

Managing User Access and Security

- Understanding User and Group Accounts **125**
- Managing User Account Control and Elevation Prompts **131**
- Managing Local Logon **137**
- Managing Stored Credentials **144**
- Managing Local User Accounts and Groups **149**
- Managing Remote Access to Workstations **159**

Computers running Windows 7 can be configured to be members of a home-group, a workgroup, or a domain. When a workstation is configured as a member of a homegroup or a workgroup, user access and security are configured on the workstation itself. When a workstation is configured as a member of a domain, user access and security are configured at two levels: the local system level and the domain level. User access can be configured at the local system level for a specific machine and at the domain level for multiple systems or resources throughout the current Active Directory forest. In this chapter, you'll learn how to manage local system access and local accounts. For further discussion of configuring domain access and permissions, see *Windows Server 2008 Administrator's Pocket Consultant*, Second Edition (Microsoft Press, 2010). Keep in mind that every task examined in this chapter and throughout this book can be performed through a local logon or a remote desktop connection.

Understanding User and Group Accounts

Windows 7 provides user accounts and group accounts (of which users can be members). User accounts are designed for individuals. Group accounts, usually referred to as *groups*, are designed to simplify the administration of multiple users. You can log on with a user account, but you can't log on with a group account.

Two general types of user accounts are defined in Windows 7:

- **Local user accounts** User accounts defined on a local computer are called *local user accounts*. These accounts have access to the local computer only. You add or remove local user accounts with Control Panel's User Accounts options or with the Local Users And Groups utility. Local Users And Groups is accessible through Computer Management, a Microsoft Management Console (MMC) snap-in.
- **Domain user accounts** User accounts defined in Active Directory are called *domain user accounts*. Through single sign-on, these accounts can access resources throughout a forest. When a computer is a member of an Active Directory domain, you can use it to create domain user accounts by using Active Directory Users And Computers. This MMC tool is available on the Administrative Tools menu when you install the Remote Server Administrator Tools on your Windows 7 computer.

Both local user accounts and domain user accounts can be configured as standard user accounts or administrator accounts. A standard user account on a local computer has limited privileges, and an administrator account on a local computer has extended privileges.

Local User Account Essentials

All user accounts are identified with a logon name. In Windows 7, this logon name has two parts:

- **User name** The display text for the account
- **User computer or domain** The computer or domain in which the user account exists

For the user Williams, whose account is created for the computer ENGPC85, the full logon name for Windows 7 is ENGPC85\Williams. With a local computer account, Williams can log on to his local workstation and access local resources but is not able to access domain resources.

When working with domains, the full logon name can be expressed in two different ways:

- The user account name and the full domain name separated by the At sign (@). For example, the full logon name for the user name Williams in the domain technology.microsoft.com would be *Williams@technology.microsoft.com*.
- The user account name and the domain separated by the backslash symbol (\). For example, the full logon name for Williams in the technology domain would be *technology\Williams*.

Although Windows 7 displays user names when describing account privileges and permissions, the key identifiers for accounts are security identifiers (SIDs). SIDs are unique identifiers generated when security principals are created. Each SID

combines a computer or domain security ID prefix with a unique relative ID for the user. Windows 7 uses these identifiers to track accounts and user names independently. SIDs serve many purposes, but the two most important are to enable you to easily change user names and to delete accounts without worrying that someone might gain access to resources simply by re-creating an account.

When you change a user name, you tell Windows 7 to map a particular SID to a new name. When you delete an account, you tell Windows 7 that a particular SID is no longer valid. Even if you create an account with the same user name later, the new account won't have the same privileges and permissions as the previous one because the new account will have a new SID.

User accounts can also have passwords and certificates associated with them. Passwords are authentication strings for an account. Certificates combine a public and private key to identify a user. You log on with a password interactively, whereas you log on with a certificate by using its private key, which is stored on a smart card and read with a smart card reader.

When you install Windows 7, the operating system installs default user accounts. You'll find several built-in accounts, which have purposes similar to those of accounts created in Windows domains. The key accounts are the following:

- **Administrator** Administrator is a predefined account that provides complete access to files, directories, services, and other facilities. You can't delete or disable this account. In Active Directory, the Administrator account has domainwide access and privileges. On a local workstation, the Administrator account has access only to the local system.
- **Guest** Guest is designed for users who need one-time or occasional access. Although guests have only limited system privileges, you should be very careful about using this account because it opens the system to potential security problems. The risk is so great that the account is initially disabled when you install Windows 7.

By default, these accounts are members of various groups. Before you modify any of the built-in accounts, you should note the property settings and group memberships for the account. Group membership grants or limits the account's access to specific system resources. For example, Administrator is a member of the Administrators group and Guest is a member of the Guests group. Being a member of a group makes it possible for the account to use the privileges and rights of the group.

In addition to the built-in accounts, Windows 7 has several pseudo-accounts that are used to perform specific types of system actions. The pseudo-accounts are available only on the local system. You can't change the settings for these accounts with the user administration tools, and users can't log on to a computer with these accounts. The pseudo-accounts available include the following:

- **LocalSystem** LocalSystem is used for running system processes and handling system-level tasks. This account grants the logon right Log On As

A Service. Most services run under the LocalSystem account. In some cases, these services have privileges to interact with the desktop. Services that need fewer privileges or logon rights run under the LocalService or NetworkService account. Services that run as LocalSystem include Background Intelligent Transfer Service, Computer Browser, Group Policy Client, Netlogon, Network Connections, Print Spooler, and User Profile Service.

- **LocalService** LocalService is used for running services that need fewer privileges and logon rights on a local system. By default, services that run under this account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Change The System Time, Change The Time Zone, Generate Security Audits, and Replace A Process Level Token. Services that run as LocalService include Application Layer Gateway Service, Remote Registry, Smart Card, SSDP Discovery Service, TCP/IP NetBIOS Helper, and WebClient.
- **NetworkService** NetworkService is used for running services that need fewer privileges and logon rights on a local system but must also access network resources. Like services that run under LocalService, services that run by default under the NetworkService account are granted the right Log On As A Service and the privileges Adjust Memory Quotas For A Process, Generate Security Audits, and Replace A Process Level Token. Services that run under NetworkService include BranchCache, Distributed Transaction Coordinator, DNS Client, Remote Desktop Services, and Remote Procedure Call (RPC). NetworkService can also authenticate to remote systems as the computer account.

Group Account Essentials

Windows 7 also provides groups, which you use to grant permissions to similar types of users and to simplify account administration. If a user is a member of a group that has access to a resource, that user has access to the same resource. You can give a user access to various work-related resources just by making the user a member of the correct group. Although you can log on to a computer with a user account, you can't log on to a computer with a group account. Because different Active Directory domains or local computers might have groups with the same name, groups are often referred to by *Domain\GroupName* or *Computer\GroupName* (for example, Technology\GMarketing for the GMarketing group in a domain or on a computer named Technology).

Windows 7 uses the following three types of groups:

- **Local groups** Defined on a local computer and used on the local computer only. You create local groups with Local Users And Groups.
- **Security groups** Can have security descriptors associated with them. You use a Windows server to define security groups in domains, using Active Directory Users And Computers.

- **Distribution groups** Used as e-mail distribution lists. They can't have security descriptors associated with them. You define distribution groups in domains using Active Directory Users And Computers.

As with user accounts, group accounts are tracked using unique SIDs. This means that you can't delete a group account and re-create it and then expect that all the permissions and privileges remain the same. The new group will have a new SID, and all the permissions and privileges of the old group will be lost.

When you assign user access levels, you have the opportunity to make the user a member of the following built-in or predefined groups:

- **Administrators** Members of this group are local administrators and have complete access to the workstation. They can create accounts, modify group membership, install printers, manage shared resources, and more. Because this account has complete access, you should be very careful about which users you add to this group.

- **Backup Operators** Members of this group can back up and restore files and directories on the workstation. They can log on to the local computer, back up or restore files, and shut down the computer. Because of how this account is set up, its members can back up files regardless of whether the members have read/write access to the files. However, they can't change access permissions on the files or perform other administrative tasks.

Backup Operators have privileges to perform very specific administrative tasks, such as backing up file systems. By default, no other group or user accounts are members of the operator groups. This is to ensure that you grant explicit access to the operator groups.

- **Cryptographic Operators** Members can manage the configuration of encryption, IP Security (IPSec), digital IDs, and certificates.
- **Event Log Readers** Members can view the event logs on the local computer.
- **Guests** Guests are users with very limited privileges. Members can access the system and its resources remotely, but they can't perform most other tasks.
- **Network Configuration Operators** Members can manage network settings on the workstation. They can also configure TCP/IP settings and perform other general network configuration tasks.
- **Performance Log Users** Members can view and manage performance counters. They can also manage performance logging.
- **Performance Monitor Users** Members can view performance counters and performance logs.
- **Power Users** In earlier versions of Windows, this group is used to grant additional privileges, such as the capability to modify computer settings and install programs. In Windows 7, this group is maintained only for compatibility with legacy applications.

- **Remote Desktop Users** Members can log on to the workstation remotely using Remote Desktop Services. Once members are logged on, additional groups of which they are members determine their permissions on the workstation. A user who is a member of the Administrators group is granted this privilege automatically. (However, remote logons must be enabled before an administrator can remotely log on to a workstation.)
- **Replicator** Members can manage the replication of files for the local machine. File replication is primarily used with Active Directory domains and Windows servers.
- **Users** Users are people who do most of their work on a single Windows 7 workstation. Members of the Users group have more restrictions than privileges. They can log on to a Windows 7 workstation locally, keep a local profile, lock the workstation, and shut down the workstation.

In most cases, you configure user access by using the Users or Administrators group. You can configure user and administrator access levels by setting the account type to Standard User or Administrator, respectively. While these basic tasks can be performed using Control Panel's User Accounts page, you make a user a member of a group by using Local Users And Groups under Computer Management.

Domain vs. Local Logon

When computers are members of a domain, you typically use domain accounts to log on to computers and the domain. All administrators in a domain have access to resources on the local workstations that are members of the domain. Users, on the other hand, can access resources only on the local workstations they are permitted to log on to. In a domain, any user with a valid domain account can by default log on to any computer that is a member of the domain. Once logged on to a computer, the user has access to any resource that his or her account or the groups to which the user's account belongs are granted access. This includes resources on the local machine as well as resources in the domain.

You can restrict logons to specific domain workstations on a per-user basis by using Active Directory Users And Computers. In Active Directory Users And Computers, right-click the user account and then click Properties. On the Account tab of the user's Properties dialog box, click Log On To, and then use the options in the Logon Workstations dialog box to designate the workstations to which the user is permitted to log on.

When you work with Windows 7, however, you aren't always logging on to a domain. Computers configured in workgroups have only local accounts. You might also need to log on locally to a domain computer to administer it. Only users with a local user account can log on locally. When you log on locally, you have access to any resource on the computer that your account or the groups to which your account belongs are granted access.

Managing User Account Control and Elevation Prompts

User Account Control (UAC) represents a significant change in the way in which user accounts are used and configured. It affects which privileges standard users and administrator users have, how applications are installed and run, and much more. In this section, I'll extend the discussion in Chapter 1, "Introduction to Windows 7 Administration," and provide a comprehensive look at how UAC affects user and administrator accounts. This is essential information to know when managing Windows 7 systems.

NOTE Learning how UAC works will help you be a better administrator. To support UAC, many aspects of the Windows operating system had to be reworked. Some of the most extensive changes have to do with how applications are installed and run. In Chapter 9, "Installing and Maintaining Programs," you'll find a complete discussion of how the architectural changes affect programs running on Windows 7.

Redefining Standard User and Administrator User Accounts

In Windows XP and earlier versions of Windows, malicious software programs can exploit the fact that most user accounts are configured as members of the local computer's Administrators group. Not only does this allow malicious software to install itself, but it also allows malicious software to use these elevated privileges to wreak havoc on the computer, because programs installed by administrators can write to otherwise secure areas of the registry and the file system.

To combat the growing threat of malicious software, organizations have locked down computers, required users to log on using standard user accounts, and required administrators to use the Run As command to perform administrative tasks. Unfortunately, these procedural changes can have serious negative consequences on productivity. A person logged on as a standard user under Windows XP can't perform some of the most basic tasks, such as changing the system clock and calendar, changing the computer's time zone, or changing the computer's power management settings. Many software programs designed for Windows XP simply will not function properly without local administrator rights—these programs use local administrator rights to write to system locations during installation and during normal operations. Additionally, Windows XP doesn't let you know beforehand when a task you are performing requires administrator privileges.

UAC seeks to improve usability while at the same time enhancing security by redefining how standard user and administrator user accounts are used. UAC represents a fundamental shift in computing by providing a framework that limits the scope of administrator-level access privileges and requires all applications to run in a specific user mode. In this way, UAC prevents users from making inadvertent changes to system settings and locks down the computer to prevent unauthorized applications from being installed or performing malicious actions.

Because of UAC, Windows 7 defines two levels of user accounts: standard and administrator. Windows 7 also defines two modes (run levels) for applications: standard user mode and administrator mode. Although standard user accounts can use most software and can change system settings that do not affect other users or the security of the computer, administrator user accounts have complete access to the computer and can make any changes that are needed. When an administrator user starts an application, her access token and its associated administrator privileges are applied to the application, giving her all the rights and privileges of a local computer administrator for that application. When a standard user starts an application, her access token and its associated privileges are applied to the application at run time, limiting her to the rights and privileges of a standard user for that application. Further, all applications are configured to run in a specific mode during installation. Any tasks run by standard-mode applications that require administrator privileges not only are identified during setup but require user approval to run.

In Windows 7, the set of privileges assigned to standard user accounts has changed. Tasks that standard user accounts can perform include:

- Installing fonts, viewing the system clock and calendar, and changing the time zone.
- Changing the display settings and the power management settings.
- Adding printers and other devices (when the required drivers are installed on the computer or are provided by an IT administrator).
- Downloading and installing updates (when the updates use UAC-compatible installers).
- Creating and configuring virtual private network (VPN) connections. VPN connections are used to establish secure connections to private networks over the public Internet.
- Installing Wired Equivalent Privacy (WEP) to connect to secure wireless networks. The WEP security protocol provides wireless networks with improved security.

Windows 7 also defines two run levels for applications: standard and administrator. Windows 7 determines whether a user needs elevated privileges to run a program by supplying most applications and processes with a security token. If an application has a standard token, or an application cannot be identified as an administrator application, elevated privileges are not required to run the application, and Windows 7 starts it as a standard application by default. If an application has an administrator token, elevated privileges are required to run the application, and Windows 7 prompts the user for permission or confirmation prior to running the application.

The process of getting approval prior to running an application in administrator mode and prior to performing tasks that change system configuration is known as *elevation*. Elevation enhances security and reduces the impact of malicious software

by notifying users before they perform any action that could impact system settings and by preventing applications from using administrator privileges without first notifying users. Elevation also protects administrator applications from attacks by standard applications. For more information on elevation and how UAC works with applications, see Chapter 9.

By default, Windows 7 switches to the secure desktop prior to displaying the elevation prompt. The secure desktop restricts the programs and processes that have access to the desktop environment, and in this way reduces the possibility that a malicious program or user could gain access to the process being elevated. If you don't want Windows 7 to switch to the secure desktop prior to prompting for elevation, you can choose settings that use the standard desktop rather than the secure desktop. However, this makes the computer more susceptible to malware and attack.

Optimizing User Account Control and Admin Approval Mode

Every computer has a built-in local Administrator account. This built-in account is not protected by UAC, and using this account for administration can put your computer at risk. To safeguard computers in environments in which you use a local Administrator account for administration, you should create a new local Administrator account and use this account for administration.

UAC can be configured or disabled for any individual user account. If you disable UAC for a user account, you lose the additional security protections UAC offers and put the computer at risk. To completely disable UAC or to reenable UAC after disabling it, the computer must be restarted for the change to take effect.

Admin Approval Mode is the key component of UAC that determines whether and how administrators are prompted when running administrator applications. The default way that Admin Approval Mode works is as follows:

- All administrators, including the built-in local Administrator account, run in and are subject to Admin Approval Mode.
- Because they are running in and subject to Admin Approval Mode, all administrators, including the built-in local Administrator account, see the elevation prompt when they run administrator applications.

If you are logged on as an administrator, you can modify the way UAC works for all users by completing the following steps:

1. In Control Panel, click System And Security. Under the Action Center heading, click Change User Account Control Settings.
2. On the User Account Control Settings page, shown in Figure 5-1, use the slider to choose when to be notified about changes to the computer, and then click OK. Table 5-1 summarizes the available options.

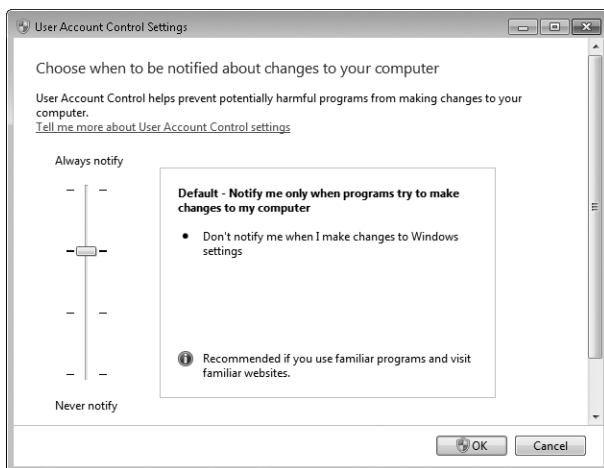


FIGURE 5-1 The User Account Control Settings page

TABLE 5-1 User Account Control Settings

OPTION	DESCRIPTION	WHEN TO USE	USES THE SECURE DESKTOP?
Always Notify	Always notifies the current user when programs try to install software or make changes to the computer and when the user changes Windows settings.	Choose this option when a computer requires the highest security possible and users frequently install software and visit unfamiliar Web sites.	Yes
Default	Notifies the current user only when programs try to make changes to the computer and not when the user changes Windows settings.	Choose this option when a computer requires high security and you want to reduce the number of notification prompts that users see.	Yes
Notify Me Only When ... (Do Not Dim My Desktop)	Same as Default but also prevents UAC from switching to the secure desktop.	Choose this option when users work in a trusted environment with familiar applications and do not visit unfamiliar Web sites.	No

OPTION	DESCRIPTION	WHEN TO USE	USES THE SECURE DESKTOP?
Never Notify	Turns off all UAC notification prompts.	Choose this option when security is not a priority and users work in a trusted environment with programs that are not certified for Windows 7 because they do not support UAC.	No

In Group Policy, you can manage Admin Approval Mode and elevation prompting by using settings under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options. These security settings are:

- **User Account Control: Admin Approval Mode For The Built-In Administrator Account** Determines whether users and processes running as the built-in local Administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means the built-in local Administrator account is subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users and processes running as the built-in local administrator are not subject to Admin Approval Mode and therefore not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.
- **User Account Control: Allow UIAccess Applications To Prompt For Elevation Without Using The Secure Desktop** Determines whether User Interface Accessibility (UIAccess) programs can automatically disable the secure desktop for elevation prompts used by a standard user. If you enable this setting, UIAccess programs, including Windows Remote Assistance, can disable the secure desktop for elevation prompts.
- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** Determines whether administrators subject to Admin Approval Mode see an elevation prompt when running administrator applications, and also determines how the elevation prompt works. By default, administrators are prompted for consent when running administrator applications on the secure desktop. You can configure this option so that administrators are prompted for consent without the secure desktop, prompted for credentials with or without the secure desktop (as is the case with standard users), or prompted for consent only for non-Windows binaries. You can also configure this option so that administrators are not prompted at all, in which case an administrator will be elevated automatically. No setting will prevent an administrator from right-clicking an application shortcut and selecting Run As Administrator.

- **User Account Control: Behavior Of The Elevation Prompt For Standard Users** Determines whether users logged on with a standard user account see an elevation prompt when running administrator applications. By default, users logged on with a standard user account are prompted for the credentials of an administrator on the secure desktop when running administrator applications or performing administrator tasks. You can also configure this option so that users are prompted for credentials on the standard desktop rather than the secure desktop, or you can deny elevation requests automatically, in which case users will not be able to elevate their privileges by supplying administrator credentials. The latter option doesn't prevent users from right-clicking an application shortcut and selecting Run As Administrator.
- **User Account Control: Run All Administrators In Admin Approval Mode** Determines whether users logged on with an administrator account are subject to Admin Approval Mode. By default, this feature is enabled, which means administrators are subject to Admin Approval Mode and also subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode. If you disable this setting, users logged on with an administrator account are not subject to Admin Approval and therefore are not subject to the elevation prompt behavior stipulated for administrators in Admin Approval Mode.
- **User Account Control: Only Elevate UIAccess Applications That Are Installed in Secure Locations** Determines whether UIAccess programs must reside in a secure location on the file system to elevate. If enabled, UIAccess programs must reside in a secure location under %SystemRoot%\Program Files, %SystemRoot%\Program Files(x86), or %SystemRoot%\Windows\System32.
- **User Account Control: Only Elevate Executables That Are Signed And Validated** Determines whether applications must be signed and validated to elevate. If enabled, only executables that pass signature checks and have certificates in the Trusted Publisher store will elevate. Use this option only when the highest security is required and you've verified that all applications in use are signed and valid.

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure these settings on a per-computer basis using local security policy. To do this, follow these steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Local Security Policy.
2. In the Local Security Policy console tree, under Security Settings, expand Local Policies, and then select Security Options, as shown in Figure 5-2.

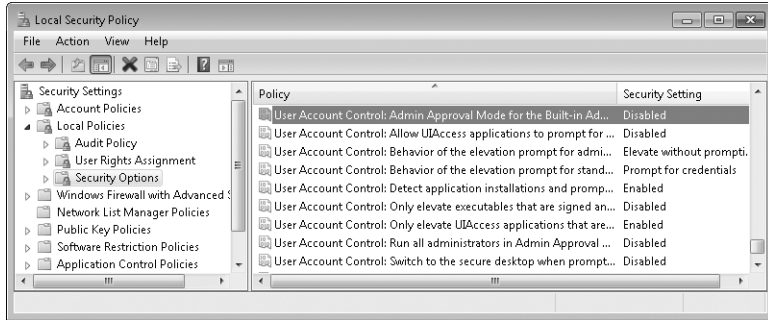


FIGURE 5-2 The Local Security Policy console

3. Double-click the setting you want to work with, make any necessary changes, and then click OK. Repeat this step to modify other security settings as necessary.

Managing Local Logon

All local computer accounts should have passwords. If an account is created without a password, anyone can log on to the account, and there is no protection for the account. However, a local account without a password cannot be used to remotely access a computer.

The sections that follow discuss how to create and work with local user accounts. Every workstation computer has local computer accounts, whether the computer is a member of a homegroup, a workgroup, or a domain.

Creating Local User Accounts in a Homegroup or Workgroup

For a computer that is a member of a homegroup or a workgroup, you can create a local user account by following these steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
As Figure 5-3 shows, the Manage Accounts page lists all configurable user accounts on the local computer by account type and with configuration details. If an account has a password, it is labeled Password Protected. If an account is disabled, it is listed as being off.
2. Click Create A New Account. This displays the Create New Account page.
3. Type the name of the local account. This name is displayed on the Welcome screen and Start menu.
4. Set the type of account as either Standard User or Administrator. To give the user full permissions on the local computer, select Administrator.
5. Click Create Account.

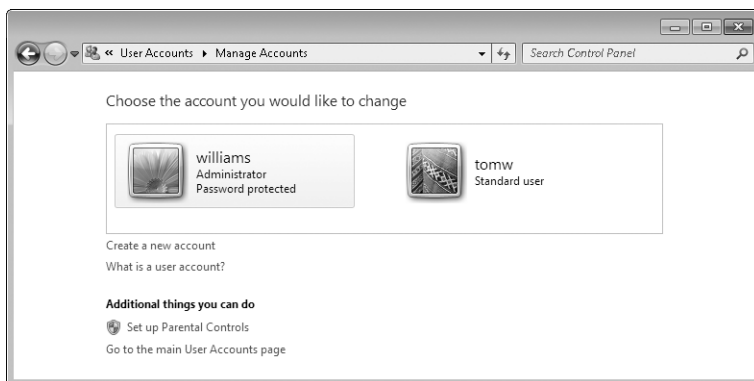


FIGURE 5-3 In a homegroup or workgroup, use the Manage Accounts page in Control Panel to add or remove local user accounts.

Granting Access to an Existing Domain Account to Allow Local Login

If a user needs to be able to log on locally to a computer and has an existing domain account, you can grant the user permission to log on locally by completing the following steps:

1. In Control Panel, under the User Accounts heading, click the Change Account Type link. This displays the User Accounts dialog box. As Figure 5-4 shows, the User Accounts dialog box lists all configurable user accounts on the local computer by domain and with group membership details.

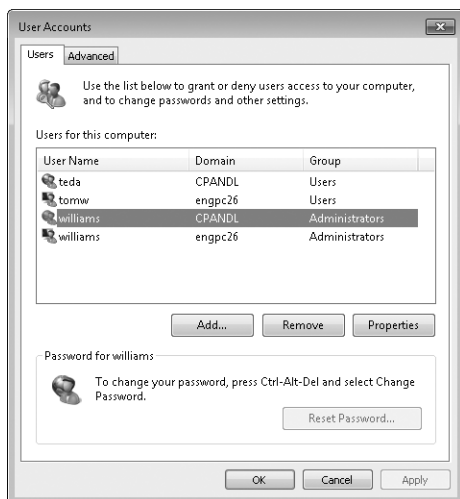


FIGURE 5-4 Use the User Accounts dialog box to manage local user accounts on a computer that is a member of a domain.

2. Click Add. This starts the Add New User wizard.
3. You are creating a local computer account for a user with an existing domain account. Type the user's domain account name and domain in the fields provided.
4. Using the options provided, select the type of user account.
5. A standard user account is created as a member of the local Users group. To give the user the permissions of a normal user, select Standard User.
6. An administrator account is created as a member of the local Administrators group. To give the user full permissions on the local computer, select Administrator.
7. An Other account is created as a member of a group you specify. To give the user the permissions of a specific group, select Other, and then select the group.
8. Click Finish. If you need to set other permissions or add the user to other local groups, follow the steps specified in the section "Managing Local User Accounts and Groups."

Changing Local User Account Types

The User Accounts utility provides an easy way to change account types for local users. You can also quickly set one of the default account types. For more advanced control, however, you need to use Local Users And Groups to assign group membership to individual accounts. (See the section "Adding and Removing Local Group Members.")

In a homegroup or workgroup, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to change, and then click Change The Account Type.
3. On the Change Account Type page, set the level of access for the user as either Standard User or Administrator, and then click Change The Account Type.

In a domain, you can change the account type for a local computer user by completing the following steps:

1. In Control Panel, click User Accounts. On the User Accounts page, click Change Account Type. This displays the User Accounts dialog box.
2. On the Users tab, click the user account you want to work with, and then click Properties.
3. In the Properties dialog box, click the Group Membership tab.

4. Set the type of account as Standard User or Administrator, or select Other and then select the group you want to use.
5. Click OK twice.

Creating Passwords for Local User Accounts

In a homegroup or workgroup configuration, local user accounts are created without passwords by default. This means that a user can log on simply by clicking his account name on the Welcome screen or by clicking OK on the classic Log On To Windows screen. To improve security, all local accounts should have passwords.

For the easiest management of local accounts, log on to each account that should have a password, and then use the User Accounts utility to assign a password to the account. If you are logged on as the user when you create a password, you don't have to worry about losing encrypted data. If you create a password without logging on as the user, the user will lose access to his or her encrypted files, encrypted e-mail, personal certificates, and stored passwords. This occurs because the user's master key, which is needed to access his or her personal encryption certificate and unlock this data, is encrypted with a hash that is based on an empty password. So when you create a password, the hash doesn't match, and there's no way to unlock the encrypted data. The only way to resolve this is to restore the original settings by removing the password from the account. The user should then be able to access his or her encrypted files. Again, this issue is related only to local user accounts for computers and not to domain user accounts.

TIP Only the User Accounts utility allows you to assign a password hint, which can be helpful in recovering a forgotten or lost password. Another technique for recovering a password is a password reset disk, which can be a floppy disk or a USB flash drive. It is important to note that these are the only techniques you should use to recover passwords for local user accounts unless you want to risk data loss. Why? Although you can create, reset, or remove a password from a user account, doing so deletes any personal certificates and stored passwords associated with this account. As a result, the user will no longer be able to access his or her encrypted files or private e-mail messages that have been encrypted with his or her personal key. In addition, he or she will lose stored passwords for Web sites and network resources. It is also important to note that this is an issue only for local user accounts. Administrators can change or reset passwords for domain user accounts without affecting access to encrypted data.

You can create a password for a local user account by completing the following steps:

1. Log on as the user whose password you want to create. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.

2. Click the account you want to work with. To prevent possible data loss, this should be the same account as the account with which you logged on. Any account that has a current password is listed as Password Protected. Any account without this label doesn't have a password.
3. Click Create A Password. Type a password, and then confirm it, as illustrated in Figure 5-5. Afterward, type a unique password hint. The password hint is a word or phrase that can be used to obtain the password if it is lost or forgotten. This hint is visible to anyone who uses the computer.

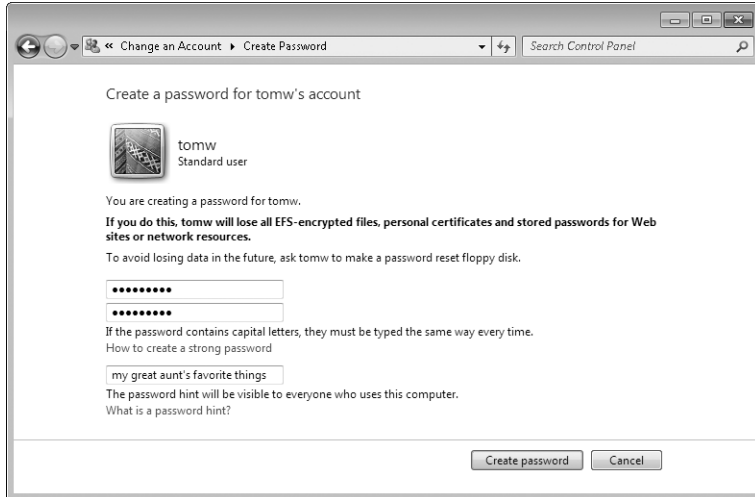


FIGURE 5-5 Create a password with a password hint.

4. Click Create Password.

Recovering Local User Account Passwords

As discussed previously, in order to preserve access to any encrypted data and stored passwords that a user might have, it is preferable to try and recover a user password rather than change or remove the password.

Windows 7 provides two ways to recover user passwords:

- **Password hint** A hint can be accessed on the Welcome screen. Ordinarily, the Welcome screen is displayed when the computer is started and no one is logged on. If someone is logged on to the workstation, ask him or her to log off. Click the user's name to display the Password prompt, and then click the blue enter button to display the password hint. Hopefully, the password hint will help the user remember the password. If it doesn't, you need to use a password reset disk.

- **Password reset disk** Password reset disks can be created for any local user account with a password. They enable anyone to change the password of the related local account without needing to know the old password. Because anyone with access to these disks can change account passwords, you should store password reset disks in a secure location. If users are allowed to create their own password reset disks, be sure they know how important the disks are.

NOTE Passwords for domain users and those for local users are managed differently. Administrators manage passwords for domain user accounts and can reset forgotten passwords using the Active Directory Users And Computers console.

Passwords for local machine accounts can be stored in a secure, encrypted file on a password reset disk, which can be a floppy disk or a USB flash device. You can create a password reset disk for the current user as discussed in “Creating and Using a Password Reset Disk” in Chapter 1. You can reset a password for a local machine account as discussed in “Resetting a User’s Password” in Chapter 1.

Controlling Logon: Welcome Screens and Classic Logons

By default, Windows 7 displays a Welcome screen when a computer is part of a homegroup or workgroup. Windows displays a Logon screen when a computer is part of a domain. The difference between the Welcome screen and the Logon screen is an important one.

In a homegroup or workgroup, the Welcome screen is displayed when no one is logged on or when the screen saver is activated and you attempt to log on again. On the Welcome screen, you see a list of accounts on the computer. To log on with one of these accounts, click the account and type a password if required. Contrary to what many people think, the Welcome screen doesn’t display all the accounts that have been created on the computer. Some accounts, such as Administrator, are hidden from view automatically.

The Welcome screen is convenient because it displays a list of available accounts and enables you to log on by clicking an account name. To enhance security in a homegroup or workgroup by not giving a list of accounts, you can use the Logon screen instead of the Welcome screen. In a domain, the Logon screen is displayed automatically when no one is logged on or when the screen saver is activated and you attempt to log on again. The Logon screen requires users to type a logon name rather than selecting an account from a list of available accounts.

The Logon screen has several features that you can control. By default, the name of the last user to log on is displayed in the User Name field of the Log On To Windows dialog box. Hiding the user name of the last user to log on can improve security by requiring users to know a valid account name for the computer. To do this, start the Local Security Policy tool from the Administrative Tools menu or type **secpol.msc** at an elevated command prompt. Then, under Local Policies\Security

Options, double-click Interactive Logon: Do Not Display Last User Name. Click Enabled, and then click OK.

You can configure whether the Welcome screen is used through the Always Use Classic Logon setting in Group Policy. You have the following options:

- Enable the policy to use the Logon screen rather than the Welcome screen.
- Disable the policy to use the Welcome screen.
- Use Not Configured to use the default configuration (the Welcome screen).

In a domain environment, you can use Active Directory–based Group Policy to apply the security configuration you want to a particular set of computers. You can also configure this setting on a per-computer basis by using local security policy. To configure a homegroup or workgroup computer to use the Logon screen rather than the Welcome screen, use the Group Policy Object Editor, which is an MMC snap-in. You can add this snap-in to an empty console and configure a computer to use the Logon screen by following these steps:

1. Click Start, type **gpedit.msc**, and then press Enter. This opens the Local Group Policy Editor with the top-level Local Group Policy object open for editing.
2. In the editor, expand Local Computer Policy, Computer Configuration, Administrative Templates, System, Logon. (See Figure 5-6.)

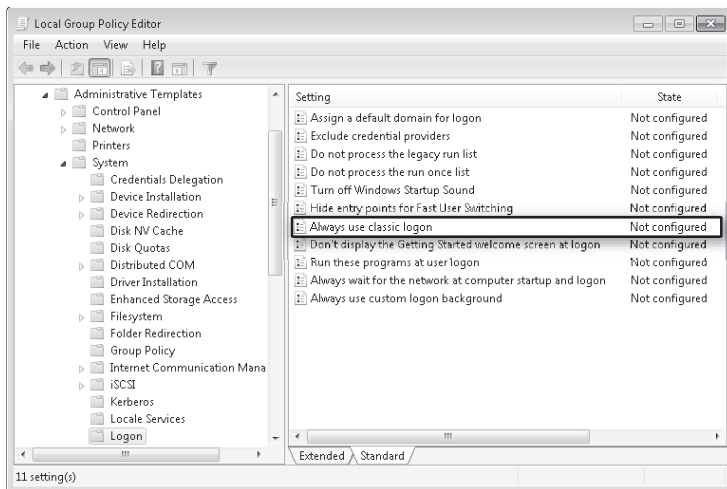


FIGURE 5-6 Enable the Always Use Classic Logon setting to use the Logon screen rather than the Welcome screen.

3. Double-click Always Use Classic Logon.
4. Select Enabled, and then click OK.

In a domain, by default you cannot bypass the requirement to press Ctrl+Alt+Del to access the Log On To Windows dialog box. You can eliminate this requirement, but it is a poor security practice. To do so, in the Local Security Policy tool, expand Local Policies\Security Options, and then double-click Interactive Logon: Do Not Require Ctrl+Alt+Del. Click Enabled, and then click OK.

Removing Accounts and Denying Local Access to Workstations

Domain administrators are automatically granted access to local resources on workstations. Other users aren't granted access to local resources on workstations other than to the computers to which they are permitted to log on. As workstations are moved around an organization, you might find that previous owners of a workstation still have access to its resources or that users who were granted temporary access to a workstation were never removed from the access list.

In a domain, you can control the workstations to which users can log on by using the account properties in Active Directory Users And Computers. Double-click the account to display the Properties dialog box. On the Account tab, click the Log On To button.

In a homegroup or workgroup, you can remove a user's local account and effectively deny logon by completing these steps:

1. Log on as a user with local administrator privileges. In Control Panel, under the User Accounts heading, click Add Or Remove User Accounts. This displays the Manage Accounts page.
2. Click the account you want to remove.
3. Click Delete The Account.
4. Before deleting the account, you have the opportunity save the contents of the user's desktop and documents folders to a folder on the current user's desktop. To save the user's desktop and documents, click Keep Files. To delete the files, click Delete Files.
5. Confirm the account deletion by clicking Delete Account.

Keep in mind that in a domain, unless further restrictions are in place with regard to logging on to a workstation, a user might still be able to gain access to the workstation by logging on with a domain account.

Managing Stored Credentials

In Windows 7, you can use Credential Manager to store credentials that can be used to try to automatically log on users to servers, Web sites, and programs. Credentials are stored in an electronic vault (called the Windows vault) that provides easy logon to essential resources, wherever they might be located. If you find that a user frequently has problems logging on to protected resources, such as the company

intranet or an external Internet site, you can create a stored credential for each resource that the user works with.

Credential Manager supports three types of stored credentials:

- **Windows credential** A credential that uses standard Windows authentication (NTLM or Kerberos) and includes a resource location, logon account name, and password.
- **Certificate-based credential** A credential that includes a resource location and uses a certificate saved in the Personal store in Certificate Manager for authentication.
- **Generic credential** A credential that uses basic or custom authentication techniques and includes a resource location, logon account name, and password.

The following sections examine techniques for working with stored credentials.

Adding Windows or Generic Credentials

Each user account has a unique Windows vault. Entries in the Windows vault are stored in the user's profile settings and contain information needed to log on to protected resources. If you are logged on to a domain account when you create a Windows vault entry, and the account has a roaming profile (instead of a local or mandatory profile), the information stored in the Windows vault entry is available when you log on to any computer in the domain. Otherwise, the information in the Windows vault entry is available only on the computer on which you create the entry.

REAL WORLD When your organization has computers that are in workgroups or homegroups rather than part of your domain, you'll find that stored credentials can save everyone a lot of time. For example, if Ted uses a computer that is a member of a workgroup for his daily activities but needs to access several different servers in several different locations or domains, you can make this process easier by creating a Windows credential for each resource. Now, no matter how Ted accesses the servers, he can be authenticated automatically and without having to provide alternate credentials. For example, if Ted maps a network drive to FileServer84 and you've set up a credential for this server, Ted doesn't have to select the Connect Using Different Credential option and then provide alternate credentials.

To add an entry to the current logged-on user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.

On the Credential Manager page, shown in Figure 5-7, you'll see a list of current entries by credential type (if there are any credentials).

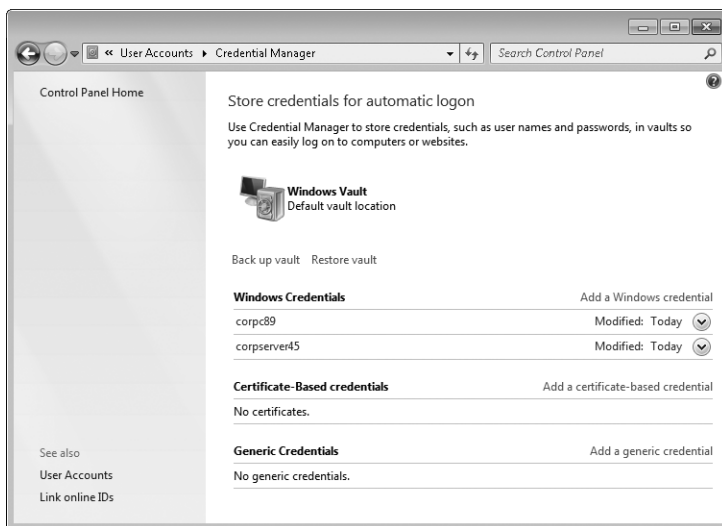


FIGURE 5-7 Review the currently available credentials and options.

2. Click Add A Windows Credential or Add A Generic Credential as appropriate for the type of credential you are creating. Then use the options provided to configure the credential (as shown in Figure 5-8). The available fields are as follows:

- **Internet Or Network Address** The network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, such as `fileserver86`; a fully qualified domain name for an Internet resource, such as `www.microsoft.com`; or an address containing a wildcard, such as `*.microsoft.com`. When you use a server name or fully qualified domain name, the entry is used for accessing a specific server or service. When you use a wildcard, the entry is used for any server in the specified domain. For example, the entry `*.microsoft.com` could be used to access `www.microsoft.com`, `ftp.microsoft.com`, `smtp.microsoft.com`, and `extranet.microsoft.com`.
- **User Name** The user name required by the server, including any necessary domain qualifiers. To use the default domain for a resource, enter only the user name, such as `Williams`. For a nondefault domain, type the full domain and account name, such as `technology\Williams`. For an Internet service, type the full service account name, such as `Williams@msn.com`.
- **Password** The password required by the server. One of the things most users forget is that whenever they change their password on the server or service, they must also change their password in their Windows vault. If a user forgets to change the password in the Windows vault, repeated

attempts to log on or connect to the server or service might result in the account being locked.

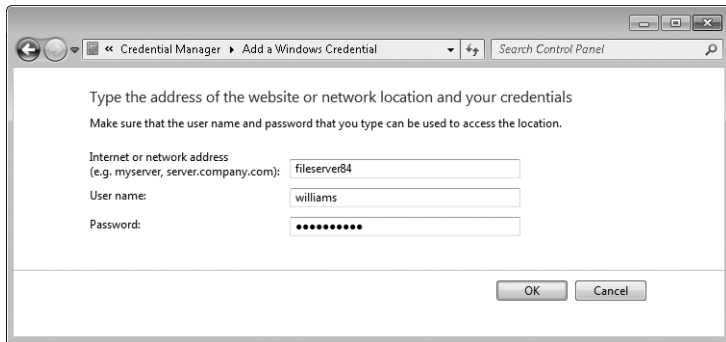


FIGURE 5-8 Create the Windows vault entry by setting the necessary login information.

4. Click OK to save the credential.

Adding Certificate-Based Credentials

The Personal certificate store in the user's profile stores certificates that have been issued to authenticate the user. Once you've added a certificate for the user, you can create a credential that uses the certificate to access a resource.

To add an entry for a certificate-based credential to the currently logged-on user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
2. On the Credential Manager page, you'll see a list of current entries by credential type (if there are any credentials).
3. Click Add A Certificate-Based Credential. In the Internet Or Network Address field, enter the name of the network or Internet resource for which you are configuring the Windows vault entry. This can be a server name, a fully qualified domain name for an Internet resource, or an address containing a wildcard.
4. Click Select Certificate. In the Select Certificate dialog box, click the personal certificate that you want to use for the resource, and then click OK.
5. Click OK again to save the credential.

Editing Windows Vault Entries

You can edit Windows vault entries at any time, but keep in mind that local Windows vault entries are visible only on the computer on which they were created. This means that if you want to modify an entry, you must log on to the local

workstation where the entry was created. The only exception is for users with roaming profiles. When a user has a roaming profile, Windows vault entries can be edited from any computer where the user is logged on.

Use the following steps to edit a user's Windows vault entries:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click the credential entry that you want to edit.
3. Click Edit.
4. As necessary, specify new values for the user name and password or the certificate associated with the credential, and then click Save.

Backing Up and Restoring the Windows Vault

You can back up a user's stored credentials by backing up the Windows vault. After you back up the Windows vault, you can restore the credentials or transfer them to a new computer simply by restoring the Windows vault. In most cases, you should back up the Windows vault to removable media.

To back up a user's Windows vault, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click Back Up Vault.
3. On the Stored User Names And Passwords page, click Browse. Use the Save Backup File As dialog box to select a save location and specify a name for the credential backup file. Credential backup files are saved with the .crd file extension. Click Save.
4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter and confirm a password for the credential backup file.
5. Click Next, and then click Finish.

To restore a user's Windows vault on the same or different computer, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
2. On the Credential Manager page, click Restore Vault.

3. On the Stored User Names And Passwords page, click Browse. Use the Open Backup File As dialog box to select the location and file in which you saved the credential backup files, and then click Open.
4. Click Next. Press Ctrl+Alt+Delete to switch to the secure desktop. When prompted, enter the password for the credential backup file.
5. Click Next, and then click Finish.

Removing Windows Vault Entries

When a user no longer needs a Windows vault entry, you should remove it. To remove a user's Windows vault entry, follow these steps:

1. Log on as the user whose Windows vault entries you want to manage. In Control Panel, click User Accounts, and then click Credential Manager.
On the Credential Manager page, you'll see a list of current entries by credential type.
2. Click the credential entry that you want to remove.
3. Click Remove From Vault. When prompted to confirm the action, click Yes.

As stated previously, local Windows vault entries can be removed only on the computer on which they were created. When a user has a roaming profile, however, Windows vault entries can be deleted from any computer to which the user is logged on.

Managing Local User Accounts and Groups

Local user accounts and groups are managed much like domain accounts. You can create accounts, manage their properties, reset accounts when they are locked or disabled, and so on. In addition to being able to manage local user accounts with Control Panel, you can create local user accounts with Local Users And Groups or with policy preferences. You should:

- Use Local Users And Groups to manage local user accounts on one computer.
- Use policy preferences to manage local user accounts on multiple computers throughout a domain.

When working with policy preferences, you can manage users and groups through Computer Configuration entries or User Configuration entries. Use Computer Configuration if you want to configure preferences that should be applied to computers regardless of who logs on. Use User Configuration if you want to configure preferences that should be applied to users regardless of which computer they log on to.

Creating Local User Accounts

You can access Local Users And Groups and create a user account by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.
2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)
3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Users. In the details pane, you should see a list of the currently defined user accounts.
4. Right-click Users, and then click New User. This opens the New User dialog box, shown in Figure 5-9.

The fields in the dialog box are used as follows:

- **User Name** The logon name for the user account. This name should follow the conventions for the local user name policy.
- **Full Name** The full name of the user, such as William R. Stanek.
- **Description** A description of the user. Normally, you would type the user's job title, such as Webmaster. You could also type the user's job title and department.
- **Password** The password for the account. This password should follow the conventions of your password policy.
- **Confirm Password** A field to ensure that you assign the account password correctly. Simply retype the password to confirm it.
- **User Must Change Password At Next Logon** If this check box is selected, the user must change the password upon logon.
- **User Cannot Change Password** If this check box is selected, the user can't change the password.
- **Password Never Expires** If this check box is selected, the password for this account never expires. This setting overrides the local account policy.
- **Account Is Disabled** If this check box is selected, the account is disabled and can't be used. Use this field to temporarily prevent anyone from using an account.



FIGURE 5-9 Configure new workstation accounts using the New User dialog box in Local Users And Groups.

5. Click Create when you have finished configuring the new account.

You can access Group Policy and use a preference item to create a user account by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local User. This opens the New Local User Properties dialog box, shown in Figure 5-10.
3. In the Action list, select Create. The rest of the fields in the dialog box are used as described in the previous procedure.
4. Use the options on the Common tab to control how the preference is applied. In most cases, you'll want to create the new account only once. If so, select Apply Once And Do Not Reapply.
5. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

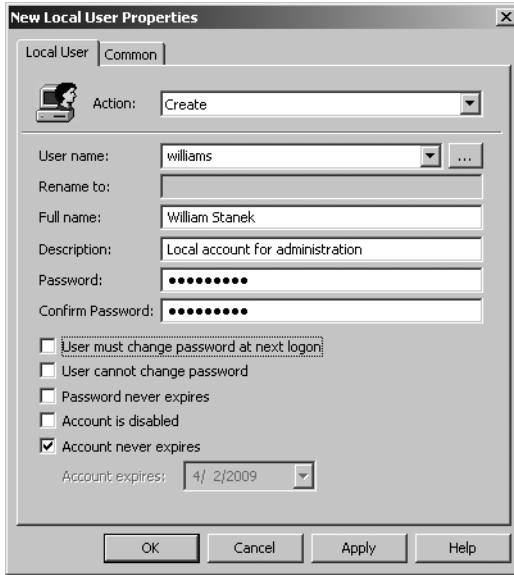


FIGURE 5-10 Configure new local user accounts in Group Policy.

Creating Local Groups for Workstations

You create local groups with Local Users And Groups or with Group Policy. You can access Local Users And Groups and create a local group by completing the following steps:

1. Click Start, point to All Programs, Administrative Tools, and then click Computer Management. Alternatively, open Control Panel, click System And Security, scroll down, click Administrative Tools, and then double-click Computer Management.
2. Right-click the Computer Management entry in the console tree, and then click Connect To Another Computer on the shortcut menu. You can now select the Windows 7 workstation whose local accounts you want to manage. (Domain controllers do not have local users or groups.)
3. Under the System Tools node, double-click the Local Users And Groups node to expand it, and then select Groups. In the details pane, you should see a list of the currently defined group accounts.
4. Right-click Groups, and then select New Group. This opens the New Group dialog box, shown in Figure 5-11.

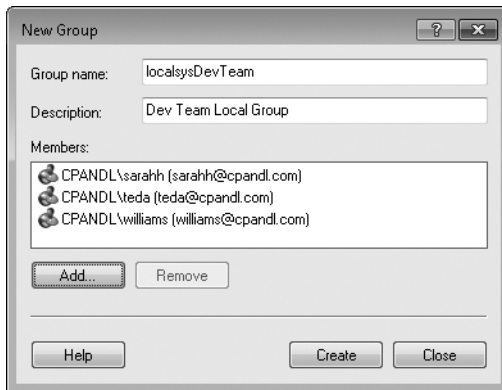


FIGURE 5-11 The New Group dialog box enables you to add a new local group to a Windows 7 workstation.

5. After you type a name and description for the group, click the Add button to open the Select Users dialog box and add names to the group.
6. In the Select Users dialog box, click Locations to select the computer or domain in which the user accounts you want to work with are located.
7. Type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK when you have finished.
8. The New Group dialog box is updated to reflect your selections. If you made a mistake, select a name and remove it by clicking Remove.
9. Click Create when you have finished adding or removing group members.

You can access Group Policy and use a preference item to create a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box, shown in Figure 5-12.

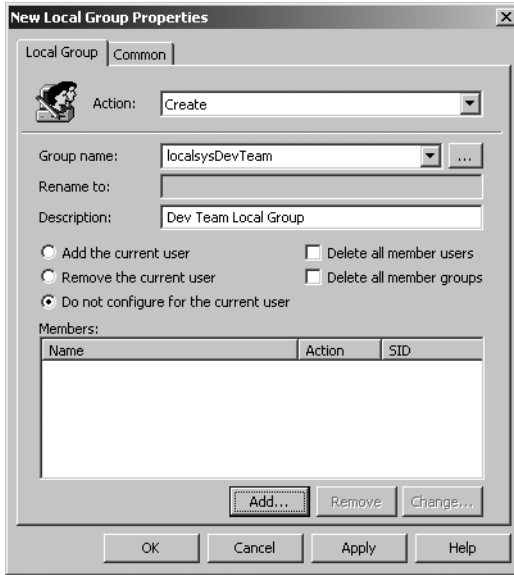


FIGURE 5-12 Configure new local group accounts in Group Policy.

3. In the Action list, select Create. Enter a name and description for the group.
4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.
5. To add members to the group, click Add. In the Local Group Member dialog box, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.
6. Use the options on the Common tab to control how the preference is applied. In most cases, you should create the new account only once. If so, select Apply Once And Do Not Reapply.
7. Click OK. The next time Group Policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Adding and Removing Local Group Members

You use Local Users And Groups to add or remove local group members. Complete the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Groups folder in the left pane. Double-click the group with which you want to work.

2. Click the Add button to add user accounts to the group. This opens the Select Users dialog box. In the Select Users dialog box, type the name of a user you want to use in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use, and then click OK. If no matches are found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.
3. Use the Remove button to remove user accounts from the group. Simply select the user account you want to remove from the group, and then click Remove.
4. Click OK when you have finished.

You can access Group Policy and use a preference item to add or remove members from a local group by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Right-click the Local Users And Groups node, point to New, and then select Local Group. This opens the New Local Group Properties dialog box.
3. In the Action list, select Update to update the group's settings, or select Replace to delete the group and then re-create it exactly as you specify. If you update a group, you can enter a new name in the Rename To box.
4. Specify whether the current user should be added or removed as a member of the group, or select Do Not Configure For The Current User.
5. Specify whether all existing member users, all existing member groups, or both should be deleted.
6. To add or remove group members, click Add. In the Local Group Member dialog box, in the Action list, select Add To This Group if you are adding a member, or select Remove From This Group if you are removing a member. Next, click the browse button (the one with the three dots). Use the Select User, Computer Or Group dialog box to select a user or group to add to the local group, and then click OK twice. Repeat this step as necessary.
7. Use the options on the Common tab to control how the preference is applied, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Enabling or Disabling Local User Accounts

Local user accounts can become disabled for several reasons. If a user forgets his password and tries to guess it, he might exceed the account policy for bad logon attempts. Another administrator could have disabled the account while a user was

on vacation. When an account is disabled or locked out, you can enable it by using the methods described here.

When an account is disabled, you can enable it on a local computer by completing the following steps:

1. Expand Local Users And Groups in Computer Management, and then select the Users folder in the left pane.
2. In the right pane, double-click the user's account name, and then clear the Account Is Disabled check box.
3. Click OK.

When an account is locked out, you can enable it on a local computer by completing the following steps:

1. In Local Users And Groups, select the Users folder in the left pane.
2. In the right pane, double-click the user's account name, and then clear the Account Is Locked Out check box.
3. Click OK.

You can enable or disable accounts and set other account options through policy preferences by completing the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. In the right pane, double-click the user's account name to open the related Properties dialog box.
3. Select Update in the Action list. Make any necessary changes, and then click OK. The next time policy is refreshed, the preference item will be applied as appropriate for the Group Policy object in which you defined the preference item.

Creating a Secure Guest Account

In some environments, you might need to set up a Guest account that can be used by visitors. Most of the time, you'll want to configure the Guest account on a specific computer or computers and carefully control how the account can be used. To create a secure Guest account, I recommend that you perform the following tasks:

- **Enable the Guest account for use.** By default, the Guest account is disabled, so you must enable it to make it available. To do this, access Local Users And Groups in Computer Management, and then select the Users folder. Double-click Guest, and then clear the Account Is Disabled check box. Click OK.

- **Set a secure password for the Guest account.** By default, the Guest account has a blank password. To improve security on the computer, you should set a password for the account. In Local Users And Groups, right-click Guest, and then select Set Password. Click Proceed at the warning prompt. Type the new password and then confirm it. Click OK twice.
- **Ensure that the Guest account cannot be used over the network.** The Guest account shouldn't be accessible from other computers. If it is, users at another computer could log on over the network as a guest. To prevent this, start the Local Security Policy tool from the Administrative Tools menu, or type `secpol.msc` at the command prompt. Then, under Local Policies\User Rights Assignment, check that the Deny Access To This Computer From The Network policy lists Guest as a restricted account.
- **Prevent the Guest account from shutting down the computer.** When a computer is shutting down or starting up, it is possible that a guest user (or anyone with local access) could gain unauthorized access to the computer. To help deter this, you should be sure that the Guest account doesn't have the Shut Down The System user right. In the Local Security Policy tool, expand Local Policies\User Rights Assignment, and ensure that the Shut Down The System policy doesn't list the Guest account.
- **Prevent the Guest account from viewing event logs.** To help maintain the security of the system, the Guest account shouldn't be allowed to view the event logs. To be sure this is the case, start Registry Editor by typing `regedit` at a command prompt, and then access the `HKLM\SYSTEM\CurrentControlSet\services\Eventlog` key. Here, among others, you'll find three important subkeys: Application, Security, and System. Make sure each of these subkeys has a DWORD value named `RestrictGuestAccess` with a value of 1.

Renaming Local User Accounts and Groups

When you rename an account, you give it a new label. Because the SID for the account remains the same, the permissions and properties associated with the account don't change. To rename an account while you are accessing a local computer, complete the following steps:

1. In Local Users And Groups, select the Users or Groups folder, as appropriate.
2. Right-click the account name, and then click Rename. Type the new account name, and then click a different entry.

To rename an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.

2. Do one of the following:

- If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Update in the Action list. In the Rename To box, type the new account name, and then click OK.
- If a preference item doesn't already exist for the user or group, you need to create one using the techniques discussed previously. Because you want to rename the user or group, select Update in the Action list, and then type the new account name in the Rename To box.

Deleting Local User Accounts and Groups

Deleting an account permanently removes it. Once you delete an account, if you create another account with the same name, you can't automatically get the same permissions because the SID for the new account won't match the SID for the account you deleted.

Because deleting built-in accounts can have far-reaching effects on the workstation, Windows 7 doesn't let you delete built-in user accounts or group accounts. In Local Users And Groups, you can remove other types of accounts by selecting them and pressing the Delete key or by right-clicking and then clicking Delete. When prompted, click Yes.

NOTE When you delete a user account using Local Users And Groups, Windows 7 doesn't delete the user's profile, personal files, or home directory. If you want to delete these files and directories, you have to do it manually.

To delete an account using Group Policy, complete the following steps:

1. Open a Group Policy object (GPO) for editing in the Group Policy Management Editor. To configure preferences for computers, expand Computer Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups. To configure preferences for users, expand User Configuration\Preferences\Control Panel Settings, and then select Local Users And Groups.
2. Do one of the following:
 - If a preference item already exists for the user or group, double-click the user or group name to open the related Properties dialog box. Select Delete in the Action list. On the Common tab, set the appropriate options, such as Apply Once And Do Not Reapply, and then click OK.
 - If a preference item doesn't already exist for the user or group, you need to create one for the user or group using the techniques discussed previously. Be sure to select Delete in the Action list, and then select the appropriate options on the Common tab.

Managing Remote Access to Workstations

Windows 7 has several remote connectivity features. With Remote Assistance, users can send invitations to support technicians, enabling the technicians to service a computer remotely. With Remote Desktop, users can connect remotely to a computer and access its resources. In this section, you'll learn how to configure Remote Assistance and Remote Desktop. Typically, neither the Remote Assistance feature nor the Remote Desktop feature is enabled, and you must enable these features manually.

Remote Assistance and Remote Desktop can function through Network Address Translation (NAT) firewalls. Remote Assistance also has built-in diagnostic tools. To allow for easier troubleshooting and escalation of support issues, two different support staff can connect to a remote computer simultaneously. When troubleshooting requires restarting the computer, Remote Assistance sessions are reestablished automatically after the computer being diagnosed reboots.

Prior to using Remote Assistance, you may want users to use the Problem Steps Recorder to create a step-by-step record of a problem they are experiencing. The Problem Steps Recorder is very easy to use. To start and use the Problem Steps Recorder, a user needs to complete the following steps:

1. To start the Problem Steps Recorder, have the user click Start, type **psr**, and then press Enter. Once the tool is started, the user can prepare the environment and then begin recording the problem.
2. To turn on recording, the user clicks Start Record. Once recording has started, the user can perform the action that isn't working and click Add Comment to add comments as she works.
3. When the user experiences the problem and the related errors have been displayed, she can stop recording by clicking Stop Record.
4. When the user stops recording, the Save As dialog box is displayed. The user selects a save location and name for the Zip file that contains the record of the problem in an .mht file.
5. The user can send the Zip file to a support technician in an e-mail message or by copying it to a file share. To review the recorded problem steps, you double-click the Zip file to display its contents in Windows Explorer and then double-click the enclosed .mht file to open it in Internet Explorer.
6. You'll then see screen captures for all the steps the user took while the problem was being recorded. After the screen captures, you'll find additional details for each step that are generated automatically. You can use this information along with any user comments to help you troubleshoot the problem.

Configuring Remote Assistance

Remote Assistance is a useful feature for help desks, whether in-house or out-sourced. A user can allow support personnel to view and take control of his or her desktop. This feature can be used to walk users through a complex process or to manage system settings while they watch the progress of the changes. The key to Remote Assistance is in the access levels you grant.

When enabled, Remote Assistance is configured by default to let support personnel view and control computers. Because users can send assistance invitations to internal and external resources, this could present a security concern for organizations. To reduce potential security problems, you might want to allow support staff to view but not control computers. A new restriction for Windows 7 is to allow connections only from computers running Windows 7 or later. This option is helpful to limit any possible compatibility issues and to ensure that any security enhancements in Windows 7 or later operating systems are available within Remote Assistance sessions.

Another key aspect of Remote Assistance you can control is the time limit for invitations. The default maximum time limit is 6 hours; the absolute maximum time limit you can assign is 30 days. Although the intent of a multiple-day invitation is to give support personnel a time window in which to respond to requests, it also means that they could use an invitation to access a computer over a period of 30 days. For instance, suppose you send an invitation with a 30-day time limit to a support person who resolves the problem the first day. That person would still have access to the computer for another 29 days, which wouldn't be desirable for security reasons. To reduce the risk to your systems, you'll usually want to reduce the default maximum time limit considerably—say, to 1 hour. If the problem is not solved in the allotted time period, you can issue another invitation.

To configure Remote Assistance, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box with the Remote tab displayed, as shown in Figure 5-13.
3. To disable Remote Assistance, clear the Allow Remote Assistance Connections To This Computer check box, and then click OK. Skip the remaining steps.
4. To enable Remote Assistance, select Allow Remote Assistance Connections To This Computer.

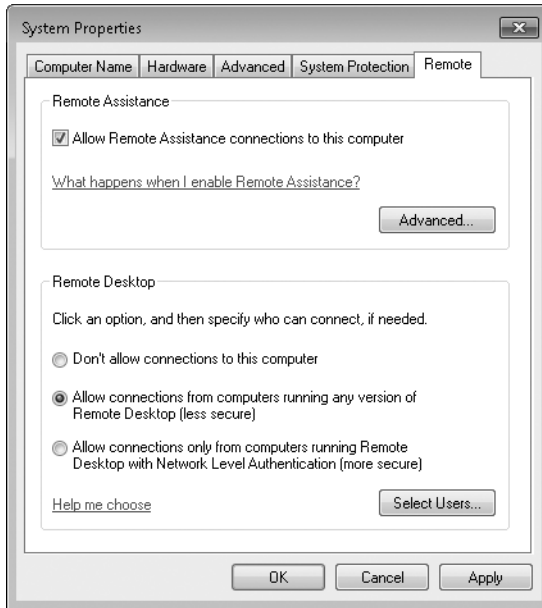


FIGURE 5-13 Use the Remote tab options to configure remote access to the computer.

5. Click Advanced. This displays the Remote Assistance Settings dialog box, shown in Figure 5-14.

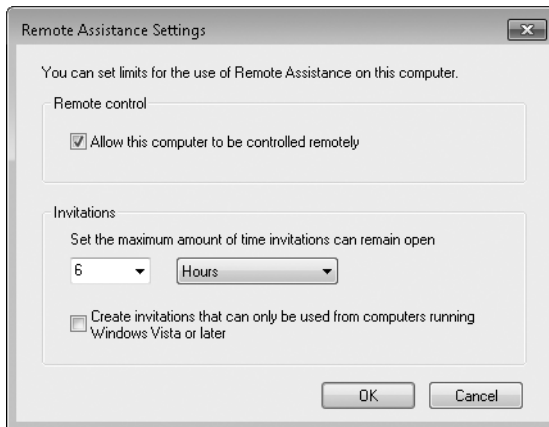


FIGURE 5-14 The Remote Assistance Settings dialog box is used to set limits for Remote Assistance.

6. The Allow This Computer To Be Controlled Remotely option sets limits for Remote Assistance. When selected, this setting allows assistants to view and control the computer. To provide view-only access to the computer, clear this check box.
7. The Invitations options control the maximum time window for invitations. You can set a value in minutes, hours, or days, up to a maximum of 30 days. If you set a maximum limit value of 10 days, for example, a user can create an invitation with a time limit up to but not more than 10 days. The default maximum expiration limit is 6 hours.
8. Click OK twice when you have finished configuring Remote Assistance options.

In Group Policy, you can manage Remote Assistance using the policy settings shown in Table 5-2. These settings are found in the Administrative Templates policies for Computer Configuration under the paths shown.

TABLE 5-2 Policy Settings for Managing Remote Assistance

SETTING	PATH
Allow Only Vista Or Later Connections	\System\Remote Assistance
Do Not Allow Windows Messenger To Be Run	\Windows Components\Windows Messenger
Offer Remote Assistance	\System\Remote Assistance
Solicited Remote Assistance	\System\Remote Assistance
Turn On Session Logging	\System\Remote Assistance

Configuring Remote Desktop Access

Unlike Remote Assistance, which provides only a view of the current user's desktop, Remote Desktop provides several levels of access:

- If a user is logged on to the desktop locally and then tries to log on remotely, the local desktop locks, and the user can access all of the running applications just as though he or she were sitting at the keyboard. This feature is useful for users who want to work from home or other locations outside the office, enabling them to continue to work with applications and documents that they were using prior to leaving the office.
- If a user is listed on the workstation's Remote Access list and is not otherwise logged on, he or she can initiate a new Windows session. The Windows session behaves as though the user were sitting at the keyboard. It can even be used when other users are also logged on to the computer. In this way, multiple users can share a single workstation and use its resources.

Remote Desktop is not enabled by default. You must specifically enable it to allow remote access to the workstation. When it is enabled, any member of the Administrators group can connect to the workstation. Other users must be placed on a remote access list to gain access to the workstation. To configure remote access, follow these steps:

1. In Control Panel, click System And Security, and then click System.
2. On the System page, click Remote Settings in the left pane. This opens the System Properties dialog box to the Remote tab.
3. To disable Remote Desktop, select Don't Allow Connections To This Computer, and then click OK. Skip the remaining steps.
4. To enable Remote Desktop, you have two options. You can:
 - Select Allow Connections From Computers Running Any Version Of Remote Desktop to allow connections from any version of Windows.
 - Select Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication to allow connections only from Windows 7 or later computers (and computers with secure network authentication).
5. Click Select Users. This displays the Remote Desktop Users dialog box, shown in Figure 5-15.

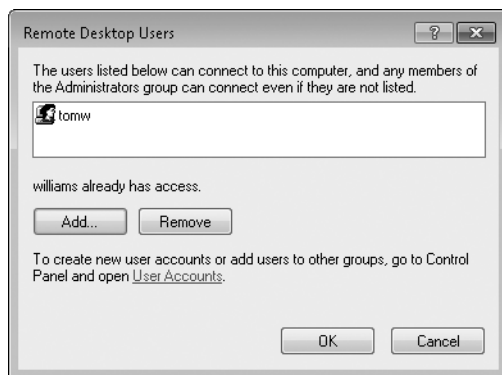


FIGURE 5-15 Specify the additional users allowed to make Remote Desktop connections.

6. To grant Remote Desktop access to a user, click Add. This opens the Select Users dialog box. In the Select Users dialog box, click Locations to select the computer or domain in which the users you want to work with are located. Type the name of a user you want to work with in the Enter The Object Names To Select field, and then click Check Names. If matches are found, select the account you want to use and then click OK. If no matches are

found, update the name you entered and try searching again. Repeat this step as necessary, and then click OK.

7. To revoke remote access permissions for a user account, select the account and then click Remove.
8. Click OK twice when you have finished.

Windows Firewall must be configured to allow inbound Remote Desktop exceptions. You can configure this on a per-computer basis in Windows Firewall for the domain profile and the standard profile. In Group Policy, you can configure this exception and manage Remote Desktop by using the policy settings shown in Table 5-3. These settings are found in the Administrative Templates policies for Computer Configuration under the path shown.

TABLE 5-3 Policy Settings for Managing Remote Desktop

SETTING	COMPUTER CONFIGURATION PATH
	PATHS UNDER WINDOWS COMPONENTS\REMOTE DESKTOP SERVICES
Allow .Rdp Files From Unknown Publishers	\Remote Desktop Connection Client
Allow .Rdp Files From Valid Publishers And User's Default .Rdp Settings	\Remote Desktop Connection Client
Always Prompt For Password Upon Connection	\Remote Desktop Session Host\Security
Automatic Reconnection	\Remote Desktop Session Host\Connections
Configure Server Authentication For Client	\Remote Desktop Connection Client
Deny Logoff Of An Administrator Logged In To The Console Session	\Remote Desktop Session Host\Connections
Do Not Allow Local Administrators To Customize Permissions	\Remote Desktop Session Host\Security
Do Not Allow Passwords To Be Saved	\Remote Desktop Connection Client
Limit Maximum Color Depth	\Remote Desktop Session Host\Remote Session Environment
Limit Maximum Display Resolution	\Remote Desktop Session Host\Remote Session Environment
Limit Maximum Number Of Monitors	\Remote Desktop Session Host\Remote Session Environment

SETTING	COMPUTER CONFIGURATION PATH
Limit The Size Of The Entire Roaming User Profile Cache	\Remote Desktop Session Host\Profiles
Require Use Of Specific Security Layer For Remote (Rdp) Connections	\Remote Desktop Session Host\Security
Set Client Connection Encryption Level	\Remote Desktop Session Host\Security
Set Compression Algorithm For Rdp Data	\Remote Desktop Session Host\Remote Session Environment
Specify Sha1 Thumbprints Of Certificates Representing Trusted .Rdp Publishers	\Remote Desktop Connection Client
OTHER PATHS	
Disable Remote Desktop Sharing	\Windows Components\NetMeeting
Windows Firewall: Allow Inbound Remote Desktop Exceptions	\Network\Network Connections\Windows Firewall\Domain Profile
Windows Firewall: Allow Inbound Remote Desktop Exceptions	\Network\Network Connections\Windows Firewall\Standard Profile

Making Remote Desktop Connections

As an administrator, you can make Remote Desktop connections to Windows servers and workstations. With Windows 2000 Server, Remote Desktop connections are enabled by installing Terminal Services and then configuring Terminal Services in remote access mode. With Windows XP Professional and later versions, Remote Desktop is installed automatically, but it is normally not enabled until you do so as discussed in the preceding section of this chapter. Once remote access is enabled on a computer, all administrators have remote access to that computer. Other users can be granted remote access as well.

To make a Remote Desktop connection to a server or workstation, follow these steps:

1. At a command prompt, type **mstsc**, or click Start, point to All Programs, Accessories, and then click Remote Desktop Connection. Click the Options button. This displays the Remote Desktop Connection dialog box, shown in Figure 5-16.

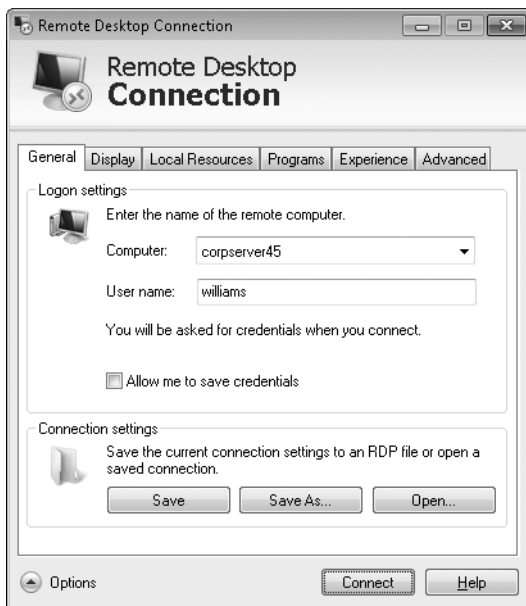


FIGURE 5-16 In the Remote Desktop Connection dialog box, type the name of the computer to which you want to connect, and then click Connect.

2. In the Computer field, type the name of the computer to which you want to connect. If you don't know the name of the computer, use the drop-down list to choose an available computer, or select Browse For More in the drop-down list to display a list of domains and computers in those domains.
3. Specify additional options as necessary. If you've configured stored credentials for the computer, your saved credentials will be used automatically. You can edit or delete the credentials as necessary.
4. Click Connect. If you haven't previously stored credentials for the computer, type your credentials when prompted, and then click OK. If the connection is successful, you'll see the Remote Desktop window on the selected computer, and you'll be able to work with resources on the computer. In the case of a failed connection, check the information you provided and then try to connect again.

NOTE Clicking Options in the Remote Desktop Connection dialog box displays additional options for creating and saving connections. These options enable you to change the display size for the Remote Desktop, manage connections to local resources (such as printers, serial ports, and disk drives), run programs automatically on connection, and enable or disable local caching and data compression.