Global Information Assurance Certification Paper

Windows 2000 Security and Tools of the Trade

by

Mark D. Tollison

Submitted

April 25, 2001

Research Paper Index

Executive Summary

As an Information Technology (IT) or Network Security professional, one constant challenge is to keep pace with the change and growth in technology. Computers, network equipment and operating systems are evolving at a record pace. This especially applies to the Microsoft suite of operating systems and software products. One of the most recent additions to the Microsoft family of operating systems is the Windows 2000 products. The Windows 2000 products come in four varieties, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server and Windows 2000 Datacenter Server. Each system has distinct capabilities and are tailored to meet the needs and required services for various types and sizes of organizations. As detailed by the Microsoft Web site [1], characteristics of these systems are listed in the following paragraphs.

Windows 2000 Professional

Windows 2000 Professional is for the personal computer you use at work—whether it's stationary on your desktop, or mobile as in a laptop or notebook computer. Windows 2000 Professional offers solid reliability, easy mobility, and improved manageability features.

Windows 2000 Server

Windows 2000 Server is the entry-level version of the server family. The multipurpose network operating system for businesses of all sizes, it is the perfect solution for

file, print, intranet, and infrastructure servers. It scales from 1 to 4 processors and up to 4 gigabytes.

Windows 2000 Advanced Server

Windows 2000 Advanced Server delivers enhanced reliability, availability, and scalability for running e-commerce and line-of-business applications. It scales from 1 to 8 processors and up to 8 gigabytes, and provides enhanced reliability and availability—with two-node clustering and 32-node network load balancing.

Windows 2000 Datacenter Server

Windows 2000 Datacenter Server is the most powerful server operating system ever offered by Microsoft. Datacenter Server is designed for enterprises that demand the highest levels of availability and scale. It scales from 1 to 32 processors and up to 64 gigabytes, and provides maximum reliability and availability—with four-node clustering, 32-node network load balancing, and systems tested through the Windows Datacenter Program.

Microsoft has included a comprehensive set of security services within Windows 2000. Additions such as Active Directory, Kerberos, IPsec, MMC, EFS, PKI, Group Policies and others are significant enhancements for user and network security. This paper focuses on some of the new security features of the Windows 2000 operating systems and some of the tools used to administer these security features. I will discuss the new Microsoft Management Console (MMC) and available security snap-ins. Also, I will examine some additional tools available on the Windows 2000 Resources kits and how these tools benefit the Windows 2000 user and system administrator.

Index

Windows 2000 Security Concepts

As mentioned earlier, Microsoft has built new security features into the Windows 2000 operating systems. Additions such as Active Directory, Kerberos, IPSec, PKI and Group Policies are a few of the added security features. As we begin a discussion of security tools, let's examine some of the new and expanded security features of the Windows 2000 operating systems and how these map to the basic tenants of Information Security. Since, this paper is limited in scope, I will rely on other great references to fill in the specific details. Two great references are the Windows 2000 Security Handbook [2] and the Windows 2000 Professional Resource Kit [3]

Security within Windows 2000 can be organized in the following broad categories.

- Accounts - Both User and Group
- Encryption (NTFS drives only)
- File and Folder Permissions (NTFS drives only)
- Shared Folder Permissions
- Printer Permissions
- Auditing
- User Rights
- Group Policy

Before I begin a detailed discussion about Windows 2000 security, let us look at one of the tool frameworks provided with this operating system. This new tool framework is called the Microsoft Management Console (MMC).

Index

Microsoft Management Console (MMC) Overview

The Microsoft Management Console (MMC) is a framework used to hosts tools for the administration of the various hardware, software and network components of the Windows systems and other applications. Functionality is added to the console by the addition of tools called a "Snap-in". Functionality of the MMC is not restricted to use of snap-ins but can include items such as ActiveX controls, web links, applications, etc. For our analysis, Snap-ins are available to monitor many of the security functions of a Windows system. Also, the administrator can use Group Policies to restrict or allow access to snap-ins.

In general there are two primary ways to use the MMC. The first is user mode, which allows the user to interact with MMC consoles that are currently available. In this mode the user can not add any new snap-ins or functionality to existing consoles. In theory, user mode is for administering a system and can be assigned with the following restrictions.

- User mode with full access
- User mode with limited access, multiple window or single window

The second mode of the MMC is the author mode. In this mode the administrator can create or edit MMC consoles. As with snap-ins, administrators can restrict the ability of a user or groups access to author mode.

Index

Microsoft Management Console (MMC) Start

In order to get a feel for the Microsoft Management Console, let's develop a console from scratch. We will add functionality to the console as we discuss the various security tools. The steps are as follows.

1. From either the Windows 2000 command prompt, or the Run menu, type **mmc.exe**. This is shown in Figure 1.

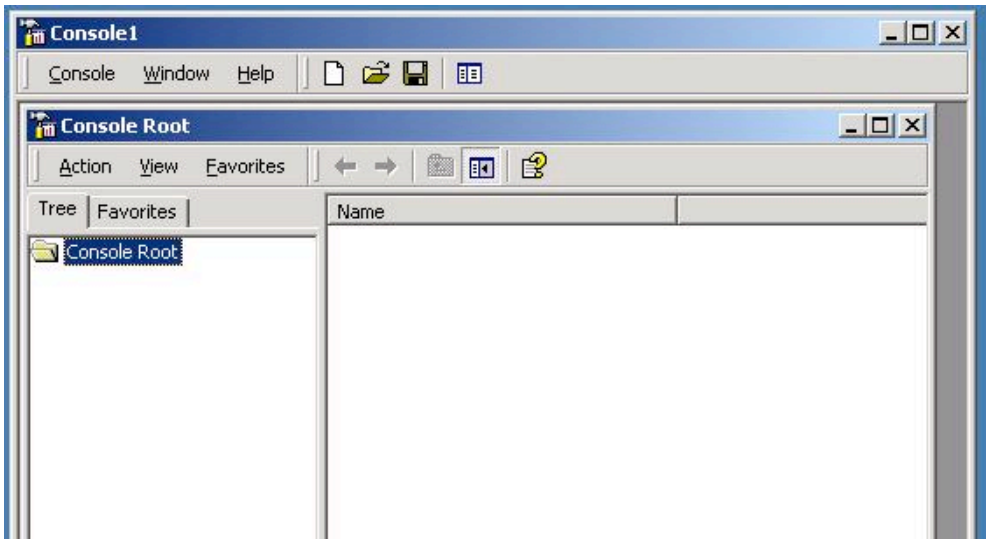


Figure 1.

1. From the top menu, choose Console, then Add/remove Snap-in (Ctrl-M). This is shown in Figure 2.

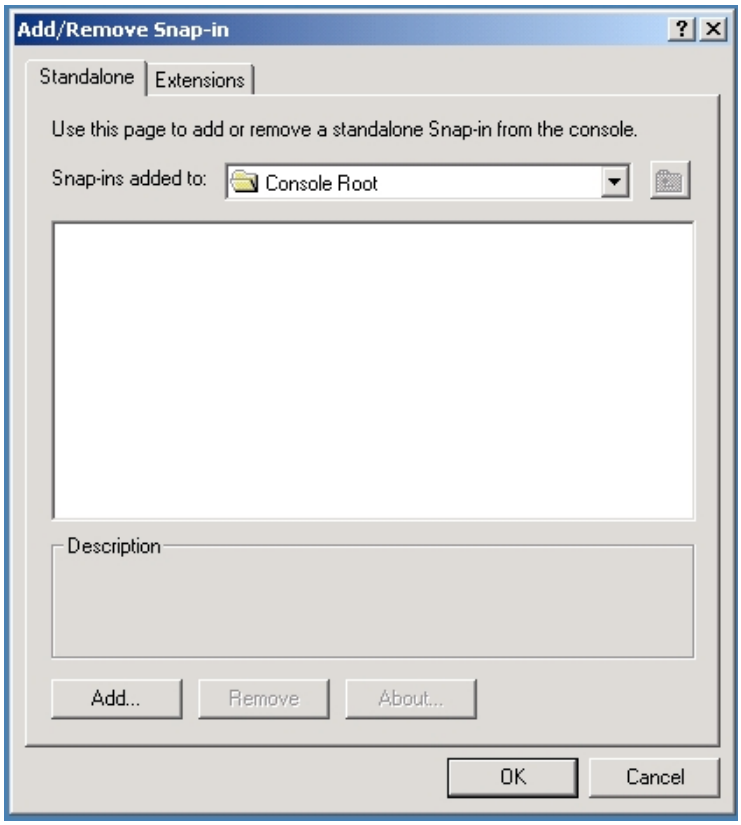
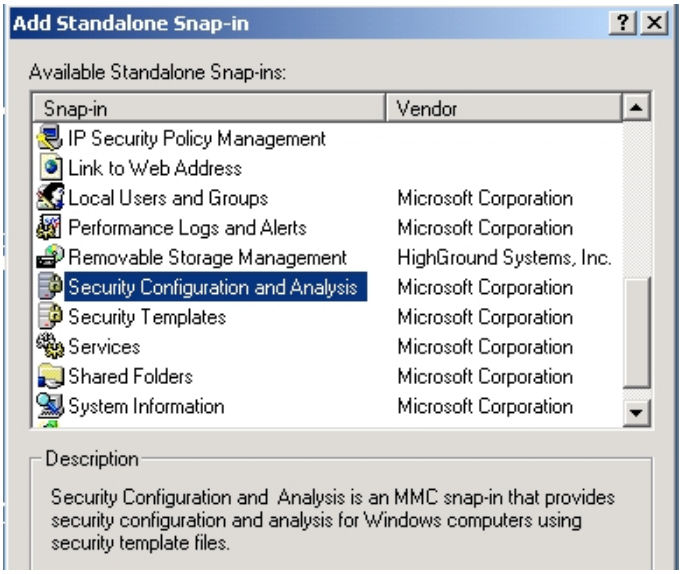


Figure 2.

1. For this example, choose the Security Configuration and Analysis snap-in. The display of this snap-in is shown in Figure 3.



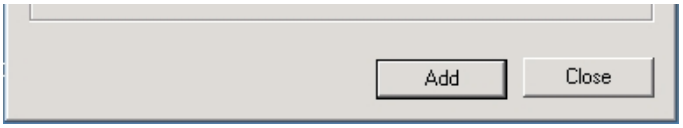


Figure 3.

Index

User and Group Accounts

User Accounts

In order to use a Windows 2000 computer, every user must have a user name and password. When a new user account is created, a unique number, a Security ID, is created for that that user. Windows 2000 internal processes use this SID for all authorization decisions. Since, SIDs are unique they cannot be reused. Deleting, then creating, a new user account with the same user name, will be associated to a new SID. This assures the authorization integrity from user to user.

Group Accounts

Every Windows 2000 user is assigned as a member of a group. Windows 2000 comes with a number of built-in groups. Depending on a users roles and responsibilities, group membership helps control which types of activities a user can perform. For example, a normal user has the need to run various software programs, but does not have a need to install software programs on the computer. Assigning certain rights and permissions to the defined groups allows users to perform their required tasks. The Microsoft Management Console (MMC) tool for working with users and groups is shown in Figure 4. This tool can be accessed via the Control Panel and selecting the Users and Passwords icon. This view shows some of the default groups in which users can be assigned. New groups can be created as required.

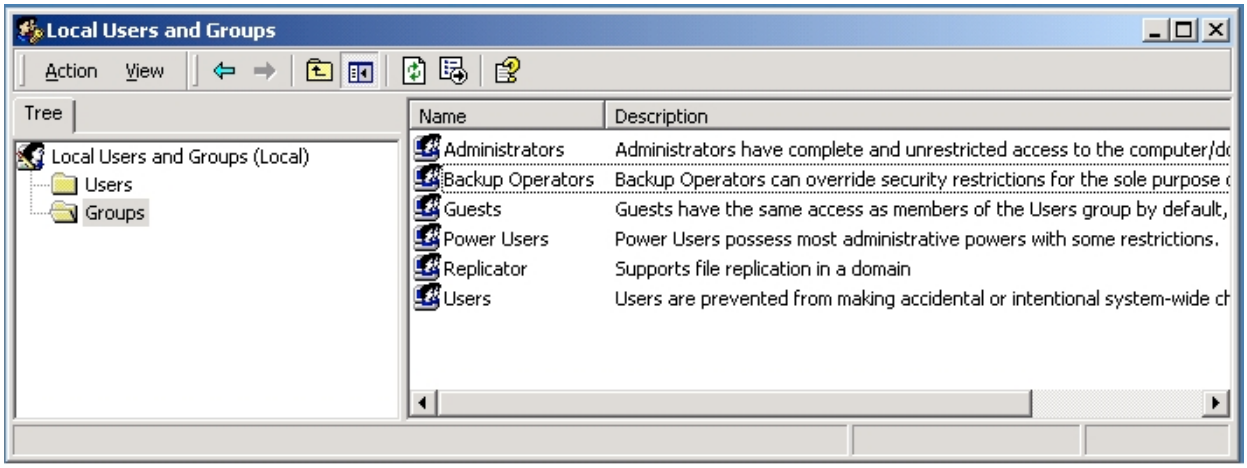


Figure 4.

Index

Encrypting File System (EFS)

One of the new features of Windows 2000, is the ability to protect sensitive data while stored locally on a NTFS Version 5 formatted drive. This protection, called Encrypting File System (EFS) is accomplished by encrypting selected files or folders using public/private key technology. This feature is especially useful for users who

travel frequently and store important data on laptop computers. Stolen laptops have received increased attention in the news [4]. Encryption can help safeguard critical business data.

The EFS does have some restrictions on its use. Files are only encrypted while they are stored locally. The files will be decrypted if they are moved to a non NTFS drives, or if they are sent across a network. System files, compressed files or folders, and the sharing of encrypted files is prohibited. Also, file encryption is linked to the user that encrypted the file. Recovery steps are needed to ensure that files can be recovered if a user is removed from the system.

Files can be encrypted using the command prompt, CIPHER command or by using the advanced features from Windows Explorer. Displays showing these steps for a folder and Microsoft Word file called "Test" is shown in Figures 5 and 6. The file was created by user Mark. When user Test tries to read the encrypted file an error is reported. This error display is shown in Figure 7. So this test proves that EFS can help protect your files.

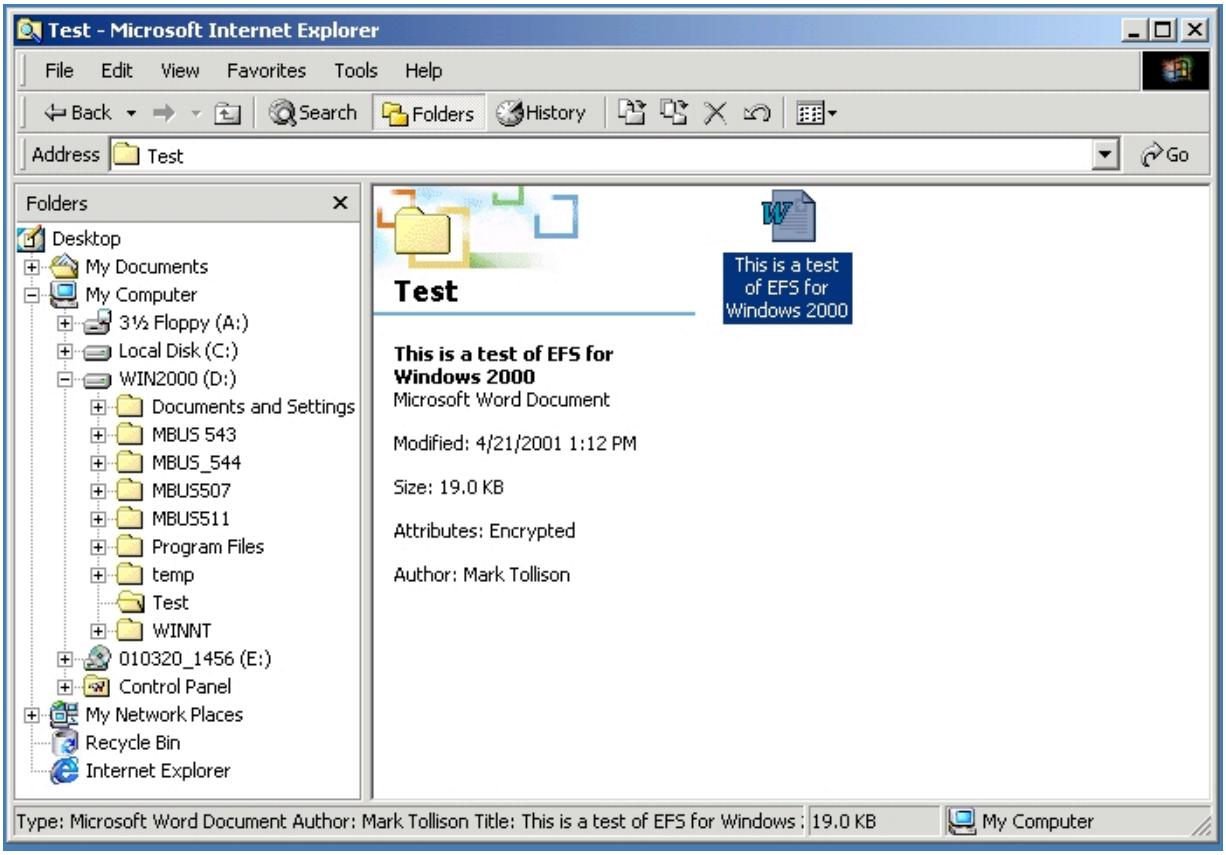
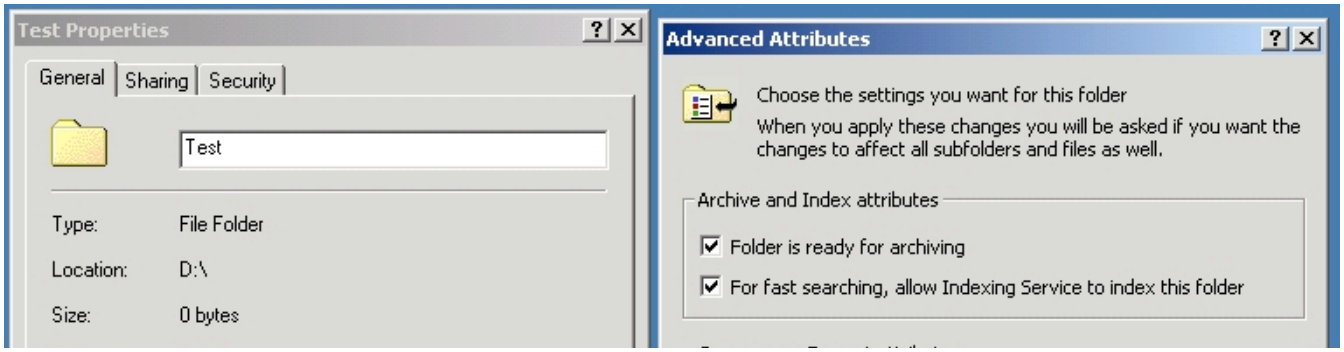


Figure 5.



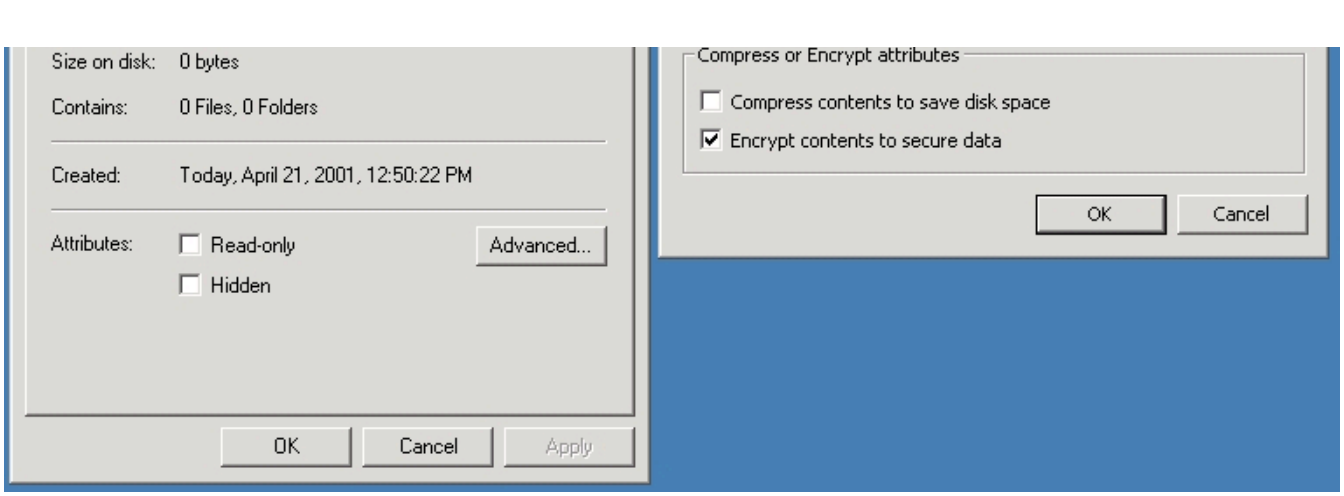


Figure 6.

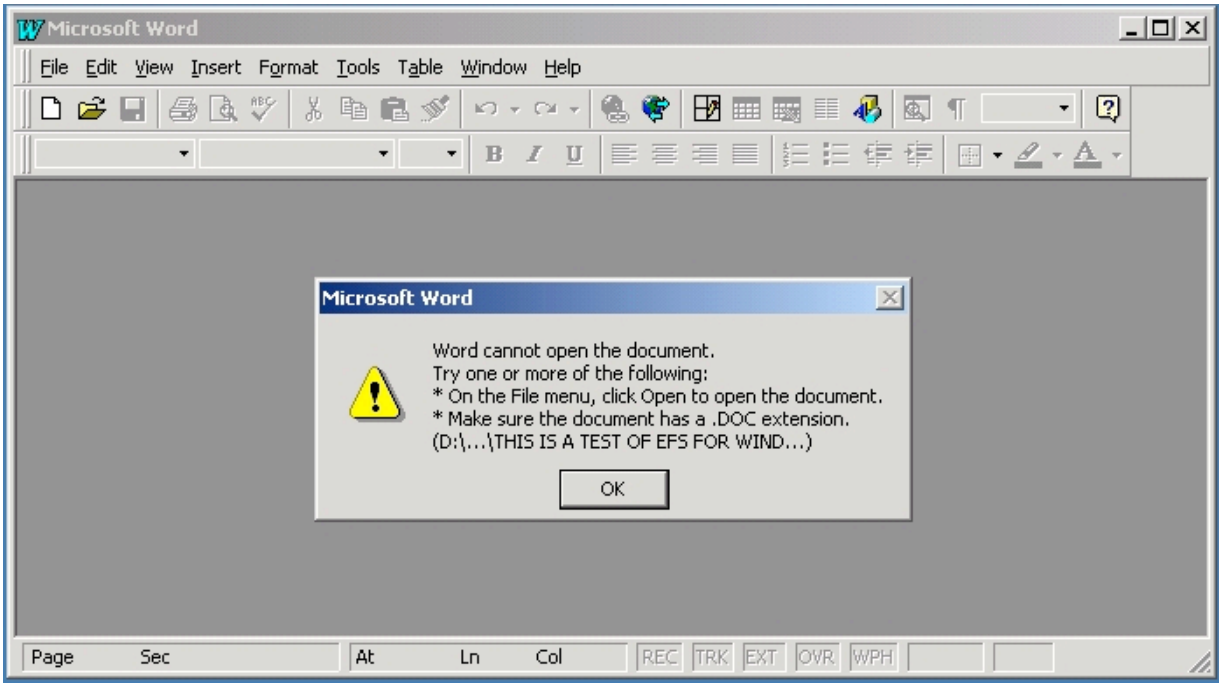


Figure 7.

Index

Permissions

By definition [5], Microsoft defines a permission to be; "A rule associated with an object to regulate which users can gain access to an object and in what manner." On a personal level, I can relate to permissions since I have young children and are frequently reminding them about whether they have permission to perform various activities. In security, we can have permission to review various documents or perform various functions. If used properly, permissions can be an effective security tool.

For Windows 2000, permissions can be grouped into the following categories. Let us take a few moments and examine these different use of permissions.

- File and Folder Permissions
- Shared Folder Permissions

- Printer Permissions

Index

File and Folder Permissions

As was the case for the Encrypting File System (EFS) permissions can only be used with Windows NT File System (NTFS) formatted drives. Specifically, Windows 2000 implements permissions using the latest version of this file system, NTFS Version 5. One attribute of the latest NTFS file system is the ability to apply permissions to file, folders or drives. For more specific control, "special permissions" can be applied. This differs from Windows NT 4, which used "permission sets" and "permissions" for lower level control. In either operating system, using permissions allows the administrator to effectively manage security and access to these system components.

As outlined in "NTFS Security --What's New in Windows 2000?"[6], file and folder permissions are listed in Tables A and B. From the same reference, the file and folder special permissions are shown in Tables C and D.

File Permissions in Windows 2000

File permission	Enables you to
Full Control	Read, write, modify, execute, change attributes, permissions, and take ownership of the file.
Modify	Read, write, modify, execute, and change the file's attributes.
Read & Execute	Display the file's data, attributes, owner, and permissions, and run the file (if it's a program or has a program associated with it for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

TABLE A.

Folder Permissions in Windows 2000

File permission	Enables you to
Full Control	Read, write, modify, and execute files in the folder, change attributes, permissions, and take ownership of the folder or files within.
Modify	Read, write, modify, and execute files in the folder, and change attributes of the folder or files within.
Read & Execute	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
List Folder	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if

	they're programs or have a program associated with them for
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

TABLE B.

File Special Permissions in Windows 2000

File Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X
Create Folders/Append Data	X	X			X
Write Attributes	X	X			X
Write Extended Attributes	X	X			X
Delete Subfolders And Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X	X			
Take Ownership	X				
Synchronize	X	X	X	X	X

TABLE C.

Folder Special Permissions in Windows 2000

Folder Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder/Execute File	X	X	X	X		
List Folder/Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create Files/Write Data	X	X				X
Create Folders/Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders And Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					
Synchronize	X	X	X	X	X	X

TABLE D.

Modifying permissions on a file, folder or drive is accomplished via various methods. One method is to change the various values by using the Windows Explorer tool. After locating the selected file, folder, or drive, right clicking, choosing properties, then selecting the Security Tab will lead you to the permissions area. This is shown in Figures 8 through 10. Also, the Windows 2000 Resource Kits include a utility, XCALS, that can be used to modify permissions. Viewing permissions can be accomplished via the PERMS command. Examples of these utilities are Shown in Figure 11.

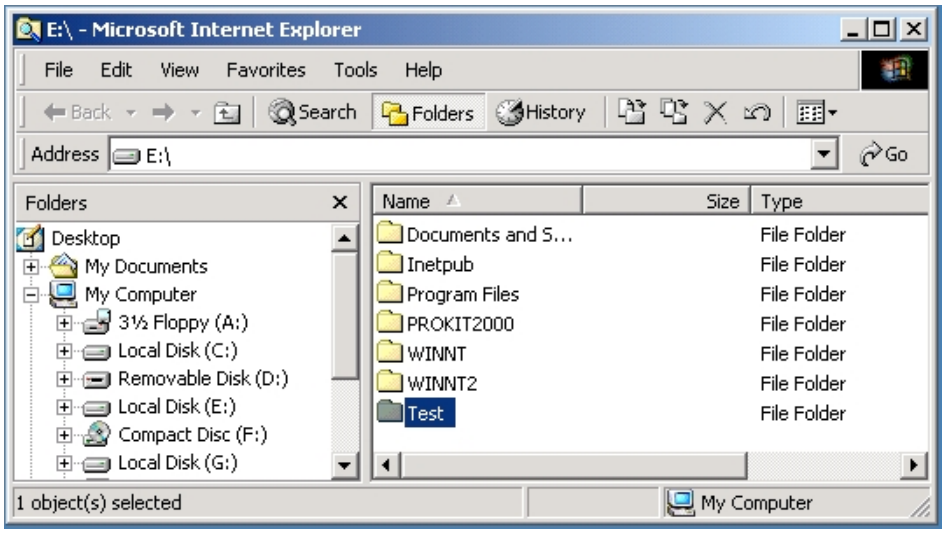


Figure 8.

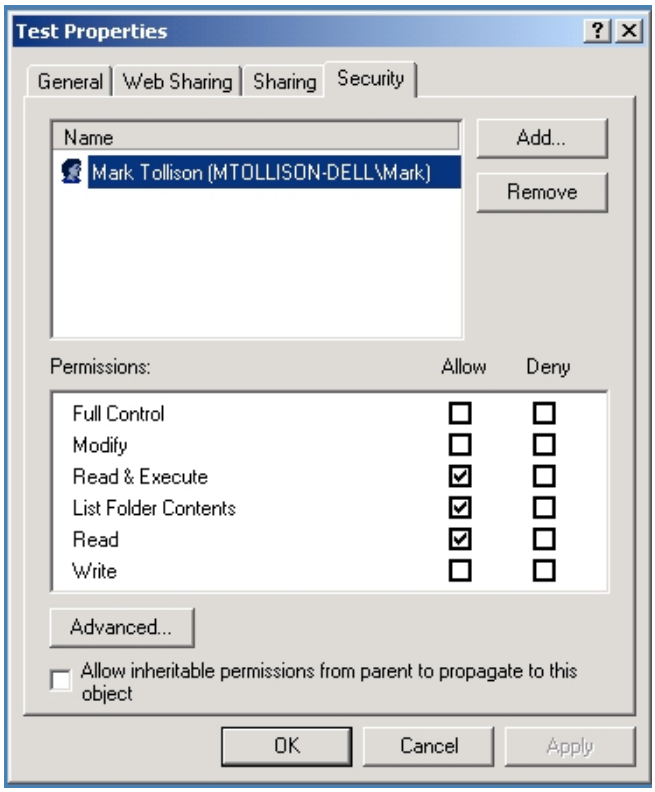


Figure 9.

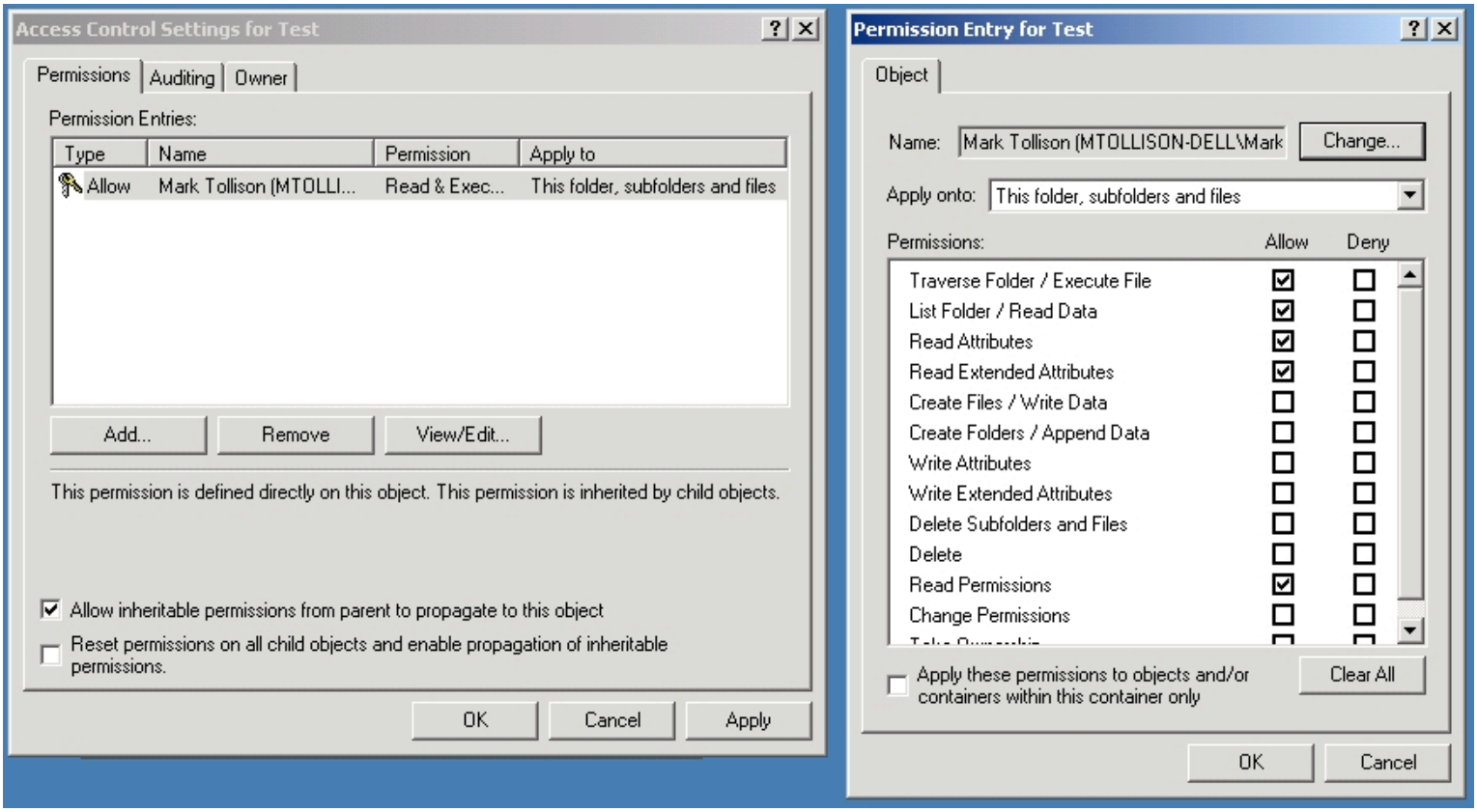


Figure 10.

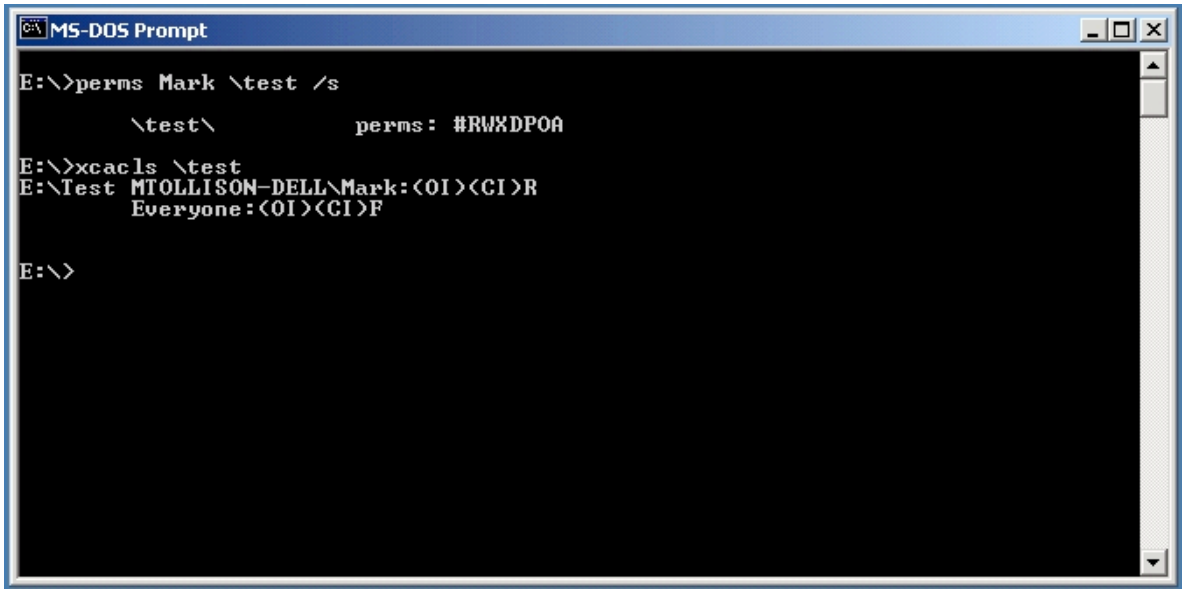


Figure 11.

Index

Shared Folder Permissions

The ability for multiple users to share files and folders over the network is not a new concept. These functions have been available in many of the previous Windows

operating systems and server products. Windows 2000 allows users to not only share out critical resources but to protect them using permissions. Setting of permissions for shared folders is very similar to those discussed earlier for other folders and files. An example of the shared folder "Test" permissions are shown in Figure 12.

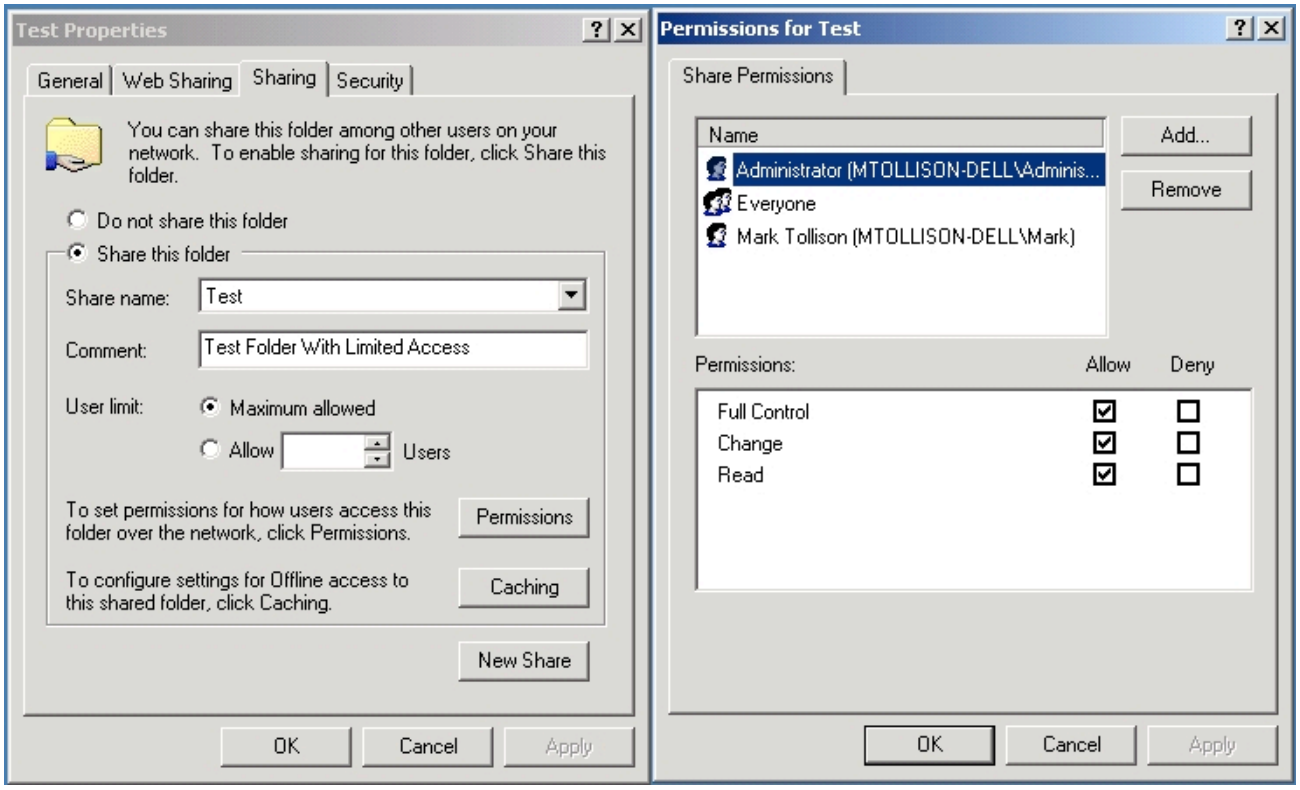


Figure 12.

I would like to make a couple of key points about permissions for shared folders. There is a difference between "Share Permissions" vs those of the "NTFS permissions". Shared permissions apply to users who access resources via the network. NTFS permissions apply to all users and can override the shared permission settings. NTFS permissions can be the most restrictive and allow for finer control of general access to resources.

Also, Windows 2000 introduces the ability to publish shared folders via Active Directory so that network users can easily locate the published folder wherever it may reside, either on a workstation or a server. Another administrate tool is the Distributed File System (DFS). DFS allow the administrator to publish physically separated network shares into one logical shared resource. This can be useful for load balancing or security. This is another MMC tools and can be found via the Control Panel.

Index

Shared Printer Permissions

In some situations it is desired to establish a printer server and share a printer among various Windows 2000 users. Shared printers do not have the same permissions as those with shared folders. NTFS permissions are used to restrict usage of these resources. An example of this is shown in Figure 13.

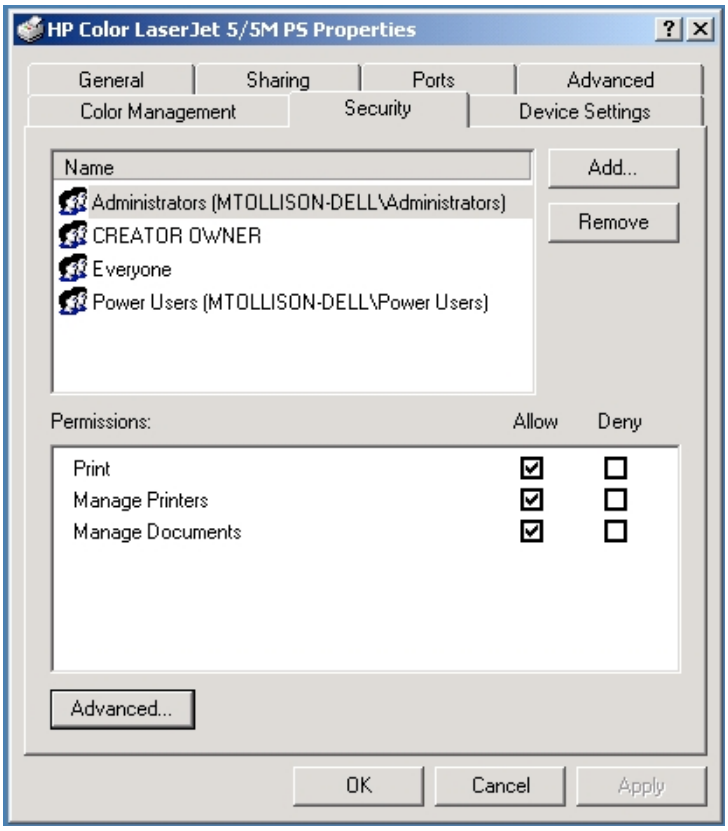


Figure 13.

Index

Auditing

For the majority of us, auditing is not a new concept. For those new to the concept, auditing is a method to help determine who, what, when and how a system related event occurs. From an Intrusion Detection perspective, auditing and the associated logs, provide a critical link in determining the details of a system compromise. An analogy would be for my house to have a burglar alarm. However, I may never know if a break-in occurred, if the system was never activated or if it was never checked periodically for proper operation. Windows 2000 auditing follows this same analogy. When installed, the system has the ability to audit many functions, unfortunately initially, it is not fully enabled. It is important for the security administrator to examine or established a company or sites security policy before enabling the required auditing. It is very difficult to find intrusions or system problems if auditing is not correctly enabled.

For Windows 2000, the system will contain a minimum of three log files. These logs are the Application, Security and System files. Other log files are available depending on the services installed. A few common log files include:

- Appevent.evt - File that contains applications event data.
- Sysevent.evt - File that contains system event data.
- Secevent.evt - File that contains security event data.
- DNSevent.evt - File that contains Microsoft DNS server event data.
- NTDS.evt - File that contains Active Directory (AD) server event data.
- NTFRS.evt - File that contains File Replication Service (FRS) event data.

Per Microsoft [5], the term event is defined as, "Any significant occurrence in the system or an application that requires users to be notified or an entry to be added to

a log". Logging is configured so that as certain events occur they are written to the appropriate log. For the remainder of this discussion I will concentrate on the Security log file and auditing.

Configuring security audit policy can be accomplished via a couple of methods. To configure the local computer audit settings, the Group Policy Snap-in for the Microsoft Management Console (MMC) can be used. Also, Active Directory (AD) level configurations can configure these setting using the same Group Policy Snap-In. I will discuss Group Policy later in this paper.

For the local policy case, I had to configure a MMC console with the Local Policy snap-in. Configuring a MMC console has been discussed earlier. The local policy information is shown in Figure 14.

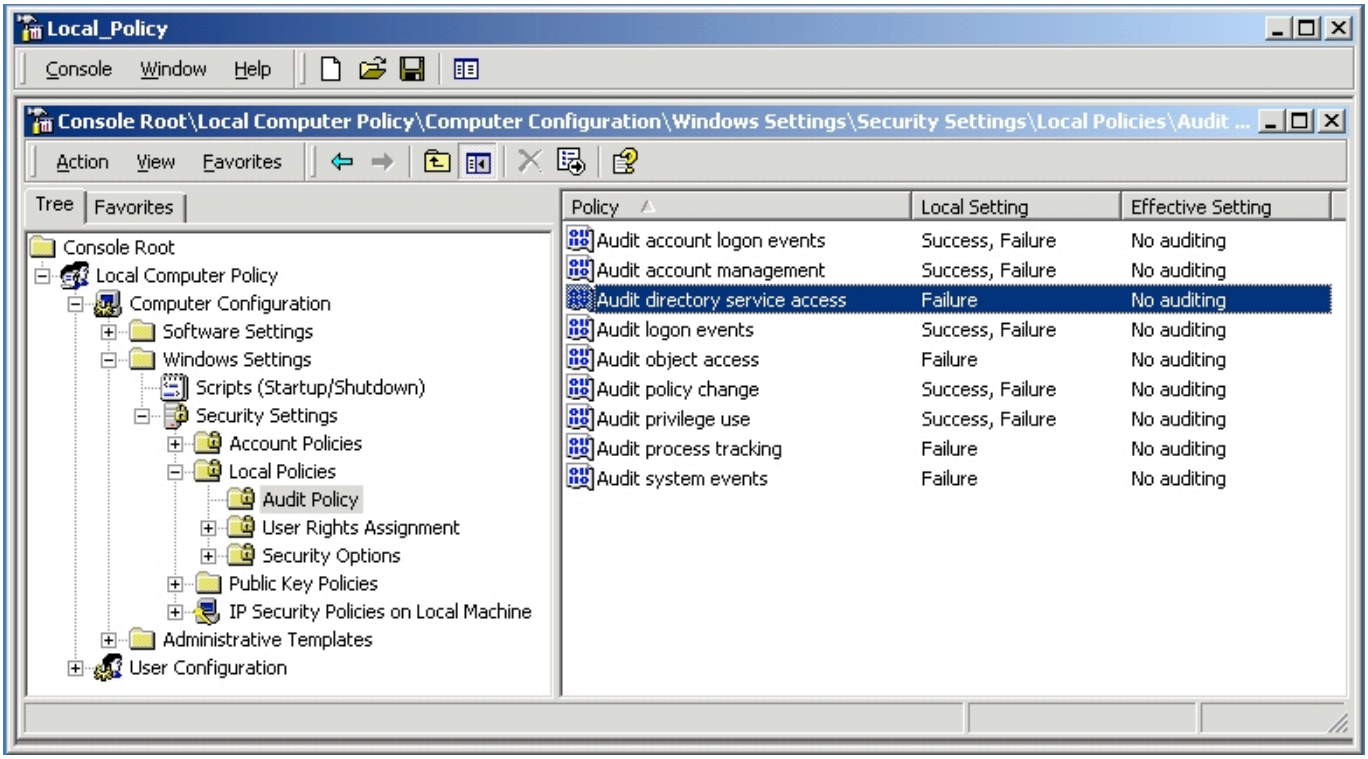
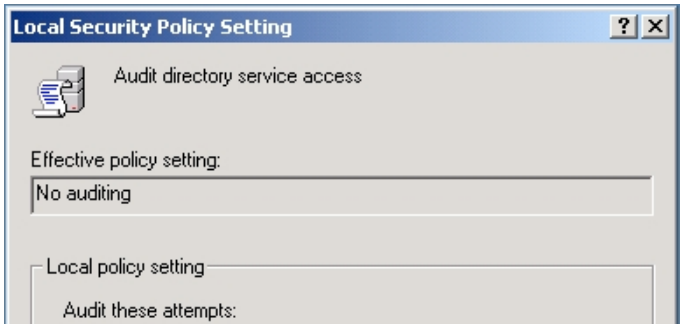


Figure 14.

Each of these audit events are initially set to "No auditing". By default an administrator would not be able to know if any of these security related events occurred. Configuring these audit events are simple. From the right panel choose an event and double click to bring up the configuration window. An example of this is shown in Figure 15.



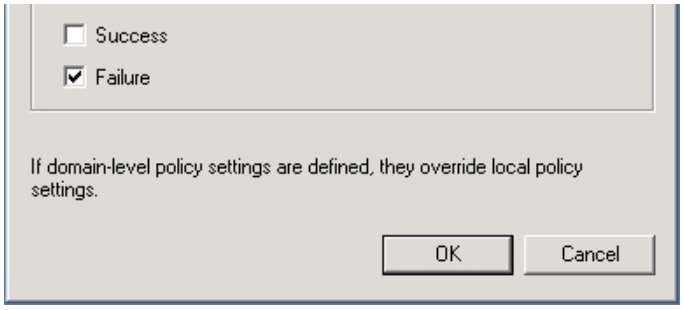


Figure 15.

Once all the security audit events are configured, some method is need to view and administer the log files. Windows 2000 comes with another MMC snap-in called Event Viewer. Event Viewer gives an administrator the ability to view and administer the log files. The event viewer can be found under the Control Panel and Administrative Tools section. If not found, a default MMC console can be configured with the Event Viewer Snap-in. An example of this is shown in Figures 16 and 17.

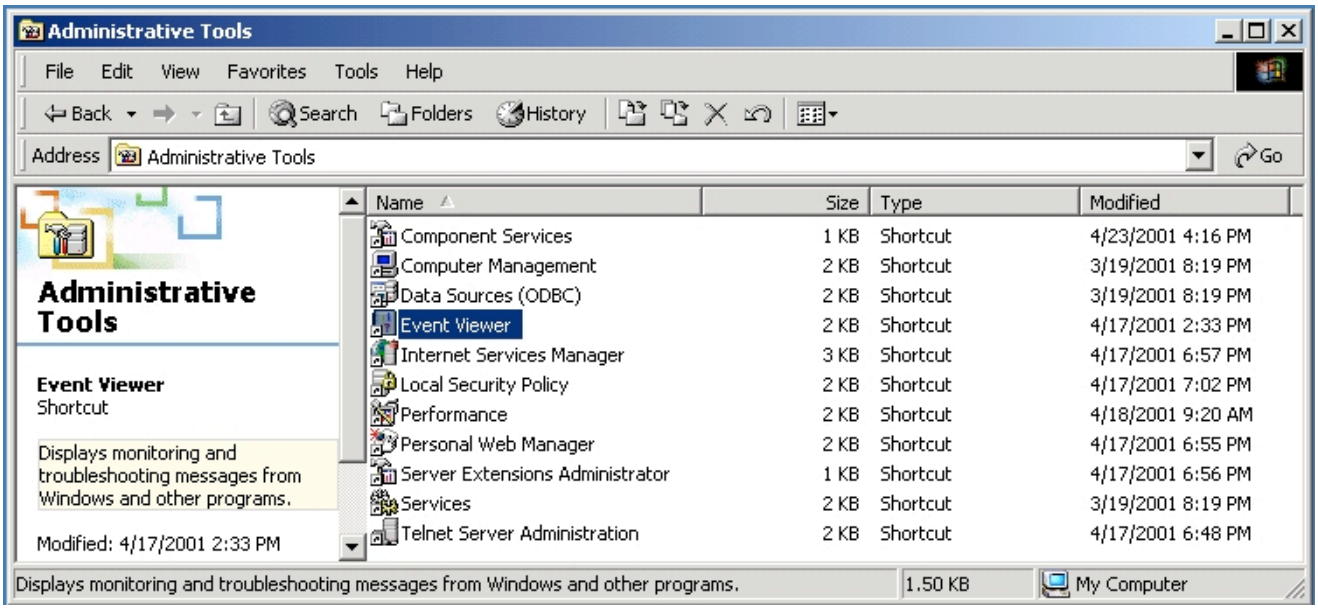
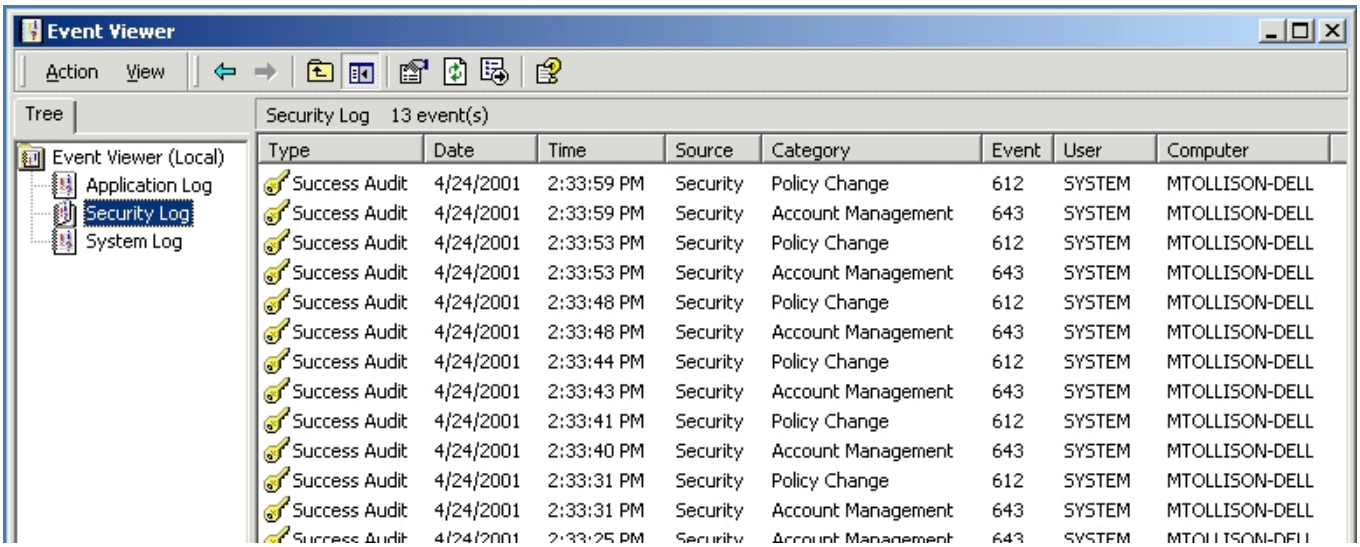


Figure 16.



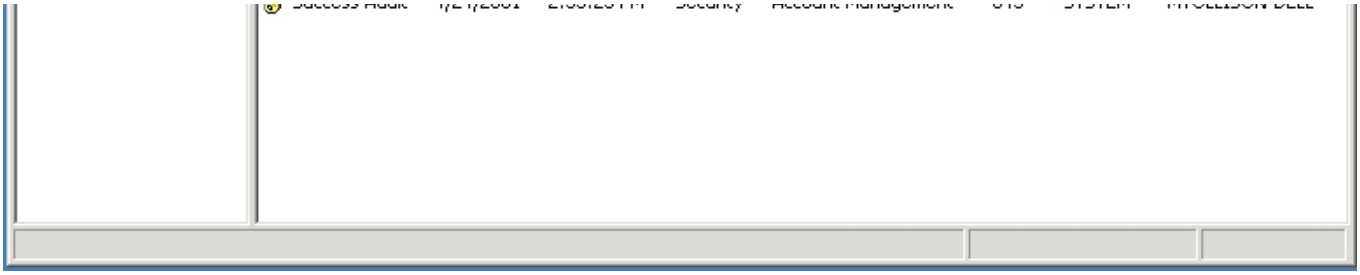


Figure 17.

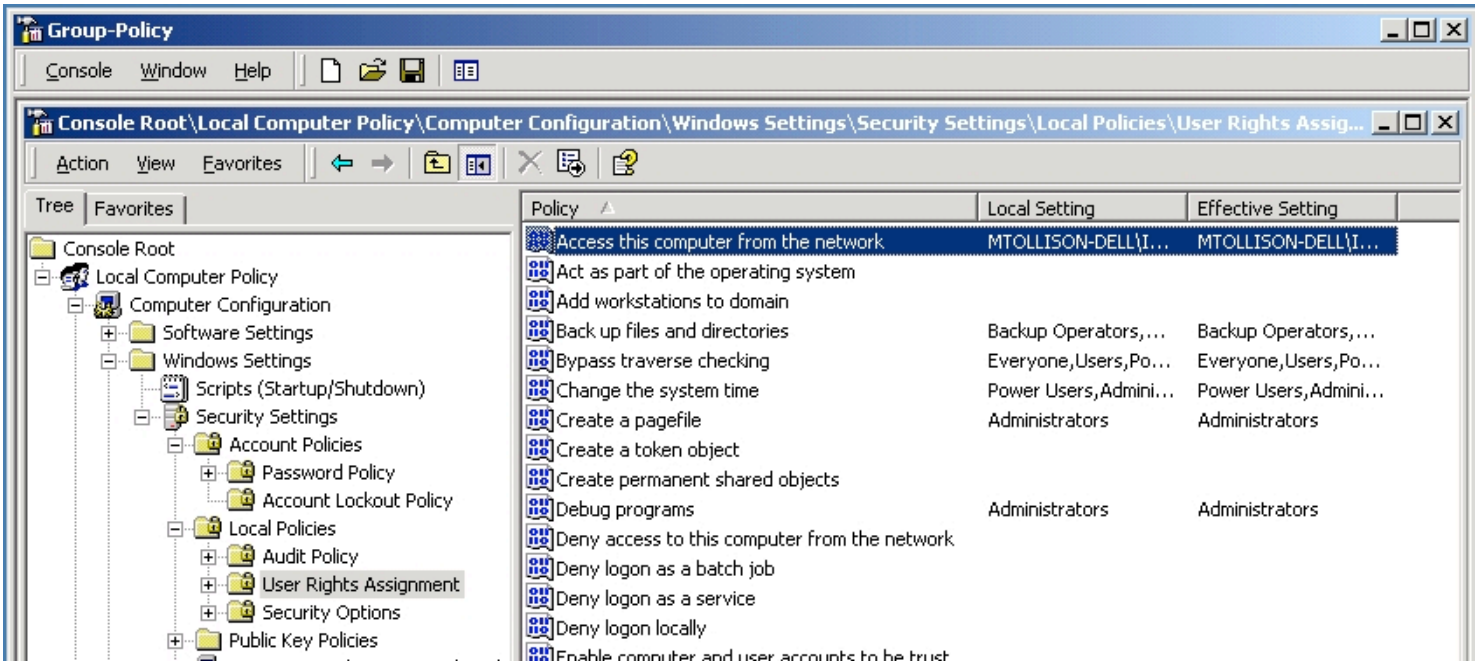
Once auditing is enabled on a system, it is very important to regularly review these files, understand the various types of events and investigate those events which are suspicious or not normal. Normal is a very relative term and will vary from system to system and dynamically change. Auditing, coupled with an effective intrusion detection strategy, will allow an administrator or security professional to better manage faults and intrusions. Various commercial and open source Intrusion Detection Systems (IDS) can be found. IDS systems are covered by other courses but one open source IDS system is SNORT [7].

Index

User Rights and Group Policy

What is a right? One definition is that rights are: "3. entitlement: an entitlement, freedom, or privilege to do something (often used in the plural) human rights" [8]. This same definition applies to the use of "User Rights" in the Windows 2000 operating system. The user is granted privileges to perform certain tasks or access certain files. Rights determine This is a key security features for many operating systems.

Earlier, the establishment of user and group accounts was discussed. It is within the "Group Policy" content that rights are assigned. Administration of rights becomes much easier when apply to a group rather than individual users. In Windows 2000, one tool for managing user rights and group policy is from another MMC snap-in, called Group Policy. Typing, mmc.exe, at the Run prompt, allows an administrator to add the snap-in to a console. The result of configuring the MMC console and viewing the User Rights Assignment is shown in Figure 18.



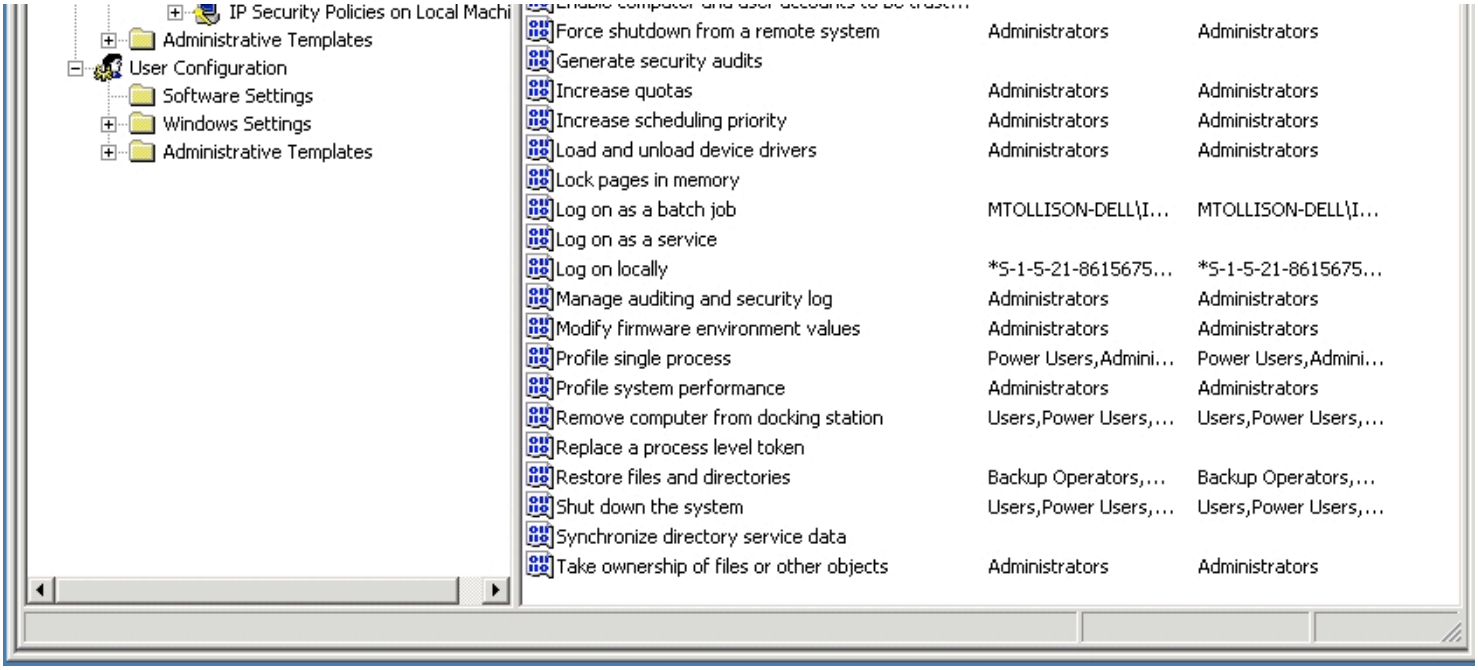


Figure 18.

As the display indicates, many security settings can be managed via the Group Policy tool. A thorough discussion of all the settings is beyond the scope of this paper. However, let's examine one setting, the case of "Access this computer from the network." Double clicking on the tool brings up the display shown in Figure 19.

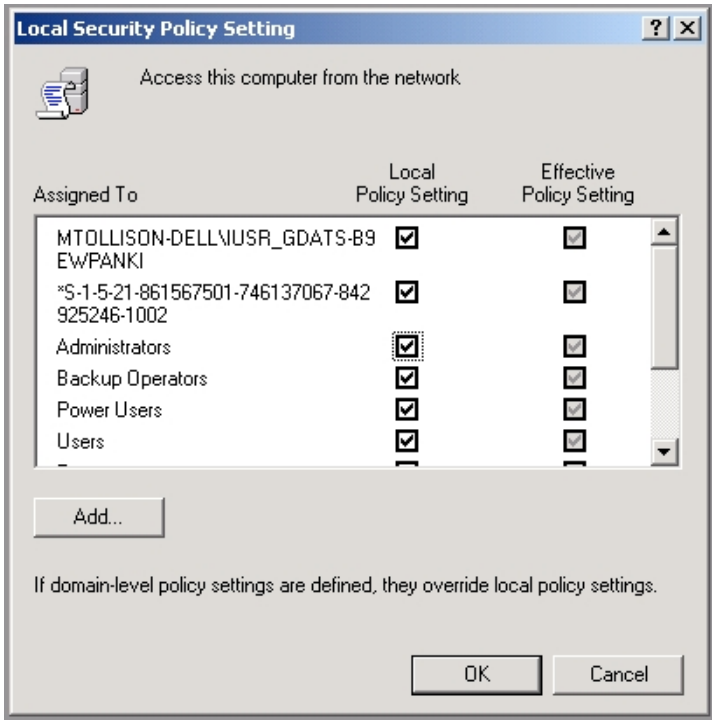


Figure 19.

Just by clicking, it is easy to select which users or groups are allowed to access the computer from the network. The Add feature allows the administrator to actively add new users or groups to access to this function. This is just one example of how user rights and group policy is used as part of the overall windows 2000 security system.

Index

Windows 2000 Resource Kits

In addition to the standard tools supplied with the operating system, Microsoft develops and markets "Resource Kits". Resource kits contain detailed explanations and setup of various system parameters. These resource kits are tailored to the different operating systems. In the case of Windows 2000, resource kits are available that discuss features of all versions of the operating system, Professional, Server, Advanced Server and Datacenter Server. Currently, the resource kits are included in two versions, Microsoft Windows 2000 Server Resource Kit and Microsoft Windows 2000 Professional Resource Kit. Also, other vendors, non Microsoft, develop and market resource kits for the Windows 2000 operating systems.

One key component of the resource kits are the inclusion of extra tools. The resource kit tools provide added benefit to the administrator for configuring or monitoring system parameters. The current resource tool kit includes over 200 tools. Upgrades and new tools can be obtained from the Microsoft home page.

A number of resource kit tools deal with administration and security monitoring of the various workstations and servers within a network. Listed below are a few chosen resource kit tools that might be of interest to a computer network or security administrator [3]. A detailed list of resource kit tools, as obtained from Microsoft[], is given in Appendix A.

Auditpol.exe: Audit Policy
AuditPol is a command-line tool that enables the user to modify the audit policy of the local computer or of any remote computer. To run AuditPol, the user must have administrator privileges on the target computer.

CyberSafe Log Analyst (NEW)

CyberSafe Log Analyst is a Microsoft® Windows® 2000 Security Event Log analysis tool. Designed as a snap-in to the Microsoft Management Console (MMC) used with Windows 2000, the CyberSafe Log Analyst assists you in organizing and interpreting security event logs from Windows 2000, providing more effective, system-wide user activity analysis.

Dumpel.exe: Dump Event Log

Dump Event Log is a command-line tool that dumps an event log for a local or remote system into a tab-separated text file. This tool can also be used to filter for or filter out certain event types.

Efsinfo.exe: Encrypting File System Information

This command-line tool displays information about files and folders encrypted with Encrypting File System (EFS) on NTFS partitions.

EFS is a feature of Windows 2000 that enables users to encrypt and decrypt files. This helps users keep files safe from intruders who might gain unauthorized physical access to their sensitive data (for example, by stealing a laptop or external disk drive).

In EFS, users work with encrypted files and folders just as they do with any other files or folders: encryption is transparent. If the EFS user is the same person who encrypted the file or folder, the system decrypts the file or folder when the user accesses it later. Unauthorized users or intruders, however, are prevented from accessing any encrypted files or folders.

You can also encrypt or decrypt a file or folder with the command-line tool cipher, which is included with the Windows 2000 operating system.

Elogdmp.exe: Event Log Query Tool

ElogDmp is a command-line tool that dumps information from a selected event log.

Using ElogDmp, you can display any of the following logs either locally or remotely: application, system and security. When used in conjunction with the FindStr.exe tool (in the %systemroot%\System32 directory), you can query for specific event log messages to display.
Any user on the network can use this tool to view the contents the application log on any remote computer on the network.

To view the contents of the system or security log on any remote computer you must be a Domain Administrator or be part of the local administrator's group on that computer.

Floplock.exe: Lock Floppy Disk Drives

FloppyLock is a service that allows you to control access to the floppy drives of a computer. This service can be used to help prevent unauthorized software installation or the introduction of viruses via floppy disks.

When the service is started on Windows 2000 Professional, only members of the Administrators and Power Users groups can access the floppy drives. When the service is started on Windows 2000 Server, only members of the Administrators group can access floppy drives.

FlopLock works by assigning a Discretionary Access Control List (DACL) to a floppy drive. When FlopLock has the floppy drives on a machine locked, only users in the Administrators group can use the floppy drive(s). If the FloppyLock service is configured to start automatically, the lock stays in place even after the computer is restarted.

Installing the FloppyLock service is a separate task you must perform after you install the Resource Kit tools.

Using FloppyLock is easy. Once the FloppyLock service is installed, starting

Showacls.exe

This command-line tool enumerates access rights for files, folders, and trees. It allows masking to enumerate only specific ACLs.

ShowACLs works on NTFS partitions only.

The most useful feature of ShowACLs is the ability to show permissions for a particular user. The method that ShowACLs uses to perform this is by enumerating the local and global groups that the particular user belongs to and matching the users security identifier (SID) and the SIDs of the groups the users belongs to, to the SIDs in each ACE entry.

NTFS uses Access Control Lists (ACLs) to set permissions for users and groups on objects. ACLs are made up of Access Control Entries (ACEs). Each ACE entry has information that controls the permissions for a specific user or group. There are currently four ACE type defined; Access Allowed, Access Denied, System Alarm and System Audit. Each ACE entry has a common ACE header and unique data structure. The SID associated with each ACE entry is contained in the data following the ACE header.

One of the problems with a command-line tool like ShowACLs is the amount of information that is contained in the ACL. The first version of ShowACLs attempted to display all the data in the access mask, which was very confusing. The latest version has adopted the "standard" permissions, Full, Change and Read-Only where appropriate. If a mask does not match these predefined values, the a raw dump of the mask is performed.

ShowAcls Topics

Showgrps.exe

This command-line tool shows the groups to which a user belongs, even within a given network domain.

Showmbrs.exe

This command-line tool shows the user names of members of a given group, even within a given network domain.

Showpriv.exe: Show Privilege

ShowPriv is a command-line tool that displays the users and groups granted a particular privilege. This tool must be run locally on the target computer or on a domain controller to display users and groups with domain privileges.

Tracedmp.exe: Trace Dump

TraceDmp is an event tracing command-line tool that produces a summary of event trace log items. TraceDmp processes either a trace log file generated by TraceLog or polls real time trace buffer data, and converts that information to a .csv file.

TraceDmp behaves like a WMI consumer. It takes the output from a TraceLog file, generally a .etl file, and converts it into a user-friendly format. This output provides you with a view event trace results.

TraceDmp gives you several ways to view event tracing data:

Summary.txt file: A summary of the events traced.
CSV (comma-separated format) file: Events traced are saved in chronologically sorted order. This gives you a more detailed view for each event.
Real time tracing: Tracedmp can also be used for real time event tracing. In this case, TraceDmp will read directly from the buffer instead of from a TraceLog file. The format and process is similar to that described for log files in "How TraceDmp Works" below.

Usrstat.exe

This command-line tool displays the user name, full name, and last logon date and time for each user in a given domain.

W2000events.mdb: Windows 2000 Events

This Access database file lists messages and related information from the Windows Event Log, an administrative tool that is part of Microsoft® Windows® 2000. This database contains the messages from the System, Security, and Application logs along with their corresponding Event ID, Source, and Type.

You must have Microsoft® Access installed on your computer to view this database. You might get a notice the first time the file is opened stating it is a read-only file. If file attributes need to be changed to allow writes, this can be done using Windows Explorer.

Whoami.exe

This command-line tool returns the domain or computer name and the user name of the user who is currently logged onto the computer on which the tool is run.

WhoAmI displays the complete contents of the access token (for example, of the current user's security context) on standard output (STDOUT). It displays the user name and security identifier (SID), the groups and their SIDs, the privileges and their status (for example, enabled or disabled) and the logon ID.

WhoAmI Topics

Xcacls.exe

This tool allows you to set all file-system security options accessible in Windows Explorer from the command line. XcAcls does this by displaying and modifying the access control lists (ACLs) of files.

XcAcls is especially useful in unattended installations of Microsoft® Windows® 2000 Professional or Server. With this tool, you can set the initial access rights for folders in which the operating system resides. When you distribute software to servers or workstations, XcAcls also offers one-step protection against deletion of directories or files by users

Index

Final Thoughts

I would be very neglect as I close this discussion of Windows 2000 security not to mention the importance of Active Directory (AD) and Kerberos Version 5. Both technologies are used to enhance the security and management of a Windows 2000 computer network.

Active Directory (AD) is a Lightweight Directory Access Protocol (LDAP) directory service that contains information about all objects in a Windows 2000 network. The Active Directory Service can be distributed among various sets of computers, or domains, and allows management of all people and resources within the network. Security is integrated with this directory service via authentication and access control. Many of the tools discussed in this paper can be used with the Active Directory. The configuration and management of the Active Directory is not trivial. A detailed understanding of the needed services and security requirements are needed before establishing a network using Active Directory. Additional information about the installation of Active Directory can be found from various Microsoft and third party vendor resources.

Kerberos Version 5 is a standard protocol used for handling authentication of users or systems. Kerberos involves the use of tickets for authentication and granting access to services. Because of increased security and ease of use, Kerberos replaces NT Lan Manager (NTLM) as the preferred network authentication protocol. Additional information about the kerberos can be found from various resources and from RFC-1510.

Index

Conclusion

As this paper indicates, Windows 2000 has a wealth of new security features and enhancements. However, security does not come without a price. The increased complexity of these new security features can impose a greater burden on the system or security administrator. However, this burden is easier to manage given the plethora of tools provided with Windows 2000. In this discussion, I only briefly touched on the main concepts and tool categories available. Hopefully, this discussion will have peaked your interest enough to explore these tools in more detail.

Index

References

[1] "Which Windows 2000 Is Best For You?" URL: http://www.microsoft.com/Windows2000/guide/choices.asp (25 April 2001)

[2] Cox, Philips and Sheldon, Tom. "Windows 2000 Security Handbook" 2001. Osborne/McGraw-Hill

[3] "Microsoft Windows 2000 Professional Resource Kit" 2000. Microsoft Press

[4] "A Losing Battle? Stolen Laptops Put Your Files in the Hands of Strangers" September 2000. URL: http://abcnews.go.com/sections/tech/DailyNews/laptops000919.html (25 April 2001)

[5] "Microsoft Windows 2000 Help", 2001. (25 April 2001)

[6] "NTFS Security --What's New in Windows 2000?" August 1999. URL: http://msdn.microsoft.com/library/periodic/period99/ntsf.htm (25 April 2001)

[7] Roesch, Martin "What is Snort?" URL: http://www.snort.org/what_is_snort.htm (25 April 2001)

[8] "Right." Microsoft Encarta - World English Dictionary. URL: http://dictionary.msn.com/find/entry.asp?search=rights

[9] "Windows 2000 Serve Resource Kit Tools" URL: http://www.microsoft.com/windows2000/library/resources/reskit/rktour/server/S_tools.asp

Index

Links of Interest

Windows 2000 Resource Kits Information - http://www.microsoft.com/windows2000/library/resources/reskit/default.asp

Microsoft Developer Network - http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/adsi/dsstartpage_8nqr.htm

Index

Appendix A.

Utility Description
A
Activeperl.exe: Active Perl Scripting Language C-like scripting language ported from UNIX to Windows 2000.

Addiag.exe: Application Deployment Diagnosis Provides information on current state of software either installed or available for installation on a PC managed by IntelliMirror Software Installation and Maintenance.

Addusers.exe: Add Users Adds multiple users from a comma-delimited text file.

Apimon.exe: API Monitor Monitors the API calls made by a process.

Associate.exe Adds "file extension, executable program" associations to the registry.

Atanlyzr.exe: AppleTalk network device ANaLYZeR Analyzes AppleTalk Devices.

Atmarp.exe: Windows ATM ARP Server Information Tool Used to troubleshoot the status of the ATM ARP/MARS Service that ships with Windows 2000.

Atmlane.exe: Windows ATM LAN Emulation Client Information Tool Used to troubleshoot the status of the ATM LAN Emulation (LANE) client that ships with Windows 2000.

Auditpol.exe: Audit Policy Enables user to modify the audit policy of local or remote computers

Autoexnt.exe: AutoExNT Service Allows you to start a custom batch file at startup without having to log on to that computer.

B

Browmon.exe: Browser Monitor Monitors the status of browsers on selected domains.

C

Cachemov.exe: Offline Files Cache Mover Allows user to move offline files cache to a different drive volume.

Cconnect.exe: Con-Current Connection Limiter Provides a method of tracking concurrent connection of users and monitoring what computers users are logged into.

Chklnks.exe: Link Check Wizard Scans all of the shortcut (link) files on a computer and lets user remove inactive ones.

Choice.exe: User Input for Batch Files Prompts user to make a choice in a batch program.

Cla.msc: Cybersafe Log Analyst Assists in organizing and interpreting security event logs from Windows 2000 by analyzing and generating detailed reports.

Clearmem.exe: Clear Memory Forces pages out of RAM.

Clip.exe: Clip To Clipboard Dumps STDIN to Clipboard

Clippool.exe: Clip Pool Transparently shares a single logical clipboard among multiple computers.

Cliptray.exe: Clipboard Organizer Stores and organizes chunks of text that can be copied into text-based files using the Clipboard.

Clusrest.exe: Cluster Quorum Restore Utility Restores the quorum disk of a cluster, which is not done by a restore process using NtBackup.

Cmdhere.exe: Command Prompt Here Adds a "CMD Prompt Here" item to some right-click menus displayed by Windows Explorer.

Compress.exe: File Compression Utility Compresses files.

Confmgr.htm: IP Multicast Conference Management Tool Manages IP Multicast conferences.

Counters.chm: Windows 2000 Performance Counters Reference Presents descriptions of all of standard performance counters installed with Windows 2000.

Cpustres.exe: CPU Stress Utility Consumes processor cycles continuously by executing an endless loop.

Creatfil.exe: Create File Creates files of a specified size.

Crystal Reports Enables you to create, view, and distribute presentation-quality or Web-ready reports from varied data sources.

Ctpc.exe: Third-Party QoS Control Agent Allows an administrator to manage Quality of Service (QoS), including Create, Remove, Update, and Query sessions, from the command prompt.

Ctrlist.exe: Counter List Lists all objects and counters installed in the system for the given language ID.

Cusrmgr.exe: Console User Manager Enables editing of many of the Local Users and Groups user properties from the command line.

D

Defptr.exe: Default Printer Shows a list of available printers and lets user easily select a default printer.

Delprof.exe: User Profile Deletion Utility Deletes Windows 2000 user profiles.

Delrp.exe: Delete File and Reparse Points Deletes a file or directory and any associated NTFS reparse points.

Delsrv.exe: Delete Service Unregisters a service with the service control manager.

Designed for Windows Logo Program Web site Describes the technical requirements that must be satisfied by an application to receive the Designed for Windows Logo.

Dh.exe: Display Heap Displays information about heap usage in a user-mode process or pool usage in kernel-mode memory.

Dhcmp.exe: DH Compare Compares two dumps of heap usage generated by Dh.exe, matching the backtraces from each file, to find leaks.

Dhcploc.exe: DHCP Server Locator Utility Locates DHCP servers on a network.

Dhcpobjs.exe: DHCP Objects In-process server (DLL) that exposes COM interfaces for automating DHCP Server administration.

Diruse.exe: Directory Disk Usage Determines amount of disk space used by a directory's contents, similarly to UNIX's DU.

Diskmap.exe Displays information about a disk and the contents of its partition table.

Diskpar.exe: Disk Alignment Tool Finds and modifies the starting sector on a disk to improve disk performance.

Diskuse.exe Scans a directory tree and reports the amount of space used by each user.

Dmdiag.exe Saves disk volume configuration to a text file and writes a signature to a disk partition.

Dommon.exe: Domain Monitor Monitors the status of servers and domain controllers for a domain and its trusted domains.

Drivers.exe: List Loaded Drivers Displays information on installed device drivers, their files, and their code.

Dumpcfg.exe: Dump Configuration Simplifies the manual system recovery process associated with storage configuration.

Dumpel.exe: Dump Event Log Dumps an Event Log to a tab-separated text file.

Dumpfsmos.cmd: Dump FSMO Roles Dumps the Floating Single Master Operations roles.

Dupfinder.exe: Duplicate File Finder Locates duplicate files for deletion or renaming.

Dureg.exe: Registry Size Estimator Shows how much data is stored in the registry, or in any registry subtree, key, or subkey.

E

Efsinfo.exe: Encrypting File System Information Displays information about encrypted files on NTFS partitions.

Elogdmp.exe: Event Log Dump Dumps information from a selected event log.

Empty.exe Frees the working set of a specified task or process.

Enumprop.exe: Enumerate Properties Dumps all properties set on any directory services object.

Exctrlst.exe: Extensible Performance Counter List Displays information on extensible performance counter DLLs installed on a computer.

Exetype.exe: Finding the Executable Type Identifies the operating-system environment and processor required to run a particular executable file.

Expand.exe: File Expansion Utility Expands compressed files.

Extract.exe: Extract Cabinet Extracts files from cabinet (.cab) files.

F

Filespy.exe: File Spy Allows users to monitor local and network drives to see what types of IRP and Fast I/O operation are running in the system.

Findgrp.exe: Find Group Gets a user's direct and indirect group memberships.

Floplock.exe: Lock Floppy Disk Drives Locks a computer's floppy disks so that only members of the Administrators and PowerUsers groups can access them.

Forfiles.exe Enables batch processing of files in a directory or tree.

Freedisk.exe: Free Disk Space Checks for free disk space, returning a 0 if there is enough space for an operation and a 1 if there isn't.

Ftedit.exe: FT Registry Information Editor Edits the registry for fault tolerance settings.

G

Getmac.exe: Get MAC Address Gets a computer's MAC (Ethernet) layer address and binding order.

Getsid.exe: Get Security ID Compares the security IDs of two user accounts.

Gettype.exe: Get Type Version Information Determines what kind of Windows operating system a computer is running and whether it is serving as a domain controller by querying the registry and setting ERRORLEVEL.

Global.exe: Global Groups Lists contents of global groups across domains and workstations.

Gp.chm: Windows 2000 Group Policy Reference Provides detailed descriptions of the group policies in Windows 2000, describing the effect of enabling, disabling, and not configuring each policy, as well as explanations of how related policies interact.

Gpolmig.exe: Group Policy Migration Migrates settings from Windows NT policy files to the Windows 2000 group policy object structure.

Gpotool.exe: Group Policy Objects Allows administrators to check Group Policy object integrity and monitor policy replication.

Gpresult.exe: Group Policy Results Displays information about the result Group Policy has had on the current computer and logged-on user.

Grpcpy.exe: Group Copy Copies the user names in an existing group to another group in the same or a different domain.

Guid2obj.exe: GUID to Object Maps a globally unique identifier (GUID) to a distinguished name.

H

Hardware Compatibility List Web site Lists Windows NT and Windows 2000-compatible hardware.

Heapmon.exe Enables user to view system heap information.

I

Ie5ntwa.exe: Internet Explorer Web Accessories Enhances Microsoft® Internet Explorer 5.

Ierk5.chm: Internet Explorer 5 Resource Kit Online version of the Internet Explorer 5 Resource Kit.

Ifmember.exe Checks whether a user is a member of a specified group.

Iisv5migrationutility_x86.exe: IIS Migration Wizard Migrates third-party Web servers and settings to Internet Information Server in Windows 2000.

Installation Monitor Tracks changes made by setup programs in the registry, .ini files, and other child processes.

Instsrv.exe: Service Installer Installs and uninstalls executable services and assigns names to them.

Internet Explorer 5 Administration Kit Enables administrators to create, distribute, and update customized installations of Internet Explorer.

Internet Scanner Network security scanner that generates comprehensive report detailing security vulnerabilities.

Inuse.exe: File-In-Use Replace Utility Performs on-the-fly replacement of files currently in use by the operating system.

Ipsecpol.exe: Internet Protocol Security Policies Tool Configures IP Security policies in the Directory Service or in a local or remote registry.

J

Javareg.exe: Java/COM Registration Utility Registers Java Classes, performing functions similar to Regsvr32.exe.

K

Kerbtray.exe Displays ticket information for a given computer running the Kerberos protocol.

Kernprof.exe: Kernel Profiler Provides counters for and profiles of various functions of the operating system kernel.

Kix32.exe: KiXtart 95 Processes logon scripts and provides an enhanced batch language.

Klist.exe Views and deletes the Kerberos tickets granted to the current logon session.

L

Lbridge.cmd: L-Bridge Command-line script that assists in migration from Windows NT 4.0 LMRepl to Windows 2000 File Replication Service.

Leakyapp.exe: Leaky Application Appropriates system memory to test performance in low-memory situations.

Linkd.exe Links an NTFS directory to a target object.

List.exe Displays and searches a text file.

Local.exe: Local Groups Lists contents of local groups across domains and workstations.

Logevent.exe: Event Logging Utility Logs events to a local or remote computer.

Logoff.exe Logs off a user.

Logtime.exe Logs start or finish times of programs running in a batch file.

M

Mcast.exe Sends multicast packets or listens for packets being sent to a multicast group address.

Mcopy.exe: Multiple Copy Copies files and creates a log of the operation.

Mibcc.exe: SNMP MIB Compiler Compiles Management Information Bases for Simple Network Management Protocol.

Moveuser.exe: Move Users Changes the security of a profile from one user to another, allowing for either the account domain or the user name to change.

Mscep.dll: Certificate Enrollment Module for Routers ISAPI filter for IIS that enables CEP Cisco Enrollment Protocol.

Msinfosetup.exe: Microsoft System Information Extensions Extensions used to view System Information Files created as .nfo files or Windows Report Tool-created .cab files within the System Information MMC snap-in.

Mtc.exe: Multiple Tree Copy Copies whole directory trees and their files.

Mtfcheck.exe: Microsoft Tape Format Verification Tool Verifies that tape media are Microsoft Tape Format compliant.

N

Netclip.exe: Remote Clipboard Viewer Shows contents of clipboards on local and remote computers and enables users to cut and paste data between them.

Netcons.exe: Net Connections Displays current network connections.

Netsvc.exe: Command-line Service Controller Remotely starts, stops, and queries the status of services over a network.

Nlmon.exe: NL Monitor Lists and tests domains and trust relationships.

Now.exe Echos the current date and time plus any arguments passed to it.

Ntdetect.com (Installd.com): Startup Hardware Detector Installs a debug version of Startup Hardware Detector used for troubleshooting hardware detection issues.

Ntimer.exe Measures how long a program runs.

Ntrights.exe Grants or revokes Windows 2000 rights to or from users or groups.

O

Oh.exe: Open Handles Shows the handles of open windows, processes or objects.

Oidgen.exe: OID Generator Generates a pair of base Object Identifier values for use in extending the Acive Directory schema.

Oleview.exe: OLE/COM Object Viewer Browses, configures, and tests Microsoft Component Object Model classes installed on a computer.

Os2api.txt: OS/2 API Information Describes which APIs for the OS/2 operating system are supported by Windows 2000 and which are not.

P

Pathman.exe: Path Manager Adds or removes components of the system or user path.

Perf2mib.exe: Performance Monitor MIB Builder Tool Creates Management Information Bases based on Performance Monitor counters.

Perfmon4.exe: Performance Monitor 4 Provides detailed data about system resources used by specific components of the operating system and programs designed to collect performance data.

Perfmtr.exe: Performance Meter Displays performance statistics in a text-based format.

Permcopy.exe: Permission Copy Copies file- and share-level permissions from one share to another.

Perms.exe: File Access Permissions per User Displays a user's access permissions for a file or directory.

Pfmon.exe: Page Fault Monitor Lists the source and number of page faults generated by an application's function calls.

POSIX Utilities Set of UNIX-like utilities recompiled to run on Windows NT and Windows 2000.

Prnadmin.dll: Printer Administration Objects Manages printers, printer drivers, and printer ports on local and remote computers.

Pstat.exe: Process and Thread Status Shows the status of all running processes and threads.

Ptree.exe: Process Tree Allows you to query the process inheritance tree and quit

processes on local or remote computers.

Pulist.exe Lists processes running on local or remote computers.

Q

Qgrep.exe Performs string search routines on files, much like the POSIX tool Grep.exe.

Qslice.exe: CPU Usage by Processes Shows the percentage of total CPU usage per process.

Qtcp.exe Measures end-to-end network service quality.

Quickres.exe: Quick Resolution Changer Changes display settings without restarting the computer.

Quiktray.exe: Quick Tray Organizes the icons in the status area of the Windows 2000 desktop.

R

Raslist.exe: RAS List Displays Remote Access Service server announces from a network.

Rasmon.exe: RAS Monitor Dispays detailed information on Remote Access Service connections.

Rasusers.exe: Enumerating Remote Access Users Lists Remote Access Service users on a domain or server.

Rdpclip.exe: File Copy Copies files between Terminal Services server and client.

Reducer.exe: Reduce Trace Data Processes one or more trace log files and produce a per-process, per-thread workload profile.

Regback.exe: Registry Backup Backs up all or part of the Registry.

Regdmp.exe: Registry Dump Dumps of all or part of the registry to standard output.

Regentry.chm: Technical Reference to the Windows 2000 Registry Explains registry entries in detail.

Regfind.exe Searches and optionally replaces registry data.

Regini.exe: Registry Change by Script Modifies registry entries with a batch file.

Regrest.exe: Registry Restoration Restores all or part of the registry.

Remapkey.exe: Remap Windows Keyboard Layout Changes keyboard layout by remapping the scancode of keys.

Remote Administration Scripts Visual Basic scripts for administering Active Directory through Active Directory Services Interface.

Remote Command Service (Rcmd.exe & Rcmdsvc.exe) Provides secure client and server for remotely running command-line programs.

Remote Console Enables a client to run a command-line session remotely on machines running the corresponding service.

Remote Process Kill Enumerates and kills processes on a remote computer

Robocopy.exe: Robust File Copy Utility Maintains multiple mirror images of large folder trees on network servers.

RPC Ping: RPC Connectivity Verification Tool Checks whether Windows 2000 Server services are responding to remote procedure call requests from network clients.

Rpcdump.exe: RPC Dump Dumps all the endpoints in the endpointmapper database, pings each endpoint, gathers some other information, sorts it, and outputs the data.

Rshsvc.exe: TCP/IP Remote Shell Service Provides a command-line shell or single command execution service for remote users.

Rsm_dbic.exe: Removable Storage Integrity Checker Checks the integrity of the RSM database for media and removable media drives and libraries.

Rsm_dbutil.exe: Removable Storage Database Utility Steps through the RSM database and inspects each database object attribute for valid values and referential integrity.

Rsmconfg.exe: Removable Storage Manual Configuration Wizard Aids in manually configuring libraries that RSM's autoconfiguration can't, from the command prompt.

RunExt: Run Extension Adds a Run command to the Windows Explorer context menu.

S

Sc.exe: Service Controller Tool Retrieves information about services from Service Controller.

Scanreg.exe: Registry Scan Searches for a string in registry key names, value names, and value data.

Sclist.exe Shows services and their status.

Setedit.exe: PerfMon Chart Setting Editor Edits Performance Monitor chart settings files.

Setspn.exe: Manipulate Service Principal Names for Accounts Manages the Service Principal Names directory property for an Active Directory account.

Setupmgr.exe: Setup Manager Generates answer files for unattended installations or upgrades on multiple computers.

Setx.exe Sets environmental variables in the the user or computer environment.

Showacls.exe: Show ACLs Enumerates access rights for files, folders, and trees.

Showdisk.exe: Show Disk Space Displays configuration and fault-tolerance information for primary partitions and logical drives.

Showgrps.exe: Show Groups Shows the groups to which a user belong.

Showmbrs.exe: Show Members Shows the user names of members of a group.

Showperf.exe: Performance Data Block Dump Utility Dumps the contents of the Performance Data block so you can view and debug the raw data structure.

Showpriv.exe: Show Privilege Displays the users and groups granted a particular privilege on the local computer.

Shutdown.exe: Remote Shutdown Shuts down or reboots a local or remote computer.

Sipanel.exe: Soft Input Panel Allows computers to use a pen device for input.

Sleep.exe: Batch File Wait Causes a computer to wait for a specified amount of time.

Smart Sketch LE Technical drawing and diagramming application.

Snmpmon.exe: SNMP Monitor Monitors Simple Network Management Protocol variables for multiple nodes and logs them to a database.

Snmputil.exe: SNMP Browser Queries a Simple Network Management Protocol host or community for Management Information Base values from command prompt.

Soon.exe: Near-Future Command Scheduler Schedules commands to run within the next 24 hours.

Srvany.exe: Applications As Services Utility Enables applications to run as services.

Srvcheck.exe: Server Share Check Lists shares on a computer and enumerates the access-control lists for each one.

Srvinfo.exe: Server Information Displays network, disk drive, and service information about a local or remote server.

Srvinstw.exe: Service Installation Wizard Installs and deletes services and device drivers on a local or remote computer.

Srvmgr.exe: Server Manager Manages Windows NT 4.0 or Windows NT 3.51 domains and computers.

Su.exe Enables a user to run a process in the security context of a different user.

Subinacl.exe Migrates security information between users, groups and domains.

Support Online Web site Helps users find troubleshooting information, downloads, and technical support on the Web.

Svcacls.exe: Service ACL Editor Sets access-control lists on service objects.

Svcmon.exe: Service Monitoring Tool Monitors services on local or remote computers and notifies the administrator when their status changes.

Sysdiff.exe: Automated Installation Tool Pre-installs applications as part of an automated setup.

Sysprep.exe: System Preparation Utility Automates the cloning of a customized configuration of Windows 2000 to multiple computers.

Sysscansetup.exe: System Scanner Scans sytems and generates comprehensive report detailing security vulnerabilities.

T

Takeown.exe Cleans up multiple boot drives without formatting the drive.

Terminal Server Capacity Planning Tools Suite of tools that assist organizations with Windows 2000 Terminal Services capacity planning.

Textview.exe: Text Viewer Displays contents of multiple text files on local or shared drives.

Timeout.exe Pauses execution of a command for a specified period.

Timestmp.sys: QoS Time Stamp Provides kernel mode time-stamping support for Qtcp.exe.

Timethis.exe Times how long it takes to run a given command.

Timezone.exe: Daylight Saving Time Update Utility Updates daylight saving time information in the registry for a time zone.

Tlocmgr.exe: Telephony Location Manager Configures telephony locations and properties for portable computers.

Top.exe: Time-Ordered Processes Lists processes that are using the most processor time.

Totlproc.exe: Total Processors Counter that measures the memory usage of all installed processors.

Tracedmp.exe: Trace Dump Processes a trace log file or real time trace buffers and converts them to a .csv file.

Traceenable.exe Enables tracing and displays current tracing options.

Tracelog.exe Starts, stops or enables trace logging.

Typeperf.exe: Performance Data in the Command Window Displays real-time data from Performance Monitor counters in a command window.

Tzedit.exe: Time Zone Editor Creates and edits time-zone entries for the Date/Time option in Control Panel.

U

Unattend.doc: Unattended Setup Parameters Guide Provides detailed information on how to automate Windows 2000 installation through the use of answer files.

Uptime.exe Displays system uptime, events and statistics.

Usrmgr.exe: User Manager for Domains Manages security for Windows NT 4.0 domains, member servers, and Windows 2000 Professional computers.

Usrstat.exe: User Statistics Lists user names, full names, and last logon date and time for all user accounts in a domain.

Usrtogrp.exe: Add Users to a Group Adds users to a group from a text file.

V

Vadump.exe: Virtual Address Dump Shows the state and size of each segment of virtual address space.

Vfi.exe: Visual File Information Retrieves and generates detailed information on files, such as attibutes, version, and flags.

W

W2000events.mdb: Windows 2000 Events Lists Event Log messages and related information.

W2000msgs.chm: Windows 2000 Error and Event Messages Help Provides explanations of Windows 2000 error messages.

Waitfor.exe Synchronizes a task across multiple computers.

Wdsbm.exe: Who Is Designated Subnet Bandwidth Manager? Identifies the ACS SBM that manages the segment to which a specific host is attached.

Where.exe Locates files on a hard disk or network.

Whoami.exe Returns the domain or computer name and user name of the user who is currently logged on.

Windows NT 4.0 OEM Support Tools Set of Kernel extensions and related debugging tools for Windows NT 4.0

Winexit.scr: Windows Exit Screen Saver Logs off the current user after a specified time has elapsed.

Winrpsdk15.doc: Windows Report Tool Deployment Software Development Kit Documents Windows Report Tool, which provides a means for uploading system information and a request for assistance over the Internet or an intranet to a helpdesk or support center.

Winschk.exe Checks inconsistencies in Windows Internet Name Service databases and verifies replication activity.

Winscl.exe: WINS Administration Tool Manages Windows Internet Name Service activities and databases.

Wperf.exe: Perf Monitor Monitors performance and presents data a little differently than Performance Monitor.

X

Xcacls.exe Displays and modifies security options for system folders.