Operating System

What's New in Security for Windows XP Professional and Windows XP Home Edition

Microsoft Corporation
Published: July 2001

Abstract

This article presents a technical overview of what's new in security and privacy services for Windows® XP. Windows XP is available in two editions—Windows XP Home Edition for home use, and Windows XP Professional for businesses of all sizes.

If you're planning on using Windows XP as the operating system on a computer that's a stand-alone machine or part of a workgroup, you'll be particularly interested in fast user switching and Internet connection firewall; and if you're using or administering Windows XP Professional as part of a domain, you'll be interested in learning what's new for controlling network access and setting software restriction policies.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Acknowledgements

Dionysia Sofos, Technical Writer, Microsoft Corporation

Mike Danseglio, Technical Writer, Microsoft Corporation

Michael Kessler, Technical Editor, Microsoft Corporation.

Some material in this paper also appears in the upcoming Windows XP Professional Resource Kit.

Introduction

Windows® XP provides the most dependable version of Windows ever—with the best security and privacy features Windows has ever provided. Overall, security has been improved in Windows XP to help you have a *safe, secure, and private* computing experience. Windows XP is available in two editions—Windows XP Home Edition for home use, and Windows XP Professional for businesses of all sizes.

Security features in Windows XP Home Edition make it even safer for you to shop and browse on the Internet. Windows XP Home Edition comes with built-in Internet Connection Firewall software that provides you with a resilient defense to security threats when you're connected to the Internet—particularly if you use always-on connections such as cable modems and DSL.

Windows XP Professional includes all of the security capabilities of Windows XP Home Edition, plus other security management features. These important new security features will reduce your IT costs and enhance the security of your business systems.

Windows XP Home Edition

- Personalized Login
- Fast User Switching
- Personal Privacy
- Internet Connection Firewall
- Shared Documents Folder

Windows XP Professional

- Corporate Security
- Controlled Network Access
- Simple Sharing
- Blank Password Restrictions
- Encrypting File System
- Certificate Services
- Credential Management
- Fast User Switching
- Personal Privacy
- Internet Connection Sharing
- Internet Connection Firewall
- Software Restriction Policies

- Internet Protocol Security
- Smart Card Support
- Kerberos

What's New in Security for Windows XP Home Edition

Windows XP Home Edition security services have been designed to be flexible, and take into account a wide variety of security and privacy situations that you'll face as a home user. If you are already familiar with the security model in Microsoft® Windows NT® version 4.0 and Microsoft® Windows® 2000, you will recognize many of the security features in Windows XP Home Edition. At the same time, you will also find a number of familiar features that have changed significantly, along with new features that will improve your ability to manage system security.

For example, if you use the Internet to chat online or to send and receive e-mail, you may be vulnerable to hacker attacks. To protect you from these threats, Windows XP has incorporated enhanced security features that make your online experience even safer.

Let's take a look at the important security and privacy features in Windows XP Home Edition that make you and your information more secure while you're having the most productive Windows user experience ever.

Remember: When you're working with Windows XP Home Edition as part of a workgroup or in a stand-alone environment, and you have administrator rights to your computer, you'll have access to all the operating system's security features. If your Windows XP Home Edition-equipped computer is part of a network, security options will be determined by the network administrator.

Personalized Login

With Windows XP, all family members can have their own interface, complete with login and password. This added level of security ensures that no one can access—or accidentally delete—your important documents.

If you have children in the house, you can set up profiles with different security limits to filter out Internet sites that may be inappropriate for them.

Fast User Switching for Multiple Users of a Computer

Designed for the home, Fast User Switching lets everyone use a single computer as if it were their own. There is no need to log someone else off and have to decide whether to save another user's files. Instead Windows XP takes advantage of Terminal Services technology and runs unique user sessions that enable each user's data to be entirely separated. And when used with a user password, these sessions are secured from one another.

Fast User Switching is enabled by default when either Windows XP Home Edition or Windows XP Professional is installed on a stand-alone or workgroup-connected computer. If you join a domain with a computer running Windows XP Professional, you will not be able to use Fast User Switching.

Fast User Switching makes it easier for families to share a single computer. For example, if a mother uses the computer to work on finances and has to leave for a short period of time, her son can switch to his own account and play a game. The financial application is left running and open in the mother's account. All of this is done without logging off. Switching users is easy because the new Welcome screen is easily customizable with pictures for each user who logs on to the computer, as shown in Figure 1.

Figure 1 Personal Logon and Fast User Switching Welcome screen

Personal Privacy

Microsoft Internet Explorer version 6.0 helps you maintain control over your personal information when visiting Web sites by supporting the Platform for Privacy Preferences (P3P) standard from the World Wide Web Consortium (W3C). As part of W3C, Microsoft helped develop a standard for Web site privacy policies so you can make informed decisions about the amount and type of information you share online. Internet Explorer 6.0 determines whether the Web sites you visit adhere to the standards of W3C and tells you their status before you provide private information.

Once you have defined your privacy preferences for disclosing personal information in Internet Explorer 6.0, the browser determines whether the sites you visit are P3P-compliant. For P3P-compliant sites, the browser compares your privacy preferences to the privacy policies defined for the sites. Internet Explorer uses HTTP for this exchange of policy information. Based on your privacy preferences, the browser determines whether to disclose personal information to the Web sites.

Cookie Management

The P3P standard also supports cookie management features in Internet Explorer 6.0. A cookie is a small file that an individual Web site stores on your computer to provide customization features. For example, when you implement custom settings for MSN®, that information is stored in a cookie file on your computer. MSN then reads the cookie each time you visit the site and displays the options you selected.

As part of their privacy policies, P3P-compliant Web sites can provide policy information for their cookies. When you configure your privacy preferences, you can configure Internet Explorer to handle cookies in the following ways:

- Prevent all cookies from being stored on your computer.

- Refuse third-party cookies (cookies that do not originate from the same domain as the Web site being visited and therefore are not covered by that Web site's privacy policy), but allow all other cookies to be stored on your computer.
- Allow all cookies to be stored on your computer without notifying you.

See Figures 2 and 3 for additional cookie management options.

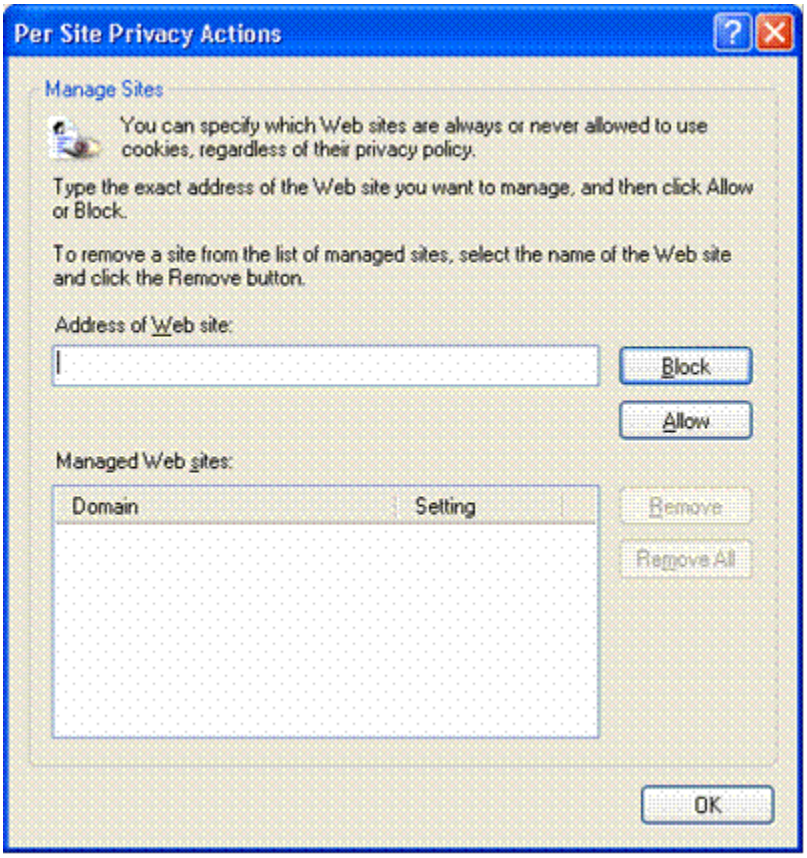

Figure 2 Cookie Management: Per Site Privacy Actions

Figure 3 Cookie Management: Advanced Privacy Settings

For more information about P3P, see the W3C Web site at http://www.w3.org/.

Internet Connection Sharing

Internet Connection Sharing (ICS) connects multiple computers to the Internet using a single Internet connection. With ICS, users can securely share DSL, cable modem, or telephone line connections among multiple computers.

How ICS Works

One computer, called the ICS host, connects directly to the Internet and shares its connection with the rest of the computers on the network. The client computers rely on the ICS host computer to provide access to the Internet. Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet. Any communication from client computers to the Internet must pass through the ICS host, a process that keeps the addresses of client computers hidden from the Internet. Client computers are protected because they cannot be seen from outside the network. Only the computer running ICS is seen from the public side. In addition, the ICS host computer manages network addressing. The ICS host computer assigns itself a permanent address and provides Dynamic Host Configuration Protocol (DHCP) to ICS clients. By assigning a unique address to each ICS client, the ICS host computer provides a way for computers to communicate with other computers on the network.

Windows XP provides the ability to share a single Internet connection with multiple computers on a home or small-business network through the ICS feature. This feature first appeared in Windows 2000 Professional and Windows 98 Second Edition, and has been improved in Windows XP.

Using Network Protocols

In Windows XP, the ICS feature provides Network Address Translation (NAT), DHCP, and Domain Name Service (DNS) to the home network, negating the need for user configuration of clients.

The DNS functionality in Windows XP has been improved to include a local DNS Resolver to provide name resolution for all clients on the home network. With the DNS Resolver, non-Windows-based network devices are able to do name resolution for network clients. Internet names needing name resolution are still forwarded to the Internet service provider's DNS servers for resolution.

Remote Discovery and Control Functionality

ICS also includes remote discovery and control functionality. Using Universal Plug and Play, network clients detect the presence of the ICS host, then query and determine its Internet connection status.

When you want to browse the Internet on another personal computer within your home, the Windows XP personal computer automatically connects to the Internet—if it's not already connected—on behalf of the other computer. Or, the user on the client computer elsewhere in the house will know if there's an existing Internet connection, and can disconnect it to use the telephone for normal voice communications, if desired. This is useful if you're charged by the minute for dial-up connections, or prefer to turn off your Internet connection during periods of inactivity.

See Figure 4 for an illustration of the options for setting up ICS.

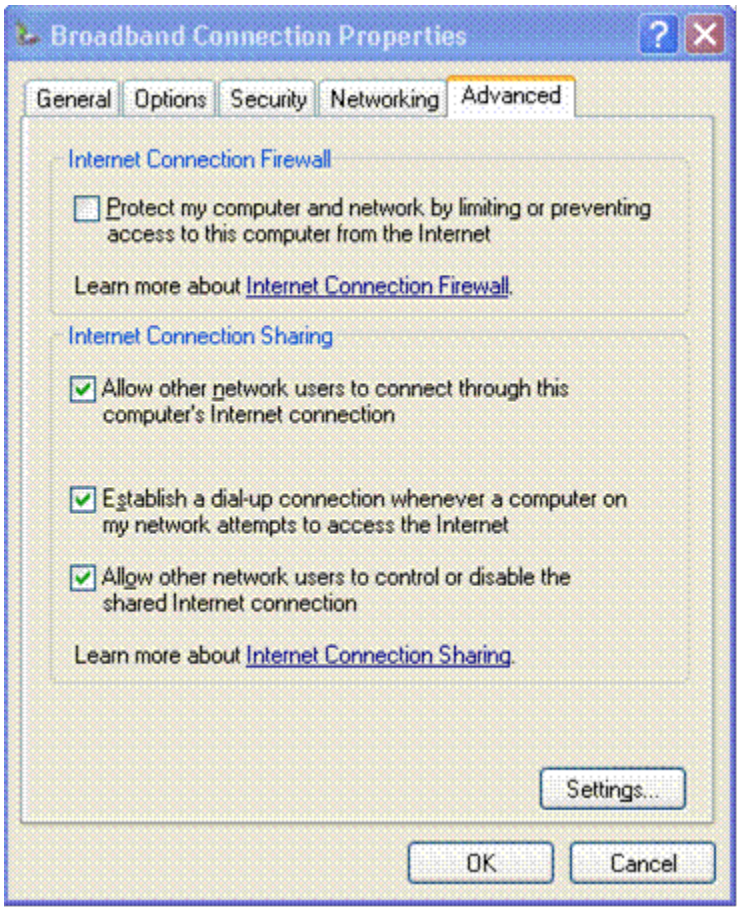

Figure 4 Setting up ICS

Internet Connection Firewall

Windows® XP provides Internet security in the form of the new Internet Connection Firewall (ICF). For years, business networks have been able to protect themselves from outside attacks by using firewalls. Windows XP offers that same security to consumers with its ICF protection feature. This means that your information, computers, and family's data are safer from intruders as soon as you start using Windows XP.

An Increased Need for Security

As more homes and businesses adopt broadband Internet access, there's an increased need for security measures to protect personal computers and other devices and content connected to these home networks. Even computers that connect to the Internet using dial-up modems are not immune from attack.

Designed for use in the home or small business, the ICF provides protection for the Windows XP personal computer directly connected to the Internet, or for the personal computers or devices connected to the Internet Connection Sharing host computer that is running the ICF.

How the Internet Connection Firewall Works

The Windows XP ICF makes use of active packet filtering, which means that ports on the firewall are dynamically opened only for as long as needed to enable you to access the services you're interested in. This type of firewall technology, which is usually associated with more sophisticated enterprise firewalls, prevents would-be hackers from scanning your computer's ports and resources—including file and printer shares. This significantly reduces the threat of external attacks. The ICF is enabled on a per-connection basis.

This firewall feature is available for local area network (LAN), Point-to-Point Protocol Over Ethernet (PPPoE), VPN, or dial-up connections. PPPoE is a new IETF draft standard. It's used to make broadband connectivity through cable modems or digital subscriber lines as easy to establish as dial-up modem connections. Windows XP is the first Windows operating system to include this native PPPoE support.

When you're on the road with your portable computer and accesses the Internet through a dial-up connection or other means, the ICF feature can be automatically enabled for security.

It's Easy to Activate Firewall Protection

When you run the Network Setup Wizard, it automatically enables ICF on any active Internet connections that it finds. To double-check whether a connection is using ICF:

- Open Control Panel.
- Click **Network and Internet Connections**.
- Click **Network Connections**.
- Right-click your Internet connection, and then click **Properties**.
- Click the Advanced tab of your connection's **Properties** dialog box.

See Figure 5 for an illustration on how to activate the ICF.

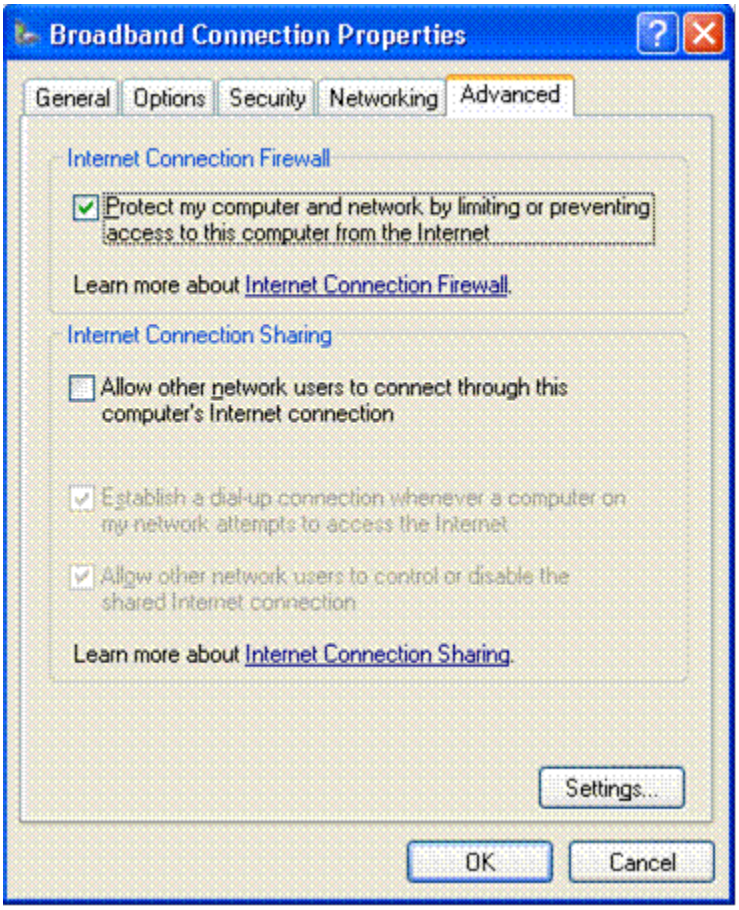

Figure 5 Activating the ICF

Port Mapping

By default, the ICF does not let unsolicited in-bound traffic in. If you need to allow other people access to your computer over the Internet—for example, if you're hosting a Web site or an Internet session of a computer game—Windows XP allows you to open holes in the firewall that allow traffic on specific ports. This is called "port mapping."

Shared Documents Folder

Shared folders are counterparts to your personal folders: My Documents, My Pictures, and My Music. Shared Documents, Shared Pictures, and Shared Music provide a place for you to store files, pictures, and music that everyone on your computer can access. For example, Billy can put his homework in Shared Documents so that Mom can check his work. And Dad can put digital pictures from the family vacation in Shared Pictures so that the whole family can see them.

Since home computers are generally a trusted environment, Windows XP home users get separate but accessible file storage by default, with optional password protection. This approach allows a family to easily share documents, pictures, music, and videos on a single computer, and on multiple computers on a home network.

However, when you create a password for yourself, Windows offers to lock down your “My Documents” folder, as well as any subfolder. That way if you have a password and want privacy, you will be protected from other non-administrator users of the computer.

Note This is only the case if your hard drive is formatted in NTFS; this feature won’t work if you’ve formatted in file allocation table (FAT) or FAT32.

What's New in Security for Windows XP Professional

Windows XP Professional is the operating system of choice for businesses of all sizes, and provides the most dependable security services for business computing. Windows XP Professional includes the security features you need for business networking and security. These security features deliver new management capabilities that will lower the costs of IT and allow you to spend more time building business services and solutions.

If you are already familiar with the security model in Microsoft® Windows NT® 4.0 and Microsoft® Windows® 2000, you will recognize many of the features in Windows XP Professional. At the same time, you will also find a number of familiar features that have changed significantly, and new features that will improve your ability to manage system security.

Remember: When you're working with Windows XP Professional as part of a workgroup or in a stand-alone environment, and you have administrator rights to your computer, you'll have access to all of the operating system's security features. If your Windows XP Professional-equipped computer is part of a domain, your options will be determined by the policies set by the IT administrator.

Corporate Security

Windows XP Professional offers robust security features to help businesses protect sensitive data and provide support for managing users on the network. One of the great features available in Windows XP Professional is the use of Group Policy objects (GPO). GPOs allow system administrators to apply a single security profile to multiple computers and optionally use smart card technology to authenticate users by using information stored on a smart card.

Security Enhancements

Windows XP Professional includes a number of features that businesses can use to protect selected files, applications, and other resources. These features include access control lists (ACLs), security groups, and Group Policy—in addition to the tools that allow businesses to configure and manage these features. Together they provide a powerful, yet flexible, access control infrastructure for business networks.

Windows XP offers thousands of security-related settings that can be implemented individually. The Windows XP operating system also includes predefined security templates, which businesses can implement without modifications or use as the basis for a more customized security configuration. Businesses can apply these security templates when they:

- Create a resource, such as a folder or file share, and either accept the default access control list settings or implement custom access control list settings.
- Place users in the standard security groups, such as Users, Power Users, and Administrators, and accept the default ACL settings that apply to those security groups.
- Use the Basic, Compatible, Secure, and Highly Secure Group Policy templates that have been provided with the operating system.

Each of the Windows XP security features—ACLS, security groups, and Group Policy—have default settings that can be modified to suit a particular organization. Businesses can also make use of relevant tools to implement and modify access control. Many of these tools, such as the Microsoft Management Console snap-ins, are components of Windows XP Professional. Other tools are included with the Windows XP Professional Resource Kit.

Controlled Network Access

Windows XP provides built-in security to keep intruders out. It does this by limiting anyone trying to gain access to your computer from a network to "guest"-level privileges. If intruders attempt to break into your computer and gain unauthorized privileges by guessing passwords, they will be unsuccessful—or obtain only limited, guest-level access.

Managing Network Authentication

An increasing number of Windows XP Professional–based systems are connected directly to the Internet rather than to domains. This makes proper management of access control (including strong passwords and permissions associated with different accounts) more critical than ever. To ensure security, the relatively anonymous access control settings commonly associated with open Internet environments need to be curtailed.

As a result, the default in Windows XP Professional requires all users logging on over the network to use the Guest account. This change is designed to prevent hackers attempting to access a system across the Internet from logging on by using a local Administrator account that has no password.

Simple Sharing

By default, on Windows XP Professional systems that are not connected to a domain, all attempts to log on from across the network will be forced to use the Guest account. In addition, on computers that are using the simple sharing security model, the Security Properties dialog box is replaced by a simplified Shared **Documents Properties** dialog box.

Force Guest

The sharing and security model for local accounts allows you to choose between the Guest-only security model or the Classic security model. In the Guest-only model, all attempts to log on to the local computer from across the network will be forced to use the Guest account. In the Classic security model, users who attempt to log on to the local computer from across the network authenticate as themselves. This policy does not apply to computers that are joined to a domain. Otherwise, Guest-only is enabled by default.

If a guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the Guest account.

If the “force network logons using local accounts to authenticate as Guest” policy is enabled, local accounts must authenticate as a Guest. This policy determines whether a local account that connects directly to a computer on the network must authenticate as a Guest user. You can use this policy to limit the permissions of a local account that is attempting to access system resources on the target computer. If you enable this policy, all local accounts that attempt to connect directly are limited to Guest permissions, which are usually severely restricted.

Blank Password Restriction

To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity *except* at the main physical console logon screen. For example, you cannot use the secondary logon service (RunAs) to start a program as a local user with a blank password.

Assigning a password to a local account removes the restriction that prevents logging on over a network. It also permits that account to access any resources it is authorized to access, even over a network connection.

Caution If your computer is not in a physically secured location, it is recommended that you assign passwords to all local user accounts. Failure to do so allows anyone with physical access to the computer to log on using an account that does not have a password. This is especially important for portable computers, which should always have strong passwords on all local user accounts.

Note This restriction does not apply to domain accounts. It also does not apply to the local guest account. If the guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the guest account.

If you want to disable the restriction against logging on to the network without a password, you can do so through Local Security Policy.

Encrypting File System

The increased functionality of Encrypting File System (EFS) has significantly enhanced the power of Windows® XP Professional by providing additional flexibility for corporate users when they deploy security solutions based on encrypted data files.

EFS Architecture

EFS is based on public-key encryption and takes advantage of the CryptoAPI architecture in Windows XP. The default configuration of EFS requires no administrative effort—you can begin encrypting files immediately. EFS automatically generates an encryption key pair and a certificate for a user if one does not exist already.

EFS can use either the expanded Data Encryption Standard (DESX) or Triple-DES (3DES) as the encryption algorithm. Both the RSA Base and RSA Enhanced software that cryptographic service providers (CSPs) included in the operating system may be used for EFS certificates, and for encryption of the symmetric encryption keys.

If you encrypt a folder, all files and subfolders created in, or added to, the encrypted folder are automatically encrypted. It is recommended that you encrypt at the folder level to prevent plain-text temporary files from being created on the hard disk during file conversion.

EFS and NTFS

Encrypting File System (EFS) protects sensitive data in files that are stored on disk using the NTFS file system. EFS is the core technology for encrypting and decrypting files stored on NTFS volumes. Only the user who encrypts a protected file can open the file and work with it. This is especially useful for mobile

computer users because even if someone else gains access to a lost or stolen laptop, he or she will not able to access any of the files on the disk. For Windows XP, EFS now works with Offline Files and Folders.

EFS enables you to encrypt individual files and folders. Encrypted files will remain confidential even if an attacker bypasses system security by, for instance, installing a new operating system. EFS provides strong encryption through industry standard algorithms, and because it is tightly integrated with NTFS, it is easy to use. EFS for Windows® XP Professional offers new options for sharing encrypted files or disabling data recovery agents, and facilitates management through Group Policy and command-line utilities.

Maintaining File Confidentiality

Security features such as logon authentication or file permissions protect network resources from unauthorized access. However, anyone with physical access to a computer can install a new operating system on that computer and bypass the existing operating system's security. In this way, sensitive data can be exposed. Encrypting sensitive files through EFS adds another layer of security. When files are encrypted, their data is protected even if an attacker has full access to the computer's data storage.

Only authorized users and designated data recovery agents can decrypt encrypted files. Other system accounts that have permissions for a file—even the Take Ownership permission—cannot open the file without authorization. Even the administrator account cannot open the file if that account is not designated as a data recovery agent. If an unauthorized user tries to open an encrypted file, access will be denied.

Figure 6 shows where you would create settings for EFS.

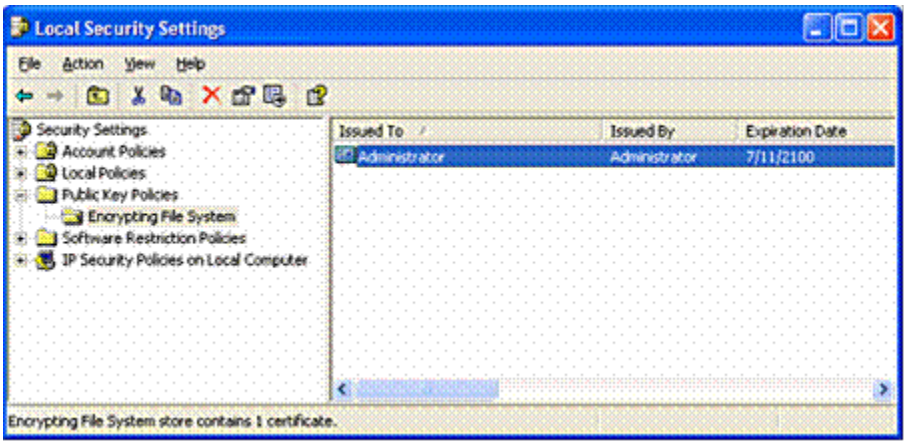

Figure 6 EFS Local Security Settings

How EFS Works

EFS enables you to store confidential information about a computer when people who have physical access to your computer could otherwise compromise that information, intentionally or unintentionally. EFS is especially useful for securing sensitive data on portable computers or on computers shared by several users. Both kinds of systems are susceptible to attack by techniques that circumvent the restrictions of ACLs.

In a shared system, an attacker can gain access by starting up a different operating system. An attacker could also steal a computer, remove the hard drive(s), place the drive(s) in another system, and gain access to the stored files. Files encrypted through EFS, however, appear as unintelligible characters when the attacker does not have the decryption key.

Because EFS is tightly integrated with NTFS, file encryption and decryption are transparent. When you open a file, it is decrypted by EFS as data is read from disk. When you save the file, EFS encrypts the data as it is written to disk. As an authorized user you might not even realize that the files are encrypted because you can work with them as you normally do.

In its default configuration, EFS enables you to start encrypting files from Windows Explorer with no administrative effort. From a user's point of view, encrypting a file is simply a matter of setting a file attribute. The encryption attribute can also be set for a file folder. This means that any file created in or added to the folder is automatically encrypted.

Configuring EFS for Your Environment

EFS is enabled by default. You can encrypt files if you have permission to modify the files. Because EFS relies on a public key to encrypt files, you need a public-private key pair and a public key certificate for encryption. Because EFS can use self-signed certificates, it does not require administrative effort before it can be used.

If EFS is not appropriate in your environment, or if you have files that you do not want encrypted, you can disable EFS in various ways. There are also a number of ways in which you can configure EFS to meet the specific needs of your organization.

In order to use EFS, all users must have EFS certificates. If you do not currently have a Public Key Infrastructure (PKI), you can use self-signed certificates that are generated by the operating system automatically. If you have certification authorities, however, you might want to configure them to provide EFS certificates. You will also need to consider a disaster recovery plan if you use EFS on your system.

What Can Be Encrypted

Individual files and file folders (or subfolders) on NTFS volumes can be set with the encryption attribute. Although it is common to refer to file folders with the encryption attribute set as "encrypted," the folder itself is not encrypted, and no public-private key pair is required to set the encryption attribute for a file folder. When encryption is set for a folder, EFS automatically encrypts the following:

- All new files created in the folder.
- All plaintext files copied or moved into the folder.
- Optionally, all existing files and subfolders.

Offline Files, known in Windows 2000 as client-side caching, can also be encrypted through EFS.

Encrypting Offline Files

Windows 2000 introduced client-side caching functionality, now called Offline Files. This is a Microsoft IntelliMirror® management technology that allows network users to access files on network shares even when the client computer is disconnected from the network. When disconnected from the network, mobile users can still browse, read, and edit files because they have been cached on the client computer. When the user later connects to the server, the system reconciles the changes with the server.

The Windows XP Professional client can use EFS to encrypt offline files and folders. This feature is especially attractive for traveling professionals who need to work offline periodically and maintain data security.

Encrypting the Offline Files Database

You now have the option to encrypt the Offline Files database. This is an improvement over Windows 2000, where the cached files could not be encrypted. Windows XP offers you the option of encrypting the Offline Files database to safeguard all locally cached documents from theft while at the same time providing additional security to your locally cached data.

For example, you can use offline files while keeping your sensitive data secure. And if you're an IT administrator you can use this feature to safeguard all locally cached documents. Offline Files is an excellent safeguard if your mobile computer with confidential data saved in the Offline Files cache gets stolen.

This feature supports the encryption and decryption of the entire offline database. Administrative privileges are required to configure how the offline files will be encrypted. To encrypt offline files go to **Folder Options** under **Tools in My Computer** and check **Encrypt offline files to secure data** under the **Offline Files** tab.

See Figure 7 for an illustration showing options for encrypting the Offline Files database.

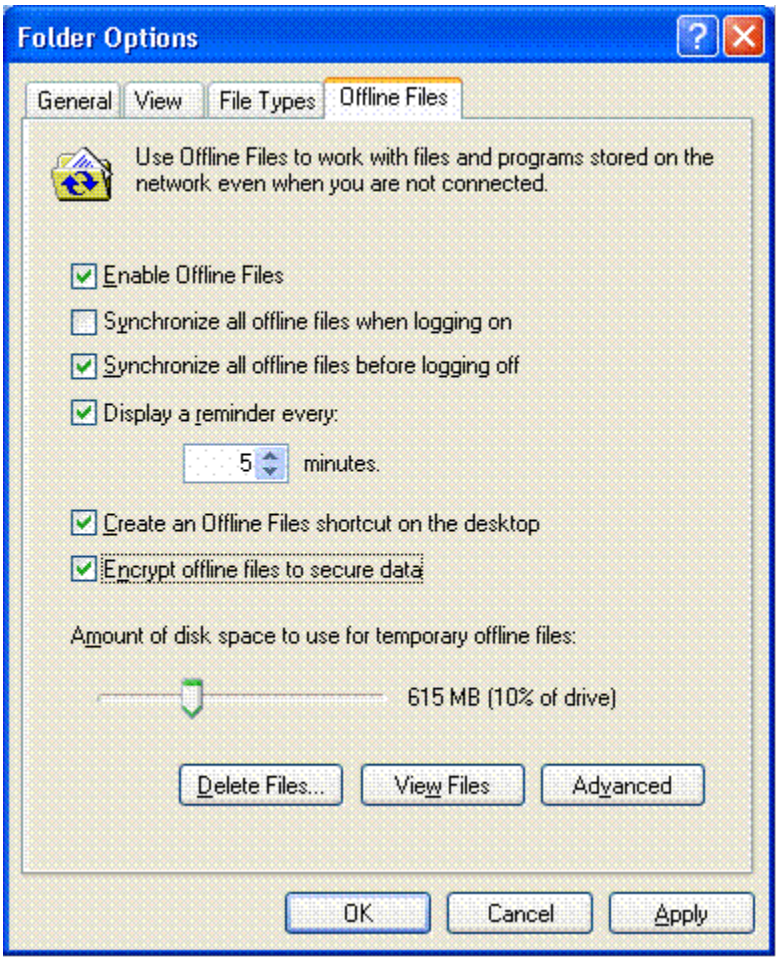

Figure 7 Encrypting the Offline Files database

Remote EFS Operations on File Shares and Web Folders

You can encrypt and decrypt files that are stored on network file shares or on Web Distributed Authoring and Versioning (WebDAV) Web folders. Web folders have many advantages compared to file shares, and Microsoft recommends the use of Web folders whenever possible for remote storage of encrypted files.

Web folders require less administrative effort and are more secure than file shares. Web folders can also securely store and deliver encrypted files over the Internet using standard HTTP file transfers. Using file shares for remote EFS operations requires a Windows 2000 or later domain environment. This is necessary because EFS must impersonate the user through Kerberos protocol delegation to encrypt or decrypt files for the user.

Key Difference

The primary difference between remote EFS operations on files stored on file shares and files stored on Web folders is where the operations occur.

When files are stored on file shares, all EFS operations occur on the computer on which the files are stored. For example, if you connect to a network file share and choose to open a file that you previously encrypted,

the file is decrypted on the computer on which the file is stored and then transmitted in plaintext over the network to your computer.

When files are stored on Web folders, all EFS operations occur on your local computer. For example, if you connect to a Web folder and choose to open a file that you previously encrypted, the file remains encrypted during transmission to your computer and is decrypted by EFS on your computer.

This difference in where EFS operations occur also explains why file shares require more administrative configuration than Web folders.

Remote EFS Operations in a Web Folder Environment

When you open encrypted files stored on Web folders, the files remain encrypted during the file transfer, and EFS decrypts them locally. Both uploads to and downloads from Web folders are raw data transfers, so even if an attacker could access the data during the transmission of an encrypted file, the captured data would be encrypted and unusable.

EFS with Web folders eliminates the need for specialized software to securely share encrypted files between users, businesses, or organizations. Files can be stored on common intranet file servers or Internet communities for easy access while maintaining strong security through EFS.

WebDAV Redirector

The WebDAV Redirector is a mini-redirector that supports the WebDAV protocol, an extension to the HTTP version 1.1 standard, for remote document sharing over HTTP. The WebDAV redirector supports the use of existing applications, and it allows file sharing across the Internet (for example, through firewalls, routers) to HTTP servers. Internet Information Services (IIS) version 5.0 (Windows 2000) supports Web folders.

You access Web folders in the same way that you access file shares. You can map a network drive to a Web folder using the **Net Use** command, or through Windows Explorer. Upon connecting to the Web folder, you can choose to copy, encrypt, or decrypt files exactly as you would with files on file shares.

Certificate Services

Certificate Services is the part of the core operating system that allows a business to act as its own certification authority (CA), and issue and manage digital certificates. Windows XP Professional supports multiple levels of a CA hierarchy and a cross-certified trust network: This includes offline and online certificate authorities.

Certificate and Public Key Storage

Windows XP Professional stores your public key certificates in the personal certificate store. Certificates are stored in plaintext because they are public information, and they are digitally signed by certification authorities to protect against tampering.

User certificates are located in Documents and Settings*username*\ApplicationData\ Microsoft\ SystemCertificates\My\Certificates for each user profile. These certificates are written to the personal store in the system registry each time you log on to your computer. For roaming profiles, your certificates can be stored anywhere and will follow you when you log on to different computers in the domain.

Private Key Storage

Private keys for the Microsoft-based cryptographic service providers (CSPs), including the Base CSP and the Enhanced CSP, are located in the user profile under *RootDirectory*\Documents and Settings*username*\Application Data\Microsoft\Crypto\RSA.

In the case of a roaming user profile, the private key resides in the RSA folder on the domain controller and is downloaded to your computer, where it remains until you log off or the computer is restarted.

Because private keys must be protected, all files in the RSA folder are automatically encrypted with a random, symmetric key called the user's master key. The user's master key is 64 bytes in length and is generated by a strong random number generator. 3DES keys are derived from the master key and are used to protect private keys. The master key is generated automatically and is periodically renewed.

When storing the master key on disk, it is triple-DES protected by a key based in part on your password. It encrypts each file in the RSA folder automatically as the file is created.

User Certificate Autoenrollment

Windows 2000 introduced user certificate autoenrollment. Autoenrollment for computer or domain controller certificates is enabled through Group Policy and Microsoft Active Directory™. Autoenrollment of computer certificates is most useful in facilitating an IPSec or L2TP/IPSec VPN connection with Windows XP Routing and Remote Access servers and other similar devices.

Certificate autoenrollment lowers total cost of ownership and simplifies the certificate management life cycle for users and administrators. Automatic smart card enrollment and self-registration authority features provide enhanced security for enterprise users, in addition to simplified security processes for security conscious organizations.

Pending Certificate Requests and Renewal

User autoenrollment in Windows XP Professional supports both pending certificate requests and renewal features. You can manually or automatically request a certificate from a Windows .NET Server CA. This request is held until administrative approval is received or the verification process is completed. Once the certificate has been approved or issued, the autoenrollment process will complete and install your certificates automatically.

The process for renewing expired user certificates also takes advantage of the autoenrollment mechanism. Certificates are automatically renewed on behalf of the user—dependent upon the specifications in the certificate template in Active Directory.

Certificates and keys are protected by default. Additionally, you can implement optional security measures to provide extra protection. If you need to increase the security of your certificates and keys, you can export private keys and store them in a secure location.

Figure 8 shows some of the options available for setting up certificate autoenrollment.

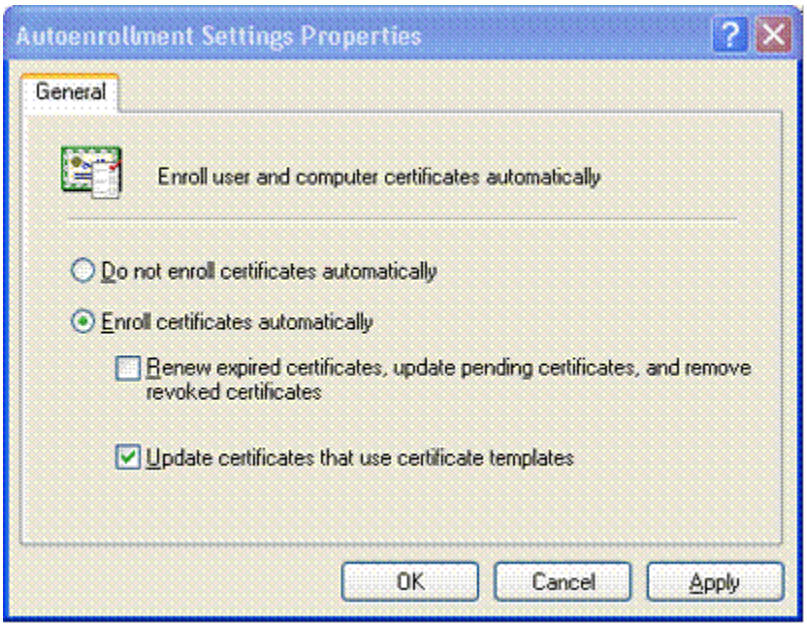

Figure 8 Autoenrollment Settings Properties

Credential Management

Credential Management in Windows XP has three components: credential prompting UI, stored user names and passwords, and the keyring. Together, these three components create a single sign-on solution.

Credential Prompting

The credentials prompting UI is displayed by an application when an authentication error is returned by the authentication package. (This is only applicable for applications that have implemented the UI.)

From the dialog box you can enter a user name and password, or select a X.509 certificate from the My Store object. The application also has the option of displaying the **Remember my password** check box, which allows you to save your credential for later use.

Only integrated authentication packages (for example, Kerberos protocol, NTLM, SSL, and so on) allow credentials to be saved. For basic authentication the credentials prompting UI will still be shown, but you will not have the option of saving your credential. See Figure 9 for an example of the prompt for credentials UI.

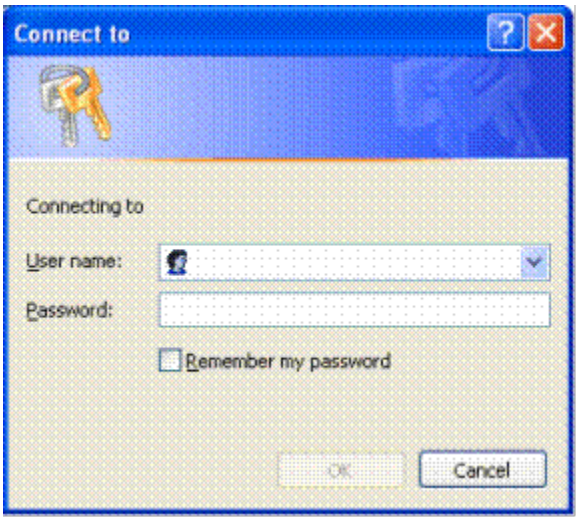

Figure 9 Prompt for Credentials User Interface

Stored User Names and Passwords

Stored User Names and Passwords is the secure roamable store where your saved credentials are kept. Access to the credentials is controlled by the Local Security Settings (LSA). The credentials are stored based on the target Information returned by the resource.

When the credential is saved by checking the **Remember my password** check box on the credentials prompting UI, the credential will be saved in the most general form possible. For example, if you were accessing a specific server in a domain, the credential could be saved as *.domain.com. Saving a different credential for a different server in this domain would not overwrite this credential. It would be saved against more specific target Information.

When a resource is accessed through an integrated authentication package, the authentication package will look in stored user names and passwords for the most specific credential that matches the target Information returned by the resource. If one is found, the credential will be used by the authentication package without any interaction from you. If a credential is not found, an authentication error will be returned to the application that attempted to access the resource.

Note The application that is accessing the resource does not need to have implemented the credential prompting UI to use this seamless authentication. If the application uses an integrated authentication package, the authentication package will attempt to retrieve the credential. In fact, if you entered the credential, only the authentication package can retrieve it.

See Figures 10, 11a, and 11b for examples of password-management UIs.

Figure 10 Classic Password Management UI (Windows XP Professional in a Domain)

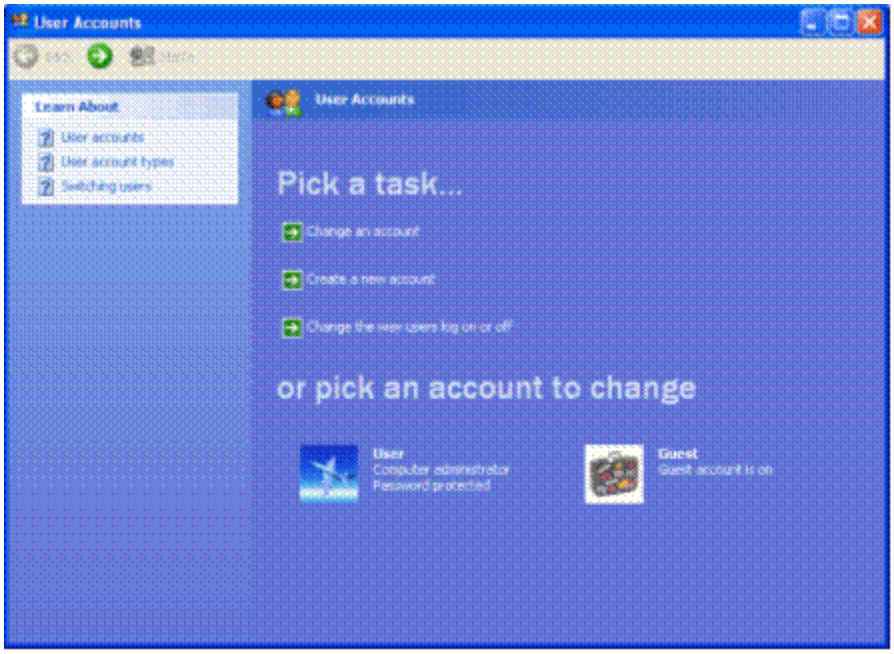

Figure 11a Friendly Password Management UI (Windows XP Home Edition and Windows XP Professional in a Workgroup)

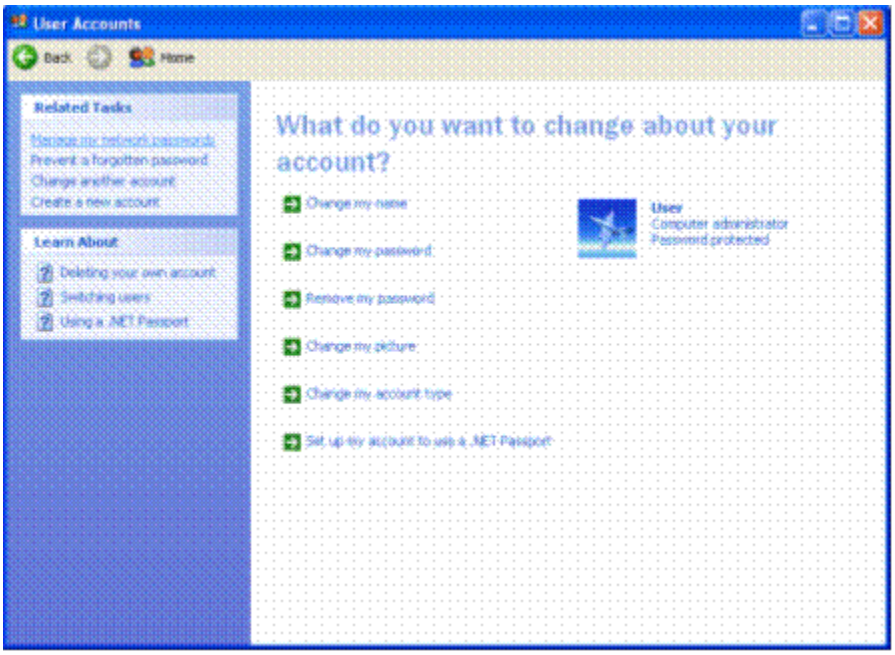

Figure 11b Friendly Password Management UI (Windows XP Home Edition and Windows XP Professional in a Workgroup)

Keyring

The keyring allows you to manually manage the credentials that are in stored user names and passwords. The keyring is accessed through the user accounts Control Panel applet.

In the keyring you will see a list of all the credentials currently in stored user names and passwords. When each credential is highlighted, a description field at the bottom will display a brief description of the credential. From there you can add a new credential, edit an existing credential, or remove an existing credential.

- **Adding a credential.** To add a credential you will be presented with a UI similar to the credential prompting UI, and you will need to fill in the target Information. Remember that target information can accept wildcards in the form of "*".
- **Editing a credential.** Editing a credential enables you to change the target information or the credentials itself. If this is a user name and/or password credential, you can change the password on the server from here. You will not be able to use the credentials prompting UI to edit credentials that have been created specifically by an application. For example, you cannot edit passport credentials.
- **Removing a credential.** You can remove any credential.

The ability to save credentials in stored user names and passwords can be switched on or off through Group Policy.

To allow other software developers to use this mechanism, the credentials prompting API and the underlying credentials API are documented in the Platform Software Development Kit (SDK).

Fast User Switching

All the Fast User Switching features available in Windows® XP Home Edition are available in Windows XP Professional. (Refer to Fast User Switching in the Windows XP Home Edition section of this document for details.)

On computers running Windows XP Professional that are not connected to a domain, you can switch from one user account to another without logging off or closing your applications.

Note Fast User Switching on the Windows XP Professional operating system is only available when your computer is part of a workgroup or in a stand-alone configuration. If your computer is part of a domain, your options for logging on to a computer will be determined by the policies set by the IT administrator.

Personal Privacy

The privacy issues that concern users operating Windows XP Home Edition are the same ones affecting users operating Windows XP Professional. (Refer to Personal Privacy in the Windows XP Home Edition section of this document for details.)

Note: If you're operating Windows XP Professional as part of a workgroup or in a stand-alone configuration, the privacy features available to you will be different than what would otherwise be available if your computer were part of a domain. When your computer is part of a domain, the policies determined by the system administrator take precedence.

Internet Connection Sharing

All the ICS features available in Window XP Home Edition are available in Windows XP Professional. (Refer to Internet Connection Sharing in the Windows XP Home Edition section of this document for details.)

Location-aware Group Policy in ICS

What's unique to ICS in Windows XP Professional is that it has a location-aware group policy. This is useful for mobile users. When a Windows XP Professional computer is a member of a domain, the domain administrator can create a group policy preventing the use of Internet Connection Sharing on the corporate network. When you bring your computer home Internet Connection Sharing is available because the policy does not pertain to your home network

---

Note: Internet Connection Sharing on the Windows XP Professional operating system is only available when your computer is part of a workgroup or in a stand-alone configuration. If your computer is part of a domain, your options for connecting to the Internet will be determined by the policies set by the IT administrator.

Internet Connection Firewall

All of the Internet Connection Firewall features available in Windows XP Home Edition are available in Windows XP Professional. The Windows XP Professional Internet Connection Firewall (ICF) provides desktop and mobile computers with protection from security threats when using DSL, cable modem, or dial-up modem connections to an Internet service provider (ISP).

Location-aware Group Policy in ICF

What's unique to the ICF in Windows XP Professional is that it has a location-aware group policy. This is useful for mobile users who wish to protect their work mobile computers at home or in other locations, such as hotels, airports, or other public Internet connection "hot spots."

When a Windows XP Professional computer is a member of a domain, the domain administrator can create a group policy preventing the use of the ICF while the computer is connected to the corporate network. This enables the laptop to use enterprise network resources with no added complexity for you or the network administrator. When you bring the computer home or to a public Internet connection hot spot, the ICF is available, as the policy does not pertain outside of the work network.

How the ICF Works

The ICF functions as a stateful packet filter that uses technology shared with ICS. Although the ICF feature is stand-alone, you can also run it on the shared adapter to protect your home network.

When enabled, this stateful filter blocks all unsolicited connections originating from the public network interface. To accomplish this, the ICF uses the Network Address Translation (NAT) flow table and validates any incoming flow against the entries in the NAT flow table. Incoming data flows are only allowed if there is an existing NAT flow table mapping that originated from the firewall system or from within the internal protected network. In other words, if the network communication did not originate within the protected network, the incoming data will be dropped.

When you use the Windows XP Professional ICF you can feel comfortable that hackers will not be able to scan your systems or connect to your resources. There is a tradeoff, however. The firewall will make it difficult to configure your system to function as a server to others across the Internet.

Note The ICF on the Windows XP Professional operating system is only available when your computer is part of a workgroup or in a stand-alone configuration. If your computer is part of a domain, your firewall protection capabilities and features will be determined by the policies set by the IT administrator.

Security-related Group Policy Settings

Windows XP includes security templates, which are pre-configured collections of security-related policies that can be used to ensure the appropriate level of security on workstations. These templates represent standard low, medium, and high security configurations, and can be customized to meet specific security needs.

You can also set security policies for password management items, such as:

- Determining minimum password lengths.
- Setting the interval between required password changes.
- Controlling access to resources and data.

Software Restriction Policies

Software restriction policies provide administrators with a policy driven mechanism that identifies software running in their domain, and controls the ability of that software to execute. Using a software restriction policy, an administrator can prevent unwanted applications from running; this includes viruses and Trojan horses, or other software that's known to cause conflicts when installed.

Using Software Restriction Policies

If you're an administrator, you can use a software restriction policy to confine execution to a set of trusted applications. Applications are made known to the policy by file path, file hash, Microsoft® Authenticode® signer certificate, or Internet Zone. Once identified, the system enforces the policies set by the administrator.

Software restriction policies can also help protect against script-based viruses and Trojan horses. An administrator can configure a software restriction policy to only allow scripts to run that are signed by a member of the IT organization. This prevents all script-based viruses, such as ILOVEYOU.VBS. Software restriction policies also can be used to regulate what applications users can install onto their computers.

Software restriction policies can be used on a stand-alone computer by configuring the local security policy. Software restriction policies also integrate with Group Policy and Active Directory. It is possible to customize different software restriction policies for different sets of users or computers. It is possible to use a Windows XP computer to create a software restriction policy in a Windows 2000 environment. The Windows 2000 computers in the domain will ignore the software restriction policy, while the Windows XP computers will enforce it.

Creating a Software Restriction Policy

A software restriction policy is created through the Microsoft Management Console (MMC) Group Policy snap-in. A policy consists of a default rule about whether programs are allowed to run and exceptions to that rule. The default rule can be set to *unrestricted* or *disallowed*—essentially "run" or "don't run." Setting the default rule to "unrestricted" enables an administrator to define exceptions that are just the set of programs that are forbidden to run. A more secure approach involves setting the default rule to disallowed, and specifying only the programs that are known and trusted to run.

Two Types of Software Restriction Policies

There are two ways to use software restriction policies. If administrators have identified all the software that should be allowed to run, they can use a software restriction policy to limit execution to only that list of trusted applications. If administrators do not know about all the applications their users will run, they will have to be reactive and restrict inappropriate applications as they're identified.

Software restriction policies can be applied to the following scenarios:

- **Only let trusted code run.** If all trusted code can be identified, the administrator can effectively lock down the system. The following are examples of where to apply an "only let trusted code run" policy:
    - Application station
    - Task station
    - Kiosk

For these cases, the default rule would be set to "disallowed." Exceptions would be made to that rule allowing only the trusted applications to run. An example of this policy would be a computer where only certain application software should be running, and users should not be able to install other software on the computer. An administrator could create a policy where only Microsoft Word and Microsoft Excel are allowed to run on the computer. If the user downloads a program or runs one from a floppy disk, the program would be prevented from running, because it is not on the trusted list defined by the policy.

- **Prevent unwanted code from running.** In some cases an administrator cannot predict the entire list of software that users will need to run. In these cases the administrator can only react and identify undesirable code as it is encountered. Companies with loosely managed clients would fall into this model. The following scenarios are examples of this case:
    - Lightly managed personal computers
    - Moderately managed personal computers

For example, should the administrator find that many users are running file sharing applications and creating a drain on network bandwidth, the administrator can create a rule that identifies the file sharing program and prevents it from running. If users are installing a program that is known to cause conflicts with existing software, the administrator can create a rule that identifies the setup program of that software and prevent it from being installed.

See Figure 12 for an illustration of software restriction policy settings.

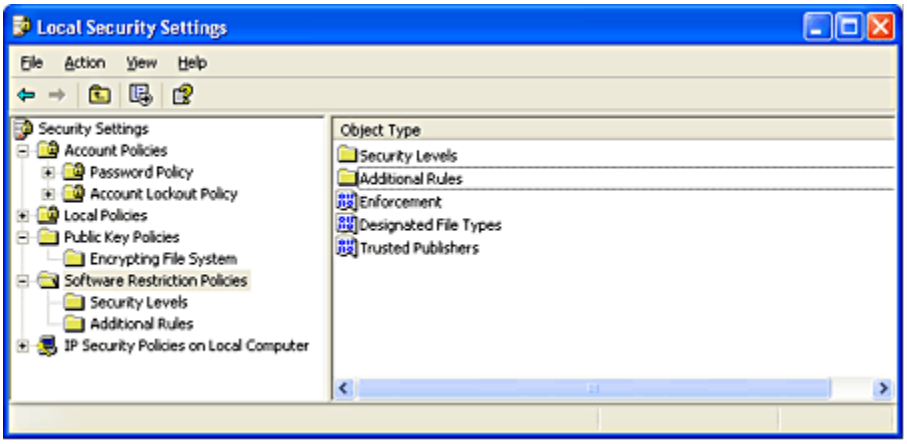

Figure 12 Software Restriction Policies—Local Security Settings

Software Identification Rules

An administrator identifies software through one of the following rules:

- **Hash rule.** A software restriction policy's MMC snap-in allows an administrator to browse to a file and identify that program by calculating its hash. A hash is a digital fingerprint that uniquely identifies a program or file. A file can be renamed or moved to another folder or computer and it will still have the same hash.
- **Path rule.** A path rule can identify software by a full path name, such as C:\Program Files\Microsoft

Office\Office\excel.exe; or by the path name leading to the containing folder, such as C:\Windows\System32. (This would refer to all programs in that directory and its subdirectories.) Path rules can also use environment variables, such as %userprofile%\Local Settings\Temp.

- **Certificate rule.** A certificate rule identifies software by the publisher certificate used to digitally sign the software. For example, an administrator can configure a certificate rule that only allows software signed by Microsoft or its IT organization to be installed.
- **Zone rule.** A zone rule identifies software that comes from the Internet, local intranet, trusted sites, or restricted sites zones.

Controlling Digitally Signed Software

Software restriction policies improve an administrator's ability to control digitally signed software in the following ways:

- **Limiting Microsoft ActiveX® Controls.** An administrator can specify the ActiveX controls that will run in Internet Explorer for a particular domain by using a software restriction policy that lists trusted software publisher certificates. If the publisher of an ActiveX control is on the trusted publisher list, its software automatically runs when downloaded. A software restriction policy can also list disallowed publishers. This automatically prevents ActiveX controls signed by those publishers from running.

  Using a software restriction policy, it's also possible to control who can make a trust decision about an unknown publisher—a publisher that's not explicitly trusted or distrusted. Software restriction policies can be set up to allow only local administrators, or domain administrators, to decide which publishers to trust, and to prevent users from making those decisions.
- **Using Windows Installer.** Programs installed using the Windows Installer can be digitally signed. Using a software restriction policy, an administrator can require that only software digitally signed by certain software publishers can be installed. Windows Installer will then check to verify that an approved signature is present before installing software on the computer.
- **Using Microsoft Visual Basic® Script.** Visual Basic Script files can be digitally signed. An administrator can configure a software restriction policy so that Visual Basic Script files (.vbs) have to be digitally signed by approved software publishers before they can run.

Internet Protocol Security (IPSec)

The need for IP-based network security is almost universal in the current interconnected business world of the Internet, intranets, branch offices, and remote access. Because sensitive information constantly crosses networks, the challenge for network administrators and other information service professionals is to ensure that this traffic is:

- Safe from data modification while in transit.
- Safe from interception, viewing, or copying.
- Safe from being impersonated by unauthenticated parties.
- Safe from being captured and replayed later to gain access to sensitive resources; typically, an

encrypted password can be used in this manner.

These security services are known as data integrity, data confidentiality, data authentication, and replay protection.

Why IPSec Is Needed

IP does not have a default security mechanism, and IP packets are easy to read, modify, replay, and forge. Without security, both public and private networks are susceptible to unauthorized monitoring and access. While internal attacks might be the result of minimal or nonexistent intranet security, risks from outside the private network stem from connections to both the Internet and extranets. Password-based, user access controls alone do not protect data transmitted across a network.

As a result, IPSec was designed by the Internet Engineering Task Force (IETF) to support network-level data authentication, data integrity, data confidentiality, and replay protection. IPSec integrates with Windows 2000 and Windows XP Professional security to provide the ideal platform for safeguarding intranet and Internet communications. It uses industry-standard encryption algorithms and a comprehensive security management approach to provide security for all TCP/IP communications on both sides of an organization's firewall. The result is a Windows 2000 and Windows XP Professional end-to-end security strategy that defends against both external and internal attacks.

IP security is deployed below the transport layer, sparing network managers the difficulty and expense of trying to deploy and coordinate security one application at a time. By deploying Windows XP Professional and Windows 2000 IPSec, network managers provide a strong layer of protection for the entire network, with applications automatically receiving protection from IPSec-enabled servers and clients.

See Figure 13 for an illustration of IPSec settings.

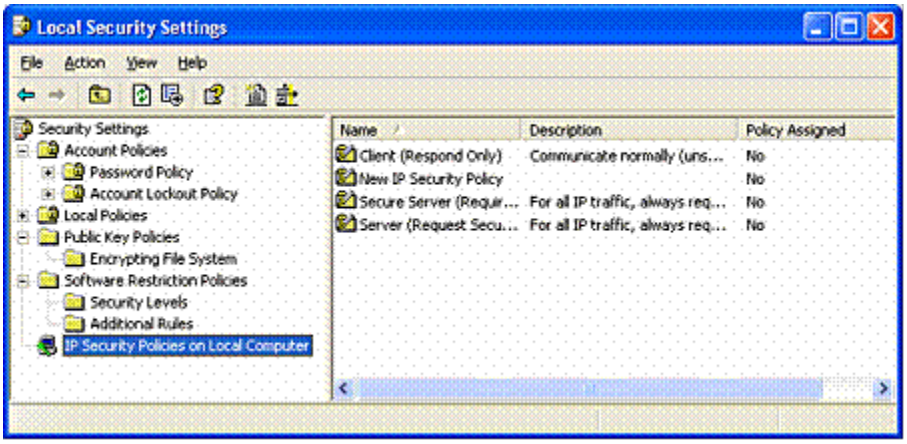

Figure 13 IPSec—Local Security Settings

How IP Security Prevents Network Attacks

Without security measures in place, data might be subjected to an attack. Some attacks are passive; that is, the information is simply monitored. Others are active, meaning that the information is altered with intent to corrupt or destroy the data or the network itself.

Table 1 shows some common security risks found in current networks, and how to use IPSec to prevent them.

Table 1 Types of Network Attacks and Preventing Them by Using IPSec

Attack type	Description	How IPSec prevents attack
Eavesdropping (also called sniffing, snooping)	Monitoring of plaintext or unencrypted packets.	Data is encrypted before transmission, preventing access to the original data even if the packet is monitored or intercepted. Only peers have knowledge of the encryption key.
Data modification	Alteration and transmission of modified packets.	Data hashing attaches a cryptographic checksum to each packet, which is checked by the receiving computer to detect modification.
Identity spoofing	Use of constructed or captured packets to falsely assume the identity of a valid address.	Kerberos version 5 protocol, public key certificates, or preshared keys authenticate peers before secure communication begins.
Denial-of-service	Preventing access of network by valid users. An example is to flood the network with packet traffic.	Ports or protocols can be blocked.
Man-in-the-middle	Diversion of IP packets to an unintended third party, to be monitored and possibly altered.	Authentication of peers.
Known-key	Used to decrypt or modify data.	In Windows XP Professional, cryptographic keys are periodically refreshed, reducing the possibility that a captured key can be used to gain access to secure information.
Application layer attack	Mainly directed at application servers, this attack is used to cause a fault in a network's operating system or applications, or to introduce viruses into the network.	Because IPSec is implemented at the network layer, packets that do not meet the security filters at this level are never passed to applications, protecting applications and operating systems.

Cryptography-based Mechanisms

IPSec prevents attacks by using cryptography-based mechanisms. Cryptography allows information to be transmitted securely by hashing and encrypting the information.

A combination of an algorithm and a key is used to secure information:

- The algorithm is the mathematical process by which the information is secured.
- A key is the secret code or number required to read, modify, or verify secured data.

IPSec uses a policy-based mechanism to determine the level of security required during a communication session. Policies can be distributed throughout a network by means of Windows® 2000 domain controllers, or created and stored locally within the registry of a Windows XP Professional– based computer.

IPSec at Work

Before the transmission of any data, an IPSec-enabled computer negotiates the level of security to be maintained during the communication session. During the negotiation process, the authentication method, a hashing method, a tunneling method (optional), and an encryption method (also optional) are determined. The secret authentication keys are determined locally at each computer by using information that is exchanged at this time. No actual keys are ever transmitted. After the key is generated, identities are authenticated, and secured data exchange can begin.

The resulting level of security can either be low or high, dependent upon the IP security policy of the sending or receiving computer. For example, a communication session between a Windows XP Professional– based computer and a non-IPSec-aware host might not require a secure transmission channel. Conversely, a communication session between a Windows 2000 server containing sensitive information and an intranet host might require high security.

Smart Card Support

A smart card is an integrated circuit card (ICC) approximately the size of a credit card. You can use it to store certificates and private keys and to perform public key cryptography operations, such as authentication, digital signing, and key exchange.

A smart card enhances security as follows:

- It provides tamper-resistant storage for private keys and other forms of personal identification.
- It isolates critical security computations involving authentication, digital signatures, and key exchange from parts of the system that do not require this data.
- It enables moving credentials and other private information from one computer to another (for example, from a workplace computer to a home or remote computer).

A PIN Instead of a Password

A smart card uses a personal identification number (PIN) instead of a password. The smart card is protected from misuse by the PIN, which the owner of the smart card selects. To use the smart card, you insert the card into a smart card reader attached to a computer, and then enter the PIN.

A PIN offers more protection than a standard network password. Passwords (or derivations, such as hashes) travel over the network and are vulnerable to interception. The strength of the password depends on its length, how well it is protected, and how difficult it is for an attacker to guess. In contrast, a PIN never travels

on the network. In addition, smart cards allow a limited number (typically three to five) of failed attempts to key in the correct PIN before the card locks itself. After the limit is reached, entering the correct PIN does not work. The user must contact a system administrator to unlock the card.

Smart Card Standards

Windows 2000 supports industry-standard, Personal Computer/Smart Card (PC/SC)−compliant smart cards and Plug and Play smart card readers that conform to specifications developed by the PC/SC Workgroup. To function with Windows 2000 Server and Windows XP Professional, a smart card must conform physically and electronically to ISO 7816-1, 7816-2, and 7816-3 standards.

Smart card readers attach to standard personal computer peripheral interfaces such as RS-232, PC Card, and Universal Serial Bus (USB). Some RS-232 readers have an extra cable that plugs into the PS/2 port to draw power for the reader. However, the reader does not communicate through the PS/2 port.

Readers are standard Windows devices, and they carry a security descriptor and a Plug and Play identifier. Smart card readers are controlled by standard Windows device drivers, and you can install and remove them by using the Hardware Wizard.

Windows 2000 Server and Windows XP Professional include drivers for various commercially available plug and play smart-card readers that are certified to display the Windows-compatible logo. Some manufacturers might provide drivers for non-certified smart card readers that currently work with the Windows operating system. Nevertheless, to ensure continued support by Microsoft, it is recommended that you purchase only smart card readers that display the Windows-compatible logo.

Logging On Using a Smart Card

Smart cards can only be used to log on to domain accounts, not local accounts. When you use a password to log on interactively to a domain account, Windows 2000 Server and Windows XP Professional use the Kerberos V5 protocol for authentication. If you use a smart card, the operating system uses Kerberos version 5 authentication with X.509 v3 certificates unless the domain controller is not running Windows 2000 Server.

- **To initiate a typical logon session,** you must prove your identity to the Kerberos Key Distribution Center (KDC) service by providing information known only to you and the KDC. The secret information is a cryptographic shared key derived from your password. A shared secret key is symmetric, which means that the same key is used for both encryption and decryption.

- **To support logging on by using a smart card,** Windows 2000 Server implements a public key extension to the Kerberos protocol's initial authentication request. In contrast to shared secret key cryptography, public key cryptography is asymmetric; that is, two different keys are needed—one to encrypt, another to decrypt. Together, the keys needed to perform both operations make up a private-public key pair.

When a smart card is used in place of a password, a private-public key pair stored on your smart card is substituted for the shared secret key derived from your password. The private key is stored only on the smart card. The public key can be made available to anyone with whom you wish to exchange confidential information.

Smart Cards for Administrative Use

Administrators need tools and utilities that allow them to use alternate credentials so they can do their normal business—with normal user privileges—while at the same time carrying out their special administrator functions. Utilities such as Net.exe and Runas.exe meet this need. In Windows XP Professional, these tools have been enabled to support smart card credentials.

Kerberos Version 5 Authentication Protocol

In Windows 2000 and Windows XP Professional, your credentials can be supplied by a password, a Kerberos ticket, or a smart card if the computer is equipped to handle a smart card.

The Kerberos V5 protocol provides a means for mutual authentication between a client, such as a user, computer, or service, and a server. This is a more efficient means for servers to authenticate clients, even in the largest and most complex network environments.

Kerberos Assumption

The Kerberos protocol is based on the assumption that initial transactions between clients and servers take place on an open network. This is an environment in which an unauthorized user can pose as either a client or a server and intercept or tamper with communication between authorized clients and servers. Kerberos V5 authentication also provides secure and efficient authentication for complex networks of clients and resources.

The Kerberos version 5 protocol uses secret key encryption to protect logon credentials that travel across the network. The same key can then be used to decrypt these credentials on the receiving end. This decryption and the subsequent steps are performed by the Kerberos Key Distribution Center, which runs on every domain controller as part of Active Directory.

Authenticator

An *authenticator*—a piece of information, such as a time stamp, that is different each time it is generated—is included with the encrypted login credentials to verify that previous authentication credentials are not being reused. A new authenticator is generated and incorporated with the KDC's encrypted response to the client to confirm that the original message was received and accepted. If the initial logon credentials and the authenticator are accepted, the KDC issues a ticket-granting ticket (TGT) that is used by the LSA to get service tickets. These service tickets can then be used to access network resources without having to re-authenticate the client as long as the service ticket remains valid. These tickets contain encrypted data that confirms your identity to the requested service. Except for entering an initial password or smart card credentials, the authentication process is transparent.

See Figure 14 for an illustration of authentication rule properties.

Figure 14 Authentication Rule Properties

Kerberos Key Distribution Center Service

This is the service used, together with the Kerberos authentication protocol, to authenticate logon requests to Active Directory.

Even though the Kerberos version 5 authentication protocol is the default for Windows 2000 Server and Windows XP Professional, both network domain controllers and client computers must be running

Windows 2000 or Windows XP Professional for Kerberos authentication to be used. The alternative NTLM protocol is used for authentication if the above conditions are not met.

Summary

Windows XP is available in two editions—Windows XP Home Edition for home use, and Windows XP Professional for businesses of all sizes. Overall, security has been improved in Windows XP to help you have a *safe, secure, and private* computing experience.

If you're using Windows XP Home Edition, you will enjoy security services designed to be flexible and that take into account a wide variety of the security and privacy situations that you'll face as a home user. With Windows XP Professional installed on your computer, you'll have the security features you need for business networking and security—features that deliver new management capabilities that will lower the costs of IT and allow you to spend more time building business services and solutions.

Related Links

- Read the article, Windows XP Networking Features and Enhancements at http://www.microsoft.com/windowsxp/pro/techinfo/howitworks/networking/default.asp
- To learn more about Windows security, visit the Security section of the Windows 2000 Web site at http://www.microsoft.com/windows2000/technologies/security/default.asp.