Global Knowledge™

Experts Teaching Experts

Expert Reference Series

# Windows 2003/2000/XP Security Architecture Overview

# Windows 2003/2000/XP Security Architecture Overview

By Glenn Weadock, MCSE, A+

ABSTRACT

Windows 2003 Server, its workstation cousin Windows XP, and its predecessor, Windows 2000, all bring substantial advances in both reliability and security compared to Windows NT 4.0. However, Windows security has so many different components that just getting a handle on them all can be a major conceptual challenge. Additionally, the number and variety of threats to computer security is increasing daily, and the cost of lost, damaged, or compromised data can be very high.

This briefing lays out the main security features in the Windows 2003 operating system family, and puts them all into a "big picture" context. It is intended for any person who must plan, implement, manage, or administer Windows 2003 family security for networked desktop computers, notebook computers, or stand-alone systems. It is not intended as an exhaustive treatment of all the possible security breaches that a Windows network administrator may face, but rather as a framework for understanding, planning, and discussing specific security features, as well as organizational policies and procedures.

## TABLE OF CONTENTS

4. Security Configuration and Analysis

H. Auditing

1. Logon Auditing
2. Object Auditing

## A. Pre-Logon Security: Computer Accounts

The first category of Windows security measures is one that a networked computer bumps into shortly after being powered on. Before you even see the logon dialog box, the computer has already "checked in" with a Windows 2000 or 2003 server by means of a *computer account*. That is, regardless of who logs on to that PC, the server can apply some restrictions to the machine through the use of Registry-modifying *policies*. (Windows 95 and 98 do not have computer accounts.)

You can think of computer accounts as analogous to a locked gate in front of your house's driveway. Nobody can even get to the front door and present himself for identification before he gets through the front gate. Computer accounts are the first line of defense against harm – but note that they are only effective in a Microsoft network environment.

When you first install a Windows 2000 or XP Professional workstation into a networked environment by joining the computer to a domain, you must do one of two things: Create a computer account for the PC ahead of time (e.g. in Active Directory Users and Computers), or, during the installation, provide (when prompted) the user name and password of a user (such as a domain administrator) with authority to create a computer account on the domain.

To control the operations that any user can perform at any given computer, regardless of the account that the user logs in with, open Active Directory Users and Computers, right-click the domain or Organizational Unit of interest, and choose Properties. Click the Group Policy tab and double-click the entry for the policy object (for example, Microsoft supplies a default domain policy). All of the settings that appear under the node "Computer Configuration" are policy settings that you can make for all computers in the domain. For example, under *Computer Configuration\Administrative Templates\System*, you could set the *Disable Autoplay* policy to prevent CD-ROMs from running automatically after being inserted into the drive (see Figure 1).

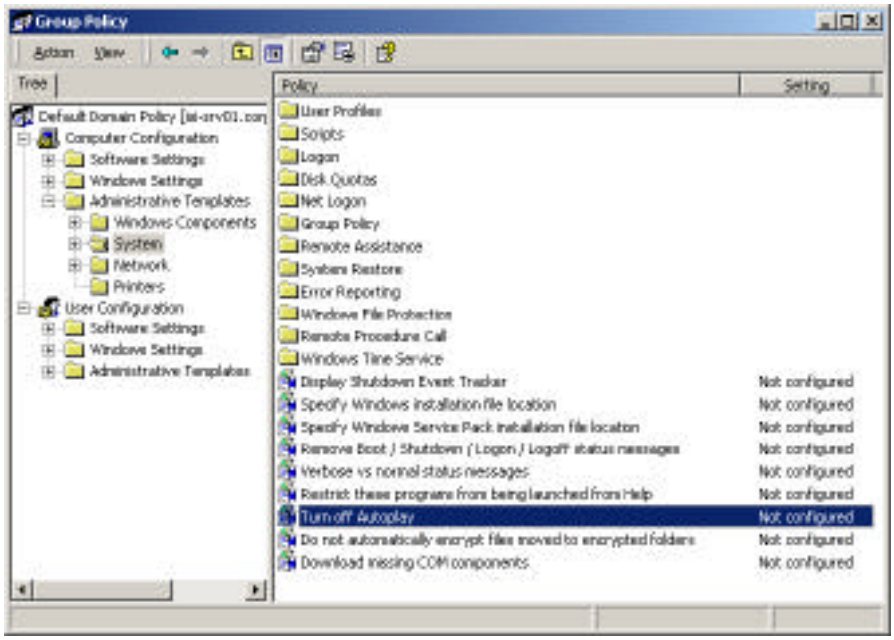


**Figure 1. Computer accounts let you make settings regardless of who logs on.**

## B. Logon Security: Getting in the Door

Logon security is the second type of security (the second line of defense, after computer accounts, against both intentional and unintentional harm) that Windows 2000/2003/XP lets you configure. The default behavior is to require a user name and password before you can log on. You can change that behavior for a stand-alone Windows 2000 or XP PC, but think twice before you do. Removing that protection makes your PC much less secure. You can think of logon security and user authentication as a locked front door on your house, with a peephole to identify visitors.

Windows 2000/2003/XP can use various technologies to authenticate a network user's logon request: *Kerberos* (the default "behind-the-scenes" technology), *certificates* (optional for secure identification of workstation users), and *smart cards* (such as SecurID, which require the user to have both a physical credit-card size device and know a password to log on).

### 1. User Names

Every Windows user account must have a user name and a password. A cracker would have to know both the user name and the password to gain access to a system or network. Therefore, choosing a user name has security implications. The less obvious the user name, the harder it is for someone else to guess it.

Having said that, most people find it difficult enough to remember a properly obscure account password, much less an obscure password *and* an obscure user name. The typical convention is to build the user name from the user's actual last name and the initial of the first name; thus, Larry Ellison becomes LEllison. A user name must be unique among all other user names and group names in the forest (or workgroup).

### 2. Passwords and Password Policies

Logon security depends on passwords. The problem with passwords is that they are too easily guessed or not complex enough to foil crackers. On a networked computer, however, you can apply some policies to enforce better passwords and better password maintenance. Choose the Domain Security Policy command on a server's Administrative Tools menu (see Figure 2). Change an account policy by double-clicking it and modifying its value. Password policies that you set for the domain will apply to every member of the domain.

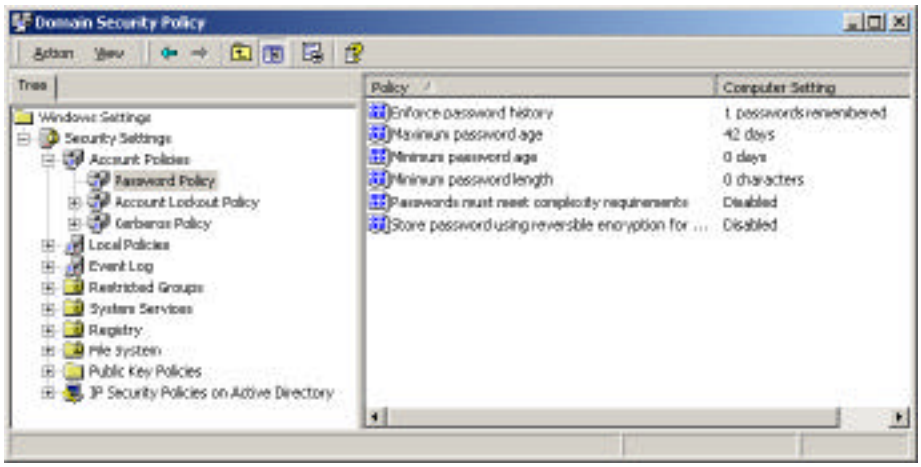


**Figure 2. Password policies let you strengthen logon security.**

Because logon security is such an important element of Windows security, Microsoft provides a way for you to "lock" a computer when you plan to be away for only a brief while and would rather not shut the system down. Press Ctrl+Alt+Del to display the Windows Security dialog box, and click the Lock Computer button. (You can implement an even quicker method by creating a shortcut to "**%windir%\system32\rundll32.exe user32.dll,LockWorkStation"**.) You will need to log on again when you return to the machine. A locked desktop is typically much more secure than a password-protected screen saver. Also, existing programs (a download, a disk defragmentation operation, etc.) continue to run while the computer is locked. In this way, the machine can be doing useful work while you are away, yet is still protected against someone else using the machine interactively. User education is a key part of enhancing Windows security via desktop locking.

What if you are running Windows 2000 or XP logged in as say, a Power User, and you need to perform a Registry edit that only an Administrator can perform? You can log off and log back on, but a faster way exists. For example, hold down the Shift key and right-click REGEDT32.EXE. (You don't need to hold down Shift in Windows 2003 or XP.) Then, choose the "Run As" option, which lets you enter the Administrator's name and password so you can run REGEDT32 as the Administrator. You can use this capability to run any program, not just REGEDT32 and REGEDIT.

Windows sometimes prompts you when you try to perform a task that requires administrative privileges, but sometimes it does not. The RunAs service lets you run any program under any security context. The major benefit is that even network administrators and IT support personnel need not perform routine daily work with their administrative account. That's an important security issue, because any virus or potentially malicious code that you may run across when logged on to a PC with administrative privileges will operate in your security context.

### 3. Account Lockout

Account lockout policies help frustrate intruders who repeatedly try to log on to a PC to which they have no approved access. These policies, which you view in the Domain Security Policy console of a Windows 2000/2003 Server domain controller, are as follows:

- **Account lockout duration.** How many minutes Windows locks out a user after the user makes X number of invalid logon attempts.
- **Account lockout threshold.** How many invalid logon attempts trigger the lockout, at which point Windows will not permit more tries until the lockout duration period has passed.
- **Reset account lockout counter after.** How many minutes to wait after an account lockout before giving the user a "clean slate" to try logging on again.

### 4. Remote Access Security I: RRAS, IAS, and AD

Maintaining the security of that locked front door in our analogy becomes somewhat more complex when employees are telecommuting or otherwise working remotely. The Windows world provides some additional requirements for users connecting via dial-up lines or Internet links – appropriate, considering that virtually anyone can potentially "dial in" to a computer network from the outside world, whereas only persons with physical access to a network PC can log on to a wired LAN.

#### *a. Authentication Protocols*

The manner in which a remote link conveys a user's credentials has significant security implications. PAP (Password Authentication Protocol), for example, is generally not considered a good idea, because it specifies that the user name and password travel the link in cleartext (that is, unencrypted). MS-CHAPv2 is a much better idea and is supported by Windows 2000 Server and Windows 2003 Server. Smart cards generally use EAP (Extensible Authentication Protocol).

#### *b. AD Authentication*

Authentication does not guarantee access. By default, no one can access an Active Directory network unless their user account permits such access. AD administrators can limit dial-in access privileges through the Active Directory Users and Computers tool, as well as through network-based Group Policy settings.

#### *c. RRAS and IAS*

If you use Microsoft's remote access software, you'll use RRAS (Routing and Remote Access Service), IAS (Internet Authentication Service), or both. RRAS is the software, running on a

member server or domain controller, that permits users to dial in and access either the RRAS server itself, or the network to which the RRAS server connects (in which case the RRAS server functions as a gateway to the rest of the internal network). You can think of IAS as an "authentication clearinghouse" when multiple remote access servers are needed and an organization wants to centralize the authentication chores. (RRAS servers don't share information with each other and are configured independently.) IAS is an example of RADIUS, Remote Access Dial-In User Service.

In a native-mode environment (that is, no NT 4.0 domain controllers), both RRAS and IAS offer good flexibility in creating rules to restrict who can gain remote access to the network; when that access can occur; and what type of access it will be. Administrators can define *remote access policies and profiles* in the RRAS management console to specify these restrictions in considerable detail.

## 5. Remote Access Security II: Securing System Software

It has become increasingly clear in recent months and years that operating system vulnerabilities remain a major security concern, even at this late date. Although the types of OS vulnerabilities vary, many of the more serious ones operate by overloading an input buffer in such a way that the OS becomes overwhelmed and can no longer handle its security chores properly. In our homeowner's analogy, you could think of these intrusive attacks as a group of mice that sneak in to your house unnoticed when you crack open the front door to speak with the UPS guy.

Microsoft has provided two mechanisms for deploying operating software patches and upgrades: *Windows Update* and the related *Software Update Server* (*SUS*). The company has also offered software to help secure the Internet-related components of the Windows distribution: proxy servers and firewalls. Finally, a strong antivirus software strategy can foil those few instances of malicious code that may still get past the foregoing security measures.

### *a. Windows Update*

The Windows Update feature that has appeared as a shortcut on the Start menu for several generations of Windows has been enhanced in XP, 2003, and Windows 2000 SP3 to provide an automatic notification/installation feature. A downloadable ActiveX control scans the local PC and checks for critical updates and patches on Microsoft's public web site. While Windows Update can be a handy tool for home users to download the latest critical security patches, it has created difficulties in the business environment because of a lack of control. That is, users can install patches that IS has not tested for compatibility. Windows Update can also create a situation in which support staff don't know which machines have had which updates applied, making support and troubleshooting more difficult. Microsoft's response is Software Update Server.

### *b. Software Update Server*

Software Update Server (freely downloadable from Microsoft) provides a staging environment where organizations can receive updates from Microsoft, test them for compatibility within the organization's network environment, then flag them for deployment to clients. Group Policy settings "point" client machines away from Microsoft's public Windows Update site and towards the internal SUS machine. In this way, administrators get some of the benefit of automatic updates, while still limiting the risks of deploying fixes that may break other applications. A key to the success of SUS is an organization's commitment to rapid testing, because soon after Microsoft publishes QFEs (Quick Fix Engineering), virus authors release software that exploits the documented vulnerabilities.

### *c. Proxy Servers and Firewalls*

With Windows comes Internet Explorer, and with Windows Servers comes IIS (Internet Information Server), Microsoft's Web hosting environment. Securing Internet access used to be a much simpler task when the Web was in its infancy and 99% of all Web pages presented black text on a gray background. As the Web has become a richer environment, supporting applets and plug-ins and ActiveX controls and such, the possibilities for programs to sneak into a corporate network via Web pages have grown.

IIS itself includes many features for increasing the security of IIS-hosted web sites. These are accessible through the IIS management console. Note that these security features are in addition to any NTFS file-and-folder permissions that you may implement on the Web server. Microsoft's proxy server-slash-firewall product, ISA (Internet Security and Acceleration) Server, succeeds the earlier Proxy Server product and offers intrusion detection, outgoing access controls, application-specific traffic filters and VPN support.

In a corporate environment, you probably do not need firewall software on every PC if you use something like ISA Server, but Windows XP Professional does come with a reasonably effective firewall (ICF, Internet Connection Firewall) that you may want to activate in special circumstances – or on a home network.

The use of proxy servers and firewalls does not preclude another type of security risk, the so-called Denial Of Service attack, in which many computers simultaneously bombard a company's Web server with traffic, overwhelming it. While such attacks can be difficult to prevent, your organization may wish to have a contingency plan to follow in order to mitigate the effects of a DOS attack, such as changing the IP address of key servers.

### *d. Antivirus Software*

Even with the most aggressive policy of patching system software and deploying firewalls to help prevent the mice from sneaking in through the open door, some will squeak by. In those cases, organizations that go beyond Microsoft's offerings and implement best-of-class antivirus measures can stop viruses before they spread – or at least slow them down enough to limit the damage they do. Microsoft does not offer antivirus software as such, but organizations can leverage Windows technologies to deploy such software, either through RIS (Remote Installation Service, for creating and distributing workstation images), Group Policy's software distribution feature (for deploying updates), logon/startup scripts (also implemented via Group Policy), or all of the above. User and group rights and object permissions (discussed next) can also limit damage from unwelcome software intruders that bypass logon security.

## C. User and Group Rights

In the Windows scheme of things, *rights* are *privileges*, that is, actions that specific users and/or groups are permitted to perform on the system. Logging on to the local computer (as opposed to the domain) is a right; so is backing up your hard drive, and submitting a print job. For an analogy, think of friends whom you would allow to use the phone in your house. Other friends you may even trust to walk the dog or water the plants.

Windows lets you assign different rights on the PC and on the network by user and by group. A *group* is simply a collection of user accounts. Users can belong to multiple groups at one time, and groups can belong to other groups. The reason groups exist is to make the assignment of privileges and restrictions easier, because these can be set on a group basis instead of on an individual basis. (Groups exist even on a non-networked Windows system.)

To make life easier, Microsoft endows Windows 2000, 2003, and XP with various built-in user and group accounts. You have the flexibility to create new users and groups, with a customized set of rights; but on a small to medium-size network, you may find that the built-in accounts provide all the security options you need.

- **Local accounts** exist in the local security database only and allow access to local resources. A stand-alone Windows 2000 or XP Professional computer would use only local accounts. A workstation in a *workgroup*-type network (also called *peer-to-peer*) would also use local accounts only.
- **Domain accounts** exist on domain controllers (servers), and allow access to network resources. A networked Windows 2000 or XP Professional computer would normally use a domain account for everyday work, for security, centralized administration, and access to domain-based resources.

Check out the details of which rights go with which local groups by choosing Local Security Policy from the Administrative Tools menu, and opening the node *Security Settings\Local Policies\User Rights Assignment* (see Figure 3).

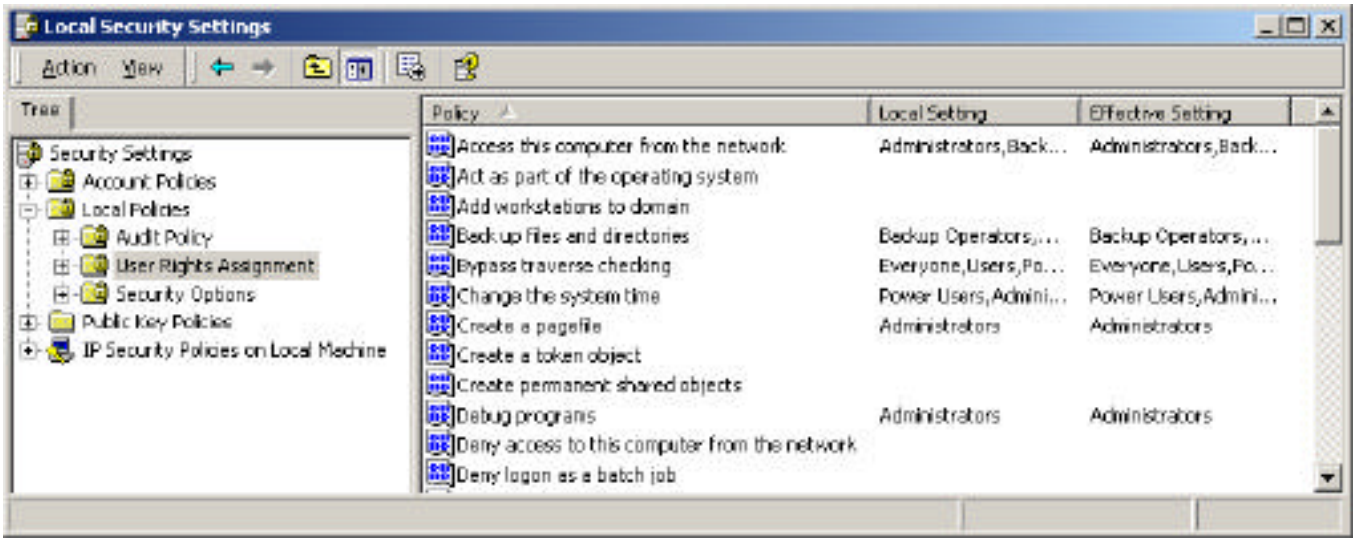


**Figure 3. Checking out user rights for various built-in groups.**

## 1. Built-In Local User and Group Accounts

### *a. Local User Accounts*

Windows 2000 and XP Professional come with two built-in local user accounts: *Administrator* and *Guest*. (You can see these accounts via the *Users and Passwords* control panel.)

Here are a few tips about the Administrator account:

- This account has full access to the machine, so you would typically use it when you need to perform system management or configuration tasks.
- You should always rename the Administrator account. Crackers look for it first, because if you can crack this account, you can do whatever you want on the system.
- You should not use the Administrator account for day-to-day use. You could unintentionally damage your system. Any virus, Java applet, or ActiveX control that you execute while logged on as Administrator has full access to your computer.
- You cannot delete this account.

And on the Guest account:

- This account has very limited access and is probably unsuitable for anyone to use on a day-to-day basis. Microsoft recommends it for occasional and temporary use.
- The Guest account is disabled by default.
- If you do use this account, give it a password, and consider renaming it.
- You cannot delete this account.

### *b. Local Group Accounts*

Windows ships with a number of predefined, or built-in, local groups. (You can modify membership in local groups.) These groups offer convenient groupings of user rights that correspond to different user roles on the PC.

Local groups live on the local PC's security database, and their reason for being is to control rights and permissions to resources on the local PC. Local groups exist on Windows 2000/XP Professional computers and on Windows 2000/2003 Server computers that do not function as domain controllers. These include Administrators, Backup Operators, Guests, Users, Power Users, and Replicators. Here are some details on these groups:

***Administrators***

- This group includes the built-in local Administrator user account.
- Membership means you can do virtually anything on the PC.

***Backup Operators***

- Members can back up and restore files on the system even if file access permissions would otherwise prevent access.
- A member of the Users group cannot perform a full backup unless a member of this group.

***Guests***

- This group includes the built-in local Guest user account.
- Members cannot change their desktop setup.
- You must normally grant Guests additional rights for them to do productive work.

***Users***

- Members can run logo-compliant Windows applications.
- Members may not have sufficient rights to run Windows NT applications.
- Cannot create local printers.
- Cannot modify any systemwide settings.
- Cannot install programs for use by other Users.
- Cannot designate folders to be shared.

***Power Users***

- Corresponds with NT4 “Users” group.
- Appears in Windows user interface sometimes as “Standard Users.”
- Can stop and start system services, except those that start automatically.
- Can install applications that do not install operating system services or modify operating system files.
- Can remove users from Guests, Users, and Power Users groups.
- Cannot take ownership of files.
- Cannot modify membership in Administrators or Backup Operators.
- Cannot modify or delete user accounts that they did not create.

***Replicators***

- Only present for compatibility with NT; used by the File Replication service.

Windows XP Professional adds the *HelpServicesGroup* (for use by Microsoft personnel in connection with the Remote Assistance tool), the *Remote Desktop Users* group (for use in connection with the Remote Desktop tool), and the *Network Configuration Operators* group (which can manage network configurations without having full administrative privileges).

You can modify the user rights assigned to users in different groups by applying *security templates* with the Security Analysis and Configuration management console snap-in. (Section G of this paper discusses this tool.) For example, you could apply the COMPATWS.INF template to relax many restrictions on the Users group to permit members to run applications designed for Windows NT 4.0 but not Windows 2000/XP. You can also use the SECEDIT command-line utility to change the rights associated with different groups.

Further, you can create your own local groups, although Microsoft discourages you from doing so on a domain PC. Just as with local user accounts, local group accounts do not gain access to domain resources, nor are they able to be centrally administered.

## 2. Built-In Domain User and Group Accounts

### *a. Domain User Accounts*

In the Windows networking scheme, domain user accounts live on a domain controller – specifically, in the Active Directory database (NTDS.DIT) on a domain controller. The built-in domain user accounts include the following:

- **Domain Admin** (a built-in account for administering the domain)

- **External User** (this account specifies an external or "outside" user who does not have a named account in the Active Directory database)
- **Guest** (similar to the built-in local account of the same name)
- **IUSR_<*servername*>** (an anonymous account used by any unnamed user who accesses IIS, Internet Information Server, Microsoft's Web server product)
- **IWAM_<*servername*>** (an account used by IIS to start external processes)
- **krbtgt** (the key distribution center service account, used for public key encryption)
- **TsInternetUser** (used by Terminal Services only)

***b. Domain Group Accounts***

Domain groups, like domain user accounts, live in the Active Directory database on a Windows 2000/2003 domain controller. The precise list of built-in domain groups on a server machine depends to some extent on what network services run on that machine, but here is a fairly representative list: Account Operators, Cert Publishers, DHCP Administrators, DHCP Users, DnsAdmins, DnsUpdateProxy, Domain Admins, Domain Computers, Domain Controllers, Domain Guests, Domain Users, Enterprise Admins, Group Policy Creator Owners, Print Operators, RAS and IAS Servers, Schema Admins, Server Operators, WINS Users.

Details on membership in these groups are available in the Windows 2000/2003 Server help system and in the Resource Kit (both print and on-line versions).

**3. System Groups**

Windows 2003/2000/XP includes some built-in "system groups" that do not fall neatly into any of the previous categories. (You cannot modify membership in system groups; the operating system controls them.) These include the following:

- **Everyone** (all users, including anonymous ones and guests)
- **Authenticated Users** (authenticated either on the domain or on the local PC. This group contains everyone in the Everyone group with the exception of anonymous users.)
- **Terminal Server Users** (users who have logged on to a Terminal Services machine)
- **Creator/Owner** (a placeholder group whose meaning changes depending on the current owner of an object, such as the user who creates a folder)
- **Network** (all users who have logged on via a network connection)
- **Batch** (all users logged on non-interactively through a script, task scheduler, or other batch method)
- **Interactive** (all users who have logged on interactively)

- **Anonymous Logon** (all users who have gained access to a server, such as a Web server, anonymously)
- **Dialup** (all users who are logged on through a dial-up link)

## D. Object Permissions

If rights are “actions that users and groups can or can’t take,” then permissions are “objects that users and groups can or can’t modify.” The distinction is a subtle one, but the main point to remember is that users have rights, while objects have permissions.

Continuing the homeowner analogy, you may allow your adult neighbors to help themselves to a bottle of wine from your refrigerator when they come over to visit, but you probably would not extend that permission to their eight-year-old child. In fact, it is likely that you would not allow any children to have a glass of wine. The wine bottle is an object, and you control which users and groups can access that object, and the ways in which they can access it.

Windows includes the concept of an object’s *owner*. If you own the wine bottle, you can change the rules that specify who can drink from it. Likewise, in Windows 2003/2000/XP, if you own an object (such as a file folder or Registry key), then you can change the permissions for that object.

The main types of object permissions are as follows:

- Share permissions
- File and folder (NTFS) permissions
- Registry permissions
- Printer permissions

### 1. Share Permissions

When you share a resource (typically, a file folder) for use by other computer users, you can specify which users and groups you want to have access to that resource, and how much access you want them to have. The basic share permissions in Windows 2000 are *read*, *change*, and *full control*.

- **Read** means users can run programs, and open and read files and file attributes, but not change them.
- **Change** means users can do everything allowed by the read permission, plus change files and file attributes and delete folders and files.
- **Full control** means users can do everything allowed by the change permission, plus take ownership of files and change permissions.

Share permissions work on FAT, FAT32, and NTFS disks, and you set them in Windows Explorer using the Sharing dialog box (see Figure 4). To share a folder, you must have the File and Printer Sharing for Microsoft Networks service installed for your network connection. To increase security, disable or uninstall this service on workstations that don’t share resources. You can grant access based on user names and group memberships.

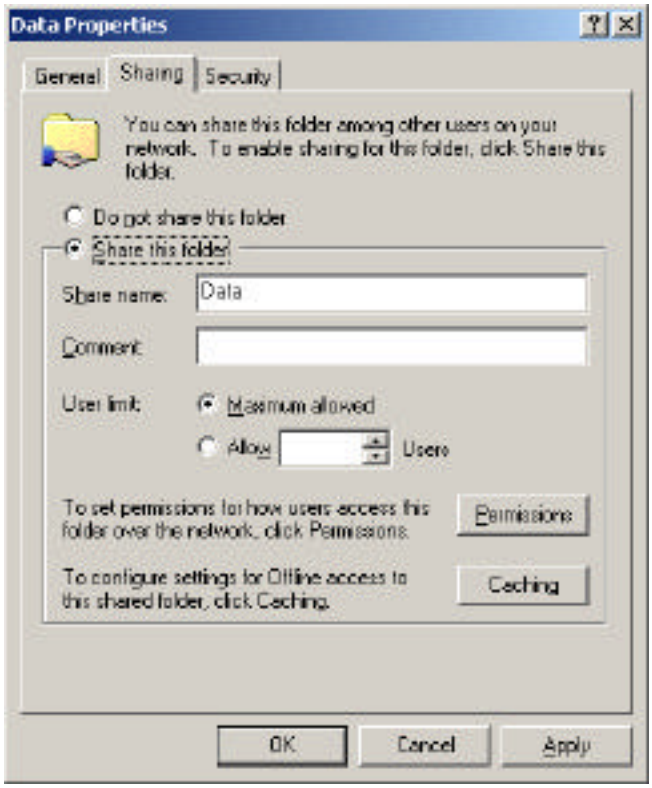


**Figure 4. Click the Permissions button to specify the "who" and "what" access controls.**

A few notes on share permissions:

- Share permissions do *not* affect what a local user can do with a resource on the local PC! They control access across the network *only*.
- You cannot share single files using share permissions, just folders and drives. To share a file, put it into a shared folder.
- You can share folders on removable disk devices.
- Share permissions are the only way you can restrict network user access to a FAT or FAT32 disk drive.

## 2. File and Folder (NTFS) Permissions

If you format a disk using the NT File System, or NTFS, then you have additional permissions available to you beyond share permissions for networked resources. Unlike share permissions, you can also use NTFS permissions for non-networked and non-shared resources.

- Microsoft sometimes calls NTFS permissions "file and folder permissions." As you might expect, you can set these permissions at the single file level or at the folder level.

The basic NTFS permissions are *read*, *read+execute*, *write*, *modify*, (for folders only) *list folder contents*, and *full control*.

- **Read** means that users can open and read files, file attributes, subdirectories, and permissions, but not change them. (Careful: Read may convey “execute” permissions in some cases with script files.)
- **Read+execute** means that users can do everything allowed by the read permission, plus navigate across folders they do not have permissions to access in order to get to files or folders they do have permissions to access.
- **Write** means that users can modify files and subdirectories.
- **Modify** means that users can do everything allowed by the read+execute and write permissions, plus delete and change files.
- **List folder contents** means that users can, well, list folder contents. This permission applies only to folders.
- **Full control** means that users can do everything allowed by all the other permissions, plus take ownership of resources and change permissions.

View and set NTFS permissions in Windows Explorer by right-clicking the shared file or folder, clicking the Security tab, and making the relevant changes (see Figure 5). The procedure is similar to setting share permissions, but you do not have to share the file or folder first. The standard, or “shortcut,” permissions appear right away; a more granular set of detailed permissions is available by clicking the Advanced button.

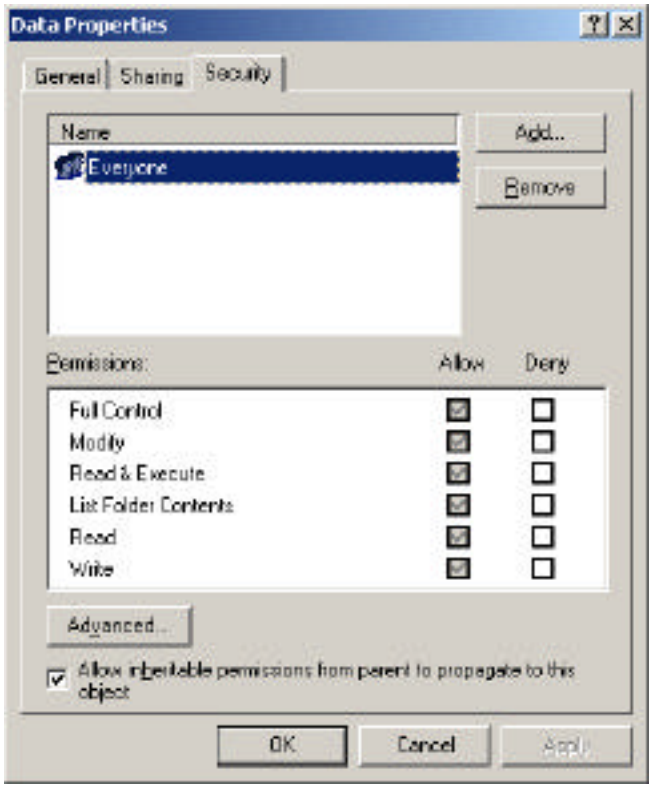


**Figure 5. NTFS permissions automatically inherit settings from the parent folder.**

## 3. Registry Permissions

The Registry is a shared resource in the sense that various applications on the machine use it, much like various users on a network use shared folders on a server. The operating system uses the Registry, too. So it makes sense that the Registry should use permissions, too, and it does.

You can assign Registry access controls on a key-by-key basis using REGEDT32.EXE, the NT-style Registry editor. (Windows 2003 Server and XP Professional offer a unified Registry editor, but you can still get to it by typing REGEDT32 in the Run dialog.) Choose Security > Permissions, and modify access controls in the ACL (Access Control List) editing window (see Figure 6). You should be cautious about using this technique to modify Registry permissions, but if a Registry permission restriction may be interfering with an application's ability to install or execute, this technique can help you find out. If you need to relax Registry access in order to install a program or driver, whenever feasible, re-secure the access control list once the software is happily installed. You can tighten Registry permissions domain-wide via security templates and Group Policy settings.

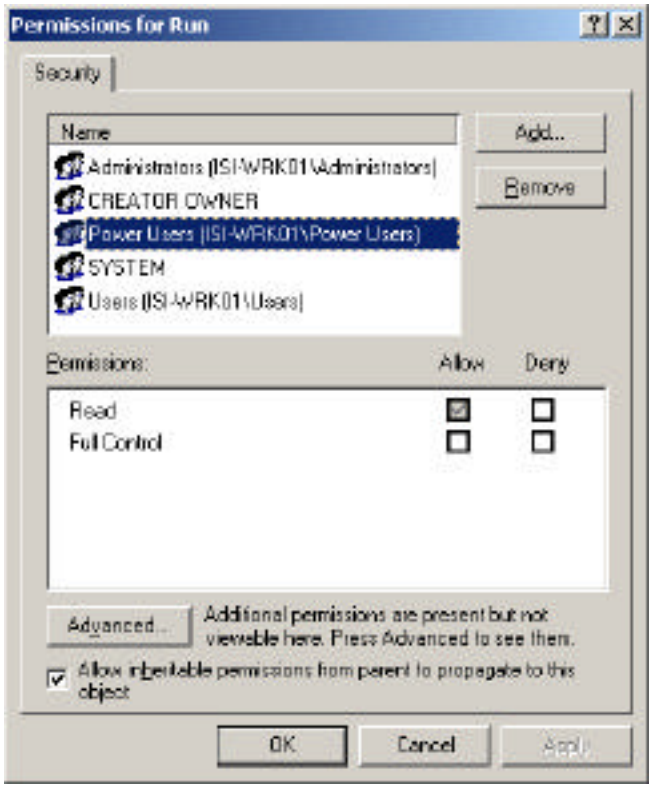


**Figure 6. Registry permissions have tightened up with more recent versions of Windows.**

## 4. Printer Permissions

You can assign permissions for local and networked printers in order to control access to those printers. The **Print** permission gives you the ability to print, pause, resume, cancel, and restart document print jobs that you own, that is, that you submitted with a print command. The **Manage**

**Documents** permission gives you the ability to modify jobs submitted by other users. The **Manage Printers** permission gives you the ability to have full administrative control of the printer, that is, stop it, start it, share it, and change its properties (such as driver software). Set these permissions on the Security tab of the printer's property page. Administrators and Power Users have all three printer permissions by default.

## E. Security for Stored Data

Windows 2003/2000/XP provides several mechanisms to increase the security of stored data residing on disks: *digital signatures and driver signing*, *Windows File Protection*, and (on NTFS volumes) *Encrypting File System (EFS)*.

### 1. Digital Signatures and Driver Signing

Microsoft brands a digital signature into the core operating system files and drivers that it ships with Windows. That way, Windows can "tell" when a program installation tries to replace one of those core files with a version not "signed" by Microsoft. Some shops believe that by requiring drivers to have a Microsoft signature, the probability of security breaches caused by buggy or malicious software is reduced.

Microsoft also brands a digital signature into files and drivers released subsequently that have passed testing at Windows Hardware Quality Labs (WHQL). Microsoft has stated that all files that appear on the Windows Update web site will be cryptographically signed.

You can set the behavior options on an individual PC via the System control panel's Hardware tab; click the Driver Signing button. You can also make this setting domain-wide via Group Policy. See *Unsigned driver installation behavior* and *Unsigned non-driver installation behavior* in the Group Policy utility under *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options*.

The three behaviors, which activate upon an attempt to install a new driver or software component, are as follows:

- **Ignore**: Unsigned drivers may load without notification.
- **Warn**: Unsigned drivers prompt a warning message to the user.
- **Fail**: Unsigned drivers may not install.

### 2. Windows File Protection

It has never really been possible to say with certainty what versions of important Windows system files (such as *.DLL and *.EXE files) are on a given PC.

- Application vendors have been allowed and even encouraged to package updates of Microsoft files for redistribution with their programs.
- Microsoft itself updates system files with some of its own applications.
- Starting with Windows 98, the Windows Update feature lets a user connect to the Internet at any time and perform system software updates.

This uncontrolled file-update frenzy has contributed to a lack of stability in Windows when running multiple applications. System files that were never tested together as a group find themselves trying to work together, sometimes successfully and sometimes unsuccessfully.

### *a. The Guardian Angel*

The Windows 2000/2003/XP approach is to run a file system "guardian angel" in the background, watching over system files (that is, the files that live in the system root folder and have the extensions DLL, EXE, FON, OCX, SYS, and TTF). When this guardian angel detects that a program has updated (or, in some cases, backdated!) one of these files, it tries to automatically restore the original version of the file, typically from the "hip pocket" folder *%systemroot%\SYSTEM32\DLLCACHE*. If the file is not in DLLCACHE or in the driver archive *%systemroot%\Driver Cache\I386\DRIVER.CAB*, then the guardian angel pops up a window asking you to supply the original installation media.

Here is an experiment you can try: Run Windows Explorer and rename NOTEPAD.EXE to NOTEPAD.SAV. If you try this trick on a machine with a small hard drive, you will probably see a message telling you to pop in the Windows CD so that the guardian angel can restore the proper NOTEPAD.EXE, which it thinks no longer exists in your *C:\WINNT* folder. If you try the trick on a machine with a large hard drive, then most likely you will not see any message, but if you take another look at the Explorer window, you will see that the operating system has quietly placed another copy of NOTEPAD.EXE into the system root folder from the *DLLCACHE* folder. (If neither of these things happens, then someone has disabled system file protection on your PC.)

### *b. Command-Line Utilities*

The automatic WFP daemon is fine, but you may run into occasions when you would like to perform a signature scan yourself. Two utilities are available for this purpose: SIGVERIF and SFC.

The SIGVERIF.EXE command-line utility, a.k.a. Signature Verification Tool, scans protected system files and verifies their digital signatures. The program creates the log file SIGVERIF.TXT to provide a record of the scan. You can use the program's advanced settings dialog box to scan non-system files, too.

Microsoft also provides a command-line program called SFC.EXE, for System File Checker. You can use SFC to scan system files for digital signatures and/or to rebuild the contents of the DLLCACHE folder if it becomes damaged – type **SFC /?** at a command prompt for more details. Note that SFC does not show you the file details that SIGVERIF does, and it does not let you scan non-system files. But SFC does offer to replace any system files for you.

## 3. Encrypting File System (EFS)

If you have a safe in your house, only those who know the combination can get to the valuables. Similarly, when mere access controls are not good enough, Windows 2003/2000/XP offer another level of protection for data sitting around on storage devices: *encryption*. This feature only exists on disks formatted with NTFS, and you access it in Windows Explorer via the file or folder's property sheet.

NTFS 5 brings *encryption* to the file system for the first time. (The acronym is *EFS*, for *Encrypted File System*.) EFS is a *public key encryption* method, meaning that a public key is used to encrypt a file and a private key is used to decrypt it. Windows handles the public and private keys automatically, behind the scenes; the encryption keys actually reside on disk as part of the encrypted file's header.

Encryption is a significant security enhancement, especially for portable computer users. Without logging on with the correct user name and password, you cannot access encrypted files, even if you remove the hard drive and put it into a different computer.

### *a. Procedure*

Encrypt a folder by right-clicking it in Windows Explorer, choosing Properties, clicking the Advanced button, and checking the Encrypt Contents to Secure Data box (see Figure 7). After you encrypt a folder, you can only have access to that folder and its contents when you log on with the same user account and password that you used when you encrypted the folder originally. You can even encrypt a folder that resides on a remote computer. Windows XP Professional extends the EFS capability by permitting the encryptor to designate other users who may also gain access to the encrypted files.

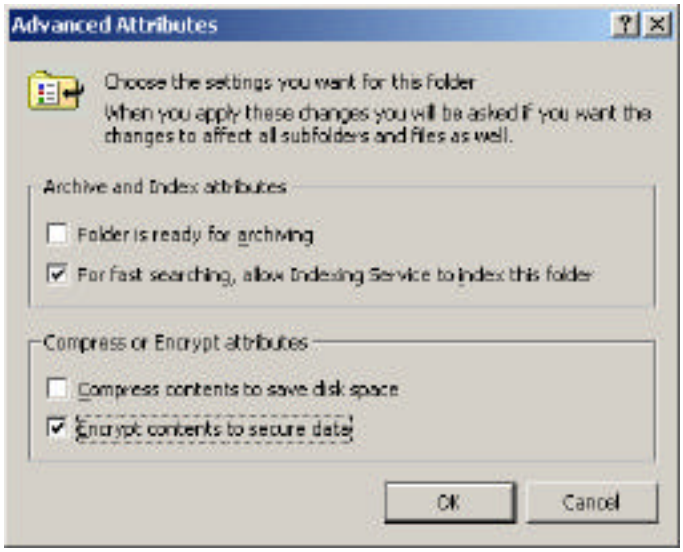


**Figure 7. You can compress or encrypt, but not both.**

Decrypting a file or folder is equally easy. Log on with the correct user account and clear the Encrypt Contents to Secure Data checkbox.

### *b. Core Facts*

- Encryption is only available with the NTFS file system.
- Encryption does not work with system files, such as PAGEFILE.SYS, for example.
- Encryption is incompatible with compression. A file or folder may be either compressed or encrypted, but not both at the same time.
- Standard EFS uses 56-bit encryption. You can get stronger, 128-bit encryption from Microsoft via the "Enhanced CryptoPak."
- When you encrypt a folder, you encrypt all the files in that folder; the folder itself is not really encrypted.
- A file stays encrypted if you rename it, move it, copy it, or back it up, *as long as the file stays on an NTFS disk.*
- Someone other than an encrypted file's owner can see the file, but gets an "access denied" error when attempting to open the file.
- You cannot share an encrypted folder.
- Encryption, like compression, is transparent. You do not have to explicitly descramble a file before you edit it and rescramble it when you are done editing it.
- The command-line utility for encryption is CIPHER.EXE.

### *c. Security Concerns*

Applications often create backup files, or temporary files, and you may wonder if they will also be encrypted if the original file on which they are based is encrypted. The answer is yes, according to Microsoft, as long as you encrypt the entire folder and the applications create such temporary or backup files within the same folder as the original data file. That is, if you open up SECRET.DOC in *C:\Personal\Letters*, which is an encrypted folder, and your word processor creates an "autosave" temporary file named ~SECRET.DOC in the same folder, then the temporary file is encrypted, just like the original file. On a related note, Microsoft promises that the encryption keys never show up in the pagefile.

In a network environment, administrators can use Windows *policies* to control the use of encryption. For example, an administrator could disable EFS for a domain, or for an organizational unit within a domain.

### *d. The Safety Net*

A user may forget an account password and have created encrypted files under that account. If that happens, the *recovery agent* has a private key that will unlock an encrypted file. By default, the recovery agent is the administrator of the local PC, or (if the PC is on a network) the domain administrator (more specifically, the first domain administrator of the first domain controller). You can specify additional recovery agents via Group Policy.

The recommended practice is to copy the encrypted file to the recovery agent's PC, where the recovery agent can decrypt the file simply by clearing the Encrypt Contents to Secure Data checkbox on the file's property sheet.

F. Security for Transmitted Data

Encryption may be fine for data that is sitting around, but you may want to protect files that *aren't* encrypted on disk when you decide to send those files across a communications link. Windows 2003/2000/XP offer a variety of methods to secure data in transit, including *IPSec* and *packet filtering*.

**1. IPSec**

IPSec is a set of software specifications designed to guarantee, through cryptographic methods, the authenticity and confidentiality of data in transit across IP networks. You can use IPSec for secure authentication (verifying that a computer is who it says it is), confidentiality (encrypting the entire data stream), or both.

You would consider using IPSec if you need to encrypt communications between Windows 2003-family computers, such as a workstation (or collection of workstations) and server, or if you need to encrypt communications between two Windows routers in a wide area network tunnel, such as a Virtual Private Network (VPN).

***a. Key Features***

Here are some of the key features of IPSec:

- IPSec operates at Layer 3 (Network) of the seven-layer OSI model. Because it runs at a relatively low layer and does not change the way Layer 3 interacts with higher layers in the modular networking stack, IPSec can provide security even for applications that are not aware of its existence. Any application that uses IP can enjoy the security benefits of IPSec. This is an advantage over Secure Sockets Layer (SSL), another cryptographic standard for transmitted data.
- IPSec works between workstations, between workstations and servers, and between servers. IPSec also works with LAN, WAN (router-to-router), and dial-up connections. IPSec is not, however, compatible with all network connectivity situations. For example, it does not work with NAT (Network Address Translation) or ICS (Internet Connection Sharing) – methods for sharing an Internet connection across a network.
- IPSec in Windows 2003/2000/XP permits configuration through Group Policy and Active Directory utilities. Support for policies reduces the administrative burden of deploying IPSec, because you can create settings that apply to Organizational Units, sites, or domains.
- Users do not have to be in the same domain to use IPSec.
- Simple routers do not need any special configuration to work with IPSec. Firewalls and other special-purpose routers may not be compatible with IPSec, but most simple traffic

routers can move IPSec packets around just like regular IP packets. The only computers that have to "understand" IPSec are the sending and receiving computers.

- The performance overhead of encrypting and decrypting packets is significant: the average packet size increases, network traffic increases, and CPU time increases. Having said that, companies such as Intel and 3Com have demonstrated that if IPSec acceleration code is built into the NIC, the performance penalty can be dramatically lower, and as much as four times less than in a software-only implementation.

### *b. IPSec and Policies*

You enable, configure, and edit IPSec parameters in Windows 2000/2003/XP with policies. Microsoft has provided several ways to do this:

- Run the Local Security Settings console in the Administrative Tools folder and click the node labeled IP Security Policies On Local Machine.
- Run the Local Group Policy tool (GPEDIT.MSC) and navigate to Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Local Machine.
- Run the Active Directory Users and Computers console and edit domain policies via the Group Policy tab of the domain (or OU) property sheet. In this case, navigate to *Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory* (see Figure 8).
- Run the Active Directory Sites and Services console, and edit the site policies (see location in previous bullet).
- Create your own custom Microsoft Management Console and add the IP Security Policy Management snap-in to it, or add the snap-in to an existing console.

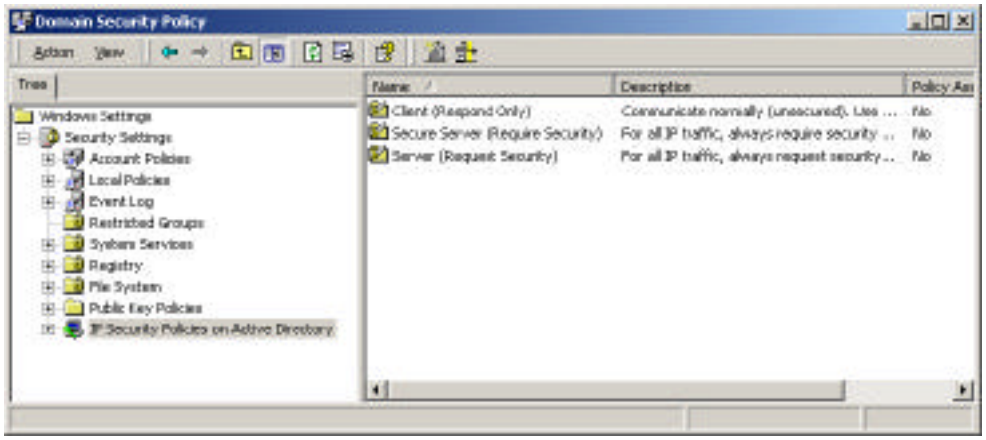


**Figure 8. Set IPSec options via Group Policy.**

All these methods present a user interface that is essentially the same, although the first two methods restrict you to configuring IPSec on the local computer. Note that you must have administrator rights on the system to enable and configure IPSec policies.

**2. Packet Filtering**

*Packet filtering* is a technique for restricting traffic or activating a security policy depending on a packet's source address, destination address, and/or traffic type. (The latter may be indicated by a TCP port number, UDP port number, or IP protocol number.) You can use packet filtering on NetWare (IPX packets), too.

The following steps demonstrate how to configure packet filtering on a Windows 2000/2003/XP machine running TCP/IP. This particular example is from a Windows 2000 Server system.

1. Right-click My Network Places and choose Properties.
2. Right-click Local Area Connection and choose Properties.
3. Double-click the listing for Internet Protocol (TCP/IP).
4. Click Advanced.
5. Click the Options tab.
6. Select TCP/IP Filtering in the list of optional settings and then click Properties.
7. Check the box labeled Enable TCP/IP Filtering (All Adapters) – see Figure 9.
8. Click the Permit Only radio button in the category you want to restrict. Your choices are TCP ports, UDP ports, and IP protocols. For example, TCP port 80 indicates Web traffic. UDP port 137 indicates WINS traffic.
9. Click Add and then enter a port or protocol number to permit. Windows 2000 filters out any ports or protocols other than the ones you expressly permit.
10. Repeat Step 9 as necessary.
11. Click OK to close out of the various dialog boxes.

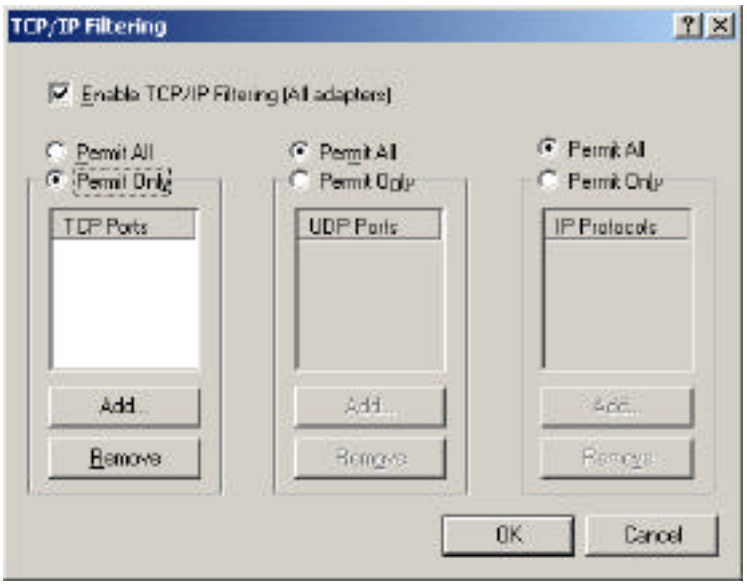


**Figure 9. Configuring TCP/IP packet filtering**

It is possible that packet filtering can have unintended consequences, especially if you choose to operate on a "permit only" basis. The most notorious example is that you can disable the PING command (essential for troubleshooting TCP/IP problems) if you permit only FTP or Web traffic and do not also explicitly permit ICMP traffic.

The best-known application for packet filtering is in *firewalls* (computers that manage connections between a private, internal network and the public Internet), but you can also put packet filtering to use on a purely private internal network that does not connect to the Internet. In fact, packet filtering is a key element of Microsoft's IPSec technology.

## 3. Wired Equivalent Privacy

The increasing use of wireless networking products is sure to continue, as speeds go up and costs go down. Wireless network cards are about 20% of their cost a mere two years ago, and access points have come down nearly as much.

As companies put more data into the air, where eavesdropping is physically far easier than when data travels in the confines of a copper wire (and the electromagnetic field surrounding it), concerns over protecting that data-in-transit have grown. Wireless has spawned a new hacking/cracking methodology: driving around business and residential neighborhoods in a "white van" and trying to pick up wireless signals.

*Wired Equivalent Privacy*, known as *WEP*, arises from the IEEE standards for wireless networks (802.11b) and encrypts the data flow between the wireless client and access point. The University of California at Berkeley found that WEP has several significant security holes, so should not be used on its own, but rather in conjunction with the other types of security covered in this paper – logon security, rights, permissions, file system security, registry security, and so on.

In particular, be aware that once the data enters the access point, it is decrypted and sent from that point forward (over wires) in an unencrypted form. WEP only covers the time that the data is "in the air." Also be aware that so-called "WEP2" implementations use a more secure key (128 bits) than WEP (40 or 64 bits). Another way to improve WEP security is to change the shared secret keys, which are configured manually, on a regular and frequent basis; some proprietary extensions to WEP provide for automated key management, which makes life significantly more difficult for would-be intruders.

## G. Local and Group Policy

Policies are really more of a mechanism for implementing and controlling the various other types of Windows 2003/2000/XP security than a new type of security themselves. You can think of policies as the “rules of the house” that set forth all the security restrictions you have chosen to implement from the areas discussed so far.

Policies do not have to apply to security concerns alone; they also have a role in ensuring the consistency of the user interface from one system to another. But even if your only interest is security, policies provide a powerful set of tools.

Policies work differently depending on whether you are running a stand-alone machine, a computer in a pure (“native”) Windows 2000/2003 network, or a computer in a “mixed-mode” network with NT 4.0 clients and servers. However, although the details vary, the concept is basically the same: After an Administrator sets them, policies automatically modify the Registry at boot time, logon time, and periodic refresh intervals.

- The Local Group Policy utility, GPEDIT.MSC, runs on a Windows 2000/XP Professional workstation. You can use this tool to set policies for the local machine only.
- The Local Security Policy console (in the Administrative Tools folder) presents a subset of policies from GPEDIT.MSC that pertain to security for the local workstation.
- You set network Group Policy via various Active Directory administrative tools on a Windows 2000 Server machine. For example, you can run Active Directory Users and Computers, right-click a domain controller or OU, choose Properties, and click the Group Policy tab.
- The Domain Security Policy console (in the Administrative Tools folder of a server) presents a subset of policies that pertain to security for the domain.
- The new Group Policy Management Console, or GPMC, provides a “one-stop shop” for policy management and is freely downloadable from Microsoft. This tool requires Windows 2003 Server or Windows XP Professional to run, however.

*Important Note for Mixed-Mode Networks:* Windows 2003/2000 Group Policy does not provide client support for Windows NT 4.0 and 9x machines. Policy support for Windows NT 4.0 clients has to be provided using Windows NT 4.0 administrative templates (.ADM files) and NT 4.0 System Policy Editor files, while Windows 9x clients will need to be managed with the System Policy Editor.

### 1. Hierarchical Structure

The best thing about Group Policy is that it applies across your network’s hierarchical structure. In Active Directory, an enterprise network has different levels, as follows:

- Forests

- Sites
- Trees
- Domains
- Organizational Units

Any Group Policy setting that exists at a higher level in the hierarchy will take precedence over any Group Policy setting at a lower level. In practice, what this usually means is that network administrators set Group Policy at a domain level and make exceptions as necessary for particular users on their local workstations. The actual priority, from top to bottom, is OU, domain, site, and local PC; the chronological sequencing of policy processing is the exact reverse.

Note that if a policy setting conflicts with a *user right* that a user would normally have, the policy setting takes precedence.

**2. Local Security Policy and Domain Security Policy**

You do not have to wade through the complete set of Group Policies if your primary interest is security. Windows provides the Local Security Policy console in the Administrative Tools folder of a workstation machine, and the Domain Security Policy console in the Administrative Tools folder of a server, to enable you to work only with security-related policies.

If you want to see for yourself how the Local Security Policy console is simply a subset of the entire set of policies, open GPEDIT.MSC via the Start > Run dialog box, and navigate to *\Local Computer Policy\Computer Configuration\Windows Settings\Security Settings*. Now, open the Local Security Policy console via Administrative Tools > Local Security Policy. See how the windows match up?

**3. Security Templates**

Microsoft knows that many network administrators have other things to do with their time than painstakingly set dozens or even hundreds of individual policies to achieve a proper level of security and consistency from PC to PC. So, the company has provided a way to set a whole bunch of policies in one fell swoop – and a whole bunch of file system and Registry access permissions, too. That mechanism is the *security template*.

Security templates preconfigured for you by Microsoft have the suffix INF and live in *%systemroot%\security\templates*. (Your organization may have one or more custom templates that may reside in other locations.) You can apply a security template to a stand-alone PC, or to a domain or organizational unit (via the Import Policy command on the context menu of the object's Security Settings node). The National Security Agency makes additional templates available at *www.nsa.gov*.

You have to build a custom Microsoft Management Console to view and edit (but not apply!) the prebuilt security templates. The technique is to run MMC.EXE and add the Security Templates snap-in (see Figure 10). This method is a whole lot easier than studying the INF files in a text editor.

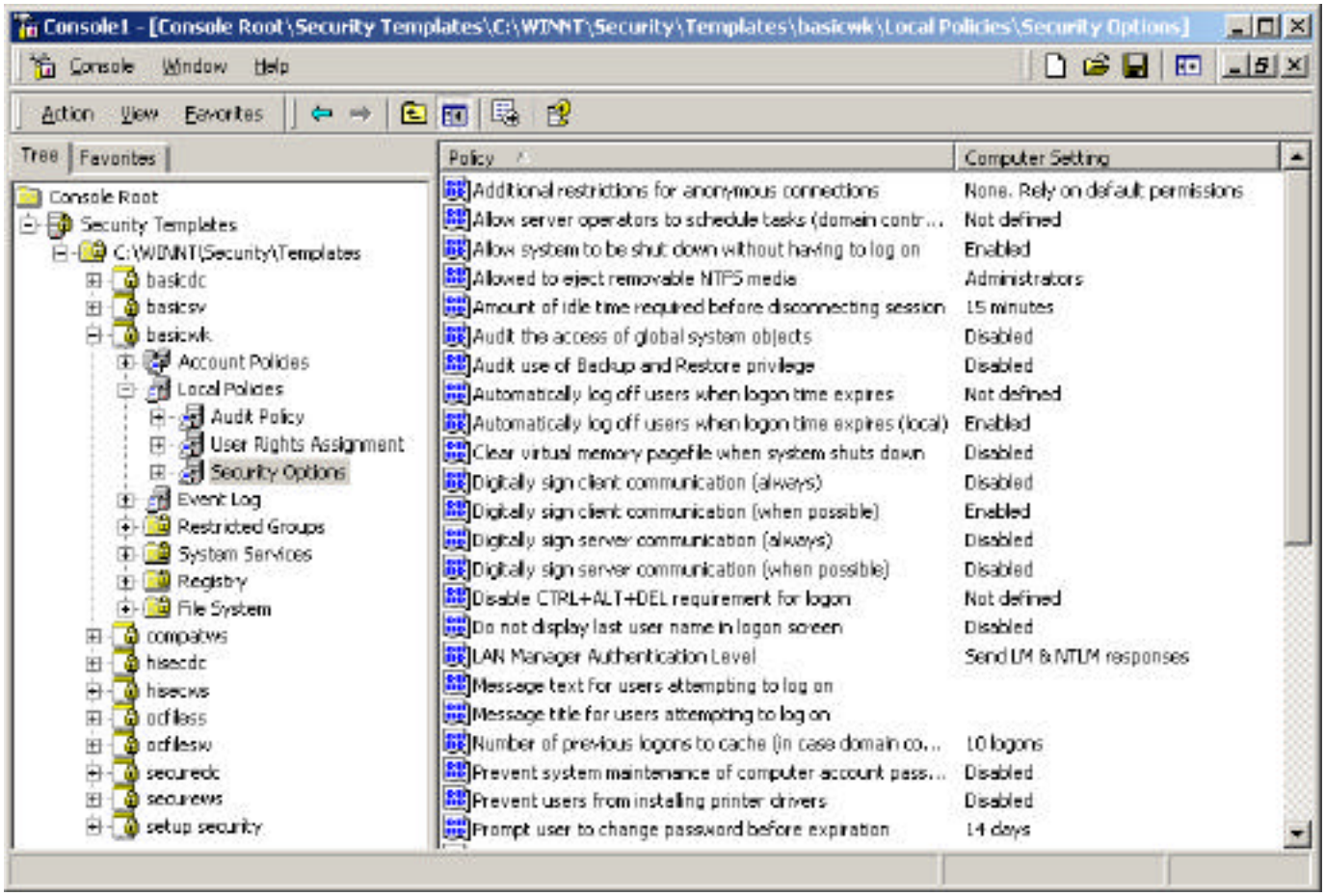


**Figure 10. View INF file contents in an organized way with the Security Templates snap-in.**

The prebuilt templates include the following:

- **BASICDC** is a “regular” domain controller.
- **BASICSV** is a “regular” server.
- **BASICWK** is a “regular” workstation.
- **COMPATWS** is a special workstation template that eases access controls for the Users group, providing compatibility with applications designed for Windows NT.
- **HISECDC** is a maximum-security domain controller.
- **HISECWS** is a maximum-security workstation.
- **SECUREDC** is a high-security domain controller.

- **SECUREWS** is a high-security workstation.

You can interactively *apply* a template to a computer using the Security Configuration and Analysis console snap-in, as the next section describes.

### 4. Security Configuration and Analysis

The Security Configuration and Analysis console snap-in does two things. It lets you compare a machine's present setup against a specific security template. It also lets you apply a template to a local PC, or to a Group Policy object such as a domain or organizational unit.

First, you have to build the console. Run MMC.EXE and add the Security Configuration and Analysis snap-in (use the Console > Add/Remove Snap-In command). Then, save your console so that you do not have to rebuild it again.

If you want to compare a given PC's present security setup versus that specified by a particular security template, right-click the Security Configuration and Analysis node in the left window and choose Open Database. (If the database is new, Windows asks you to name which security template you want to load into the database. For example, if you want to compare your PC against the "compatible workstation" template, select COMPATWS.) To perform the analysis, simply right-click Security Configuration and Analysis, and choose Analyze Computer Now.

Navigate the details pane (on the right) and note the green check marks and red X marks (Figure 11). The green check marks mean that your PC's setting matches the one in the database; the red X marks mean that your PC's setting is less secure than the one in the database.

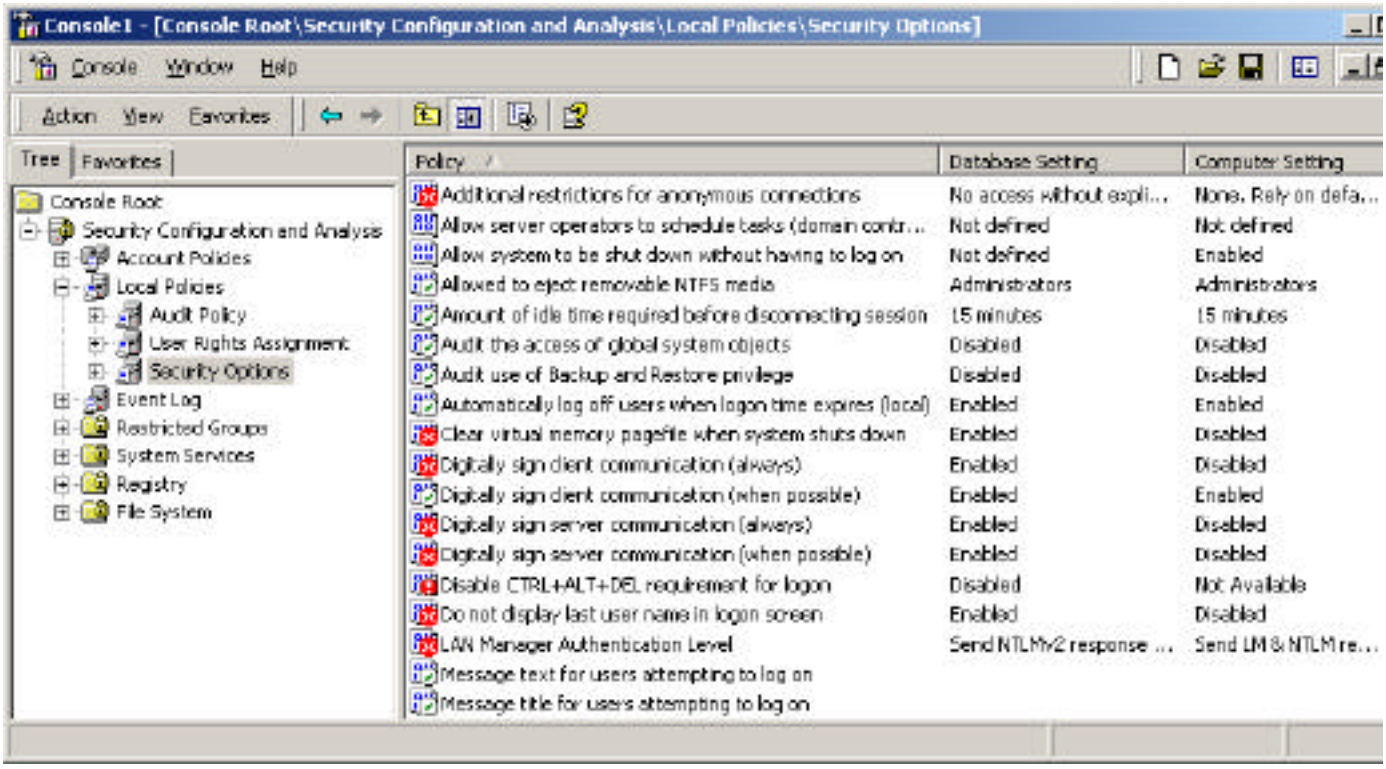


**Figure 11. Analyzing a specific computer with respect to a specific security template.**

Many more ways exist of using Group Policy to enhance security. For example, you can use Registry-based policy (“Administrative Templates”) to lock down user desktops, so that they cannot perform actions on their local PC or on the network that a) they should not ever need to perform and b) could compromise system security. You can also use Group Policy to restrict the applications that users can run, control whether users can take network data “offline,” and manage the distribution of security-related software, such as antivirus updates.

## H. Auditing

*Auditing* is keeping track of events that may reflect on system security. Think of auditing like a security camera pointing at your front door: The camera itself does not present any physical impediment to entry, but it creates a recorded document that you can use later on to prove a security breach.

Windows 2003/2000/XP's "videotapes" are the *event logs* that reside by default in the folder *%systemroot%\system32\config* and have the suffix EVT. You view these with the Event Viewer, one of Windows' administrative tools, accessible from the Computer Management console (COMPMGMT.MSC).

You can activate various types of auditing, but two of particular interest are *logon auditing* and *object auditing*, described in the following sections.

### 1. Logon Auditing

Windows can monitor logons, both successful and unsuccessful, and record them in the Security event log. You would use logon auditing to discover if and when a cracker is trying to break into a PC by guessing account names and passwords, or why a company employee is logging on to his system at unusual hours.

Here is how to activate logon auditing on a particular machine:

1. In the Administrative Tools menu, double-click Local Security Policy.
2. In the tree pane to the left, expand Local Policies.
3. In the tree pane, click Audit Policy. All the various quantities that you can audit now appear in the details pane to the right.
4. In the details pane, double-click Audit Logon Events.
5. In the ensuing dialog box, if you are interested in logging failed attempts, which would be typical of intruder detection, click Failure; if you are interested in unusual behavior by an authorized employee, click Success.
6. Click OK and close the Local Security Policy console.
7. Restart the machine.

Once you have gone through the above steps, watch the Security log in the Event Viewer. (You must be an Administrator to access this log.)

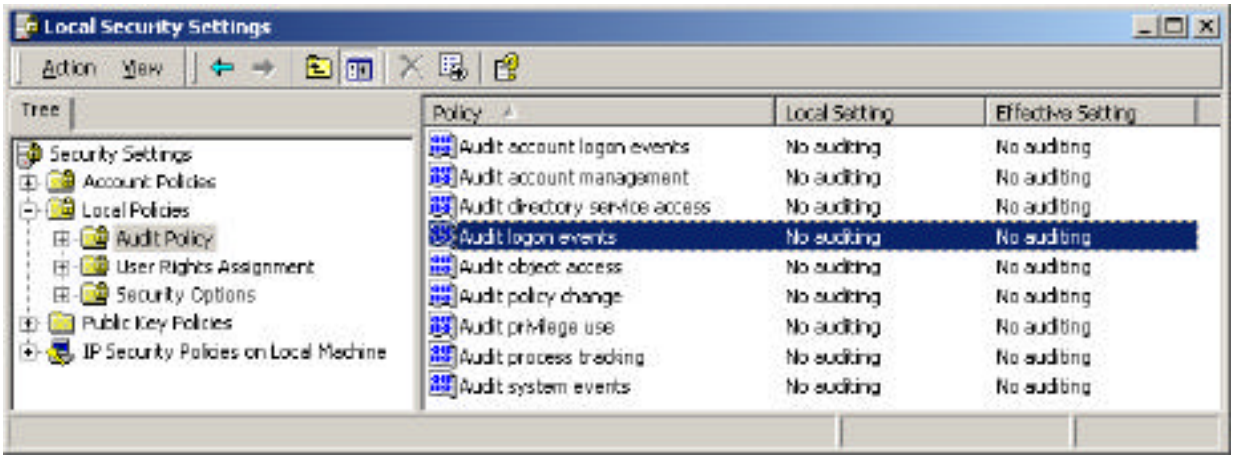


**Figure 12. Setting up to audit logon events.**

- To track domain logon events – that is, actual or foiled logons to a domain controller – then double-click Audit Account Logon Events instead of Audit Logon Events in step #4 above.

## 2. Object Auditing

Beyond auditing logon events, Windows 2000 can also monitor successful and unsuccessful accesses to objects – namely files, folders, the Registry, and printers – and record those accesses into the Security event log. The details that Windows records are as follows:

- What was done to or with the object
- Who did it
- When it was done
- Whether the action succeeded or failed

Auditing failed object accesses is handy if you believe that someone who is able to log on successfully is, intentionally or unintentionally, damaging or deleting files or interfering with the Registry. Auditing successful object accesses is one method of performing capacity and performance analysis.

The procedure for enabling object auditing is very similar to the procedure for enabling logon auditing (see previous section); the only difference is that you would choose “Audit object access” instead of “Audit logon events” in the Local Security Policy console.

After you have enabled object auditing, you must take an extra step and tell Windows which particular objects you want to audit.

- On an NTFS disk, you would open Windows Explorer, right-click the file or folder to audit, choose Properties, click the Security tab, click the Advanced button, and finally click the Auditing tab. From the Auditing tab, click the Add button and specify whose actions you want to audit. When Windows displays the Auditing Entry dialog box, you would then

choose what actions you want to audit, by checking the appropriate box or boxes (Delete, Traverse Folder, Change Permissions, and so on).

- For the Registry, you would open REGEDT32, navigate to the Registry key that you want to audit, click it, and choose Security > Permissions. Click the Advanced button and click the Auditing tab. The rest of the procedure is very similar to the previous bullet, although the actions are somewhat different because you are dealing with a Registry key, not a file or folder.

Do not forget to turn object auditing off when you no longer need it, either by reversing the actions described in the bullets above, or by modifying the Local Security Policy console settings to disable auditing for all objects. Auditing, particularly when successful operations are specified, can add dramatically to system overhead.

## ABOUT THE AUTHOR

Glenn Weadock, MCSE, A+, is president of Independent Software, Inc. (*www.i-sw.com*), a Colorado-based consulting firm he founded in 1982 after graduating from Stanford University's engineering school. ISI's client list includes the US Department of Justice, Ernst & Young LLC, and Lucent Technologies, among dozens of other firms both large and small. Through ISI, Glenn has taught Windows to thousands of students in the United States, United Kingdom, Canada, and Southeast Asia in more than 250 seminars since 1988.

Glenn is also the author of twenty published books for publishers such as McGraw-Hill, Sybex, IDG and Wiley, including *MCSE Windows XP Professional For Dummies* and *MCSE Windows 2000 Network Infrastructure For Dummies*. He presently teaches Windows 2003 Server, Windows XP, Windows 2000, Active Directory, and Group Policy for Global Knowledge.