoft Malware Protection Center

Let's look at each one of these Windows Defender options in greater detail.

OPTIONS

Click Options on the Tools and Settings menu to enable you to configure the default behavior of Windows Defender. You can configure the following options:

Automatic Scanning You can configure Windows Defender to scan automatically, how often automatic scans should occur, the time that scans will occur, and the type of scan to perform.

You can also configure whether definitions should be updated before scanning, and whether the default actions should be taken on any spyware that is found.

Default Actions You can configure the actions Windows Defender should take on High, Medium, and Low Alert items. You can set each level so that Windows Defender can take the default action for that level, always remove the item, or always ignore the item.

Real-Time Protection You can configure whether real-time protection is enabled, which security agents you want to run, how you should be notified about threats, and whether a Windows Defender icon is displayed in the notification area.

Excluded Files And Folders You can set up files and folders that are to be excluded during a scan.

Excluded File Types You can specify certain file types that will be excluded from a scan, as shown in Figure 9.24. For example, you can exclude all `.doc` files if needed.

Advanced These options let you configure whether to:

- Archived files and folders are scanned.
- Email is scanned.
- Removable drives.
- Heuristics are used to detect unanalyzed software.
- A restore point is created before removing spyware.

You can also specify file locations that are exempt from scanning.

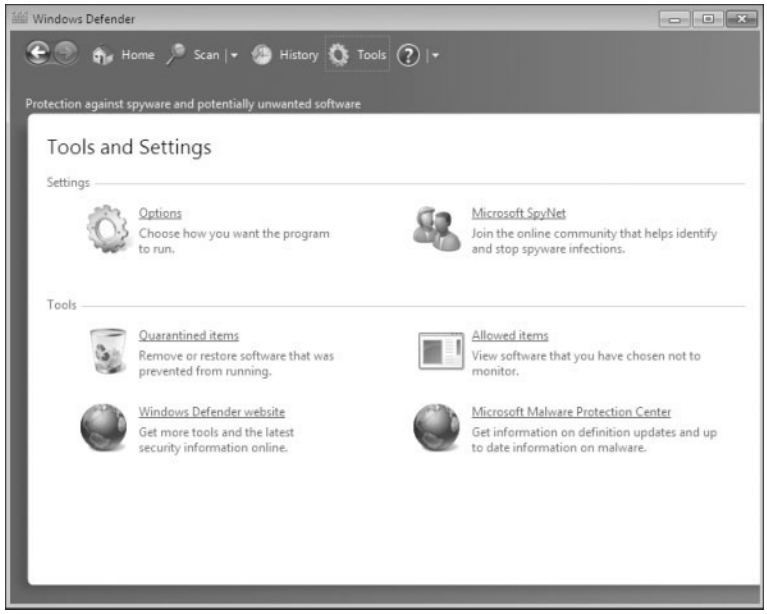
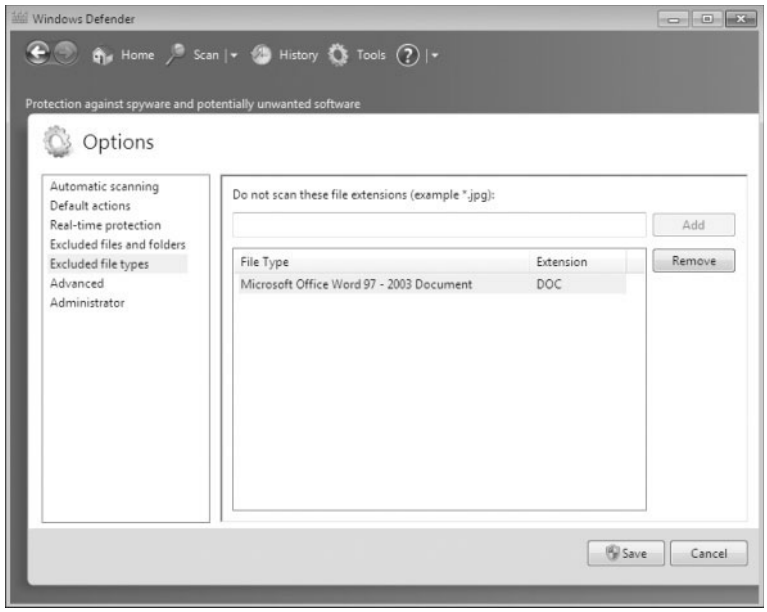


FIGURE 9.23
Windows Defender Tools and Settings menu

Administrator These options let you configure whether Windows Defender is enabled, and whether you display items from all users on this computer.

FIGURE 9.24
Excluded File Types



The next option that we look at from the Windows Defenders Tools is Microsoft SpyNet.

MICROSOFT SPYNET

Microsoft SpyNet is an online community that can help you know how others respond to software that has not yet been classified by Microsoft. Participation in SpyNet is voluntary, as shown in Figure 9.25, and subscription to SpyNet is free. If you choose to volunteer, your choices will be added to the community so that others can learn from your experiences.

To join the SpyNet community, click Microsoft SpyNet on the Tools menu, and then choose either a basic or advanced membership. The level of membership will specify how much information is sent to Microsoft when potentially unwanted software is found on your computer.

By default, I Do Not Want To join Microsoft SpyNet At This Time is selected, but you can choose to participate in SpyNet by selecting the appropriate radio button. If you choose not to participate, no information is sent to Microsoft, and Windows Defender does not alert you regarding unanalyzed software.

QUARANTINED ITEMS

Software that has been quarantined by Windows Defender is placed in Quarantined Items. Quarantined software will remain here until you remove it. If you find that a legitimate application is accidentally removed by Windows Defender, you can restore the application from Quarantined Items.

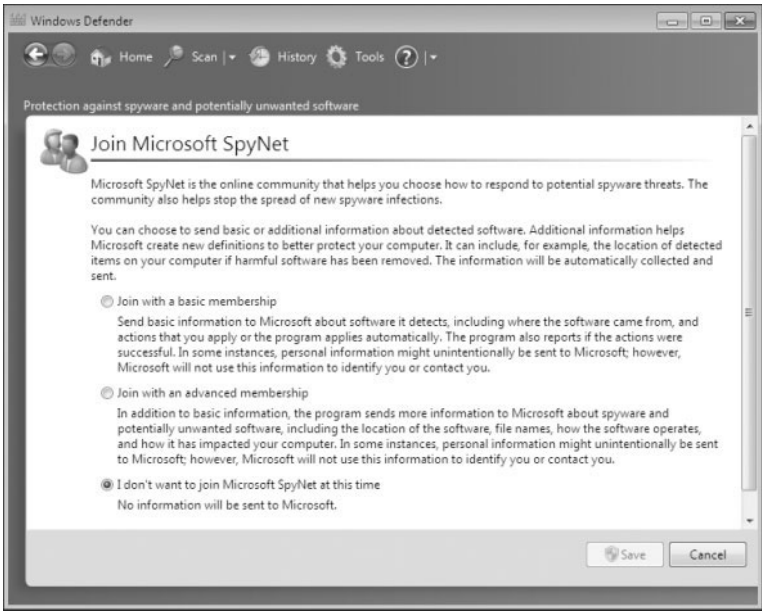


FIGURE 9.25
Microsoft SpyNet participation options

ALLOWED ITEMS

Software that has been marked as allowed is added to the Allowed Items list. Only trusted software should be added to this list. Windows Defender will not alert you regarding any software found on the Allowed Items list. If you find that a potentially dangerous application has been added to the Allowed Items list, you can remove it from the list so that Windows Defender can detect it.

WINDOWS DEFENDER WEBSITE

Clicking Windows Defender Website opens Internet Explorer and takes you to the Windows Defender website. Here you can find information on Windows Defender, spyware, and security.

MICROSOFT MALWARE PROTECTION CENTER

Clicking Microsoft Malware Protection Center opens Internet Explorer and takes you to the Malware Protection Center website. Here, you can find information on antimalware research and responses.

HISTORY MENU OPTION

There is also a History menu option next to the tools option. You can use the History menu option to see what actions have been taken by Windows Defender. Information is included about each application, the alert level, the action taken, the date, and the status. Information is retained until you click the Clear History button.

In the next section, we look at using Windows BitLocker Drive Encryption and how it can help you protect your hard drive.

Using BitLocker Drive Encryption

To prevent individuals from stealing your computer and viewing personal and sensitive data found on your hard disk, some editions of Windows 7 come with a new feature called BitLocker Drive Encryption. BitLocker encrypts the entire system drive. New files added to this drive are encrypted automatically, and files moved from this drive to another drive or computers are decrypted automatically.

Only Windows 7 Enterprise and Ultimate include BitLocker Drive Encryption and only the operating system drive (usually C:) or internal hard drives can be encrypted with BitLocker. Files on other types of drives must be encrypted using BitLocker To Go.

BitLocker uses a Trusted Platform Module (TPM) version 1.2 or higher to store the security key. A TPM is a chip that is found in newer computers. If you do not have a computer with a TPM, you can store the key on a removable USB drive. The USB drive will be required each time you start the computer so that the system drive can be decrypted.

If the TPM discovers a potential security risk, such as a disk error, or changes made to BIOS, hardware, system files, or startup components, the system drive will not be unlocked until you enter the 48-digit BitLocker recovery password or use a USB drive with a recovery key.

BitLocker Recovery Password

The BitLocker recovery password is very important. Do not lose it, or you may not be able to unlock the drive. Even if you do not have a TPM, be sure to keep your recovery password in case your USB drive becomes lost or corrupted.

BitLocker requires that you have a hard disk with at least two partitions, both formatted with NTFS. One partition will be the system partition that will be encrypted. The other partition will be the active partition that is used to start the computer; this partition will remain unencrypted.

In the next section, we look at two of the most important security features available: proper permissions and file and folder security.

Managing File and Folder Security

Setting up proper file and folder security is one of the most important tasks that an IT professional can perform. If permissions and security are not properly configured, users will be able to access resources that they shouldn't.

File and folder security defines what access a user has to local resources. You can limit access by applying security for files and folders. You should know what NTFS security permissions are and how they are applied.

A powerful feature of networking is the ability to allow network access to local folders. In Windows 7, it is easy to share folders. You can also apply security to shared folders in a manner that is similar to applying NTFS permissions. After you share a folder, users with appropriate access rights can access the folders through a variety of methods.

Before diving into the security section of folders, let's first look at some folder options.

Folder Options

The Windows 7 Folder Options dialog box allows you to configure many properties associated with files and folders, such as what you see when you access folders and how Windows

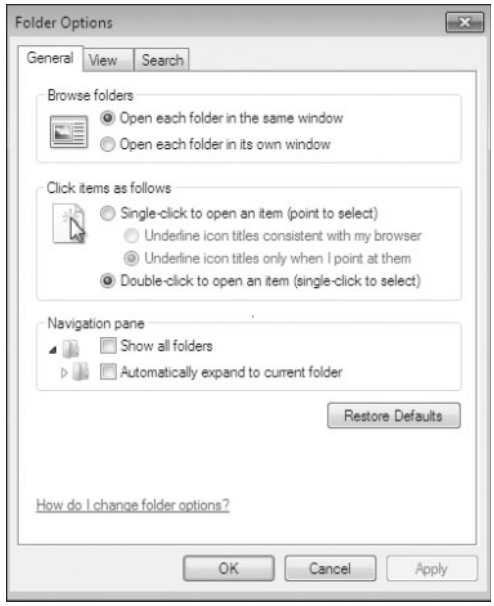
searches through files and folders. To open the Folder Options dialog box, click Start ➢ Computer, and then select Folder And Search Options under the Organize drop-down list. You can also access Folder Options by clicking its icon in Control Panel, selecting Large Icons View, and clicking Folder Options. The Folder Options dialog box has three tabs: General, View, and Search. The options on each of these tabs are described in the following sections.

Folder General Options

The General tab of the Folder Options dialog box, shown in Figure 9.26, includes the following options:

- Whether folders are opened all in the same window when a user is browsing folders or each folder is opened in a separate window
- Whether a user opens items with a single mouse click or a double-click
- A navigation pane that allows you to show all folders or automatically expand to the current folder

Figure 9.26
The General tab of the Folder Options dialog box



Folder View Options

The options on the View tab of the Folder Options dialog box, shown in Figure 9.27, are used to configure what users see when they open files and folders. For example, you can change the default setting so that hidden files and folders are displayed. Table 9.8 describes the View tab options.

FIGURE 9.27
The View tab of the Folder Options dialog box

TABLE 9.8: Folder View Options

OPTION	DESCRIPTION	DEFAULT VALUE
Always Show Icons, Never Thumbnails	Shows icons for files instead of thumbnail previews.	Not selected
Always Show Menus	Shows the File, Edit, View, Tools, and Help menus when browsing for files.	Not selected
Display File Icon On Thumbnails	Displays the file icon on thumbnails.	Enabled
Display File Size Information In Folder Tips	Specifies whether the file size is automatically displayed when you hover your mouse over a folder.	Enabled
Display The Full Path In The Title Bar (Classic Theme Only)	Specifies whether the title bar shows an abbreviated path of your location. Enabling this option displays the full path, such as `C:\Word Documents\Sybex\Windows 7 Book\Chapter 9` as opposed to showing an abbreviated path, such as `Chapter 9`.	Not selected
Hidden Files And Folders	Specifies whether files and folders with the Hidden attribute are listed. Choosing Show Hidden Files And Folders displays these items.	Do Not Show Hidden Files And Folders
Hide Empty Drives In The Computer Folder	This option will not display drives that are empty in the computer folder.	Enabled

TABLE 9.8: Folder View Options (*CONTINUED*)

OPTION	DESCRIPTION	DEFAULT VALUE
Hide Extensions For Known File Types	By default, filename extensions, which identify known file types (such as `.doc` for Word files and `.xls` for Excel files) are not shown. Disabling this option displays all filename extensions.	Enabled
Hide Protected Operating System Files (Recommended)	By default, operating system files are not shown, which protects operating system files from being modified or deleted by a user. Disabling this option displays the operating system files.	Enabled
Launch Folder Windows In A Separate Process	By default, when you open a folder, it shares memory with the previous folders that were opened. Enabling this option opens folders in separate parts of memory, which increases the stability of Windows 7 but can slightly decrease the performance of the computer.	Not selected
Show Drive Letters	Specifies whether drive letters are shown in the Computer folder. When disabled, only the name of the disk or device will be shown.	Enabled
Show Encrypted Or Compressed NTFS Files In Color	Displays encrypted or compressed files in an alternate color when they are displayed in a folder window.	Enabled
Show Pop-up Description For Folder And Desktop Items	Displays whether a pop-up tooltip is displayed when you hover your mouse over files and folders.	Enabled
Show Preview Handlers In Preview Pane	Shows the contents of files in the Preview pane.	Enabled
Use Check Boxes To Select Items	Adds a check box to each file and folder so that one or more of them may be selected. Actions can then be performed on selected items.	Not selected
Use Sharing Wizard (Recommended)	This option allows you to share a folder using a simplified sharing method.	Enabled
When Typing Into List View	Selects whether text is automatically typed into the search box or whether the typed item is selected in the view.	Select The Typed Item In The View

Search Options

You can use the Search tab of the Folder Options dialog box, shown in Figure 9.28, to configure how Windows 7 searches for files. You can choose for Windows 7 to search by filename only, by filenames and contents, or a combination of the two, depending on whether indexing is enabled. You can also select from the following options:

- Include Subfolders
- Find Partial Matches
- Use Natural Language Search
- Don't Use The Index When Searching the File System
- Include System Directories (in nonindexed locations)
- Include Compressed Files in Non-indexed Locations

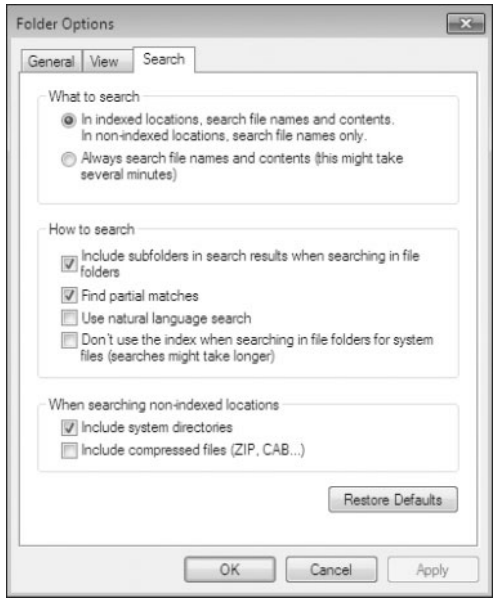


Figure 9.28
The Search tab of the Folder Options dialog box

To search for files and folders, click Start ➢ Search and type your query in the search box. In the next section we look at how to secure these folders and files.

Securing Access to Files and Folders

On NTFS partitions, you can specify the access each user has to specific folders or files on the partition, based on the user's logon name and group associations. Access control consists of rights and permissions. A right (also referred to as a privilege) is an authorization to perform a specific action.

Permissions are authorizations to perform specific operations on specific objects. The owner of an object or any user who has the necessary rights to modify permissions can apply permissions to NTFS objects. If permissions are not explicitly granted within NTFS, they are

implicitly denied. Permissions can also be explicitly denied, which then overrides explicitly granted permissions.

The following sections describe design goals for access control, as well as how to apply NTFS permissions and some techniques for optimizing local access. Let's look at design goals for setting up security.

Design Goals for Access Control

Before you start applying NTFS permissions to resources, you should develop design goals for access control as a part of your overall security strategy. Basic security strategy suggests that you provide each user and group with the minimum level of permissions needed for job functionality. Some of the considerations when planning access control include the following:

- Defining the resources that are included within your network — in this case, the files and folders residing on the file system
- Defining which resources will put your organization at risk; this includes defining the resources and defining the risk of damage if the resource was compromised
- Developing security strategies that address possible threats and minimize security risks
- Defining groups that security can be applied to based on users within the group membership who have common access requirements, and applying permissions to groups, as opposed to users
- Applying additional security settings through Group Policy, if your Windows 7 clients are part of an Active Directory network
- Using additional security features, such as EFS, to provide additional levels of security or file auditing to track access to critical files and folders

After you have decided what your design goals are, you can start applying your NTFS permissions.

Applying NTFS Permissions

NTFS permissions control access to NTFS files and folders. This is based on the technology that was originally developed for Windows NT. Ultimately, the person who owns the object has complete control over the object. You configure access by allowing or denying NTFS permissions to users and groups.

Normally, NTFS permissions are cumulative, based on group memberships if the user has been allowed access. This means that the user gets the highest level of security from all the different groups they belong to. However, if the user had been denied access through user or group membership, those permissions override the allowed permissions. Windows 7 offers the following six levels of NTFS permissions:

Full Control This permission allows the following rights:

- Traverse folders and execute files (programs) in the folders. The ability to traverse folders allows you to access files and folders in lower subdirectories, even if you do not have permissions to access specific portions of the directory path.
- List the contents of a folder and read the data in a folder's files.

- See a folder's or file's attributes.
- Change a folder's or file's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.
- Delete subfolders and files.
- Delete files.
- Compress files.
- Change permissions for files and folders.
- Take ownership of files and folders.

If you select the Full Control permission, all permissions will be checked by default and can't be unchecked.

Modify This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.
- Delete files.

If you select the Modify permission, the Read & Execute, List Folder Contents, Read, and Write permissions will be checked by default and can't be unchecked.

Read & Execute This permission allows the following rights:

- Traverse folders and execute files in the folders.
- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.

If you select the Read & Execute permission, the List Folder Contents and Read permissions will be checked by default and can't be unchecked.

List Folder Contents This permission allows the following rights:

- Traverse folders.
- List the contents of a folder.
- See a file's or folder's attributes.

Read This permission allows the following rights:

- List the contents of a folder and read the data in a folder's files.
- See a file's or folder's attributes.
- View ownership.

Write This permission allows the following rights:

- Overwrite a file.
- View file ownership and permissions.
- Change a file's or folder's attributes.
- Create new files and write data to the files.
- Create new folders and append data to the files.

Special Permissions This permission allows you to configure auditing, take ownership, and permissions beyond the normal permissions (for example, List or Traverse Folder).

Any user with Full Control access can manage the security of a folder. However, to access folders, a user must have physical access to the computer as well as a valid logon name and password. By default, regular users can't access folders over the network unless the folders have been shared. Sharing folders is covered in the ''Creating Shared Folders'' section later in this chapter.

To apply NTFS permissions, right-click the file or folder to which you want to control access, select Properties from the context menu, and then select the Security tab. The Security tab lists the users and groups that have been assigned permissions to the file or folder. When you click a user or group in the top half of the dialog box, you see the permissions that have been allowed or denied for that user or group in the bottom half.

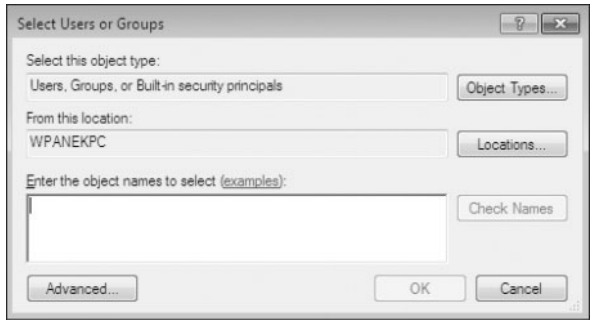
Perform the following steps to manage NTFS permission:

1. Right-click the file or folder to which you want to control access, select Properties from the context menu, and click the Security tab.
2. Click the Edit button to modify permissions.
3. Click the Add button to open the Select Users Or Groups dialog box, as shown in Figure 9.29. You can select users from the computer's local database or from the domain you are in (or trusted domains) by typing the user or group name in the Enter The Object Names To Select portion of the dialog box and clicking OK.
4. You return to the Security tab of the folder's Properties dialog box. Highlight a user or group in the top list box, and in the Permissions list, specify the NTFS permissions to be allowed or denied. When you have finished, click OK.

By clicking the Advanced button on the Security tab, you can configure more granular NTFS permissions, such as Traverse Folder and Read Attributes permissions.

To remove the NTFS permissions for a user, computer, or group, highlight that entity in the Security tab and click the Remove button. Be careful when you remove NTFS permissions. You won't be asked to confirm their removal, as you are when deleting most other types of items in Windows 7.

FIGURE 9.29
The Select Users Or Groups dialog box



Controlling Permission Inheritance

Normally, the directory structure is organized in a hierarchical manner. This means you are likely to have subfolders in the folders to which you apply permissions. In Windows 7, by default, the parent folder's permissions are applied to any files or subfolders in that folder, as well as any subsequently created objects. These are called inherited permissions.

You can specify how permissions are inherited by subfolders and files through the Advanced options from the Security tab of a folder's Properties dialog box by clicking the Advanced button. This calls up the Permissions tab of the Advanced Security Settings dialog box. To edit these options, click the Change Permissions button. The options can include the following:

- Include Inheritable Permissions From This Object's Parent
- Replace All Existing Inheritable Permissions On All Descendants With Inheritable Permissions From This Object

If an Allow or a Deny check box in the Permissions list on the Security tab has a shaded check mark, this indicates that the permission was inherited from an upper-level folder.

If the check mark is not shaded, it means the permission was applied at the selected folder. This is known as an explicitly assigned permission. Knowing which permissions are inherited and which are explicitly assigned is useful when you need to troubleshoot permissions.

Understanding Ownership and Security Descriptors

When an object is initially created on an NTFS partition, an associated security descriptor is created. A security descriptor contains the following information:

- The user or group that owns the object
- The users and groups that are allowed or denied access to the object
- The users and groups whose access to the object will be audited

After an object is created, the Creator owner of the object has full permissions to change the information in the security descriptor, even for members of the Administrators group. You can view the owner of an object from the Security tab of the specified folder's Properties and click the Advanced button. Then click the Owner tab to see who the owner of the object is. From this dialog box, you can change the owner of the object.

Although the owner of an object can set the permissions of an object so that the Administrator can't access the object, the Administrator or any member of the Administrators

group can take ownership of an object and thus manage the object's permissions. When you take ownership of an object, you can specify whether you want to replace the owner on subdirectories and objects of the object. If you would like to see who owns a directory from the command prompt, type **`dir /q`**.

Real World Scenario

USING THE TAKE OWNERSHIP OPTION

You are the administrator of a large network. The manager of the accounting department, Will, set up a series of files and folders with a high level of security. Will was the owner of these and all of the associated files and folders. When he set up NTFS security for his files and folders, he removed access for everyone, including the Administrators group. Will recently left the company, and Kevin has been hired to take over the accounting manager's job. When Kevin tries to access Will's files, he can't. When you log on as Administrator, you also can't access any of the files.

In this case, you should access the Owner tab of the parent folder for the files and folders and change the owner to Kevin. You should ensure that you check Replace Owner On Subcontainers And Objects, and Kevin will then have Full Control permissions to the resources.

In the next section, we discuss how to determine the effective permission of a file or folder.

Determining Effective Permissions

To determine a user's effective rights (the rights the user actually has to a file or folder), add all the permissions that have been allowed through the user's assignments based on that user's username and group associations. After you determine what the user is allowed, you subtract any permissions that have been denied the user through the username or group associations.

As an example, suppose that user Marilyn is a member of both the Accounting and Execs groups. The following assignments have been made to the Accounting group permissions:

Permission	Allow	Deny
Full Control		
Modify	X	
Read & Execute	X	
List Folder Contents		
Read		
Write		

The following assignments have been made to the Execs group permissions:

Permission	Allow	Deny
Full Control		
Modify		
Read & Execute		
List Folder Contents		
Read	X	
Write		

To determine Marilyn's effective rights, you combine the permissions that have been assigned. The result is that Marilyn's effective rights are Modify, Read & Execute, and Read so she basically has Modify (the highest right).

As another example, suppose that user Dan is a member of both the Sales and Temps groups. The following assignments have been made to the Sales group permissions:

Permission	Allow	Deny
Full Control		
Modify	X	
Read & Execute	X	
Permission	Allow	Deny
List Folder Contents	X	
Read	X	
Write	X	

The following assignments have been made to the Temps group permissions:

Permission	Allow	Deny
Full Control		
Modify		X
Read & Execute		
List Folder Contents		
Read		
Write		X

To determine Dan's effective rights, you start by seeing what Dan has been allowed: Modify, Read & Execute, List Folder Contents, Read, and Write permissions. You then remove anything that he is denied: Modify and Write permissions. In this case, Dan's effective rights are Read & Execute, List Folder Contents, and Read. Now let's see what rights users have.

Viewing Effective Permissions

If permissions have been applied at the user and group levels, and inheritance is involved, it can sometimes be confusing to determine what the effective permissions are. To help identify which effective permissions will actually be applied, you can view them from the Effective Permissions tab of Advanced Security Settings, or you can use the ICACLS command-line utility.

To see what the effective permissions are for a user or group, click the Select button and then type the user or group name. Then click OK. If a box is checked and not shaded, that means explicit permissions have been applied at that level. If the box is shaded, the permissions to that object were inherited.

The ICACLS command-line utility can also be used to display or modify user access rights. The options associated with the ICACLS command are as follows:

- `/grant` grants permissions.
- `/remove` revokes permissions.
- `/deny` denies permissions.
- `/setintegritylevel` sets an integrity level of Low, Medium, or High.

One issue that IT people run into is what happens to the security when you move or copy a file or folder. Let's look at NTFS permissions when moved or copied.

Determining NTFS Permissions for Copied or Moved Files

When you copy or move NTFS files, the permissions that have been set for those files might change. The following guidelines can be used to predict what will happen:

- If you move a file from one folder to another folder on the same volume, the file will retain the original NTFS permissions.
- If you move a file from one folder to another folder between different NTFS volumes, the file is treated as a copy and will have the same permissions as the destination folder.
- If you copy a file from one folder to another folder on the same volume or on a different volume, the file will have the same permissions as the destination folder.
- If you copy or move a file or folder to a FAT partition, it will not retain any NTFS permissions.

Now that we know how to deal with the NTFS security, let's look at shared permissions.

Managing Network Access

In every network, there are resources that the users need to gain access to. As IT professionals, we share these resources so that our users can do their jobs.

Sharing is the process of allowing network users access to a resource located on a computer. A network share provides a single location to manage shared data used by many users. Sharing also allows an administrator to install an application once, as opposed to installing it locally at each computer, and to manage the application from a single location.

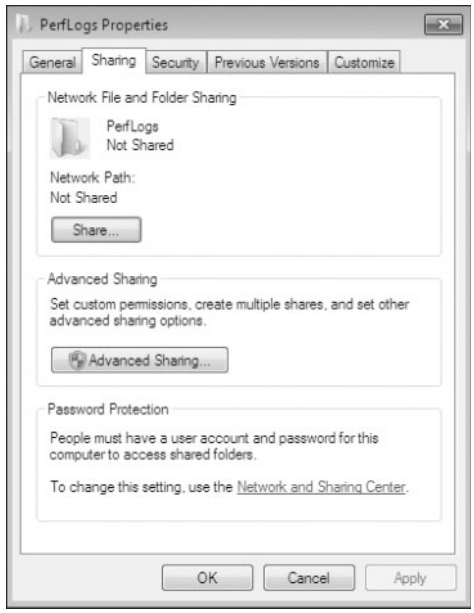
The following sections describe how to create and manage shared folders, configure share permissions, and provide access to shared resources.

Creating Shared Folders

You can share a folder in two ways. Right-click a folder and select Share to use the Sharing Wizard. If the Sharing Wizard feature is enabled, you will see the File Sharing screen. Here, you can add local users.

However, you cannot use the Sharing Wizard to share resources with domain users. To share a folder with domain users, you should right-click the folder and select Properties, and then select the Sharing tab, as shown in Figure 9.30.

FIGURE 9.30
The Sharing tab of a folder's PerfLogs Properties dialog box



Clicking the Share button takes you to the Sharing Wizard. To configure Advanced Sharing, click the Advanced Sharing button, which opens the Advanced Sharing dialog box. When you share a folder, you can configure the options listed in Table 9.9.

If you share a folder and then decide that you do not want to share it, just deselect the Share This Folder check box. You can easily tell that a folder has been shared by the group icon located at the bottom left of the folder icon. The following statements also hold true:

- Only folders, not files, can be shared.
- Share permissions can be applied only to folders and not to files.
- If a folder is shared over the network and a user is accessing it locally, then share permissions will not apply to the local user; only NTFS permissions will apply.
- If a shared folder is copied, the original folder will still be shared but not the copy.
- If a shared folder is moved, the folder will no longer be shared.
- If the shared folder will be accessed by a mixed environment of clients, including some that do not support long filenames, you should use the 8.3 naming format for files.
- Folders can be shared through the Net Share command-line utility.

TABLE 9.9: Share Folder Options

OPTION	DESCRIPTION
Share This Folder	Makes the folder available through local access and network access
Share Name	A descriptive name by which users will access the folder
Comments	Additional descriptive information about the share (optional)
Limit The Number Of Simultaneous Users To	The maximum number of connections to the share at any one time (no more than 10 users can simultaneously access a share on a Windows 7 computer)
Permissions	How users will access the folder over the network
Caching	How folders are cached when the folder is offline

Now let's look at configuring share permissions for your users.

Configuring Share Permissions

You can control users' access to shared folders by assigning share permissions. Share permissions are less complex than NTFS permissions and can be applied only to folders (unlike NTFS permissions, which can be applied to files and folders).

To assign share permissions, click the Permissions button in the Advanced Sharing dialog box. This brings up the Permissions For PerfLogs dialog box, as shown in Figure 9.31.

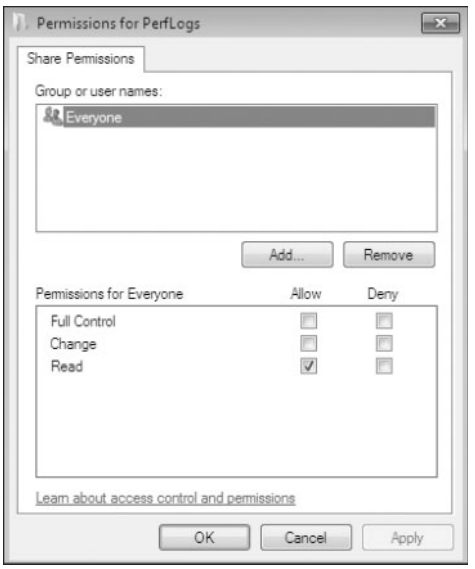


FIGURE 9.31
The Permissions For PerfLogs dialog box

You can assign the following three types of share permissions:

Full Control Allows full access to the shared folder.

Change Allows users to change data within a file or to delete files.

Read Allows a user to view and execute files in the shared folder. Read is the default permission on shared folders for the Everyone group.

Shared folders do not use the same concept of inheritance as NTFS folders. If you share a folder, there is no way to block access to lower-level resources through share permissions.

Combining Share and NTFS

When Share and NTFS permissions conflict, the most restrictive permissions apply. Remember that Share and NTFS permissions are both applied only when a user is accessing a shared resource over a network. Only NTFS permissions apply to a user accessing a resource locally.

So for example, if a user's NTFS security settings were Read Only on a resource and the Share permission was Full Control on that same resource, the user would have Read Only when they connect to that resource. The most restrictive set of permissions wins.

The Bottom Line

Understand Local Group Policy Objects. Local Group Policy Objects (LGPOs) are a set of security configuration settings that are applied to users and computers. LGPOs are created and stored on the Windows 7 computer.

If your Windows 7 computer is a part of a domain, which uses the services of Active Directory, then you typically manage and configure security through Group Policy Objects (GPOs). LGPOs are rules that can be placed on either users or computers.

> **Master It** You are the administrator for a large computer company. You need to make sure that all of the Windows 7 machines reset their passwords every 45 days. How can you accomplish this?

Understand User Account Control (UAC). User Account Control (UAC) enables nonadministrator users to perform standard tasks, such as install a printer, configure a VPN or wireless connection, and install updates, while preventing them from performing tasks that require administrative privileges, such as installing applications.

> **Master It** You are the administrator for a small plumbing company. You need to set 20 Windows 7 machines so that the users can always run applications with elevated privileges. How do you accomplish this goal?

Configure NTFS security. NTFS permissions control access to NTFS files and folders. The person who owns the object has complete control over the object. You configure access by allowing or denying NTFS permissions to users and groups.

NTFS permissions are cumulative, based on group memberships if the user has been allowed access. This means that the user gets the highest level of security from all the different groups they belong to. However, if the user had been denied access through user or group membership, those permissions override the allowed permissions.

Master It You are the administrator for a small organization that has decided to use NTFS on each Windows 7 machine. The company needs to make sure that all files and folders are secure. How do you make sure that all files and folders are secure on the Windows 7 NTFS drives?

Manage shared permissions. Sharing is the process of allowing network users access to a resource located on a computer. A network share provides a single location to manage shared data used by many users. Sharing also allows an administrator to install an application once, as opposed to installing it locally at each computer, and to manage the application from a single location.

Master It You are the administrator for a large computer company. You need everyone in the company to have access to the reports folder on Server A. How should you give everyone enough access to change and create reports?