Computer Security and Windows 2000

Glenn Weadock

mightywords™

Computer Security and Windows 2000

By Glenn Weadock

Published by MightyWords, Inc.
2550 Walsh Avenue
Santa Clara, CA 95051
www.mightywords.com

ISBN 0-7173-0427-2

Table of Contents

Executive Summary

Windows 2000 and its predecessor, Windows NT, have become known for two main features: reliability and security. (The “home” versions of Windows, 95, 98, and ME are known on the other hand for their ability to run just about any device or program.) The problem is that Windows 2000 security has so many different components that just getting a handle on them all can be a major conceptual challenge. This briefing lays out the main security features in Windows 2000 and puts them all into a “big picture” context.

Windows 2000 costs more than Windows 95, 98, or ME, but it offers security features that those other operating systems lack. Most individuals and organizations that pay the extra money for Windows 2000 want to maximize their return on investment by employing the various security features that the operating system offers. The number and variety of threats to computer security is increasing daily, and the cost of lost, damaged, or compromised data can be very large.

This article is for any person who must plan, implement, manage, or administer Windows 2000 security for networked desktop computers, notebook computers, or stand-alone systems.

Chapter 1

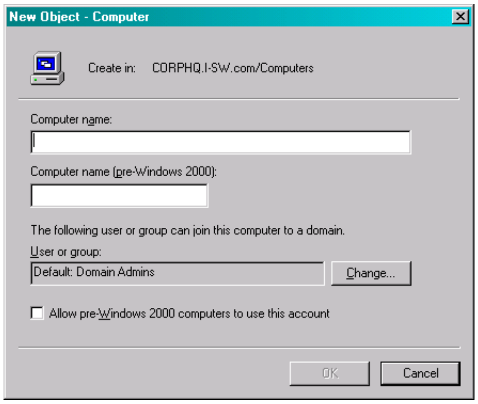
Pre-Logon Security: Computer Accounts

The first category of Windows 2000 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 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* (one of this article’s main topics). (Windows 95 and 98 do not have computer accounts.)

I 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 Windows 2000 Professional in a networked environment, you must do one of two things: Create a computer account for the PC ahead of time, or, during the installation, provide (when prompted) the user name and password of a user with authority to create a computer account on the domain.

If you choose to create the computer account ahead of time, do so on a domain controller via the Active Directory Users and Computers console (in the Administrative Tools folder). Right-click the Computers icon in the left windowpane, and choose New➔Computer. Then, fill in the fields in the New Object–Computer dialog box (see **Figure 1**).



New Object - Computer

Create in: CORPHQ.I-SW.com/Computers

Computer name:

Computer name (pre-Windows 2000):

The following user or group can join this computer to a domain.

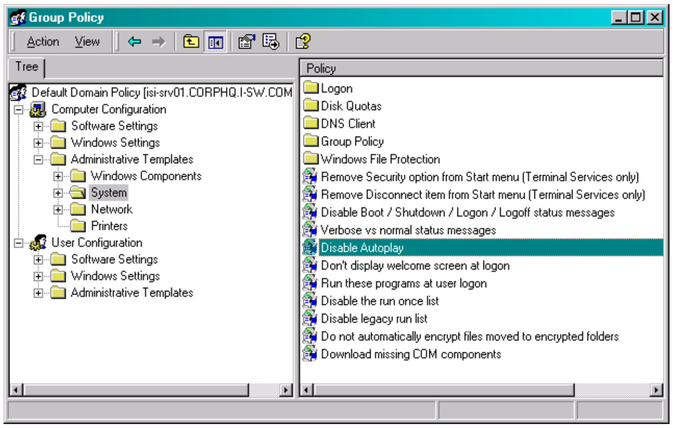
User or group: Default: Domain Admins

☐ Allow pre-Windows 2000 computers to use this account

Figure 1: Creating a new computer object in Active Directory.

Computer names should be 15 characters or less. In a TCP/IP environment, they should not contain any special characters other than the hyphen (“-’’).

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 of interest, and choose Properties. Click the Group Policy tab and double-click the entry for 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-ROM’s from running automatically after being inserted into the drive (see **Figure 2**).



- Default Domain Policy [isi-srv01.CORPHQ.I-SW.COM
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
      - System
      - Network
      - Printers
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Logon
Disk Quotas
DNS Client
Group Policy
Windows File Protection
Remove Security option from Start menu (Terminal Services only)
Remove Disconnect item from Start menu (Terminal Services only)
Disable Boot / Shutdown / Logon / Logoff status messages
Verbose vs normal status messages
Disable Autoplay
Don't display welcome screen at logon
Run these programs at user logon
Disable the run once list
Disable legacy run list
Do not automatically encrypt files moved to encrypted folders
Download missing COM components

Figure 2: Computer accounts let you make settings regardless of who logs on.

Chapter 2

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 lets you configure. The default behavior for Windows 2000 is to require a user name and password before you can log on. (You can change that behavior for a stand-alone Windows 2000 PC, but think twice before you do.)

Windows 2000 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).

You can think of logon security and user authentication as a locked front door on your house, with a peephole to identify visitors.

User Names

Every Windows 2000 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.

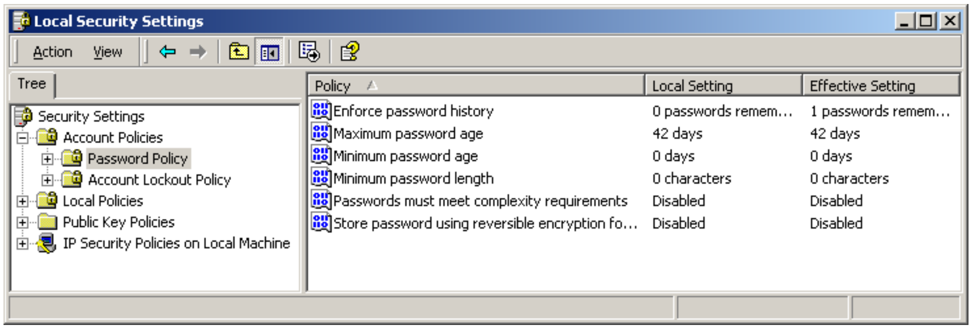
- A user name must be unique among all other user names and group names in the domain or workgroup.
- A user name cannot exceed 20 characters in length.

Passwords and Password Policies

Logon security depends on passwords. The problem with passwords is they are too easily guessed or not complex enough to foil crackers.

On a networked computer, you can apply some policies to enforce better passwords and better password maintenance. View account policies for the local workstation in the Local Security Policy console (it is in the Administrative Tools control panel folder). Change an account policy by double-clicking it and modifying its value (see **Figure 3**).

If the same policy exists at the domain level, the domain policy overrides the local policy. So, you can set password policies at a domain controller and they will apply to every member of the domain. The command is Start➔Programs➔Administrative Tools➔Domain Security Policy.



Policy	Local Setting	Effective Setting
Enforce password history	0 passwords remem...	1 passwords remem...
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet complexity requirements	Disabled	Disabled
Store password using reversible encryption fo...	Disabled	Disabled

Figure 3: Password policies let you strengthen logon security.

The password policies mean:

- **Enforce password history.** How many new passwords the user must specify before Windows allows her to reuse an old one.
- **Maximum password age.** How long Windows 2000 lets you keep the same password before making you change it. This value is in days, and the default is 42. A value of zero means the password does not ever expire.
- **Minimum password age.** How many days a user must keep a password before changing it. Zero means you can change a password at any time, which defeats the "Enforce password history" setting.

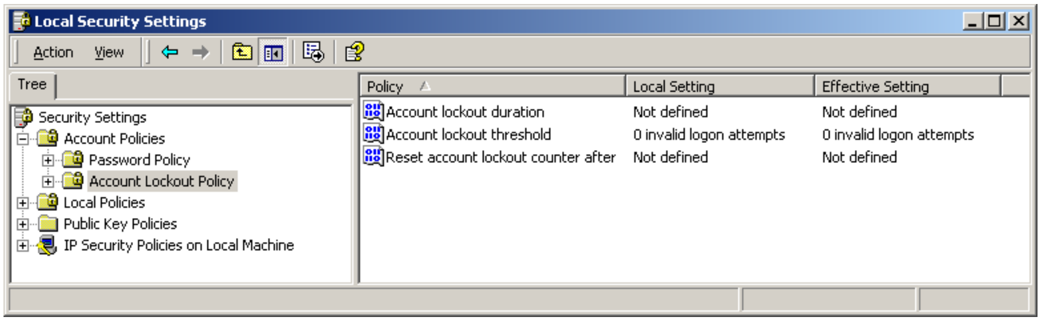
- **Minimum password length.** The range is 0 to 14 characters; 0 means no password is required for the account (not a good plan!). Active Directory, when initially set up, defaults to zero.
- **Passwords must meet complexity requirements.** This option makes the user include numbers or punctuation marks in the password, and forbids including the user's account name or full name (if defined).
- **Store password using reversible encryption for all users in the domain.** Choose this only if you want to set up your network to use *digest authentication*, which prevents browsers from sending Windows user names and passwords to intranet servers in clear text. If you do this, you must also make a few settings in Active Directory; see the term *digest authentication* in Windows 2000 Server help for more details.

The above policies apply to all local user accounts on the computer. For example, you cannot set one account to have a different minimum password length than another account.

Account Lockout

Account lockout policies help frustrate intruders who repeatedly (see **Figure 4**) try to log on to your PC. These policies, which you also view in the Local Security Policy console of a Windows 2000 Professional workstation (or in the Domain Security Policy console of a Windows 2000 Server domain controller), are as follows:

- **Account lockout duration.** How many minutes Windows 2000 locks out a user after the user makes X number of invalid logon attempts. A value of zero means "until an Administrator clears the account."
- **Account lockout threshold.** How many invalid logon attempts trigger the lockout, at which point Windows will not let the user try any more until the account lockout duration period has passed. The range is 0 to 999.
- **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. The range is 1 to 99,999 minutes.



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Public Key Policies
  - IP Security Policies on Local Machine

Policy	Local Setting	Effective Setting
Account lockout duration	Not defined	Not defined
Account lockout threshold	0 invalid logon attempts	0 invalid logon attempts
Reset account lockout counter after	Not defined	Not defined

Figure 4: Account lockout settings help deter potential intruders.

The RunAs Service

What if you are running Windows 2000 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. 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 nifty capability to run any program, not just REGEDT32 and REGEDIT.

Windows 2000 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.

Also note that you can RunAs to see how a program would behave for a “regular” user, if you happen to be logged on already as an Administrator. That is, you can use RunAs to temporarily give yourself fewer rights on the system as well as more rights.

Locking the System

Because logon security is such an important element of Windows 2000 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. Simply press Ctrl+Alt+Del to display the Windows Security dialog box, and click the Lock Computer button. 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.

Existing programs continue to run while the computer is locked. For example, if you are performing a download, disk defragment operation, etc., the operation continues after you lock the computer. 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.

Chapter 3

User and Group Rights

In the Windows 2000 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.

Windows 2000 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 2000 Professional system.)

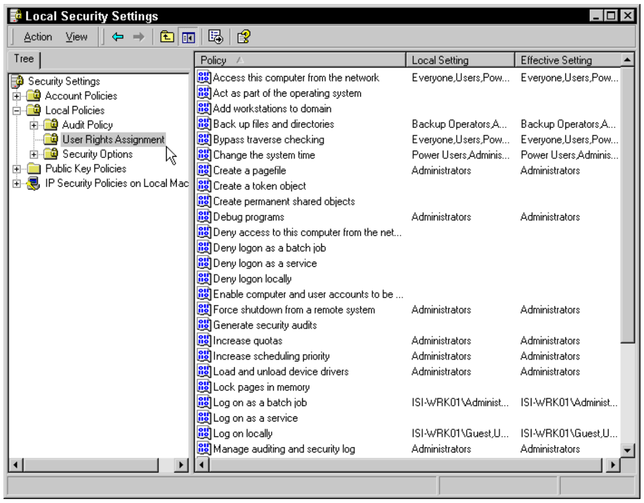
To make life easier, Microsoft endows Windows 2000 with various *built-in* user and group accounts. You have the flexibility to create new users and groups, with a customized set of rights; but on a small to medium-size network, you may find that the built-in accounts provide all the security options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

The rest of this section deals with the built-in user and group accounts. I have divided them further by *local* versus *domain* accounts, as follows:

- **Local Accounts:** Exist in the local security database only, and allow access to local resources. A stand-alone Windows 2000 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 Professional computer would normally use a domain account for everyday work, for security, centralized administration, and access to domain-based resources.

It used to be that *all* user and group rights lived in the Registry, in the SAM (Security Accounts Manager). They still live there for “local” users and groups, that is, those defined on the logon machine; but user and group rights on a Windows 2000 network now live in the Active Directory database rather than the Registry.

Check out the details of which rights go with which local groups by choosing Start→Settings→Control Panel→Administrative Tools→Local Security Policy, and opening the node *Security Settings\Local Policies\User Rights Assignment* (see **Figure 5**).

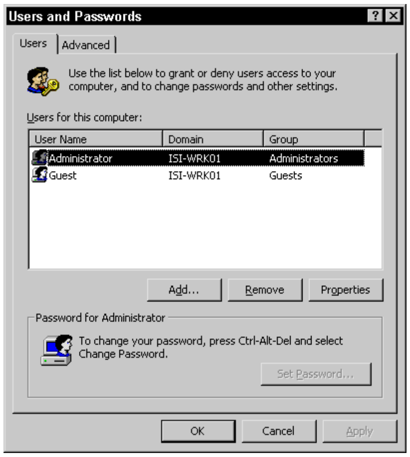


Policy	Local Setting	Effective Setting
Access this computer from the network	Everyone,Users,Pow...	Everyone,Users,Pow...
Act as part of the operating system		
Add workstations to domain		
Back up files and directories	Backup Operators,A...	Backup Operators,A...
Bypass traverse checking	Everyone,Users,Pow...	Everyone,Users,Pow...
Change the system time	Power Users,Adminis...	Power Users,Adminis...
Create a pagefile	Administrators	Administrators
Create a token object		
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from the net...		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user accounts to be ...		
Force shutdown from a remote system	Administrators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		
Log on as a batch job	ISI-WRK01\Administ...	ISI-WRK01\Administ...
Log on as a service		
Log on locally	ISI-WRK01\Guest,U...	ISI-WRK01\Guest,U...
Manage auditing and security log	Administrators	Administrators

Figure 5: Checking out user rights for various built-in groups.

Built-In Local User Accounts

Windows 2000 Professional comes with two built-in local user accounts: Administrator and Guest. (You can see these accounts via the Users and Passwords control panel. See **Figure 6**.)



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	ISI-WRK01	Administrators
Guest	ISI-WRK01	Guests

Password for Administrator

To change your password, press Ctrl-Alt-Del and select Change Password.

Figure 6: Log on as an Administrator to use 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.

Built-In Local Groups

Windows 2000 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 Professional computers and on Windows 2000 Server computers that do not function as domain controllers. These are:

- Administrators
- Backup operators
- Guests
- Users
- Power users (the default assignment for newly created users)
- Replicators

And now for some details on each group:

Administrators

- This group includes the built-in local Administrator user account.
- Membership means you can do 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 2000 applications.
- Members may not have sufficient rights to run Windows NT applications.

- Cannot create local printers.
- Cannot modify any system wide 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 2000 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.

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. (Chapter 7 of this article 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. 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 administrable centrally.

Built-In Domain User Accounts

In the Windows 2000 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.)

Built-In Domain Groups

Domain groups, like domain user accounts, live in the Active Directory database on a Windows 2000 domain controller. The precise list of built-in domain groups on a Windows 2000 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 Server help system and in the Windows 2000 Server Resource Kit (both print and on-line versions).

System Groups

Windows 2000 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.)

Chapter 4

Object Permissions

Windows 2000 includes several types of 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 andgroups can access that object.

Windows 2000 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 2000, 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 in Windows 2000 are as follows:

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

The following sections explain each type.

Share Permissions

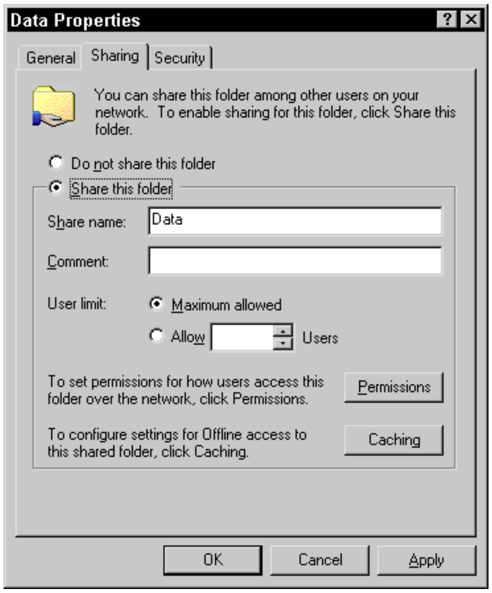
When you share a resource (typically, a file folder) for use by other computer users, you can specify which users and groups you want to have access to that resource, and how much access you want them to have.

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 7**). Get to the Sharing dialog box by right-clicking the shared folder or drive and clicking the Sharing menu choice. (To share a folder, you must have the File and Printer Sharing for Microsoft Networks service installed for your network connection.) You can grant access based on user names and group memberships.



You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Data

Comment:

User limit: ● Maximum allowed

○ Allow Users

To set permissions for how users access this folder over the network, click Permissions. Permissions

To configure settings for Offline access to this shared folder, click Caching. Caching

Figure 7: 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 disc devices.

- Share permissions are the only way you can restrict network user access to a FAT or FAT32 disk drive.

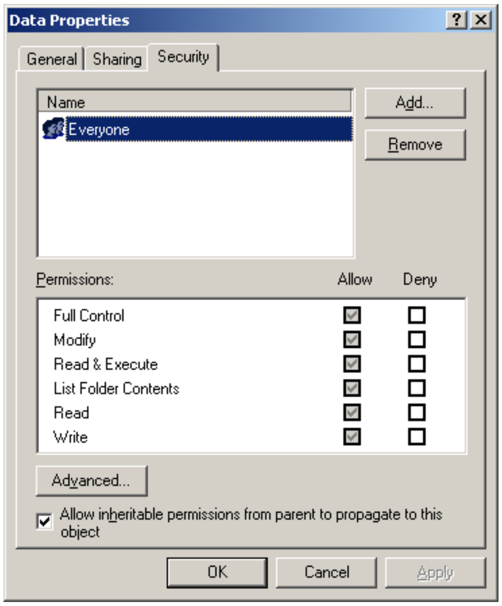
File and Folder (NTFS) Permissions

If you format a disk using the NT File System, or NTFS (now in Version 5 for Windows 2000), 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.
- **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 8**). The procedure is similar to setting share permissions, but you do not have to share the file or folder first.



Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

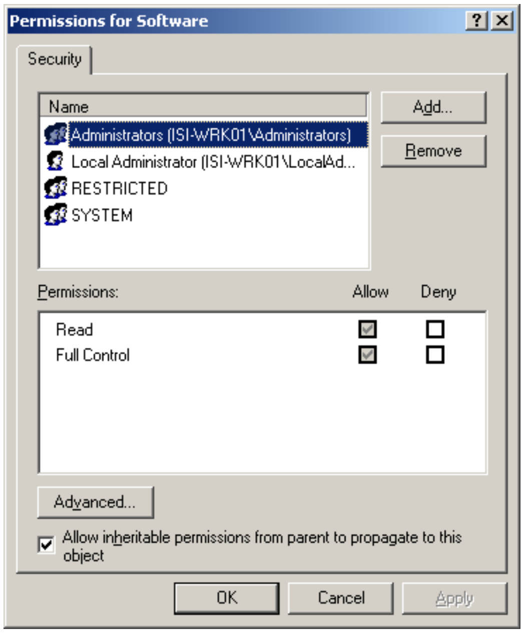
☑ Allow inheritable permissions from parent to propagate to this object

Figure 8: NTFS permissions automatically inherit settings from the parent folder.

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. 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 (see **Figure 9**). Choose Security➔ Permissions, and modify access controls in the ACL (Access Control List) editing window. 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 execute, this technique can help you find out.



Name
- Administrators (ISI-WRK01\Administrators)
- Local Administrator (ISI-WRK01\LocalAd...
- RESTRICTED
- SYSTEM

Permissions:	Allow	Deny
Read	☑	□
Full Control	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

Figure 8: You must use REGEDT32, not REGEDIT, to view or modify Registry permissions.

Printer Permissions

You can assign permissions for local and networked printers in order to control access to those printers. Here are a few details:

- 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.

Set these permissions on the Security tab of the printer's property page. Administrators and Power Users have all three printer permissions by default.

Chapter 5

Security for Stored Data

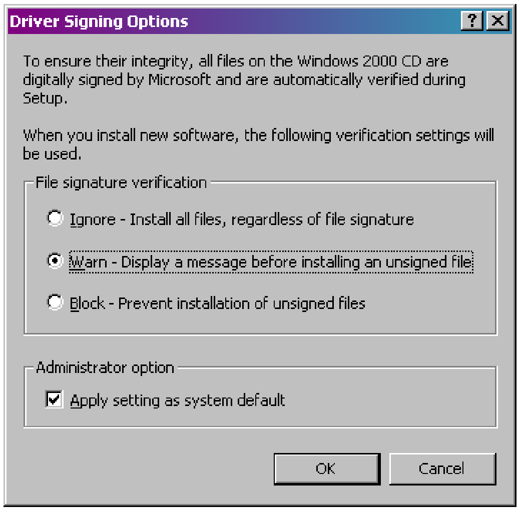
Windows 2000 provides several mechanisms to increase the security of stored data residing on disks: *digital signatures and driver signing*, *Windows File Protection*, and (on NTFS volumes) a new feature, *Encrypting File System (EFS)*.

Digital Signatures and Driver Signing

Microsoft brands a digital signature into the core operating system files and drivers that it ships with Windows 2000. That way, Windows 2000 can “tell” when a program installation tries to replace one of those core files with a version not “signed” by Microsoft.

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 (see **Figure 10**). If you have administrative privileges on the machine, you can make one setting the default for all users who log on to the PC.



Driver Signing Options

To ensure their integrity, all files on the Windows 2000 CD are digitally signed by Microsoft and are automatically verified during Setup.

When you install new software, the following verification settings will be used.

File signature verification

○ Ignore - Install all files, regardless of file signature

● Warn - Display a message before installing an unsigned file

○ Block - Prevent installation of unsigned files

Administrator option

☑ Apply setting as system default

Figure 10: Setting driver-signing options on a single PC.

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.

The Registry contains settings that govern how Windows 2000 behaves with respect to driver signing: *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*.

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.
- With Windows 98 (and now Windows 2000), 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.

The Guardian Angel

The Windows 2000 approach is to run a file system *guardian angel* in the background, watching over system files (that is, the files that come with Windows 2000 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 *C:\WINNT\SYSTEM32\DLLCACHE*. If the file is not in DLLCACHE, or in the driver archive *C:\WINNT\Driver Cache\I386\DRIVER.CAB*, then the guardian angel pops up a window asking you to supply the original Windows 2000 installation media.

Here is an experiment you can try: Run Windows Explorer, open *C:\WINNT*, and rename NOTEPAD.EXE to NOTEPAD.SAV. Say Yes to the confirmation question. 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 2000 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 *C:\WINNT* from the *DLLCACHE* folder. (If neither of these things happens, then someone has disabled system file protection on your PC.)

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.

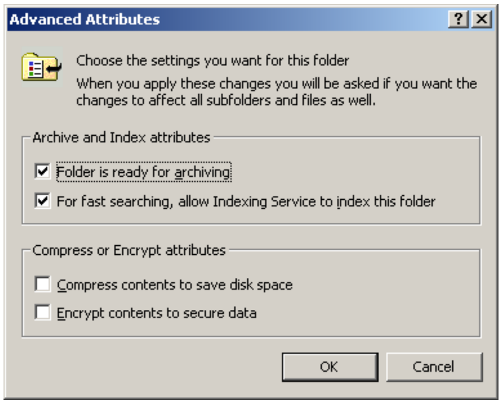
Encrypting File System (EFS)

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 2000 offers 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.

Windows 2000's 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 2000 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.

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. 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 (see **Figure 11**).



Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

☐ Compress contents to save disk space

☐ Encrypt contents to secure data

Figure 11: You can compress or encrypt, but not both. (The boxes should be radio buttons.)

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

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.

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 2000 *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.

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).

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.

Chapter 6

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 2000 offers a variety of methods to secure data in transit, including *IPSec* and *packet filtering*.

Although this section only examines these two methods in detail, other ways exist to improve security for transmitted data. For example:

- The security features of *PPTP* (Point-to-Point Tunneling Protocol) help protect computers in Virtual Private Networks (VPNs).
- Windows 2000 supports *callback security* for dial-up remote access connections.
- Active Directory lets you specify who can dial into a server remotely, when they can dial in, and what constraints may apply to their remote sessions, through *remote access policies* and *remote access profiles*.

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 2000 computers, such as a workstation (or collection of workstations) and server, or if you need to encrypt communications between two Windows 2000 routers in a wide-area network tunnel, such as a Virtual Private Network (VPN).

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 2000 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 entire groups 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. So, IPSec should only be used if and where necessary.

IPSec and Policies

You enable, configure, and edit IPSec parameters in Windows 2000 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.
- On a domain controller, run the Active Directory Users and Computers console, and edit domain policies via the Group Policy tab of the domain property sheet. In this case, navigate to *Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory*.
- 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.

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.

Packet Filtering

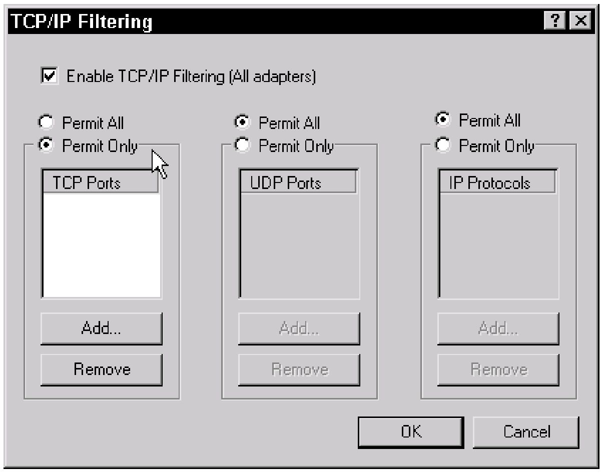
Packet filtering is a technique for restricting traffic or activating a security policy depending on a packet's source address, destination address, and/or traffic type. (A TCP port number, UDP port number, or IP protocol number may indicate the latter.) You can use packet filtering on NetWare (IPX packets), too, although this section discusses it in the context of IP packets.

Basic Packet Filtering

The following steps demonstrate how to configure packet filtering on a Windows 2000 Server or Windows 2000 Professional computer running TCP/IP (see **Figure 12**).

1. Choose Start➔Settings➔Network and Dial-Up Connections.
2. Right-click the Local Area Connection icon 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).
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.



TCP/IP Filtering

☑ Enable TCP/IP Filtering (All adapters)

○ Permit All
● Permit Only
TCP Ports

● Permit All
○ Permit Only
UDP Ports

● Permit All
○ Permit Only
IP Protocols

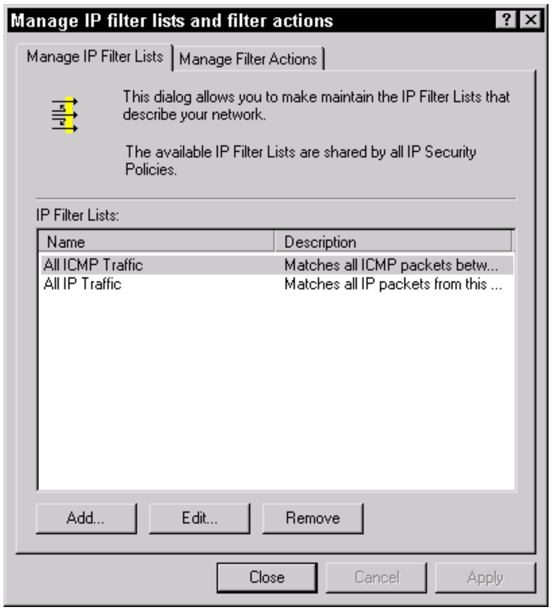
Figure 12: Configuring TCP/IP packet filtering.

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.

More Advanced Filtering

Right-click the IP Security Policies On Local Machine node in the tree pane of the console and choose Manage IP Filter Lists and Filter Actions. You see the dialog box in **Figure 13** below, which has two tabs: Manage IP Filter Lists, and Manage Filter Actions. This dialog box is global: It reflects all the filter lists and all the filter actions defined on the computer.



Manage IP filter lists and filter actions

This dialog allows you to make maintain the IP Filter Lists that describe your network.

The available IP Filter Lists are shared by all IP Security Policies.

IP Filter Lists:

Name	Description
All ICMP Traffic	Matches all ICMP packets betw...
All IP Traffic	Matches all IP packets from this ...

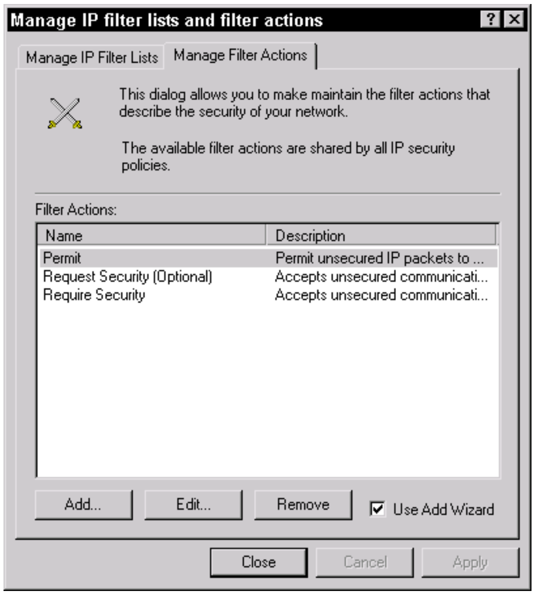
Figure 13: Lists let you group filters; actions specify what Windows should do.

A *filter list* is a list of filters that Windows treats as a single filter. A filter list does not *have* to include multiple filters—the two prefabricated lists, All IP Traffic and All ICMP Traffic, do not. But they can, which offers you some flexibility if you want to create (for example) a single filter list that covers traffic on two different physical subnets having different IP address ranges.

Each filter has the following fields, which you can edit by clicking the filter in the list and then clicking Edit:

- **Mirror:** The filter should apply bidirectionally, to outbound and inbound traffic, if the source and destination addresses are reversed.
- **Description:** Optional.
- **Protocol:** For example, TCP, UDP, and ICMP.
- **Source Port and Destination Port:** These are only available if the Protocol is TCP or UDP.
- **Source and Destination Addresses:** DNS name, IP address, and subnet mask.

Filter actions tell Windows 2000 what it is supposed to *do* when it encounters a match against a filter list. That is the purpose of the Manage Filter Actions tab (see **Figure 14**).



This dialog allows you to make maintain the filter actions that describe the security of your network.

The available filter actions are shared by all IP security policies.

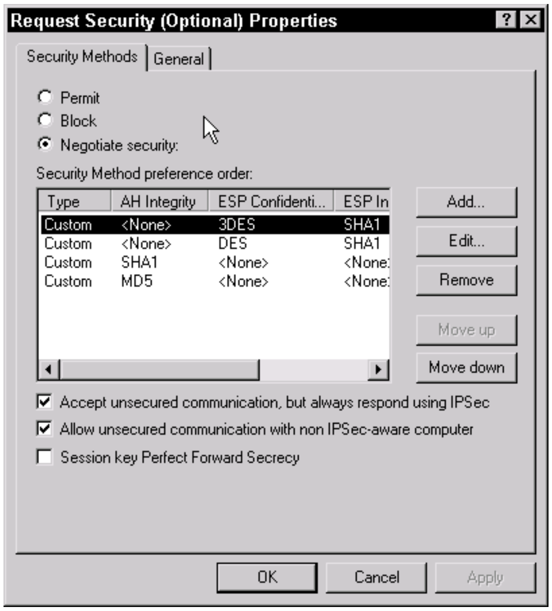
Filter Actions:

Name	Description
Permit	Permit unsecured IP packets to ...
Request Security (Optional)	Accepts unsecured communicati...
Require Security	Accepts unsecured communicati...

☑ Use Add Wizard

Figure 14: Here is where you tell Windows what actions it can associate with a filter or list.

The list of filter actions is entirely independent of the filter lists. That is, you can associate any filter list with any defined filter action. If you double-click the action named Request Security (Optional), you see the filter action Properties dialog box in **Figure 15** below. The core of this dialog box is the Security Methods tab.



○ Permit
○ Block
● Negotiate security:

Security Method preference order:

Type	AH Integrity	ESP Confidenti...	ESP In
Custom	<None>	3DES	SHA1
Custom	<None>	DES	SHA1
Custom	SHA1	<None>	<None
Custom	MD5	<None>	<None

☑ Accept unsecured communication, but always respond using IPSec
☑ Allow unsecured communication with non IPSec-aware computer
□ Session key Perfect Forward Secrecy

Figure 15: Specifying a filter action.

Take a look at the radio buttons at the top of the dialog box. You can make a decision to permit traffic or block traffic, without letting the two computers involved negotiate. Or, you can permit a negotiation in which the computers decide between themselves—based on the criteria you specify—whether to employ security, and if so, what kind.

Chapter 7

Local and Group Policy

Policies are really more of a mechanism for implementing and controlling the various other types of Windows 2000 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 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 Professional workstation. You can use this tool to set policies for the local machine only (see **Figure 16**).
- 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, 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.

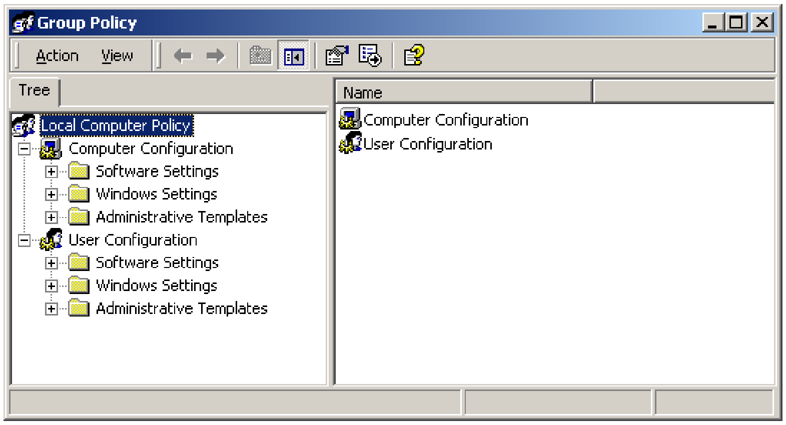


Figure 16: Run GPEDIT.MSC on a workstation to see all the policy settings.

Important Note for Mixed-Mode Networks: Windows 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.

Hierarchical Structure

The best thing about Group Policy (which is what Microsoft calls this feature, although I keep thinking of it as “policies” in the plural) is that it applies across your network’s hierarchical structure. In Active Directory, an enterprise network has different levels, as follows:

- Forests
- Trees
- Domains
- Organizational Units
- Groups

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.

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

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 2000 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.

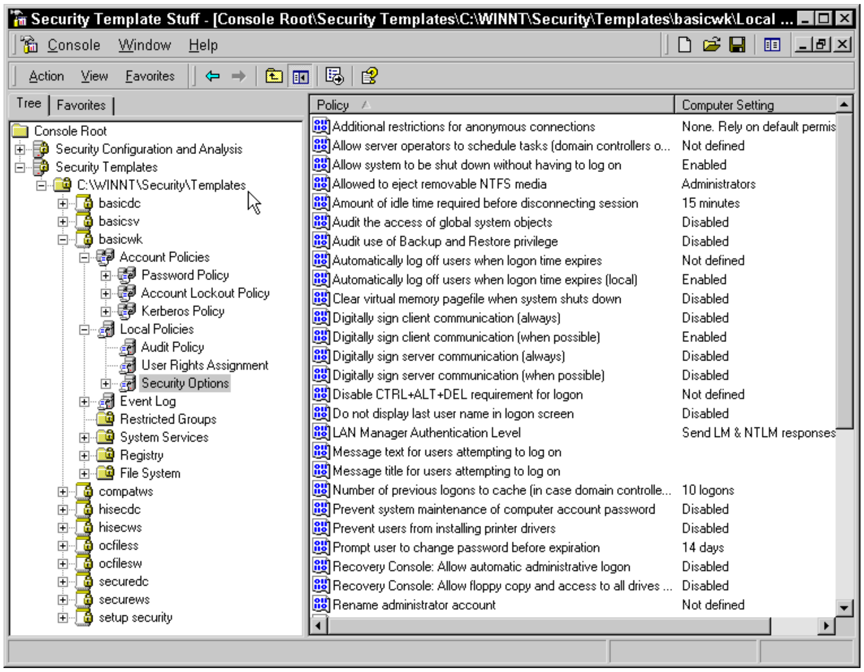
If you want to see for yourself how the Local Security Policy console is simply a subset of the entire set of policies, open GPEDIT.MSC via the Start➔Run dialog box, and navigate to *\Local Computer Policy\Computer Configuration\Windows Settings\Security Settings*. Now, open the Local Security Policy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

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 pre-configured for you by Microsoft have the suffix INF and live in *C:\WINNT\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).

You have to build a custom Microsoft Management Console to view and edit (but not apply!) the pre-built security templates. The technique is to run MMC.EXE and add the Security Templates snap-in (see **Figure 17**). This method is a whole lot easier than studying the INF files in a text editor.



Policy	Computer Setting
Additional restrictions for anonymous connections	None. Rely on default permis
Allow server operators to schedule tasks (domain controllers o...	Not defined
Allow system to be shut down without having to log on	Enabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon time expires	Not defined
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Disabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Not defined
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send LM & NTLM responses
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache (in case domain controlle...	10 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives ...	Disabled
Rename administrator account	Not defined

Figure 17: View INF file contents in an organized way with the Security Templates snap-in.

The pre-built 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 *apply* a template to a computer using the Security Configuration and Analysis console snap-in, as the next section describes.

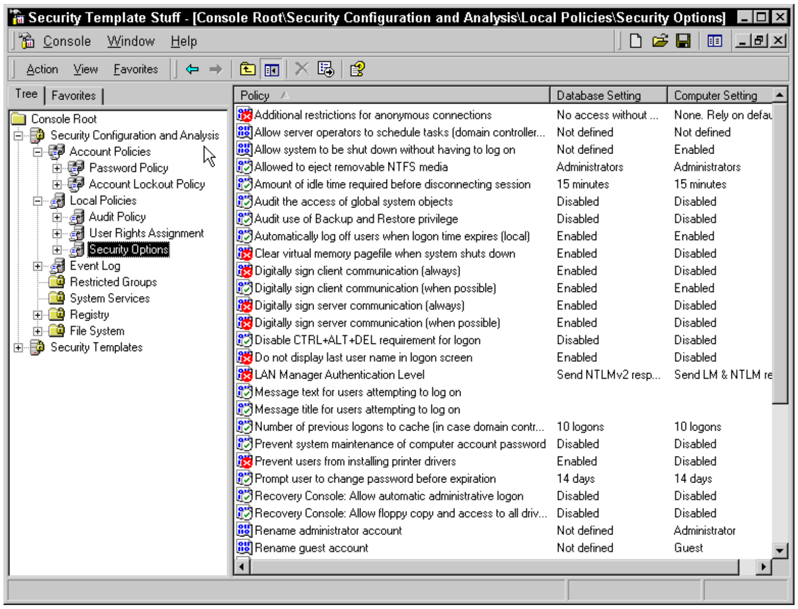
Security Configuration and Analysis

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. 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 (see **Figure 18**).



Policy	Database Setting	Computer Setting
✗ Additional restrictions for anonymous connections	No access without ...	None. Rely on defau
Allow server operators to schedule tasks (domain controller...	Not defined	Not defined
Allow system to be shut down without having to log on	Not defined	Enabled
✓ Allowed to eject removable NTFS media	Administrators	Administrators
✓ Amount of idle time required before disconnecting session	15 minutes	15 minutes
✓ Audit the access of global system objects	Disabled	Disabled
✓ Audit use of Backup and Restore privilege	Disabled	Disabled
✓ Automatically log off users when logon time expires (local)	Enabled	Enabled
✗ Clear virtual memory pagefile when system shuts down	Enabled	Disabled
✗ Digitally sign client communication (always)	Enabled	Disabled
✓ Digitally sign client communication (when possible)	Enabled	Enabled
✗ Digitally sign server communication (always)	Enabled	Disabled
✗ Digitally sign server communication (when possible)	Enabled	Disabled
✓ Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
✗ Do not display last user name in logon screen	Enabled	Disabled
✗ LAN Manager Authentication Level	Send NTLMv2 resp...	Send LM & NTLM re
✓ Message text for users attempting to log on		
✓ Message title for users attempting to log on		
✓ Number of previous logons to cache (in case domain contr...	10 logons	10 logons
✓ Prevent system maintenance of computer account password	Disabled	Disabled
✗ Prevent users from installing printer drivers	Enabled	Disabled
✓ Prompt user to change password before expiration	14 days	14 days
✓ Recovery Console: Allow automatic administrative logon	Disabled	Disabled
✓ Recovery Console: Allow floppy copy and access to all driv...	Disabled	Disabled
Rename administrator account	Not defined	Administrator
Rename guest account	Not defined	Guest

Figure 18: Analyzing a specific computer with respect to a specific security template.

Chapter 8

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 2000's "videotapes" are the *event logs*, which reside in the folder *C:\WINNT\SYSTEM32\CONFIG* and have the suffix EVT. You view these with the Event Viewer, one of Windows 2000's administrative tools.

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

Logon Auditing

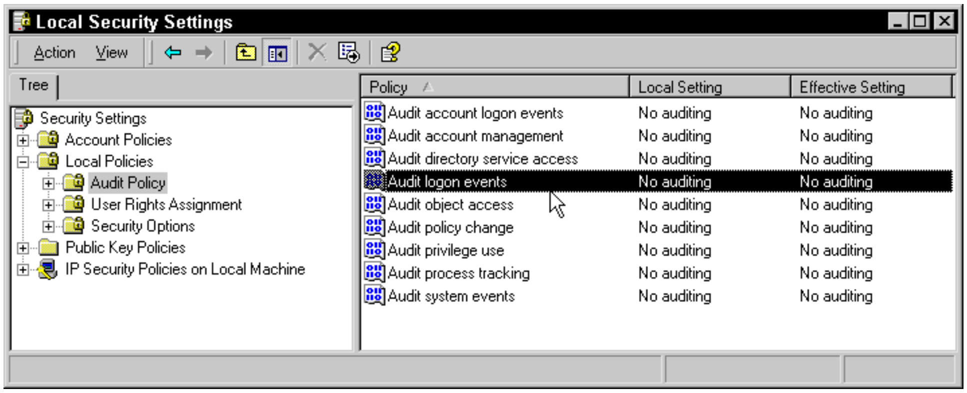
Windows 2000 can monitor logons, both successful and unsuccessful, and record them in the Security event log (which you can view with the Event Viewer utility). You would use logon auditing to discover if and when a cracker is trying to break into a PC by guessing account names and passwords, or why a company employee is logging on to his system at unusual hours.

Here is how to activate logon auditing (see **Figure 19**):

1. Choose Start➔Settings➔Control Panel.
2. Double-click Administrative Tools.
3. Double-click Local Security Policy.
4. In the tree pane to the left, expand Local Policies.
5. In the tree pane, click Audit Policy. All the various quantities that you can audit now appear in the details pane to the right.
6. In the details pane, double-click Audit Logon Events.
7. 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.

8. Click OK and close the Local Security Policy console.
9. 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).



Policy	Local Setting	Effective Setting
Audit account logon events	No auditing	No auditing
Audit account management	No auditing	No auditing
Audit directory service access	No auditing	No auditing
Audit logon events	No auditing	No auditing
Audit object access	No auditing	No auditing
Audit policy change	No auditing	No auditing
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

Figure 19: 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.

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 he did it.
- 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.

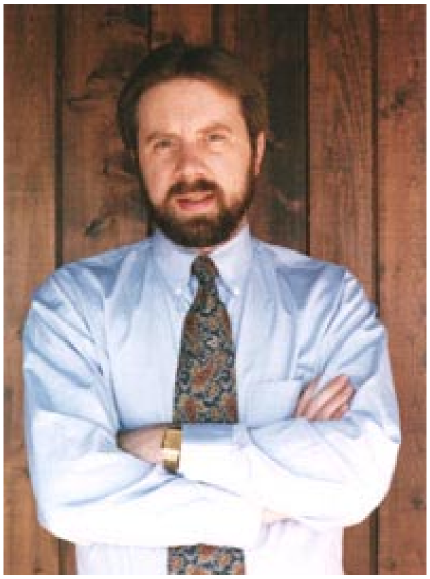
The procedure for enabling object auditing is very similar to the procedure for enabling logon auditing (see previous section); the only difference is that you would choose "Audit object access" instead of "Audit logon events" in the Local Security Policy console.

After you have enabled object auditing, you must take an extra step and tell Windows 2000 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, is president of Independent Software, Inc. (www.i-sw.com), a consulting firm he founded in 1982 after graduating from Stanford University's engineering school. One of the country's most popular technical trainers, Glenn has taught Windows to thousands of students in the United States, United Kingdom, and Canada in more than 200 seminars since 1988. Glenn is the author of fifteen published books, including *MCSE Windows 2000 Professional For Dummies*, *Windows 2000 Registry For Dummies*, and *MCSE Windows 2000 Network Infrastructure For Dummies*. He recently served as an expert witness in the Microsoft antitrust trial.