

Windows XP Security Management

Volume 1, Issue 1

June 2004

In this issue...

How software restrictions help secure Windows XP5

Windows XP security tips8

Attention!

Subscribe to our FREE *Windows XP Security Management* newsletter, and you'll get an e-mail notification when we publish each quarterly edition. No more surfing to find it on the site. No more reminders on your calendar that it's time to look for it. You won't miss an issue. [Just instantly sign up now!](#)

Configure IT Quick: Make EFS part of your Windows XP security plan

By Debra Shinder

Once upon a time, encryption was something that was used only by government agencies, contractors working on top-secret military projects, and the most paranoid of private sector corporate entities. Times have changed. Today almost all businesses and many individuals have information stored in digital form that could cause embarrassment or even disaster if it fell into the wrong hands. We carry sensitive data around on portable computers, which are easily lost or stolen. We put confidential information on desktop machines that are located in physically vulnerable areas. We store critical trade secrets and personal client records on servers that are connected to the Internet and exposed to hackers. Today encryption is for everybody. It provides another layer of protection for information that must be kept private.

Luckily, encryption is getting easier and less expensive. Beginning with Windows 2000, Microsoft has built encryption capabilities into the operating system, and the encryption functionality has been improved in Windows XP. In this article, I will explore how Microsoft's Encrypting File System (EFS) compares to third-party encryption methods. I'll provide a brief overview of how EFS works "under the hood," and I'll explain how the version of EFS in Windows XP differs from that in Windows 2000. I will also discuss EFS vulnerabilities and list best practices for making EFS more secure.

Data encryption methods

There are several different methods for encrypting data. Different methods can be categorized by the state of the data when encrypted (stored on disk or in transit on the network), by the number of keys required (symmetric or asym-

metric encryption), by the algorithms used (DES, IDEA, RSA, and so on), and in a number of other ways.

NOTE:

In this article, I am discussing only methods of encrypting stored data. There are other encryption mechanisms, such as IPsec, used to encrypt data in transit across the network.

Categorizing methods for encrypting stored data

You can categorize methods of encrypting data stored on disk based on the level at which the encryption occurs. For example:

- **Disk level encryption:** Here the entire disk is encrypted, including operating system, swap files, and so on and a password, smart card, or other authentication mechanism is required in order to boot the computer.
- **Partition level encryption:** A partition is created for encrypted data. Any data stored on that partition is automatically encrypted, with no action required on the part of the user.
- **Virtual drive encryption:** Virtual drives (which are called containers, but are actually considered files) are created and encrypted with a key stored on the system or elsewhere (such as on a smart card or floppy). Separate secure containers can be created for different users or for devices such as Zip/Jaz drives.
- **File/folder level encryption:** Data can be encrypted on a file-by-file or folder-by-folder basis.

Advantages of file/folder level encryption

Microsoft's EFS gives you the ability to encrypt data at the file or folder level. Other encryption software, such as **Kryptel**, **SecretAgent**, and many other third-party products also offer file level encryption. Some of these products use symmetric (secret key) encryption; they require that you set a password on each file you want to encrypt, and the same password must be entered to decrypt the file.

ScramDisk and **DriveCrypt** are third-party products that create virtual drives. An advantage is that they let you encrypt data on FAT-formatted partitions (EFS works only on NTFS partitions). Another product that uses virtual drives is **SafeDisk**. You access the containers using a password, and it can be used with Windows 9x operating systems. **PGPdisk** lets you set aside a location on disk that will be encrypted, which can be accessed using either a pass phrase or a PGP private key. EFS uses digital certificates and a combination of symmetric and asymmetric (public key) encryption, as I'll discuss in the "under the hood" section later in this article.

The biggest advantage of file/folder level encryption is the flexibility it gives you to encrypt only those files you want to protect, without worrying about where the files are stored. With other methods, every file on a particular partition, virtual drive, or disk is encrypted. Encrypting certain files, such as operating system and application files, can cause problems in performance.

Although partition and virtual drive encryption provide convenience—all a user has to do is put the file on the partition or drive to encrypt it—the same effect can be achieved with EFS by creating encrypted folders. Then any file that you create in or

move to that folder will automatically be encrypted.

A big advantage of EFS is its transparency to the user. Because it relies on certificates and keys that are assigned to the logged on user, there is no need for an authorized user to enter passwords or take other action to view and work with encrypted files. However, if an unauthorized user attempts to open the files, he/she will receive an "access denied" message.

How EFS works "under the hood"

EFS is integrated with the NTFS file system and, thus, only files/folders on NTFS-formatted partitions can be encrypted. If you move an encrypted file to a FAT partition or floppy, it will be decrypted. Microsoft has implemented encryption as a file attribute, so that encrypting a file or folder is as easy as accessing its properties sheet, clicking the Advanced button, and selecting a check box.

TIP

Encryption-related tasks can also be performed at the command line, using the `cipher.exe` tool.

This apparent simplicity is deceiving, however, as there's a lot more going on with EFS "under the hood." Here's how it works, in a nutshell: When a user elects to encrypt a file, EFS generates a random number that becomes the file's File Encryption Key (FEK). Then a variation of the DES symmetric encryption algorithm, called DESX, encrypts the file and stores it on disk. Symmetric encryption is used because it's faster, and files to be encrypted can be large.

However, that's not the end of the story. The FEK itself is also encrypted, using asymmetric encryption, with the public key assigned to that user. Asymmetric encryption is slower, but

more secure, and since the FEK is small, performance isn't an issue this time. Now when the user wants to decrypt the file, his/her private key is used to decrypt the FEK, which is then used to decrypt the actual file. Thus EFS combines the performance advantage of secret key encryption with the higher security level of public key encryption.

The key pair is tied to an EFS certificate. If this is the first time the user has encrypted a file, a certificate will be issued and a key pair will be generated for this purpose. If the user already has an EFS certificate, the associated key pair will be used. Users can also request an EFS certificate from a certification authority (CA). If there is no CA on the network, EFS generates self-signed certificates for users. When the user logs onto the computer, his or her certificates are associated with the user account and are automatically available when encryption or decryption needs to be performed.

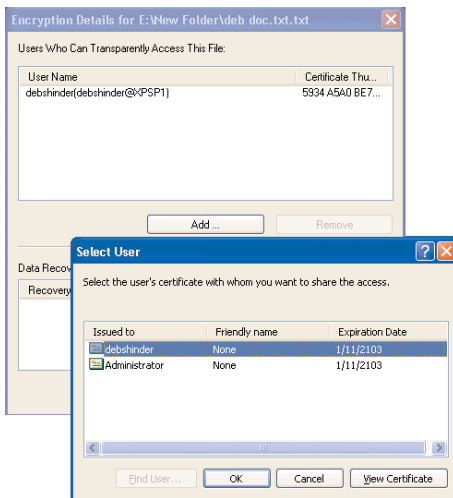
New and improved EFS in Windows XP

One serious drawback of EFS in Windows 2000 is the inability to share EFS files with other users. Because of the way the FEK encryption process was designed, only the user who encrypted the file could decrypt it. There was no way for multiple users to share encrypted files.

Microsoft fixed this problem in Windows XP. Now the user who originally encrypts the file can select to share it with others. To do this, the user must select specific users who will be allowed access to the encrypted file. These users must have a valid local or Active Directory user account and an EFS certificate associated with that account. Then the additional users can decrypt the file with their own private keys.

Figure A shows the interface, accessed from the Details button on the Advanced Attributes properties sheet, which is used to share EFS files with other users. Only the user accounts that have EFS certificates will show up in the list of users with whom you can share the file. The accounts of users who have not ever encrypted a file (or requested an EFS certificate from a CA) will not appear on this list.

Figure A



Users who have EFS certificates can be given access to encrypted files.

Enterprise issues

EFS is designed so that it's not necessary to have a CA on the network in order to use file encryption. If there's no CA, the EFS component will issue a self-signed certificate to each user the first time the user requests to encrypt a file. There are, however, some advantages to using a CA to create EFS certificates, if you're in a high-security or enterprise environment. This allows the network administrator to manage the certificates centrally, and using certificate services, you can revoke certificates and specify the length of time certificates are valid. It's also possible to set up computers as dedicated recovery computers and issue specific recovery certificates to them, instead of issuing the recovery certificate to the domain controller.

In a domain environment, a recovery policy is normally defined at the domain controller, and, by default, the domain administrator is the designated recovery agent. A recovery agent is issued a special recovery agent certificate that allows for decrypting files that were encrypted by other users. There must be at least one recovery key configured on the system; otherwise, no one will be able to encrypt files. When you try, you will get an error message.

EFS vulnerabilities

Like any other security measure, EFS is not perfect. That's why it should be part of a multilayered security plan. Most of EFS's security vulnerabilities occur when it's used on a standalone computer. The domain environment offers more protection. However, one of the most important uses of encryption is to protect data on standalone laptop/notebook systems, so it's important to be aware of the ways that a determined intruder could circumvent EFS's protections to gain access to your encrypted files.

One security disadvantage of file level encryption in comparison to disk level encryption is that the operating system files are not encrypted. This means that if someone steals your laptop, he may still be able to boot into the OS. There are a number of hacker tools available for cracking user account passwords, and he only needs the password of one user account to get into the system. The intruder will then be able to access any files that were encrypted by the user who holds that account.

What if he wants to access a particular encrypted file? Will he have to crack every user account and try each one in turn until he finds the user who encrypted the file? Unfortunately, this is not an issue for a savvy hacker because it's likely he will be familiar with such tools as `efsinfo.exe`, which

is part of the Windows 2000 resource kit. This tool can be used to determine the identity of the original user that encrypted the file.

If the intruder cracks the administrator account, though, he'll be able to read everyone's encrypted files unless you've changed the default by which the built-in administrator account is the EFS recovery agent, and even then, he can use `efsinfo.exe` again to find out which account has been designated as the recovery agent. So all the encrypted files will be wide open to him—unless you've taken steps to remove the recovery certificate from the machine.

Even in a domain environment, a hacker may be able to access cached logon credentials, capture logon information with a sniffer as it travels across the network, use replay methods to log on to the network with a valid account, or use brute force methods to guess passwords and gain access. These are not vulnerabilities of EFS itself, but because of EFS's transparent nature, once logged on while impersonating a valid user, the hacker can access all of that user's encrypted files.

EFS best practices

Following Microsoft's recommended best practices for using EFS will enhance the security of your encrypted data. For example:

- Have the recovery agent use the Export command from the Certificates MMC to back up the recovery certificate and the private key associated with it. Store this in a secure location, and delete the recovery certificate from the local machine. A hacker who cracks the recovery agent's account won't be able to use it to access everyone's encrypted files.
- Use Microsoft's Syskey utility and either put the startup key on a floppy disk, which will require that the

floppy be inserted in the drive in order to boot into the OS, or set a password that must be entered before the boot process can be completed. An advantage of this is that when Syskey is used, encrypted files become unavailable when it's disabled, so even if the hacker disables it, he won't have access to those files.

- Assign recovery agent certificates to accounts that are created for that purpose. Remove the recovery agent certificate from the default admin account, and ensure that the recovery account(s) is not used for any other purpose. Set a very strong password on the recovery agent account(s).
- In a domain environment, if you use roaming profiles, make sure that clients and the domain con-

troller are configured to use IPSec so that hackers can't capture users' private keys, which are downloaded to them at logon as part of their profile. IPSec will encrypt this data as it travels across the network.

- Be sure that encrypted files are not being saved in unencrypted form to temporary locations when you work with the files. Encrypt Temp directories and encrypt the folders in which your encrypted files are stored, rather than just encrypting the files themselves. Some applications save temporary files in the working directory.

Not the only security measure in town

Most importantly, don't rely on EFS—or any other security measure—as

your only means of protecting your data. Create a multilayered security plan in which you use EFS to act as a "vault" inside other front-line defense measures. Homeowners may put valuables into a safe inside the house, but that doesn't mean they shouldn't also put a fence around the property, lock the doors, and install an alarm system. Your data should be protected from intruders at the perimeter of the network (by a firewall), at the "front door" of the computer (by logon passwords), and once inside the OS (by access permissions), as well. If all these fail, EFS is your last line of defense that prevents intruders from reading the file once they get to it. ❖

From the TechProGuild subscription product. **Subscribe today.**

Help us help you!

We'd like to know what topics you'd like to read about in the next issue of the *Windows XP Security* newsletter. Send us some mail at itmanager@techrepublic.com and tell us which of the following topics you'd like to read about. Also please tell us if there's a topic we haven't listed that you're interested in.

- How to increase security with XP Registry edits
- How to provide remote assistance on computers behind a NAT device
- How to disable network access to floppy/CD-ROM drives
- How to use XP registry edits to view which hot fix and Service Pack patches are installed
- How to create your own Windows XP Security template
- How to set and troubleshoot NTFS permissions in Windows XP

Help from your peers

If you don't find the answer to your XP question in these pages, you may find it in our Discussion and Technical Q&A areas in the words of your peers. Here are a couple of places to get you started:

<http://techrepublic.com.com/5208-6239-0.html?forumID=47&threadID=151626>

<http://techrepublic.com.com/5208-6239-0.html?forumID=47&threadID=151327>

<http://techrepublic.com.com/5208-6286-0.html?forumID=11&threadID=15095&start=0>

<http://techrepublic.com.com/5208-6286-0.html?forumID=11&threadID=97026&start=0>

How software restrictions help secure Windows XP

By Debra Shinder

Windows XP and Windows Server 2003 include a new feature called Software Restrictions, which allows you to control what programs can run on the computer and prevent potentially unsafe software from being able to run. This strategy gives you a way to prevent the running of unauthorized programs that might pose a security threat or contain viruses and will help prevent the installation of Trojans through which hackers can gain access to the computer.

What are software restriction policies?

First, a little history: With Windows 2000, Microsoft introduced the concept of trusted code through a feature called driver signing. This provides a way to verify that a piece of software (in this case, a hardware device driver) has been tested and works properly with the operating system. This was done through the issuance of a digital signature. You could set the system to block the installation of any drivers that didn't include the Microsoft digital signature.

Software restriction policy, as implemented in XP and Windows Server 2003, takes the idea of trusted code much further. You can now control whether all types of software applications (not just drivers) can be installed by classifying each program as trusted or not trusted, based on restriction levels and rules that you configure.

Restriction levels and rules

Restriction policies can be set for one of two security levels: unrestricted or disallowed. The unrestricted level is

used for software that you want to be able to run (using the rights assigned to the account of the user who is logged on). The disallowed level prevents the software from running at all, no matter what rights the user might have. You can set a default rule at either of these levels. If you set the default as unrestricted, any programs that you don't specify will be allowed to run. Software access rights for users will be determined by each user's access rights (as set in the User Rights section of Group Policy). If you set the default as disallowed, only the programs that you specify will be allowed to run.

The rules you set up are for the purpose of specifying exceptions to the default. If the default is disallowed, you need to set up rules that specify programs you want to allow to run. If the default is unrestricted, you do the opposite—create rules to specify programs that should not be allowed to run.

There are four types of rules that can be used in restriction policies:

- Hash rules
- Certificate rules
- Path rules
- Internet zone rules

We discuss each of these rule types in the section on how software restriction policies work.

Multilayered control

Restriction policies don't replace the other mechanisms provided in Windows for controlling software installation (such as group policy settings to restrict the right to install software based on user or group account, removal of the Run command from the Start menu, and so forth). Rather, it gives administrators an additional way to exert control over what can run on your computers.

How software restriction policies work

Software restriction policies work essentially like other Group Policy. You create them with the Group Policy Object Editor MMC and apply them to GPOs that can be assigned

A WARNING ON SETTING DISALLOW AS THE DEFAULT

Setting the default as disallowed provides greater security, but might prevent employees from running needed programs if they aren't on the list of programs specifically allowed. Perhaps more importantly, some programs must run other programs in order to accomplish particular tasks. Even though the primary program is specifically allowed, it might not be able to function correctly if you haven't specified other programs that it uses. You should be very careful when setting Disallow as the default.

ANTIVIRUS SOFTWARE IS STILL VITAL

Microsoft cautions that, although software restriction policies can prevent the running of unauthorized programs that might be infected with viruses, you should always run a good antivirus program regardless of the restriction policies you have in place. Restriction policies do not check software for virus definitions, and viruses can be disseminated through e-mail, documents, and other methods.

to local computers, sites, domains or organizational units. In this article, we focus on Windows XP local policies.

In XP, software restriction policies are configured through the Local Security Settings (accessed via Start | Control Panel | Administrative Tools).

Configuring Restriction Policies

The Software Restrictions Policies folder contains two folders: Security Levels and Additional Rules. There are also three additional configuration items: Enforcement, Designated File Types, and Trusted Publishers.

Each of these elements is used as follows:

- The Security Levels folder is used to set the default security level. When you double-click this folder, you see two choices in the right pane: Disallowed and Unrestricted. The current default level is indicated by a checkmark. To change the default, right-click the level that is not currently set as the default, and select Set As Default from the context menu.
- The Additional Rules folder is used to create new certificate, hash, Internet zone, and path rules (exceptions to the default). There are no rules defined here until you explicitly create them. To create a new rule, right-click the folder and select the type of rule you want to create from the context menu. We will discuss rules in more detail in the next section.
- The Enforcement Policies dialog box is used to designate whether restriction policies should be applied to all software files, or all software files except DLLs and other library files. This item also allows you to exempt local administrators from software restriction poli-

CONFIGURING SOFTWARE RESTRICTION IN A DOMAIN

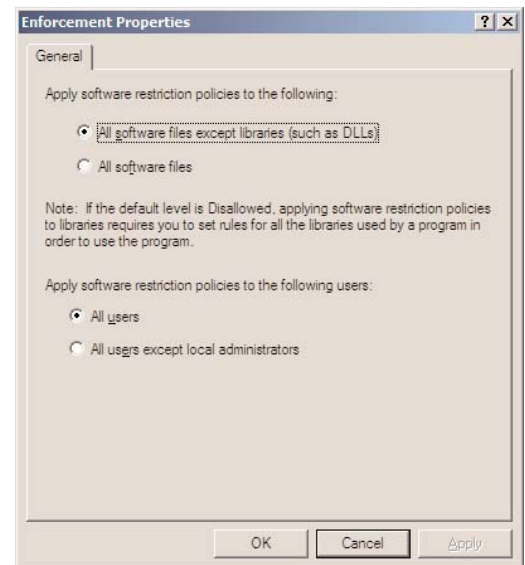
To configure restriction policies for a domain or OU, use Active Directory Users and Computers (ADUC) to open the properties of the domain or OU and select the GPO from the Group Policy tab. Then, in the GPO Editor, you'll have software restriction policies under either the Computer Configuration node (for machine policies) or the User Configuration node (for user policies). You'll have to expand Windows Settings under the appropriate node, and then expand Security Settings to find the Software Restrictions folder.

In the domain environment, like other Group Policy, restriction policies can apply to either users or machines. A machine policy is applied at bootup. A user policy is applied at logon. Machine policies are applied regardless of what user logs on to the machine, and user policies follow a user from one machine to another within a Windows domain.

cies or to specify that they be applied to all users, including administrators. Double-click the item to open its properties box and make these configuration choices, as shown in [Figure A](#).

- The Designated File Types Properties dialog allows you to specify which file types should be recognized as executable code (and thus subject to software restriction policies). Common executable file extensions are included by default (for example, batch files with the .bat extension, compiled help files with the .chm extension, command scripts with the .cmd extension, and so forth). You can add file types to the list or remove those that are already there.
- The Trusted Publishers Policies dialog box can be used to specify who can select software publishers to be trusted: end users, local computer administrators, or enterprise administrators. You can also define that either the publisher, the timestamp, or both be checked to determine whether the certificate has been revoked before considering a publisher to be trusted.

Figure A



You can select to exempt DLL file types from restriction policies, and to exempt local administrators from application of the policies.

Understanding rules

While the other configuration options for software restrictions are pretty straightforward, configuration of rules is a little more complex. However, rules are the heart of your restriction policies, so it's important to understand the various types of rules, when each is appropriate, and how to configure them.

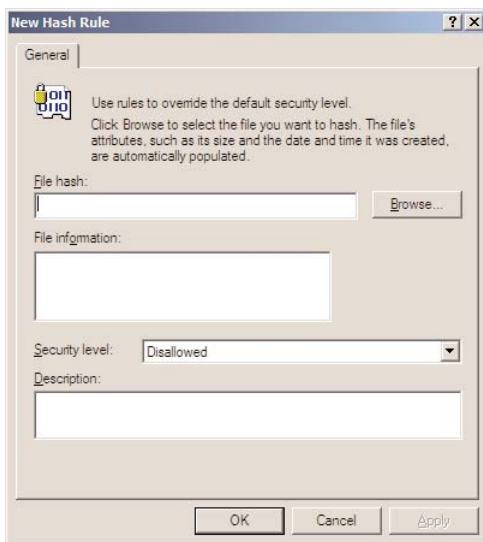
Hash rules

If you're familiar with basic cryptographic concepts, you probably know that a hash is a fixed-length value that represents a string of characters generated by the application of a hashing algorithm (also called the hash function) such as Message Digest (MD) 5 or the Secure Hash Algorithm (SHA).

Hash rules identify software files by their hashes. The hash on the file is compared with the one specified by the rule. If they match, the rule is applied. This can be useful because the hash value remains the same if the executable file is moved to a different location on the disk or if its name is changed. Note, however, that the hash value will change if anyone tampers with the contents of the file itself, and this would allow the software restriction policy to be circumvented if the unrestricted default is selected.

When you create a new hash rule by selecting New Hash Rule from the context menu when you right-click the Additional Rules folder, you first select the file that you want to hash, as shown in [Figure B](#).

Figure B



A hash value is created for the executable file you select when you make a new hash rule.

If the file has been hashed before, only hashes calculated using Software Restriction policies are recognized. However, if you used Software Restriction policies to calculate a value somewhere else, you can copy and paste that hash value in the File Hash text box. Normally you would browse for an executable file and calculate the hash. Remember that the file you select must have an extension that is in the Designated File Types list.

Certificate rules

Digital certificates are based on public key cryptography and are designed to prove the identity of a user, computer, or in this case, a program. A certificate rule identifies files based on their certificates. This applies only to certain types of executable files, most notably scripts and installer packages (.msi files). Certificate rules are not used to identify .exe and .dll files.

You create a certificate rule by selecting New certificate rule from the context menu after right-clicking the Additional Rules folder. You'll be asked to type in or browse for the certificate that applies to the file.

Internet zone rules

The Microsoft Internet Explorer Web browser (MSIE) allows you to set up security zones, including the following:

- **Internet zone:** contains all sites that haven't been put into any other zone
- **Local computer zone:** contains Web sites stored on the local computer
- **Local intranet zone:** contains Web sites located on an internal network (intranet)
- **Restricted sites:** contains Web sites that have been identified as dangerous
- **Trusted sites:** contains Web sites that have been identified as safe

With zone rules, you can identify Windows installer packages based on

the zone where the program runs, as specified through MSIE. Zone rules apply only to installer packages (.msi files).

When you create a zone rule by selecting New Internet Zone Rule from the right context menu after right-clicking the Additional Rules folder, you must select one of the Internet zones from the bulleted list above.

Path rules

A file's path shows where that file is located within the directory structure. You can create rules based on the file path, but it is important to understand that moving the file to a different location on the disk or changing its name will cause the path rule to no longer apply to it. Path rules are useful for allowing or disallowing all programs within a particular folder.

When you create a path rule by selecting New Path Rule from the context menu after right-clicking the Additional Rules folder, you must type in or browse for the path where the program file is located.

Order of precedence

If there are multiple rules configured, they are applied in order of precedence as follows:

- Hash rule
- Certificate rule
- Path rule
- Internet zone rule

This means hash rules have the highest precedence and will override rules of other types, and so forth. If a program has two different path rules assigned, the more specific one will have highest precedence. Thus, if there is a rule that applies to a particular folder and another that applies to a subfolder within it, the rule that specifies the subfolder takes precedence. If you have rules with different security levels (one set to disallow and the other set to unrestricted), disallowed takes precedence.

Use restriction policies wisely

Software restriction policy is a new weapon in your arsenal for protecting your Windows XP computer from dangerous or unauthorized code. However, before you jump in and embrace this new feature, you need to take time to understand how it works, and realize that it is not a

UPDATE GROUP POLICY TO CONFIGURE RULES

Your newly configured rules might not take effect immediately. That's because Group Policy must be updated before they apply. You can force a policy update by typing *gpupdate* at the command line. This command takes the place of the old *secedit* command that was used to refresh policy in Windows 2000.

replacement for—but rather, a supplement to—other control mechanisms such as user access rights, antivirus programs, etc. Using restriction poli-

cies in conjunction with these can add another layer of defense to your XP security strategy. ❖

From the TechProGuild subscription product. [Subscribe today.](#)

Windows XP Professional Resource Guide



Upgrade your skills for Windows XP. Master Microsoft's newest operating system.

- Install & Configure
- Configure XP VPNs
- Run 2000 and XP on One PC
- New Networking Features
- Ensure XP Works with Legacy Apps
- Guard Against Data Loss
- Customize the New GUI
- Perform Administrative Tasks Remotely

Windows XP security tips

Disable IE's downloading capability

Do you support Windows XP users who insist on downloading files from the Web via Internet Explorer—regardless of what you tell them? If so, you'll be glad to know

that you can disable Internet Explorer's ability to download files by tweaking the Security settings.

To disable IE's downloading capability, follow these steps:

1. Launch Internet Explorer.
2. From the Tools menu, select Internet Options.
3. On the Security tab, select the Internet Web content zone (if it isn't already selected), and click the Custom Level button.
4. Scroll through the Settings list box, and locate the Downloads heading.
5. Under File Download, select the Disable radio button.
6. Click OK twice.
7. The next time the user attempts to download a file, Internet Explorer will display a warning message stating that the current security settings do not allow the downloading of files.

Secure unattended workstations with the Windows Exit Screen Saver

One of the biggest security risks for an enterprise is an unattended workstation that a user leaves logged on to the network. In this situation, unauthorized access becomes a very real possibility.

However, Microsoft offers a great solution to this potential problem with the Windows Exit Screen Saver (Winexit.scr), which comes with both the Windows 2000 Server Resource Kit and the Windows Server 2003 Resource Kit. And it works with Windows XP.

The Windows Exit Screen Saver automatically quits any currently running programs and logs off the user of a workstation after a specified time period. You can find this tool on the resource kit CDs, or you can download the Windows Exit Screen Saver from Microsoft's Web site, as part of the *Windows Server 2003 Resource Kit Tools*.

Installing and configuring this tool is easy. Follow these steps:

1. Right-click Winexit.scr, and select Install.
2. On the Screen Saver tab of the Display Properties dialog box, select Logoff Screen Saver, and click the Settings button.
3. Select the Force Application Termination check box to configure the tool to close all running programs.
4. In the Countdown For *n* Seconds text box, enter the number of seconds that you want the tool to display the logoff warning message box before logging off the user.
5. In the Logoff Message text box, enter the message that you want to appear in the logoff warning message box.
6. Click OK.

After the specified period of inactivity, the Windows Exit Screen Saver will beep and display the logoff warning message. If the user takes no action before the countdown timer reaches zero, the system will initiate the logoff procedure. You can stop the process before the countdown timer reaches zero by either moving the mouse or pressing any key on the keyboard.

Put Administrative Tools on the Start Menu

If you regularly perform tasks with the utilities found in the Administrative Tools folder, navigating through Control Panel's folder structure to access these tools can become a hassle.

However, Windows XP offers a way for you to place the Administrative Tools folder on the Start menu. When you do so, the Administrative Tools folder becomes its own menu. Follow these steps:

1. Right-click the Start button, and select Properties.
2. In the Taskbar And Start Menu Properties dialog box, click the Customize button on the Start Menu tab.
3. In the Customize Start Menu dialog box, select the Advanced tab.
4. Locate System Administrative Tools in the Start Menu Items list box.
5. Select the Display On The All Programs Menu And The Start Menu radio button.
6. Click OK twice to close both dialog boxes.

Take control of cookies

In Windows XP, cookies are stored in the C:\Documents And Settings\

While some cookies are useful, others could be considered a violation of your privacy. Fortunately, Windows XP comes with a privacy feature that allows you to control the amount and type of cookies that are saved on your computer. Here's how to use the privacy feature:

1. Open Control Panel, and choose Network And Internet Connection.
2. Click Internet Options, and select the Privacy tab.
3. Use the slider to select a privacy setting.

The default privacy setting is Medium. At the top and bottom of the scale are Block All Cookies and Accept All Cookies, respectively. As you move the slider, you'll see an explanation of the level of privacy that the settings provide.