Part 1

Installation and Startup

In this section:

- **Chapter 1: What's New in Windows XP**
- **Chapter 2: Standalone Installations**
- **Chapter 3: Reaping the Rewards of Network, Automated, and Unattended Installations**
- **Chapter 4: Gaining Control of Windows XP Startup and Shutdown**

Chapter 1

What's New in Windows XP?

Windows XP suffers somewhat from a dual personality. In some ways it's a significant release, but in others it's more a maintenance release of Windows 2000. For that reason, Windows 2000 users won't see many major changes other than the interface, although numerous changes under the hood improve Windows' performance and functionality. In addition, new features and accessory applications in Windows XP simplify tasks that were a bit more difficult in Windows 2000.

For Windows 9*x*, Me, and NT users, Windows XP is a significant change. Not only is the interface considerably different, but the underlying core operating system is completely changed, with several core features either new or improved. The biggest transition is for users migrating from Windows 9*x* and Me to Windows XP—the additional security features, file system options, and management features in XP make it a distinct shift.

Now, enter Windows XP Service Pack 2. Some consider this a major update to Windows XP, but I see it more as a security overhaul for Windows. Windows Firewall has some significant changes, and Internet Explorer and Outlook Express include more minor changes targeted primarily at Internet security. There are several other changes as well, but users won't see a dramatically different Windows environment or a cornucopia of new accessory applications. Still, SP2 is a major step toward enhancing Windows XP's security and performance overall and well worth installing.

This chapter explores the new and changed features in Windows XP. In addition to an exhaustive feature list, I've included sections that will help users of specific Windows platforms get up to speed quickly on Windows XP's features and functions. The chapter also includes a quick overview of SP2's features. You'll find these features covered throughout the rest of the book where appropriate.

Major Differences between Home Edition and Professional

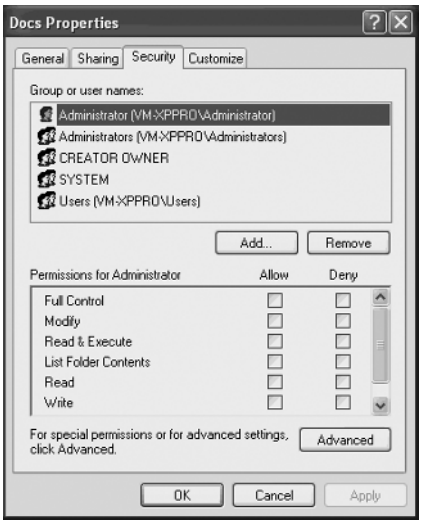
Windows XP is available in two versions: Home Edition and Professional. Many of the features are the same from one to the other, and both have the same look and feel. Because it's targeted at business users, Professional includes features that aren't really necessary for home users, such as added security, centralized administration, and remote access. The following sections provide a brief overview of the features included in the Professional version that aren't available in Home Edition.

Access Control

When you're sharing a folder under all Windows operating systems, including Windows XP, you can specify *share permissions* that control the level of access that users have to the folder across the network. For example, you might grant users the ability to read the contents of a folder but not to write to it. Both Professional and Home Edition offer the ability to share folders and set share permissions to control access.

Windows XP Professional adds the ability to apply *access control lists* (ACLs) to folders on NTFS volumes. An ACL is a set of specific access permissions for a folder or file granted to specific users or groups. For example, you might grant one group of users the ability to read the contents of a folder and grant another group full control over the contents, including the ability to modify and delete items. Figure 1.1 shows the Security tab of a folder's properties, which you use to configure permissions on the folder.

FIGURE 1.1
Use the Security tab to specify permissions for a folder.



TIP You can apply permissions on a folder or file only on NTFS volumes. FAT volumes support sharing permissions but don't allow you to assign permissions for folders or files.

Permissions you set through ACLs apply for both local and network access. For example, if you don't have permission to read a folder, you'll be unable to read the folder even if you log on locally to that computer.

NOTE For more information on setting sharing security, see Chapter 18.

Centralized Administration

Windows XP Professional systems can function as stand-alone computers, as members of a workgroup, or in a domain served by Windows NT Server, Windows 2000 Server, or Windows Server 2003 domain controllers. Windows XP Home Edition computers can function as stand-alone computers or as members of a workgroup but don't support domain membership. Domains provide several centralized administrative features, with *centralized security* being one of the most important of those features. Centralized security refers to the ability to control access to resources on multiple systems across the network with a single set of user credentials (account and password).

Domains also provide other important functionality, including the abilities to remotely manage systems and to enforce restrictions and other system properties through group policy.

NOTE For an explanation of group and local policies, see Chapter 35. Specific uses of group policy are explained in other chapters where applicable.

Encrypting File System

Encrypting File System (EFS) is a core component of Windows XP Professional that isn't available in Home Edition. EFS lets users encrypt folders and files to prevent others from being able to read those files. EFS can be an important tool for protecting data on systems that are susceptible to compromise, such as notebook computers that could be lost or stolen. EFS is also useful for protecting data on removable media.

NOTE For a detailed discussion of EFS, see Chapter 42.

It's easy to encrypt a folder or file in Windows XP: You simply select a check box in the folder's or file's properties, as shown in Figure 1.2. Windows XP takes care of the encryption and decryption process automatically. However, you should implement an EFS recovery policy, as explained in detail in Chapter 42, to ensure your ability to recover encrypted files if the encryption certificate becomes corrupted or is lost.

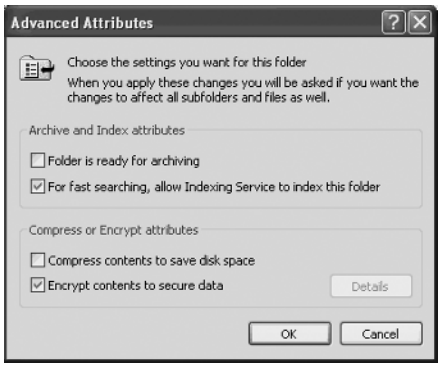


FIGURE 1.2
You can easily encrypt a folder or file through a single check box in its properties.

Group and Local Policies

Group policy is another feature supported by Windows XP Professional that isn't supported by Windows XP Home Edition. Group and local policies allow a broad range of properties and restrictions to be applied to Windows XP for a specific computer or user. For example, an administrator can use group policy to redirect a user's `My Documents` folder to a network server, so that the folder is always available regardless of the user's logon location and can be easily backed up.

Group policy has much broader implications than just managing a user's data, however. It provides a means for *change control*, which is the ability to regulate the changes that users can make to their systems and Windows environment. Group policy is also the mechanism through which technologies such as Remote Installation Services (RIS) and IntelliMirror allow administrators to automatically deploy operating systems and applications to computers across the enterprise.

NOTE Group policies rely on Windows 2000 Server or Windows Server 2003 domain controllers and domain membership. You can apply local policies to Windows XP Professional computers in a domain, workgroup, or stand-alone configuration.

NOTE For a complete discussion of group and local policies and their implications, see Chapter 35.

Multilingual User Interface Add-On

Windows XP is currently available in numerous localized versions in addition to English. Localization provides menus, dialog boxes, and other elements in a specific language. The Multilingual User Interface Pack is an add-on for Windows XP Professional that allows administrators to switch the user interface elements such as menus, dialog boxes, and Help files into a different language. For more information on this add-on, see `www.microsoft.com/technet/prodtechnol/winxppro/evaluate/muiovw.mspx`.

Offline Files

Windows XP Professional includes a feature called Offline Files, which allows users to continue to work with network resources even when those resources are unavailable or disconnected from the network. For example, assume a server in your network provides access to a set of common documents that you need to use on a regular basis. Most of the time you're in the office and connected to the network, which means the documents are available from the server. Occasionally, however, you need to use your notebook while out of the office and still work with those documents. With Offline Files, Windows XP creates a local copy of the offline resource on your computer and lets you work with the resource there rather than from its network location. XP makes the transition between online and offline use transparent to the user and provides the mechanism to automatically synchronize changes when the network resource again becomes available.

TIP You can't use Offline Files on a system that has Fast User Switching enabled. Configure Fast User Switching through the option "Change the way users log on or off" in the User Accounts object in Control Panel.

You enable Offline Files for a particular folder through the Offline Files tab of the folder's properties (see Figure 1.3).

FIGURE 1.3 Enable Offline Files through the Folder Options dialog box.

Remote Desktop Connection

Remote Desktop Connection allows you to work with a Windows XP Professional computer from a remote location. For example, you might use Remote Desktop Connection to connect from your home computer to your office computer, in order to access files, printers, or other resources, working with your office PC as if you were physically in the office. You can also use the client portion of Remote Desktop Connection to connect to a Windows 2000 or 2003 Terminal Server.

Windows XP Home Edition includes the client portion of Remote Desktop Connection, enabling you to connect to a Windows XP Professional computer that is configured to allow access to Remote Desktop users (Figure 1.4), or to a Terminal Server. You can't connect to a Windows XP Home Edition computer through Remote Desktop—Home Edition doesn't include the server-side components of Remote Desktop.

FIGURE 1.4
Use Remote Desktop to connect to and use a system remotely.

TIP A handful of third-party applications, such as pcAnywhere, VNC, and Unicenter Remote Control, provide capabilities similar to Remote Desktop for remote access and control. These third-party apps typically provide expanded functionality, such as the ability to let the local user continue working while the remote session is active.

NOTE For more information on Remote Desktop Connection and its alternatives, see Chapter 23.

Remote Installation Services

Windows XP Professional includes support for Remote Installation Services (RIS), which lets you install Windows 2000, XP, and 2003 on a computer remotely. In a typical RIS deployment, the computer boots from a PXE-compliant network adapter, which allows it to submit a request to a RIS

server for service. (PXE stands for Preboot Execution Environment, an open industry standard that allows the system to boot directly from a PXE-compliant network card to initiate an operating system installation or repair.) The RIS server provides the client computer with OS installation options based on the computer's membership in Active Directory. After the user selects the OS options to install, RIS installs the operating system across the network. A system that doesn't include a PXE-compliant network adapter can use a special boot disk created by RIS to allow it to communicate with available RIS servers at boot.

TIP RIS relies on the Active Directory and therefore requires domain membership. Windows XP Home Edition systems don't support RIS.

RIS is primarily a server-side feature requiring either Windows 2000 Server or Windows Server 2003, and it must be configured and managed by a system administrator. For that reason, RIS isn't covered except in passing in this book.

TIP For a detailed discussion of RIS, see *Mastering Windows 2003 Server* by Mark Minasi (Sybex, 2003).

Roaming User Profiles

A *user profile* is a collection of folders and data that make up the majority of a user's working environment. A user's profile includes the `My Documents` folder, Start menu, Desktop, and other folders. On stand-alone computers and in many network installations, the user profile resides on the local computer. The disadvantage to this is that when you log on from another computer, you don't receive the same desktop settings, documents, or other environment settings as when you log on from your primary workstation. A *roaming* profile overcomes that disadvantage by storing your profile on a network server and copying it to the current logon location. This means that you have the same Desktop, documents, and settings regardless of where you log on—in other words, your working environment follows you around the network.

Scalable Processor Support

Windows XP Home Edition supports a single processor. Windows XP Professional supports up to two processors to provide better performance.

Folder Redirection Complements Roaming Profiles

As explained in Chapter 37, you can redirect folders from the default profile location to a network server. For example, you might redirect `My Documents` to a folder on the server. When the user logs on and opens the `My Documents` folder, he sees the files stored in his folder on the network server, rather than the `My Documents` folder that would otherwise be stored on his local computer. Redirecting folders in this way helps ensure that the user's documents are always available regardless of logon location. In some ways this might seem to be exactly what roaming profiles achieve. However, folder redirection and roaming profiles are different.

If a user had a roaming profile without folder redirection, the folder would be copied from the server where the profile is stored to the user's local computer at logon. With folder redirection, the folder remains on the server, and the user's computer is redirected to the server when she opens the folder. Folder redirection therefore complements roaming profiles and reduces the amount of data that must be copied across the network during logon.

Software Installation and Maintenance

With Windows 2000, Microsoft introduced a feature called IntelliMirror, which is an umbrella term for a selection of technologies. Windows XP Professional also includes support for IntelliMirror. One of IntelliMirror's major purposes is to let applications be installed, updated, and managed automatically. When a user logs on, group policy and Active Directory membership determine which applications should be installed on the user's computer and which should be made available as an option. Applications that are *assigned* through IntelliMirror appear as if they're already installed on the user's computer. Attempting to start the application causes it to be installed automatically across the network. Applications that are *published* through IntelliMirror are available for installation but aren't installed automatically. Instead, the user can add these applications through the Add Or Remove Programs object in Control Panel.

Most aspects of IntelliMirror are primarily server-side features and are configured and managed at the server level. For that reason, software installation and maintenance are covered only in passing in this book.

TIP For more information on IntelliMirror and automated application deployment, see *Group Policy, Profiles, and IntelliMirror for Windows 2003, Windows 2000, and Windows XP* by Jeremy Moskowitz (Sybex, 2004) and *Windows 2000 Automated Deployment and Remote Administration* by Christa Anderson (Sybex, 2001).

Windows XP Service Pack 2 Overview

New!

Windows XP Service Pack 2 (at one point called Windows XP Reloaded) incorporates several updates to Windows XP, many targeted at security. XP's features are discussed throughout this book, but this section offers a quick overview to get you up to speed on the new features and changes included in SP2. This section isn't intended to provide a detailed look at each feature but rather to give you a feel for what SP2 contains.

Changes in Networking and Network Security

One of the major changes in SP2 is the introduction of Windows Firewall (Figure 1.5), a replacement for the Internet Connection Firewall (ICF) in Windows XP SP1a and earlier. Windows Firewall incorporates several improvements over ICF, including the following:

Boot-time security Windows Firewall is enabled during boot with a predefined configuration that prevents connections on all but a limited set of ports. Basic network functions such as DHCP, DNS, and application of group policy are allowed, but other traffic is denied. This protects systems during boot until the user's firewall configuration takes over.

Global configuration Changes that you make in Windows Firewall apply to all interfaces, simplifying configuration. However, you can still apply unique settings and exceptions to individual interfaces as needed.

Local subnet restriction You can configure the scope for incoming traffic to restrict it to your own subnet, to all computers, or to a custom list. Local subnet restriction makes it easy to allow connections from your local network while denying those same connections if attempted from the Internet.

Command-line support The Netsh console command in SP2 now provides command-line configuration and management of Windows Firewall.

On With No Exceptions mode This mode denies all unsolicited incoming traffic and effectively locks down the computer for everything except solicited outgoing connections without requiring you to reconfigure the firewall's port settings. You can switch back to normal mode with a single mouse click.

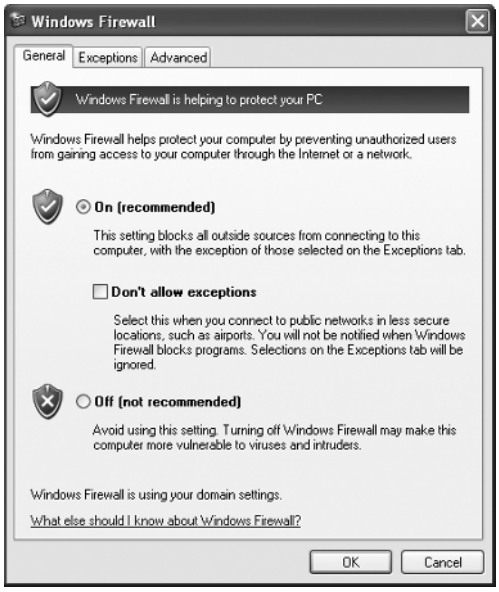


FIGURE 1.5
Windows Firewall replaces Internet Connection Firewall and adds several new network security features.

Exception lists You can use Windows Firewall's exception lists to specify applications that are allowed to listen for incoming traffic on specific ports that are otherwise blocked.

Multiple profiles Domain users can specify different firewall configurations for different scenarios, easily switching between them. For example, when you're working behind your corporate firewall, you can use a firewall configuration that's different from the one you'd use when connecting from a public location. Workgroup and stand-alone computers have a single firewall profile.

Support for RPC Windows Firewall allows incoming Remote Procedure Call (RPC) traffic to RPC server applications that run in the Local System, Network Service, or Local Service contexts. You can also add RPC server applications explicitly to the exceptions list to enable those applications to receive RPC traffic.

Group policy Windows Firewall supports complete configuration through group policy, enabling administrators to easily control personal firewall settings across the enterprise.

Installation and configuration To simplify configuration, Windows Firewall offers a Restore Defaults feature that quickly restores the firewall to its default settings. You can also configure the default settings for an existing installation and define default settings for unattended installation of Windows XP.

Protocol support Windows Firewall supports both IPv4 and IPv6 with a single interface, simplifying firewall configuration.

TIP Windows Firewall is enabled by default when you install SP2. This will concern many administrators because it could cause applications and network connectivity to stop working properly after SP2 is applied. You can mitigate these potential problems during Setup by preconfiguring the firewall settings. For existing Windows XP installations, you can ue group policy to configure the firewall as necessary. Where group policy isn't a viable solution, you can script changes to the firewall settings with Netsh and Windows Script Host. See Chapter 6 for a discussion of Windows Script Host.

In addition to Windows Firewall, SP2 incorporates other network-related changes. For example, the Alerter and Messenger services' startup modes are set to Disabled when SP2 is installed. Prior to SP2, the Alerter service was set by default to Manual, and Messenger was set to Automatic startup. Setting both of these services to Disabled reduces the computer's attack surface for worms, viruses, and other network-borne threats.

NOTE Don't confuse the Windows XP Messenger service with the Windows Messenger application. The Messenger service transmits simple messages across the local network, whereas Windows Messenger is a desktop conferencing and chat application included with Windows XP. MSN Messenger is a superset of Windows Messenger that offers additional features for MSN users.

Windows Messenger gets an update in SP2. For example, Windows Messenger blocks file transfers if they come from someone not on your contact list or if the file is on the unsafe attachment list defined by Outlook Express. Messenger in SP2 also requires a display name that is different from the contact's e-mail address.

Wireless networking also sees some improvements in SP2 with the addition of a Wireless Network Setup Wizard that greatly simplifies wireless network configuration (Figure 1.6). The wizard creates a set of configuration files that it stores on USB flash drive or floppy disk, which you can use with the wizard on other computers to configure wireless settings. SP2 also adds support for Wireless Provisioning Services, a feature of Windows Server 2003 Service Pack 1 that provides a framework for connecting wireless users to an infrastructure network. Wireless Provisioning Services are targeted at companies that want to offer hotspot wireless access, and inclusion of these capabilities in Windows XP makes it easy for users to connect via wireless hotspots.

Memory Exploit Protection

Windows XP SP2 adds support for Data Execution Prevention (DEP), a feature of newer processors from AMD and Intel that prevents execution of code in memory pages not marked as executable. With DEP enabled, an attempt to run code in unmarked memory causes a processor exception. Preventing the code from executing can help prevent viruses, worms, and other malicious code from running on the computer.

SP2 adds two new startup switches for Windows XP to support DEP:

/NOEXECUTE Enables DEP. Applications that attempt to run in unmarked pages will fail.

/EXECUTE Disables DEP. Applications won't generate a processor exception if they attempt to run in unmarked pages. Use this switch to enable known applications to run if they don't function properly with DEP enabled.

TIP You can use application compatibility settings to disable DEP for specific applications in Windows. See Chapter 7 for a discussion of compatibility options.

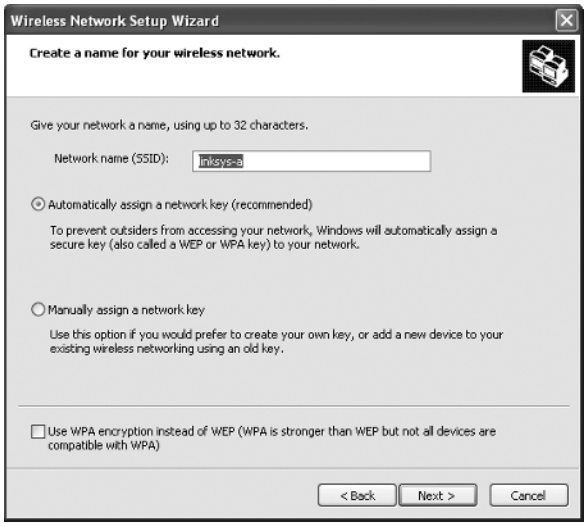


FIGURE 1.6
Use the Wireless Network Setup Wizard to quickly and easily set up a small wireless network.

Outlook Express

SP2 adds a handful of features to Outlook Express to improve security. Like Outlook 2003, Outlook Express with SP2 blocks external HTML content. You can configure Outlook Express to allow the content, or you can download it for each message as desired. To help prevent HTML script exploits, you can configure Outlook Express to render downloaded messages in plain text by default. If you need to view the message in HTML, you can click the message and choose View ➢ Message in HTML to render it with HTML.

Internet Explorer

Internet Explorer has several changes in SP2, most of which are targeted at improved security. First, IE incorporates changes for downloading files. You can configure IE to block files from specified publishers and prompt you for others. IE also displays more information about file publishers to help you decide whether to allow add-on downloads. And, it does a better job of detecting and handling add-on crashes, enabling you to block problematic add-ons. Administrators can configure a handful of group policy settings to control these features.

A welcome addition to IE in SP2 is an integrated pop-up blocker. IE blocks all pop-ups by default, but you can configure it to allow pop-ups from specific sites. A new Information Bar (Figure 1.7) displays information about blocking and other security and status information. The Information Bar automatically hides when you navigate away from the page that generated the message.

Along with the pop-up blocker comes a different way to handle windows. IE prevents windows from being opened outside of the viewable area of the Desktop in an effort to prevent sites from hiding content from the user and preventing the user from closing the window. IE with SP2 also enables the status bar for all windows, to let users view information that might otherwise be hidden by a particular site or page.

IE incorporates several changes to help mitigate certain types of exploits. First, binary behaviors—which enable site developers to build functions that can modify HTML tags and their behavior—are blocked in IE's Restricted Sites security zone. In addition, IE applies the ActiveX security model to all

instances where URL binding is used to instantiate and initialize an object. This feature is called *BindToObject Mitigation*. IE can also perform *mime sniffing*, which lets IE detect a file type by bit signature rather than file extension and thereby prevent attacks and infections by scripts or other types of masquerading files. In addition, IE incorporates changes to lock down the Local Machine security zone, prevent privilege elevation, and restrict script-initiated pop-up windows.

TIP You can configure many of IE's new security features with group policy settings.

FIGURE 1.7
The Information Bar displays information about blocked pop-ups and other security messages.

Other changes in SP2 for IE are the capability to block all content from specific publishers, even if the content is signed, and to block all code with invalid signatures. These changes prevent repeated prompts to install otherwise blocked code. IE also prevents a page from accessing objects cached by another site, which can prevent users' personal data from being exposed to potentially malicious sites. In addition, IE now prevents the security context for a given page from being higher than the overall security context for the site's root URL, and it blocks JavaScript navigation if the security context is missing.

NOTE See Chapter 28 for a complete discussion of SP2 features for Internet Explorer and how to optimize IE's security.

Setup and Configuration

SP2 introduces several changes to Windows XP setup and configuration. First, a trip to the Add Or Remove Programs applet in Control Panel will show you that updates and patches are now hidden from the applet. A check box at the top of the applet lets you turn on or off the display of updates (Figure 1.8). Administrators can control this feature with a group policy setting or Registry modification.

SP2 adds support for new features of Windows Update Services running on Windows Server 2003. Administrators can now deploy updates for drivers, Microsoft Office, SQL Server, and Exchange Server using Windows Update Services. There are several new switches for the `Update.exe` package installer and a new version 3.0 of the Windows Installer service.

Finally, the Security Center (Figure 1.9) applet in Control Panel provides security-related notifications to users in the areas of virus protection, Windows Firewall, and Windows Updates. You can disable these notifications through the Security Center and through group policy.

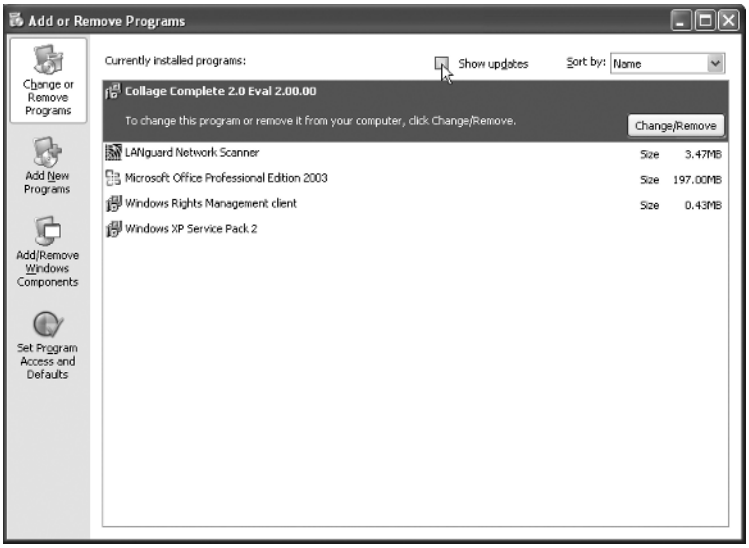


FIGURE 1.8
You can turn on or off the display of updates and patches in Add Or Remove Programs.

FIGURE 1.9
Use the Security Center to configure notifications about security-related features.

Where to Go for More Details

This chapter discusses some of the core features in Windows XP that are either new or improved over previous Windows platforms. These are by no means the only changes and improvements, however. There are also significant interface changes, a wealth of new features for remote access and management, improved recoverability, additional system installation and update options, firewalls and other security features, and much more. Rather than cover all these changes in this one chapter, I've opted to describe them throughout the remainder of the book to put them in context. However, several good references are available to help you get an overview of the new features in Windows XP. The following list offers several sources:

- *Mastering Windows XP Home Edition*, 3d ed., by Guy Hart-Davis (Sybex, 2004)
- *Mastering Windows XP Professional*, 3d ed., by Mark Minasi (Sybex, 2004)
- Windows XP Home Edition evaluation web page: `www.microsoft.com/windowsxp/home/evaluation/features.mspx`
- Windows XP Professional evaluation web page: `www.microsoft.com/windowsxp/pro/evaluation/features.mspx`
- Windows XP Service Pack 2 web page: `www.microsoft.com/windowsxp/downloads/updates/default.mspx`