Chapter 1

Implementing User Accounts, Groups, and Logon Security

Securing your computer is in many ways like securing your home — you shouldn't rely on any one method to keep the outside world from getting in. Instead, you take a number of different measures that might include locking doors, installing an alarm system, and hopefully not alerting would-be attackers that lots of cool stuff is inside.

When it comes to securing Windows XP, you're given the choice of leaving the front door open or putting a lock in place. This door lock is known as a ***user account***, specifically a user account that includes a password. For a first line of defense in the quest to secure Windows XP and ensure user privacy, begin with user accounts.

This isn't to say that user accounts are strictly a security-related feature of Windows XP; they certainly have other reasons for being. However, user accounts are a key component toward changing your computer from being an open book to a secure fortress.

This chapter focuses on what user accounts are, the different types of accounts that exist, and how to create and configure them to ensure better system security. Along the way, you also learn about group accounts and the different user logon methods that can be used to control access to your Windows XP system.

Exploring User Accounts

When it comes to Windows XP, user accounts represent the foundation upon which all other security concepts and techniques rely. Quite simply, you can install any piece of "security" software — from firewalls and anti-virus programs to anti-spyware tools and encryption utilities — and your work is effectively all for naught if you do not implement user accounts correctly nor properly protect them. Most Windows XP users consider the user account logon process an annoyance, rather than a security feature. Unfortunately, neglecting or ignoring this essential security feature is the very reason why the majority of user desktop systems are insecure and vulnerable to an Internet's worth of security and personal privacy threats.

At the most basic level, a user account is nothing more than an object on a Windows XP system that represents a particular user. Made up of a username, and hopefully a password, user accounts represent the "credentials" that users need to supply to gain access to a Windows XP system. Beyond simply identifying a user, a user's account dictates what tasks that person can perform on a computer, what files they have access to, and more. In a nutshell, user accounts are not an optional part of securing a Windows XP system — they're absolutely essential.

In a departure from previous versions of Windows aimed at home and small office users, Windows XP offers true user account security facilities in a way that cannot be easily ignored or dismissed. Although pressing the Esc key might have gotten a user past the Logon dialog box on a Windows 95 system, Windows XP offers much more robust and comprehensive logon security. As a matter of fact, the logon security capabilities of Windows XP are fundamentally the same as those used to secure servers running Windows 2000 Server or Windows Server 2003. In other words, Windows XP user account security offers a high level of protection for your system. If you're serious about your system's security and privacy, you'll want to take advantage of it.

The good news is that Windows XP makes it easy to create and manage user accounts via tools such as the User Accounts applet in the Control Panel (see Figure 1-1). Before you jump into creating any accounts, however, it's essential for you to understand the benefits that user accounts provide and important details on the different types of accounts that exist.

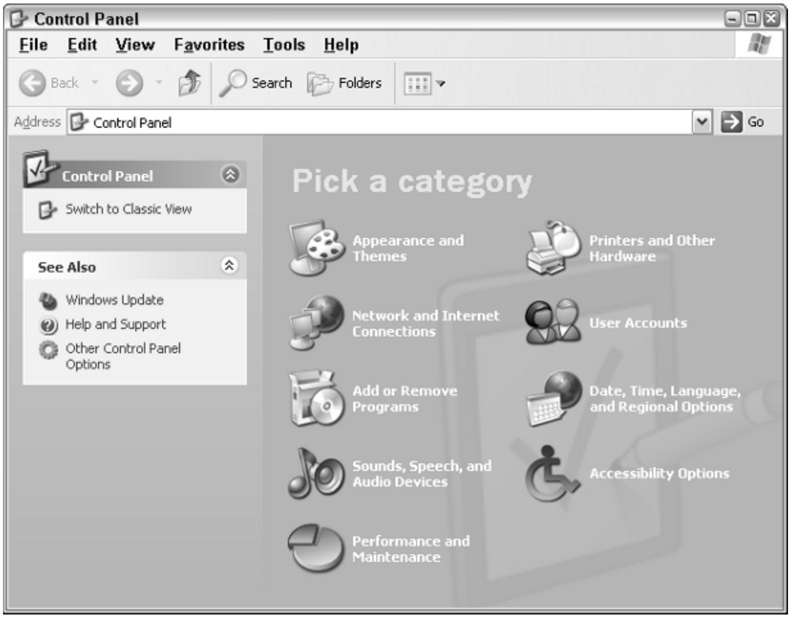

Control Panel
File Edit View Favorites Tools Help
Back
Search
Folders
Address
Control Panel
Go
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance

Figure 1-1: Click the User Accounts icon to create and manage user accounts.

Benefits of user accounts

Some user accounts are configured for general day-to-day use, including tasks like surfing the Web, working with e-mail, and playing games. Others are designed with system administration and configuration tasks in mind, including installing software and making changes to firewall settings. Ultimately, each person who uses a Windows XP system should be assigned their own personal user account, which provides the following benefits:

- A dedicated and customizable desktop environment
- A dedicated user profile where personal files, e-mail messages, and settings are stored
- The capability to control access to the desktop environment by adding a user account password
- The ability to secure personal files and folders, making them inaccessible by other users

Creating a dedicated user account for every person who uses a Windows XP system is not unlike setting up a number of Windows XP systems, in which each user has her own personal desktop environment. This model eliminates the hassles associated with older systems such as Windows 3.1, where users shared a common desktop and all related settings. In the world of Windows XP, having your own user account means being able to log on, set your desktop wallpaper image to something crazy or fun, and not having to deal with friends or family members who decide to change it. Your desktop can be neatly organized (recommended), or a complete mess (recommended only if you thrive in chaotic environments). Most important, having your own user account allows you to control which users can access your files and to what extent.

User account types

Although the idea of each user having their own dedicated account is a great, all user accounts are not created equal. There's a definite hierarchy in this part of the computing world, and Windows XP offers no exception. Some user accounts allow unrestricted access to every last bit of a Windows XP system, including files belonging to other users. Others limit what users can do while logged on, stopping them from carrying out common tasks such as installing software. When it comes to the security of your Windows XP system, creating user accounts is important; however, assigning appropriate user account types to various users is even more critical.

Windows XP includes five different types of user accounts:

- Computer Administrator accounts
- Limited accounts
- Standard accounts
- Guest accounts
- Special user accounts

Each of these user account types is examined in more detail in the following sections.

Note

In the world of Windows XP, a user is the person actually using the computer — you, your mom, dad, son, daughter, or friend. A user account is the object assigned to a user for the purpose of logging on. Some users will have only one user account, and others might have more than one user account — one for day-to-day use and another for system administration tasks.

COMPUTER ADMINISTRATOR ACCOUNTS

In the parallel universe that is Windows XP, one type of user account stands head and shoulders above the rest: the all-seeing and all-knowing ***Computer Administrator account***. User accounts of this type have complete control over every element of a Windows XP system; users with this privilege level can literally do anything, up to and including actions that could irreparably damage a Windows XP installation.

A user configured as a Computer Administrator can do the following:

- Install and uninstall programs, hardware, and drivers
- Make system-wide configuration changes
- Create, delete, and manage all user and group accounts
- Read or open any file, including those belonging to other users
- Grant rights to or implementing restrictions on other users

One limitation is that the Computer Administrator cannot delete his account or change its type to Limited if it is the last Computer Administrator account on the Windows XP system.

Windows XP creates one Computer Administrator account by default (named Administrator) during its installation process. You might not even be aware that this account exists, as it's not displayed on the Welcome logon screen by default. This account is always present, however, and cannot be deleted.

The Computer Administrator user account type is supposed to work for the forces of good, not evil; however, this account type was never designed with normal, everyday, use in mind. As the list of its broad capabilities shows, Computer Administrators yield complete control over not only the Windows XP system itself, but also other users' accounts.

For this reason, regular users should never be granted Computer Administrator privileges. In fact, for security purposes alone, even the Computer Administrator should never log on to Windows XP with a Computer Administrator account unless he needs to perform configuration tasks that require this level of power. Unfortunately, many Windows XP systems run into security-related problems (such as infections by viruses and spyware programs) due to unnecessary or careless everyday use of the massive firepower the Computer Administrator account.

Toward the end of the Windows XP installation process, the installer is prompted to create at least one, and up to a maximum of five, additional user accounts for the people who will be using this computer (these accounts are above and beyond the default Administrator account that is always created). For reasons technically unknown (but almost certainly associated with making the system as easy to use as possible), Windows XP automatically makes each of these accounts a Computer Administrator.

Obviously, this is not a good thing. Although having each user account configured as a Computer Administrator means fewer restrictions for users (who can then do whatever they please), it also presents a very real security risk. Thankfully, all is not lost. You can change the type of any user account that you create, as you learn later in this chapter.

Caution

The decision as to which users should be granted Computer Administrator rights is ultimately up to you, but always keep system security in mind. Generally, any user with access to the Computer Administrator account should have an appropriate level of Windows XP knowledge. More importantly, they should be someone who can be trusted not to abuse or misuse the account's power. On some systems, every user may be responsible enough to be granted access to a Computer Administrator account to perform tasks such as installing programs. On others, the situation might dictate that only the owner of the PC has access to a Computer Administrator account. The bottom line is that on your computer, you get to choose who has access to Computer Administrator accounts, so choose wisely.

LIMITED USER ACCOUNTS

Unlike Computer Administrator accounts, ***Limited user accounts*** are designed for everyday personal use. Many people argue that these accounts are excessively restrictive because they stop users from carrying out common tasks such as installing hardware and software, changing security settings, and making system configuration changes. Indeed these statements are true, but they're also very much to the point — limited user accounts are designed to keep users from making potential harmful and dangerous changes to a system and by extension help to ensure a better-performing and more secure Windows XP system overall.

A user with a Limited account:

- Can add, change, or remove their user account password
- Can create a password reset disk for use in cases where their password is lost or forgotten
- Can make changes to their user desktop environment
- Can make their personal files private (except from the Computer Administrator)
- Can use software programs installed for all users
- Cannot make changes to system configuration settings or delete key files
- Typically cannot install hardware or software programs

Although Limited user accounts typically cannot install hardware and software, there are exceptions. On the hardware front, Windows XP systems do allow Limited users to plug in and use a variety of USB devices including pen drives, MP3 players, and the like. Most other hardware changes are restricted. As for software, Limited users can often install single-user programs that do not make any changes to system configuration settings, as is the case with many older programs designed for previous Windows versions; however, Limited users cannot install multi-user programs, or those that install new system services. Words such as “often,” “typically,” “many,” and “most” are the name of the game here. The best way to see whether a program will install for a Limited user is to attempt the installation. In some cases it may get the job done, but in others it will fail. Although the conveniences associated with being a Computer Administrator have appeal, everyday user accounts should always be of the Limited type if you're serious about securing your system. Unfortunately, going this route can lead to frustration (and even conflict) when one user wants to do something on a computer but is unable to due to restrictions imposed as a result of their Limited user status.

This is why the Computer Administrator account type exists, and there's nothing wrong with granting a responsible and trusted user the ability to use a Computer Administrator account if and when necessary. Later in this chapter, you learn how you can allow "trusted" Limited users to perform administrative tasks without leaving the safe confines of their everyday user account.

As a best practice, always try to follow what is known as the ***principle of least privilege*** when configuring security settings for any PC. This principle dictates that you give users only the minimum level of privilege that they require, and nothing more. Although the level of control that a particular user needs is open to debate (especially in their eyes), sticking to the least privilege maxim will help to ensure a more secure computer. In the case of user accounts, this means assigning all users Limited accounts for normal everyday use. Many viruses and spyware programs rely on the current user having administrator-level access to thoroughly infect systems and do their damage, so sticking with Limited accounts can help to mitigate potential risks. Suffice it to say that when it comes to Windows XP, user accounts, and security, less can actually be more.

Note

While Limited User accounts are the way to go for better overall system security, some popular programs refuse to work for users logged on with Limited accounts. A list of these programs can be found at `support.microsoft.com/default.aspx?scid=kb;en-us;307091`.

STANDARD USER ACCOUNTS

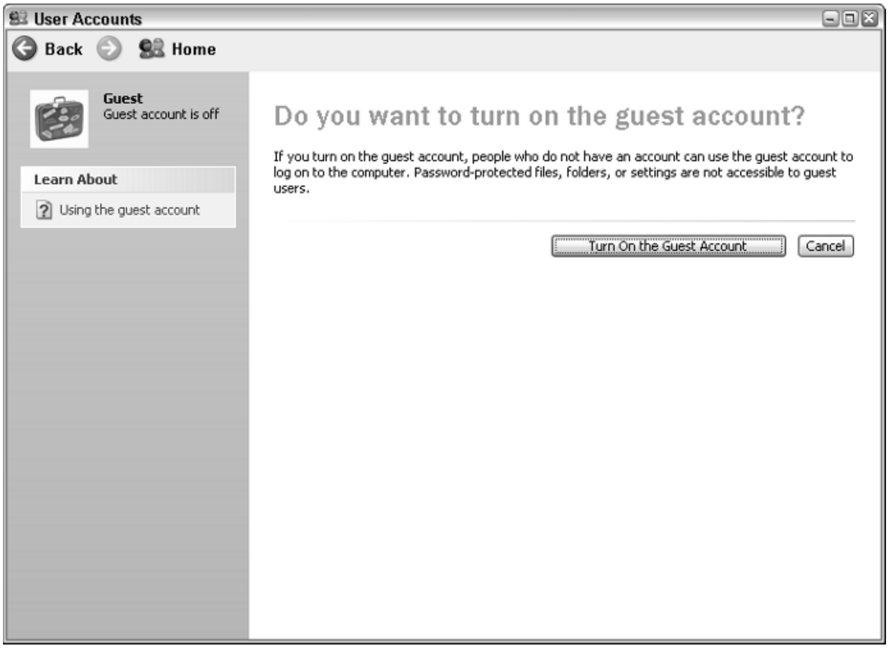
In the vast majority of cases, users running Windows XP on a home or small business network will have their systems configured as part of what is known as a ***workgroup***. This is the name that Microsoft gives to a collection of Windows computers connected to a network that is not centrally administered by a server running Windows 2000 Server or Windows Server 2003. Networks that include a Windows Server system dedicated to tasks like validating user logons are known as ***domains***.

Although both Windows XP Home and Windows XP Professional systems can both be members of a workgroup, only Windows XP Professional systems can be made members of a domain. This isn't surprising, considering that Windows XP Home is primarily designed with the home user in mind, while Windows XP Professional includes additional capabilities more geared toward business users.

When made a member of a domain network, Windows XP Professional systems include an additional user account type, the *Standard user*. Standard users are fundamentally similar to Limited users in terms of what they're allowed to do, with one key exception — these users can install and remove software programs as long as the task in question doesn't affect other users. So, a Standard user could install a program for personal use but could not remove another program available to all users.

GUEST USER ACCOUNT

Along with Administrator, Windows XP also automatically creates a user account named Guest. As its name suggests, this account is meant for users without their own dedicated user account. Disabled by default (see Figure 1-2), the Guest account does not (and cannot) have a password assigned and has little in the way of powers beyond running installed programs.



Do you want to turn on the guest account?

If you turn on the guest account, people who do not have an account can use the guest account to log on to the computer. Password-protected files, folders, or settings are not accessible to guest users.

Figure 1-2: Windows XP's built-in Guest account is disabled by default.

The fact that the Guest account is disabled by default (and cannot be assigned a password) is a good indication that it represents a potential security risk. As a best practice, always leave the Guest account disabled and create Limited accounts for users who require occasional access to your Windows XP system. As you'll see later in this chapter, you can create a user account in less than a minute — well worth the effort from a security perspective.

SPECIAL USER ACCOUNTS

Although there's technically no such thing as "special" user accounts on a Windows XP system, you may encounter additional user accounts beyond the ones that you create. Rarely, programs will require a user account to be created in order to function correctly. Although these user accounts are typically hidden from view on the Windows XP Welcome screen, exceptions do exist.

The most common such event that you're likely to come across is a user account named ASP.NET Machine Account. If you happen to see an account by this name on your Welcome screen or in the User Accounts dialog box shown in Figure 1-3, don't panic. This user account is added to your system after you have installed the .NET Framework, a component from Microsoft that's used to build and run Windows-based programs. If you're not sure how the .NET Framework got onto your system, it's possible that you downloaded it as part of visiting the Windows Update Web site, or because it was required by another program you were attempting to install. In any case, having the ASP.NET account configured on your system does not present any inherent security risk. If you're still bothered by it, however, you can remove the user account from your Welcome screen or completely disable it by following the instructions outlined later in this chapter.

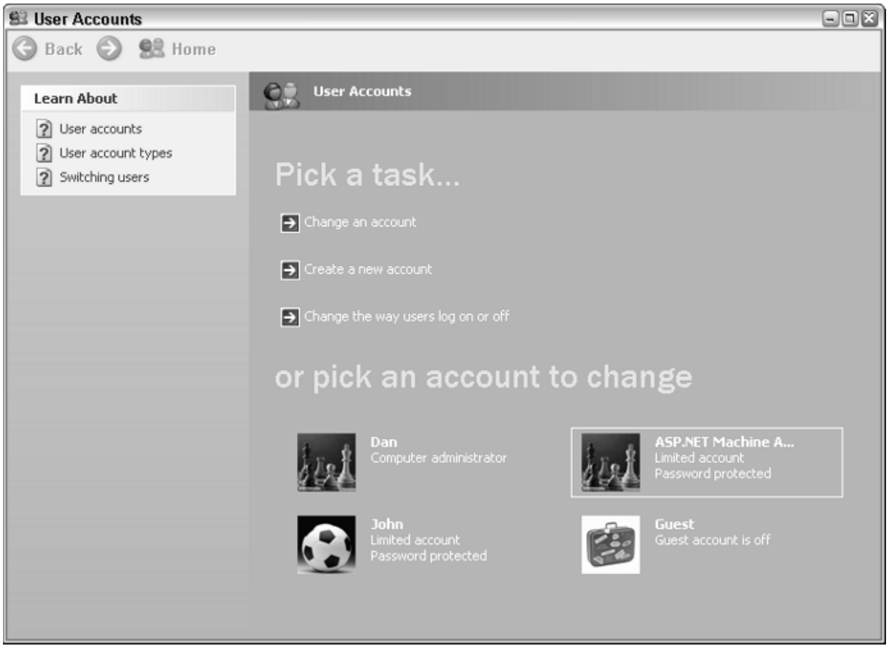


Figure 1-3: ASP.NET is a special user account created when you install Microsoft's .NET Framework.

Creating User Accounts

Now that you're familiar with user accounts and the different types that exist, it's time to get down to the business of actually creating them. As you'll soon see, creating user accounts couldn't be easier.

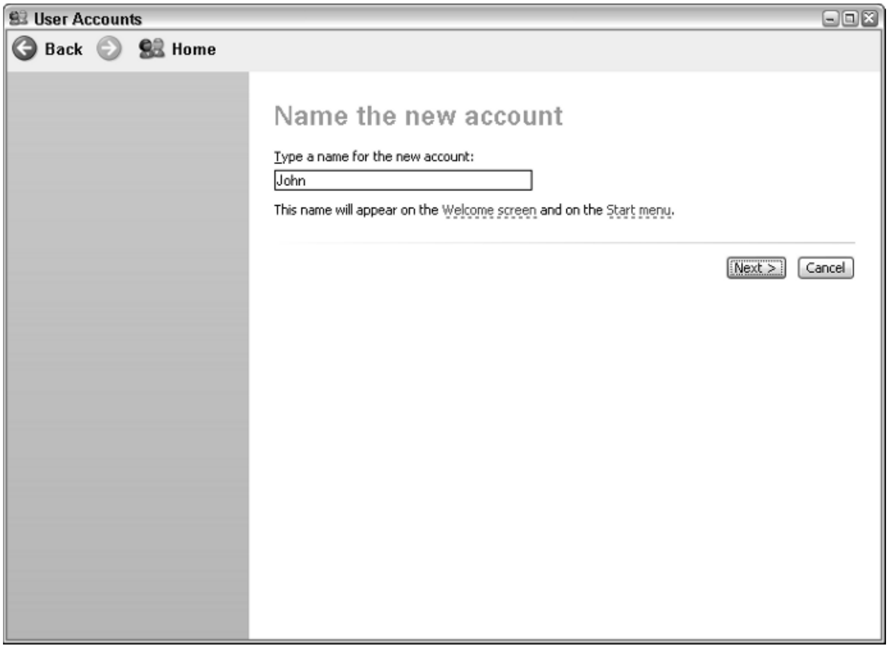
The primary tool used to create user accounts on both Windows XP Home and Professional systems is the User Accounts applet in the Control Panel. On Windows XP Professional systems, however, you also have the option of using the Computer Management tool to get the job done.

Creating user accounts in Control Panel

The User Accounts applet in Control Panel is the most intuitive and user-friendly tool for creating user accounts on a Windows XP system. Computer Administrators can use this tool to create accounts, as well as manage existing ones. Limited users can use the tool to manage settings related to their own account only.

Follow these steps to create new user accounts in Control Panel:

1. Click Start → Control Panel → User Accounts. The User Accounts Pick a Task screen appears.
2. Click Create a new account.
3. The Name the new account screen appears, as shown in Figure 1-4. In the field provided, type a name for the new account. This is the name that will appear on the Windows XP Welcome screen and on the Start menu. Click Next.



Name the new account

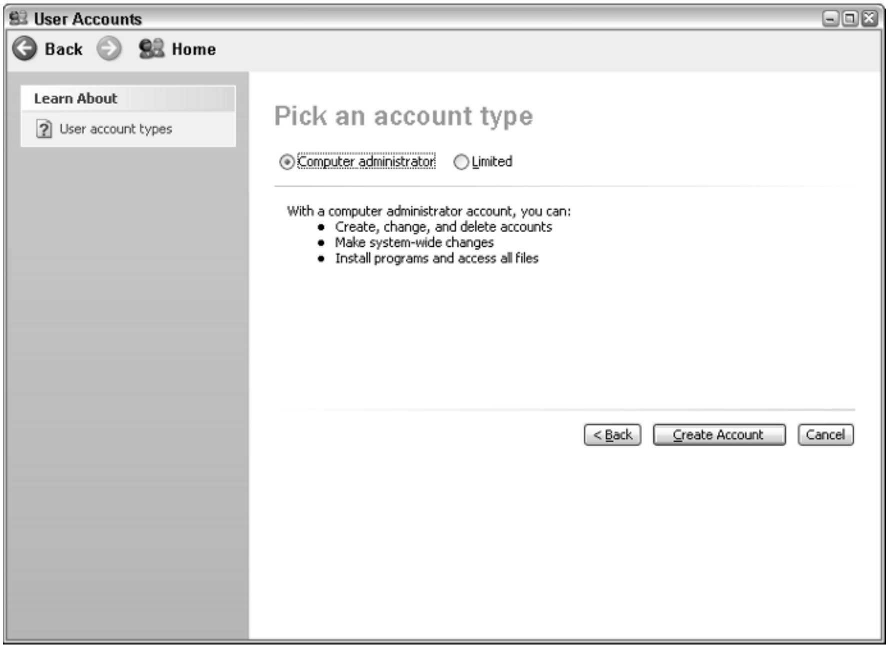
Type a name for the new account:

John

This name will appear on the Welcome screen and on the Start menu.

Figure 1-4: Supply the name for a new user account.

4. At the Pick an account type screen, select Computer Administrator or Limited (see Figure 1-5) and then click Create Account.



Pick an account type

◉ Computer administrator ○ Limited

With a computer administrator account, you can:

- Create, change, and delete accounts
- Make system-wide changes
- Install programs and access all files

Figure 1-5: Select the new user account's type.

Creating user accounts with Computer Management

If you're running Windows XP Professional, you also have the option of creating and managing user accounts using the Local Users and Groups tool in the Computer Management MMC (Microsoft Management Console). Although not as user-friendly as the Users Accounts applet in the Control Panel, this tool often appeals to more advanced users who like the convenience of having access to many system configuration tools from within a single console window.

Follow these steps to create user accounts on a Windows XP Professional system using Computer Management:

1. Click Start, right-click My Computer, and click Manage.
2. At the Computer Management window, expand the Local Users and Groups folder by clicking on the plus sign (see Figure 1-6).
3. Right-click the Users folder and click New User.
4. In the New User window, enter a user name, full name, and description for the account.
5. Enter a password for the user account and then confirm it.
6. Click Create. A new user account is created to match the information you supplied.

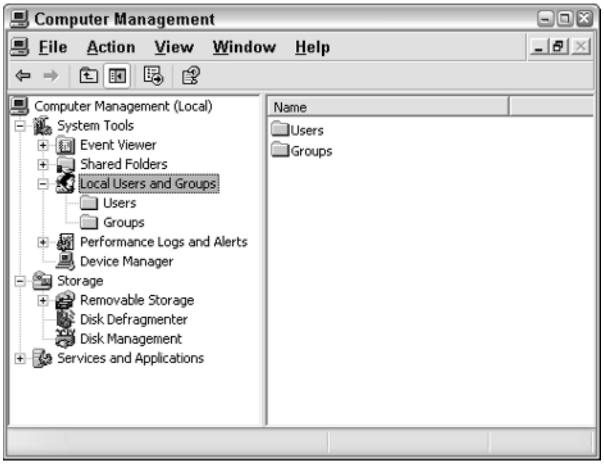


Figure 1-6: The Local Users and Groups tool is displayed in the Computer Management MMC.

Managing User Accounts

Creating user accounts is only part of the job of a Computer Administrator. After you create an account, occasionally you will need to manage it. Examples of security-related tasks associated with managing user accounts include the following:

- Changing account types
- Renaming accounts
- Adding, changing, and resetting passwords
- Disabling accounts
- Deleting accounts

Each of these tasks is explained in more detail in the following sections.

Changing user account types

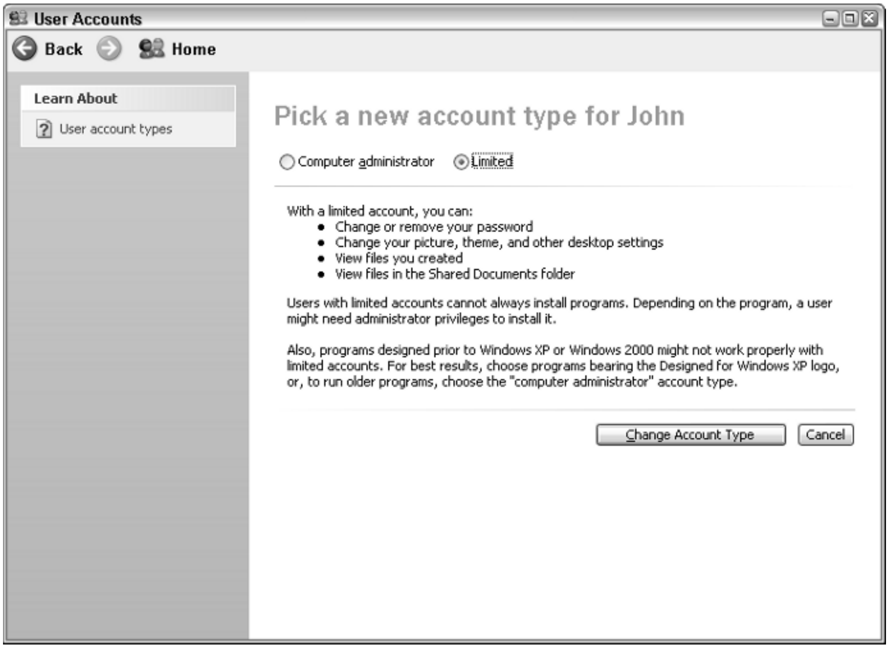
As you're now aware, using a Computer Administrator account as your everyday user account is not recommended. Thankfully, the User Accounts tool in Windows XP makes it easy to change an account from one type to another, such as switching a Computer Administrator account to a Limited user, or vice versa.

Follow these steps to change a user account's type:

1. Click Start → Control Panel → User Accounts.
2. Click the user account name whose type you want to change.

3. Click Change the account type.

4. Select the type to which the account should be changed, as shown in Figure 1-7.



Pick a new account type for John

○ Computer administrator ● Limited

With a limited account, you can:

- Change or remove your password
- Change your picture, theme, and other desktop settings
- View files you created
- View files in the Shared Documents folder

Users with limited accounts cannot always install programs. Depending on the program, a user might need administrator privileges to install it.

Also, programs designed prior to Windows XP or Windows 2000 might not work properly with limited accounts. For best results, choose programs bearing the Designed for Windows XP logo, or, to run older programs, choose the "computer administrator" account type.

Figure 1-7: You can change an existing user account's type with the User Accounts tool.

5. Click Change Account Type.

Note

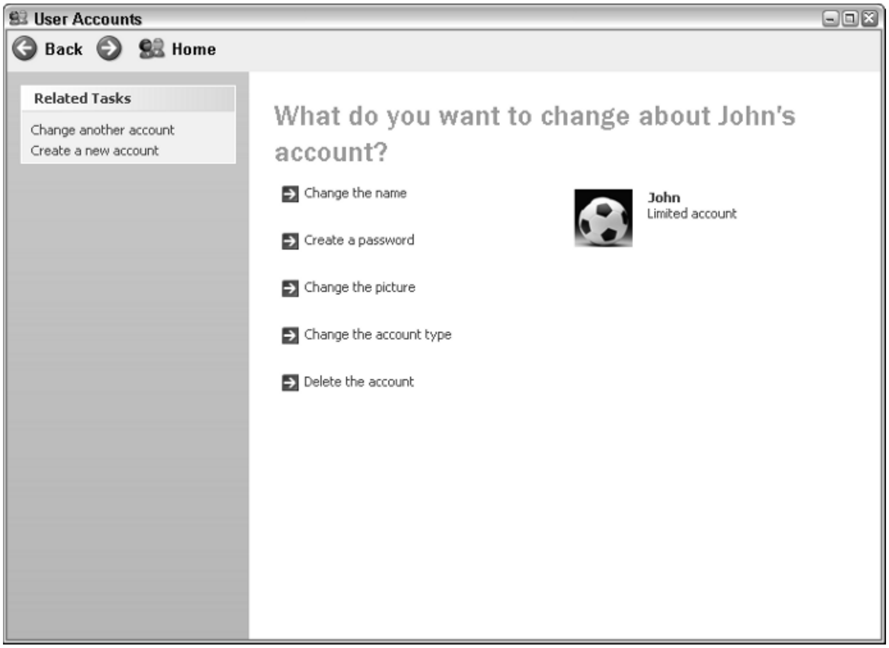
Only a Computer Administrator can change a user account's type. If the user whose account type is being changed is also logged onto the Windows XP system when the change is made, the new account type takes effect the next time the user logs on.

Renaming user accounts

Changing the name associated with an existing user account is significantly different than creating an account. When you rename an account, only the name is changed — the actual user account fundamentally remains the same. Accounts often are renamed in corporate environments to make the transition between a departing user and their replacement easier. If the account is renamed, the new user has the same rights and permissions as the old user, along with access to the old user's files and desktop environment. This is often preferable to creating an entirely new account and then configuring required rights and permissions manually. On a home PC, user accounts are typically only renamed when a user wants to change their onscreen display name.

Follow these steps to rename an existing user's account name in Control Panel:

1. Click Start → Control Panel → User Accounts.
2. Click the account you want to rename.
3. Click Change the name, as shown in Figure 1-8.



What do you want to change about John's account?

Figure 1-8: You can rename a user account.

4. Type a new name for the account and then click Change Name.

Tip

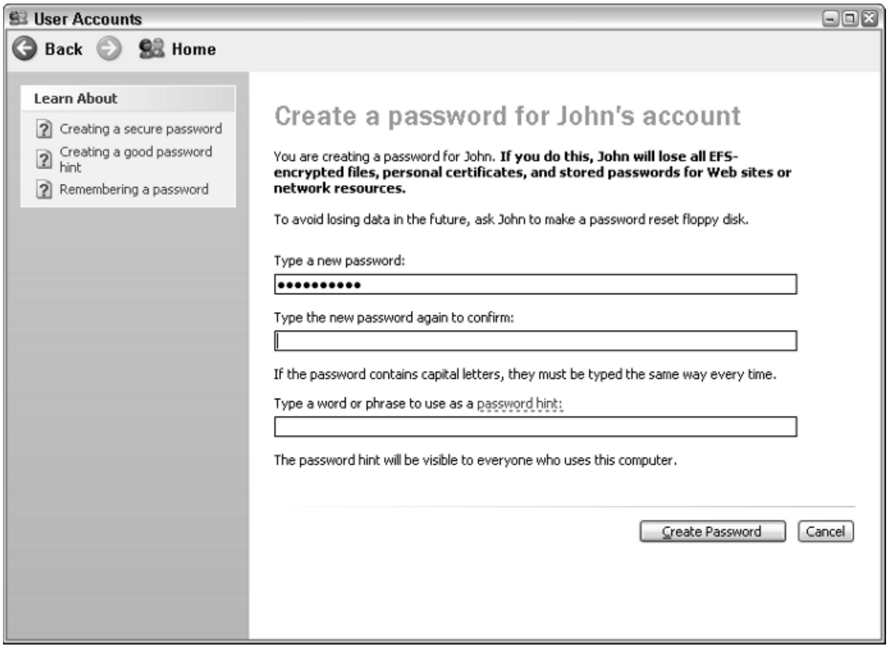
The built-in Administrator user account may be hidden from the Windows XP Welcome screen by default, but rest assured that hackers and others attempting to gain access to your computer know that it exists. Although you cannot delete this account, you can (and should) rename it to something less obvious. Choose a username for it that you'll remember and then assign it a sufficiently complex password. This isn't to say that changing the name of this account will keep a determined hacker out of your system, but it will foil less experienced users and make life a little more difficult for those in the know.

Managing user account passwords

Creating individual user accounts for every person that uses your Windows XP system is a great start, but it's only part of the story as far security is concerned. For user accounts to do anything more than act as a facility for separating user desktops and working environments, they must be assigned passwords. Every user should assign a password to their user account and, as a security/privacy precaution, be the only person who knows the password.

Follow these steps to add a password to an existing user account in Control Panel:

1. Click Start → Control Panel → User Accounts.
2. Click the name of the user account to which you want to add a password.
3. Click Create a password.
4. Enter the password for the user in the Type a new password box (see Figure 1-9).



Create a password for John's account

You are creating a password for John. **If you do this, John will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.**

To avoid losing data in the future, ask John to make a password reset floppy disk.

Type a new password:

●●●●●●●●●●●

Type the new password again to confirm:

If the password contains capital letters, they must be typed the same way every time.

Type a word or phrase to use as a password hint:

The password hint will be visible to everyone who uses this computer.

Figure 1-9: Adding a password to a user account is essential for system security.

5. Enter the same password again in the Type the new password again to confirm box.
6. Optionally, add a password hint in the Type a word or phrase to use as a password hint box.
7. Click the Create Password button.

Caution

Password hints exist to help you remember your password but are visible to all users from the Windows XP Welcome screen. If your hint is too obvious, other users may be able to guess your password. As a best practice, choose a password hint that makes sense to you but won't give your password away to others. Better still, don't configure a password hint at all.

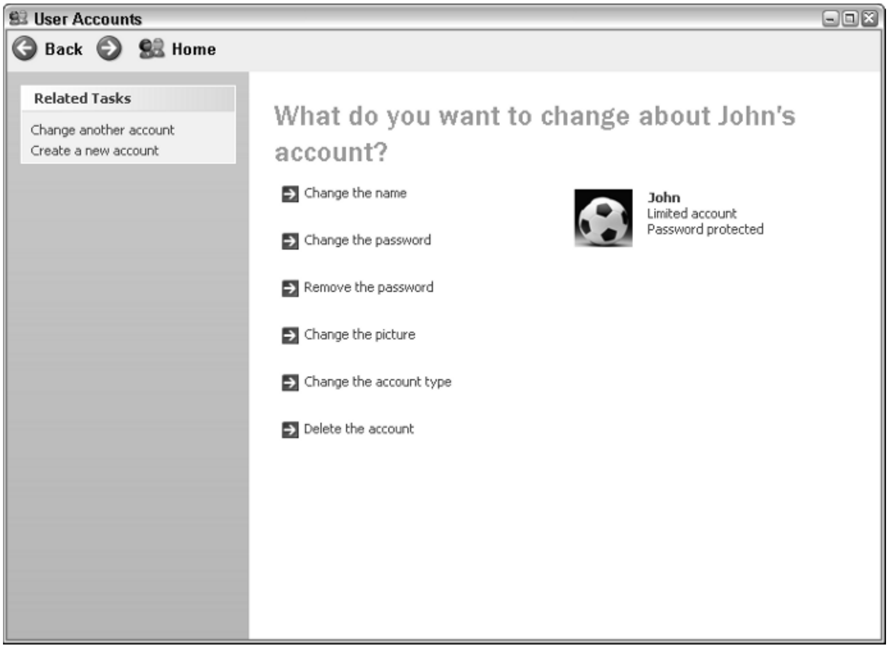
Adding a password to your user account is an important step forward, but if you're serious about security, make a point of changing your password at least once every month or so. The User Accounts applet in Control Panel makes it easy to change (or even remove) the password associated with your user account.

Caution

Toward the end of the Windows XP installation process, you're prompted to create at least one personal user account. If you opt to create only one, Windows XP uses this Computer Administrator account to automatically log you on, bypassing the Welcome screen. This behavior occurs because you haven't configured a password for the account; however, Windows XP can also be configured to log you on automatically when you do have a password, via configuration changes to the Registry. Many third-party "tweaking" and customization tools make this easy, but it's definitely not a good idea from a system security standpoint. Such "tweaks" store your password in the Registry in plain text, and going this route effectively eliminates all of the security benefits associated with having a password in the first place.

Follow these steps to change the password associated with a user account in Control Panel:

1. Click Start → Control Panel → User Accounts.
2. Click the name of the user account whose password you want to remove or change.
3. To change the user account's password, click Change my password (if this is your account) or Change the password (if you are the Computer Administrator). Figure 1-10 shows the options on the administrator's screen.
4. Enter the new password for the user account, confirm it, and optionally add a password hint.
5. Click Change Password.



What do you want to change about John's account?

John
Limited account
Password protected

Figure 1-10: Changing your user account password regularly to enhance security.

Tip

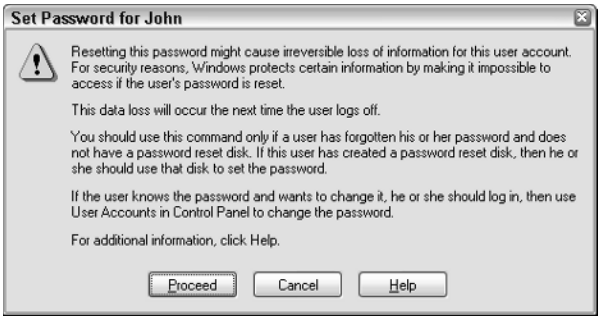
Assigning a password to all user accounts is important, even if you're the only person using a computer. Any accounts left unprotected make easier for hackers, viruses, and spyware, and that's a risk not worth taking. Additionally, if your computer is ever lost or stolen, not having a password assigned gives others easy access to any personal data or files stored on your system.

Occasionally you may run into an issue where someone has forgotten the password associated with their user account and cannot log on. Should this happen, a Computer Administrator can reset their password by changing it using the User Accounts tool, or by using the Set Password option in the Computer Management MMC.

Follow these steps to reset a forgotten password using Computer Management:

1. Click Start, right-click on My Computer, and click Manage.
2. In the Computer Management window, expand the Local Users and Groups folder.
3. Click the Users folder and then right-click on the user account whose password you want to reset.
4. Click Set Password.

5. Read the warning message that appears with respect to the dangers associated with resetting user password (see Figure 1-11). Click Proceed to continue.



Set Password for John

Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.

This data loss will occur the next time the user logs off.

You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he or she should use that disk to set the password.

If the user knows the password and wants to change it, he or she should log in, then use User Accounts in Control Panel to change the password.

For additional information, click Help.

Figure 1-11: The warning message is presented when a Computer Administrator attempts to set another user's password in Computer Management.

6. Enter the new password, confirm it, and click OK.

Caution

As a general rule, do not add, change, or reset passwords for other user's accounts except during the original account creation process. If you add, change, or reset a password on their behalf (even with the best intentions) that user will lose access to her encrypted files, stored Internet certificates, and stored Web site passwords. Instead, have the user log on and add a password to their account using the User Accounts applet in Control Panel.

Understanding that users may forget their passwords, Windows XP allows all users to create a password reset floppy disk. This disk allows a user to log on and change his password without the need to worry about losing access to encrypted files and other stored settings. You'll learn more about creating a password reset disk in Chapter 2.

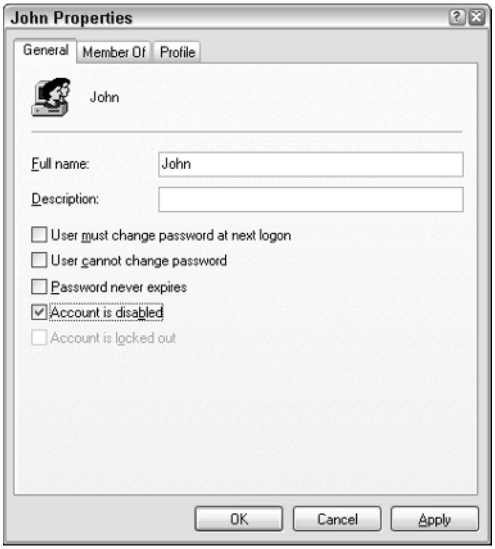
Disabling user accounts

Although it's not terribly common, you may encounter situations in which a person will not be using your Windows XP system for an extended period of time. In cases such as this, it makes good security sense to disable the account until it's needed again.

For a Windows XP Professional system, follow these steps to disable an existing user account using Computer Management:

1. Click Start, right-click My Computer, and click Manage.
2. At the Computer Management window, expand Local Users and Groups, and click the Users folder.

3. Right-click the user account you want to disable and click Properties.
4. Check the Account is disabled checkbox as shown in Figure 1-12 and then click OK.



John

Full name: John

Description:

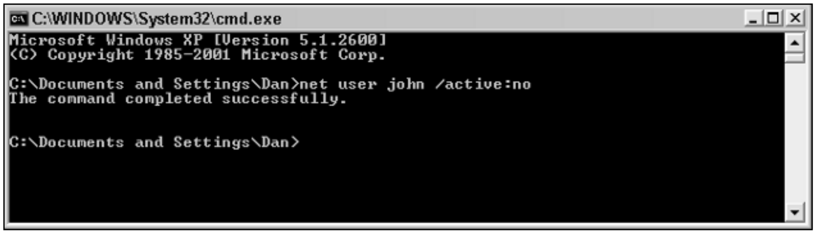
□ User must change password at next logon
□ User cannot change password
□ Password never expires
☑ Account is disabled
□ Account is locked out

Figure 1-12: Disabling a user account.

The User Accounts tool in Control Panel does not include an option to disable accounts (with the exception of the Guest account). As such, if you want to disable (or re-enable) user accounts on a Windows XP Home system, you need to use the Command Prompt to accomplish the task.

Follow these steps to disable or enable user accounts on Windows XP Home systems:

1. Click Start → All Programs → Accessories → Command Prompt.
2. To disable an account, at the Command Prompt, type `net user` *`username`* `/active:no` and then press Enter (see Figure 1-13), where *`username`* is the name of the account to be disabled.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dan>net user john /active:no
The command completed successfully.


C:\Documents and Settings\Dan>
```

Figure 1-13: Disabling a user account from the command line.

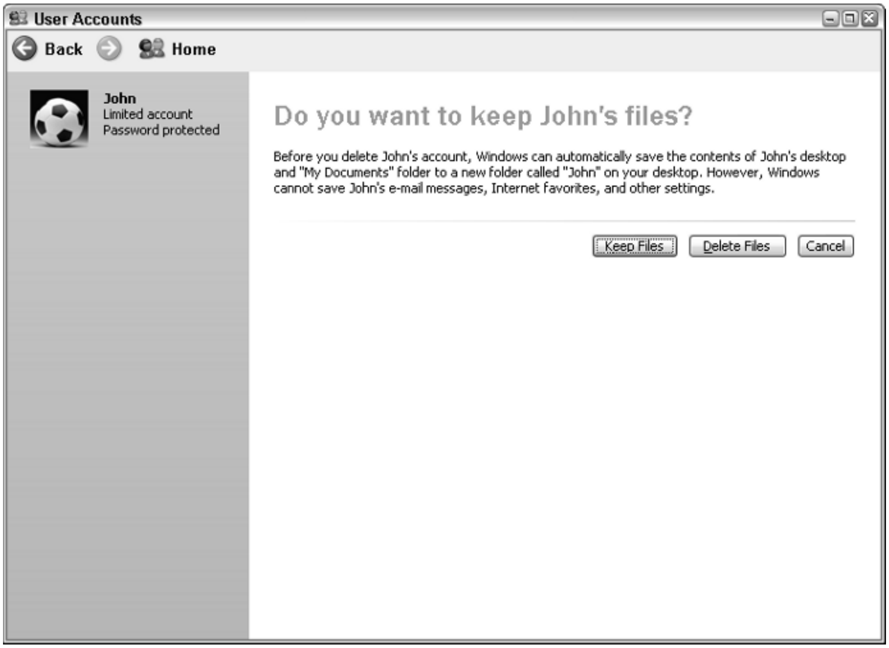
3. To enable a disabled account from the command line, issue the command `net user username /active:yes` and then press Enter.

Deleting user accounts

Creating individual user accounts is essential, but it's also important to delete user accounts that are no longer needed. If you believe that an account will be used again at some point in the future, disable it. If there's no chance that it will be again, deleting it is the more secure option.

Follow these steps to delete an existing user account in Control Panel:

1. Click Start → Control Panel.
2. Double-click User Accounts.
3. Click the user account name you want to delete.
4. Click Delete the account.
5. At the screen asking whether you want to keep the user's files, click Keep Files to save the contents of the user's My Documents folder to your desktop, or Delete Files to remove them, as shown in Figure 1-14.



John
Limited account
Password protected

Do you want to keep John's files?

Before you delete John's account, Windows can automatically save the contents of John's desktop and "My Documents" folder to a new folder called "John" on your desktop. However, Windows cannot save John's e-mail messages, Internet favorites, and other settings.

Figure 1-14: Options associated with deleting a user account.

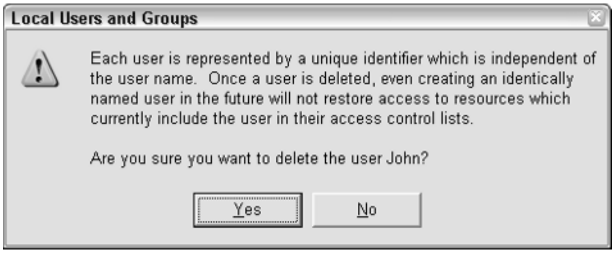
6. When prompted, click Delete Account.

What's in a Name?

After deleting a user account, would a new user account of the same name not smell as sweet? When it comes to how Windows XP deals with user account names, the answer is actually no.

Imagine that your system includes a user account named Mike. When this user is created on a Windows XP system, it is assigned an identifier value known as a Security ID, or SID. A SID is a series of numbers that uniquely identifies a given security principal (user or group) on your system. Windows XP identifies different users and groups using their SIDs but names like "Mike," "Administrator," or "Guest" simply exist to help the mere humans keep things straight.

The reason this is important is that Mike isn't always necessarily Mike. For example, if you create a user account named Mike, delete it, and then create another user account named Mike, the two accounts are not the same. They may have the same name, and even belong to the same person. As far as Windows XP is concerned, however, you've created one unique account (with a unique SID), deleted it, and then created another unique account (with its own unique SID). In other words, if the old Mike account had been granted any rights or permissions, or been made a member of any groups, the new Mike account is not automatically granted the same levels of access or membership. Similarly, the new Mike may not be able to access the old Mike's files. When you attempt to delete a user account in Computer Management on a Windows XP Professional system, a message to this effect is displayed, as shown in the following figure.



Each user is represented by a unique identifier which is independent of the user name. Once a user is deleted, even creating an identically named user in the future will not restore access to resources which currently include the user in their access control lists.

Are you sure you want to delete the user John?

Warning message displayed when you attempt to delete a user account.

What it comes down to is this — deleting an account and then creating another with the same name does not the same user make.

Caution

When preparing to delete a user account, think carefully about whether there's any possibility that the user's personal files will be needed again in the future. The User Accounts tool asks whether you want to save the contents of the user's My Documents folder to your desktop, but all other files associated with the account (including e-mail messages) will be lost. Strangely, things work differently when you delete a user account using the Local Users and Groups tool in Computer Management on a Windows XP Professional system. In this scenario, when a user account is deleted, all of that user's personal files and settings are left untouched. Although the User Accounts tool offers to save the contents of a user's My Documents folder as part of deleting an account, you may want to save the user's e-mail messages, Internet Explorer Favorites, and other personal files. The easiest way to do this is to back up the user's profile folder prior to deleting the account. To do this, open My Computer and browse to the C:\Documents and Settings folder (your drive letter may be different, depending on how you installed Windows XP). Next, back up the folder bearing the user's name. With a saved copy of this folder, files and settings associated with the user can be restored at a later time should the need arise.

Understanding Group Accounts

Although user accounts provide the credentials (a unique username and password) that an individual uses to log on to a Windows XP system, group accounts exist for a slightly different purpose. As you may have guessed, a group is a collection of users, or more specifically, user accounts. On a Windows XP system, groups are used to grant (or deny) collections of users different rights to perform tasks, or permissions to access files and folders.

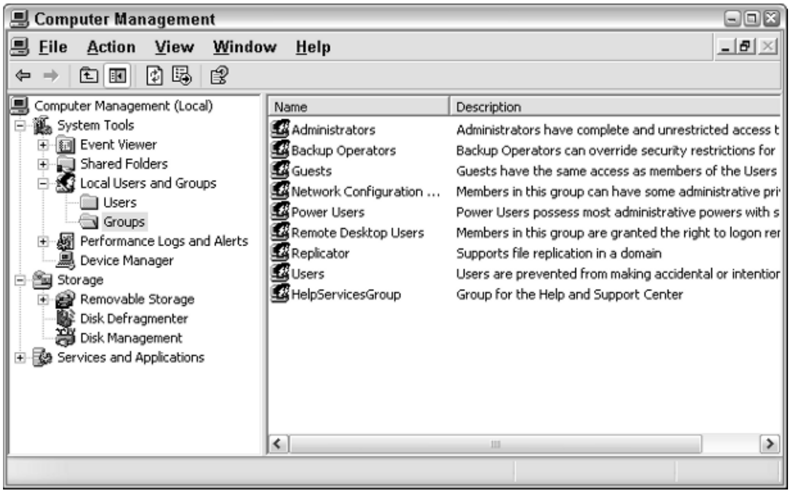
Windows XP includes a number of built-in groups by default, but Computer Administrators can also create custom groups to meet different needs. In a nutshell, groups exist to make life easier for system administrators — users with common needs can be placed into a group, and then that group can be assigned rights and permissions. When a user account is added to a group, it automatically inherits all of the privileges assigned to that group; therefore, instead of granting three different users the exact same level of access to a particular folder, an administrator could create a group, add the three users to it, and then assign the permissions for the folder to the group just once. If the group option sounds like more work initially, it is; however, after the group is created, adding rights or permissions to it again in the future becomes a great deal simpler that dealing with individual user accounts.

Exploring Windows XP's built-in groups

Windows XP Professional systems include nine different built-in groups by default, as shown in Figure 1-15.

Note

Windows XP Home does not provide access to the Local Users and Groups tool in Computer Management. As such, you can only modify group membership or create groups on Windows XP Professional systems. Additionally, group creation and management is limited to users with Computer Administrator accounts.



Name	Description
Administrators	Administrators have complete and unrestricted access t
Backup Operators	Backup Operators can override security restrictions for
Guests	Guests have the same access as members of the Users
Network Configuration ...	Members in this group can have some administrative pri
Power Users	Power Users possess most administrative powers with s
Remote Desktop Users	Members in this group are granted the right to logon rer
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentior
HelpServicesGroup	Group for the Help and Support Center

Figure 1-15: Windows XP's built-in group accounts.

Users accounts added to these groups automatically inherit the rights and capabilities associated with the group. Windows XP Professional's built-in groups include the following:

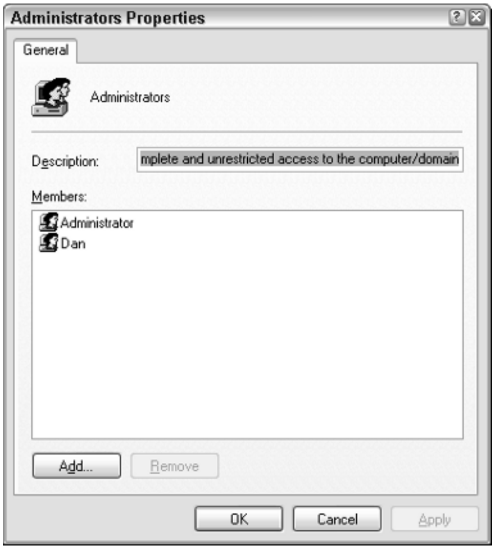
- **Administrators:** Membership in this group grants the user complete control over a Windows XP system. All Computer Administrator user accounts are members of this group.
- **Backup Operators:** Members of this group have the ability to back up and restore all user files, regardless of security restrictions.
- **Guests:** Members of this group are granted only basic access to a Windows XP system. By default, the Guest account is a member of this group.
- **Network Configuration Operators:** Members of this group have the ability to change network configuration settings, such as IP address settings.
- **Power Users:** Members of this group have more system access than Limited users, but less than Computer Administrators. Power users have the ability to install and remove most programs.
- **Remote Desktop Users:** Members of this group have the ability to log on to a Windows XP system remotely.
- **Replicator:** Members of this group are allowed to replicate files between systems in a domain network environment.
- **Users:** All user accounts created on a Windows XP system are members of the Users group.
- **HelpServicesGroup:** Members of this group can use the Help and Support center to remotely log onto and diagnose problems with a Windows XP system over a network.

Creating and managing groups with Computer Management

Windows XP Professional gives you the ability to add or remove users from group accounts, based on your specific needs. For example, you might want to add a user to the Backup Operators group to allow them to back up and restore files, or the Remote Desktop Users group to allow them to connect to and interact with your Windows XP system from another location. A user can be a member of multiple groups at the same time.

Follow these steps to manage the membership of an existing group on a Windows XP Professional system using Computer Management:

1. Click Start, right-click My Computer, and click Manage.
2. In the System Tools section, expand Local Users and Groups.
3. Click the Groups folder to view its contents. By default, Windows XP's nine built-in groups are listed.
4. Right-click the Administrators group and click Properties. The Members section of the General tab displays all user accounts that are currently a member of the Administrators group, as shown in Figure 1-16.



Administrators Properties

Administrators

Description: mplete and unrestricted access to the computer/domain

Members:
Administrator
Dan

Figure 1-16: Members of the Administrators group.

5. Click the Add button.
6. At the Select Users windows, type the name of user you would like to add to the Administrators group and then click OK. If you're unsure of the exact username of the user you would like to add, click the Advanced button.

7. To view a list of all users and groups that can be added to the Administrators group, click the Find Now button.
8. When the list of user and group accounts appear, select the user account you want to add to the group and then click OK. Click OK again to close the Select Users window.
9. If you mistakenly add a user to the wrong group, click the user's name and then click Remove.
10. Click OK to close the group properties window.

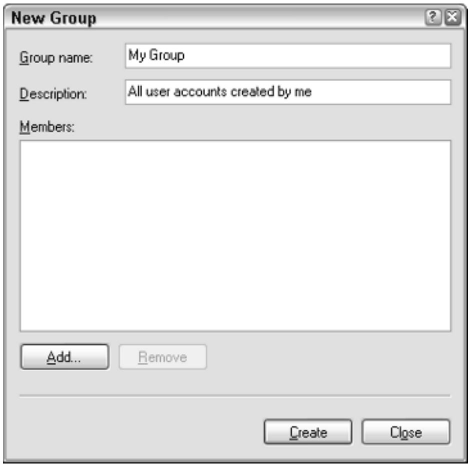
Note

When you add a user to a group, the change takes effect the next time the user logs on.

Beyond its built-in groups, Windows XP Professional also allows you to create your own group accounts for the purpose of assigning users different rights and permissions collectively, rather than individually. These custom group accounts come in especially handy when you want more control over how users interact with different files and folders, a concept you'll learn more about in Chapter 12. For the time being, it's enough to be familiar with how group membership is managed and how group accounts are created on a Windows XP Professional system.

Follow these steps to create a new group on a Windows XP Professional system using Computer Management:

1. Right-click the Groups folder in Computer Management and then click New Group.
2. Enter a name for the group and an appropriate description, as shown in Figure 1-17.
3. Click the Create button. Your new group is added to the list of accounts.



Group name: My Group

Description: All user accounts created by me

Members:

Figure 1-17: Creating a new group account.

Although you can use the General tab in the properties of a group to add or remove members as shown earlier, you can also complete this task from the properties of a user account. To add a user to a group using this method, follow these steps:

1. Click the Users folder. Right-click a user account and then click Properties.
2. Click the Member Of tab. All groups that this user is a member of will be displayed.
3. Click the Add button.
4. At the Select Groups window, type the name of group you would like to add this account to, and click OK. If you're unsure of the exact name of the group, click the Advanced button.
5. To view a list of all groups that this user can be added to, click the Find Now button.
6. When the list of group accounts appears, select the group to add the user to and then click OK. Click OK again to close the Select Groups window.
7. If you mistakenly add a user to the wrong group, click the group name on the Member Of tab and then click Remove.
8. Click OK to close the user properties window.

Any groups that you create can also be deleted. Deleting a group does not delete user accounts that are members of the group.

Cross-Reference

You'll learn more about group accounts and how they can be used to control access to files and folders in Chapter 12.

Exploring User Logon Options

It's entirely possible that Windows XP was preinstalled on your new computer with a single, password-free user account already configured. If that was indeed the case, it's also possible that you've never actually seen the Windows XP Welcome screen.

Strange as it may sound, this logon screen only appears on Windows XP systems with at least two user accounts configured, or when you finally get around to adding a password to your single user account. As should now be crystal clear, implementing user accounts (complete with passwords) is a key and critical step towards securing Windows XP.

Although the Welcome screen is the logon facility with which most Windows XP users are familiar, other methods can be used to log on or supply your user credentials (the combination of your username and password) to access your system. The primary logon methods supported by Windows XP include the following:

- The Welcome logon screen, which is configured by default
- The classic Windows logon screen, which prompts for a username and password
- The Run As command, which won't log you on to your personal desktop environment but is a logon method all the same

Each of these Windows XP logon options is presented in more detail in the following sections.

Welcome screen/Fast User Switching

Windows XP is the first Microsoft operating system to introduce the concept of the Welcome screen as a user logon facility. When used, the Welcome screen allows users to access their personal desktop environment by clicking their username and then typing their password, assuming one is configured. If the password supplied is correct, the user is logged on and able to go about their business.

In conjunction with the Welcome screen, Windows XP also introduces a new feature known as Fast User Switching. Understanding that Windows XP systems are shared by multiple users in many households, Microsoft decided that it would be a great idea to allow user switching, a technique whereby one user can temporarily log off, leave programs running and files open, and allow another user to log on to the system, perhaps to quickly check their e-mail. When the second user has completed their tasks, they can log off completely, or choose the option to switch users. The original user can then select their username at the Welcome screen and continue with their work as if they were never interrupted.

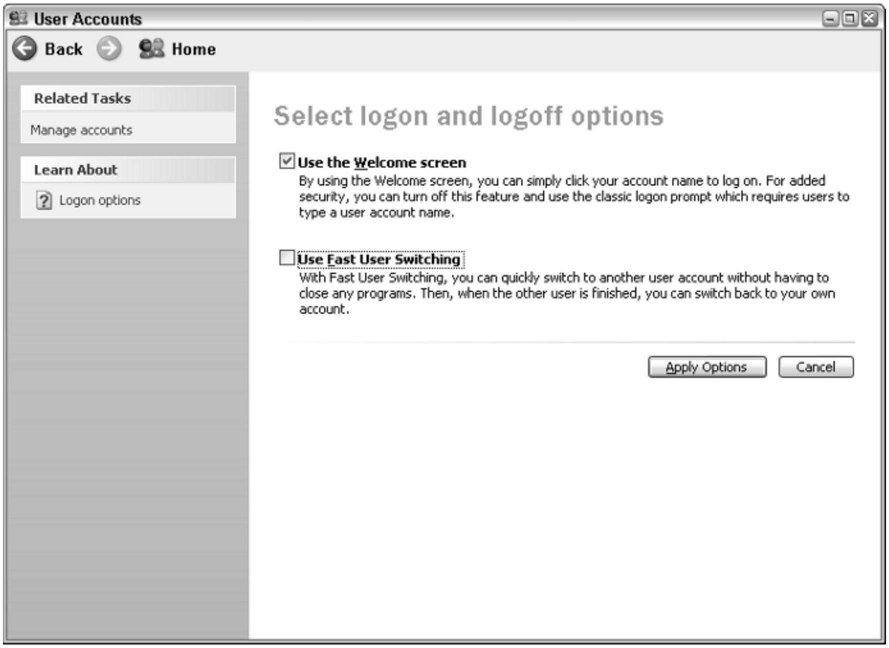
Obviously, Fast User Switching can be a very good thing. It eliminates the hassles of requiring one user to save their work, close all programs, and log off completely to allow another user to gain access to the computer for a short period of time. Also, switching users is a much faster undertaking that the full logon/logoff process that requires user profiles to be loaded and unloaded.

Even with these benefits, Fast User Switching does have a downside, namely much higher resource consumption. When this feature is enabled, users have a tendency to leave their accounts logged on all the time, complete with running programs. Multiply that by three or four logged-on users, and it doesn't take long for all of a system's memory to be consumed and significant slowdowns to ensue.

Love it or leave it, the good news is that you have a choice in the matter. Although Fast User Switching doesn't present a security risk, you can disable it if you want to avoid the performance hit associated with having multiple users logged on simultaneously.

Follow these steps to disable Windows XP's Fast User Switching feature:

1. Open the Control Panel from the Start menu.
2. Click User Accounts.
3. Under Pick a task, click Change the way users log on or off.
4. At the Select logon and logoff options screen (shown in Figure 1-18), uncheck the Use Fast User Switching option. If your goal is to use Fast User Switching, you may receive a message stating that the option cannot be enabled if Windows XP's Offline Files feature is enabled. Disabling Offline Files will remedy the issue, if encountered.



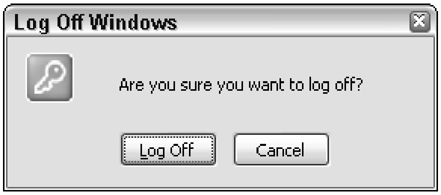
Select logon and logoff options

☑ Use the Welcome screen
By using the Welcome screen, you can simply click your account name to log on. For added security, you can turn off this feature and use the classic logon prompt which requires users to type a user account name.

□ Use Fast User Switching
With Fast User Switching, you can quickly switch to another user account without having to close any programs. Then, when the other user is finished, you can switch back to your own account.

Figure 1-18: Disabling Fast User Switching.

5. Click Apply Options to save your changes.
6. Close the User Accounts and Control Panel windows.
7. Click Start and then click the Log Off button. When the Log Off Windows dialog box appears (see Figure 1-19), notice that the Switch User option is no longer available. Click Log Off.



Are you sure you want to log off?

Figure 1-19: The Log Off Windows dialog box when Fast User Switching is disabled.

8. To log back on to Windows XP, enter your username and password and then click the green arrow button (or press Enter).

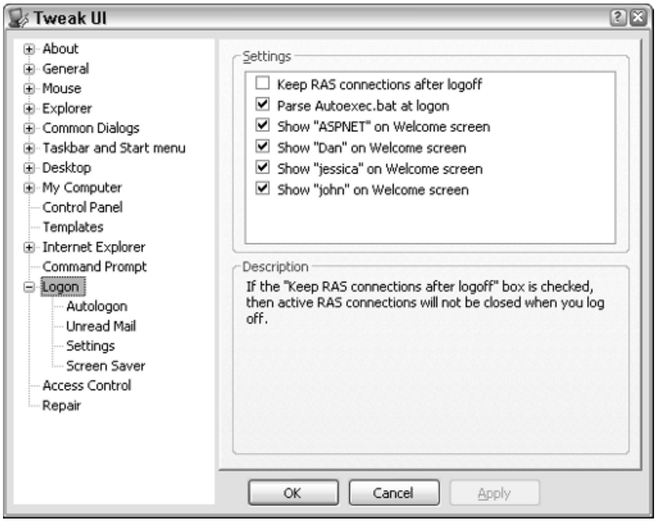
Tweaking Logon Settings

Most Windows XP users opt to use the Welcome screen to log on, if only because they're not aware that any other options exist. Truth be told, the Welcome screen is the most convenient logon environment for a multi-user Windows XP system, but it certainly is not the most secure option as far as user privacy is concerned.

Specifically, the Welcome screen automatically displays a list of all accessible user accounts on a system, with the exception of the built-in Computer Administrator account. Additionally, this screen also displays details about how many unread e-mail messages are waiting for other logged on users. Although this doesn't mean that one user can read another's e-mail, this behavior could be seen as infringing on other users' privacy.

Thankfully, the Windows XP Welcome screen (and the information it displays) can be controlled and customized. For example, you can opt to hide certain user accounts from being displayed, as well as do away with notifications about unread e-mail messages. All you need is a little help, which is available in the form of a free program download from Microsoft called TweakUI.

TweakUI is a Windows XP PowerToy, part of a set of different utilities that allow you to tweak and tune XP's behavior and get at settings that aren't normally accessible via Window's graphical configuration tools. While TweakUI provides access to no shortage of customizations (many of which will be examined throughout this book), the ones that are pertinent here are those in its Logon section, as shown in the following figure.



Settings

□ Keep RAS connections after logoff
☑ Parse Autoexec.bat at logon
☑ Show "ASPNET" on Welcome screen
☑ Show "Dan" on Welcome screen
☑ Show "jessica" on Welcome screen
☑ Show "john" on Welcome screen

Description

If the "Keep RAS connections after logoff" box is checked, then active RAS connections will not be closed when you log off.

TweakUI allows you to customize a variety of Windows XP settings, including some related to system security.

Specifically, clicking the Logon item allows you to control which usernames are displayed on the Welcome screen. Uncheck the box next to a username, and it no longer appears (although it still exists). If you want to stop seeing the ASP.NET account installed with the .NET Framework, for example, this is a great way to go about it.

A bit of a quandary would seem to exist if you were to stop regular user's names from appearing on the Welcome screen. The fact of the matter is that the Welcome screen is not the be all and end all of the logon process. In fact, you can log on using any enabled account from the Welcome screen by pressing the Ctrl+Alt+Delete keyboard sequence. This displays the classic Windows logon dialog box, where you can enter username and password details.

To stop the Welcome screen from displaying notifications about unread e-mail messages, expand the Logon section in TweakUI and click Unread Mail. Unchecking the Show unread mail on Welcome screen checkbox stops Windows XP from displaying details about your unread messages, but this setting can also be applied to all user accounts on your system.

To download TweakUI for Windows XP, visit `www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx`. Note that the latest version of TweakUI requires that your Windows XP system has at least Service Pack 1 installed.

Note

Only users with a Computer Administrator account can turn Fast User Switching on and off, and this feature cannot be disabled if more than one user is currently logged on to the computer. Additionally, while the Welcome screen is available when you boot a Windows XP system into Safe Mode, only Computer Administrator accounts are displayed and accessible — Limited users do not have access to a system running in Safe Mode.

Classic Windows XP logon

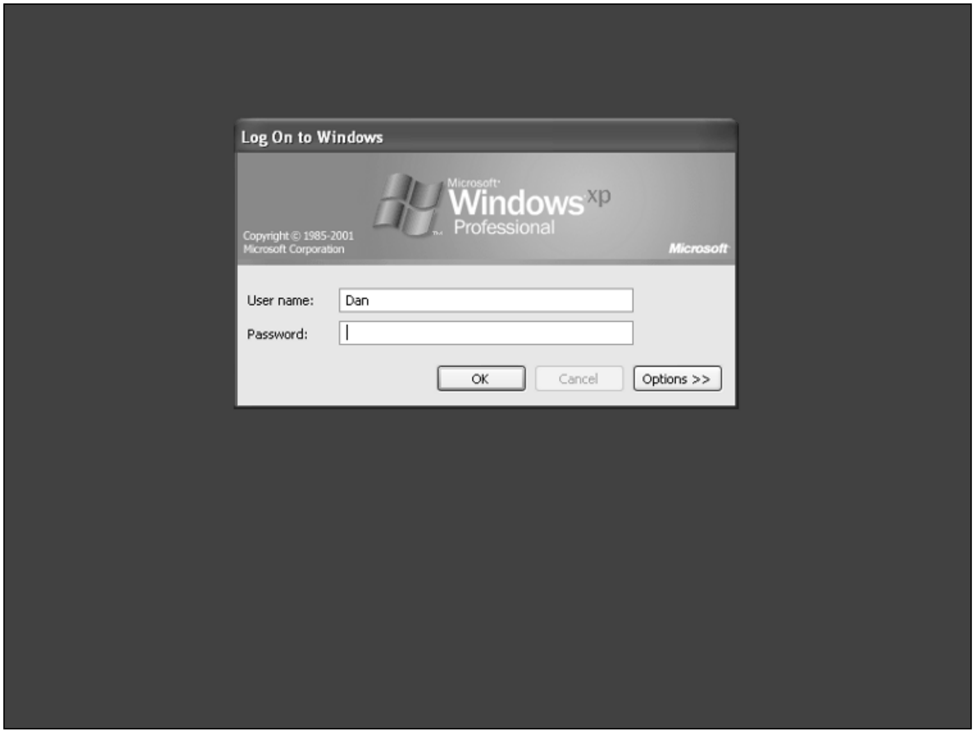
Windows XP's Welcome screen makes it easy for less experienced users to gain access to their user account — all they typically need to do is click their user name (which appears next to a fun little icon, of course) and enter their password. Although this method makes the entire logon process less frightening, it suffers from one serious security flaw, namely the fact that all user account names are displayed for the world to see. Worse still, the use of password hints can make determining the passwords associated with these accounts almost laughably simple.

With that in mind, any Windows XP owner who is serious about system security should consider passing on the Welcome screen logon in favor of the more secure classic Windows logon option. Although both perform the same basic user authentication process, the classic Windows logon screen doesn't suffer from the same rash of "helpfulness" that makes logging on from the Welcome screen not unlike a children's guessing game.

Follow these steps to disable the Welcome logon screen on a Windows XP system and use the classic Windows XP logon screen:

1. Open the Control Panel from the Start menu.
2. Click User Accounts.

3. Under Pick a task, click Change the way users log on or off.
4. At the Select logon and logoff options screen, uncheck the Use the Welcome screen checkbox. The Use Fast User Switching option will be disabled automatically, as it can only be used in conjunction with the Welcome screen.
5. Click Apply Options to save your changes.
6. Close the User Accounts and Control Panel windows.
7. Click Start and then click the Log Off button. When the Log Off Windows dialog box appears, click Log Off.
8. The Welcome screen has now been replaced with the Log On to Windows dialog box (Figure 1-20). To log back on to Windows XP, enter your password and then click OK.



User name: Dan

Password:

Figure 1-20: The classic Windows logon screen.

If you opt to use the classic Windows logon rather than the Welcome screen, you can add a little additional security into the mix by stopping Windows XP from displaying the name of the last user to logon to the system in the User name text box. Windows XP displays this name automatically, trying to save you from having to type in both your username *and* your password.

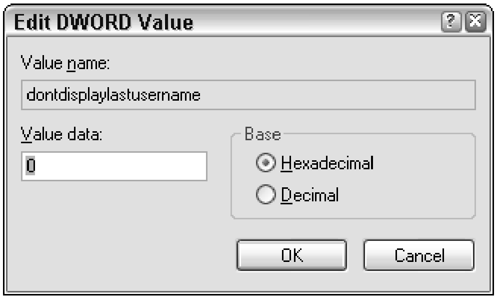
Unfortunately, as half of the information required to gain access to a Windows XP system, displaying a valid username automatically is not a good idea. With this information in hand, any malicious user who gains access to the computer needs only to guess or crack the account's password — typically not all that difficult a job. With this in mind, hiding the last username from appearing is a good security practice; typing this information adds a second or two to the logon process at most.

Note

See the related sidebar "Working with the Windows XP Registry" before attempting these steps.

Follow these steps to hide the username of the last person to log on to a Windows XP system:

1. Click Start ➝ Run and then type Regedit.exe in the Open text box. Click OK.
2. In the Registry Editor window, browse to HKEY_LOCAL_MACHINE ➝ Software ➝ Microsoft ➝ Windows ➝ CurrentVersion ➝ policies ➝ system.
3. In the right pane, double-click `dontdisplaylastusername`, as shown in Figure 1-21.



Value name: dontdisplaylastusername

Value data: 0

Base
● Hexadecimal
○ Decimal

Figure 1-21: Disabling display of the last username.

4. Change the Value data field from 0 (which displays the last username) to 1 (which means that the last username will not be displayed). Click OK.
5. Close the Registry Editor window and reboot Windows XP for the changes to take effect. When the Log On to Windows dialog box appears, the Username field should now be empty. To log back on to Windows XP, enter your username and password and then click OK.

Working with the Windows XP Registry

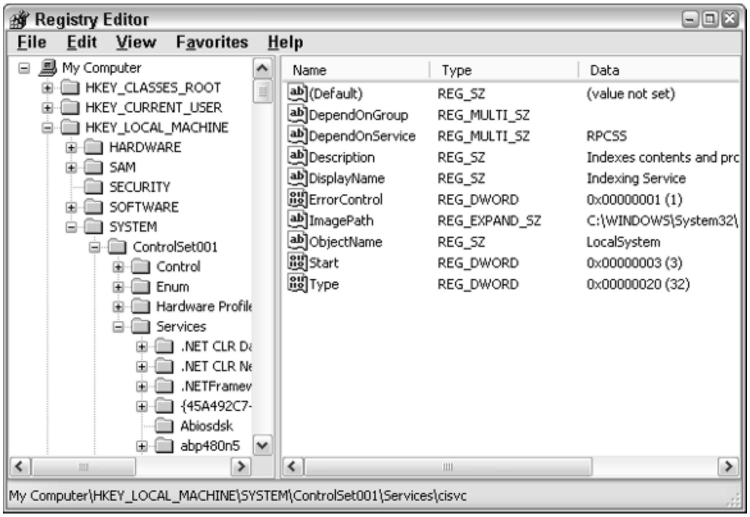
Back in the olden days, operating systems like MS-DOS stored all user and system configuration settings in what amounted to glorified text files. Things changed with the release of Windows 95, when a new centralized configuration database known as the Registry was introduced.

Windows XP continues to use the Registry as its primary storage database of user and system settings, but the vast majority of users never interact with the Registry directly. This is because Windows XP provides graphical tools that act as intermediaries for common configuration changes. For example, a user who wants to change his screen settings uses the Display applet in Control Panel, which in turn makes the necessary changes to the Registry.

In cases where Windows supplies a graphical or command-line tool for making configuration changes, it should be your primary choice. Quite simply, the Registry is a dangerous place where making any incorrect changes can affect system stability or even render it completely unable to boot. If you visit the Microsoft Web site and see Registry changes suggested, you'll always find accompanying warnings on the potential dangers of the undertaking.

Although there's no question that editing the Windows XP Registry can be dangerous, there are still times when you'll need or want to edit it directly — if only because no suitable graphical or command line tool exists to get the job done. With several Registry-related changes outlined in this book, it's important that you be familiar with the steps used to back up and restore portions of the Registry, should the need arise.

The primary tool used to edit the Registry is known, quite simply, as Registry Editor. To open this tool, click Start → Run, type Regedit.exe in the Open text box, and click OK. What you'll be presented with is what appears to be a folder hierarchy, complete with all sorts of crazy folder names and contents, as shown in the following figure. Note that the Registry is a "live" database of configuration settings, so you'll never be prompted to save your changes. This is but one reason why it's so important to be careful.



Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnGroup	REG_MULTI_SZ	
DependOnService	REG_MULTI_SZ	RPCSS
Description	REG_SZ	Indexes contents and prc
DisplayName	REG_SZ	Indexing Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\WINDOWS\System32\
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000020 (32)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\cisvc

Windows XP's Registry Editor is used to make changes to Registry settings.

Prior to adding, deleting, or editing any Registry setting, right-click the folder (known as a “key” in Registry-speak) where the change will be made. If you click Export, you’ll be prompted to save the key’s contents to a file with a .REG extension. Save this file to an appropriate folder as a backup. If you want to take a look at the contents of the file out of curiosity, just right-click it and select Edit to open it in Notepad.

Should you need to restore the Registry settings saved in a .REG file, all you need to do is browse to the file and double-click it. You’ll be presented with a message asking you to confirm that you want to add the contents of the file to the Registry. After you click OK, the Registry key in question is overwritten with the backed up settings.

You can also back up the entire Registry, but this is a longer and somewhat more arduous process. The Backup utility included with Windows XP is capable of getting this done by selecting the option to back up an object known as System State. For details on using Windows Backup to get the job done, visit `support.microsoft.com/kb/308422/`.

Run As

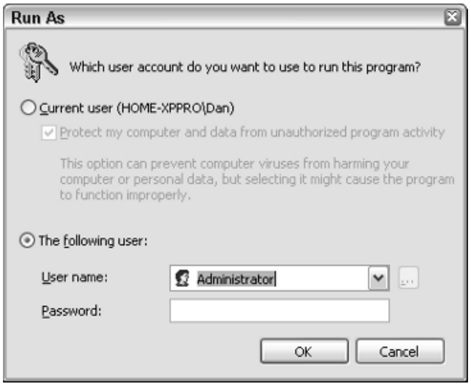
Earlier in this chapter you were led to believe that a way existed for a Limited user to perform tasks requiring the powers of a Computer Administrator—without the need to log off and back on, no less. Well, it’s actually true, the product of a Windows XP feature known as Run As.

Run As is a feature available on both Windows XP Home and Professional systems that allows you to open a program or install software by supplying alternate user account credentials for that particular task only. For example, imagine that you’re logged on with your Limited user account, and need to install a new piece of software. Rather than log off and then log on with a Computer Administrator account to complete the task, you can use the Run As command to open the program’s installer file. As part of doing this, you’ll be prompted to supply the username and password associated with an account allowed to carry out such a task, in this case a Computer Administrator.

Assuming that you’ve supplied a valid username and password, the installation process (and that particular process only) will proceed as it normally would for a Computer Administrator. When it’s done (the installation is complete, or the program that you opened is closed), the privileges associated with the account used with the Run As command effectively disappear until you use it again.

Follow these steps to open or install a program using the credentials of another user account via the Run As feature:

1. Click Start → My Computer.
2. Browse to the program file or shortcut that you wish to open using another user’s credentials.
3. Right-click the file and then click Run as.
4. When the Run As dialog box appears, click The following user, as shown in Figure 1-22.
5. Enter the name of the alternate user account in the User name field.
6. Enter the password associated with the user account in the Password field.



Run As

Which user account do you want to use to run this program?

○ Current user (HOME-XPPRO\Dan)

☑ Protect my computer and data from unauthorized program activity

This option can prevent computer viruses from harming your computer or personal data, but selecting it might cause the program to function improperly.

● The following user:

User name: Administrator

Password:

Figure 1-22: The Run As window.

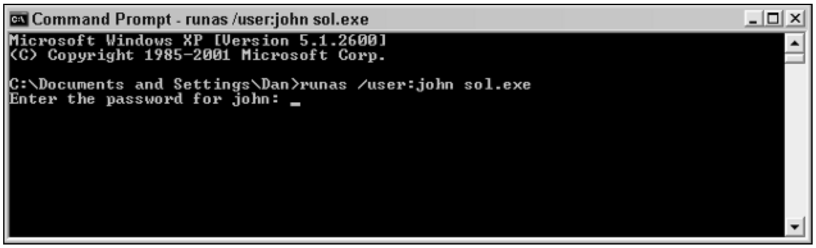
7. Click OK. The program opens and functions according to the rights and privileges associated with the user account information supplied.

8. Complete the required task(s) and then close the program. Your privilege levels are again those associated with the account you originally used to log on to Windows XP.

An alternate version of Run As is available to those who prefer working from the Windows XP Command Prompt, in the form of the `runas.exe` command. The basic syntax of the command is:

```
runas /user:username program
```

Username is user account name that will be used to launch the program or shortcut file specified. After this command is entered, you're prompted to supply the user's password, as shown in Figure 1-23. For a complete breakdown of switches and settings associated with the `runas` command, enter `runas /?` at the Command Prompt.



Command Prompt - runas /user:john sol.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dan>runas /user:john sol.exe
Enter the password for john: _
```

Figure 1-23: Using runas.exe from the Command Prompt.

Tip

The Run As command makes it practical for everyone to use a Limited user account for day-to-day business on a Windows XP system; however, if you use the command frequently it can be difficult to keep track of which credentials have been used to open a certain program or process. Rather than guess or need to dig through process details in Task Manager, consider downloading and installing PrivBar. This add-on toolbar for Windows Explorer and Internet Explorer displays the username and privilege level (for example, member of Administrators) associated with the user that opened the program. With this toolbar installed, you'll never be in the dark about the powers associated with a particular Explorer or IE window. For details on installing and configuring PrivBar, visit blogs.msdn.com/aaron_margosis/archive/2004/07/24/195350.aspx.

Using Run As with Windows Explorer

Although the Run As command works perfectly with just about any EXE file or shortcut you need to launch, it does not function as you might expect with Windows Explorer. In fact, if you try to launch Windows Explorer with the Run As command, what you'll find is that exactly nothing appears to happen.

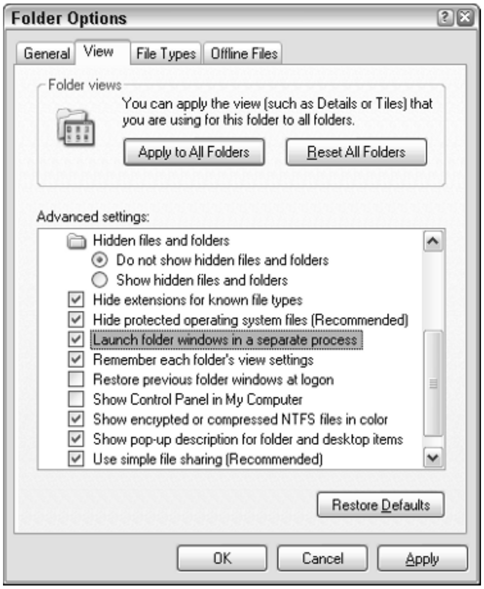
In fact, something does happen, but you don't see it. Windows Explorer is not only a tool for browsing for files and folders, but also the Windows XP shell process that supplies you with your desktop, Start menu, and more. By default, Windows XP does not allow two versions of Windows Explorer to run under different user credentials at the same time. So, when you use the Run As command to open Explorer.exe as a different user, the system sees that Windows Explorer is already running, and closes the newer process, sight unseen.

This default behavior is somewhat annoying, especially because Windows Explorer is such a powerful tool for system administration — it provides the capability to launch and install programs, access Control Panel tools, and more. Thankfully, it is possible to get around the issue by following these steps:

1. Log on to Windows XP system using your Computer Administrator account.
2. Click Start → My Computer.
3. Click Tools → Folder Options.
4. Click the View tab.
5. Scroll down the list of Advanced settings, check Launch folder windows in a separate process as shown in the figure, and click OK.

Continued

Using Run As with Windows Explorer (Continued)



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Hidden files and folders
- ● Do not show hidden files and folders
- ○ Show hidden files and folders
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☑ Launch folder windows in a separate process
- ☑ Remember each folder's view settings
- □ Restore previous folder windows at logon
- □ Show Control Panel in My Computer
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☑ Use simple file sharing (Recommended)

Configuring Windows XP to launch folder windows in a separate process.

6. Log off and then log back on with your Limited user account.
7. Use the Run As command to open Windows Explorer, specifying the username and password of your Computer Administrator account.

After completing these steps, you can now open Windows Explorer under the credentials of your Computer Administrator account while logged on with your Limited account.

Summary

The security of any Windows XP system is only as good as the security associated with its user accounts, groups, and logon settings. Keep the following points in mind when it comes to maximizing the security of your system:

- Each user should have a personal user account.
- Every user account should have a password configured.
- A user's everyday user account should always be of the Limited type.

- Only trusted users should be granted access to a Computer Administrator account. Even with this access, this account should not be used for everyday tasks.
- User accounts that will not be used for an extended period of time should be disabled.
- Users accounts that are no longer needed should be deleted.
- It's important to be familiar with Windows XP's built-in groups, the capabilities they assign to members, and how to create new groups if required.
- For better security, use the classic Windows logon screen (with the last username hidden) rather than the Welcome screen.
- Use the Run As command to perform administrative tasks when required.