Windows 2000
Security Configuration Guide

Version 1.0

October 4, 2002

Prepared For:

Microsoft Corporation

Corporate Headquarters

One Microsoft Way

Redmond, WA 98052-6399

Prepared By:

Science Applications International Corporation

7125 Gateway Drive

Columbia, MD 21046

This Page Intentionally Left Blank

Windows 2000 Security Configuration Guide

Version 1.0, 10/04/2002

1. Introduction

Welcome to the Microsoft Windows 2000 Security Configuration Guide. This document provides guidance to allow for the secure installation and configuration of Windows 2000 in accordance with the Windows 2000 Common Criteria Security Target (ST).

The Windows 2000 Common Criteria Security Target, henceforth referred to as the Windows 2000 ST, provides a set of security requirements taken from the Common Criteria (CC) for Information Technology Security Evaluation. The Windows 2000 product was evaluated against the Windows 2000 ST and found to satisfy the ST requirements.

This document is targeted at those responsible for ensuring the installation and configuration process results in a secure configuration. For the purposes of this document, a secure configuration is one that enforces the requirements presented in the Windows 2000 ST, henceforth referred to the Evaluated Configuration.

Audience Assumptions

This document assumes the audience is familiar with the general installation process of Windows 2000 and the configuration tools provided by Windows 2000 to adjust the configuration settings.

Document Overview

This document has the following chapters:

Chapter 1, “Introduction”, introduces the purpose and structure of the document and the assumptions of the audience.

Chapter 2, “Hardware and Software Overview”, identifies the hardware and software included in the Evaluated Configuration.

Chapter 3, “Operating System Installation”, describes how to install the Evaluated Configuration of Windows 2000.

Chapter 4, “Secure Configuration”, describes how to configure Windows 2000 into the Evaluated Configuration of Windows 2000.

Chapter 5, “Windows 2000 Common Criteria Secure Configuration Templates” describes how to partially automate the configuration of the Evaluated Configuration of Windows 2000 with the application of configuration templates.

Chapter 6, “References” provides the references used to develop this document.

Appendix A, “Windows 2000 Default Security Policy Settings”, identifies the Windows 2000 default security policy settings (prior to the application of the procedures that result in the Evaluated Configuration of Windows 2000).

Appendix B, “Audit Categories and Events”, presents the Windows 2000 system audit events that correspond to the events required to be auditable by the Windows 2000 ST.

Appendix C, “User Rights and Privileges”, identifies the default user rights assignments on Windows 2000, defines their applicability to the Windows 2000 ST, and provides change requirements and recommendations necessary to comply with the Windows 2000 ST.

Appendix D, “User and Group Accounts”, identifies the default user and group accounts on Windows 2000, defines their applicability to the Windows 2000 ST, and presents changes to the accounts necessary to comply with the Windows 2000 ST.

Appendix E, “Windows 2000 Security Configuration Checklist for the Evaluated Configuration” presents a configuration checklist to ensure all necessary installation and configuration steps are taken to result in the Evaluated Configuration of Windows 2000.

Appendix F, “Windows 2000 Security Configuration Templates for the Evaluated Configuration” presents the configuration templates to support the automation of the required changes to the default settings to allow for the configuration of the Evaluated Configuration of Windows 2000. Additionally, the appendix presents the configuration templates to support the automation of the required and recommended changes to the default settings.

Terminology and Conventions

Throughout the document, the following terminology and conventions are followed:

Evaluated Configuration: used to refer to the configuration of Windows 2000 that was evaluated and determined to meet the Windows 2000 ST.

Warnings: warnings are provided to highlight text that is critical to consider in ensuring the system is secure. Warnings are identified with the bolded word Warning (e.g. “**Warning**”).

Notes: text that is important to take notice of is identified with a bolded word “Note” or “Notes” (e.g. **Note**).

Mandatory settings: when referring to setting policy or security options, if a policy or option must be set to a specific value to meet the Windows 2000 ST the setting is identified as a “Required” setting.

Recommended settings: when referring to setting policy or security options, if it is not necessary for a policy or option to be set to a specific value to meet the Windows 2000 ST, however, a specific value represents good security practice, then the setting is identified as a “Recommended” setting.

2. Hardware and Software Environment

This section defines the hardware and software requirements for the Evaluated Configuration.

General Hardware Configuration

Set Power-On Password

On many hardware platforms, the system can be protected using a power-on password. A power-on password prevents unauthorized personnel from starting an operating system other than Windows 2000, which would compromise system security. Power-on passwords are a function of the computer hardware, not the operating system software. Therefore the procedure for setting up the power-on password depends on the type of computer, and is available in the vendor's documentation supplied with the system.

Restrict the Boot Process

Most personal computers support the ability to start a number of different operating systems. For example, even if users normally start Windows 2000 from the C:\ drive, someone could boot another operating system from removable media on another drive, such as a floppy disk drive or a CD-ROM drive. If this happens, any security precautions taken to secure the Windows 2000 operating system might be circumvented.

For a secure system, install only one version of Windows 2000 on the C:\ partition or drive and do not install any other operating systems on the computer (do not make the computer multi-boot capable). The CPU also needs to be physically protected to ensure that no other operating system is loaded. Depending on particular configuration circumstances, the floppy disk drive or drives may be removed. In some computers setting switches or jumpers inside the BIOS can disable booting from the floppy disk drive. If hardware settings are used to disable booting from the floppy drive, the computer case should be locked (if that option is available with the computer) or the machine can be locked in a cabinet with a hole in the front to provide access to the floppy disk drive. If the CPU is in a locked area away from the keyboard and monitor, drives cannot be added or hardware settings changed for the purpose of starting from another operating system.

Enable Hardware BIOS Protection

Protect the BIOS configuration of each Windows 2000 computer with a BIOS setup password. On many hardware platforms, opening the case and clearing the BIOS through a set of jumpers or by removing the motherboard battery can disable the BIOS password. To prevent this, protect the hardware as described above in the "Restrict the boot process" subsection.

Evaluated Hardware Configuration

The evaluated hardware configuration includes the following platforms configured as shown:

- Dell PE 2500
- Dell PE 6450/550
- Dell PE 2550
- Dell PE 1550
- Dell Optiplex GX400
- Compaq Proliant ML570
- Compaq Professional Workstation AP550
- Compaq Proliant ML330

Evaluated Software Configuration

The Evaluated Configuration of Windows 2000 includes the Windows 2000 Professional, Server, and Advanced Server products configured in any one of the roles shown in the table below and in accordance with the installation and configuration instructions provided in this document. For further information regarding the specific security requirements met by Windows 2000, see the Windows 2000 Security Target.

Product	Role
Microsoft Windows 2000 Advanced Server	Domain Controller Domain Member Server Workgroup Member Server Stand-Alone
Microsoft Windows 2000 Server	Domain Controller Domain Member Server Workgroup Member Server Stand-Alone
Microsoft Windows 2000 Professional	Domain Member Workgroup Member Stand-Alone

It is important to understand the difference between a domain and a workgroup environment. The main difference been a domain and a workgroup is that workgroup environments use decentralized administration. This means that every computer must be administrated independently of the others. Domains use centralized administration, in which administrators can create one domain account and assign permissions to all resources within the domain to that one central user or group of users. Centralized administration requires less administration time and provides a more secure environment. In general, workgroup configurations are used in very small environments that do not have security concerns. Larger environments and environments that must have tight security on data should use a domain configuration. Basic definitions are provided below.

- **Domain**. A collection of computers defined by the administrator of a Windows 2000 Server network that share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains and represents a single security boundary of a Windows 2000 computer network.
- **Workgroup**. A logical grouping of networked computers that share resources, such as files and printers. A workgroup is sometimes referred to as a peer-to-peer network because all computers in the workgroup can share resources as equals, without a dedicated server. Each Windows 2000 Server and Professional computer in a workgroup maintains a local security database, which contains a list of user accounts and resource security information specific to that computer.
- **Domain Controller**. For a Windows 2000 Server domain, the server that authenticates domain logons and maintains the security policy and the security accounts master database for a domain. Domain controllers manage user access to a network, which includes logging on, authentication, and access to the directory and shared resources.
- **Workgroup Member**. A Windows 2000 Server or Professional computer that is a member of a Windows 2000 workgroup, formed as a logical grouping of networked computers for the purpose of sharing resources.
- **Domain Member**. A Windows 2000 Server or Professional computer that is a member of a Windows 2000 domain environment.
- **Stand-Alone**. Standard desktop, such as a Windows 2000 Professional computer, or Server computer that is not connected to any network as either a domain or workgroup member.

3. Operating System Installation

This section provides the initial installation procedures for the Windows 2000 Professional, Server, and Advanced Server operating systems.

Preparing for Installation

During Installation, the Setup program will ask for information on how to install and configure Windows 2000. Prepare for the Windows 2000 operating system installation by collecting hardware information and establishing configuration decisions prior to initiating the installation process. The following checklist provides some guidelines as to the information that needs to be defined prior to initiating the installation process.

Table 3.1 Windows 2000 Pre-Installation Checklist

	Description
❑	**Hardware Compatibility:** Review all hardware to ensure compatibility with the Windows 2000 operating system and, if desired, the Evaluated Configuration hardware configuration. Hardware components include: Motherboard, network adapters, video card, sound card, CD-ROM drives, etc. The Windows 2000 Hardware Compatibility List (HCL) can be found at: http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/
❑	**Disk Space:** Ensure the system has sufficient disk space. The minimum disk space recommended for installation of Windows 2000 is 2 gigabytes (GB).
❑	**Disk Partitions:** Determine disk-partitioning requirements, keeping in mind the minimum disk space recommendations for installation of the Windows 2000 operating system. It is recommended that the operating system for Evaluated Configuration platforms be installed on the primary disk partition.
❑	**File System:** The file system must be configured as NTFS in order to allow configuration of the evaluated security mechanisms and conformance to the ST requirements.
❑	**Licensing Mode:** Select the desired licensing mode. The two modes are per-server and per-seat. The mode can be switched from per-server to per-seat after installation, but not from per-seat to per-server. The "Select a licensing mode for Windows 2000 Server and Advanced Server" subsection provides a description of the two licensing modes.
❑	**Computer Name:** Determine the name to be used by the new computer. If the computer is to be a member of any Windows network environment, its name must be unique within the network.
❑	**Network Membership:** If the computer is to become part of a network, determine the type of network group the computer will join. The computer can either be in a Domain or a Workgroup. If it will be joined to a Domain, the Domain name is needed and a computer account needs to be created within the Domain for the new computer. The computer account can be created prior to installation or it can be created during the installation process with an appropriate Domain administrator account and password. The "Join a domain or workgroup" subsection provides descriptions for Domain and Workgroup.
❑	**Installation Method:** Determine whether the Windows 2000 operating system will be installed from Setup boot disks, CD-ROM, or over-the-network. Procedures provided in this document describe installations from boot disks or from CD-ROM.
❑	**Service Components:** Prior to installation, determine the services that will be required for the installed operating system. For server installations, considerations may include Active Directory, DNS, WINS, or DHCP. A list of evaluated services that may be used in an Evaluated Configuration installation is provided in the "Evaluated Configuration System Services" subsection.

Windows 2000 Installation Process

Installation Methods

Windows 2000 can be installed as either an upgrade to an existing Windows operating system or as a new operating system installation. To ensure the Evaluated Configuration the Windows 2000 operating system must be the only operating system on the computer and must be installed on a clean partition. That is, any previous operating system must be wiped clean from the all hard disk partitions within the computer prior to installing Windows 2000.

There are three methods available to install the Windows 2000 operating system:

- Setup boot disks
- CD-ROM
- Over-the-network

This section describes the installation of Windows 2000 via setup boot disks or CD-ROM.

> **Note:** An over-the-network installation shall not be used for the Evaluated Configuration, as it requires the use of an existing operating system such as Windows 9x, Windows Me, Windows NT, or MS-DOS.

The setup boot disk installation method requires the use of four setup floppy disks. The setup boot disk method of installation will be required if the computer on which the operating system is to be installed does not support the bootable CD-ROM format.

The CD-ROM installation method requires configuration of the computer's motherboard BIOS to detect and boot from a bootable Windows 2000 installation CD.

The subsections that follow provide procedures for initiating the installation of Windows 2000 from either the setup boot disks or a bootable CD-ROM.

Initiating the Installation from Setup Boot Disks

If the computer on which the Windows 2000 operating system is to be installed does not support booting from a CD-ROM, it will be necessary to use the setup boot disk method of installation. If Windows 2000 setup disks are not already available, they can be created on another computer from the installation CD-ROM.

Creating Setup Startup Disks

If the original setup boot disks are not available, new ones can be created as follows:

1. Obtain four blank, 1.44 MB formatted 3.5-inch disks. Label them "Setup Disk 1," "Setup Disk 2," "Setup Disk 3," and "Setup Disk 4." Indicate on each of the disks whether they are for Windows 2000 Server or for Windows 2000 Professional.
2. Use a second working computer running a Windows operating system to create the setup boot disks.
3. Insert the disk labeled "Setup Disk 1" into the floppy disk drive, and insert the Windows 2000 operating system CD into the CD-ROM drive.

4. Click **Start**, and then click **Run**. Otherwise open an MS-DOS Command prompt.
5. At the prompt, type the following command, replacing the **d:** and **a:** drive letters with the appropriate letter of the CD-ROM drive and floppy disk drive of the computer being used:

   d:\bootdisk\Makeboot.exe a:

6. Follow the instructions that appear.

Start Setup from the Boot Disks

Once Setup is started from the boot disks, it works in several stages, prompting for insertion of specific boot disks and the CD-ROM, requesting information, copying files, and restarting.

Start Setup from the setup boot disks as follows:

1. With the computer turned off, insert "Setup Disk 1" into drive A: of the computer.
2. Turn on the computer.
3. Follow the Setup instructions on the screen. The text mode installation phase that will follow is explained below in the "Text Mode Installation Phase."

Initiating the Installation from a Bootable CD-ROM

Using a bootable CD-ROM is the simplest method of initiating the Windows 2000 Setup program, given that the computer's motherboard BIOS supports this capability. Once the Setup program is started, it works in several stages, prompting for information, copying files, and restarting.

Start Setup from a bootable CD-ROM as follows:

1. Insert the CD-ROM in the drive.
2. Restart the computer and wait for Setup to display a dialog box.
3. Follow the Setup instructions on the screen. The text mode installation phase that will follow is explained below in the "Text Mode Installation Phase" subsection.

Text Mode Installation Phase

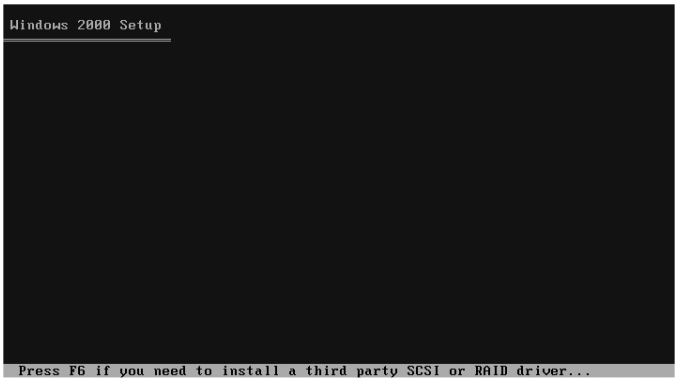
This subsection provides details for the text mode installation phase of the Windows 2000 operating system. This installation phase is similar for either boot disk or CD-ROM installation, with the exception that the boot disk installation will prompt the user whenever the next setup disk is required. Once the setup phase has been initiated, the setup process will begin as follows:

1. Setup will begin by first inspecting the computer's hardware. The screen will display the message "Setup is inspecting your computer's hardware configuration…"
2. The screen will then move on to an interactive stage, where the first interaction will depend on whether there are third party SCSI or RAID drivers required by the hardware. If a third party SCSI or RAID driver is required press the **F6** key on the keyboard. Otherwise, allow the setup process to continue and proceed to **Step 8**.

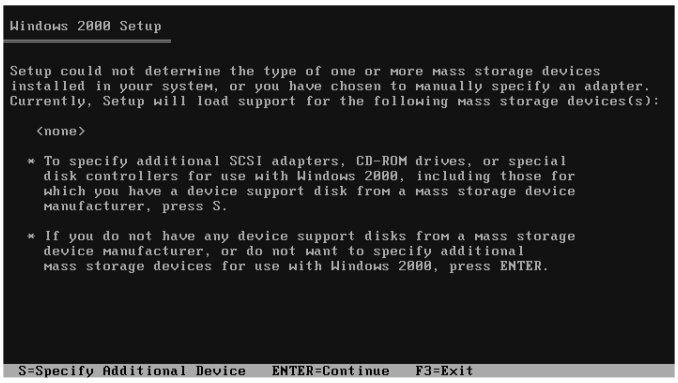
   Note: When installing Windows 2000 on a new computer, or on a computer containing the latest SCSI or IDE controller technology, it may be necessary to use an OEM device driver to support the new mass storage controller in order to continue with the installation. This is done by pressing the **F6** key as described above. Otherwise, Windows Setup

may stop with the following message if the controller is not properly detected when booting from the Installation Floppy Disks or CD-ROM:

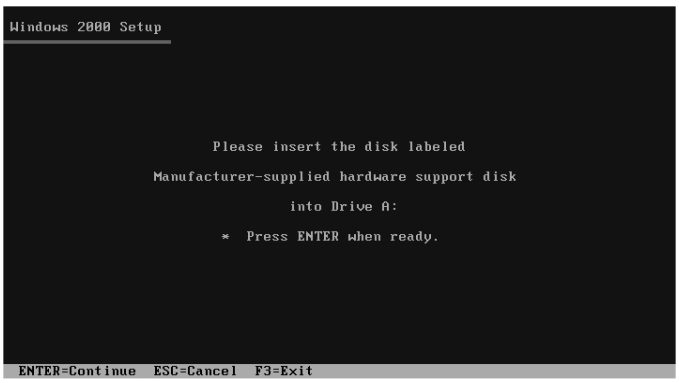
> Setup did not find any hard disk drives installed in your system



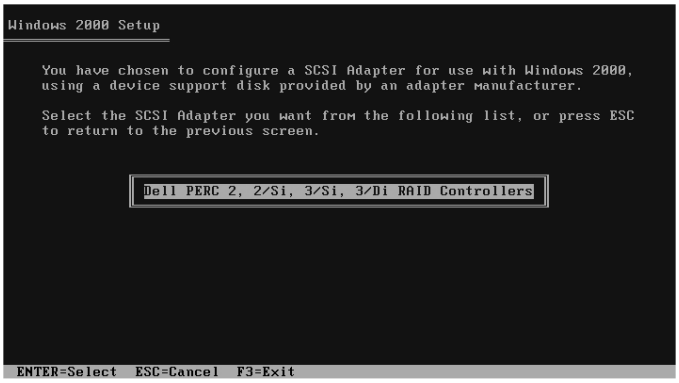
3. If the **F6** key is pressed, the setup process will proceed to loading files until it reaches the stage where it requires the third party driver.
4. When setup reaches the stage where it requires the third party driver, it will provide the following interactive display:



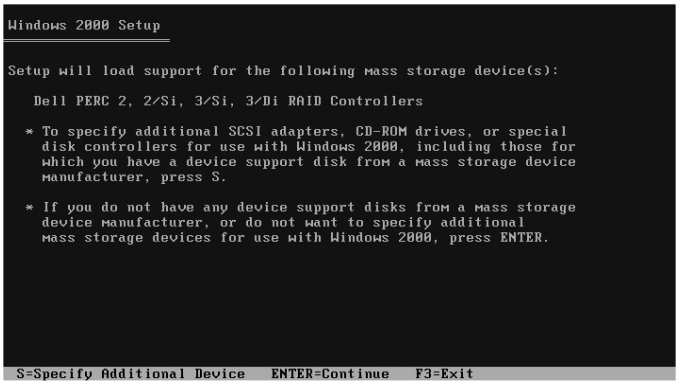
5. Pressing the **S** key on the keyboard will cause Setup to search the A: drive for a driver. If there is no disk in the drive, the following interactive display will appear:



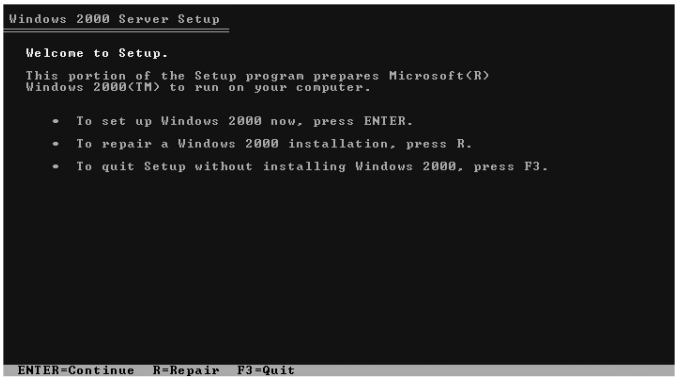
6. Place the disk containing the manufacturer supplied driver in drive A: and press the **ENTER** key on the keyboard to continue. Setup will read the information on the floppy disk and will display the available driver choices as shown below.



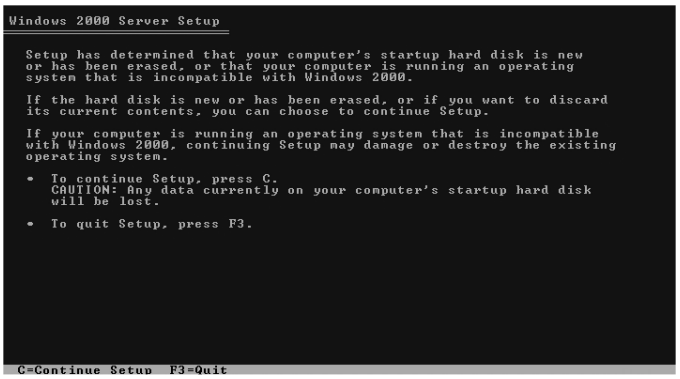
7. Make sure the proper driver is selected and press the **ENTER** key on the keyboard to continue. Setup will begin loading the selected driver. A confirmation of the selected driver will be shown in an interactive display. If additional drivers are to be installed, press the **S** key on the keyboard, otherwise press the **ENTER** key on the keyboard to continue.



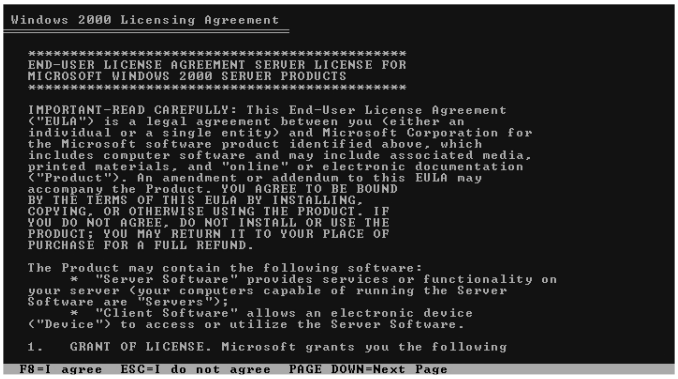
8. Setup will continue loading files for a short period of time. Once the necessary files have been loaded, a message will appear for a brief moment stating; "**Setup is starting Windows 2000**." In the interactive display that follows the user has the option of selecting whether to setup Windows 2000 (install), repair an existing installation, or exit the Setup process. Press the **ENTER** key on the keyboard to continue.



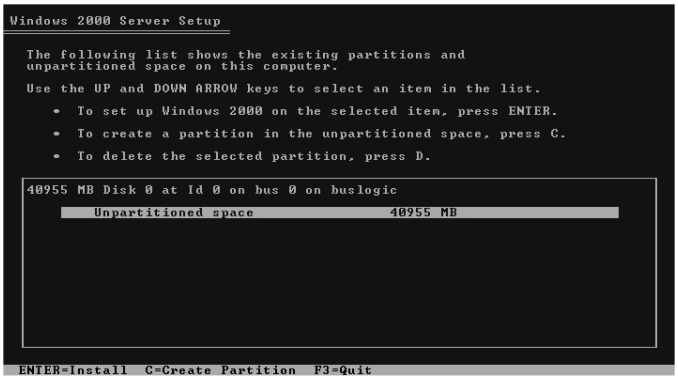
9. If the hard disk on which the operating system is being installed is new and unformatted, or if there is an operating system on the hard disk that the Windows 2000 Setup process cannot recognize, an interactive display will appear informing the user of this fact. The user then has the option of continuing with the Setup by pressing the **C** key on the keyboard quitting the Setup by pressing the **F3** key on the keyboard. Read the caution information in the display and press the **C** key on the keyboard to continue if it has been determined that it is safe to do so. Otherwise, press the **F3** key on the keyboard and make appropriate configuration changes or backup measures before restarting the Setup process again.



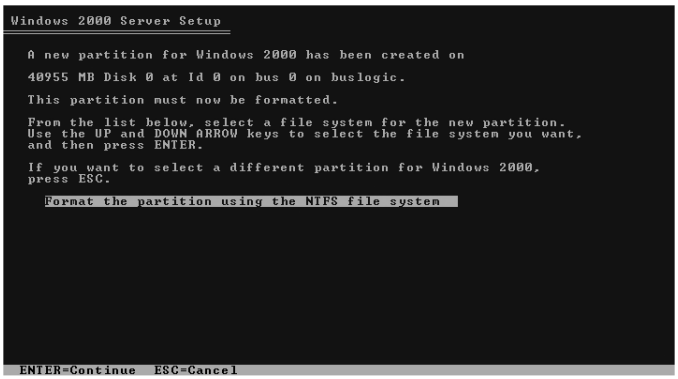
10. The **Windows 2000 Licensing Agreement** will appear in an interactive display. User the **PAGE DOWN** key on the keyboard to scroll through the text while reading it. After reading the Licensing Agreement, make sure the page has been scrolled all the way to the bottom and press the **F8** key on the keyboard to agree with the **Windows 2000 Licensing Agreement** and continue with the installation.



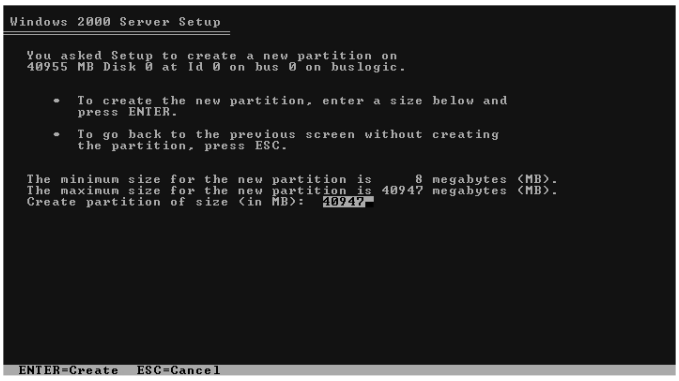
11. The next interactive display will show the existing hard disks and partitions that are available in the computer. If there are multiple partitions or multiple hard disks they will be identified in the interactive display. Any unpartitioned space on the disk will need to be partitioned and formatted before it can be used. The interactive display example below shows a 40 Gigabyte Hard disk that is not partitioned. To use all of the existing unpartitioned space, press the **ENTER** key on the keyboard and continue at **Step 12** of these procedures. In order to partition the disk for use press the **C** key on the keyboard and proceed to **Step 13**.



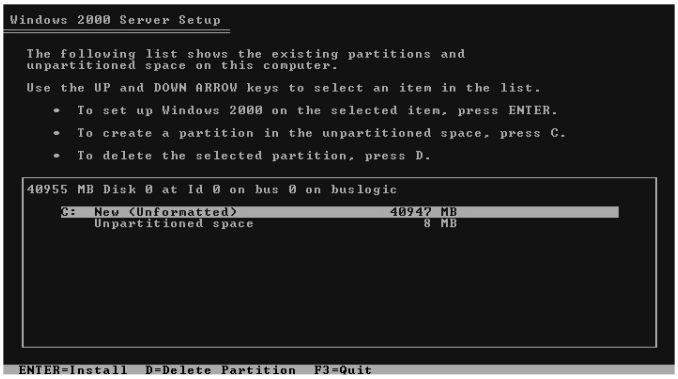
12. The interactive display shows that the new partition was created and must be formatted. To format the partition press the **ENTER** key on the keyboard and proceed to **Step 16**.



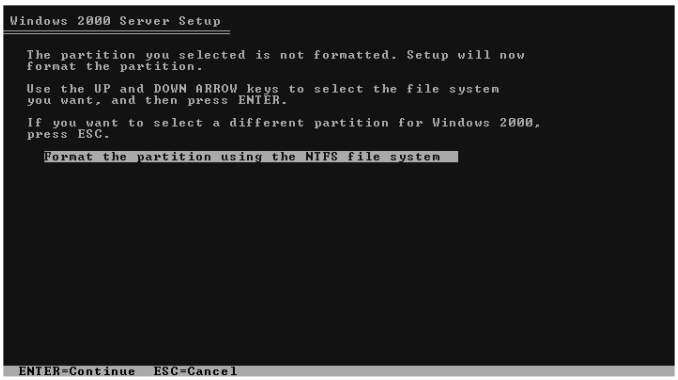
13. If selecting to create a partition, the next interactive display will provide the ability to define the size of the new partition. The default size selected will be the full amount of the unpartitioned space that was previously selected. Either reduce the size for the required partition from the number shown on the screen, or accept the default. Press the **ENTER** key on the keyboard to accept the settings and proceed.



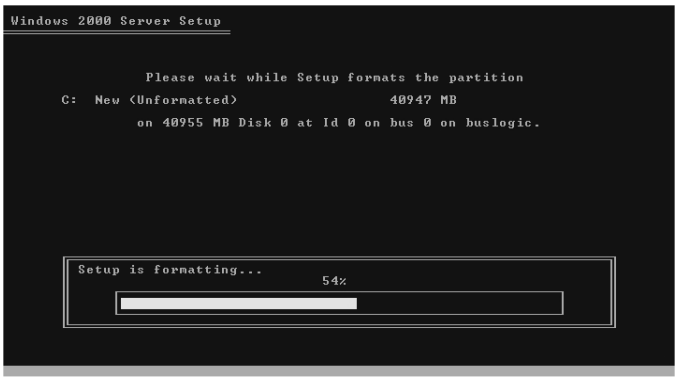
14. The interactive display will once again show the available disk partitions. This time it will display the new partition that is available for installation. Select the newly created partition and press the **ENTER** key to proceed with the installation.



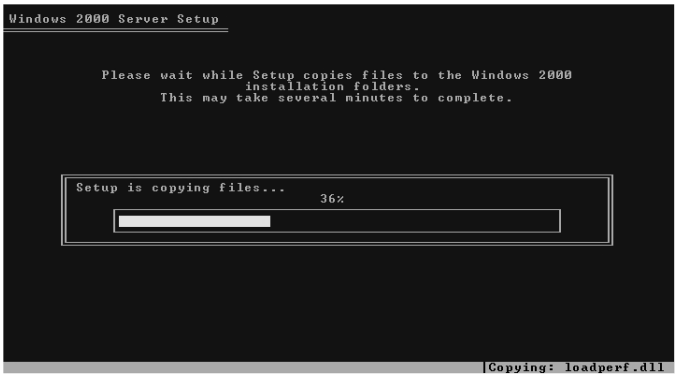
15. The interactive display will present the options for formatting the selected partition. The Evaluated Configuration requires the use of NTFS. Select **NTFS** and press the **ENTER** key on the keyboard to continue.



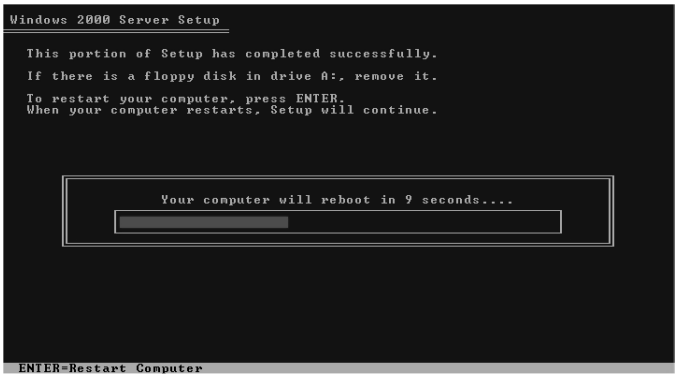
16. Windows 2000 Setup will start formatting the partition.



17. Once formatting is completed, Windows 2000 Setup will examine the disks and then proceed to copy the necessary operating system files to the hard disk.



18. When all files have been copied to the hard disk, Windows 2000 Setup will restart the computer. Make sure to remove any disk from the floppy drive. Allow Setup to count down to the restart, or press the **ENTER** key on the keyboard to restart the computer.



19. When the Computer reboots, the installation will continue in the GUI mode. The GUI mode installation phase is explained in the subsection that follows.

GUI Mode Installation Phase

This subsection addresses several of the key installation settings that are called for during the GUI mode phase of the Setup process. This phase allows selection of optional components to install and allows the setting of the Administrator password. There are a series of dialog boxes that Windows 2000 will use to collect configuration information for setting up the operating system. Most of the sample screen shots and dialog boxes presented in this subsection are based on a Windows 2000 Advanced Server installation. However, the setup process described also applies to Window 2000 Server and Professional product installations, unless otherwise specified.

GUI Mode Start Up Process

Once the Windows 2000 Setup completes its text mode installation phase, the computer will reboot and begin the GUI Mode phase of the installation.

1. The Windows GUI mode will begin by displaying the appropriate startup background for Windows 2000 Professional, Server, or Advanced Server.

2. A **Windows 2000 Setup Wizard** will appear. Click the **Next** button to continue, or wait a few seconds and the Wizard will start on its own.

3. The **Windows 2000 Setup Wizard** will begin by automatically detecting and installing hardware devices. This may take a few minutes and the screen may flicker during the process. During this process, the **Next** button on the **Installing Devices** setup window will be inactive. When this process completes, the **Regional Settings** dialog box will appear.

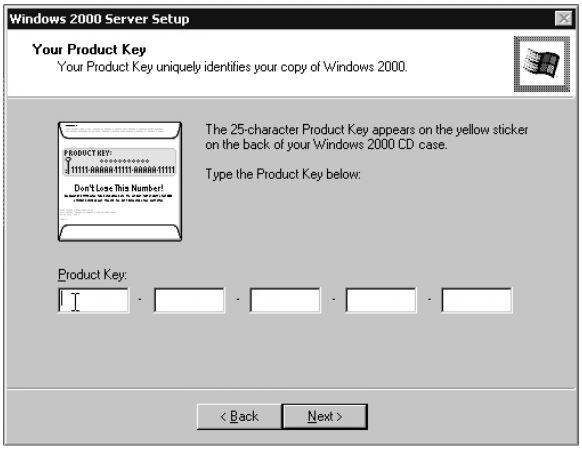
Specify regional options, name, product key, and licensing mode

The initial dialog box will allow configuration of regional settings. The default setting will be displayed; this will most likely be shown as **English (United States)**. The next two dialog boxes will allow entering a user and organization name and the preferred licensing mode.

1. In the **Regional Settings** dialog box, verify or change the default settings for language, locale, and accessibility settings. Click the **Next** button to continue.

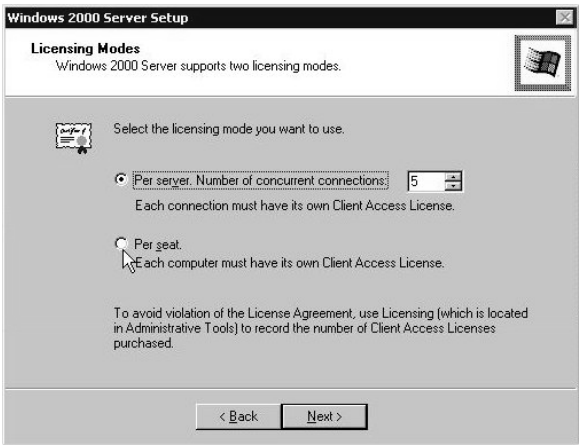
2. In the **Personalize Your Software** dialog box, type the user name and, optionally, the name of an organization. Click the **Next** button to continue.

3. In the **Your Product Key** dialog box, enter the 25-character product key for the Windows operating system being installed. Click the **Next** button to continue.



Select a licensing mode for Windows 2000 Server and Advanced Server

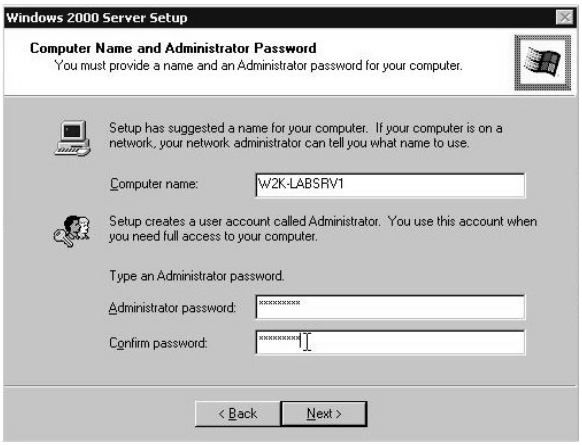
In the **Licensing Modes** dialog box, select the client-licensing mode, either Per seat or Per Server. If unsure of which mode to use, select Per Server because a change is allowed once from Per server to Per seat at no cost. A description of the **Licensing Modes** is provided below. Once the licensing mode is selected, click the **Next** button to continue with Setup.



- **Per Server**. Per server licensing means that each concurrent connection to this server requires a separate Client Access License (CAL). This means that at any one time, this Windows 2000 Server can only support a fixed number of connections. For example, if the Per server client licensing mode is selected with five concurrent connections, this Windows 2000 Server could only have five computers (clients) connected at any one time. Those computers would not need any additional licenses.
- **Per Seat**. If the Per seat mode is chosen, each computer that accesses a Windows 2000 Server will require a separate CAL. With one CAL, a particular client computer can connect to any number of Windows 2000 servers. This is the most commonly used licensing method for companies with more than one Windows 2000 Server.

Assign a computer name and Administrator account password

The **Computer Name and Administrator Password** dialog box provides a means of naming the computer so that it may be recognized on the network by a distinct name, and setting the password for the default Administrator account. The requirements and procedures for computer names and administrator passwords are provided in the subsections that follow.



Computer name

Enter a computer name in the **Computer Name and Administrator Password** dialog box. The recommended length for most languages is 15 characters or less. It is recommended that only Internet-standard characters be used in the computer name. The standard characters are the numbers 0 to 9, uppercase and lowercase letters from A to Z, and the hyphen (-) character. If Microsoft DNS Service is used on the network, a wider variety of characters can be used, including Unicode characters and other nonstandard characters such as the ampersand (&). However, using nonstandard characters might affect the interoperability of any non-Microsoft software on the network.

The maximum length for a computer name is 63 bytes. If the name is longer than 15 bytes (15 characters in most languages, 7 characters in some), pre-Windows 2000 computers will recognize this computer by the first 15 bytes of the name only. In addition, there are additional configuration steps for a name longer than 15 bytes.

Note: If this computer will be part of a domain, choose a computer name that is different from any other computer in the domain.

Administrator password

The Windows 2000 Setup program creates a user account on the computer called Administrator that has administrative privileges for managing the overall configuration of the computer. The Administrator account is intended for the person who manages this computer. For security reasons, it is necessary to specify a password for the Administrator account. Leaving **Administrator password** blank indicates no password for the account.

1. In the **Computer Name and Administrator Password** dialog box, next to **Administrator password**, type a password of up to 127 characters. For the strong password security, use a password of at least 8 characters, and use a mixture of uppercase and lowercase letters, numbers, and other characters such as *, ?, or $.

   Note: The Evaluated Configuration requires a minimum password length of 8 characters.

2. In **Confirm password**, type the password again.
3. Click **Next** to continue with Setup.

For security reasons, it is recommended that a strong password be assigned to the Administrator account.

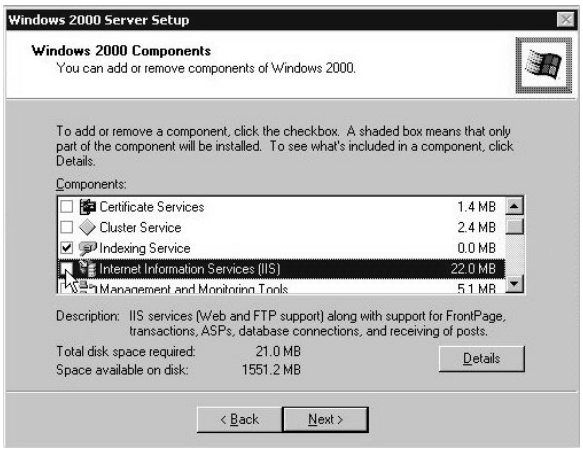
The password typed in **Confirm password** must exactly match the password typed in **Administrator password**. Take special care to remember and protect the password.

> **Note:** After Setup is completed, for best security, change the name of the Administrator account (it cannot be deleted) and keep a strong password on the account at all times.

Choose service components for Windows 2000 Server and Advanced Server

In the **Windows 2000 Components** dialog box, select the necessary components for the server being installed. This dialog box allows addition or removal of components during installation.

1. Components often needed on networks that use TCP/IP include DHCP, DNS, and WINS. To select these components, in the **Windows 2000 Components** dialog box, select the **Networking Services** check box, click **Details**, and then select the component or components needed. Subcomponents of networking services that must not be selected for the Evaluated Configuration include: **COM Internet Services Proxy, Internet Authentication Service**, **QoS Administration Control Service**, **Simple TCP/IP Services**, and **Site Server ILS Services**.
2. For server installations, **Indexing Service**, **Internet Information Service (IIS)**, and **Script Debugger** are selected for installation by default in the **Windows 2000 Components** dialog box. However, the Evaluated Configuration must not have these components installed. Therefore, unselect the **Indexing Service**, **Internet Information Service (IIS)**, and **Script Debugger** from the **Components:** window.



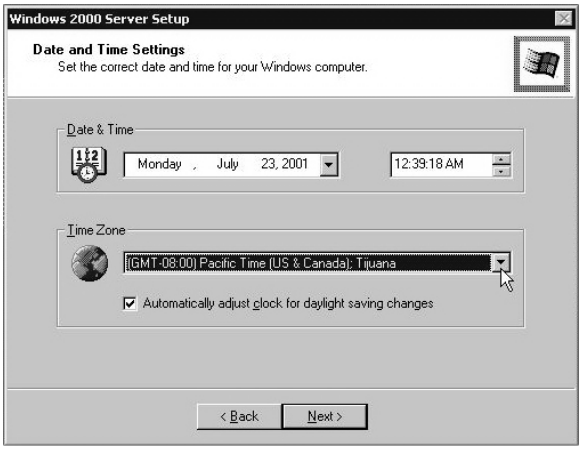
3. Click **Next** to continue with Setup.

If Setup is completed and it is later decided that other components are needed, they can be added at a later time. To do this, after running Setup, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**. In Add/Remove Programs, click **Add/Remove Windows Components**.

Set the date and time

The **Date and Time Settings** dialog box allows selection of the appropriate time zone and adjustment of date and time settings, including the ability to set automatic adjustments for daylight savings time.

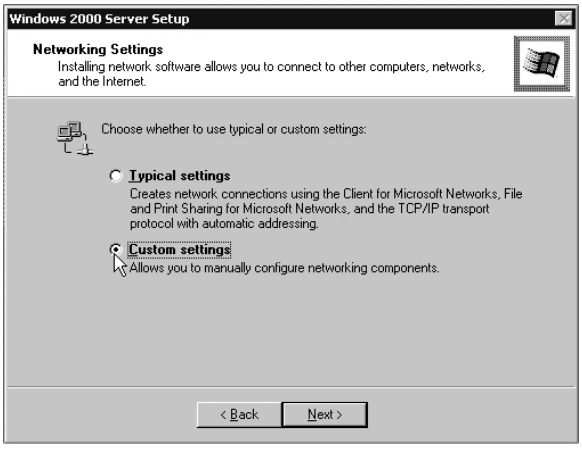
1. During Setup, in the **Date and Time Settings** dialog box, set the date, time, and time zone.



2. Set the system to automatically adjust for daylight saving time by selecting the **Automatically adjust clock for daylight saving changes** check box.
3. Click **Next** to continue with Setup. Windows Setup will begin installing networking software.

Configure network settings

The **Networking Settings** dialog box allows setting the configuration options for connecting to other computers, networks, and the Internet. Select either **Typical settings** or **Custom settings** based on the information gathered obtained from the network administrator. If uncertain, select **Typical settings** at this stage as it may be changed later.



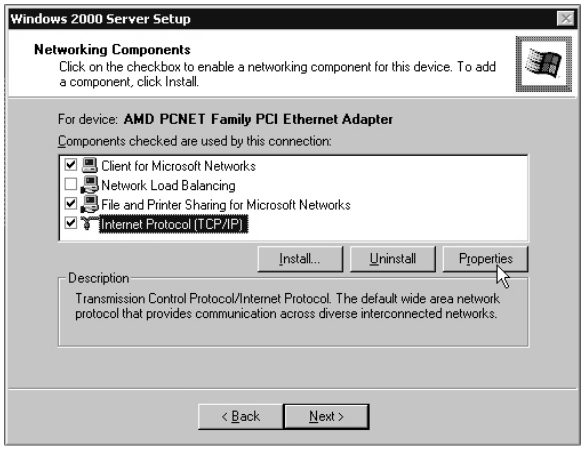
- **Typical Settings**. When the **Typical settings** radio button is selected in the **Networking Settings** dialog box, Windows 2000 Setup checks to see if there is a Dynamic Host Configuration Protocol (DHCP) Server within the domain. If there is a DHCP server, that server provides the IP address. If there is no DHCP server within the domain, Automatic IP

Addressing (APIPA) assigns an IP address. APIPA provides automatic IP address assignment for computers on networks without a DHCP server. A Windows 2000 Professional – based client assigns itself an IP address from a reserved class B network (169.254.0.0 with the subnet mask of 255.255.0.0), which cannot directly communicate with hosts outside this subnet, including Internet hosts. This option is most suitable for small, single-subnet networks, such as a home or small office.

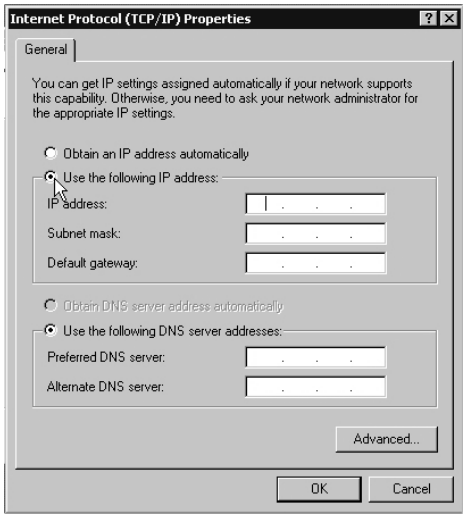
- **Custom settings**. When the **Custom settings** radio button is selected in the **Networking Settings** dialog box, Windows 2000 Setup will open the **Networking Components** dialog box to allow customized configuration of network components including the selection of dynamic or static IP address and networking information.

For Evaluated Configuration installations, either static or dynamic IP addresses may be assigned. All servers should have a static IP address. To specify a static local IP address and settings needed for DNS and WINS:

1. In the **Networking Settings** dialog box, select the **Custom settings** radio button and click the **Next** button to continue.
2. In the **Networking Components** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.



3. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Use the following IP address**.



4. In **IP address** and **Subnet mask**, type the appropriate numbers. (If appropriate, specify the **Default gateway** as well).
5. Under **Use the following DNS server addresses**, type the address of a preferred DNS server and, optionally, an alternate DNS server. If the local server is the preferred or alternate DNS server, type the same IP address as assigned in the previous step.
6. If a WINS server will be used, click **Advanced**, and on the **WINS** tab, click **Add** to add the IP address of one or more WINS servers. If the local server is a WINS server, type the IP address assigned in step 5.
7. Click **OK** in each dialog box, and click **Next** in the **Networking Components** dialog box continue with Setup.

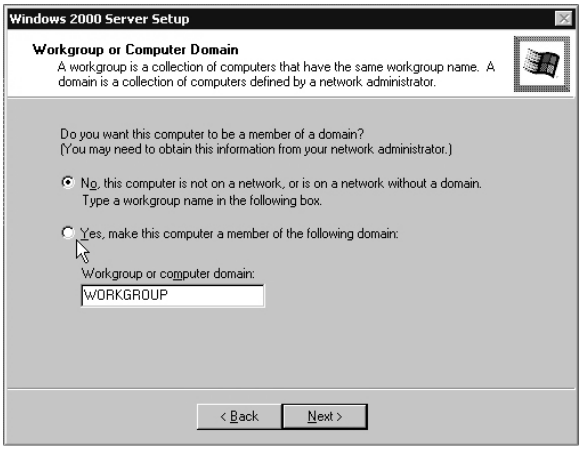
Join a domain or workgroup

The **Workgroup or Computer Domain** dialog box allows the option of joining a workgroup or a domain.

1. Select to join a workgroup or a domain by selecting either the **No, this computer is not on the network**… radio button for a workgroup, or the **Yes, make this computer a member of the following domain**: radio button for a domain.

Note: If the computer is a server that is to become the first Domain Controller for a Domain, select the No, this computer is not on the network… radio button. The server can be converted later to a Domain Controller, as instructed in the "Convert Windows 2000 Server to a Domain Controller" subsection.

2. Enter the name of the workgroup or domain in the **text** box and click the **Next** button to continue with Setup.
3. Windows Setup will install all the previously defined Windows 2000 components.
4. Click the **Finish** button to reboot the computer.



- **Workgroup**. A workgroup is one or more computers with the same workgroup name. Any user can join a workgroup. If the computer will not be joining a network, specify that it will be part of a workgroup. To join a workgroup, provide an existing or new workgroup name.
- **Domain**. A domain is a collection of computers defined by a network administrator for security and administrative purposes. Check with the network administrator to determine the proper domain name information required for joining the domain. Joining a domain requires a

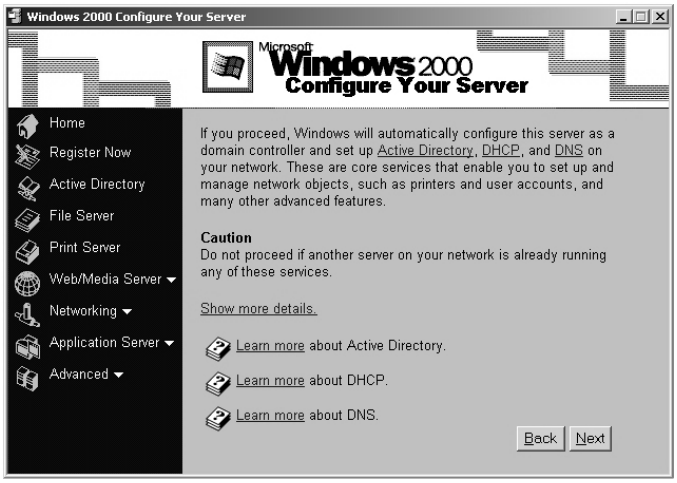
computer account in the specified domain. Ask the network administrator to create a computer account in the domain prior to proceeding with Setup. Otherwise, have an authorized administrator create the account and join the domain during Setup.

Windows 2000 Server and Advanced Server Configuration Options

When the Setup wizard completes the installation of Windows 2000, the computer restarts. Setup has now performed the basic installation. For Windows 2000 Server and Advanced Server installations, the **Configure Your Server** program, which appears on the screen if logged on as the computer's administrator, makes further configuration easy. At this point Windows 2000 Server can be registered and configured as needed.

The initial Server choices page provides three options for configuring the server:

- **This is the only server on my network**. Selecting this option and clicking the **Next** button will present a page informing the administrator that Windows will automatically configure the server as a Domain Controller if the administrator chooses to proceed. To proceed and configure the server as a Domain Controller click the **Next** button and follow all subsequent directions. Otherwise, click the **Back** button and select another option.



- **One or more servers are already on my network**. Selecting this option and clicking the **Next** button will present the administrator with the **Configure Your Server** page. From this page, the administrator can choose from any of the options on the left hand column for step-by-step instructions in configuring the server as required.

- **I will configure this server later**. Selecting this option and clicking the **Next** button will present the administrator with the **Configure Your Server** page just as explained with the previous option.

Start **Configure Your Server** at any time by clicking **Start**, pointing to **Programs**, pointing to **Administrative Tools**, and then clicking **Configure Your Server**. The configuration options available through the **Configure Your Server** program are listed in Table 3.2.

Table 3.2 Server Service Configuration Options

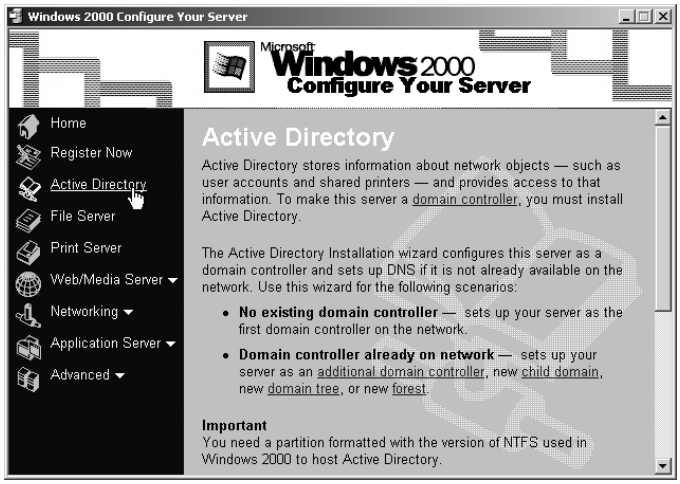
Icon	Elements
	**Active Directory** User accounts, Domains, server roles, permissions, and other security functions.
	**File Server** Shared folders and other shared network resources.
	**Print Server** Printers, printer queues, and other elements related to printing.
	**Web/Media Server** Web sites, multimedia sites, FTP sites, and other functionality. To use these services, appropriate components in Windows 2000 Server must be installed.
	**Networking** Protocols, remote access, and routing.
	**Application Server** Component Services and related support for applications distributed across a network; also includes Terminal Services.
	**Advanced** Windows 2000 Resource Kit support tools and optional components such as Remote Installation.

Convert a Windows 2000 Server to a Domain Controller

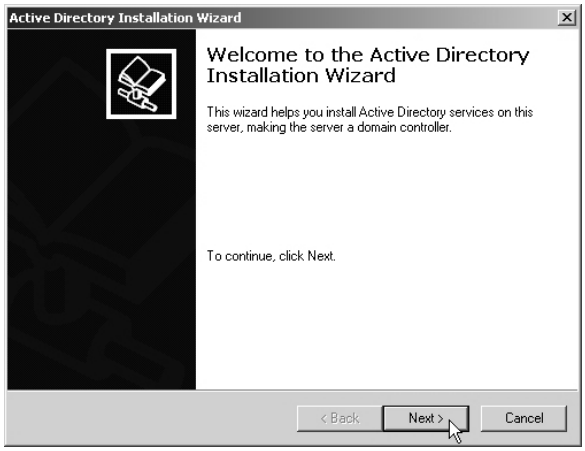
To configure a Domain Controller after a server installation has been completed and after either the **One or more servers are already on my network** or the **I will configure this server later** options have been selected as mentioned above, use the following procedures:

1. Log on as an administrator (if not already logged on).
2. If the **Configure Your Server** page is not open, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click on **Configure Your Server**.
3. From the left hand column of the **Configure Your Server** page, click **Active Directory**.

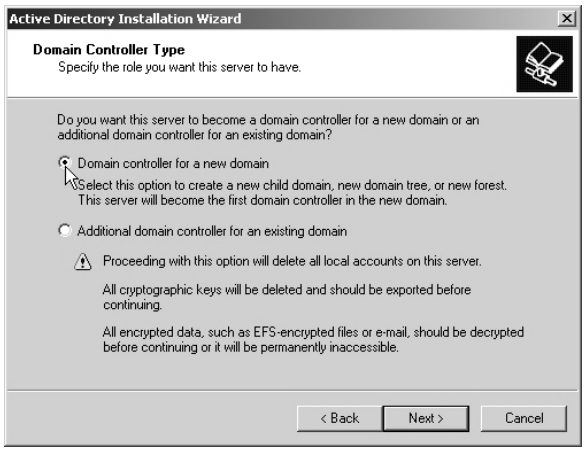
4. The **Active Directory** page will appear with important information about configuring Active Directory. Read the information and scroll down to the bottom of the page to click on the **Start the Active Directory Wizard** link.



5. The **Active Directory Installation Wizard** will appear. Click the **Next** button to continue.



6. Select whether the server will be a Domain Controller for a new Domain or whether it will be an additional Domain Controller within an existing Domain and click the **Next** button (be sure to read the warning message on selection of the later).



7. Follow all the subsequent instructions from the **Active Directory Installation Wizard** to complete the configuration of the Domain Controller.

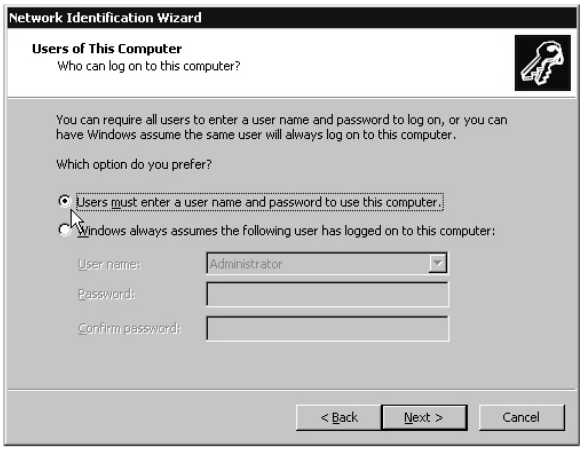
Note: During the Domain Controller configuration process through the **Active Directory Installation Wizard**, a dialog window will appear labeled **Permissions**. On this dialog window, the **Permissions compatible with Windows 2000 servers** radio button must be selected.

Windows 2000 Professional Network Identification Wizard

When the Setup wizard completes the installation of Windows 2000, the computer restarts. Setup has now performed the basic installation. For Windows 2000 Professional installations, the **Network Identification Wizard** will appear on the screen. The wizard is used to select the option of either requiring a user name and password every time someone logs on to the computer or allowing the computer to automatically log a specified user onto the computer upon startup. For the Evaluated Configuration users must be required to enter individual user names and passwords in order to access the computer and the network. Configure this network identification requirement as follows:

1. At the **Welcome to the Network Identification Wizard** window, click the **Next** button to continue.

2. The Users of this Computer window will appear. Select the radio button for the **Users must enter a user name and password to use this computer** option. Click the **Next** button to continue.



3. Click the **Finish** button to close the **Network Identification Wizard**. The **Windows 2000 Professional logon** window will appear.

Windows 2000 Service Packs and Hotfixes

Windows 2000 Service Packs for Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server provide the latest updates for the Windows 2000 operating systems. These updates are a collection of fixes in the following areas: application compatibility, operating system reliability, security, and setup. Each Service Pack update is cumulative, including all the updates contained in previous Windows 2000 Service Packs.

Windows 2000 post Service Pack Hotfixes provides product updates to address specific issues that may occur between Service Pack builds. All Hotfixes are generally rolled into each successive Service Pack build. For example, Windows 2000 Service Pack 3 contains all the updates in Service Pack 2 plus all of the post Service Pack 2 Hotfixes. The Evaluated Configuration must be configured with Service Pack 3 installed, along with the Q326886 Post

Service Pack 3 Hotfix that resolves the “Flaw in Network Connection Manager” security vulnerability in Windows 2000.

Windows 2000 Service Pack Encryption

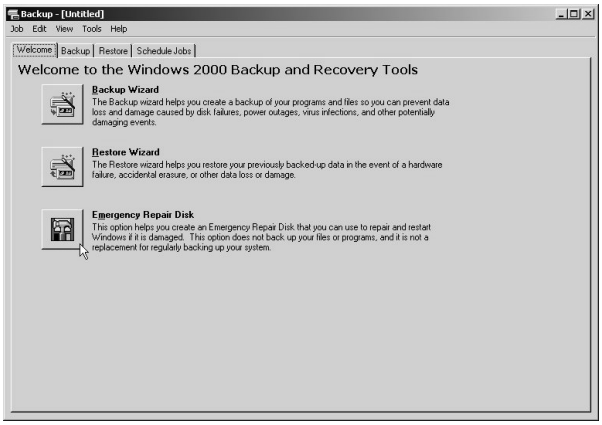
Windows 2000 Service Packs 2 and higher support high encryption (128-bit) as a default, and will automatically upgrade the operating system from standard encryption (56-bit) if it has not been upgraded already. It is not possible to disable or uninstall this feature. If the Service Pack is removed after installation, the operating system will continue to use 128-bit encryption; it will not revert to back to 56-bit encryption.

Windows 2000 Service Packs 2 and higher add high encryption support for all Windows 2000 encryption-based services, including Kerberos, Encrypting File System, RAS, RPC, SSL/TLS, CryptoAPI, Terminal Services RDP, and IPSec. High encryption support is intended to improve the security of stored data and online transactions, as well as any other content shared over networks or the Internet.

Recommended Actions Prior to Installing Service Pack and Hotfix Updates

Before installing any Service Pack or Hotfix updates:

1. Close all applications.
2. Update the Emergency Repair Disk (ERD):
    - Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then select **Backup**.



    - On the **Welcome** tab, click **Emergency Repair Disk**.
    - In the **Emergency Repair Diskette** window, choose **Also back up the registry to the repair directory to save the current registry files in a folder called \RegBack within the %systemroot%\Repair folder**. This is useful if there is a need to recover the system in the event of a failure.
    - Click **OK** to create the ERD.
    - When the ERD is created, the files described in the table below will be copied from the %systemroot%\Repair folder to a floppy disk.

File Name	Contents
Autoexec.nt	A copy of %systemroot%\System32\Autoexec.nt, which is used to initialize the MS-DOS environment.
Config.nt	A copy of the %systemroot%\System32\Config.nt, which is used to initialize the MS-DOS environment.
Setup.log	A log of which files were installed and of Cyclic Redundancy Check (CRC) information for use during the emergency repair process. This file has the read-only, system, and hidden attributes, and it is not visible unless the computer has been configured to show all files.

3. Perform a full backup of the computer, including the Registry files.
4. Verify available disk space with update requirements, which are generally found in the corresponding Readme file.
5. If recent changes were made to the system it may be necessary to restart the computer prior to installing a Service Pack update.

Installing Service Pack and Hotfix Updates

Windows 2000 Service Pack 3 can be installed from a Service Pack CD, from a network drive, of from the Windows 2000 Service Pack Web site at:

http://www.microsoft.com/windows2000/downloads/servicepacks/

Detailed procedures for each installation method can be found in the Service Pack readme file. During the installation process, the Service Pack program installs its files in the computer and automatically creates a backup of the files and settings that the service pack installer changes and saves the backup files in a $NTServicepackUninstall$ folder within the %systemroot% folder.

The Q326886 Post Service Pack 3 Hotfix can be downloaded from the Microsoft Critical Updates Web site at:

http://www.microsoft.com/windows2000/downloads/critical/

4. Secure Configuration

This section provides detailed procedures for making security configuration changes to the standard install base of Windows 2000 in support of the Evaluated Configuration. Tables are provided describing the security objective and the configuration actions necessary to meet that objective. Actions are described for Windows 2000 Professional (Stand-alone and Domain Member), Server (Stand-alone and Domain Member), and Domain Controller configurations.

If a Domain Security Policy is to be applied for all computers across a Domain, the settings defined for Windows 2000 Professional and Server must be used to comprise the requirements for the Domain Security Policy, as applicable. The Domain Controller settings defined in the document tables apply only to a Domain Controller Security Policy.

Section 5 of this document provides the procedures for automating most of the security settings defined in this section by applying pre-defined security configuration templates. For convenience, a Windows 2000 Security Configuration Checklist is provided in Appendix E of this document.

Windows 2000 Security Policies

This subsection explains the various security policy tools and their order of precedence with respect to application of security policies. By default, Group Policies are inherited and cumulative, and affect all computers in an Active Directory container. Group Policies are administered through the use of Group Policy Objects (GPOs), which are data structures attached in a specific hierarchy to selected Active Directory Objects, such as Sites, Domains, or Organizational Units (OUs).

These GPOs, once created, are applied in a standard order: LSDOU, which stands for (1) Local, (2) Site, (3) Domain, (4) OU, with the later policies being superior to the earlier applied policies. Local Group Policy Objects are processed first, and then domain policy. If a computer is participating in a domain and a conflict occurs between domain and local computer policy, domain policy prevails. However, if a computer is no longer participating in a domain, local Group Policy object is applied.

When a computer is joined to a domain with the Active Directory and Group Policy implemented, a Local Group Policy Object is processed. Note that LGPO policy is processed even when the Block Policy Inheritance option has been specified.

Account policies (i.e., password, lockout, Kerberos) are defined for the entire domain in the default domain Group Policy Object (GPO). Local policies (i.e., audit, user rights, and security options) for Domain Controllers (DCs) are defined in the default Domain Controllers GPO. For DCs, settings defined in the default DC GPO have higher precedence than settings defined in the default Domain GPO. Thus, if a user privilege were configured (for example, Add workstations to domain) in the default Domain GPO, it would have no impact on the DCs in that domain.

Options exist that allow enforcement of the Group Policy in a specific Group Policy Object so that GPOs in lower-level Active Directory containers are prevented from overriding that policy. For example, if there is a specific GPO defined at the domain level and it is specified that the GPO be enforced, the policies that the GPO contains apply to all OUs under that domain; that is, the lower-level containers (OUs) cannot override that domain Group Policy.

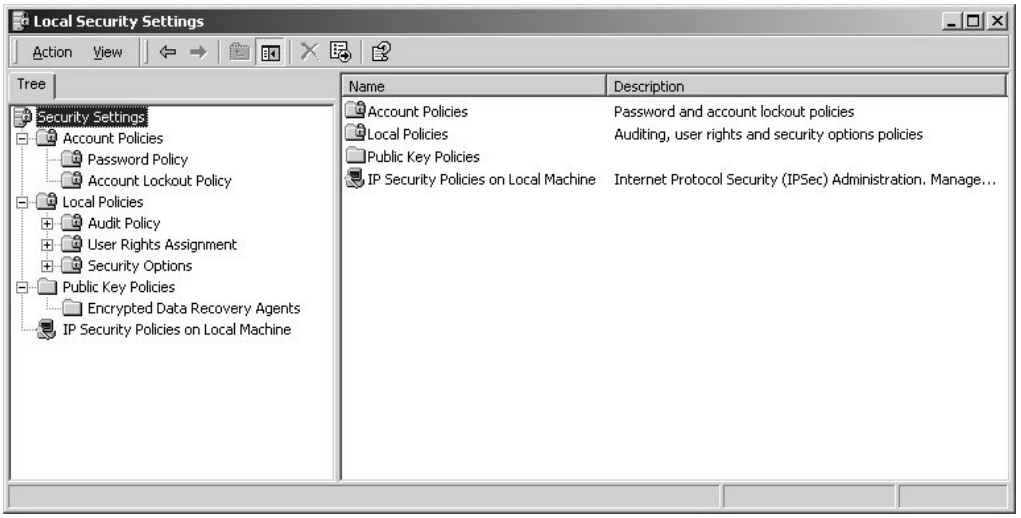
Note: The Account Policies security area receives special treatment in how it takes effect on computers in the domain. All DCs in the domain receive their account policies from GPOs configured at the domain node **regardless of where the computer object for the DC is.** This ensures that consistent account policies are enforced for all domain accounts. All non-DC computers in the domain follow the normal GPO hierarchy for getting policies for the local accounts on those computers. By default, member workstations and servers enforce the policy settings configured in the domain GPO for their local accounts, but if there is another GPO at lower scope that overrides the default settings, then those settings will take effect.

Local Security Policy

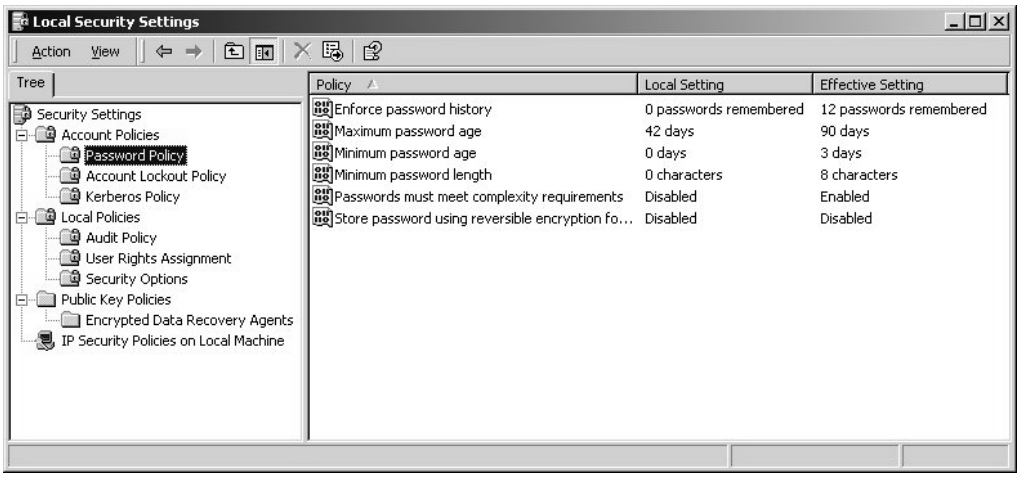
A Local Security Policy is used to set the security requirements on the local computer. It is primarily used for stand-alone computers or to apply specific security settings to a Domain member. Within an Active Directory managed network the Local Security Policy settings have the least precedence.

To open the Local Security Policy:

1. Log on to the computer with administrative rights.
2. In a Windows 2000 Professional computer, **Administrative Tools** is not displayed as a Start menu option by default. To view the **Administrative Tools** menu option in Windows 2000 Professional, click **Start**, point to **Settings**, and select **Taskbar and Start Menu**. In the **Taskbar and Start Menu Properties** window, click the **Advanced** tab. Check the **Display Administrative Tools** checkbox in the **Start Menu Settings** dialog box. Click the **OK** button to complete the setting.
3. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the Local Security Settings console.



Note: Local Security Policies display Local Settings for the computer and the Effective Settings resulting from the addition of Domain level security policy settings. Domain level security policy settings take precedence over any local settings, as shown below.

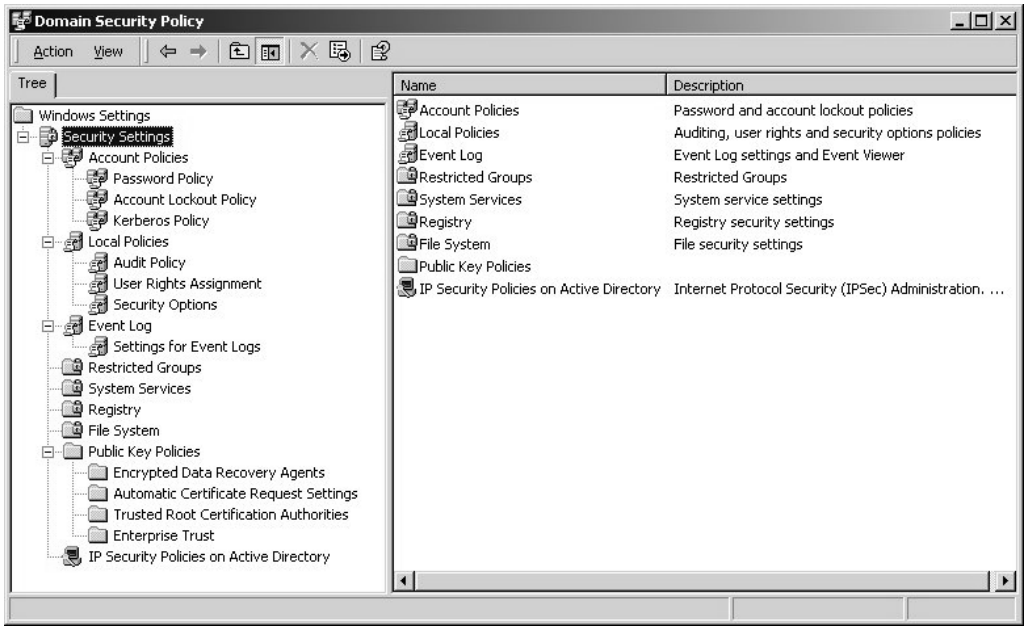


Domain Security Policy

A Domain Security Policy is used to set and propagate security requirements for all computers in the Domain. The Domain Security Policy overrides Local Security Policy settings for all computers within the Domain.

To open the Domain Security Policy:

1. Log on to the Domain Controller with administrative rights.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Security Policy**. This opens the Domain Security Policy console.

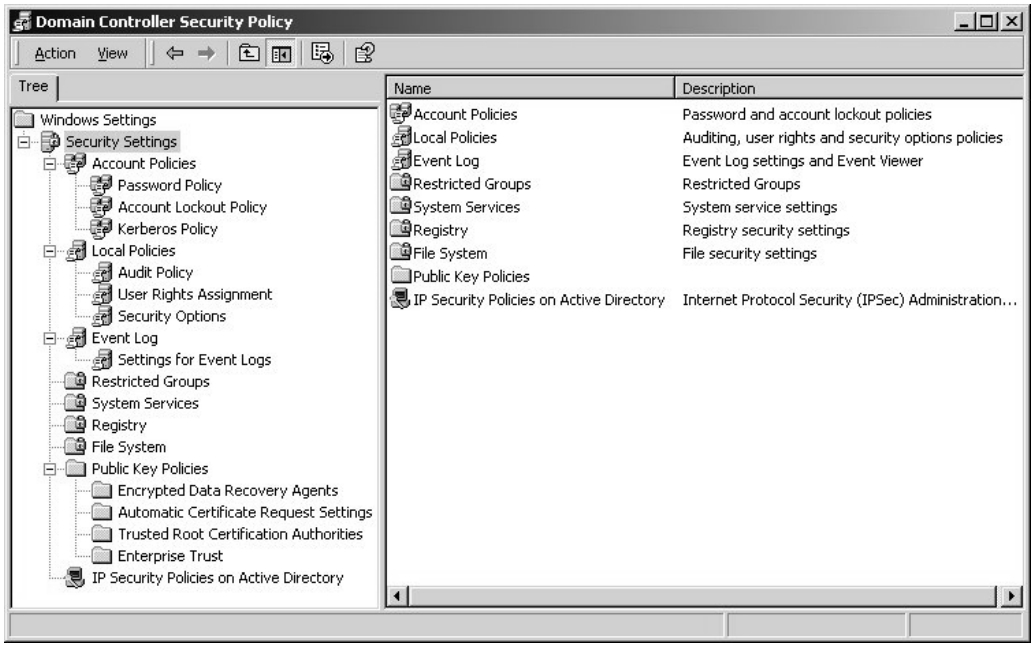


Domain Controller Security Policy

A Domain Controller Security Policy is used to set and propagate security requirements for Domain Controllers. The Domain Controller Security Policy applies strictly to all Domain Controllers within the applicable Domain and is not overwritten by the Domain Security Policy.

To open the Domain Controller Security Policy:

1. Log on to the Domain Controller with administrative rights.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Controller Security Policy**. This opens the Domain Controller Security Policy console.



Organizational Unit Group Policy Objects

This document will not cover the implementation of OU GPOs. However, it should be noted that an OU GPO may override security policy settings implemented by the previously discussed policy interfaces. For example, if a policy that is set for the domain is incompatible with the same policy configured for a child OU, the child does not inherit the domain policy setting. Instead, the setting in the child OU is applied. This can be avoided by selecting the No Override option when creating an OU GPO. The **No Override** option forces all child containers to inherit the parent's policies even if those policies conflict with the child's policies, and even if **Block Inheritance** has been set for the child. The **No Override** check box is located by clicking the **Options** button on the GPO's **Properties** dialog box.

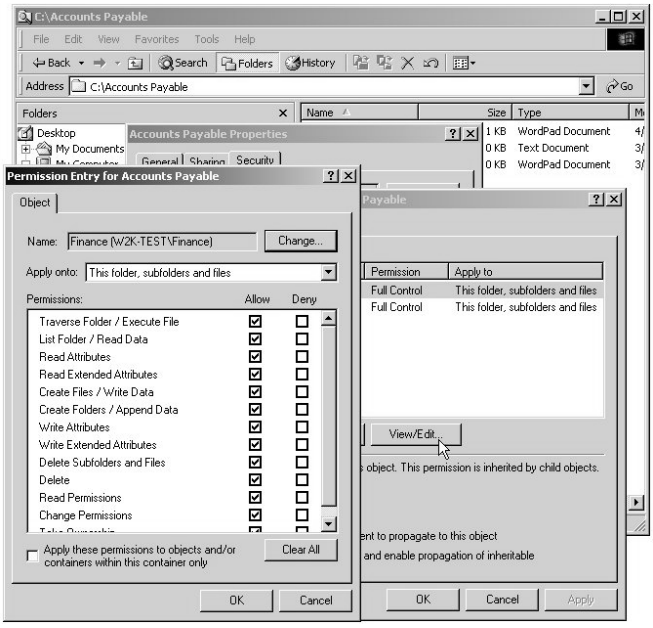
Additional Security Configuration Interfaces

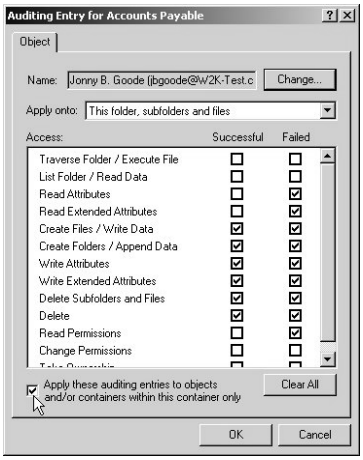
For ease of discussion and implementation, this document focuses on managing security settings through the interfaces describe above, Windows 2000 Security Policies. However, additional tools are available, and may be addressed in cases where stand-alone policy interfaces do not provide a capability to address specific security management options. These tools include

several of the standard Windows 2000 management interfaces, as well as the Security Configuration Tool Set which can not only be used to apply specific security setting, but also to test the operating systems for compliance with established policy requirements. Details on using each of these interfaces can be found in the Windows 2000 Evaluated Configuration Administrator's Guide.

Windows Explorer

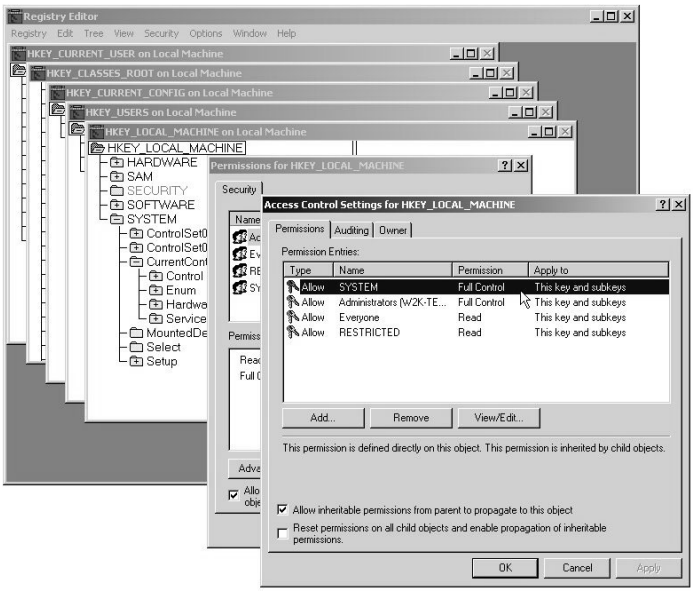
Windows Explorer can be used to configure permission and audit settings on specific files and folders. Shares and share permissions can also be set through the **Windows Explorer** interface, as illustrated below.





Registry Editors

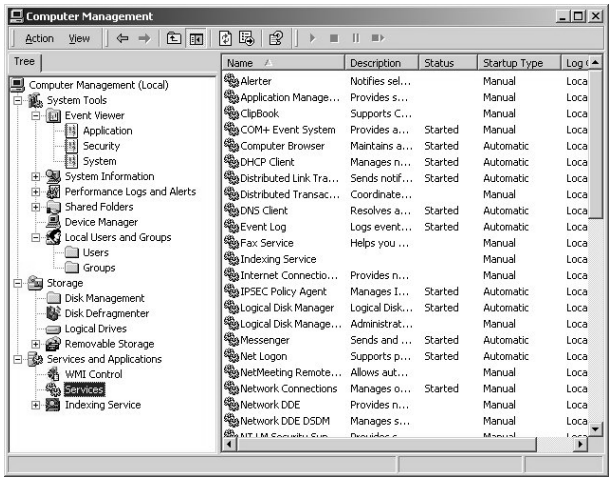
Two Registry editors are available with Windows 2000; **Regedit.exe** and **Regedt32.exe**. Of the two, **Regedt32.exe** is the only one that supports editing of permission and audit settings for Registry key objects. In the Evaluated Configuration, only Regedt32.exe should be used.



Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows 2000 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

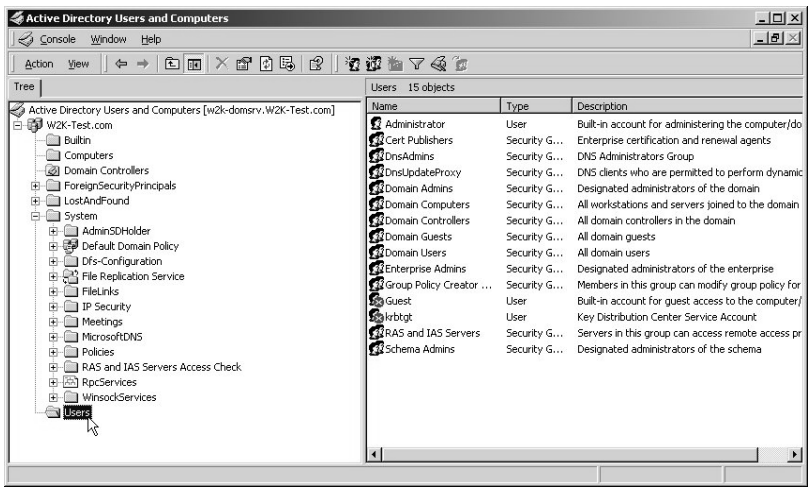
Computer Management Interface

The **Computer Management** interface is available on all Windows 2000 operating systems. It supports management of audit logs, share assignments and permissions, system services, as well as user and groups accounts. On Domain Controllers the user and group accounts are managed from **Active Directory Users and Computers** interface instead of the **Computer Management** interface.



Active Directory Users and Computers

The **Active Directory Users and Computers** interface is used to create and manage users, computers, and other Active Directory objects for a domain and is only available on Domain Controllers.



Microsoft Security Configuration Tool Set

The Microsoft Security Configuration Tool Set consists of a set of Microsoft Management Console (MMC) snap-ins designed to provide a capability for security configuration and analysis of Windows 2000 operating systems. The Security Configuration Tool Set allows administrators to configure security on Windows 2000 operating systems, and then perform periodic analysis of the systems to ensure that the configuration remains intact or to make necessary changes over time.

Detailed information on using the Microsoft Security Configuration Tool Set documentation is available for download at:
http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp.

Account Policies

Account policies are the rules that control three major account authentication features: password configuration, account lockout, and Kerberos authentication.

- **Password policy.** For local user accounts, determines settings for passwords such as enforcement, and lifetimes.
- **Account lockout policy.** For local user accounts, determines when and for whom an account will be locked out of the system.
- **Kerberos policy.** Kerberos authentication is the primary authentication mechanism used in an Active Directory domain.

Account policies can be applied to user accounts in domains, organizational units, trees, and so forth, and there is a hierarchical structure to these policies:

- Domain policies take precedence over Active Directory object policies.
- Organization unit policies take precedence over Domain policies.

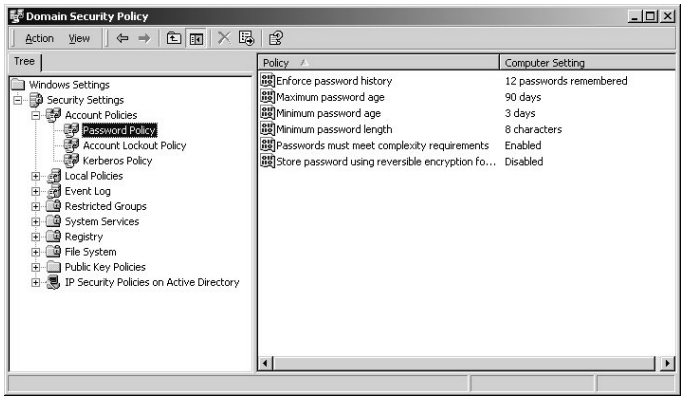
- Root domain policies take precedence over all policies.

See the Windows 2000 Evaluated Configuration Administrator's Guide for additional information on setting account policies.

Set the Password Policy

View and edit current password policy settings as follows:

1. Open the applicable Security Policy
2. Expand **Security Settings**.
3. Within **Security Settings**, expand **Account Policies** to reveal the **Password**, **Account Lockout**, and **Kerberos** policies.
4. Click on the **Password Policy** object. The right-hand details pane will reveal the configurable Password Policy settings.



5. Set the Password Policy as recommended or required in Table 4.1.

Table 4.1 Password Policy Settings

Password Policies	Professional	Server	DC	Required	Recommended
Set the Password History Requirements **Security Objective:** Set limit on how often passwords may be reused. **Procedure:** a. Double click on the **Enforce password history** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **passwords remembered** field (maximum is 24) to reflect the number of passwords the system will remember. A recommended setting is 24 passwords remembered.	✓	✓	✓		✓

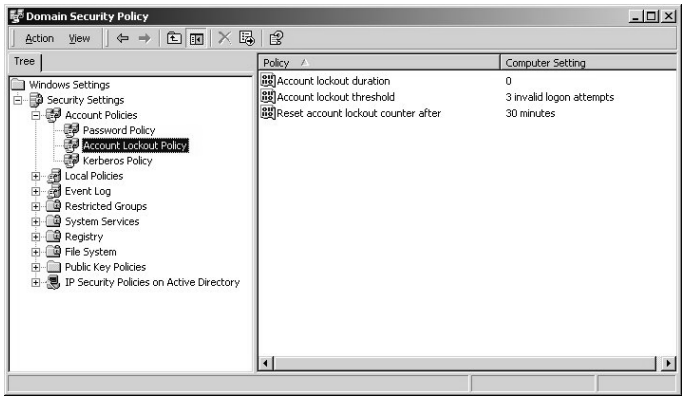
Password Policies	Professional	Server	DC	Required	Recommended
Set the Maximum Password Age **Security Objective:** Set the length of time users can keep their passwords before they have to change it. **Procedure:** a. Double click on the **Maximum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **days** field to the desired number. A recommended setting is 42 days. **Note:** The ST requires that a password expiration time be able to be set, but does not specify an expiration period. A Maximum Password Age must be set if a Minimum Password Age is used.	✓	✓	✓		✓
Set the Minimum Password Age **Security Objective:** Set the length of time users must keep a password before they can change it. **Procedure:** a. Double click on the **Minimum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **days** field to the desired number. A recommended setting is 2 days. **Note:** The ST requires that the administrator be able to set a minimum password age, but does not specify the length of time users must keep a password before they can change it. A Minimum Password Age must be set if a Maximum Password Age is used.	✓	✓	✓		✓
Set the Minimum Password Length **Security Objective:** Set the minimum number characters required for user passwords. **Procedure:** a. Double click on the **Minimum password length** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **characters** field to eight (8). **Note:** The ST requires that passwords be set to a minimum of 8 characters.	✓	✓	✓	✓	

Password Policies	Professional	Server	DC	Required	Recommended
Set the Password Complexity Requirements **Security Objective:** Requires the use of complex (strong) password. This policy will impose a requirement for a combination of alphanumeric, special, and upper and lower case characters in a password. **Procedure:** a. Double click on the **Passwords must meet complexity requirements** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Select the **Enabled** radio button. **Note:** The ST does not specify password complexity requirements.	✓	✓	✓		✓
<u>Do Not</u> Enable Reversible Encryption for Passwords **Security Objective:** Not recommended. **Procedure:** Verify the default setting is "**Disabled**."	✓	✓	✓	✓	

Set the Account Lockout Policy

View current Account Lockout Policy settings and edit as follows:

1. Open the applicable Security Policy.
2. Expand **Security Settings**.
3. Within **Security Settings** expand **Account Policies** to reveal the **Password**, **Account Lockout**, and **Kerberos** policies.
4. Click on the **Account Lockout Policy** object. The right-hand details pane will reveal the configurable Account Lockout Policy settings.



5. Set the Account Lockout Policy as recommended or required in Table 4.2.

Table 4.2 Account Lockout Policy Settings

Account Lockout Policies	Professional	Server	DC	Required	Recommended
Set Account Lockout Duration **Security Objective:** Once an account is locked for invalid password attempts, this setting keeps the account locked for a specified period of time (or until an administrator unlocks the account) before resetting. **Procedure:** a. Double click on the **Account lockout duration** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. It is recommended that the policy be set to lock the account indefinitely by changing the number in the **minutes** field to zero (0). This will require an administrator to unlock the account. **Notes:** The ST requires that a lockout duration be set. To meet the strength of function requirement, the value must be set to 1 minute or greater. The value can also be set to 0, which then requires the administrator to unlock the account. The **Account lockout duration** policy is linked to the **Reset account lockout counter after** policy. If the **Account lockout duration** policy is set to 0, the **Reset account lockout counter after** policy can be set to any value. If the **Account lockout duration** policy is set to a value other than 0, the **Reset account lockout counter after** policy will be automatically set to an equal value by default.	✓	✓	✓	✓	
Set Account Lockout Threshold **Security Objective:** Set the number of invalid login attempts that are allowed before an account is locked out. **Procedure:** a. Double click on the **Account lockout threshold** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **invalid login attempts** field to the desired number. It is required that it not be set at a value greater than 5. **Note:** The ST requires that a limit on the number of unsuccessful authentication attempts be set, but does not specify the limit. To meet the strength of function requirement, the value must be set at a value not greater than 5. Setting the **Account lockout threshold** will require that the **Reset account lockout counter after** and the **Account lockout duration** value settings be set. By default, they will be set to 30.	✓	✓	✓	✓	

Account Lockout Policies	Professional	Server	DC	Required	Recommended
Set the Account Lockout Reset Counter **Security Objective:** Every time a logon attempts fails, the value of a threshold that tracks the number of bad logon attempts is raised. This policy determines how long the lockout threshold is maintained before being reset. **Procedure:** a. Double click on the **Reset account lockout counter after** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **minutes** field to the desired number. It is recommended that the reset counter be set to a minimum of 30 minutes. **Note:** The **Reset account lockout counter after** setting is linked to the **Account lockout duration** setting. If the **Reset account lockout counter after** setting is set to a value of 30 or less, the **Account lockout duration** setting will be automatically set to 30 by default. If the **Reset account lockout counter after** setting is set to a value of 31 or greater, the **Account lockout duration** will be automatically set to an equal value by default.	✓	✓	✓	✓	

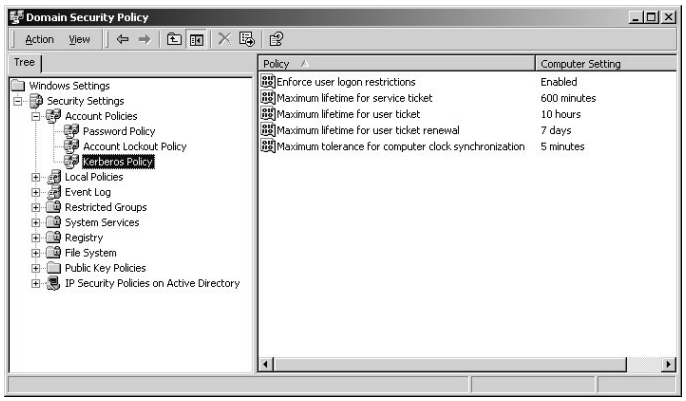
Access the Kerberos Policy Settings

View current Kerberos Policy settings and allow editing.

1. Open the Domain Security Policy or the Domain Controller Security Policy, as applicable.

   Note: The Kerberos Policy Settings are not available through a Local Security Policy tool. Domain members can inherit this policy from the Domain Security Policy.

2. Expand **Security Settings**.
3. Within **Security Settings** expand **Account Policies** to reveal the **Password**, **Account Lockout**, and **Kerberos** policies.
4. Click on the **Kerberos Policy** object. The right-hand details pane will reveal the configurable Kerberos Policy settings.



5. Set the Kerberos Policy as recommended or required in Table 4.3.

Table 4.3 Kerberos Policy Settings

Kerberos Policies	Professional	Server	DC	Required	Recommended
Enforce User Logon Restrictions **Security Objective:** Validates every logon request by checking the user rights policy to see if the user has permission to log on locally or to access the computer from the network. **Procedure**: Default settings are adequate. Verify the setting is **"Enabled."**	✓	✓	✓	✓	
Set the Maximum Lifetime for Service Ticket **Security Objective:** Sets the maximum duration for which a service ticket is valid. **Procedure:** Default settings are adequate. Verify that ticket expiration is set to "**600 minutes**."	✓	✓	✓		✓
Set the Maximum Lifetime for User Ticket **Security Objective:** Sets the maximum duration for which a user ticket is valid. **Procedure:** Default settings are adequate. Verify that ticket expiration is set to "**10 hours**."	✓	✓	✓		✓
Set the Maximum Lifetime for User Ticket Renewal **Security Objective:** Sets the renewal period for expired tickets. **Procedure:** Default settings are adequate. Verify that the ticket renewal expires in "**7 days**."	✓	✓	✓		✓

Kerberos Policies	Professional	Server	DC	Required	Recommended
Set the Maximum Tolerance for Computer Clock Synchronization **Security Objective:** Sets the maximum tolerance for synchronization between computers in the Domain. **Procedure:** Default settings are adequate. Verify that the maximum tolerance is set to "**5 minutes**."	✓	✓	✓	✓	

Local Policies

Local Policies determine the security options for a user or service account. Local policies are based on the computer a user is logged into, and the rights the user has on that particular computer. Local Policies can be used to configure:

- **Audit policy.** Determines which security events are logged into the Security log on the computer (i.e., successful attempts, failed attempts or both). The Security log is part of Event Viewer.
- **User rights assignment.** Determines which users or groups have logon or task privileges on the computer.
- **Security options.** Enables or disables security settings for the computer, such as digital signing of data, Administrator and Guest account names, floppy drive and CD ROM access, driver installation, and logon prompts.

Note: Local policies, by definition, are local to a computer. When these settings are imported to a Group Policy object in Active Directory, they will affect the local security settings of any computer accounts to which that Group Policy object is applied. Therefore, it is important to note the order of precedence for security policies. Security policies associated with Group Policy (Organizational Units) override policies established at the local level. Policies from the domain override locally defined policies. In either case, user account rights may no longer apply if there is a local policy setting that overrides those privileges. This is important because the behavior of Microsoft Windows 2000 can be quite different from the behavior in Microsoft Windows NT. For example, when password policies are configured for the Domain group policy (as they are by default), they affect every computer in that domain. This means that the local account databases (on individual workstations) in the domain have the same password policy as the domain itself.

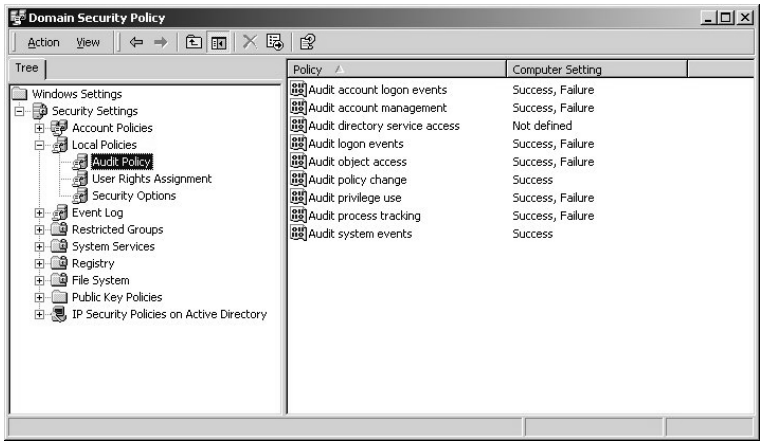
Set Event Audit

Enable auditing of security related events:

1. Open the applicable Security Policy.
2. Expand **Security Settings**.

3. Within **Security Settings**, expand **Local Policies** to reveal the **Audit**, **User Rights Assignment**, and **Security Options** policies.

4. Click on the **Audit Policy** object. The right-hand details pane will reveal the configurable Audit Policy settings



5. To set auditing of a security event, double click on the desired audit policy in the right-hand details pane. This will open the Security Policy Setting dialog window.

6. For Domain-level policies, check the **Define these policy settings** box, and check success or failure of the event as shown below.

7. Follow these procedures to set auditing of event categories as defined in Table 4.4.

Table 4.4 Audit Policy Settings

Audit Policies			Professional	Server	DC	Required	Recommended
Audit Event Categories	**Success**	**Failure**					
Audit Account Logon Events	✓	✓	✓	✓	✓		✓
Audit Account Management	✓	✓	✓	✓	✓		✓
Audit Directory Service Access	✓	✓	✓	✓	✓		✓
Audit Logon Events	✓	✓	✓	✓	✓		✓
Audit Object Access	✓	✓	✓	✓	✓		✓
Audit Policy Change	✓		✓	✓	✓		✓
Audit Privilege Use	✓	✓	✓	✓	✓		✓
Audit Process Tracking	✓	✓	✓	✓	✓		✓
Audit System Events	✓		✓	✓	✓		✓

Notes:

1. The Evaluated Configuration must include the "ability" to provide specific audit information. However, it is not required that the audit information be generated.

2. Setting an **Audit Object Access** policy only enables the capability to audit objects. To collect object access audit events, an auditing SACL must be set on each specific object for which access attempts are to be logged. The same applies if setting the **Audit Directory Service Access** policy.

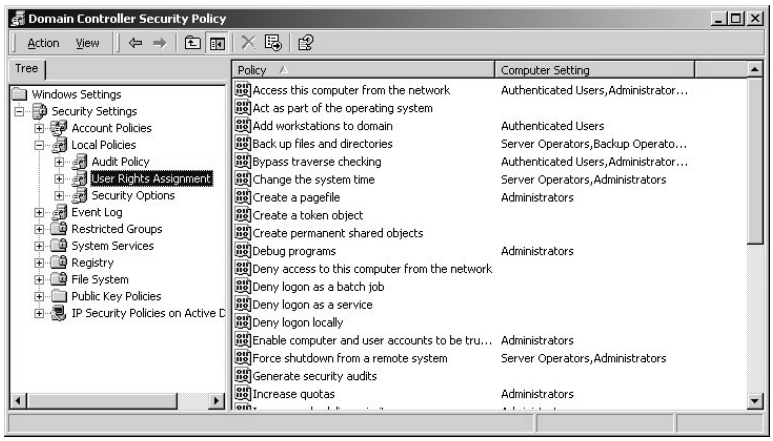
3. Appendix B – Audit Categories and Events, provides a matrix of Windows 2000 audit events, applicable ST requirements, and recommended audit settings.

4. "Account logon events" are generated where the account resides, such as on a Domain. "Logon events" are generated where the logon attempt occurs.

Modify Logon Rights and Privileges

Modify Logon Rights and Privileges for user accounts and services:

1. Open the applicable Security Policy.
2. Expand **Security Settings**.
3. Within **Security Settings**, expand **Local Policies** to reveal the **Audit**, **User Rights Assignment**, and **Security Options** policies.
4. Click on the **User Rights Assignment** object. The right-hand details pane will reveal the configurable user rights policy settings.



5. To set a user Logon Right or Privilege, double click on the desired policy in the right-hand details pane. This will open the Security Policy Setting dialog window.
6. For Domain-level policies, check the **Define these policy settings** box.
7. To remove a Logon Right or Privilege for an account, click on the account name to highlight it and click the **Remove** button.
8. To add a Logon Right or Privilege to an account, click the **Add** button and browse the appropriate account directory for the desired account.
9. There are several default assignments of user rights and privileges that the administrator should or must (see recommended or required columns in Table 4.5) change to maintain the evaluated configuration.

Note: The Power Users account does not exist on a Domain Controller. Therefore modifications affecting user rights and privileges for the Power Users group cannot be done manually from a Domain Controller. Also note that although the Power Users group does not reside on the Domain Controller, there may still exist references to this group in the Domain Controller's local policy, which remain after the computer is upgraded from a Server to a Domain Controller.

Table 4.5 User Rights and Privileges

User Rights and Privilege Assignment			Professional	Server	DC	Required	Recommended
Logon Right	**Default**	**Modified**					
Access this computer from the network ***(Professional/Server)***	Administrators Backup Operators Power Users Users Everyone	Administrators Backup Operators Power Users Users Authenticated Users	✓	✓		✓	

User Rights and Privilege Assignment			Professional	Server	DC	Required	Recommended
Access this computer from the network ***(Domain Controller)***	Administrators Authenticated Users Everyone	Administrators Authenticated Users			✓	✓	
Log on Locally ***(Professional)***	Administrators Backup Operators Power Users Users *Machinename*\Guest	Administrators Backup Operators Power Users Users	✓			✓	
Log on Locally ***(Server)***	Administrators Backup Operators Power Users Users *Machinename*\Guest *Machinename*\TsInternetUser	Administrators Backup Operators Power Users Users **Note:** The *Machinename*\TsInternetUser account is removed because Windows 2000 Terminal Server is not part of the Evaluated Configuration.		✓		✓	
Log on Locally ***(Domain Controller)***	Administrators Account Operators Backup Operators Print Operators Server Operators TsInternetUser	Administrators Account Operators Backup Operators Print Operators Server Operators **Note:** The TsInternetUser account is removed because Windows 2000 Terminal Server is not part of the Evaluated Configuration.			✓	✓	

User Rights and Privilege Assignment			Professional	Server	DC	Required	Recommended
Privilege	**Default**	**Modified**					
Add Workstations to the Domain ***(Domain Controller)***	Authenticated Users	Remove the Authenticated Users account. Do not grant this privilege to other users. **Note:** Domain Administrators have this privilege by default.			✓	✓	
Increase Quotas ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	
Increase Scheduling Priority ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	
Load and Unload Device Drivers ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	
Manage Auditing and Security Log ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	
Modify Firmware Environment ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	

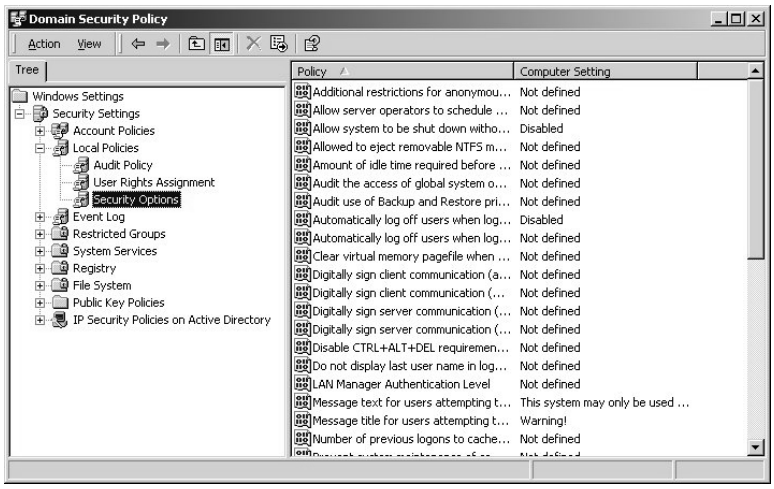
User Rights and Privilege Assignment			Professional	Server	DC	Required	Recommended
Profile System Performance ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	
Shut Down the System ***(Professional)***	Administrators Backup Operators Power Users Users	Administrators Backup Operators Power Users Authenticated Users	✓				✓
Take Ownership of Files and Objects ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators			✓	✓	

Note: Appendix C – User Rights and Privileges, provides a matrix of Windows 2000 user rights and privileges, applicable ST requirements, and the recommended/required modifications.

Modify Security Options

Modify predefined security related Registry settings:

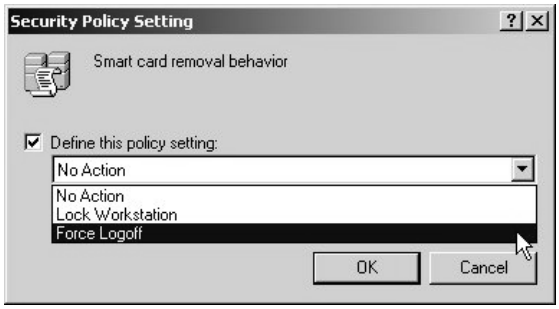
1. Open the applicable Security Policy.
2. Expand **Security Settings**.
3. Within **Security Settings**, expand **Local Policies** to reveal the **Audit**, **User Rights Assignment**, and **Security Options** policies.
4. Click on the **Security Options** object. The right-hand details pane will reveal the configurable security options.



5. To set a Security Option, double click on the desired policy in the right-hand details pane. This will open the Security Policy Setting dialog window.

6. For Domain-level policies, check the **Define these policy settings** box.

7. Input to the **Security Policy Setting** dialog boxes for selected security options will vary depending on the configuration requirements of the option. For example some security options may require selection from a drop down menu or a text input as shown below.



8. Modify the Security Options as shown in Table 4.6.

Table 4.6 Security Option Settings

Security Options	Professional	Server	DC	Required	Recommended
Set Additional Restrictions for Anonymous Connections **Security Objective:** Disable ability of anonymous user to enumerate SAM accounts and shares. **Procedure:** a. Double click on **Additional restrictions for anonymous connections** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Do not allow enumeration of SAM accounts and shares**. d. Click the **OK** button.	✓	✓	✓	✓	
Allow server operators to schedule tasks (domain controllers only) **Security Objective:** Determines if Server Operators are allowed to submit jobs by means of the AT schedule facility. By default, a user must be an administrator in order to submit jobs by means of the AT scheduler. Enabling this security policy setting allows members of the Server Operators group to submit AT schedule jobs on Domain Controllers without having to make them Administrators. **Procedure:** Do not enable this feature. The AT schedule facility is not part of the Evaluated Configuration. **Note:** The Domain level policy default is "**Not Defined**." It is recommended that the policy be set to **Disabled**.			✓	✓	
Disable Shutdown Without Logon **Security Objective:** Disable the ability to shut down the computer without first authenticating to the system. **Procedure:** a. Double click on **Allow system to be shut down without having to log on** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Restrict Ability to Eject Removable NTFS Media **Security Objective:** Ensure integrity of ACL settings on data contained in removable media by allowing only authorized administrators the capability of removing the media from the computer. **Procedure:** a. Double click on **Allowed to eject removable NTFS media** in the right-hand details pane.	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Administrators** and click the **OK** button.					
Amount of idle time required before disconnecting a session **Security Objective:** Determines the amount of continuous idle time that must pass in a Server Message Block (SMB) session before the session is disconnected due to inactivity. Administrators can use this policy to control when a computer disconnects an inactive SMB session. If client activity resumes, the session is automatically reestablished. This policy is defined for servers by default in Local Computer Policy with a default value of 15 minutes. This policy is not defined on workstations. For this policy setting, a value of 0 means to disconnect an idle session as quickly as reasonably possible. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Audit the Access of Global System Objects **Security Objective:** Enable the capability to audit access of global system objects. When this policy is enabled, it causes system objects such as mutexes, events, semaphores, and DOS Devices to be created with a default system access control list (SACL). If the **Audit object access** audit policy is also enabled, then access to these system objects will be audited. **Procedure:** a. Double click on **Audit the access of global system objects** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** In the evaluated configuration, these objects must be auditable, however, enforcing this audit capability is optional. To audit these objects, the administrator must set this option. This setting will generate a large amount of audit information. Therefore, it should only be enabled where there is a strict audit management process in place for reviewing, archiving, and clearing the audit logs on a regular basis. The maximum log size should also be edited to support an increase in the number of events being logged.	✓	✓	✓		✓
Audit the Use of Backup and Restore Privilege **Security Objective:** Enable the capability to create audit event entries whenever the **Backup files and directories** or the **Restore files and directories privileges** are used. By default, the use of backup and restore privileges are not audited. When the **Audit privilege use** audit policy is enabled and this security option is set, the use of the Backup and Restore privileges will be audited. **Procedure:** a. Double click on **Audit use of Backup and Restore privilege** in the right-hand details pane.	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** In the evaluated configuration, these objects must be auditable, however, enforcing this audit capability is optiona. To audit these objects, the administrator must set this option. This setting will generate a large amount of audit information. Therefore, it should only be enabled where there is a strict audit management process in place for reviewing, archiving, and clearing the audit logs on a regular basis. The maximum log size should also be edited to support an increase in the number of events being logged.					
Automatically Log Off Users When Logon Time Expires **Security Objective:** Force a user log off of the *network* when that user remains logged on beyond the allowed hour range. **Procedure:** a. Double click on **Automatically log off users when logon time expires** in the right-hand details pane. b. Check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** This Security Option can only be set at the Domain Controller.			✓		✓
Automatically Log Off Users When Logon Time Expires (Local) **Security Objective:** Force a user log off of the local computer when that user remains logged on beyond the allowed hour range. **Procedure:** a. Double click on **Automatically log off users when logon time expires (local)** in the right-hand details pane. b. For Domain-level policies, check **the Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓		✓
Clear Virtual Memory Page File When System Shuts Down **Security Objective:** Removes the virtual memory pagefile when the system is shut down. The pagefile is reinitialized the next time a user logs in. The purpose is to ensure that any information that may remain within the page file is not available to the next user that logs on to the machine. **Procedure:** a. Double click on **Clear virtual memory pagefile when system shuts down** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	

Security Options	Professional	Server	DC	Required	Recommended
Digitally sign client communications (always) **Security Objective:** Determines whether the computer will always digitally sign client communications. The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a "man-in-the-middle" attack, and supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Enabling this option requires the Windows 2000 SMB client to perform SMB packet signing. If this policy is disabled, it does not require the SMB client to sign packets. This policy is disabled by default. For the Evaluated Configuration, this policy option may be disabled and the following security option, **"Digitally sign client communications (when possible)"** may be enabled. Since the Evaluated Configuration operating environment is a closed network with all computers configured to the same requirements, communications will use SMB signing (see note below). **Procedure:** a. Double click on **Digitally sign client communications (always)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button. **Note:** In order to use SMB signing, it must be either enabled or required on both the SMB client and the SMB server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, then a client will not be able to establish a session unless it is at least enabled for SMB signing.	✓	✓	✓	✓	
Digitally sign client communications (when possible) **Security Objective:** If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on **Digitally sign client communications (when possible)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** See note for **Digitally sign client communications (always)**.	✓	✓	✓	✓	

Security Options	Professional	Server	DC	Required	Recommended
Digitally sign server communications (always) **Security Objective:** If this policy is enabled, it requires the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on **Digitally sign server communications (always)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button. **Note:** See note for **Digitally sign client communications (always)**.	✓	✓	✓	✓	
Digitally sign server communications (when possible) **Security Objective:** If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default on workstation and server platforms in Local Computer Policy. This policy is enabled by default on Domain Controllers.. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on **Digitally sign server communications (when possible)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** See note for **Digitally sign client communications (always)**.	✓	✓	✓	✓	
Disable CTRL+ALT+DEL Required for Logon **Security Objective:** **DO NOT ENABLE THIS OPTION.** Enabling this option will disable the trusted path mechanism. The purpose of the trusted path mechanism is to prevent spoofing of user login sessions. The default setting of this option is Disabled on a Windows 2000 computer, although a policy tool may show it as Not Defined. **Procedure:** Verify that the **Disable CTRL+ALT+DEL requirement for logon** option in the right hand details pane is **set to Not Defined or is Disabled**.	✓	✓	✓	✓	
Do Not Display Last User Name on Logon Screen **Security Objective:** By default, the Windows 2000 login interface displays the user ID of the last user that logged onto the computer. Enabling this option removes the name of the last user from the login session. As a result, an intruder attempting to break into the computer locally would not only need to guess the password, but would also need to guess a correct user ID. **Procedure:**	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
a. Double click on **Do not display user name in the logon screen** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.					
LAN Manager Authentication Level **Security Objective:** This Security Option is used to set the Windows Challenge/Response authentication level. It is used to establish which challenge/response authentication protocol is used for network logons. The choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted as per the following selection options: • **Send LM & NTLM responses**: Clients use LM and NTLM authentication, and never use NTLMv2 session security; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send LM & NTLM - use NTLMv2 session security if negotiated**: Clients use LM and NTLM authentication, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLM response only**: Clients use NTLM authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only\refuse LM**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM (accept only NTLM and NTLMv2 authentication). • **Send NTLMv2 response only\refuse LM & NTLM**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM and NTLM (accept only NTLMv2 authentication). The default setting for servers is **Send LM & NTLM responses**. LM authentication allows clear text passwords. Security weaknesses found with the NTLM protocol allow password crackers to decrypt NTLM-protected authentication. To counteract this, NTLM version 2 was developed. NTLMv2 introduces additional security features, including • **Unique session keys per connection**. Each time a new connection is established, a unique session key is generated for that session. This way a captured session key will serve no useful purpose after the connection is completed. • **Session keys protected with a key exchange**. The session key can't be intercepted and used unless the key pair used to protect the session key is obtained. • **Unique keys generated for the encryption and integrity of session**	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
data. The key that's used for the encryption of data from the client to the server will be different from the one that's used for the encryption of data from the server to the client. **Procedure:** a. Double click on **LAN Manager Authentication level** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Send NTLMv2 response only\refuse LM & NTLM** and click the **OK** button.					
Implement an Authorized Usage Warning **Security Objective:** Configure the interactive logon screen to display a logon banner with a title and warning. **Procedure:** a. To set a message title, double click on **Message title for users attempting to log on** in the right-hand details pane. This will open the Security Policy Setting dialog window. b. For Domain-level policies, check the **Define these policy settings** box. c. Enter the title for the logon message (for example, "Warning") and click **OK**. d. To set the message, double click on **Message text for users attempting to log on** in the right-hand details pane. This will open the Security Policy Setting dialog window. e. For Domain-level policies, check the **Define these policy settings** box. f. Enter the message text and click **OK**. **Note:** The Evaluated Configuration must allow for the ability to set a banner, it is not required that one be set.	✓	✓	✓		✓
Disable Caching of Logon Information **Security Objective:** Windows 2000 has the capability to cache logon information. If the Domain Controller cannot be found during logon and the user has logged on to the system in the past, it can use those credentials to log on. The CachedLogonsCount Registry valued determines how many user account entries Windows 2000 saves in the logon cache on the local computer. If the value of this entry is 0, Windows 2000 does not save any user account data in the logon cache. In that case, if the user's Domain Controller is not available and a user tries to log on to a computer that does not have the user's account information, Windows 2000 displays the following message: **The system cannot log you on now because the domain <Domain-name> is not available.** If the Administrator disables a user's domain account, the user could still use the cache to log on by disconnecting the net cable. To prevent this,	✓	✓	✓	✓	

Security Options	Professional	Server	DC	Required	Recommended
Administrators should disable the caching of logon information. This results in a somewhat longer logon time, but prevents hackers from tapping logon information from short-term memory. **Procedure:** a. Double click on **Number of previous logons to cache (in case domain controller is not available** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. In the **Cache:** text box, set the number of logons to 0 and click the **OK** button.					
Prevent System Maintenance of Computer Account Passwords **Security Objective:** Determines whether the computer account password should be prevented from being reset every week. As a part of Windows 2000 security, ***computer account*** passwords are changed automatically every seven days. If this policy is enabled, the machine is prevented from requesting a weekly password change. If this policy is disabled, a new password for the computer account will be generated every week. This policy is disabled by default. **Procedure:** Do not enable this policy. Verify that local policies are set to **Disabled** and that Domain policies are either **Disabled** or **Not defined**.	✓	✓	✓		✓
Prevent Users from Installing Print Drivers **Security Objective:** Determines whether members of the Users group are prevented from installing print drivers. If this policy is enabled, it prevents users from installing printer drivers on the local machine. This prevents users from "Adding Printers" when the device driver does not exist on the local machine. If this policy is disabled, then a member of the Users group can install printer drivers on the computer. By default, this setting is enabled on servers and disabled on workstations. **Procedure:** Do not change the defaults for servers and stand-alone computers. For Domain policies: a. Double click on **Prevent users from installing print drivers** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Prompt User to Change Password Before Expiration **Security Objective:** Determines how far in advance Windows 2000 should warn users that their password is about to expire. By giving the user advanced warning, the user has time to construct a sufficiently strong password. By default, this value is set to 14 days. **Procedure:** None. The default setting is adequate.	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
Recovery Console: Allow Automatic Administrative Logon **Security Objective:** By default, the Recovery Console requires that a password be provide the for the Administrator account before accessing the system. If this option is enabled, the Recovery Console does not require a password and will automatically log on to the system. By default, this setting is disabled, although a policy tool may show it as Not Defined. **Procedure:** Do not enable this option. **Note:** The Windows 2000 Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.	✓	✓	✓	✓	
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders **Security Objective:** Enabling this option enables the Recovery Console SET command, which allows the following Recovery Console environment variables to be set: • **AllowWildCards** - Enable wildcard support for some commands (such as the DEL command). • **AllowAllPaths** - Allow access to all files and folders on the computer. • **AllowRemovableMedia** - Allow files to be copied to removable media, such as a floppy disk. • **NoCopyPrompt** - Do not prompt when overwriting an existing file. By default, the SET command is disabled and all these variables are not enabled, although a policy tool may show it as Not Defined.. **Procedure:** Do not enable this option. **Note:** The Windows 2000 Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.	✓	✓	✓		✓
Rename Administrator Account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the account “Administrator.” This reduces the chances of administrator exploit attempts by forcing a potential hacker to not only have to guess the password, but also the user ID associated with the Administrator account. **Procedure:** a. Double click on **Rename administrator account** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. In the text box, enter the new name for the Administrator account and click the **OK** button.	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
Rename Guest Account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the account "Guest." This reduces the chances of anonymous exploit attempts by forcing a potential hacker to not only have to guess the password, but also the user ID associated with the Guest account. **Procedure:** a. Double click on **Rename guest account** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. In the text box, enter the new name for the Guest account and click the **OK** button. **Note:** The Guest account must be disabled in the evaluated configuration (see Table 4-8).	✓	✓	✓		✓
Restrict CD-ROM Access to Locally Logged-On User Only **Security Objective:** Determines whether a CD-ROM is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable CD-ROM media. If no one is logged on interactively, the CD-ROM may be shared over the network. If this policy is disabled, then the local user and remote users can access the CD-ROM simultaneously. **Procedure:** a. Double click on **Restrict CD-ROM access to locally logged-on user only** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Restrict Floppy Access to Locally Logged-On User Only **Security Objective:** Determines whether removable floppy media is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable floppy media. If no one is logged on interactively, the floppy media may be shared over the network. If this policy is disabled, then the local user and remote users can access the floppy media simultaneously. **Procedure:** a. Double click on **Restrict floppy access to locally logged-on user only** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	

Security Options	Professional	Server	DC	Required	Recommended
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic must be either signed or encrypted. If this policy is disabled, signing and encryption are negotiated with the domain controller. By default, this policy is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Secure Channel: Digitally Encrypt Secure Channel Data (When Possible) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be encrypted. If this policy is disabled, outgoing secure channel traffic will not be encrypted. By default, this option is enabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Secure Channel: Digitally Sign Secure Channel Data (When Possible) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be signed. If this policy is disabled, no outgoing secure channel traffic will be signed. By default, this option is enabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Secure Channel: Require Strong (Windows 2000 or Later) Session Key **Security Objective:** If this policy is enabled, all outgoing secure channel traffic will require a strong (Windows 2000 or later) encryption key. If this policy is disabled, the key strength is negotiated with the DC. This option should only be enabled if all of the DCs in all trusted domains support strong keys. By default, this value is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
Send Unencrypted Password to Connect to Third-Party SMB Servers **Security Objective:** If this policy is enabled, the Server Message Block (SMB) redirector is allowed to send clear-text passwords to non-Microsoft SMB servers that do not support password encryption during authentication. By default, this option is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Shut Down the System Immediately if Unable to Log Security Audits **Security Objective:** Determines whether the system should shut down if it is unable to log security events. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either **Do Not Overwrite Events** or **Overwrite Events by Days**. If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error will occur: **STOP: C0000244 {Audit Failed}** **An attempt to generate a security audit failed.** To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired. By default, this policy is disabled. **Procedure:** a. Double click on **Shut down system immediately if unable to log security audits** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note:** Use this security policy on servers and Domain Controllers only after implementing strict procedures for archiving and clearing the audit logs on a regular basis. **Note:** The ST requires the system to be able to prevent auditable events from occurring, except those taken by the administrator, if the audit log is full. If the administrator desires this functionality, this option must be enabled.	✓	✓	✓		✓
Smart Card Removal Behavior **Security Objective:** Determines what should happen when the smart card for a logged-on user is removed from the smart card reader. The options are: • **No Action** • **Lock Workstation** • **Force Logoff** By default, **No Action** is specified. If **Lock Workstation** is specified, then the workstation is locked when the smart card is removed allowing users to leave	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
the area, take their smart card with them, and still maintain a protected session. If Force Logoff is specified, then the user is automatically logged off when the smart card is removed. **Procedure:** a. Double click on **Smart card removal behavior** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Lock Workstation** and click the **OK** button. **Note:** The integration of smart card technology is not part of the Evaluated Configuration.					
Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links) **Security Objective:** Determines the strength of the default discretionary access control list (DACL) for objects. Windows 2000 maintains a global list of shared system resources such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create. By default, this option is enabled locally on Windows 2000 Professional and Server, but is not defined in the Domain Security Policy. **Procedure:** a. Double click on **Strengthen default permissions of global system objects (e.g. Symbolic Links)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. d. For stand-alone computers/domain members, verify that this security option is enabled in the local policy.	✓	✓	✓	✓	
Unsigned Driver Installation Behavior **Security Objective:** Determines what should happen when an attempt is made to install a device driver (by means of the Windows 2000 device installer) that has not been certified by the Windows Hardware Quality Lab (WHQL). The options are: • **Silently succeed** • **Warn but allow installation** • **Do not allow installation** The default setting is to **Warn but allow installation**. **Procedure:**	✓	✓	✓		✓

Security Options	Professional	Server	DC	Required	Recommended
a. Double click on **Unsigned driver installation behavior** in the right-hand details pane. b. For local policies, make sure the behavior is set to **Warn but allow installation**. c. For Domain-level policies, check the **Define these policy settings** box. d. From the drop-down menu, select **Warn but allow installation** and click the **OK** button.					
Unsigned Non-Driver Installation Behavior **Security Objective:** Determines what should happen when an attempt is made to install any non-device driver software that has not been certified. The options are: • **Silently succeed** • **Warn but allow installation** • **Do not allow installation** The default setting is to **Silently succeed**. **Procedure:** a. Double click on **Unsigned non-driver installation behavior** in the right-hand details pane. b. For local policies, make sure the behavior is set to **Warn but allow installation**. c. For Domain-level policies, check the **Define these policy settings** box. d. From the drop-down menu, select **Warn but allow installation** and click the **OK** button.	✓	✓	✓		✓

Additional Security Settings

The additional security settings described in this subsection are not available in the security policy GUIs and must therefore be configured through the Registry Editor. Instructions for using the Registry editor are available in the Windows 2000 Evaluated Configuration Administrator's Guide.

Information on how to edit the Registry is also available through the **Help** tool in **Regedit.exe**. For example, for instructions on adding a key to the Registry:

1. Click the **Start** button and select **Run…**
2. Within the **Run** dialog window's text box, type **regedt32** and click the **OK** button to open the **Registry Editor** (Regedt32.exe).
3. From the editor's **Help** menu, select **Contents**.

4. In the right-hand pane of the Registry Editor's Help tool, click on the "**Add and delete information in the registry**" hyperlink.
5. The pane will change to provide a list of help topics for adding and deleting information in the Registry. Click on the "**Add a key to the registry**" hyperlink to obtain the detailed instructions.

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows 2000 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Required Registry Settings

The Registry settings described in this subsection are required in order to conform to Evaluated Configuration requirements. All numerical values are shown in decimal, unless otherwise noted.

Disable DirectDraw

The DirectDraw feature exists to enable high-performance multimedia applications. It does this by providing applications with the most direct path possible to the 2-D graphics hardware on a system. The DirectDraw feature is not part of the Evaluated Configuration and must be disabled.

Disable DirectDraw by editing the Registry and changing the Timeout value to 0 as shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers		Format	Value
Key: DCI	**Value Name:** Timeout	REG_DWORD	0

Remove OS/2 and POSIX subsystems

The OS/2 and POSIX subsystems were not included in the evaluated configuration, and should therefore be removed. To remove OS/2 and POSIX support from Windows 2000, edit the Registry and delete the value as shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager		Format	Value
Key: SubSystems	**Value Name:** Optional	REG_MULTI_SZ	Delete the value

Disable unnecessary devices

For the Evaluated Configuration, it is necessary to disable all of the devices listed below by editing the Registry and changing the **Start** value to 4 as shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services		Format	Value
Key: audstub	**Value Name:** Start	REG_DWORD	4
Key: mnmdd	**Value Name:** Start	REG_DWORD	4
Key: ndistapi	**Value Name:** Start	REG_DWORD	4
Key: ndiswan	**Value Name:** Start	REG_DWORD	4
Key: ndproxy	**Value Name:** Start	REG_DWORD	4
Key: parvdm	**Value Name:** Start	REG_DWORD	4
Key: pptpminiport	**Value Name:** Start	REG_DWORD	4
Key: ptilink	**Value Name:** Start	REG_DWORD	4
Key: rasacd	**Value Name:** Start	REG_DWORD	4
Key: rasl2tp	**Value Name:** Start	REG_DWORD	4
Key: raspti	**Value Name:** Start	REG_DWORD	4
Key: wanarp	**Value Name:** Start	REG_DWORD	4

Protect kernel object attributes

This step is necessary to ensure that the object manager may change attributes of a kernel object in the object table for the current process if and only if the previous mode of the caller is kernel mode. To enable this capability edit the Registry to create and set the value of the Registry entry shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Control		Format	Value
Key: Session Manager	**Value Name:** EnhancedSecurityLevel	REG_DWORD	1

Restrict Null Session Access

Null sessions are a weakness that can be exploited through the various shares that are on the computer. Modify null session access to shares on the computer adding **RestrictNullSessAccess**, a Registry value that toggles null session shares on or off to determine whether the Server service restricts access to clients logged on to the system account without username and password authentication. Setting the value to 1 restricts null session access to unauthenticated users to all server pipes and shares except those listed in the **NullSessionPipes** and **NullSessionShares** entries.

Key Path: HKLM\SYSTEM\ CurrentControlSet\Services\LanmanServer		Format	Value
Key: parameters	**Value Name:** RestrictNullSessAccess	REG_DWORD	1

Restrict null session access over named pipes

Restricting such access helps prevents unauthorized access over the network. To restrict null session access over named pipes and shared directories, edit the Registry and delete the values as shown in the table below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer			Format	Value
Key: parameters	**Value Names:**	NullSessionPipes NullSessionShares	REG_MULTI_SZ	Delete all values

Service Pack 3 Registry entries

Service Pack 3 introduces a number of new registry entries that can be configured to enhance the security provided by the operating system.

Prevent interference of the session lock from application generated input

Service Pack 3 introduces a Registry key value that can be used to prevent application generated keyboard/mouse input messages from interfering with the session lock. The keys name is BlockSendInputResets and as with most policy settings the key resides in:

HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop (Policy) and

HKCU\Control Panel\Desktop (User)

Policy takes precedence over the User applied setting. The key will be REG_SZ to be consistent with other related keys and will be interpreted as a Boolean value with any non –zero value meaning the key is set and the feature active. A zero value or the key not existing will maintain the current functionality.

When this key is set only ‘real’ (mouse or keyboard) input will reset the screensavers timer. Currently there are 3 cases where ‘injected’ will reset the time.

- Input injected via SendInput – This is the case where an app is intentionally trying to simulate input and will be blocked.
- Window activation – When a new window becomes active the counter is reset. This will be blocked unless the screensaver is already active.
- Calls to SystemParametersInfo() that set SPI_SETSCREENSAVETIMEOUT, SPI_SETSCREENSAVEACTIVE, SPI_SETLOWPOWERTIMEOUT, SPI_SETLOWPOWERACTIVE, SPI_SETPOWEROFFTIMEOUT, SPI_SETPOWEROFFACTIVE. These will no longer result in the timer being reset if BlockSendInputResets is set. This should not have an effect on user experience, as a user setting these values will result in ‘real’ input from their mouse movement and keystrokes.

To enable this capability, edit the following Registry key value as shown in the table below. The key path will need to be created, under the **HKCU\Software\Policies \Microsoft** key, along with the necessary value.

Key Path: (Policy) HKCU\Software\Policies\Microsoft\Windows\Control Panel		Format	Value
Key: Desktop	**Value Name:** BlockSendInputResets	REG_SZ	1

Note: It is important to note that the appropriate screen saver settings must be set in conjunction with this key for the feature to make sense. The necessary screen saver settings are:

- A selected screen saver
- Password protection
- A screen saver timeout period

If the screensaver is not properly configured this feature will essentially have no effect on the machines overall security. Procedures for setting a password protected screen saver are available in the "Enable Automatic Screen Lock Protection" subsection.

Generate an audit event when the audit log reaches a percent full threshold

Service Pack 3 includes a feature for generating a security audit in the security event log when the security log reaches a configurable threshold. To enable this capability create the key value shown in the table below with a value setting that will designate the percent value that will cause the event to be recorded in the security log. The value shown in the table below is a recommendation and can be configured to an appropriate value based on local operational needs. For example, if set as shown below, and the security log size reaches the percent shown (90), the security log will show one event entry for eventID 523 with the following text: "The security event log is 90 percent full."

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\Eventlog		Format	Value
Key: Security	**Value Name:** WarningLevel	REG_DWORD	90

Recommended Registry Settings

The Registry settings described in this subsection are recommended in order to establish a more secure operating system configuration.

Harden the TCP/IP stack against denial of service attacks

Denial of service attacks are network attacks aimed at making a computer or a particular service on a computer unavailable to network users. The following Registry TCP/IP-related values help to increase the resistance of the Windows 2000 TCP/IP Stack in Windows 2000 against denial of service network attacks. Some of the key values listed below will need to be added the specified Registry key. Additional details can be found in Microsoft Knowledge Base Article Q315669, "HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000."

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip		Format	Value
Key: Parameters	**Value Name:** DisableIPSourceRouting	REG_DWORD	2
Key: Parameters	**Value Name:** EnableDeadGWDetect	REG_DWORD	0
Key: Parameters	**Value Name:** EnableICMPRedirect	REG_DWORD	0
Key: Parameters	**Value Name:** EnablePMTUDiscovery	REG_DWORD	0
Key: Parameters	**Value Name:** EnableSecurityFilters	REG_DWORD	1
Key: Parameters	**Value Name:** KeepAliveTime	REG_DWORD	300,000
Key: Parameters	**Value Name:** PerformRouterDiscovery	REG_DWORD	0
Key: Parameters	**Value Name:** SynAttackProtect	REG_DWORD	2
Key: Parameters	**Value Name:** TcpMaxConnectResponseRetransmissions	REG_DWORD	2
Key: Parameters	**Value Name:** TcpMaxConnectRetransmissions	REG_DWORD	3
Key: Parameters	**Value Name:** TCPMaxPortsExhausted	REG_DWORD	5

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\NetBT		Format	Value
Key: Parameters	**Value Name:** NoNameReleaseOnDemand	REG_DWORD	1

Make screensaver password protection immediate

The grace period allowed for user movement before screensaver lock is considered is set to a default of 5 seconds. An entry to the registry can be made to adjust the length of the delay. To make password protection effective immediately, it is "recommended" that the value of this entry be set to 0. To set this value, edit the Registry key as shown in the table below and create the value name ScreenSaverGracePeriod with a value of 0.

Key Path: HKLM\Software\Microsoft\Windows NT\CurrentVersion		Format	Value
Key: Winlogon	**Value Name:** ScreenSaverGracePeriod	REG_SZ	0

Review time service authentication

Review the key shown in the table below to ensure the "type" value is set to NT5DS. This ensures the Evaluated Configuration is operating with authenticated time service.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\W32Time		Format	Value
Key: Parameters	**Value Name:** type	REG_SZ	Nt5DS

Disable LMHash creation

Windows 2000-based servers can authenticate computers running all previous versions of Windows. However, previous versions of Windows do not use Kerberos for authentication, so Windows 2000 supports LAN Manager (LM), Windows NT (NTLM) and NTLM version 2 (NTLMv2). The LM hash is relatively weak compared to the NTLM hash and therefore prone to rapid brute force attack. For the Evaluated Configuration LM authentication is not required and can therefore be disabled to ensure greater security. Windows 2000 Service Packs 2 and higher provide a registry setting to disable the storage of the LM hashes. Additional details can be found in Microsoft Knowledge Base article Q299656 "New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager". To set this value, edit the Registry key as shown in the table below and create the key name NoLMHash.

Key Path: HKLM\SYSTEM\CurrentControlSet\Control\Lsa		**Format**	**Value**
Key: NoLMHash	**Value Name:** A value name is not necessary	N/A	N/A

Disable autorun

Autorun begins reading from a drive as soon as media is inserted in it. As a result, the setup file of programs and the sound on audio media starts immediately. To prevent a possible malicious program from starting when media is inserted, create the following Registry value to disable autorun on all drives.

Key Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies		**Format**	**Value**
Key: Explorer	**Value Name:** NoDriveTypeAutoRun	REG_DWORD	255

Review Service Pack 3 Registry entries

Service Pack 3 introduces a number of new registry entries that can be configured to enhance the security provided by the operating system.

LDAP BIND command request settings

This value is used to determine the LDAP server (ldapagnt.lib) handling of LDAP bind command requests as follows.

- 1 (default) or not defined: The AD's LDAP agent always supports LDAP client request for LDAP traffic signing when handling a LDAP bind command request which specifies a SASL authentication mechanism.
- 2: The AD's LDAP agent only supports SASL in a LDAP bind command request unless the incoming request is already protected with TLS/SSL. It rejects the LDAP bind command request if other types of authentication are used. If the LDAP bind command request does not come in via TLS/SSL, it requires the LDAP traffic signing option in the client security context.

To set this value, edit the Registry key as shown in the table below and create the value name LdapServerIntegrity with a value of 2.

Key Path: HKLM\System\CurrentControlSet\Services\NTDS		Format	Value
Key: Parameters	**Value Name:** LdapServerIntegrity	REG_DWORD	2

Generate administrative alert when the audit log is full

To add Alerter service recipients for Windows 2000 based computers, edit the Registry (using Regedt32.exe) as shown in the table below. The Value entry will be the name of each recipient (user name or computer name) that is to receive the administrative alerts. Each recipient should be on a separate line in the **Data** dialog box.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\Alerter		Format	Value
Key: Parameters	**Value Name:** AlertNames	REG_MULTI_SZ	As explained above

Note: Administrative alerts rely on both the Alerter and Messenger services. Make sure that the Alerter service is running on the source computer and that the Messenger service is running on the recipient computer.

Audit Log Management

Management options for event logs, including the security log, can be configured for all computers in a domain by using the Even Log folder within the Domain Security Policy or a specific Group Policy object associated with domains, OUs, and sites (Domains). The Event Log folder does not appear in the Local Security Policy object.

For domain members, the management options for local audit can be configured using the Event Viewer Snap-In. From the Event Viewer, the applicable Properties interface is selected to set the management options for a particular log, such as the Security log.

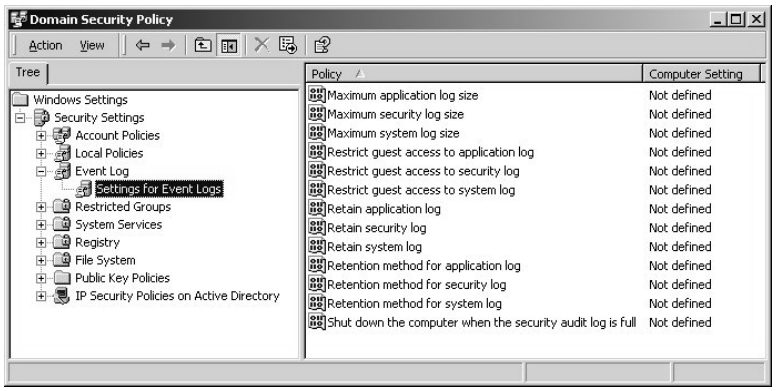
These interfaces allow for viewing, sorting, filtering, and searching the event logs as well as setting the maximum log size or clearing the log. The user must have access to the event log file in order to successfully view it. To view the contents of the security log, the user must be logged on as a member of the Administrator's group. No special privilege is required to use the Event Viewer itself. Security is enforced by the ACL on the log and certain registry settings.

Access the Settings for Event Logs

View current settings for event logs and allow editing.

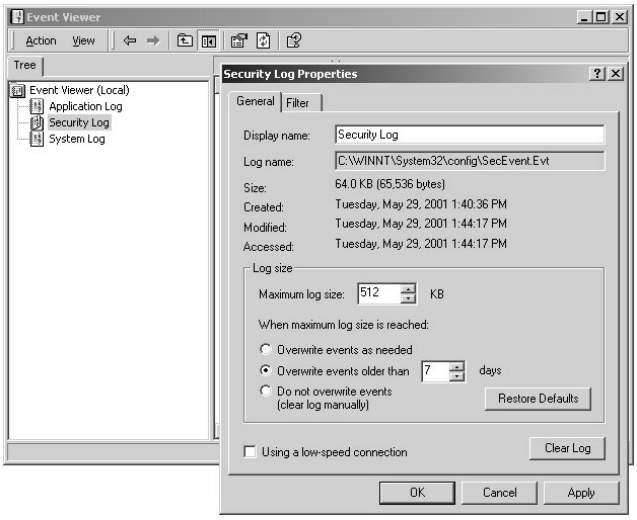
Procedure for Domain and Domain Controller Policies:

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand **Security Settings**.
3. Within **Security Settings**, expand **Event Log** to reveal the **Settings for Event Logs** policy.
4. Click on the **Settings for Event Logs** object. The right-hand details pane will reveal the configurable audit log management settings.



Procedure for Standalone Workstations and Servers:

1. Open the Event Viewer, Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**.
2. Right-click on the **Security Log** object and select **Properties**. The **Security Log Properties** window will appear revealing the configurable audit log management settings.



Set the Audit Policies as required or recommended in Table 4.8.

Table 4.8 Audit Management Settings

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
Set Maximum Application Log Size **Security Objective:** Specifies the maximum size for the Application event log. The default is 512KB, and the maximum size is 4GB (4,194,240KB). Requirements for the Application log size vary depending the function of the platform and the need for historical records of application related events. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum application log size** in the right-hand details pane. b. Check the **Define this policy setting** box. c. Enter the desired value for the application log size in the text box. For most environments, the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** a. In the **Application Log Properties** window, under the **General** tab, enter the desired value for the application log size in the **Maximum log size:** text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. b. Click the **OK** button.	✓	✓	✓		✓
Set Maximum Security Log Size **Security Objective:** Specifies the maximum size for the Security event log. The default is 512KB, and the maximum size is 4GB. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum security log size** in the right-hand details pane. b. Check the **Define this policy setting** box. c. Enter the desired value for the security log size in the text box. The log retention method for the security log should be set to not overwrite events, therefore a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button.			✓		✓

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
Procedure for Standalone Windows 2000 Professional and Server: a. In the **Security Log Properties** window, under the **General tab**, enter the desired value for the application log size in the **Maximum log size**: text box. The log retention method for the security log should be set to not overwrite events, therefore a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. b. Click the **OK** button.	✓	✓			✓
Set Maximum System Log Size **Security Objective:** Specifies the maximum size for the System event log. The default is 512KB, and the maximum size is 4GB. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum system log size** in the right-hand details pane. b. Check the **Define this policy setting** box. c. Enter the desired value for the system log size in the text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** a. In the **System Log Properties** window, under the **General** tab, enter the desired value for the system log size in the **Maximum** log size: text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared. b. Click the **OK** button.	✓	✓	✓		✓
Restrict Guest Access to the Application Log **Security Objective**: Prevent anonymous access to the Application event log. If this policy is enabled, guests are prevented from access to the Application event log. By default, this policy is disabled locally on all Windows 2000 operating systems. **Procedure for Domain and Domain Controller Policies**: a. Double click on **Restrict guest access** to application log in the right-hand details pane. b. Check the **Define these policy** settings box.			✓		✓

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
c. Select the Enabled radio button and click the **OK** button. **Procedure for Standalone Workstations and Servers:** Not available on standalone workstations and servers.					
Restrict Guest Access to the Security Log **Security Objective:** Prevent anonymous access to the Security event log. If this policy is enabled, guests are prevented from access to the Security event log. By default, this policy is disabled locally on all Windows 2000 operating systems. A user must possess the **Manage auditing and security log** user right in order to access the security log. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Restrict guest access to security log** in the right-hand details pane. b. Check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** Not available on standalone workstations and servers.			✓		✓
Restrict Guest Access to the System Log **Security Objective:** Prevent anonymous access to the System event log. If this policy is enabled, guests are prevented from access to the System event log. By default, this policy is disabled locally on all Windows 2000 operating systems. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Restrict guest access to system log** in the right-hand details pane. b. Check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** Not available on standalone workstations and servers.			✓		✓
Retain Application Log **Security Objective:** Determines the number of days' worth of events that should be retained for the Application log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **Application Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum Application log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**."			✓		✓

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
Procedure for Standalone Windows 2000 Professional and Server: Do not change the default number of days (7) set in the **Overwrite events older than** option of the **Application Log Properties** window.	✓	✓			✓
Retain Security Log **Security Objective:** Determines the number of days' worth of events that should be retained for the Security log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **Security Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum Security log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**." **Procedure for Standalone Windows 2000 Professional and Server:** Do not change the default number of days (7) set in the **Overwrite events older than** option of the **Security Log Properties** window.	✓	✓	✓		✓
Retain System Log **Security Objective:** Determines the number of days' worth of events that should be retained for the System log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **System Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum System log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**." **Procedure for Standalone Windows 2000 Professional and Server:** Do not change the default number of days (7) set in the **Overwrite events older than** option of the **System Log Properties** window.	✓	✓	✓		✓

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
Retention Method for Application Log **Security Objective:** Determines how Application logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of **"Not defined."** **Procedure for Standalone Windows 2000 Professional and Server:** Do not change the **Overwrite events older than** (7 days) option of the **System Log Properties** window.	✓	✓	✓		✓
Retention Method for Security Log **Security Objective:** Determines how Security logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Retention method for Security log** in the right-hand details pane. b. Check the **Define these policy settings** box. c. Select the **Do not overwrite events (clear log manually)** radio button and click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** a. In the **Security Log Properties** window, under the **General** tab, select the **Do not overwrite events (clear log manually)** radio button. b. Click the **OK** button.	✓	✓	✓		✓
Retention Method for System Log **Security Objective:** Determines how System logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**." **Procedure for Standalone Windows 2000 Professional and Server:** Do not change the **Overwrite events older than** (7 days) option of the **System Log Properties** window.	✓	✓	✓		✓
Shut Down the Computer when the Security Log is Full **Security Objective:** Determines whether the system should shut down if it is unable to log security events. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method	✓	✓	✓		✓

Audit Management and Configuration	Professional	Server	DC	Required	Recommended
specified for the security log is either **Do Not Overwrite Events** or **Overwrite Events by Days.** **Procedure**: Use the Shut down system immediately if unable to log security audits security option instead of this policy setting. This policy setting is not available in standalone workstations and servers. **Note:** The ST requires the system to be able to prevent auditable events from occurring, except those taken by the administrator, if the audit log is full. If the administrator desires this functionality, this option must be enabled.					

Default Group Accounts

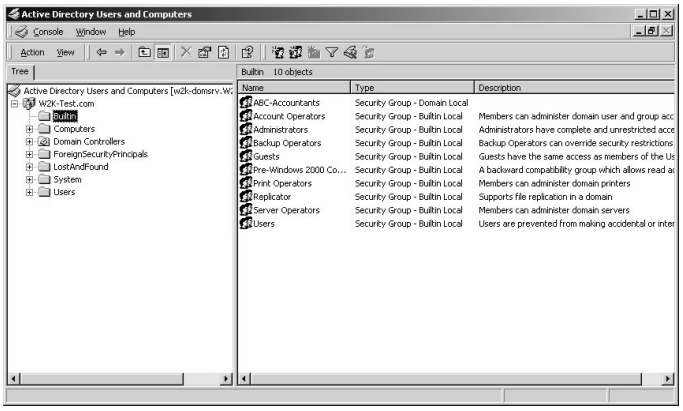
This subsection discusses required and recommended changes to default group memberships for the built-in groups found in default Windows 2000 operating system installations. These built-in groups have a predefined set of user rights and privileges as well as group members. The four built-in groups are defined as follows:

- **Global Groups.** When a Windows 2000 domain is established, built-in global groups are created in the Active Directory store. Global groups are used to group common types of user and group accounts for use throughout the entire domain.
- **Domain Local Groups.** Domain local groups provide users with privileges and permissions to perform tasks specifically on the domain controller and in the Active Directory store.
- **Local Groups.** Stand-alone Windows 2000 Servers, member servers, and Professional workstations have built-in local groups. These built-in local groups provide members with the capability to perform tasks only on the specific computer to which the group belongs.
- **System Groups.** System groups do not have specific memberships that can be modified. Each is used to represent a specific class of users or to represent the operating system itself. These groups are created within Windows 2000 operating systems automatically, but are not shown in the group administration GUIs.

Note: Appendix D – User and Group Accounts, provides a complete description of the default group account settings to be maintained in the evaluated configuration, including additional details, applicable ST requirements, and recommended changes.

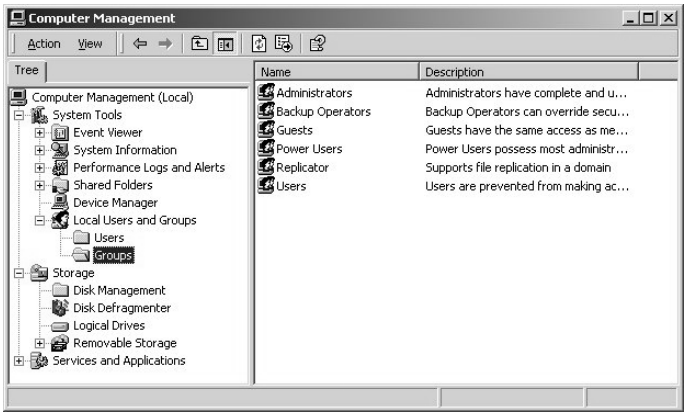
Review / Modify Group Account Memberships for a Domain

1. To access group accounts within a Domain, log in with an administrative account on the Domain Controller.
2. Open **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, double-click the domain node.
4. Group accounts are found in the **Builtin** and **Users** containers.



Review / Modify Group Account Memberships for a Standalone

1. To access group accounts within a Standalone or individual Domain Member computer, log in with an administrative account.
2. Open **Start**, point to **Administrative Tools**, and then click **Computer Management**.
3. In the console tree, double-click on **Local Users and Groups**.
4. Group accounts are found in the **Groups** container.



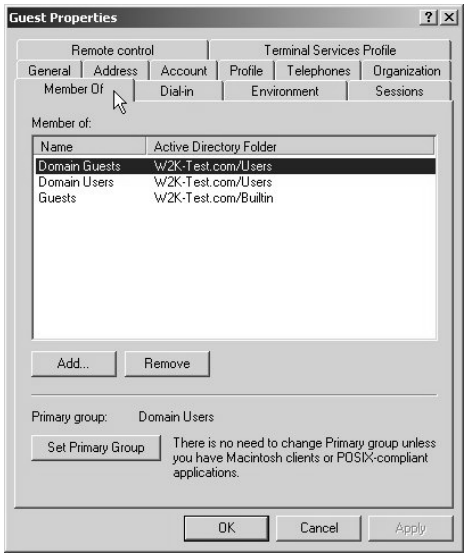
Note: Set Group Memberships as required or recommended in Table 4.9.

Change the Primary Group Membership of an Account

Some of the required group membership changes identified in the table below call for removing an account from a specific group. Within a domain, accounts must have a primary group assignment. It may therefore be necessary to first change the account's primary group membership that is set by default when a computer is joined to a domain. If an attempt is made to remove an account from its primary group, the action will be denied and the following message will appear:

Use the following procedures to change an account's primary group:

1. Log in with an administrative account on the Domain Controller.
2. Open **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, double-click the domain node.
4. User accounts are found in the **Users** container.
5. Right-click on the account name and select **Properties** from the menu. The account **Properties** GUI will appear.
6. Click on the **Member Of** tab to display the list of groups the account belongs to. Observe that when clicking any of the groups in the **Member of:** window, the **Set Primary Group** button will be either active or inactive. The **Set Primary Group** button will be active for groups which can be set as primary groups and will be inactive for groups either cannot be set as primary groups or which are already the primary group.



7. To change the primary group of the account, select the group that will become the new primary group and click on the **Set Primary Group** (must have the **Set Primary Group** button active). Note that the group identified above the **Set Primary Group** button as the **Primary group:** will change to the new selection.
8. Click the **Apply** and click **OK**.

Note: The account can also be removed from a group through **Member of** tab interface of the **Properties** GUI by selection the group from which it is to be removed and clicking the **Remove** button.

Table 4.9 Group Memberships

Group Account Modifications			Professional	Server	DC	Required	Recommended
Global Groups	**Default Members**	**Modification / Verification**					
DnsUpdateProxy	None	Do not add accounts to this group.			✓	✓	
Domain Admins	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Domain Guests	Guest	Do not add accounts to this group.			✓	✓	
Domain Users	Administrator Guest Krbtgt TsInternetUser (All new users are added by default)	Remove the Guest account and ensure the TsInternetUser account is disabled. **Note:** Before removing the Guest account, change the primary group for that account to Domain Guests.			✓	✓	
Enterprise Admins	Administrator (Domain Controller Administrator)	Do not add non-administrative accounts to this group.			✓	✓	
Group Policy Creator Owner	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Schema Admins	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Domain Local Groups	**Default Members**	**Modification / Verification**					
Account Operators	None	Do not add non-administrative accounts to this group.			✓	✓	

Group Account Modifications			Professional	Server	DC	Required	Recommended
Administrators	Administrator Domain Admins Enterprise Admins	Do not add non-administrative accounts to this group.			✓	✓	
Backup Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
DnsAdmins	None	Do not add non-administrative accounts to this group.			✓	✓	
Guests	Guest (Local) Domain Guests TsInternetUser	Do not use this group. Remove all accounts, including Guest, from this group.			✓	✓	
Pre-Windows 2000 Compatible Access	None	Provides backward compatibility with pre-Windows 2000 operating systems. Does not meet objectives of the TOE, therefore do not use this group.			✓	✓	
Print Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
Replicator	None	Do not add non-administrative accounts to this group.			✓	✓	
Server Operators	None	Do not add non-administrative accounts to this group.			✓	✓	

Group Account Modifications			Professional	Server	DC	Required	Recommended
Users	Authenticated Users Domain Users INTERACTIVE (All new local users are added by default)	Do not add accounts with a potential for unauthenticated access (such as Guest) to this group.			✓	✓	
Local Groups	**Default Members**	**Modification / Verification**					
Administrators	**Stand-Alone**: Administrator **Domain Member**: Administrator Domain Admins	Do not add non-administrative accounts to this group.	✓	✓		✓	
Backup Operators	None	Do not add non-administrative accounts to this group.	✓	✓		✓	
Guests	**Stand-Alone Professional**: Guest **Stand-Alone Server**: Guest TsInternetUser **Domain Member**: Add Domain Guests to the above	Do not use this group. Remove all accounts, including Guest, from this group.	✓	✓		✓	
Power Users	None	Do not add non-administrative accounts to this group.	✓	✓		✓	

Group Account Modifications			Professional	Server	DC	Required	Recommended
Replicator	None	Do not add non-administrative accounts to this group.	✓	✓		✓	
Users	**Stand-Alone**: Authenticated Users INTERACTIVE (All new local users are added by default) **Domain Member**: Authenticated Users Domain Users INTERACTIVE (All new local users are added by default)	Do not add accounts with a potential for unauthenticated access (such as Guest) to this group.	✓	✓		✓	
System Groups	**Default Members**	**Modification / Verification**					
Anonymous Logon	All unauthenticated users	Do not use this group. Do not grant resource permissions or user rights to this group.	✓	✓	✓	✓	
Authenticated Users	All authenticated users	Use the Authenticated Users group instead of the Everyone to prevent the potential for anonymous access to a resource.	✓	✓	✓	✓	
DIALUP	All dial-in users	Dial-up service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.	✓	✓	✓	✓	

Group Account Modifications			Professional	Server	DC	Required	Recommended
Everyone	All users accessing the computer, either locally, through the network, or through RAS. This includes all authenticated and unauthenticated users.	Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.	✓	✓	✓	✓	
TERMINAL SERVER USER	None	Terminal Service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.	✓	✓	✓	✓	

Default User Accounts

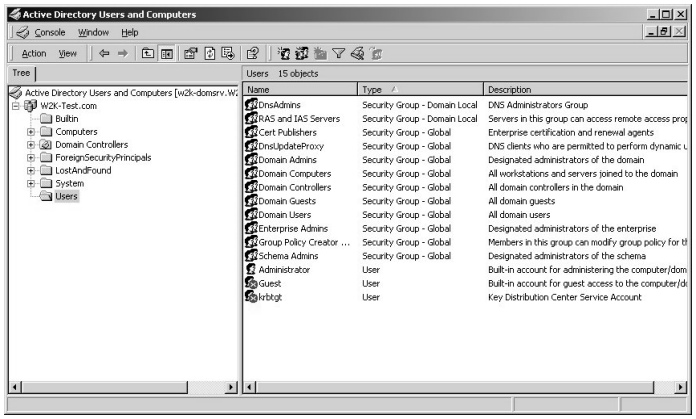
This subsection discusses required and recommended changes to built-in user accounts found in default Windows 2000 operating system installations. The built-in user accounts include Administrator, Guest, and TsInternetUser.

Note: Appendix D – User and Group Accounts, provides a complete description of the default group account settings to be maintained in the evaluated configuration, including additional details, applicable ST requirements, and recommended changes.

Review / Modify Default User Accounts for a Domain

Review or modify user accounts to ensure compliance with ST requirements.

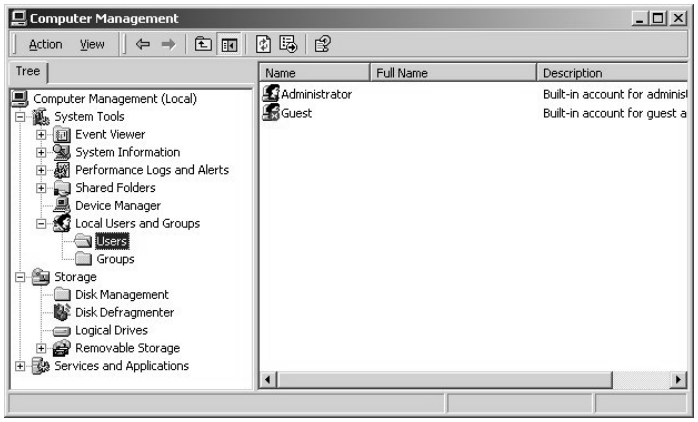
1. To access user accounts within a Domain, log in with an administrative account on the Domain Controller.
2. Open **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, expand the domain node.
4. User accounts are found in the **Users** container.



Review / Modify Default User Accounts Locally

Review or modify user accounts within a Standalone or individual Domain Member computer to ensure compliance with ST requirements.

1. Open **Start**, point to **Administrative Tools**, and then select **Computer Management**.
2. In the console tree, expand **Local Users and Groups**.
3. User accounts are found in the **Users** container.



Modify User Accounts as required or recommended in Table 4.10.

Table 4.10 Default User Accounts

User Account Modifications			Professional	Server	DC	Required	Recommended
Local User Accounts	**Description**	**Modification / Verification**					
Administrator	Built-in account for administering the computer/Domain.	Do not use this account for day-to-day administration. Assign roles to authorized administrators by placing their user accounts in administrative groups appropriate to their level of responsibility. Rename the Administrator account and secure the password for emergency use only.	✓	✓	✓	✓	
Guest	Built-in account for guest access to the computer/Domain.	This account must remain disabled.	✓	✓	✓	✓	
TsInternetUser	User account used by Terminal Services. It is used by the Terminal Services Internet Connector License and is available on Windows 2000 Servers. When Internet Connector Licensing is enabled, a Windows 2000-based server accepts 200 anonymous-only connections. Terminal Services clients are not prompted with a logon dialog box; they are logged on automatically with the TsInternetUser account.	Terminal Services is not an objective of the Evaluated Configuration and accounts that support anonymous access are not to be allowed. Therefore, disable this account.		✓	✓	✓	

System Services

Table 4.11 lists the system services that may be enabled in an Evaluated Configuration. To remain in the Evaluated Configuration, it is acceptable to have all of the listed services, or a subset of them, enabled and running.

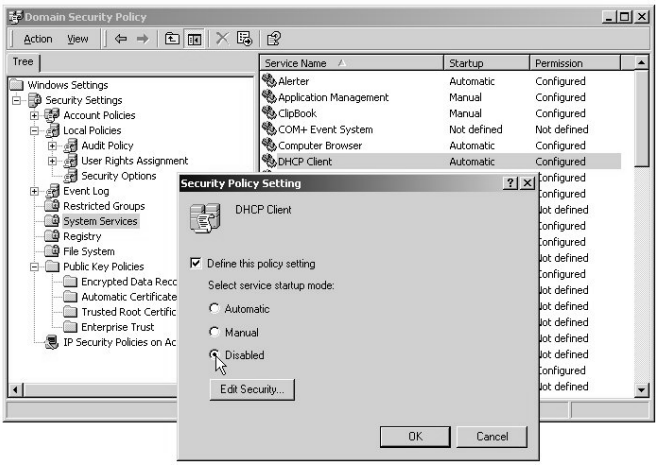
To enable or disable services on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local settings on individual Windows 2000 platforms can be set through the Computer Management interface.

Note: Enabling or installing new services not identified as enabled in the table below is outside the scope of Common Criteria Evaluated Configuration. The Common Criteria Evaluated Configuration includes no auditing capability for administrators installing, enabling, or disabling services. Hence, management of services can only be accomplished outside the Evaluated Configuration, though the Evaluated Configuration can be reestablished subsequently.

Disable Unnecessary System Services on Domain Computers

Set a policy to disable unnecessary services within a Domain. Set a policy to disable unnecessary services for Domain Controllers.

1. Open the **Domain Security Policy** or the **Domain Controller Security Policy** as applicable.
2. Expand **Security Settings** and click on **System Services**.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Security**.
4. In the **Security Policy Setting** dialog window, check the **Define this policy setting** box and then select the **Disabled** radio button.

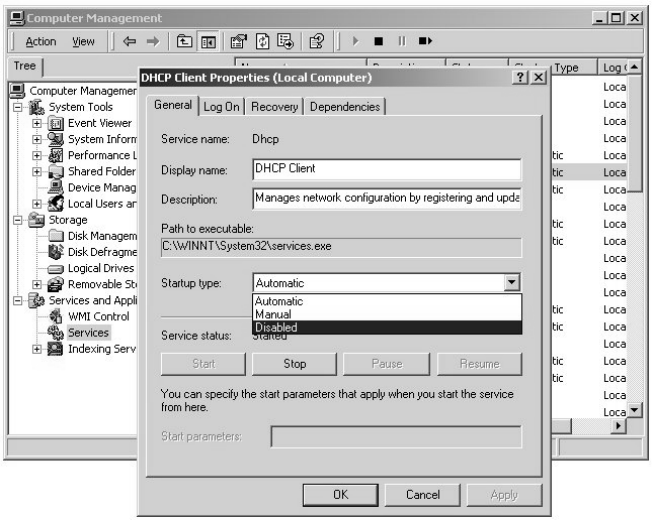


5. Click the **OK** button.

Disable Unnecessary System Services Locally

Disable unnecessary services locally on Windows 2000 Server or Professional operating systems.

1. Open the **Computer Management** interface.
2. In the console tree, expand **Services and Applications** and select **Services**.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Properties**.
4. The **Properties** dialog box for the selected services will appear. From the **Startup type:** drop down menu, select **Disabled**.



5. Under **Service status:** click on the **Stop** button.
6. Click the **OK** button.

Evaluated Configuration System Services

Table 4.11 lists the system services that may be enabled in an Evaluated Configuration. To remain in the Evaluated Configuration, it is acceptable to have all of the listed services, or a subset of them, enabled and running, all other services must be disabled.

Table 4.11 Acceptable Services for the Evaluated Configuration

List of Evaluated Services	
Alerter Service	Network Connections
COM+ Event System	NTLM Security Support Provider
Computer Browser	Plug and Play
DHCP Client	Print Spooler
DHCP Server	Protected Storage
Distributed File System (DFS)	Remote Procedure Call (RPC)
DNS Client	Remote Procedure Call (RPC) Locator
DNS Server	Remote Registry Service
Event Log	Security Accounts Manager
File Replication Service	Server
Intersite Messaging	System Event Notification
IPSec Policy Agent	TCP/IP NetBIOS Helper Service
Kerberos Key Distribution Center	Windows Internet Name Service (WINS)
Logical Disk Manager	Windows Management Instrumentation
Logical Disk Manager Administrative Service	Windows Management Instrumentation Driver Extensions
Messenger	Windows Time
Net Logon	Workstation

Securing the File System

Among the files and directories to be protected are those that make up the Windows 2000 operating system itself. The default set of file and directory permissions provides a minimal level of security that allows ease of software installation and customization of the operating environment without impacting usability. Default file and directory permissions that are applied during operating system installation are captured into the “setup security.inf” security template file, which is described as containing the “out of box default security settings.”

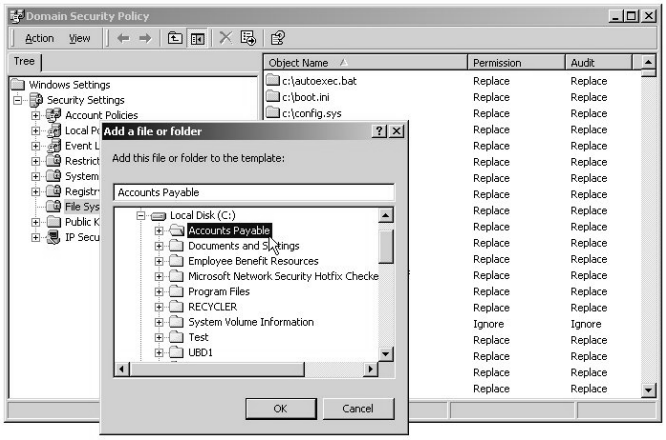
To ensure greater security, consider modifying file, directory, and subdirectory permissions as recommended in the table presented in this subsection, immediately after installing the operating system. Be sure to apply permissions to parent directories before applying them to subdirectories. The permission changes recommended below apply to all Windows 2000 operating systems. To implement permissions on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local permissions on individual Windows 2000 platforms can be set through the Windows Explorer interface.

Detailed instructions for setting individual permissions using the Windows Explorer interface are provided in the Data Protection subsection of the Windows 2000 Evaluated Configuration Administrator’s Guide.

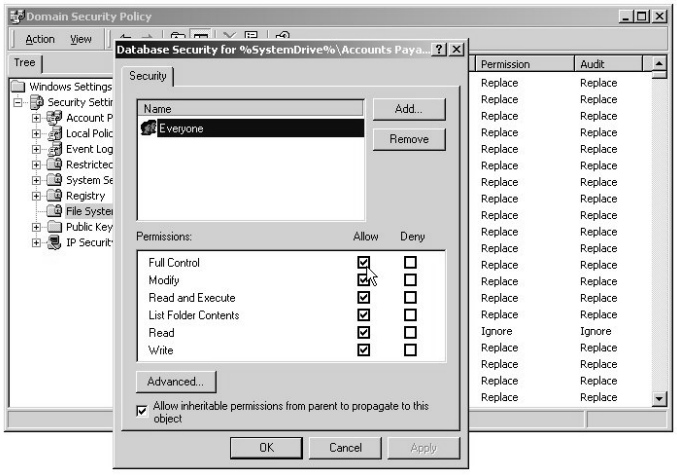
Set Permissions through a Domain Policy

Set a file and folder permissions policy for the Domain. Set a file and folder permissions policy for Domain Controllers.

1. Open the **Domain Security Policy** or the **Domain Controller Security Policy** as applicable.
2. Expand **Security Settings**.
3. Within **Security Settings**, right-click on **File System**.
4. Select **Add File**.
5. From the **Add a file or folder window**, navigate to and select the desired file or folder.



6. Click the **OK** button. A **Database Security for *path\filename* Properties** window will appear.

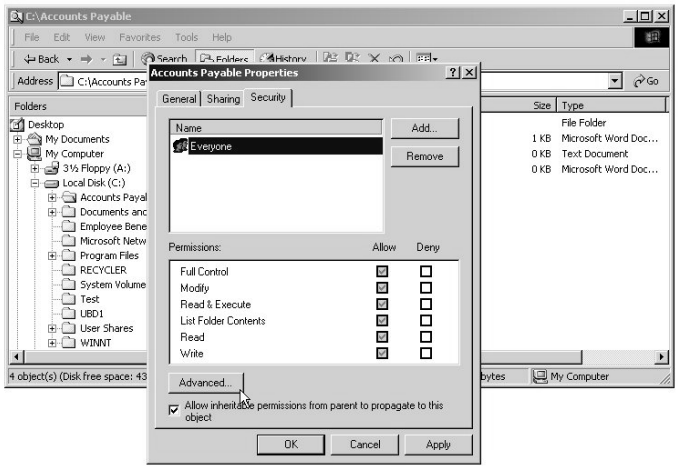


7. Set permissions as necessary. Detailed procedures are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. File and Folder permission settings are provided in Table 4.12.

Set Permissions Locally through Windows Explorer

Set file and folder permissions locally on Windows 2000 Server or Professional operating systems.

1. Open **Windows Explorer**.
2. Navigate to and select the desired file or folder.
3. Right-click on the file or folder and select **Properties**.
4. In the properties window, select the **Security** tab. Click **Advanced** for more detailed permission settings.



5. Set permissions as necessary. Detailed procedures are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. File and Folder permission settings are provided in Table 4.12.

Note: Through the Advanced tab, permissions are propagated by applying them to the current folder, subfolder, and files. Permissions are replaced locally by applying them only to the current folder and files, or the current file object.

Table 4.12 File and Folder Permission Settings

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
C:\autoexec.bat	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace	✓	
C:\boot.ini	**Administrators:** Full Control **SYSTEM:** Full Control	Replace	✓	

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
C:\config.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace	✓	
C:\ntbootdd.sys **Note:** used when SCSI is available.	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
C:\ntdetect.com	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
C:\ntldr	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%ProgramFiles%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDirectory%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDirectory%\appmgmt	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\config	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\dllcache	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\DTCLog	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\GroupPolicy	**Administrators:** Full Control **Authenticated Users:** Read, Execute	Propagate		✓

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
	SYSTEM: Full Control			
%SystemDirectory%\ias	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\Ntbackup.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\NTMSData	**Administrators:** Full Control **SYSTEM:** Full Control	Propagate		✓
%SystemDirectory%\rcp.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\Regedt32.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\repl	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\repl\export	**Administrators:** Full Control **CREATOR OWNER:** Full Control **Replicator:** Read, Execute **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\repl\import	**Administrators:** Full Control **Replicator:** Modify **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\rexec.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\rsh.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\secedit.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\Setup	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
%SystemDirectory%\spool\Printers	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (Folder and Subfolders)	Replace		✓
%SystemDrive% **Note:** Drive where the Windows 2000 operating system is installed.	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDrive%\Documents and Settings	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDrive%\Documents and Settings\ Administrator	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDrive%\Documents and Settings\ All Users	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson **Note:** Folder containing Dr Watson application error log.	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson\ drwtsn32.log **Note:** Dr Watson application error log file.	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control **Users:** Modify	Replace	✓	

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
%SystemDrive%\io.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDrive%\msdos.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDrive%\Temp	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	
%SystemRoot%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemRoot%\$NtServicePackUninstall$	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemRoot%\debug	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemRoot%\debug\UserMode	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** (Folder only) - Traverse folder, List folder, Create files. (Files only) – Create files, create folders	Propagate		✓
%SystemRoot%\regedit.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
%SystemRoot%\Registration	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read	Propagate		✓
%SystemRoot%\repair	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemRoot%\ Temp	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	

Share Folder Permissions

The native Windows 2000 file sharing service is provided using the SMB-based server and redirector services. Even though only administrators can create shares, the default security placed on the shares allows the group Everyone to have Full Control access. These permissions allow access to the network-visible shares themselves. Access to the files and subfolders displayed through the share is controlled by the NTFS permissions that are set on the underlying folder a share maps to. It is therefore recommended that proper security be applied via NTFS permissions to any files and folders mapped by a share. Detailed procedures for setting share permissions are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. However, the Evaluated Configuration must not include any shares other than the administrative shares that are set by default during installation. A description of administrative shares is provided in the Windows 2000 Evaluated Configuration Administrator's Guide.

Securing the Registry

In addition to the considerations for standard security described in this document, security administrators may want to increase protections on certain keys within the Windows 2000 Registry. By default, protections are set on various components of the registry that allow work to be done while providing standard-level security. Default Registry key permissions that are applied during operating system installation are captured into the "setup security.inf" security template file, which is described as containing the "out of box default security settings."

Microsoft has made improvements to the default Registry ACL settings for Windows 2000 to address security issues associated with the default Registry ACL settings identified for Windows NT 4.0. To ensure compliance with Evaluated Configuration requirements for restricting Registry access for non-administrators, it is essential that the default settings not be altered with the exception of the required ACL changes defined in Table 4.13. The changes should be done with caution, because programs that users require in order to access their applications often need

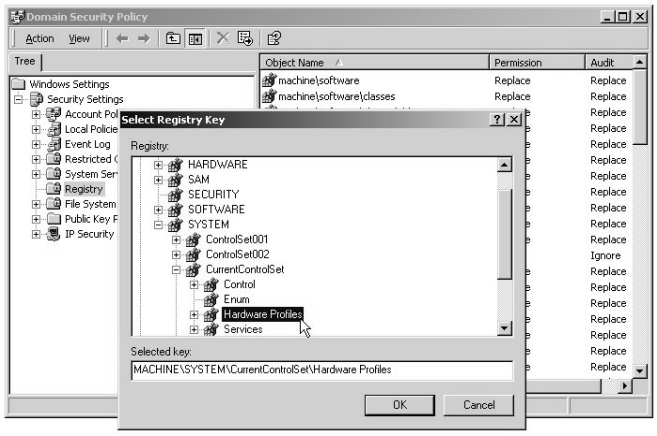
access to certain Registry keys on the user's behalf. The required permission changes apply to all Windows 2000 operating systems.

To implement permissions on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local permissions on individual Windows 2000 platforms can be set through the Regedt32.exe interface. To change a Registry key, a user must have the TakeOwnership privilege or be the owner of the key.

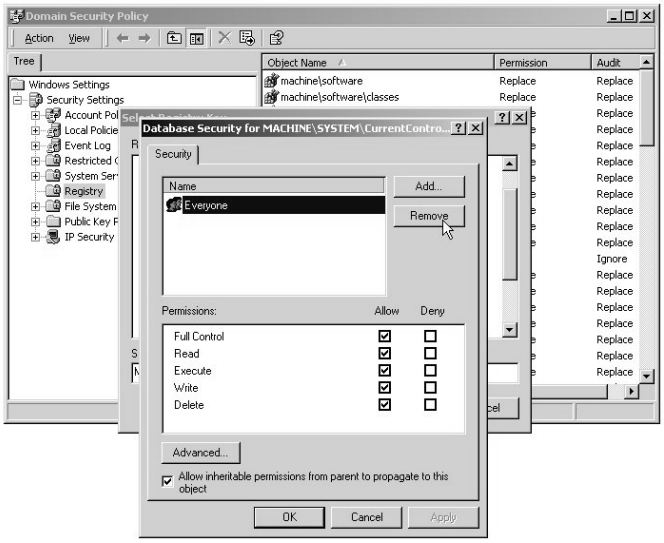
Set Registry Permissions through a Domain Policy

Set Registry permissions policies for the Domain and for Domain Controllers.

1. Open the **Domain Security Policy** or the **Domain Controller Security Policy** as applicable.
2. Expand **Security Settings**.
3. Within **Security Settings**, right-click on **Registry**.
4. Select **Add key**.
5. From the **Select Registry Key** window, navigate to and select the desired key.



6. Click the **OK** button. A **Database Security for *path* Properties** window will appear.

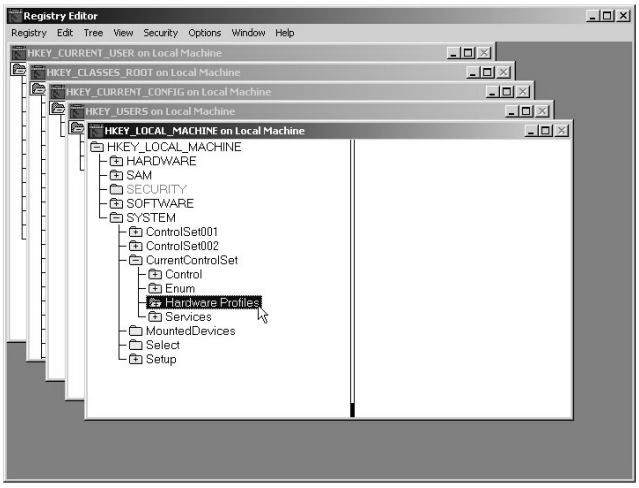


7. Set permissions as necessary. Required ACL changes are provided in Table 4.13.

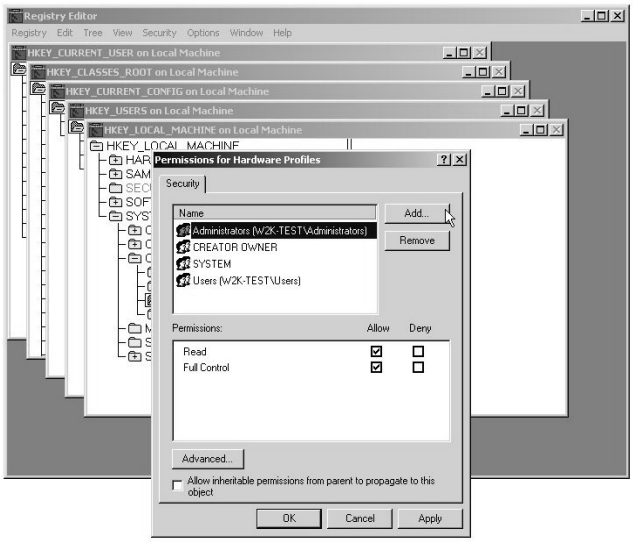
Set Registry Permissions through Regedt32.exe

Set file and folder permissions locally on Windows 2000 Server or Professional operating systems.

1. Click the **Start** button and select **Run…**
2. Within the **Run** dialog window's text box, type **regedt32** and click the **OK** button to open the **Registry Editor** (Regedt32.exe).
3. Navigate to and select the desired Registry key.



4. From the **Security** menu, select **Permissions**. The **Permissions for…** dialog window will appear. Click **Advanced** for more detailed permission settings.



5. Set permissions as necessary. Required ACL changes are provided in Table 4.13.

Notes:

- Through the Advanced tab, permissions are propagated by applying them to the current key, and subkeys. Permissions are replaced by applying them to the current key only.
- The "Read Control" ACL in Regedt32.exe is called "Read Permissions" in the Security Policy tools.
- The Power Users group shown in the table below is not available on a Domain Controller and cannot be manually set from a Domain Controller.

Table 4.13 Required Registry Permission Changes

Registry Key	Subkey ACL Settings Special (Read, Write, Delete) = Query value, set value, create subkey, enumerate subkey, notify, delete, read control Read = Query value, enumerate subkey, notify, read control Apply to "This subkey and subkeys" unless otherwise noted.	Inheritance Method (Used via Security Policy tools)
HKEY_LOCAL_MACHINE		
\SOFTWARE	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **Power Users**: Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\classes	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate

Registry Key	Subkey ACL Settings Special (Read, Write, Delete) = Query value, set value, create subkey, enumerate subkey, notify, delete, read control Read = Query value, enumerate subkey, notify, read control Apply to "This subkey and subkeys" unless otherwise noted.	Inheritance Method (Used via Security Policy tools)
\SOFTWARE\classes\.hlp	**Administrators**: Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\classes\helpfile	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\Microsoft\OS/2 Subsystem for NT	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **SYSTEM:** Full Control **Note:** It may be necessary to remove the inheritance and replace the ACLs.	Propagate
\SOFTWARE\Microsoft\Windows NT\CurrentVersion	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\ComputerName	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\currentcontrolset\control \ContentIndex	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Keyboard Layout	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Keyboard Layouts	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Print\Printers	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete)	Replace

Registry Key	Subkey ACL Settings Special (Read, Write, Delete) = Query value, set value, create subkey, enumerate subkey, notify, delete, read control Read = Query value, enumerate subkey, notify, read control Apply to "This subkey and subkeys" unless otherwise noted.	Inheritance Method (Used via Security Policy tools)
	SYSTEM: Full Control **Users:** Read **Note:** Remove inheritance and replace all ACLs. Inherited ACLs may be copied to the current key.	
\SYSTEM\CurrentControlSet\ Control\ProductOptions	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\ Services\Eventlog	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\ Services\Tcpip	**Authenticated Users:** Read **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
HKEY_CLASSES_ROOT		
\HKEY_CLASSES_ROOT **Note:** This key is an alias to HKEY_LOCAL_MACHINE \SOFTWARE\Classes	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate

IPSec Policy

IPSec policies, rather than application programming interfaces (APIs), are used to configure IPSec security services. The policies provide variable levels of protection for most traffic types in most existing networks. IPSec policies can be configured to meet the security requirements of a user, group, application, domain, site, or global enterprise. Microsoft Windows 2000 provides an administrative interface called IPSec Policy Management to define IPSec policies for computers at the Active Directory level for any domain members, or on the local computer for non–domain members.

IPSec policies can be applied to computers, sites, domains, or any organizational units created in Active Directory. IPSec policies should be based on an organization's guidelines for secure operations. Through the use of security actions, called ***rules***, one policy can be applied to heterogeneous security groups of computers or to organizational units.

There are two storage locations for IPSec policies:

- Active Directory
- The local registry for stand-alone computers and computers which are not joined to the domain. When the computer is temporarily not joined to a trusted Microsoft Windows 2000 domain, the policy information is cached in the local registry.

Each policy should apply to a scenario considered in an organization's established security plan. Special configuration settings might apply if policies are assigned to a DHCP server, Domain Name System (DNS), Windows Internet Name Service (WINS), Simple Network Management Protocol (SNMP), or remote access server.

Detailed procedures for creating IPSec policies are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. There are no specific IPSec setting requirements for the Evaluated Configuration.

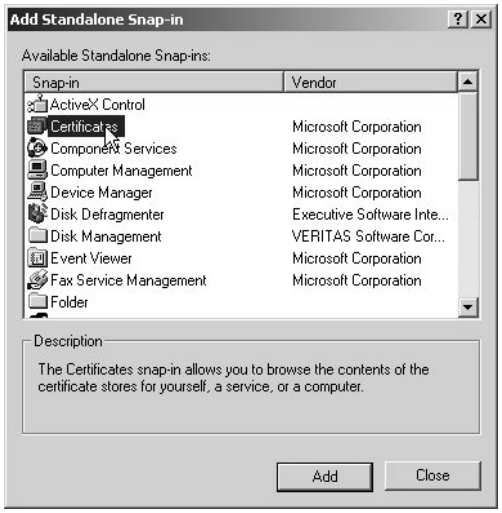
Encrypting File System

Windows 2000 operating systems provide a native ability to encrypt files and folders on an NTFS volume through the use of its Encrypting File System (EFS). EFS uses a private key encryption mechanism for storing data in encrypted form on the network. EFS runs as a service and uses both private key encryption and public key encryption.

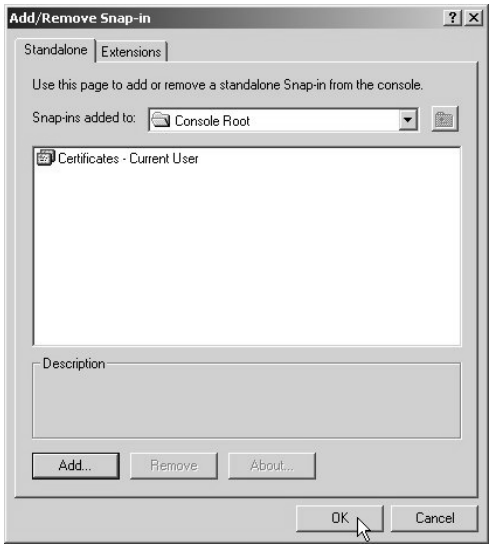
The ST requires the ability to enable, disable, and control EFS on NTFS volumes, however, there are no specific EFS configuration requirements for the Evaluated Configuration. Detailed procedures for enabling, using, and managing EFS, as well as for the storage and retrieval of encryption keys are provided in the Windows 2000 Evaluated Configuration Administrator's Guide.

After the initial installation of the operating system, it is recommended that a backup of the Administrator's encryption certificate and private key be made. The backup procedures are as follows:

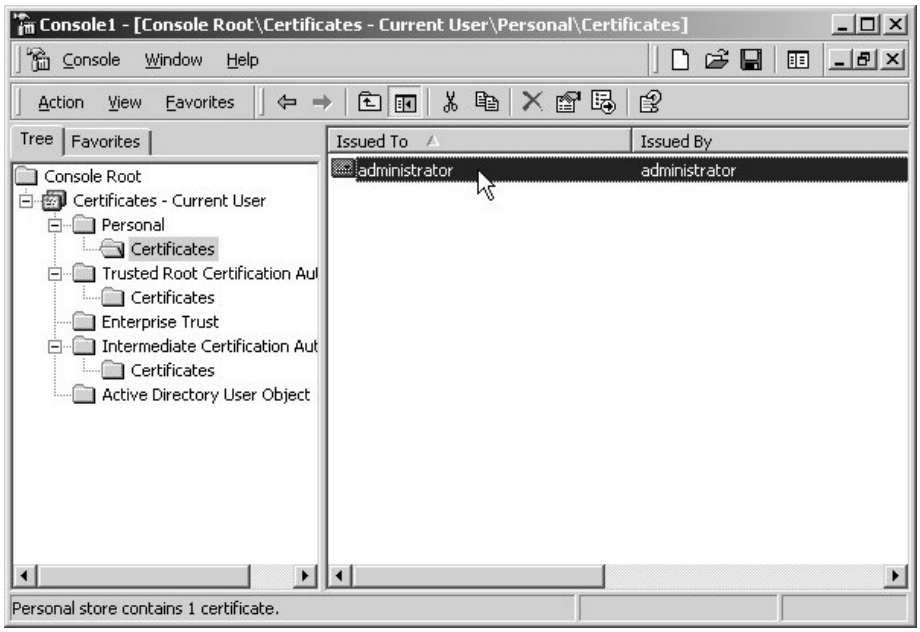
1. Click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
2. On the **Console** menu, click **Add/Remove snap-ins**, and click **Add**.
3. Locate the **Certificates** snap-in, and click **Add**.



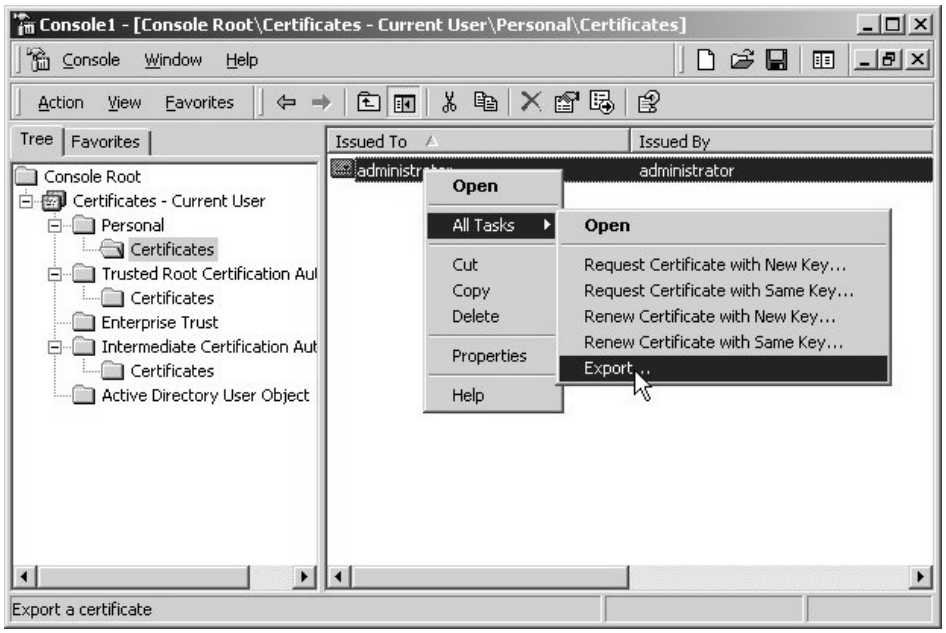
4. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.



5. Locate the **Encrypting File System** certificates in the Personal certificate store. Click the **+** next to **Certificates–Current User**. Expand the **Personal** folder. Select **Certificates**.



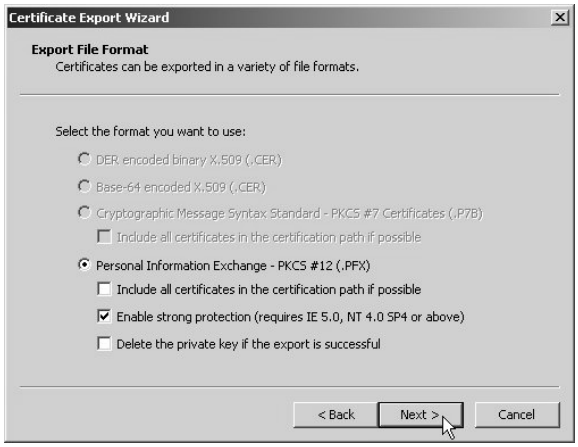
6. Right-click on the Administrator certificate, from the menu, select **All Tasks**, and click **Export**.



7. This starts the **Certificate Manager Export** wizard. Click **Next**.

8. Select the **Yes, export the private key** radio button. Click **Next**.

9. The export format available is **Personal Information Exchange-PKCS#12**, or .pfx - personal exchange format. Click **Next**.



10. Provide the password to protect the .pfx data. Click **Next**.
11. Provide the path and file name where the .pfx data is to be stored. For example, **c:\mykey**. Click **Next**.

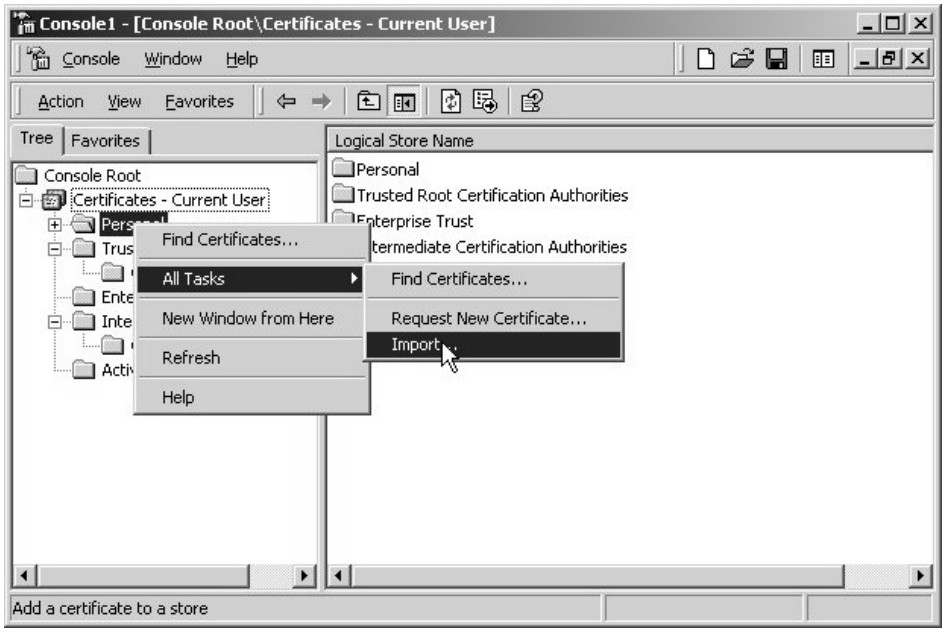
12. A list of certificates and keys to be exported is displayed. Click **Finish** to confirm.
13. Click **OK** to close the wizard, and close the snap-in.

This exports the encryption certificate and private key to a .pfx file that must be backed up securely.

To restore the encryption certificate and private key on a different system do the following:

1. Copy the .pfx file to a floppy disk, and take it to the computer where the encryption certificate and private key will be imported to.
2. Start the **Certificates** snap-in by clicking **Start**, clicking **Run**, and then typing **mmc**.
3. On the **Console** menu, click **Add/Remove snap-ins**, and click **Add**.
4. Click **Certificates**, and click **Add**. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.

5. Right-click **Personal store**, click **All Tasks**, and click **Import** to import the .pfx file.



6. This starts the **Certificate Manager Import** wizard. Follow the wizard steps to successfully import the certificate and private key.

7. Provide the path to the .pfx file.
8. Type the password to unwrap the .pfx data.
9. Click **Place all certificates in the following store**, and accept the Personal certificate store. Click **Next**.

10. Click **Finish**, and then click **OK** to start the import operation. When the import is complete, click **OK** to close the wizard.

Once the same keys are available, encrypted files that may have been backed up on different computer can be transparently used.

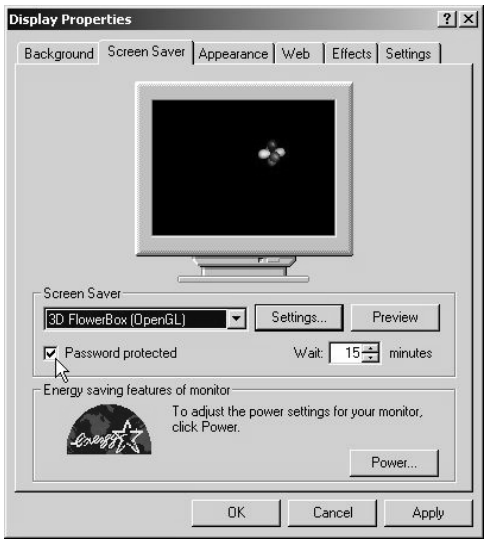
Enable Automatic Screen Lock Protection

Enable a password-protected screensaver for the Evaluated Configuration. Doing so will enable a user desktop to be locked for security reasons by setting an automatic screen lock that is initiated with the screensaver after a set period of inactivity. Once the computer screen lock is invoked, access to the computer will only be allowed to the user whose account is currently logged on to the computer or by an authorized administrator.

Set an automatic screen lock by setting screensaver based screen lock as follows:

1. Right click on the user desktop and select **Properties**. The **Display Properties** window will appear.
2. Click on the **Screen Saver** tab.
3. Select a screen saver from the **Screen Saver** drop down menu.
4. Enter the number of minutes of inactivity that the system must wait before initiating the screen saver in the **Wait**: dialog box (the default of 15 minutes is recommended).

5. Select the **Password Protected** box.



6. Click **OK** to set the password protected screen saver.

Update the system Emergency Repair Disk

Update the system's ERD to reflect all the changes made. For instructions, see "Recommended Actions Prior to Installing Service Pack and Hotfix Updates."

Application Installation Procedures on a Secure Configuration

Installation of applications conforming to Windows Installer-based package requirements will have difficulty installing from a CD-ROM on a computer running a Windows 2000 operating system in the Evaluated Configuration. The reason is that the Windows Installer service is not a service that was evaluated and is therefore disabled in the Evaluated Configuration of Windows 2000. Additionally, the AllocateCDRoms Registry value that is set in the Evaluated Configuration will not allow Windows Installer to open a .Cap file directly from a CD-ROM. Therefore, to install an application conforming to Windows Installer-based package requirements, the Windows Installer service must be temporarily enabled and the "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms" Registry value must be temporarily set to 0 (this can be accomplished through the Local Security Policy interface).

> **Note**: To un-install applications conforming to Windows Installer-based package requirements, the Windows Installer service must be again temporarily enabled. After un-installing the application, the Windows Installer service should then be disabled to return to the evaluated configuration. To un-install an application, the "AllocateCDRoms" Registry value need not be modified; it should remain enabled, as set in the evaluated configuration.

The procedures are as follows:

1. Start the Windows Installer service:
   a. Log on to the computer with administrative rights.

b. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**. This opens the local system **Services** interface.

c. In the right-hand pane, right-click on **Windows Installer** and select **Properties**. The **Windows Installer Properties** interface will appear.

d. In the **General** tab view, change the **Startup type** from **Disabled** to **Manual** by using the drop down menu.

e. Click the **Apply** button. The **Start** button under **Service status** will become active.

f. Click the **Start** button to start the **Windows Installer** service.

g. Click the **OK** button to close the **Windows Installer Properties** interface.

h. Close the **Services** interface.

2. Change the Restrict CD-ROM access to locally logged-on user only setting in the Local Security Policy's Security Options:

   a. Logged on as an administrator, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the local system **Local Security Policy** interface.

   b. Expand Security Settings.

   c. Within Security Settings, expand **Local Policies** to reveal the Audit, User Rights Assignment, and Security Options policies.

   d. Click on the **Security Options** object. The right-hand details pane will reveal the configurable security options.

   e. Double click on **Restrict CD-ROM access to locally logged-on user** only in the right-hand details pane.

   f. Select the **Disabled** radio button and click the OK button.

   g. Close the **Local Security Policy** interface and reboot the computer.

3. Install the software application from CD-ROM:

   a. Once the computer reboots, log on with administrative rights.

   b. Insert the application installation CD-ROM in the CD-ROM drive and follow the installation procedures.

After completing the application installation, it will be necessary to reset the Evaluated Configuration settings on the computer by disabling the **Windows Installer** service and resetting the **Restrict CD-ROM access to locally logged-on user only** policy setting to **Enabled**.

1. Reset the Evaluated Configuration settings as follows:

   a. Follow the procedures in **Step 1** above to open the **Service** interface and access the **Windows Installer** service.

   b. Change the **Startup type** from **Manual** to **Disabled** by using the drop down menu.

   c. Click the **Stop** button to stop the **Windows Installer** service.

d. Click the **OK** button to close the **Windows Installer Properties** interface.

e. Close the **Services** interface.

f. Next, open the **Security Options** policy in the **Local Security Policy** by following the procedures in **Step 2** above.

g. Double click on **Restrict CD-ROM access to locally logged-on user only** in the right-hand details pane.

h. Select the **Enabled** radio button and click the **OK** button.

i. Close the **Local Security Policy** interface and reboot the computer.

5. Windows 2000 Common Criteria Security Configuration Templates

For convenience, this document includes a set of Windows 2000 Common Criteria security configuration templates. The templates may be used to automate the application of required and recommended Common Criteria security settings defined in this document. However, it is highly recommended that all settings be carefully reviewed prior to applying a security configuration template, since an organization's local security policies may require adjustments to the recommended values or security settings defined in the templates.

The templates supporting this document are listed in the table below and are included in Appendix F of this document. The baseline security configuration templates are used to apply all of the Common Criteria required security settings. The high-security templates are used to apply all of the Common Criteria required security settings, and provide stronger security by also applying the recommended security settings.

Template Name	Operating System Type/Configuration	Template Description
CC_Baseline_W2K_Server.inf	Windows 2000 Server	Required Common Criteria Evaluated Configuration security settings for Windows 2000 Server configured as standalone or member server.
CC_Baseline_W2K_Professional.inf	Windows 2000 Professional	Required Common Criteria Evaluated Configuration security settings for Windows 2000 Professional configured as standalone or Domain member.
CC_Baseline_W2K_Domain.inf	Windows 2000 Domain Controller	Required Common Criteria Evaluated Configuration security settings for Windows 2000 Domain members.
CC_Baseline_W2K_DC.inf	Windows 2000 Domain Controller	Required Common Criteria Evaluated Configuration security settings for Windows 2000 Domain Controllers. Used with a Domain template, or a Server template if a Domain policy is not used.
CC_HiSec_W2K_Server.inf	Windows 2000 Server	Required and recommended Common Criteria Evaluated Configuration security settings for Windows 2000 Server configured as standalone or member server.
CC_HiSec_W2K_Professional.inf	Windows 2000 Professional	Required and recommended Common Criteria Evaluated Configuration security settings for Windows 2000 Professional configured as standalone or Domain member.
CC_HiSec_W2K_Domain.inf	Windows 2000 Domain Controller	Required and recommended Common Criteria Evaluated Configuration security settings for Windows 2000 Domain members.

Template Name	Operating System Type/Configuration	Template Description
CC_HiSec_W2K_DC.inf	Windows 2000 Domain Controller	Required and recommended Common Criteria Evaluated Configuration security settings for Windows 2000 Domain Controllers. Used with a Domain template, or a Server template if a Domain policy is not used.

Template Modifications and Manual Settings

The settings below are either not included, in the Windows 2000 Common Criteria security configuration templates, or are commented out. These settings must either be manually set through a Security Policy interface or may be uncommented in the templates and edited as appropriate. The **Security Templates snap-in** tool may also be used as describe in the "Viewing and editing a security configuration template" subsection below.

Under the Security Options policies, the following recommended settings should be reviewed and edited as applicable:

- **Audit the access of global system objects** is commented out in the templates. It generates a large amount of audit events and should be implemented when strict audit management practices are in place. See the "Modify Security Options" subsection for details.
- **Audit the use of Backup and Restore privilege** is commented out in the templates. It generates a large amount of audit events and should be implemented when strict audit management practices are in place. See the "Modify Security Options" subsection for details.
- **Rename Administrator account** is commented out in the templates. The policy implementer must select a unique name. See the "Modify Security Options" subsection for details.
- **Rename Guest account** is commented out in the templates. The policy implementer must select a unique name. See the "Modify Security Options" subsection for details.
- **Shut down the system immediately if unable to log security audits** is commented out in the templates. This setting can create a management burden if applied across all computers in a Domain and should only be applied on critical system when strict audit management practices are in place. See the "Modify Security Options" subsection for details.
- **Message title for users attempting to log on**. The text in the templates is a placeholder that must be edited to conform to an organization's local requirements. See the "Modify Security Options" subsection for details.
- **Message text for users attempting to log on**. The text in the templates is a placeholder that must be edited to conform to an organization's local requirements. See the "Modify Security Options" subsection for details.

The following required Registry setting must be applied:

- **Prevent interference of the session lock from application generated input**, see the "Service Pack 3 Registry entries" subsection for details. The security templates cannot create the path necessary to apply this setting. It must therefore be applied manually by

using the **Regedt32.exe** Registry editor. Procedures for using **Regedt32.exe** are available in the Windows 2000 Evaluated Configuration Administrator's Guide.

The following required User and group account modifications must be applied:

- **TsInternetUser**. Disable the TsInternetUser account on Windows 2000 Servers and Domain Controllers. A security template cannot disable the account. See the "Default User Accounts" subsection for details.
- **Domain Users**. Remove the Guest account from the Domain Users group. The security templates allow setting restricted groups with a defined set of members that are allowed, however, the Domain Users group needs to allow all new users to automatically become members. See the "Default Group Accounts" subsection for details.

Additional configuration procedures:

- **Enable automatic screen lock protection**. The procedures are available in the "Enable Automatic Screen Lock Protection" subsection of this document.
- **Update the Emergency Repair Disk**. The procedures are available in the "Recommended Actions Prior to Installing Service Pack and Hotfix Updates" subsection of this document.
- **Back up the Administrator's encryption certificates**. The recommended procedures are available in the "Encrypting File System" subsection of this document.

Security Configuration Template Application Tools

Authorized administrators can use the following tools to edit and apply the Common Criteria security configuration templates.

- **Security Templates snap-in**. The Security Templates snap-in is a stand-alone Microsoft Management Console (MMC) snap-in that allows the creation of a text-based template file that contains security settings for all security areas.
- **Security Configuration and Analysis snap-in**. The Security Configuration and Analysis snap-in is a stand-alone MMC snap-in that can configure or analyze Windows 2000 operating system security. Its operation is based on the contents of a security template that was created using the Security Templates snap-in. This is the preferred tool for applying a template to a standalone computer or domain member.

At the Domain level, the Domain Security Policy and Domain Controller Security Policy templates must be applied using the Domain Controller's **Local Security Policy**, **Domain Security Policy** and **Domain Controller Security Policy** GUIs described in the "Windows 2000 Security Policies" subsection of this document.

Managing and Applying Security Configuration Security Templates

This subsection provides procedures for editing and applying the Common Criteria security configuration templates. The templates are available in Appendix F of this document.

Viewing and editing a security configuration template

The Common Criteria security configuration templates may be edited by opening them in a text editor, such as **Notepad.exe**, or by opening them in the **Security Templates snap-in** tool.

Notepad.exe is recommended if modification are to be made to recommended registry settings that are not visible via the Security Templates snap-in tool, such as those defined in the "Additional Security Settings" subsection of this document. Use the following procedures to edit a template using the Security Templates snap-in tool:

1. First copy the desired template into the "\%Systemroot%\Security\Templates" (or "C:\WINNT\Security\Templates") folder of the system partition.
2. Next, click **Start**, click **Run**, type mmc, and then click **OK**.
3. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
4. Select **Security Templates**, click **Add**, click **Close**, and then click **OK**.
5. To save the snap-in setting click **Save** on the **Console** menu. Type a name for this console, and then click **Save**.
6. In the Security Templates snap-in, double-click **Security Templates**.
7. Double-click the default path folder (%Systemroot%\Security\Templates), and then double-click the Common Criteria security configuration template that is to be modified to display the security policies (such as **Account Policies**).
8. Double-click the security policy that to be modified.
9. Click the security area that is to be customized (such as **Password Policy**), and then double-click the security attribute to modify (such as **Minimum Password Length**).
10. Modification procedures are the same as those described in the "Secure Configuration" section of this document.
11. Once modifications are completed, right-click the name of the Common Criteria security configuration template that was modified and select **Save**.

Applying a Common Criteria security template to a local computer

Use the following procedures to apply the Common Criteria templates locally on a computer running Windows 2000 Server or Professional. If computers that are Domain members are to inherit all the security settings from the Domain, these procedures are not needed on the local computer.

1. Log on to the computer with administrative rights.
2. Copy the desired template into the "\%Systemroot%\Security\Templates" (or "C:\WINNT\Security\Templates") folder of the system partition.
3. Next, click **Start**, click **Run**, type mmc, and then click **OK**.
4. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
5. Select **Security Configuration and Analysis**, click **Add**, click **Close**, and then click **OK**.
6. To save the snap-in setting click **Save** on the **Console** menu.
7. In the **Security Configuration and Analysis** snap-in, right-click **Security Configuration and Analysis**.
    - If a working database is not already set, click **Open Database** to set a working database. Type a name for the new database, with a ".sdb" extension, and click **Open**. Find and select the Common Criteria security configuration template so that it appears in the **File name:** text box. Check the **Clear this database** check box and click the **Open** button.

- If a working database is already set, click **Import Template**. Find and select the Common Criteria security configuration template so that it appears in the **File name:** text box. Check the **Clear this database** check box and click the **Open** button.

8. Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**. A window will appear showing the path to the error log file, click **OK**. Note that the security settings are set immediately. Some settings, though applied, will not become effective until the computer is rebooted.
9. Close the **Security Configuration and Analysis** tool and reboot the computer.

Importing a Common Criteria security template to a Domain level Security Policy

If a Domain policy is not to be used (for example, if clients are to have all settings applied locally), then a Common Criteria Server template should be applied locally on the Domain Controller followed by the Common Criteria Domain Controller template. Otherwise, the procedure on a Domain controller is:

1. Import the Domain security configuration template to the Domain Security Policy console.
2. Import the Domain Controller security configuration template to the Domain Controller Security Policy console.
3. Reboot the Domain Controller.

Import a Common Criteria Domain security configuration template

Use the following procedures to import a Common Criteria template for Domains:

1. Log on to the Domain Controller with administrative rights.
2. Copy the desired template into the "\%Systemroot%\Security\Templates" (or "C:\WINNT\Security\Templates") folder of the system partition.
3. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Security Policy**. This opens the Domain Security Policy console.
4. In the console tree, right-click **Security Settings**.
5. Click **Import Policy**.
6. Find and select the Common Criteria security configuration template so that it appears in the **File name:** text box. Check the **Clear this database** check box and click the **Open** button.
7. Close the **Domain Security Policy**.
8. Follow the procedures below to import a Common Criteria template for Domain Controllers.

Import a Common Criteria Domain Controller security configuration template

Use the following procedures to import a Common Criteria template for Domain Controllers:

1. Log on to the Domain Controller with administrative rights.
2. Copy the desired template into the "\%Systemroot%\Security\Templates" (or "C:\WINNT\Security\Templates") folder of the system partition.

3. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Controller Security Policy**. This opens the Domain Controller Security Policy console.
4. In the console tree, right-click **Security Settings**.
5. Click **Import Policy**.
6. Find and select the Common Criteria security configuration template so that it appears in the **File name:** text box. Check the **Clear this database** check box and click the **Open** button.
7. Reboot the Domain Controller.

6. References

- Microsoft Windows 2000 Server Documentation |http://www.microsoft.com/windows2000/en/server/help/
- Microsoft Windows 2000 Professional Documentation|http://www.microsoft.com/windows2000/en/professional/help/
- Microsoft White Paper - Windows 2000 Server Security Configuration Tool Set |http://www.microsoft.com/WINDOWS2000/techinfo/howitworks/security/sctoolset.asp
- Microsoft Windows 2000 Service Pack Installation and Deployment Guide
- MCSE Training Kit: Designing Microsoft Windows 2000 Network Security, Microsoft Press
- MCSE Training Kit: Microsoft Windows 2000 Server, Microsoft Press
- Microsoft Windows 2000 Security Technical Reference, Microsoft Press
- Default Windows 2000 Permissions |http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/ProRK/prdd_sec_njrp.htm
- Microsoft White Paper, Securing Windows NT Server
- Microsoft Windows NT, Ver. 4.0 – C2 Administrator's and User's Security Guide Revision 1.1, Microsoft Corporation
- Microsoft Resource Kit: Windows 2000 Server Distributed Systems Guide, Microsoft Press
- Microsoft Windows 2000 Server Resource Kit: Supplement 1 – Server Resource Kit Books |http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/
- Readme for Service Pack 3 |http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/ReadMeSP.htm
- Windows 2000 Group Policy White Paper, Microsoft TechNet
- Limited OEM Driver Support with F6 During Windows Setup (Q225125) |http://support.microsoft.com/default.aspx?scid=kb;en-us;Q225125
- Microsoft Prescriptive Guidance: Security Operations Guide for Windows 2000 Server
- Microsoft Windows 2000 Server Security Configuration Tool Set white paper |http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/securcon.asp
- Microsoft TechNet: Step-by-Step Guide to Using the Security Configuration Tool Set |http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/walkthru/seconfig.asp

Appendix A
Windows 2000 Default Security Policy Settings

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Account Policies			
Password Policy			
Enforce password history	0 passwords remembered	Not defined	1 passwords remembered
Maximum password age	42 days	Not defined	42 days
Minimum password age	0 days	Not defined	0 days
Minimum password length	0 characters	Not defined	0 characters
Passwords must meet complexity requirements	Disabled	Not defined	Disabled
Store passwords using reversible encryption for all users in the domain	Disabled	Not defined	Disabled
Account Lockout Policy			
Account lockout duration	Not defined	Not defined	Not defined
Account lockout threshold	0 invalid login attempts	Not defined	0 invalid login attempts
Reset account lockout counter after	Not defined	Not defined	Not defined
Kerberos Policy	**(POLICY NOT AVAILABLE)**		
Enforce user logon restrictions	(Not available) (Local default is Enabled)	Not defined	Enabled
Maximum lifetime for service ticket	(Not available) (Local default is 60 minutes)	Not defined	600 minutes
Maximum lifetime for user ticket	(Not available) (Local default is 7 hours)	Not defined	10 hours
Maximum lifetime for user ticket renewal	(Not available) (Local default is 10 days)	Not defined	7 days
Maximum tolerance for computer clock synchronization	(Not available) (Local default is 60 minutes)	Not defined	5 minutes
Local Policies			
Audit Policy			
Audit account logon events	No auditing	No auditing	Not defined
Audit account management	No auditing	No auditing	Not defined

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Audit directory service access	No auditing	No auditing	Not defined
Audit logon events	No auditing	No auditing	Not defined
Audit object access	No auditing	No auditing	Not defined
Audit policy changes	No auditing	No auditing	Not defined
Audit privilege use	No auditing	No auditing	Not defined
Audit process tracking	No auditing	No auditing	Not defined
Audit system events	No auditing	No auditing	Not defined
User Rights Assignment			
Access this computer from the network	Administrators Backup Operators Power Users Users Everyone	Administrators Authenticated Users Everyone IUSR_W2K-*machinename* IWAM_W2K-*machinename*	Not defined
Act as part of the operating system	(Blank)	(Blank)	Not defined
Add workstations to domain	(Blank)	Authenticated Users	Not defined
Back up files and directories	Administrators Backup Operators	Administrators Backup Operators Server Operators	Not defined
Bypass traverse checking	Administrators Backup Operators Power Users Users Everyone	Administrators Authenticated Users Everyone	Not defined
Change the system time	Administrators Power Users	Administrators Server Operators	Not defined
Create a pagefile	Administrators	Administrators	Not defined
Create a token object	(Blank)	(Blank)	Not defined
Create permanent shared objects	(Blank)	(Blank)	Not defined
Debug programs	Administrators	Administrators	Not defined

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Deny access to this computer from the network	(Blank)	(Blank)	Not defined
Deny logon as a batch job	(Blank)	(Blank)	Not defined
Deny logon as a service	(Blank)	(Blank)	Not defined
Deny logon locally	(Blank)	(Blank)	Not defined
Enable computer and user accounts to be trusted for delegation	(Blank)	Administrators	Not defined
Force shutdown from a remote system	Administrators	Administrators Server Operators	Not defined
Generate security audits	(Blank)	(Blank)	Not defined
Increase quotas	Administrators	Administrators	Not defined
Increase security scheduling priority	Administrators	Administrators	Not defined
Load and unload device drivers	Administrators	Administrators	Not defined
Lock pages in memory	(Blank)	(Blank)	Not defined
Logon as a batch job	(Blank)	IUSR_W2K-*machinename* IWAM_W2K-*machinename*	Not defined
Logon as a service	(Blank)	(Blank)	Not defined
Log on locally	Administrators Backup Operators Power Users Users *Machinename*/Guest *Machinename*/TsInternetUser (Server/Adv. Server only)	Administrators Authenticated Users Backup Operators IUSR_W2K-*machinename* Print Operators Server Operators TsInternetUser	Not defined
Manage auditing and security log	Administrators	Administrators	Not defined
Modify firmware environment values	Administrators	Administrators	Not defined
Profile single process	Administrators Backup Operators	Administrators	Not defined
Profile system performance	Administrators	Administrators	Not defined

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Remove computer from docking station	Administrators Backup Operators Users	Administrators	Not defined
Replace process level token	(Blank)	(Blank)	Not defined
Restore files and directories	Administrators Backup Operators	Administrators Backup Operators Server Operators	Not defined
Shut down the computer	Administrators Backup Operators Power Users Users (Professional only)	Account Operators Administrators Backup Operators Print Operators Server Operators	Not defined
Synchronize directory service data	(Blank)	(Blank)	Not defined
Take ownership of files and other objects	Administrators	Administrators	Not defined
Security Options			
Additional restrictions for anonymous connections	None. Rely on default permissions.	Not defined	Not defined
Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined	Not defined
Allow system to be shut down without having to log on	Enabled (Professional Only) Disabled (Server/Adv. Server only)	Not defined	Not defined
Allowed to eject removable NTFS media	Administrators	Not defined	Not defined
Amount of idle time required before disconnecting session	15 minutes	Not defined	Not defined
Audit the access of global system objects	Disabled	Not defined	Not defined
Audit use of Backup and Restore privilege	Disabled	Not defined	Not defined
Automatically log off users when logon time expires	(Option not available on standalone Professional, Server, or Advanced Server)	Not defined	Disabled
Automatically log off users when logon time expires (local)	Enabled	Not defined	Not defined
Clear virtual memory pagefile when system shuts down	Disabled	Not defined	Not defined
Digitally sign client communications (always)	Disabled	Not defined	Not defined

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Digitally sign client communications (when possible)	Enabled	Not defined	Not defined
Digitally sign server communications (always)	Disabled	Not defined	Not defined
Digitally sign server communications (when possible)	Disabled	Enabled	Not defined
Disable CTRL+ALT+DEL requirement for logon	Not Defined (Professional only) Disabled (Server/Adv. Server only)	Not defined	Not defined
Do not display user name in the logon screen	Disabled	Not defined	Not defined
LAN Manager Authentication Level	Send LM & NTLM response	Not defined	Not defined
Message text for users attempting to log on	(Blank)	Not defined	Not defined
Message title for users attempting to log on	(Blank)	Not defined	Not defined
Number of previous logons to cache (in case domain controller is not available	10 logons	Not defined	Not defined
Prevent system maintenance of computer account passwords	Disabled	Not defined	Not defined
Prevent users from installing print drivers	Disabled (Professional only) Enabled (Server/Adv. Server only)	Not defined	Not defined
Prompt user to change password before expiration	14 days	Not defined	Not defined
Recovery Console: Allow automatic administrative logon	Disabled	Not defined	Not defined
Recovery Console: Allow floppy copy and access to all drives and folders	Disabled	Not defined	Not defined
Rename administrator account	Not defined	Not defined	Not defined
Rename guest account	Not defined	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only	Disabled	Not defined	Not defined
Restrict floppy access to locally logged-on user only	Disabled	Not defined	Not defined
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Not defined	Not defined
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Not defined	Not defined
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Not defined	Not defined

Windows 20000 Default Security Policy Settings			
Security Settings	**Local security Policy (Professional and Server/Adv. Server)**	**Domain Controller Security Policy**	**Domain Security Policy**
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Not defined	Not defined
Secure system partition (for RISC platforms only)	(Option not available on standalone Professional, Server, or Advanced Server)	Not defined	Not defined
Send unencrypted password to connect to third-party SMB servers	Disabled	Not defined	Not defined
Shut down system immediately if unable to log security audits	Disabled	Not defined	Not defined
Smart card removal behavior	No action	Not defined	Not defined
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Not defined	Not defined
Unsigned driver installation behavior	Not defined	Not defined	Not defined
Unsigned non-driver installation behavior	Not defined	Not defined	Not defined
Event Log			
Settings for Event Logs	**Set in Event Viewer log properties**		
Maximum application log size	512 Kb	Not defined	Not defined
Maximum security log size	512 Kb	Not defined	Not defined
Maximum system log size	512 Kb	Not defined	Not defined
Restrict guest access to application log	(Not available)	Not defined	Not defined
Restrict guest access to security log	(Not available)	Not defined	Not defined
Restrict guest access to system log	(Not available)	Not defined	Not defined
Retain application log	Overwrite events older than 7 days	Not defined	Not defined
Retain security log	Overwrite events older than 7 days	Not defined	Not defined
Retain system log	Overwrite events older than 7 days	Not defined	Not defined
Retention method for application log	Overwrite events older than 7 days	Not defined	Not defined
Retention method for security log	Overwrite events older than 7 days	Not defined	Not defined
Retention method for system log	Overwrite events older than 7 days	Not defined	Not defined
Shut down the computer when the security audit log is full	(Not available)	Not defined	Not defined

Appendix B– Audit Categories and Events

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
FAU_GEN.1	Start-up and Shutdown of the audit functions	**Category: Policy change** 612 – Audit policy change. (The event is generated whenever audit is enabled or disabled for any of the audit categories. A list of audit changes is displayed in the event log.)	✓	
FAU_GEN.2	None			
FAU_SAR.1	Reading of information from the audit records	**Category: Privilege use** 578 – Privileged object operation. (Accessing the Security Event Log. Success should result for SeSecurityPrivilege.)	✓	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	**Category: Privilege use** 578 – Privileged object operation. (Failure should result for SeSecurityPrivilege.)		✓
FAU_SAR.3	None			
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	**Category: Policy change** 612 – Audit policy change. (A list of audit changes is displayed in the event log.)	✓	
FAU_STG.1	None			
FAU_STG.3	Actions taken due to exceeding of a threshold	**Category: System** 516 – Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. 517 – The audit log was cleared. (Review action taken by an authorized administrator to clear the event logs in response to the system exceeding a predefined audit threshold.) 523 – The audit log is “x” percent full	✓	

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
		Note: the above event is generated only with SP3 (key value must set to the percentage the administrator wants the audit record to be cut upon. (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel)		
FAU_STG.4	Actions taken due to the audit storage failure	517 – The audit log was cleared. (Review action taken by an authorized administrator to clear the event logs in response to the system exceeding a predefined audit threshold.)		
FDP_ACC.1(a)	None			
FDP_ACF.1(a)	All requests to perform an operation on an object covered by the SFP	**Category: Object access** 563 – Object open for delete. 564 – Object deleted. 565 – Object open. 566 – Object operation. **Category: Process tracking** 594 – A handle to an object has been duplicated. 595 – Indirect access to an object has been obtained.	✓	✓
FDP_RIP.2	None			
FDP_RIP.2. Note 1	None			
FIA_ATD.1	None			
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	**Category: Logon** 528 – Successful logon. 529 – Logon failure: Unknown user name or bad password. 535 – Logon failure: The specified account's password has expired. 540 – Successful network logon. 545 – IPSec peer authentication failed.	✓	✓

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
		Category: Account logon 680 – Account used for logon. 681 – The logon account: <client name> by: <source> from workstation <workstation> failed. The error code was <error>.	✓	✓
FIA_UAU.7	None			
FIA_USB.1	Success and failure of binding user security attributes to a subject (e.g., success and failure to create a subject)	**Category: Process tracking** 592 – A new process has been created.	✓	✓
FMT_MSA.1(a)	All modifications of the values of object security attributes	**Category: Object access** 560 – Object open. (Under Description: → Accesses, there should be the following entries; AppendData, ReadAttributes and WriteAttributes.)	✓	
FMT_MSA.3(a)	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.	**Category: Object access** 560 – Object open.	✓	
FMT_MTD.1(a) CAPP – 5.4.3	All modifications to the values of TSF data (audit log creation, deletion, and clearing)	**Category: System** 517 – The audit log was cleared. **Category: Object access** (Theses events can log direct deletion of the security log files when audit is set on the security log files.) 563 – Object open for delete. 564 – Object deleted. **Category: Privilege use** 578 – Privileged object operation. (Shown as use of SeSecurityPrivilege, with actual changes noted in event 612)	✓ ✓ ✓	

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
		Category: Policy change 612 – Audit policy change.	✓	
FMT_MTD.1(b) CAPP – 5.4.4	All modifications to the values of TSF data (audit log modification - including the new value of the TSF data)	**Category: Policy change** 612 – Audit policy change.		
FMT_MTD.1(c) CAPP – 5.4.5	All modifications to the values of TSF data (user security attributes - including the new value of the TSF data)	**Category: Policy change** 608 – User right assigned. 609 – User right removed. **Category: Account management** 624 – User account created. 625 – User account type changed. 626 – User account enabled. 629 – User account disabled. 630 – User account deleted. 631 – Security enabled Global Group created. 632 – Security enabled Global Group member added. 633 – Security enabled Global Group member removed. 634 – Security enabled Global Group deleted. 635 – Security enabled Local Group created. 636 – Security enabled Local Group member added. 637 – Security enabled Local Group member removed. 638 – Security enabled Local Group deleted. 639 – Security enabled Local Group changed. 641 – Security enabled Global Group changed. 642 – User account changed.	✓ ✓	

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
		644 – User account locked. 648 – Security disabled Local Group created. 649 – Security disabled Local Group changed. 650 – Security disabled Local Group member added. 651 – Security disabled Local Group member removed. 652 – Security disabled Local Group deleted. 653 – Security disabled Global Group created. 654 – Security disabled Global Group changed. 655 – Security disabled Global Group member added. 656 – Security disabled Global Group member removed. 657 – Security disabled Global Group deleted. 658 – Security enabled Universal Group created. 659 – Security enabled Universal Group changed. 660 – Security enabled Universal Group member added. 661 – Security enabled Universal Group member removed. 662 – Security enabled Universal Group deleted. 663 – Security disabled Universal Group created. 664 – Security disabled Universal Group changed. 665 – Security disabled Universal Group member added. 666 – Security disabled Universal Group member removed. 667 – Security disabled Universal Group deleted. 668 – Group type changed.		
FMT_MTD.1(d) CAPP- 5.4.6	All modifications to the values of TSF data (authentication data)	**Category: Account management** 627 – Change password attempt. 628 – User account password set.	✓	✓

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
FMT_REV.1(a) CAPP – 5.4.7	All attempts to revoke security attributes (user attributes)	**Category: Policy change** 609 – User right removed. **Category: Account management** 629 – User account disabled. 644 – User account locked.	✓ ✓	
FMT_REV.1(b) CAPP – 5.4.8	All modifications to the values of TSF data (object attributes)	(See FMT_MSA.1a)		
FMT_SMR.1	Modifications to the group of users that are part of a role Every use of the rights of a role. (Additional/ Detailed)	**Category: Privilege use** 578 – Privileged object operation. **Category: Account management** 632 – Security enabled Global Group member added. 633 – Security enabled Global Group member removed. 634 – Security enabled Global Group deleted. 636 – Security enabled Local Group member added. 637 – Security enabled Local Group member removed. 638 – Security enabled Local Group deleted. 639 – Security enabled Local Group changed. 640 – General account database change. 641 – Security enabled Global Group changed. 648 – Security disabled Local Group created. 649 – Security disabled Local Group changed. 650 – Security disabled Local Group member added. 652 – Security disabled Local Group deleted. 654 – Security disabled Global Group changed. 655 – Security disabled Global Group member added.	✓ ✓	✓

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
		656 – Security disabled Global Group member removed. 657 – Security disabled Global Group deleted. 659 – Security enabled Universal Group changed. 660 – Security enabled Universal Group member added. 661 – Security enabled Universal Group member removed. 662 – Security enabled Universal Group deleted. 664 – Security disabled Universal Group changed. 665 – Security disabled Universal Group member added. 666 – Security disabled Universal Group member removed. 668 – Group type changed.		
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the test.	Not Applicable		
FPT_RVM.1	None			
FPT_SEP.1	None			
FPT_STM.1	Changes to the time	**Category: Privilege use** 577 – Privileged service called. (Shown as use of SeSystemTimePrivilege.)	✓	✓
FIA_AFL.1	Logon Failure (Disabling of account due to meeting a predefined threshold)	**Category: Logon** 529 – Logon failure: Unknown user name or bad password. (leading to the lockout) **Category: Account management** 642 – User account changed – account locked 644 – User account locked.	✓	✓

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
FIA_UAU.2	The use of the authentication mechanism	**Category: Logon** 528 – Successful logon. 529 – Logon failure: Unknown user name or bad password. 540 – Successful network logon. **Category: Account logon** 680 – Account used for logon. 681 – The logon account: <client name> by: <source> from workstation <workstation> failed. The error code was <error>.	✓	✓
FIA_UID.2	All use of the user identification mechanism, including the identity provided during successful attempts	**Category: Logon** 528 – Successful logon. 529 – Logon failure: Unknown user name or bad password. 535 – Logon failure: The specified account's password has expired. 540 – Successful network logon. 545 – IPSec peer authentication failed. **Category: Account logon** 625 – Pre-authentication failed. 681 – The logon account: <client name> by: <source> from workstation <workstation> failed. The error code was <error>.	✓	✓
FMT_MOF.1(a)	Audit Policy Changes	**Category: Privilege use** 578 – Privileged object operation. (Shown as use of SeSecurityPrivilege.) **Category: Policy change** 612 – Audit policy change.	✓ ✓	✓
FMT_MTD.1(g)	Attempt to use an authorized administrator privilege to change the TSF Time	**Category: Privilege use** 577 – Privileged service called. (Shown as use of SeSystemTimePrivilege.)	✓	

Security Target Compliance Matrix for Audit				
Component	**Event**	**Audit Event**	**Required Setting**	
			S	**F**
TRANSFER_PROT_EX	IPSEC related events	**Category: Logon** 541 – IPSec security association established. 542 – IPSec security association ended. Mode: Data Protection (Quick mode). 543 – IPSec security association ended. Mode: Key Exchange (Main mode). 544 – IPSec security association establishment failed because peer could not authenticate. 545 – IPSec peer authentication failed. 546 – IPSec security association establishment failed because peer sent invalid proposal. 547 – IPSec security association negotiation failed. **Category: Policy change** 613 – IPSec policy agent started. 614 – IPSec policy changed. 615 – IPSec policy agent encountered a potentially serious failure. 616 – IPSec policy agent encountered a potentially serious failure.	✓ ✓	✓ ✓
FTA_SSL1	Attempt to unlock	**Category: Logon** 528 – Logon successful (entry 7 is unlock) 529 – Logon failure (entry 7 is unlock)	✓	✓
FTA_SSL.2	Attempt to unlock	**Category: Logon** 528 – Logon successful (entry 7 is unlock) 529 – Logon failure (entry 7 is unlock)	✓	✓
FTA_TSE.1	Logon Failure	**Category: Logon** 535 – Logon failure: The specified account's password has expired.		✓

Appendix C– User Rights and Privileges

The table below identifies the default user rights assignments on Windows 2000 systems, defines their applicability to the Windows 2000 Security Target, and provides change requirements and recommendations necessary to comply with Security Target objectives.

The table identifies the default user rights assigned to users on stand-alone Windows 2000 Professional and Server systems and on a Windows 2000 Domain Controller. It also identifies the default user rights in a Domain Security Policy (all "not-defined" by default). Assignments in the Domain Security Policy will override Local Security Policy settings for domain members. The "Required" changes noted in the table are necessary to meet compliance with ST requirements.

User right/privilege assignments can be found in the Local and Domain Security Policy GUI, as follows:

- **Windows 2000 Professional:**

  Administrative Tools → Local Security Policy → Security Settings\Local Policies\User Rights Assignment

- **Windows 2000 Server:**

  Administrative Tools → Local Security Policy → Security Settings\Local Policies\User Rights Assignment

- **Windows 2000 Domain Controller:**

  Administrative Tools → Domain Controller Security Policy → Windows Settings\Security Settings\Local Policies\User Rights Assignment

  Administrative Tools → Domain Security Policy → Windows Settings\Security Settings\Local Policies\User Rights Assignment

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Logon Rights						
Access this Computer from the Network (SeNetworkLogonRight)	Determines which users are allowed to connect over the network to the computer.	**Default:** Administrators Backup Operators Power Users Users Everyone **Required Change:** Administrators Backup Operators Power Users Users Authen. Users	**Default:** Administrators Backup Operators Power Users Users Everyone **Required Change:** Administrators Backup Operators Power Users Users Authen. Users	**Default:** (Not Defined) **Required:** No Change	**Default:** Administrators Authen. Users Everyone **Required Change:** Administrators Authen. Users	Supports the following TOE Security Functional Requirement: FIA_UAU.2.1, Authentication and FIA_UID.2, User Identification before any action. Implements the following TOE Security functions: Para 6.1.3, Identification and Authentication for network logons. **Changes:** Do not allow Guest/anonymous logons. Remove/replace accounts with a potential to allow unauthenticated/anonymous access (if Guest were somehow

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						enabled). Replace "Everyone" with "Authenticated User."
Log on as a batch job (SeBatchLogonRight)	Allows a user to log on by using a batch-queue facility.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Log on locally (SeInteractiveLogonRight)	Allows a user to log on locally at the computer's keyboard.	**Default:** Administrators Backup Operators Power Users Users *Machinename*\Guest **Required Change:** Administrators Backup Operators Power Users Users	**Default:** Administrators Backup Operators Power Users Users *Machinename*\Guest *Machinename\TsInternetUser* **Required Change:** Administrators Backup Operators Power Users Users	**Default:** (Not Defined) **Required:** No Change	**Default:** Administrators Account Operators Backup Operators Print Operators Server Operators TsInternetUser **Required Change:** Administrators Account Operators Backup Operators Print Operators	Supports the following TOE Security Functional Requirement: FIA_UAU.2.1, Authentication and FIA_UID.2, User Identification before any action. Implements the following TOE Security functions: Para 6.1.3, Identification and Authentication for local logons. **Changes:** Do not allow Guest/anonymous

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					Server Operators	logons. Remove Guest accounts since they allow unauthenticated/anonymous access. Remove TsInternetUser account – Terminal Services will not be implemented for the TOE.
Logon as a service (SeServiceLogonRight)	Allows a security principal to log on as a service. Services can be configured to run under the LocalSystem account, which has a built-in right to log on as a service. Any service that runs under a separate account must be assigned the right.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Deny Access to this computer from the network (SeDenyNetworkLogonRight)	Prohibits a user or group from connecting to the computer from the network.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Deny local logon (SeDenyInteractiveLogonRight)	Prohibits a user or group from logging on locally at the keyboard.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Deny logon as a batch file (SeDenyBatchLogonRight)	Prohibits a user or group from logging on through a batch-queue facility.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Deny logon as a service (SeDenyServiceLogonRight)	Prohibits a user or group from logging on as a service.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Privileges						
Act as part of the operating system (SeTcbPrivilege)	Allow a process to authenticate as a user and thus gain access to the same resources as a user. Only low-level authentication	**Default:** None **Required:** No Change	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** None **Required:** No Change	Default settings support the following TOE Security Functional Requirements: FPT_SEP.1.2, Domain Separation.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	services should require this service. The potential access is not limited to what is associated with the user by default, because the calling process may request that arbitrary additional accesses be put in the access token. Of even more concern is that the calling process can build an anonymous token that can provide any and all accesses. Additionally, the anonymous token does not					Misuse of this privilege can violate FAU_GEN.1, Audit Generation, FAU_GEN.2, User Identity Association, and FIA_USB.1, User Subject Binding. Implements the following TOE Security functions: Para 6.1.5.5, Domain Separation. Use of this privilege by accounts other than LocalSystem can violate the accountability security requirement due to the potential for generating anonymous tokens. **Changes:** Set the Domain Policy to None to enforce the default settings on the domain and ensure support of FPT_SEP.1.2,

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	provide a primary identity for tracking events in the audit log. The LocalSystem account uses this privilege by default.					FAU_GEN.1, FAU_GEN.2, and FIA_USB.1.
Add workstations to the domain (SeMachineAccountPrivilege)	Allows a user to add a computer to a specific domain. For the privilege to be effective, it must be assigned to the user as part of local security policy for domain controllers in the domain. A user who has this privilege can add up to 10 workstations to the domain. In Windows 2000, the behavior of this privilege is	**Default:** None **Required:** No Change	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** Authen. Users **Required Change:** Domain Admins	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.4.1, Security Management Functions, describing the domain management function that allows an "authorized administrator" to add and remove machines to and from a domain.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	duplicated by the Create Computer Objects permission for organizational units and the default Computers container in Active Directory. Users who have the Create Computer Objects permission can add an unlimited number of computers to the domain.					Para 6.1.4.1, Roles. Can be used to grant authorized users the privilege to add and remove machines from the domain. **Changes:** Set the default on Domain Controller Security Policy from Authenticated Users to Domain Admins to ensure trusted administration and configuration control of the domain infrastructure.
Backup files and directories (SeBackupPrivilege)	Allows the user to circumvent file and directory permissions to backup the system. The privilege is selected only when the application attempts to access through the NTFS backup	**Default:** Administrators Backup Operators **Required:** No Change	**Default:** Administrators Backup Operators **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** Administrators Backup Operators Server Operators **Required:** No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Misuse of this privilege violates FDP_ACF.1(a), Discretionary Access Control by allowing a user to bypass ACL

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	application interface. Otherwise normal file and directory permissions apply.					restrictions. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the privilege to conduct backups. Do not assign this privilege to any account, other than the defaults, in order to ensure that only authorized administrators are granted this right though membership in the Administrators, Backup Operators, or Server Operators groups.
Bypass traverse checking (SeChangeNotifyPrivilege)	Allows the user to pass through folders to which the user otherwise has no access while navigating an object path in any Microsoft Windows file system or in the	**Default:** Administrators Backup Operators Power Users Users Everyone **Recommended**	**Default:** Administrators Backup Operators Power Users Users Everyone **Recommended**	**Default:** (Not Defined)	**Default:** Administrators Authen. Users Everyone	

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	Registry. This privilege does not allow the user to list the contents of a folder; it allows the user only to traverse its directories.	**Change:** No Change	**Change:** No Change	**Recommended Change**: No Change	**Recommended Change:** No Change	
Change the system time (SeSystemTimePrivilege)	Allows the user to set the time for the internal clock of the computer.	**Default:** Administrators Power Users **Required Change:** No Change	**Default:** Administrators Power Users **Required Change:** No Change	**Default:** (Not Defined) **Required Change:** No Change	**Default:** Administrators Server Operators **Required Change:** No Change	Default settings support the following TOE Security Functional Requirements: FMT_SMR.1 Security Roles, and FMT_MTD.1.1(g) Management of TSF Time. Implements the following TOE Security functions: Para 6.1.4.1, Roles and para 6.1.5.6 Time Service. Can be used to grant authorized users the privilege to set the system time.
Create a token object (SeCreateTokenPrivilege)	Allows a process to create an access token by	**Default:** None	**Default:** None	**Default:** (Not Defined)	**Default:** None	Default settings support the following TOE Security Functional

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	calling NtCreateToken() or other token token-creating APIs.	**Required Change:** No Change	**Required Change:** No Change	**Required:** None	**Required:** No Change	Requirements: FPT_SEP.1.2, Domain Separation. Implements the following TOE Security functions: Para 6.1.5.5, Domain Separation. The use of this privilege is not auditable. Misuse of this privilege can lead to the violation of FIA_USB.1, User Subject Binding, and FAU_GEN.1, Audit Data Generation. **Change:** Set the Domain Policy to None for this privilege to enforce the default settings on the domain and ensure support of FPT_SEP.1.2. When a process requires this privilege, use the *LocalSystem* account (which already

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						has this privilege), rather than creating a separate account and assigning it this privilege to it.
Create permanent shared objects (SeCreatePermanentPrivilege)	Allow a process to create a directory object in the Windows 2000 object manager. This privilege is useful to kernel-mode components that extend the Windows 2000 object namespace. Components that are running in kernel mode already have this privilege; it is not necessary to assign it to them.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	
Create a pagefile (SeCreatePagefilePrivilege)	Allows the user to create and change the size of a pagefile.	**Default:** Administrators **Required:** No Change	**Default:** Administrators **Required:** No Change	**Default:** (Not Defined) **Required:** Administrators	**Default:** Administrators **Required:** No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the privilege to change pagefile settings. **Change:** Set the Domain Policy to Administrators for this privilege to support trusted administration and protect against unauthorized system modifications.
Debug programs (SeDebugPrivilege)	Allows the user to attach a debugger to any process.	**Default:** Administrators **Required:** No Change	**Default:** Administrators **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** Administrators **Required:** No Change	Assignment of this privilege violates the FAU_GEN.1, Audit Data Generation and FDP_ACF.1(a), Discretionary Access Control TOE Security Functional Requirements. This privilege allows the user access to objects regardless of the ACLs.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						This privilege is not auditable and should not be assigned to any users, including administrators. **Changes:** Changed all default privilege assignments to None to ensure compliance with FAU_GEN.1 and FDP_ACF.1(a).
Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)	Allows the user to change the Trusted for Delegation setting on a user or computer in Active Directory. The user or computer that is granted this privilege must also have write access to the account control flag on the object.	**Default:** None **Required:** No Change	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required Change:** None	**Default:** Administrators **Required:** No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the Trusted for Delegation settings on a user or computer in Active Directory.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						Misuse of this privilege or the Trusted for Delegation settings can make the network vulnerable to sophisticated attacks on the system that use Trojan horse programs, which impersonate incoming clients and use their credentials to gain access to network resources. **Changes:** Set the Domain Policy to None for this privilege to protect against the unauthorized access and modification.
Force shutdown from a remote system (SeRemoteShutdownPrivilege)	Allows a user to shut down a computer from a remote location on the network.	**Default:** Administrators **Recommended Change:** No Change	**Default:** Administrators **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** Administrators	**Default:** Administrators Server Operators **Recommended Change:** No Change	
Generate security audits	Allows a process to generate	**Default:**	**Default:**	**Default:**	**Default:**	Supports the following TOE security

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
(SeAuditPrivilege)	entries in the security log. The security log is used to trace unauthorized system access and other security relevant activities.	None **Required**: No Change	None **Required**: No Change	(Not Defined) **Required**: No Change	None **Required**: No Change	requirement through the LocalSystem account: FAU_GEN.1.1, Audit Data Generation. If granted to users, this privilege would allow non-TFS generated audit records in the audit log. Use of this privilege is not auditable. **Changes**: Set the Domain Policy to None for this privilege. This privilege should not be allowed for any user, including administrators.
Increase quotas (SeIncreaseQuotaPrivilege)	Allows a process that has Write Property access to another process to increase the processor quota that is assigned to the other process. This privilege is useful for system tuning, but it can be abused, as in a	**Default**: Administrators **Recommended**: No Change	**Default**: Administrators **Recommended**: No Change	**Default**: (Not Defined) **Required Change**: Administrators	**Default**: Administrators **Recommended**: No Change	Could be used to support the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. However, there is not an ST requirement that specifically mandates that this ability be

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	denial of service attack.					restricted to the administrator. Can support the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability to increase the processor quota assigned to a process. Misuse of this privilege can cause a Denial of service, which is a serious security issue. Since managing the processor quota affects performance and availability. However, the ST does not claim to address Denial of Service. **Changes**: Set the Domain Policy to Administrators for this privilege to enforce trusted administration.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Increase scheduling priority (SeIncreaseBasePriorityPrivilege)	Allows a process that has Write Property access to another process to increase the execution priority of the other process.	**Default**: Administrators **Recommended**: No Change	**Default**: Administrators **Recommended**: No Change	**Default**: (Not Defined) **Required Change**: Administrators	**Default**: Administrators **Recommended**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. However, there is not an ST requirement that specifically mandates that this ability be restricted to the administrator. Can be used to support the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability to increase process execution priorities. Misuse of this privilege can cause a Denial of service, which is a serious security issue. Since managing the processor quota affects performance and

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						availability. However, the ST does not claim to address Denial of Service. **Changes**: Set the Domain Policy to Administrators for this privilege to enforce trusted administration.
Load and unload device drivers (SeLoadDriverPrivilege)	Allows a user to install and uninstall Plug and Play device drivers. This privilege does not apply to device drivers that are not Plug and Play; only Administrators can install these device drivers. Note that device drivers run as Trusted (highly privileged) processes; a user can abuse this privilege by installing hostile	**Default**: Administrators **Required**: No Change	**Default**: Administrators **Required**: No Change	**Default**: (Not Defined) **Required Change**: Administrators	**Default**: Administrators **Required**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability to install and configure device drivers. **Changes**: Set the Domain Policy to Administrators for this

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	programs and giving them destructive access to resources.					privilege to support trusted administration.
Lock pages in memory (SeLockMemoryPrivilege)	Allows a process to keep data in physical memory, which prevents the system from paging data to virtual memory on disk. Assigning this privilege can result in significant degradation of system performance.	**Default**: None **Recommended Change**: No Change	**Default**: None **Recommended Change**: No Change	**Default**: (Not Defined) **Recommended Change**: No Change	**Default**: None **Recommended Change**: No Change	
Manage auditing and security log (SeSecurityPrivilege)	Allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and Registry keys. Object access auditing is not actually performed unless it has been enabled it in Audit	**Default**: Administrators **Required**: No Change	**Default**: Administrators **Required**: No Change	**Default**: (Not Defined) **Required Change**: Administrators	**Default**: Administrators **Required**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles, FAU_SAR.1.1, Audit Review, FAU_SAR.2.1, Restricted Audit Review, FAU_SAR.3, Selectable Audit

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	Policy. A user who has this privilege also can view and clear the security log from event viewer.					Review, FAU_SEL.1, Selective Audit, FAU_STG.1.1, FAU_STG.1.2, Guarantees of Audit Availability FMT_MOF.1.1(a), Management of Audit FMT_MTD.1.1(a), Management of the Audit Trail FMT_MTD.1.1(b), Management of Audited Events Implements the following TOE Security functions: Para 6.1.4.1, Roles and para 6.1.1 Audit Function. Can be used to grant authorized users the administrative capability to configure and manage audit data. **Changes**: Set the Domain Policy to Administrators for this

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						privilege to support trusted administration.
Modify firmware environment values (SeSystemEnvironmentPrivilege)	Allows modification of system environment variables either by a process through an API or by a user through the System Properties applet.	**Default**: Administrators **Recommended Change**: No Change	**Default**: Administrators **Recommended Change**: No Change	**Default**: (Not Defined) **Recommended Change**: Administrators	**Default**: Administrators **Recommended Change**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability to modify system environment variables. **Changes**: Set the Domain Policy to Administrators for this privilege to support trusted administration.
Profile a single process (SeProfileSingleProcessPrivilege)	Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to	**Default**: Administrators Power Users **Recommended**	**Default**: Administrators Power Users **Recommended**	**Default**: (Not Defined) **Recommended**	**Default**: Administrators **Recommended**	Could be used to supports the following TOE Security Functional Requirement:

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	monitor the performance of nonsystem processes.	**Change**: No Change	**Change**: No Change	**Change**: No Change	**Change**: No Change	FMT_SMR.1 Security Roles. Could be used to support the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability run performance diagnostics of nonsystem processes. However, the ST does not claim to address the ability provided by this privilege specifically.
Profile system performance (SeSystemProfilePrivilege)	Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to monitor the performance of system processes.	**Default**: Administrators **Required**: No Change	**Default**: Administrators **Required**: No Change	**Default**: (Not Defined) **Required Change**: Administrators	**Default**: Administrators **Required**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles Supports the following TOE Security functions: Para 6.1.4.1, Roles and para 6.1.5.1, System Integrity. Can be used

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						to grant authorized users the administrative capability to performance diagnostics of system processes. **Changes**: Set the Domain Policy to Administrators for this privilege to support trusted administration.
Remove computer from docking station (SeUndockPrivilege)	Allows a user of a portable computer to unlock the computer by clicking “Eject PC” on the Start menu.	**Default**: Administrators Power Users Users **Recommended Change**: No Change	**Default**: Administrators Power Users Users **Recommended Change**: No Change	**Default**: (Not Defined) **Recommended Change**: No Change	**Default**: Administrators **Recommended Change**: No Change	
Replace a process-level token (SeAssignPrimaryTokenPrivilege)	Allows a parent process to replace the access token that is associated with a child process.	**Default**: None **Required**: No Change	**Default**: None **Required**: No Change	**Default**: (Not Defined) **Required**: No Change	**Default**: None **Required**: No Change	Assignment of this privilege violates the following TOE Security Functional Requirement: FDP_ACF.1(a), Discretionary Access Control Functions and

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						FIA_USB.1, User Subject Binding, and FAU_GEN.1, Audit Data Generation. This privilege is not auditable. **Changes**: Changed default Domain Security Policy privilege assignments to None to ensure Domain compliance with FDP_ACF.1(a), FIA_USB.1, and FAU_GEN.1. Do not assign this privilege to any user.
Restore files and directories (SeRestorePrivilege)	Allows a user to circumvent file and directory permissions when restoring backed-up files and directories and to set any valid security principal as the owner of an object.	**Default**: Administrators Backup Operators **Required**: No Change	**Default**: Administrators Backup Operators **Required**: No Change	**Default**: (Not Defined) **Required**: No Change	**Default**: Administrators Backup Operators Server Operators **Required**: No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Misuse of this privilege violates FDP_ACF.1(a), Discretionary Access Control by allowing a user to bypass ACL

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						restrictions. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the privilege to restore backups. Do not assign this privilege to any account, other than the defaults, in order to ensure that only authorized administrators are granted this right though membership in the Administrators, Backup Operators, or Server Operators groups.
Shut down the system (SeShutdownPrivilege)	Allows a user to shut down the local computer.	**Default:** Administrators BACKUP OPERATORS Power Users Users	**Default:** Administrators Backup Operators Power Users	**Default:** (Not Defined)	**Default:** Administrators Account Operators Backup Operators Server Operators Print Operators	

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
		Recommended Change: Administrators Backup Operators Power Users Authenticated Users	**Recommended Change:** Administrators Backup Operators Power Users Authenticated Users	**Recommended Change:** No Change	**Recommended Change:** No Change	
Synchronize directory service data (SeSyncAgentPrivilege)	Allows a service to provide directory synchronization services. This privilege is relevant only on Domain Controllers. Required for a domain controller to use the LDAP directory synchronization services. This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** (Not Defined) **Recommended Change:** No Change	**Default:** Administrator **Recommended Change:** No Change	

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers					
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	Allows the user to take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, Registry keys, processes, and threads.	**Default:** Administrators **Required:** No Change	**Default:** Administrators **Required:** No Change	**Default:** (Not Defined) **Required Change:** Administrators	**Default:** Administrators **Required:** No Change	Supports the following TOE Security Functional Requirement: FMT_SMR.1 Security Roles. Misuse of this privilege violates FDP_ACF.1(a), Discretionary Access Control by allowing a user to bypass ACL restrictions. Implements the following TOE Security functions: Para 6.1.4.1, Roles. Can be used to grant authorized users the administrative capability of any securable object in the system.

User Rights/Privileges	Description	Groups Assigned this Right on Stand Alone Windows 2000 Professional	Groups Assigned this Right on Stand Alone Windows 2000 Servers	Groups Assigned this Right in Windows 2000 Domain Security Policy (Located on Domain Controller)	Groups Assigned this Right on Windows 2000 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
						Changes: Set the Domain Policy to Administrators for this privilege to support trusted administration.
Read unsolicited data from a terminal device (SeUnsolicitedInputPrivilege)	Required to read unsolicited input from a terminal device. It is obsolete and unused. it has no effect on the system.	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	**Default:** None **Recommended Change:** No Change	

Appendix D– User and Group Accounts

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Local User Accounts	**Default Local user accounts.**					
Administrator	Built-in account for administering the computer/domain.	✓	✓	✓		Use of this account by more than one authorized administrator violates FAU_GEN.2, User Identity Association which states that each auditable event must be associated with the identity of the user that caused the event. **Requirement**: Assign roles to authorized administrators by placing their user accounts in administrative groups appropriate to their level of responsibility. This ensures that all administrative actions can be tracked in audit logs to specific user accounts. Rename the Administrator account and secure the password for emergency use only.
Guest	Built-in account for guest access to the computer/domain.	✓	✓	✓		Misuse of this account can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. This account is disabled on all systems by default. **Requirement**: This account must remain disabled.
TsInternetUser	User account used by Terminal Services. It is used by the Terminal Services Internet Connector License. When Internet Connector Licensing is enabled, a Windows 2000-based server accepts 200		✓	✓		Use of this account by more than one user violates FAU_GEN.2, User Identity Association. **Requirement**:

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	anonymous-only connections. Terminal Services clients are not prompted with a logon dialog box; they are logged on automatically with the TsInternetUser account.					Terminal Services is not an objective of the TOE and accounts that support anonymous access are not to be allowed. Therefore, disable this account.
krbtgt	Key distribution service center account. Windows 2000 Kerberos authentication is achieved by the use of tickets enciphered with a symmetric key derived from the password of the server or service to which access is requested. To request such a session ticket, a special ticket, called the Ticket Granting Ticket (TGT) must be presented to the Kerberos service itself. The TGT is enciphered with a key derived from the password of the krbtgt account, which is known only by the Kerberos service.			✓		Use of this account by more than one user violates FAU_GEN.2, User Identity Association. This account is disabled on Domain Controllers by default. **Requirement**: Unlike other user accounts, the krbtgt account cannot be used to log on to the domain and in fact, cannot be enabled
Global Groups	**When a domain is created, Windows 2000 creates the following built-in global groups in the Active Directory store to group common types of user accounts for use throughout the domain.**					**Global groups provide the ability to assign users to authorized administrator and authorized user roles with unique domain-level access restrictions based on the global group to which the user is assigned. Global groups support the FMT_SMR.1, Security Roles TOE Security Functional Requirement.**
Cert Publishers	Enterprise certification and renewal agents. Includes all computers that are running an enterprise certificate authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.			✓	None	Windows 2000 Cert Server is not in the Evaluated Configuration

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
DnsUpdateProxy	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).			✓	None	The TOE will support FQDN and does not require membership in this group. **Requirement**: Do not add accounts to this group
Domain Admins	This group is only available on Windows 2000 servers acting as Domain Controllers. Its members are allowed administrative privileges for the entire domain. By default, this group has the local Administrator account on the Domain Controller as its member.			✓	Administrator	Supports assignment of administrative role with control within a specific domain. **Requirement:** Do not add non-administrative accounts (users) to this group.[1]
Domain Computers	All servers and workstations joined to the domain, excluding domain controllers.			✓	None	Supports assignment of user role supporting access to domain-computer-specific resources.
Domain Controllers	Group account for all Domain Controllers in the domain.			✓	DC_Name	Supports assignment of user role supporting access to domain-controllers-specific resources
Domain Guests	This group is only available on Windows 2000 servers acting as Domain Controllers. Members of this group are only allowed to access the system from across the network and have very limited privileges by default and initially only contains the Guest user account for the domain.			✓	Guest	Guest/anonymous accounts can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement**: Do not use this group. Remove all accounts including Guest from this group.

[1] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Domain Users	This group is only available on Windows 2000 servers acting as Domain Controllers. In a domain environment, the Administrator account and all new user accounts are automatically included as members of this group. This group is also a member of the Users local group for the domain and for every Windows computer in the domain.			✓	Administrator Guest Krbtgt TsInternetUser (all new users are added by default)	Supports assignment of user role supporting access to domain resources. Guest/anonymous accounts can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement**: Remove the Guest, and TsInternetUser accounts.
Enterprise Admins	Provides administrative control over the entire network. By default, the Domain Controller's Administrator account is a member. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains.			✓	Administrator (Domain Controller)	Supports assignment of administrative role with control over the entire network.
Group Policy Creator Owner	Members in this group can modify group policy for the domain. The group that is authorized to create new Group Policy objects in Active Directory.			✓	Administrator	Supports assignment of administrative role designated to maintain domain level group policies. **Requirement**: Do not add non-administrative accounts to this group.[2]
Schema Admins	Designated administrators of the Active Directory schema. The group is authorized to make schema changes in Active Directory.			✓	Administrator	Supports assignment of administrative role designated to administer the Active Directory Schema. **Requirement**:

[2] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
						Do not add non-administrative accounts to this group.[3]
Domain Local Groups	**Domain local groups provide users with privileges and permissions to perform tasks specifically on the domain controller and in the Active Directory store.**					**Domain local groups provide the ability to assign users to authorized administrator and authorized user roles with unique Domain Controller access restrictions based on the domain local group to which the user is assigned. Domain local groups support the FMT_SMR.1, Security Roles TOE Security Functional Requirement.**
Account Operators	This group is only available on Windows 2000 servers acting Domain Controllers. It allows its members to administer user and group accounts for systems and domains. By default, Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units (OUs) of Active Directory except the Builtin container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.			✓	None	Supports assignment of administrative role designated to manage user accounts within a domain. **Requirement:** Do not add non-administrative accounts to this group.[4]

[3] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

[4] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Administrators	Members can perform all administrative tasks on all domain controllers and the domain itself.			✓	Administrator Domain Admins Enterprise Admins	Supports assignment of administrative role with full administrative access rights to all domain controllers and resources within a domain. **Requirement**: Do not add non-administrative accounts to this group.[5]
Backup Operators	Members can back up and restore files on all domain controllers by using Windows Backup, regardless of the permissions that protect those files. Backup Operators also can log on to the computer and shut it down.			✓	None	Misuse of this account can violate FDP_ACF.1(a), Discretionary Access Control. A member of the Backup Operators group can extract files and directories for which the user would normally not have access. Membership in this group permits users to open any file for backup purposes; however, once the file has been opened for read access it can be redirected by the Backup Operator to any location. By default, users are allowed to backup and restore files for which they have the appropriate file and directory permissions without requiring membership in the Backup Operators group. The Administrator account already has full backup rights. **Requirement**:

[5] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
						Do not add non-administrative accounts to this group.[6]
DnsAdmins	DNS administration group. This group has Full Control over a DNS Server and its zones.			✓	None	Supports assignment of administrative role responsible for administering DNS. **Requirement**: Do not add non-administrative accounts to this group.[7]
Guests	The Guest group offers limited access to resources on the system. Members cannot make permanent changes to their desktop environment. Some services automatically add users to this group when they are installed. For example, IIS adds anonymous user accounts to the Guests built-in group.			✓	Guest (local) Domain Guests TsInternetUser	Guest/anonymous accounts can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement**: Do not use this group. Remove all accounts including Guest from this group.
Pre-Windows 2000 Compatible Access	A backward compatibility group that allows read access on all users and groups in the domain.			✓	None	**Requirement**: Backward compatibility with pre-Windows 2000 systems is not an objective of the TOE. Therefore, do not add users to this group.
Print Operators	A built-in group that exists only on domain controllers. Members can set up and manage network printers on domain controllers. Members of this group are			✓	None	Supports assignment of administrative role responsible for managing print services within a domain. **Recommendation**:

[6] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

[7] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	given the rights to create, change, and delete printer shares within the domain. Members can also log on to systems locally and shut them down.					This is an administrative function, therefore only add authorized administrators to this group.
Replicator	Supports file replication on Domain Controllers. It is used by the File Replication service on domain controllers. Members can configure file replication services. The directory replicator service is used to automatically copy files, such as user logon scripts, between Windows 2000-based computers.			✓	None	Can be used in support of requirements identified in para 6.1.5.3, TFS Data Replication Consistency. Supports assignment of administrative role responsible for administering directory replication services within a domain. **Requirement**: Do not add non-administrative accounts to this group.[8]
RAS and IAS Servers	Servers in this group can access remote access properties of users.			✓	None	
Server Operators	This group is only available on Windows 2000 Servers acting as Domain Controllers. Members of this group can perform server management tasks such as creating, changing, and deleting shared printers, shared directories, and files. They can also back up and restore files, lock the server console and shutdown the system. They cannot modify system policies or start and stop			✓		Supports assignment of administrative role responsible for server maintenance. **Requirement**: Do not add non-administrative accounts to this group.[9]

[8] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

[9] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	services.					
Users	This group provides the user with the necessary rights to operate the computer as an end user, such as running applications and managing files. By default, Windows 2000 adds all new local user accounts to the Users group.			✓	Authenticated Users Domain Users INTERACTIVE (all new local users are added by default)	Supports assignment of user role supporting access to resources on the domain controller. **Requirement**: Do not accounts with potential for unauthenticated access (such as Guest) to this group.
Local Groups	**All stand-alone Windows 2000 Servers, member servers, and Professional workstations have built-in local groups. These built-in local groups provide members with the capability to perform tasks on the specific computer to which the group belongs.**					**Local groups provide the ability to assign users to authorized administrator and authorized user roles with unique local access restrictions based on the local group to which the user is assigned. Local groups support the FMT_SMR.1, Security Roles TOE Security Functional Requirement.**
Administrators	Members of the Administrators group are allowed complete control over the entire computer. When a member server or a computer running Windows 2000 joins a domain, the Domain Admins group is added to the local Administrators group.	✓	✓		**Stand-alone**: Administrator **Domain Members**: Administrator Domain Admins	Supports assignment of administrative role with full administrative access rights to all local resources on a computer. **Requirement**: Do not add non-administrative accounts to this group.[10]
Backup Operators	Members can use Windows Backup to back up and restore the computer regardless of file system security.	✓	✓		None	Misuse of this account can violate FDP_ACF.1(a), Discretionary Access Control. A member of the Backup Operators group can extract files and directories for which the user

[10] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
						would normally not have access. Membership in this group permits users to open any file for backup purposes, however, once the file has been opened for read access it can be redirected by the Backup Operator to any location. By default, users are allowed to backup and restore files for which they have the appropriate file and directory permissions without requiring membership in the Backup Operators group. The Administrator account already has full backup rights. **Requirement**: Do not add non-administrative accounts to this group.[11]
Guests	The Guest group offers limited access to resources on the system. Members cannot make permanent changes to their desktop environment. By default, the Guest user account for the computer is a member. This account is disabled by default.	✓	✓		**Stand-alone Professional:** Guest **Stand-alone Server:** Guest TsInternetUser **Domain Members:** Add Domain Guests	Guest/anonymous accounts can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement**: Do not use this group. Remove all accounts including Guest from this group.

[11] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Power Users	Membership provides users with the ability to create and modify local user accounts on the computer and share resources, without giving the user complete control over the computer.	✓	✓		None	Supports assignment of user role supporting elevated user rights on a specific computer. This group provides administrative level privileges such as management of local user accounts and local resource management. Membership in this group by users who are not authorized administrators violates FMT_MTD.1(c), Management of User Attributes, FMT_MTD.1(d), Management of Authentication Data (for user created accounts), FMT_MTD.1(e), Management of Account Lockout Duration (for user created accounts), Management of Minimum Password Length (for user created accounts), and FMT_SMR.1, Security Roles to the extent that users would be privileges generally associated with an authorized administrator role. **Requirement**: Do not add non-administrative accounts to this group.[12]
Replicator	Members can configure file replication services. The directory replicator service is used to automatically copy files, such as user logon scripts, between Windows 2000-based computers.	✓	✓		None	Can be used in support of requirements identified in para 6.1.5.3, TFS Data Replication Consistency. Supports assignment of administrative role responsible for administering directory replication services within a computer.

[12] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
						Requirement: Do not add non-administrative accounts to this group.[13]
Users	This group provides the user with the necessary rights to operate the computer as an end user, such as running applications and managing files. By default, Windows 2000 adds all new local user accounts to the Users group. When a member server or a computer running Windows 2000 joins a domain, the Domain Users global group, the Authenticated Users special group, and the INTERACTIVE special group are added to the local Users group.	✓	✓		**Stand-alone:** Authenticated Users INTERACTIVE (all new local users are added by default) **Domain Members:** Authenticated Users Domain Users INTERACTIVE (all new local users are added by default)	Supports assignment of user role supporting access to local resources on the computer. **Requirement**: Do not add accounts with potential for unauthenticated access (such as Guest) to this group.
System Groups	**System groups do not have specific memberships that can be modified. Each is used to represent a specific class of users or to represent the operating system itself. These groups are created by Windows 2000 systems automatically, but are not shown in the group administration GUIs.**					

[13] It is not necessary to remove the corresponding group from DACLs of secured objects as long as this requirement is met.

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Anonymous Logon	Includes any user account that Windows 2000 did not authenticate.	✓	✓	✓	All unauthenticated users.	Misuse of this account can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement:** Do not grant resource permissions or user rights to this account.
Authenticated Users	Includes all users with a valid user account on the computer or in Active Directory services.	✓	✓	✓	All authenticated users.	Supports FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification. **Recommendation:** Use the Authenticated Users group instead of the Everyone group to prevent anonymous access to a resource.
BATCH	A group that includes all users logged on through a batch queue facility.	✓	✓	✓		
CREATOR OWNER	Includes the user account for a user who created or took ownership of a resource. If a member of the Administrators group creates a resource, the Administrators group is the owner of the resource. This group is created for each sharable resource on Windows 2000 Server or Professional. A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's creator.	✓	✓	✓	Members of this group are users who create or take ownership of resources.	Supports FDP_ACF.1(a), Discretionary Access Control Functions through assignment of object owner attributes.
CREATOR GROUP	A placeholder in an inheritable ACE.	✓	✓	✓		

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's creator.					
DIALUP	Includes any user who currently has a dial-up connection.	✓	✓	✓	All dial-in users.	**Requirement:** Dial-up service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.
ENTERPRISE DOMAIN CONTROLLER	A group that includes all domain controllers in a forest that uses an Active Directory service.			✓		
Everyone	Includes all users who access the computer. Windows 2000 will authenticate a user who does not have a valid user account as Guest. The user automatically gets all rights and permissions assigned to the Everyone group. A group that includes all users, even anonymous users and guests.	✓	✓	✓	Members of this group include all users accessing Windows 2000 Server or Professional locally, through the network, or through RAS. This includes authenticated and unauthenticated users. In essence, every user who accesses the system is a member of the Everyone group.	Misuse of this account can violate FAU_GEN.2, User Identity Association, FIA_UAU.2, Authentication, and FIA_UID.2, User Identification Before Any Action. **Requirement:** Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary
INTERACTIVE	Includes the user account for the user logged on locally at the computer. Members of the Interactive group gain access to resources on the computer at which they are physically located.	✓	✓	✓	This group includes all users who log into Windows 2000 Server or Professional locally. Users who are connected across a network are not members of this group.	

Windows 2000 Built-In Users and Groups	Description	Stand Alone Professional	Stand Alone Servers	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
NETWORK	Includes any user with a current connection from another computer on the network to a shared resource on the computer.	✓	✓	✓	This group includes all users who are connected to resources across a network, but does not include those who are connected interactively.	
PROXY	This SID is not used in Windows 2000.			✓		
RESTRICTED	This SID is not used in Windows 2000.			✓		
SELF	A placeholder in an inheritable ACE on an account object or group object in Active Directory. When the ACE is inherited, the system replaces this SID with the SID for the security principal who holds the account.			✓		
SERVICE	A group that includes all security principals logged on as a service.	✓	✓	✓		
SYSTEM	Account used by the operating system to run services, utilities, and device drivers. This account has unlimited power and access to resources that even Administrators are denied, such as the Registry's SAM.	✓	✓	✓		This account is used by Windows 2000 to execute security services such as TSF protection functions that are beyond the control of authorized administrators.
TERMINAL SERVER USER		✓	✓	✓		**Requirement**: Terminal service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.

Appendix E
Windows 2000 Security Configuration Checklist for the Evaluated Configuration

Operating System Configuration		
Operating System Type:	❑ **Windows 2000 Professional**	
	❑ **Windows 2000 Server**	❑ **Domain Controller**
	❑ **Windows 2000 Advanced Server**	❑ **Domain Controller**
		Other Service Pack Level: _____
Service Pack Level:	**Windows 2000 Service Pack 3 (Req.)**	**Post Service Pack Hotfixes:**
Network Membership:	❑ **Workgroup Name: _____**	❑ **Q326886 (Req.)**
	❑ **Domain Name: _____**	_____
		_____
Date of Installation:	_____	_____

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	**File System Configuration** **Security Objective:** Allow configuration of evaluated security mechanisms and support conformance to Security Target requirements. **File System Type: NTFS**	✓	
Account Policies			
	Password Policy		
❑	***Enforce Password History*** **Security Objective:** Set limit on how often passwords may be reused. **Computer Setting**: **_____ passwords remembered** (Recommended: 24 passwords remembered.)		✓
❑	***Maximum Password Age*** **Security Objective:** Set the length of time users can keep their passwords before they have to change it. **Computer Setting: _____ days** (Recommended: 42 days.)		✓
❑	***Minimum Password Age*** **Security Objective:** Set the length of time users must keep a password before they can change it. **Computer Setting: _____ days** (Recommended: 2 days.)		✓
❑	***Minimum Password Length*** **Security Objective:** Set the minimum number characters required for user passwords. **Computer Setting: 8 characters**	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Passwords Must Meet Complexity Requirements*** **Security Objective:** Requires the use of complex (strong) passwords. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: Enabled.)		✓
❑	***Store Passwords Using Reversible Encryption for all Users in the Domain*** **Security Objective:** **Do Not Enable.** Uses weak encryption for passwords. **Computer Setting: Disabled**	✓	
	Account Lockout Policy		
❑	***Account Lockout Duration*** **Security Objective:** After invalid password attempts, locks account for a specified period of time. **Computer Setting: _____ minutes** (The ST requires this setting, but does not specify the duration. Recommendation is to set to **0**, which requires an administrator to unlock the account.)	✓	
❑	***Account Lockout Threshold*** **Security Objective:** Set the number of bad login attempts allowed before locking the account. **Computer Setting: _____ invalid login attempts** (The ST requires this setting and specifies that it must not be set to a value greater than 5. Recommendation is to set to this value to 5 bad login attempts.)	✓	
❑	***Reset Account Lockout Counter After*** **Security Objective:** Set how long the lockout threshold is maintained before being reset. **Computer Setting: _____ minutes** (This value must be set when setting the previous two policy values. Recommended setting is **30** minutes.)	✓	
	Kerberos Policy		
❑	***Enforce User Logon Restrictions*** **Security Objective:** Validates every logon request by checking the user rights policy. **Computer Setting: Retain default settings (Enabled)**	✓	
❑	***Maximum Lifetime for Service Ticket*** **Security Objective:** Sets the maximum duration for which a service ticket is valid. **Computer Setting: _____ minutes** (Default setting is recommended: 600 minutes for domain members, 60 minutes for non-domain computers.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Maximum Lifetime for User Ticket*** **Security Objective:** Sets the maximum duration for which a user ticket is valid. **Computer Setting: _____ hours** (Default setting is recommended: 10 hours for domain members, 7 hours for non-domain computers.)		✓
❑	***Maximum Lifetime for User Ticket Renewal*** **Security Objective:** Sets the renewal period for expired tickets. **Computer Setting: _____ days** (Default setting is recommended: 7 days for domain members, 10 days for non-domain computers.)		✓
❑	***Maximum Tolerance for Computer Clock Synchronization*** **Security Objective:** Sets the maximum tolerance for synchronization between computers in the Domain. **Computer Setting: Retain default settings (5 minutes for domain members, 60 minutes for non-domain computers)**	✓	
Local Policies			
	Audit Policy		
❑	***Audit Account Logon Events*** **Security Objective:** Audit account logon/logoff events from another computer in which this computer is used to validate the account. "Account logon events" are generated where the account resides. **Computer Setting: ❑ Success ❑ Failure** (Recommended: Success, Failure)		✓
❑	***Audit Account Management*** **Security Objective:** Audit account management activities. **Computer Setting: ❑ Success ❑ Failure** (Recommended: Success, Failure)		✓
❑	***Audit Directory Service Access*** **Security Objective:** Audit access to an Active Directory object that has its own system access control list specified. **Computer Setting: ❑ Success ❑ Failure** (Recommended: Success, Failure)		✓
❑	***Audit Logon Events*** **Security Objective:** Audit local or network logon/logoff events to this computer. "Logon events" are generated where the logon attempt occurs. **Computer Setting: ❑ Success ❑ Failure** (Recommended: Success, Failure)		✓

<table>
<tr><th>Completed and Verified</th><th>WINDOWS 20000
Security Configuration Checklist

(Settings apply to all operating system versions except where otherwise noted)</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Audit Object Access
Security Objective: Audit access to an object--for example, a file, folder, registry key, or printer, which has its own system access control list specified.
Computer Setting: ❑ Success ❑ Failure
(Recommended: Success, Failure)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Audit Policy Change
Security Objective: Audit a change to user rights assignment policies, audit policies, or trust policies.
Computer Setting: ❑ Success ❑ Failure
(Recommended: Success)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Audit Privilege Use
Security Objective: Audit each instance of a user exercising a user right.
Computer Setting: ❑ Success ❑ Failure
(Recommended: Success, Failure)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Audit Process Tracking
Security Objective: Audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.
Computer Setting: ❑ Success ❑ Failure
(Recommended: Success, Failure)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Audit System Events
Security Objective: Audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.
Computer Setting: ❑ Success ❑ Failure
(Recommended: Success)</td><td></td><td>✓</td></tr>
<tr><td></td><td>User Rights Assignment</td><td></td><td></td></tr>
<tr><td>❑</td><td>Access this Computer from the Network
Security Objective: Determines which users are allowed to connect over the network to the computer.
Computer Setting: Assigned To:
<table>
<tr><th>Professional</th><th>Server/Adv. Server</th><th>Domain Controller</th></tr>
<tr><td>Administrators</td><td>Administrators</td><td>Administrators</td></tr>
<tr><td>Authenticated Users</td><td>Authenticated Users</td><td>Authenticated Users</td></tr>
<tr><td>Backup Operators</td><td>Backup Operators</td><td></td></tr>
<tr><td>Power Users</td><td>Power Users</td><td></td></tr>
<tr><td>Users</td><td>Users</td><td></td></tr>
</table>
(In Domain Policy set as indicated for Windows 2000 Professional and Servers.)</td><td>✓</td><td></td></tr>
</table>

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Act as Part of the Operating System*** **Security Objective:** Allow a process to authenticate as a user and thus gain access to the same resources as a user. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Add Workstations to Domain (Domain Controller)*** **Security Objective:** Allows a user to add a computer to a specific domain. **Computer Setting: Remove the Authenticated Users account and do not assign this privilege to other accounts. Domain Admins has this privilege by default.**	✓	
❑	***Backup Files and Directories*** **Security Objective:** Allows the user to circumvent file and directory permissions to backup the system. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Bypass Traverse Checking*** **Security Objective:** Allows the user to pass through folders to which the user otherwise has no access. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Change the System Time*** **Security Objective:** Allows the user to set the time for the internal clock of the computer. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Create a Pagefile*** **Security Objective:** Allows the user to create and change the size of a pagefile. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Create a Token Object*** **Security Objective:** Allows a process to create an access token. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Create Permanent Shared Objects*** **Security Objective:** Allow a process to create a directory object in the Windows 2000 object manager. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Debug Programs*** **Security Objective:** Allows the user to attach a debugger to any process. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Deny Access to this Computer from the Network*** **Security Objective:** Prohibits a user or group from connecting to the computer from the network. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Deny Logon as a Batch Job*** **Security Objective:** Prohibits a user or group from logging on through a batch-queue facility. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Deny Logon as a Service*** **Security Objective:** Prohibits a user or group from logging on as a service. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Deny Logon Locally*** **Security Objective:** Prohibits a user or group from logging on locally at the keyboard. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Enable Computer and User Accounts to be Trusted for Delegation*** **Security Objective:** Allows the user to change the Trusted for Delegation setting on a user or computer in Active Directory. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Force Shutdown from a Remote System*** **Security Objective:** Allows a user to shut down a computer from a remote location on the network. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Generate Security Audits*** **Security Objective:** Allows a process to generate entries in the security log. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Increase Quotas*** **Security Objective:** Allows a process that has Write Property access to another process to increase the processor quota that is assigned to the other process. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Increase Scheduling Priority*** **Security Objective:** Allows a process that has Write Property access to another process to **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
❑	***Load and Unload Device Drivers*** **Security Objective:** Allows a user to install and uninstall Plug and Play device drivers. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
❑	***Lock Pages in Memory*** **Security Objective:** Allows a process to keep data in physical memory, which prevents the system from paging data to virtual memory on disk. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Log on as a Batch Job*** **Security Objective:** Allows a user to log on by using a batch-queue facility. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Log on as a Service*** **Security Objective:** Allows a security principal to log on as a service. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Log on Locally*** **Security Objective:** Allows a user to log on locally at the computer's keyboard. **Computer Setting: Assigned To:** **Professional**: Administrators, Backup Operators, Power Users, Users **Server/Adv. Server**: Administrators, Backup Operators, Power Users, Users **Domain Controller**: Administrators, Account Operators, Backup Operators, Print Operators, Server Operators (In Domain Policy set as indicated for Windows 2000 Professional and Servers.)	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Manage Auditing and Security Log*** **Security Objective:** Allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and Registry keys. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
❑	***Modify Firmware Environment Values*** **Security Objective:** Allows modification of system environment variables either by a process through an API or by a user through the System Properties applet. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
❑	***Profile Single Process*** **Security Objective:** Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to monitor the performance of nonsystem processes. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Profile System Performance*** **Security Objective:** Allows a user to run Microsoft Windows NT and Windows 2000 performance monitoring tools to monitor the performance of system processes. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
❑	***Remove Computer from Docking Station*** **Security Objective:** Allows a user of a portable computer to unlock the computer by clicking "Eject PC" on the Start menu. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Replace a Process Level Token*** **Security Objective:** Allows a parent process to replace the access token that is associated with a child process. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Restore Files and Directories*** **Security Objective:** Allows a user to circumvent file and directory permissions when restoring backed-up files and directories and to set any valid security principal as the owner of an object. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Shut Down the System*** **Security Objective:** Allows a user to shut down the local computer **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: For Windows 2000 Professional assign to Administrators, Authenticated Users, Backup Operators, Power Users.)		✓
❑	***Synchronize Directory Service Data*** **Security Objective:** Allows a service to provide directory synchronization services. **Computer Setting: Assigned To:** _____ _____ _____ _____ _____ _____ (Recommended: Do not change the defaults)		✓
❑	***Take Ownership of Files or Other Objects*** **Security Objective:** Allows the user to take ownership of any securable object in the system. **Computer Setting: Do not change the defaults of "Assigned To: Administrators."** (In Domain Policy, assign to Administrators only.)	✓	
	Security Options		
❑	***Additional Restrictions for Anonymous Connections*** **Security Objective:** Set restrictions on anonymous connections to the computer. **Computer Setting: Do not allow enumeration of SAM accounts and shares**	✓	
❑	***Allow Server Operators to Schedule Tasks (Domain Controllers Only)*** **Security Objective:** Determines if Server Operators are allowed to submit jobs by means of the AT schedule facility. **Computer Setting: Disabled** (The AT schedule facility is not part of the Evaluated Configuration.)	✓	
❑	***Allow System to be Shut Down Without Logon Without Having to Log On*** **Security Objective:** Set a computer to allow shutdown without requiring a user to logon. **Computer Setting: Disabled**	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Allowed to Eject Removable NTFS Media*** **Security Objective:** Set the accounts allowed to eject removable NTFS media from the computer. **Computer Setting: Accounts defined in the policy: _____** (Recommended: Administrators)		✓
❑	***Amount of Idle Time Required Before Disconnecting a Session*** **Security Objective:** Set the amount of continuous idle time that must pass in a Server Message Block (SMB) session before the session is disconnected due to inactivity. **Computer Setting: _____ minutes** (Recommended: Do not change the default setting of 15 minutes.)		✓
❑	***Audit the Access of Global System Objects*** **Security Objective:** Allows access of global system objects to be audited. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled, only when there is a strict audit management process in place.)		✓
❑	***Audit the Use of Backup and Restore Privilege*** **Security Objective:** Allow auditing of Backup and Restore user rights. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled, only when there is a strict audit management process in place.)		✓
❑	***Automatically Log Off Users When Logon Time Expires*** **Security Objective:** When enabled, disconnects users that are connected to the local machine outside of their user account's valid logon hours. Can only be set on DCs. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled)		✓
❑	***Automatically Log Off Users When Logon Time Expires (Local)*** **Security Objective:** When enabled, disconnects users that are connected to the local machine outside of their user account's valid logon hours. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled)		✓
❑	***Clear Virtual Memory Pagefile When System Shuts Down*** **Security Objective:** Determines whether the virtual memory pagefile should be cleared when the system is shut down. **Computer Setting: Enabled**	✓	
❑	***Digitally Sign Client Communications (Always)*** **Security Objective:** Determines whether the computer will always digitally sign client communications. **Computer Setting: Disabled**	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Digitally Sign Client Communications (When Possible)*** **Security Objective:** If enabled, causes the SMB client to perform SMB packet signing only when communicating with an SMB server that is enabled or required to perform SMB packet signing. **Computer Setting: Enabled**	✓	
❑	***Digitally Sign Server Communications (Always)*** **Security Objective:** If enabled, requires the SMB server to perform SMB packet signing. **Computer Setting: Disabled**	✓	
❑	***Digitally Sign Server Communications (When Possible)*** **Security Objective:** If enabled, causes the SMB server to perform SMB packet signing when necessary. **Computer Setting: Enabled**	✓	
❑	***Disable CTRL+ALT+DEL Requirement for Logon*** **Security Objective:** Determines whether pressing CTRL+ALT+DEL is required before a user can log on. **Computer Setting: Disabled** (A "Disabled" setting actually enables/requires the use of CTRL+ALT+DEL)	✓	
❑	***Do Not Display Last User Name in Logon Screen*** **Security Objective:** Determines whether the name of the last user to logon to the computer is displayed in the Windows logon screen. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: Enabled)		✓
❑	***LAN Manager Authentication Level*** **Security Objective:** Determines which challenge/response authentication protocol is used for network logons. **Computer Setting: Selected Option:** _____ (Recommended: Send NTLMv2 response only/refuse LM & NTLM)		✓
❑	***Message Text for Users Attempting to Log On*** **Security Objective:** Specifies a text message that is displayed to users when they log on. **Computer Setting: Message text:** _____ _____ _____ (Recommended: Set a warning banner in accordance to local policy requirements.)		✓
❑	***Message Title for Users Attempting to Log On*** **Security Objective:** Specifies a title that appears in the title bar of the window containing the message text for users attempting to log on. **Computer Setting: Message title:** _____ (Recommended: Set a warning banner in accordance to local policy requirements.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Number of Previous Logons to Cache (In Case Domain Controller is not Available)*** **Security Objective:** Determines the number of times a user can log on to a Windows domain using cached account information. **Computer Setting: Cache: 0 logons**	✓	
❑	***Prevent System Maintenance of Computer Account Password*** **Security Objective:** Determines whether the computer account password should be prevented from being reset every week. If this policy is enabled, the machine is prevented from requesting a weekly password change. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Verify that local policies are set at the default of Disabled, and that Domain Policies are either Disabled or Not Defined.)		✓
❑	***Prevent Users from Installing Print Drivers*** **Security Objective:** Determines whether members of the Users group are prevented from installing print drivers. **Computer Setting: Enabled**	✓	
❑	***Prompt User to Change Password Before Expiration*** **Security Objective:** Determines how far in advance Windows 2000 should warn users that their password is about to expire. **Computer Setting: _____ days** (Recommended: Default setting of 14 days is adequate.)		✓
❑	***Recovery Console: Allow Automatic Administrative Logon*** **Security Objective:** If set, the Recovery Console does not require a password and will automatically log on to the system. **Computer Setting: Disabled** (The Recovery Console is not part of the Evaluated Configuration.)	✓	
❑	***Recovery Console: Allow Floppy Copy and Access to all Drives and all Folders*** **Security Objective:** Enabling this option enables the Recovery Console SET command. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Do not enable this option. The Recovery Console is not part of the Evaluated Configuration.)		✓
❑	***Rename Administrator Account*** **Security Objective:** Associates a different account name with the security identifier (SID) for the account "Administrator." **Computer Setting:** (Recommended: Change and safeguard the recorded account name. Do not record it in this document.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Rename Guest Account*** **Security Objective:** Associates a different account name with the security identifier (SID) for the account "Guest." **Computer Setting:** (Recommended: Change and safeguard the recorded account name. Do not record it in this document.)		✓
❑	***Restrict CD-ROM Access to Locally Logged-On User Only*** **Security Objective:** If enabled, this policy allows only the interactively logged-on user to access removable CD-ROM media. **Computer Setting: Enabled**	✓	
❑	***Restrict Floppy Access to Locally Logged-On User Only*** **Security Objective:** If enabled, this policy allows only the interactively logged-on user to access removable floppy media. **Computer Setting: Enabled**	✓	
❑	***Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always)*** **Security Objective:** If this policy is enabled, all outgoing secure channel traffic must be either signed or encrypted. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: By default this option is Disabled. Do not change the default setting.)		✓
❑	***Secure Channel: Digitally Encrypt or Sign Secure Channel Data (When Possible)*** **Security Objective:** If this policy is enabled, all outgoing secure channel traffic should be encrypted. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: By default this option is Enabled. Do not change the default setting.)		✓
❑	***Secure Channel: Digitally Sign Secure Channel Data (When Possible)*** **Security Objective:** If this policy is enabled, all outgoing secure channel traffic should be signed. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: By default this option is Enabled. Do not change the default setting.)		✓
❑	***Secure Channel: Require Strong (Windows 2000 or later) Session Key*** **Security Objective:** If this policy is enabled, all outgoing secure channel traffic will require a strong (Windows2000 or later) encryption key. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: By default this option is Disabled. Generally, do not change the default setting. This policy should only be enabled if "all" DCs in a trusted domain support strong keys.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Secure System Partition (For RISC Platforms Only)*** **Security Objective:** If this policy is enabled, only administrative access is allowed to a RISC-based system partition (which must be FAT) while the operating system is running. **Computer Setting: Not Defined** (This policy does not apply to the Evaluated Configuration.)		✓
❑	***Send Unencrypted Password to Connect to Third-Party SMB Servers*** **Security Objective:** If enabled, the SMB redirector is allowed to send clear-text passwords to non-Microsoft SMB servers, which do not support password encryption during authentication. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** (Recommended: By default this option is Disabled. Do not change the default setting.)		✓
❑	***Shut Down System Immediately if Unable to Log Security Audits*** **Security Objective:** Determines whether the system should shut down if it is unable to log security events. **Computer Setting:** ❑ **Enabled** ❑ **Disabled** **Note:** Use this security policy on servers and Domain Controllers only after implementing strict procedures for archiving and clearing the audit logs on a regular basis. (Recommended: Enabled. Requires archiving and clearing the logs on a regular basis.)		✓
❑	***Smart Card Removal Behavior*** **Security Objective:** Determines what should happen when the smart card for a logged-on user is removed from the smart card reader. **Computer Setting:** _____ (Recommended: If using smart cards, set to Lock Workstation. However, the integration of smart card technology is not part of the evaluated configuration.)		✓
❑	***Strengthen Default Permissions for Global System Objects (e.g., Symbolic Links)*** **Security Objective:** If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create. **Computer Setting: Enabled**	✓	
❑	***Unsigned Driver Installation Behavior*** **Security Objective:** Determines what should happen when an attempt is made to install a device driver that has not been certified by the Windows Hardware Quality Lab. **Computer Setting:** _____ (Recommended: Set to Warn but allow installation.)		✓
❑	***Unsigned Non-Driver Installation Behavior*** **Security Objective:** Determines what should happen when an attempt is made to install any nondevice driver software that has not been certified. **Computer Setting:** _____ (Recommended: Set to Warn but allow installation.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
Event Logs			
	Settings for Event Logs		
❑	***Maximum Application Log Size*** **Security Objective:** Specifies the maximum size for the application event log. **Computer Setting: _____ kilobytes** (Recommended: For most environments, the default value of 512 kilobytes is adequate.)		✓
❑	***Maximum Security Log Size*** **Security Objective:** Specifies the maximum size for the security event log. **Computer Setting: _____ kilobytes** (Recommended: A larger log size should be set based on the amount of expected activity, the amount of available disk space, and the frequency with which the logs will be manually reviewed, archived, and cleared.)		✓
❑	***Maximum System Log Size*** **Security Objective:** Specifies the maximum size for the system event log. **Computer Setting: _____ kilobytes** (Recommended: For most environments, the default value of 512 kilobytes is adequate.)		✓
❑	***Restrict Guest Access to Application Log*** **Security Objective:** If enabled, anonymous users are prevented from accessing to the application event log. This policy option is not available in standalone Windows 2000 Professional and Servers. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled.)		✓
❑	***Restrict Guest Access to Security Log*** **Security Objective:** If enabled, anonymous users are prevented from accessing to the security event log. This policy option is not available in standalone Windows 2000 Professional and Servers. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled.)		✓
❑	***Restrict Guest Access to System Log*** **Security Objective:** If enabled, anonymous users are prevented from accessing to the system event log. This policy option is not available in standalone Windows 2000 Professional and Servers. **Computer Setting: ❑ Enabled ❑ Disabled** (Recommended: Enabled.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Retain Application Log*** **Security Objective:** Determines the number of days' worth of events that should be retained for the application log if the retention method for the application log is "By Days." **Computer Setting: _____ days** (Recommended: Do not change the default settings (7 days). Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Retain Security Log*** **Security Objective:** Determines the number of days' worth of events that should be retained for the security log if the retention method for the security log is "By Days." **Computer Setting: _____ days** (Recommended: Do not change the default settings (7 days). Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Retain System Log*** **Security Objective:** Determines the number of days' worth of events that should be retained for the system log if the retention method for the system log is "By Days." **Computer Setting: _____ days** (Recommended: Do not change the default settings (7 days). Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Retention Method for Application Log*** **Security Objective:** Determines the "wrapping" method for the application log. **Computer Setting: _____** (Recommended: Do not change the default settings. Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Retention Method for Security Log*** **Security Objective:** Determines the "wrapping" method for the security log. **Computer Setting: _____** (Recommended: Do not change the default settings. Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Retention Method for System Log*** **Security Objective:** Determines the "wrapping" method for the system log. **Computer Setting: _____** (Recommended: Do not change the default settings. Defaults are "Not Defined" for Domain and Domain Controller Policies and 7 days in Log Properties.)		✓
❑	***Shut Down the Computer When the Security Audit Log is Full*** **Security Objective:** Use Shut down system immediately if unable to log security audits instead of this policy setting. **Computer Setting:** (Recommended: Set as Not Defined.)		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
System Services			
❑	***Evaluated Services*** **Security Objective:** To remain in the Evaluated Configuration it is acceptable to have all of the services listed below enabled and running. ❑ Alerter Service ❑ COM+ Event System ❑ Computer Browser ❑ DHCP Client ❑ DHCP Server ❑ Distributed File System (DFS) ❑ DNS Client ❑ DNS Server ❑ Event Log ❑ File Replication Service ❑ Intersite Messaging ❑ IPSec Policy Agent ❑ Kerberos Key Distribution Center ❑ Logical Disk Manager ❑ Logical Disk Manager Administrative Service ❑ Messenger ❑ Net Logon ❑ Network Connections ❑ NTLM Security Support Provider ❑ Plug and Play ❑ Print Spooler ❑ Protected Storage ❑ Remote Procedure Call (RPC) ❑ Remote Procedure Call (RPC) Locator ❑ Remote Registry Service ❑ Security Accounts Manager ❑ Server ❑ System Event Notification ❑ TCP/IP NetBIOS Helper Service ❑ Windows Internet Name Service (WINS) ❑ Windows Management Instrumentation ❑ Windows Management Instrumentation Driver Extensions ❑ Windows Time ❑ Workstation (Recommended: Do not disable the evaluated services listed. The default settings are appropriate.)	✓	
❑	***Non-Evaluated Services*** **Security Objective:** The default services listed below are not acceptable for the Evaluated Configuration and must be disabled. ❑ Application Management ❑ Automatic Updates ❑ Background Intelligent Transfer Service ❑ Clipbook ❑ Distributed Link Tracking Client ❑ Distributed Link Tracking Server ❑ Distributed Transaction Coordinator ❑ Fax Service ❑ FTP Publishing Service ❑ IIS Admin Service ❑ Indexing Service ❑ Internet Connection Sharing (Supports NAT) ❑ License Logging ❑ NetMeeting Remote Desktop Sharing ❑ Network DDE ❑ Network DDE DSDM ❑ Performance Logs and Alerts ❑ QoS RSVP ❑ Remote Access Auto Connection Manager ❑ Remote Access Connection Manager ❑ Removable Storage ❑ Routing and Remote Access ❑ RunAs Service ❑ Simple Mail Transport Protocol (SMTP) ❑ Smart Card ❑ Smart Card Helper ❑ SNMP Service ❑ SNMP Trap Service ❑ Task Scheduler ❑ Telephony ❑ Telnet ❑ Terminal Services ❑ Uninterruptible Power Supply ❑ Utility Manager ❑ Windows Installer ❑ World Wide Web Publishing Service (Note: Additional services not explicitly listed as Evaluated Services must also be disabled)	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
Registry Permissions				
	HKEY_LOCAL_MACHINE			
❑	❑ \SOFTWARE **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate	❑ \SOFTWARE\classes **Administrators:** Full Control Authenticated Users: Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate	✓	
❑	❑ \SOFTWARE\classes\.hlp **Administrators:** Full Control Authenticated Users: Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate	❑ \SOFTWARE\classes\helpfile **Administrators:** Full Control Authenticated Users: Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate	✓	
❑	❑ \SOFTWARE\Microsoft\OS/2 Subsystem for NT **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **SYSTEM:** Full Control **Inheritance Method:** Propagate	❑ \SOFTWARE\Microsoft\Windows NT \CurrentVersion **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	✓	
❑	❑ \SYSTEM\CurrentControlSet\Control \ComputerName **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	❑ \SYSTEM\currentcontrolset\control \ContentIndex **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
❑	❑ \SYSTEM\CurrentControlSet\Control \Keyboard Layout **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	❑ \SYSTEM\CurrentControlSet\Control \Keyboard Layouts **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	✓	
❑	❑ \SYSTEM\CurrentControlSet\Control \Print\Printers **Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Replace **Note:** Remove inheritance and replace all ACLs.	❑ \SYSTEM\CurrentControlSet\Control \ProductOptions **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	✓	
❑	❑ \SYSTEM\CurrentControlSet\Services \Eventlog **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	❑ \SYSTEM\CurrentControlSet\Services \Tcpip **Authenticated Users:** Read **Inheritance Method:** Propagate **Note:** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	✓	
	HKEY_CLASSES_ROOT			
❑	❑ \HKEY_CLASSES_ROOT **Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate			✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
File System Permissions				
❑	❑ C:\autoexec.bat **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace	❑ C:\boot.ini **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	✓	
❑	❑ C:\config.sys **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace		✓	
❑	❑ C:\ntbootdd.sys **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace **Note:** Used when SCSI is available.	❑ C:\ntdetect.com **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓
❑	❑ C:\ntldr **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %ProgramFiles% **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace		✓
❑	❑ %SystemDirectory% **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	❑ %SystemDirectory%\appmgmt **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDirectory%\config **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDirectory%\dllcache **Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
❑	❑ %SystemDirectory%\DTCLog **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate	❑ %SystemDirectory%\GroupPolicy **Administrators:** Full Control **Authenticated Users:** Read, Execute **SYSTEM:** Full Control **Inheritance Method:** Propagate		✓
❑	❑ %SystemDirectory%\ias **Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDirectory%\Ntbackup.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓
❑	❑ %SystemDirectory%\NTMSData **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Propagate	❑ %SystemDirectory%\rcp.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓
❑	❑ %SystemDirectory%\Regedt32.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDirectory%\repl **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDirectory%\repl\export **Administrators:** Full Control **CREATOR OWNER:** Full Control Replicator: Read, Execute **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate	❑ %SystemDirectory%\repl\import **Administrators:** Full Control Replicator: Modify **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDirectory%\rexec.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDirectory%\rsh.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
❑	❑ %SystemDirectory%\secedit.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDirectory%\Setup **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDirectory%\spool\Printers **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (Folder and Subfolders) **Inheritance Method:** Replace			✓
❑	❑ %SystemDrive% **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate	❑ %SystemDrive%\Documents and Settings **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDrive%\Documents and Settings\Administrator **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemDrive%\Documents and Settings\All Users **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate		✓
❑	❑ %SystemDrive%\Documents and Settings\All Users\Documents\DrWatson **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders) **Inheritance Method:** Replace	❑ %SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\ drwtsn32.log **Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control **Users:** Modify **Inheritance Method:** Replace	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)		Required	Recommended
❑	❑ %SystemDrive%\io.sys **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace	❑ %SystemDrive%\msdos.sys **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace		✓
❑	❑ %SystemDrive%\Temp **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders) **Inheritance Method:** Replace		✓	
❑	❑ %SystemRoot% **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Replace	❑ %SystemRoot%\ $NtServicePackUninstall$ **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓
❑	❑ %SystemRoot%\debug **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute **Inheritance Method:** Propagate	❑ %SystemRoot%\debug\UserMode **Administrators:** Full Control **SYSTEM:** Full Control **Users:** (Folder only) - Traverse folder, List folder, Create files. (Files only) – Create files, create folders **Inheritance Method:** Propagate		✓
❑	❑ %SystemRoot%\regedit.exe **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace	❑ %SystemRoot%\Registration **Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read **Inheritance Method:** Propagate		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	❑ %SystemRoot%\repair **Administrators:** Full Control **SYSTEM:** Full Control **Inheritance Method:** Replace		✓
❑	❑ %SystemRoot%\ Temp **Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders) **Inheritance Method:** Replace	✓	
Additional Registry Settings (Values are shown in decimal, unless otherwise noted)			
❑	***Disable DirectDraw*** **HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers** — **Format:** — **Value:** **Key:** DCI **Value Name:** Timeout — REG_DWORD — 0	✓	
❑	***Disable Unnecessary Devices*** **HKLM\SYSTEM\CurrentControlSet\Services** — **Format:** — **Value:** **Key:** audstub **Value Name:** Start — REG_DWORD — 4 **Key:** mnmdd **Value Name:** Start — REG_DWORD — 4 **Key:** ndistapi **Value Name:** Start — REG_DWORD — 4 **Key:** ndiswan **Value Name:** Start — REG_DWORD — 4 **Key:** ndproxy **Value Name:** Start — REG_DWORD — 4 **Key:** parvdm **Value Name:** Start — REG_DWORD — 4 **Key:** pptpminiport **Value Name:** Start — REG_DWORD — 4 **Key:** ptilink **Value Name:** Start — REG_DWORD — 4 **Key:** rasacd **Value Name:** Start — REG_DWORD — 4 **Key:** rasl2tp **Value Name:** Start — REG_DWORD — 4 **Key:** raspti **Value Name:** Start — REG_DWORD — 4 **Key:** wanarp **Value Name:** Start — REG_DWORD — 4	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Remove OS/2 and POSIX Subsystems*** **HKLM\SYSTEM\CurrentControlSet\Control\ Session Manager** / **Format** / **Value** **Key:** SubSystems **Value Name:** Optional / REG_MULTI_SZ / Delete the values	✓	
❑	***Protect kernel Object Attributes*** **HKLM\SYSTEM\CurrentControlSet\Control** / **Format** / **Value** **Key:** Session Manager **Value Name:** EnhancedSecurityLevel / REG_DWORD / 1	✓	
❑	***Restrict Null Session Access*** **HKLM\SYSTEM\ CurrentControlSet\Services\LanmanServer** / **Format** / **Value** **Key:** parameters **Value Name:** RestrictNullSessAccess / REG_DWORD / 1	✓	
❑	***Restrict Null Session Access Over Named Pipes*** **HKLM\SYSTEM\CurrentControlSet\Services\ LanmanServer** / **Format** / **Value** **Key:** parameters Value Names: NullSessionPipes NullSessionShares / REG_MULTI_SZ / Delete all values	✓	
❑	***Prevent Interference of the Session Lock from Application Generated Input*** **HKCU\Software\Policies\Microsoft\Windows\ Control Panel** / **Format** / **Value** **Key:** Desktop **Value Name:** BlockSendInputResets / REG_SZ / 1 **Note:** It is important to note that the appropriate screen saver settings must be set in conjunction with this key for the feature to make sense. The necessary screen saver settings are: • A selected screen saver • Password protection • A screen saver timeout period If the screensaver is not properly configured this feature will essentially have no effect on the machines overall security.	✓	

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended

Generate an Audit Event when the Audit Log Reaches a Percent Full Threshold

HKLM\SYSTEM\CurrentControlSet\Services\ Eventlog	Format	Value
Key: Security **Value Name:** WarningLevel	REG_DWORD	90

(The value may be edited to conform to local requirements.)

❑ Required: ✓

Harden the TCP/IP Stack Against Denial of Service Attacks

HKLM\SYSTEM\CurrentControlSet\Services\ Tcpip	Format	Value
Key: Parameters **Value Name:** DisableIPSourceRouting	REG_DWORD	2
Key: Parameters **Value Name:** EnableDeadGWDetect	REG_DWORD	0
Key: Parameters **Value Name:** EnableICMPRedirect	REG_DWORD	0
Key: Parameters **Value Name:** EnablePMTUDiscovery	REG_DWORD	0
Key: Parameters **Value Name:** EnableSecurityFilters	REG_DWORD	1
Key: Parameters **Value Name:** KeepAliveTime	REG_DWORD	300,000
Key: Parameters **Value Name:** PerformRouterDiscovery	REG_DWORD	0
Key: Parameters **Value Name:** SynAttackProtect	REG_DWORD	2
Key: Parameters **Value Name:** TcpMaxConnectResponseRetransmissions	REG_DWORD	2
Key: Parameters **Value Name:** TcpMaxConnectRetransmissions	REG_DWORD	3
Key: Parameters **Value Name:** TCPMaxPortsExhausted	REG_DWORD	5

HKLM\SYSTEM\CurrentControlSet\Services\ NetBT	Format	Value
Key: Parameters **Value Name:** NoNameReleaseOnDemand	REG_DWORD	1

❑ Recommended: ✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Make Screensaver Password Protection Immediate*** **HKLM\Software\Microsoft\Windows NT\CurrentVersion** / **Format** / **Value** **Key:** Winlogon / REG_SZ / 0 **Value Name:** ScreenSaverGracePeriod		✓
❑	***Disable LMHash Creation*** **HKLM\SYSTEM\CurrentControlSet\Control\Lsa** / **Format** / **Value** **Key:** NoLMHash -- You need to create this key / N/A / N/A **Value Name:** It is not necessary to have a value		✓
❑	***Disable Autorun*** **HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies** / **Format** / **Value** **Key:** Explorer / REG_DWORD / 255 **Value Name:** NoDriveTypeAutoRun		✓
❑	***Generate Administrative Alert when the Audit Log is Full*** **HKLM\SYSTEM\CurrentControlSet\Services\ Alerter** / **Format** / **Value** **Key:** Parameters / REG_MULTI_SZ / (Enter the name(s) of accounts to receive alerts) **Value Name:** AlertNames **Note:** Administrative alerts rely on both the Alerter and Messenger services. Make sure that the Alerter service is running on the source computer and that the Messenger service is running on the recipient computer.		✓
❑	***LDAP Server handling of LDAP BIND command requests*** **HKLM\System\CurrentControlSet\Services\ NTDS** / **Format** / **Value** **Key:** Parameters / REG_DWORD / 2 **Value Name:** LdapServerIntegrity		✓
Additional Recommendations			
❑	***Back up the Administrator's Encryption Certificate*** If applicable, backup the Administrator's encryption certificate and store in a secured location.		✓

Completed and Verified	WINDOWS 20000 Security Configuration Checklist (Settings apply to all operating system versions except where otherwise noted)	Required	Recommended
❑	***Enable Automatic Screen Lock Protection*** Set a password-protected screensaver. A recommended timeout period is 15 minutes.		✓
❑	***Update the System Emergency Repair Disk*** Update the system's ERD to reflect the changes made.		✓

Appendix F
Windows 2000 Security Configuration Templates for the Evaluated Configuration

G-1. Baseline Windows 2000 Server Security Configuration Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        CC_Baseline_W2K_Server.inf
; Template Version:     1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000  -         Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1


[System Access]
;-----------------------------------------------------------------------------
;Account Policies - Password Policy.
;-----------------------------------------------------------------------------
MinimumPasswordLength = 8
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-----------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-----------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
;ResetLockoutCount = 30
;LockoutDuration = -1

;-----------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-----------------------------------------------------------------------------
[Kerberos Policy]
TicketValidateClient = 1


;-----------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-----------------------------------------------------------------------------
;Note: There are no audit policy settings specified in the baseline policies.

;-----------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
```



```
;---------------------------------------------------------------------------
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544
SeInteractiveLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-32-544

;---------------------------------------------------------------------------
;Local Policies - Security Options.
;---------------------------------------------------------------------------
;---------------------------------------------------------------------------
;Registry Values.
;---------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1


;===========================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;===========================================================================

;---------------------------------------------------------------------------
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;---------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
```



```
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;-------------------------------------------------------------------------
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;-------------------------------------------------------------------------
;Protect kernel object attributes.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;-------------------------------------------------------------------------
;Restrict Nuss Session Access.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;-------------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  These edits delete the default
;values.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""

;-------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90


;-------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)
```


;Note: There are no event log settings specified in the baseline policies.

;---
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;---
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CC
LCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCS
WRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;
CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRR
C;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;SO)"

SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---
;Registry Key Permissions.
;---
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"

"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDC
LCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)
(A;CI;KA;;;SY)(A;CI;KR;;;BU)"

;---
;File and Folder Permissions.
;---
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;C
I;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"

;---
;Edit default group memberships.
;---
[Group Membership]
;---
;Remove accounts from the Guests group. These settings will not appear in the
;security policy interface.
;---
%SceInfGuests%__Members =

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator

SceInfServerOp = Server Operators
SceInfUsers = Users

[Profile Description]
Description=Evaluated Configuration minimum required security policy settings for Windows 2000 Servers.

G-2. Baseline Windows 2000 Professional Security Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        CC_Baseline_W2K_Professional.inf
; Template Version:     1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordLength = 8
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
;ResetLockoutCount = 30
;LockoutDuration = -1

;-------------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-------------------------------------------------------------------------------
[Kerberos Policy]
TicketValidateClient = 1


;-------------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-------------------------------------------------------------------------------
;Note: There are no audit policy settings specified in the baseline policies.

;-------------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
```



```
;---------------------------------------------------------------------------
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeShutdownPrivilege = *S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544

;---------------------------------------------------------------------------
;Local Policies - Security Options.
;---------------------------------------------------------------------------
;---------------------------------------------------------------------------
;Registry Values.
;---------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
;---------------------------------------------------------------------------
;The following Registry value requires a user to log on to the WIndows 2000
;Professional computer before allowing a shutdown.  It is the default on servers.
;---------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1


;===========================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;===========================================================================

;---------------------------------------------------------------------------
```



```
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;-----------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;-----------------------------------------------------------------------------
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;-----------------------------------------------------------------------------
;Protect kernel object attributes.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;-----------------------------------------------------------------------------
;Restrict Nuss Session Access.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;-----------------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  This edit deletes the default
;values.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""

;-----------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-----------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90
```



```
;-------------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

;Note: There are no event log settings specified in the baseline policies.


;-------------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CC
LCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCS
WRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;
CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
```


IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)"
SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---
;Registry Key Permissions.
;---
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"


```
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;
;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDC
LCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)
(A;CI;KA;;;SY)(A;CI;KR;;;BU)"


;---------------------------------------------------------------------------
;File and Folder Permissions.
;---------------------------------------------------------------------------
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;C
I;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"


;---------------------------------------------------------------------------
;Edit default group memberships.
;---------------------------------------------------------------------------
[Group Membership]
;---------------------------------------------------------------------------
;Remove accounts from the Guests group.  These settings will not appear in the
;security policy interface.
;---------------------------------------------------------------------------
%SceInfGuests%__Members =


[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
```


SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[Profile Description]
Description=Evaluated Configuration minimum required security policy settings for Windows 2000 Professional computers.

G-3. Baseline Windows 2000 Domain Security Policy Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       CC_Baseline_W2K_Domain.inf
; Template Version:    1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[Version]
signature="$CHICAGO$"
Revision=1


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordLength = 8
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
;ResetLockoutCount = 30
;LockoutDuration = -1

;-------------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-------------------------------------------------------------------------------
[Kerberos Policy]
MaxClockSkew = 5
TicketValidateClient = 1


;-------------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-------------------------------------------------------------------------------
;Note: There are no audit policy settings specified in the baseline policies.

;-------------------------------------------------------------------------------
```



```
;Local Policies - User Rights Assignment.
;---------------------------------------------------------------------------
;Note: This policy enforces the default Administrator rights on certain
;privileges across the Domain so that they may not be changed.

[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeShutdownPrivilege = *S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeTakeOwnershipPrivilege = *S-1-5-32-544

;---------------------------------------------------------------------------
;Local Policies - Security Options.
;---------------------------------------------------------------------------
;---------------------------------------------------------------------------
;Registry Values.
;---------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
;---------------------------------------------------------------------------
;The following Registry value requires a Domain user to log on to the computer
;before allowing a shutdown.  It is the default on servers.
;---------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
=4,0

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
```



```
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

;===========================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;===========================================================================

;---------------------------------------------------------------------------
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;---------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;---------------------------------------------------------------------------
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;---------------------------------------------------------------------------
;Protect kernel object attributes.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;---------------------------------------------------------------------------
;Restrict Nuss Session Access.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;---------------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  This edit deletes the default
;values.
;---------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""
```



```
;-------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90


;-------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

;Note: There are no event log settings specified in the baseline policies.


;-------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CC
LCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCS
WRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
```


Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)"
SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"


```
;-------------------------------------------------------------------------
;Registry Key Permissions.
;-------------------------------------------------------------------------
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWR
PSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;
;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDC
LCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)
(A;CI;KA;;;SY)(A;CI;KR;;;BU)"


;-------------------------------------------------------------------------
;File and Folder Permissions.
;-------------------------------------------------------------------------
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;C
I;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"


;-------------------------------------------------------------------------
;Edit default group memberships.
;-------------------------------------------------------------------------
[Group Membership]
;-------------------------------------------------------------------------
;Remove accounts from the Guests group.  These settings will appear in the
;Restricted Groups Policy within the Domain Security Policy MMC.
```



```
;-------------------------------------------------------------------------------
%SceInfGuests%__Members =

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users


[Profile Description]
Description=Evaluated Configuration minimum required security policy settings for Windows 2000
Domains.
```


G-4. Baseline Windows 2000 Domain Controller Security Policy Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       CC_Baseline_W2K_DC.inf
; Template Version:    1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1


[System Access]
RequireLogonToChangePassword = 0


;---------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;---------------------------------------------------------------------------
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11
SeInteractiveLogonRight = *S-1-5-32-548,*S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-550,*S-1-5-32-
549
SeMachineAccountPrivilege =
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-1-0,*S-1-5-11,*S-1-5-32-544
SeSystemtimePrivilege = *S-1-5-32-549,*S-1-5-32-544
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeBatchLogonRight =
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeCreateTokenPrivilege =
SeCreatePermanentPrivilege =
SeDenyNetworkLogonRight =
SeDenyBatchLogonRight =
SeDenyServiceLogonRight =
```



```
SeDenyInteractiveLogonRight =
SeAuditPrivilege =
SeTcbPrivilege =
SeLockMemoryPrivilege =
SeServiceLogonRight =
SeAssignPrimaryTokenPrivilege =
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-550,*S-1-5-32-551,*S-1-5-32-544,*S-1-5-32-548
SeSyncAgentPrivilege =
SeTakeOwnershipPrivilege = *S-1-5-32-544

;-------------------------------------------------------------------------
;Local Policies - Security Options.
;-------------------------------------------------------------------------
;-------------------------------------------------------------------------
;Registry Values.
;-------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                    ( 1 )
; REG_EXPAND_SZ             ( 2 )  // with environment variables to expand
; REG_BINARY                ( 3 )
; REG_DWORD                 ( 4 )
; REG_MULTI_SZ              ( 7 )
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1


;-------------------------------------------------------------------------
;Registry Key Permissions.  Cleans out Power Users references from the Domain
;Controller that were inserted by an Evaluated Configuration Domain Security
;Policy.
;-------------------------------------------------------------------------
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;
KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;
;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;S
Y)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"


[Profile Description]
```


Description=Evaluated Configuration required security policy (delta) settings for Windows 2000 Domain Controllers.

G-5. High Security Windows 2000 Server Security Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        CC_HiSec_W2K_Server.inf
; Template Version:     1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1

[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  Rename
Administrator and
;Guest accounts.  This policy setting actually appears in the Security Options
;category of the policy interface.  To set this policy via this template,
;uncomment the pertinent lines below and set an appropriate name in place of the
;sample name shown.  Otherwise, the policy may be edited using the appropriate
;Security Policy interface.  Do not use the names shown below as they are only
;sample placeholders.
;-------------------------------------------------------------------------------
;NewAdministratorName = "NewAdminName"
;NewGuestName = "NewGuestName"

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
;ResetLockoutCount = 30
```



```
;LockoutDuration = -1

;-----------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-----------------------------------------------------------------------------
[Kerberos Policy]
TicketValidateClient = 1


;-----------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-----------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 1
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 3
AuditAccountLogon = 3

;-----------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-----------------------------------------------------------------------------

[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544
SeInteractiveLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-32-544

;-----------------------------------------------------------------------------
;Local Policies - Security Options.
;-----------------------------------------------------------------------------
;-----------------------------------------------------------------------------
;Registry Values.
;-----------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
```



```
;-------------------------------------------------------------------------
;NOTICE:  The warning baner title and message shown below are temporary
;placeholders.  The warning banner title and message must be edited to comply
;with local organizational policies and legal requirements.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,This
message is a placeholder!  The local system administrator and security manager must define the
appropriate login warning message, in accordance with local organizational policies, that will
appear here when a user attempts to log in.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,Pl
aceholder for warning banner title.

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserNa
me=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4
,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainText
Password=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=
4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
;-------------------------------------------------------------------------
;The following Registry value will shut down the system immediately if it is
;unable to log security audits.  While it is a recommended setting, it should
;only be enabled where there is a strict audit management process in place for
;reviewing, archiving, and clearing the audit log on a regular basis.
;-------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1

;-------------------------------------------------------------------------
;The following Registry values for auditing access of global system objects and
;backup and restore privileges will generate a large amount of audit events.
;While they are recommended settings, they should only be enabled where there is
;a strict audit management process in place for reviewing, archiving, and
```



```
;clearing the audit log on a regular basis.  The maximum log size should also be
;edited to support an increase in events being logged.
;-----------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,1
;MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1


;=======================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;=======================================================================

;-----------------------------------------------------------------------
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;-----------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;-----------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;-----------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;-----------------------------------------------------------------------
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;-----------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;-----------------------------------------------------------------------
;Protect kernel object attributes.
;-----------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;-----------------------------------------------------------------------
;Restrict Nuss Session Access.
;-----------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;-----------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  This edit deletes the default
;values.
```



```
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""

;-------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90


;=========================================================================
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  The additional
Registry
;Value Settings listed below are recommended for added security in the Common
;Criteria Evaluated Configuration. These settings will not appear in the security
;policy interface.
;=========================================================================

;-------------------------------------------------------------------------
;Harden the TCP/IP stack against denial of service attacks. The following Registry
;TCP/IP-related values help to increase the resistance of the TCP/IP Stack in
;Windows 2000 against denial of service network attacks.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnablePMTUDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableSecurityFilters=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\NetBT\parameters\NoNameReleaseOnDemand=
4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\SynAttackProtect=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectResponseRetr
ansmissions=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectRetransmission
s=4,3
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TCPMaxPortsExhausted=4,5

;-------------------------------------------------------------------------
;Make screensaver password protection immediate.  Sets the value of this key
;entry to 0 in order to make password protection effective immediately.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=1,0

;-------------------------------------------------------------------------
;Disable LMHash creation. The LM hash is relatively weak compared to the NTLM
;hash and therefore prone to rapid brute force attack.  For the Evaluated
;Configuration LM authentication is not required and can therefore be disabled
;to ensure greater security. The string "bar" is a dummy value name for creating
;the key "NoLMHash" automatically.
```



```
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash\bar=4,0

;-------------------------------------------------------------------------
;Disable autorun. Disables autorun capabilities on all drives.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255

;-------------------------------------------------------------------------
;Generate administrative alerts when audit log is full.  Edit this key as
;necessary to specify an appropriate authorized administrative account(s) to
;receive the administrative alerts.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Alerter\Parameters\AlertNames=7,Administrators


;-------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1


;-------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```


NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)"
SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---
;Registry Key Permissions.
;---
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"

;---
;File and Folder Permissions.
;---
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"

"%SystemDrive%\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\Administrator",2,"D:PAR(A;OICI;FA;;;LA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%Systemdirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemroot%\regedit.exe",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%Systemdirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1000ae;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;CO)(A;OICI;0x1300a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1201a9;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OIIO;0x100006;;;BU)(A;;0x100023;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

;---
;Edit default group memberships.
;---
[Group Membership]
;---
;Remove accounts from the Guests group. These settings will not appear in the
;security policy interface.
;---
%SceInfGuests%__Members =

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[Profile Description]
Description=Evaluated Configuration high security policy settings for Windows 2000 Servers.

G-6. High Security Windows 2000 Professional Security Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        CC_HiSec_W2K_Professional.inf
; Template Version:     1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000  -         Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  Rename
Administrator and
;Guest accounts.  This policy setting actually appears in the Security Options
;category of the policy interface.  To set this policy via this template,
;uncomment the pertinent lines below and set an appropriate name in place of the
;sample name shown.  Otherwise, the policy may be edited using the appropriate
;Security Policy interface.  Do not use the names shown below as they are only
;sample placeholders.
;-------------------------------------------------------------------------------
;NewAdministratorName = "NewAdminName"
;NewGuestName = "NewGuestName"

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
```



```
;ResetLockoutCount = 30
;LockoutDuration = -1

;-------------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-------------------------------------------------------------------------------
[Kerberos Policy]
TicketValidateClient = 1


;-------------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-------------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 1
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 3
AuditAccountLogon = 3

;-------------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-------------------------------------------------------------------------------
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544
SeInteractiveLogonRight = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544

;-------------------------------------------------------------------------------
;Local Policies - Security Options.
;-------------------------------------------------------------------------------
;-------------------------------------------------------------------------------
;Registry Values.
;-------------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
```



```
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
;-------------------------------------------------------------------------
;The following Registry value requires a user to log on to the WIndows 2000
;Professional computer before allowing a shutdown.  It is the default on servers.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
=4,0

;-------------------------------------------------------------------------
;NOTICE:  The warning baner title and message shown below are temporary
;placeholders.  The warning banner title and message must be edited to comply
;with local organizational policies and legal requirements.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,This
message is a placeholder!  The local system administrator and security manager must define the
appropriate login warning message, in accordance with local organizational policies, that will
appear here when a user attempts to log in.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,Pl
aceholder for warning banner title.

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserNa
me=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4
,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainText
Password=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=
4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
;-------------------------------------------------------------------------
;The following Registry value will shut down the system immediately if it is
;unable to log security audits.  While it is a recommended setting, it should
;only be enabled where there is a strict audit management process in place for
;reviewing, archiving, and clearing the audit log on a regular basis.
```



```
;-------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1

;-------------------------------------------------------------------------
;The following Registry values for auditing access of global system objects and
;backup and restore privileges will generate a large amount of audit events.
;While they are recommended settings, they should only be enabled where there is
;a strict audit management process in place for reviewing, archiving, and
;clearing the audit log on a regular basis.  The maximum log size should also be
;edited to support an increase in events being logged.
;-------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,1
;MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1


;=========================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;=========================================================================

;-------------------------------------------------------------------------
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;-------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;-------------------------------------------------------------------------
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;-------------------------------------------------------------------------
;Protect kernel object attributes.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;-------------------------------------------------------------------------
```



```
;Restrict Nuss Session Access.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;-------------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  This edit deletes the default
;values.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""

;-------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90


;=========================================================================
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  The additional
Registry
;Value Settings listed below are recommended for added security in the Common
;Criteria Evaluated Configuration. These settings will not appear in the security
;policy interface.
;=========================================================================

;-------------------------------------------------------------------------
;Harden the TCP/IP stack against denial of service attacks. The following Registry
;TCP/IP-related values help to increase the resistance of the TCP/IP Stack in
;Windows 2000 against denial of service network attacks.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnablePMTUDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableSecurityFilters=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\NetBT\parameters\NoNameReleaseOnDemand=
4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\SynAttackProtect=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectResponseRetr
ansmissions=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectRetransmission
s=4,3
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TCPMaxPortsExhausted=4,5

;-------------------------------------------------------------------------
;Make screensaver password protection immediate.  Sets the value of this key
;entry to 0 in order to make password protection effective immediately.
;-------------------------------------------------------------------------
```



```
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=1,0

;-------------------------------------------------------------------------------
;Disable LMHash creation. The LM hash is relatively weak compared to the NTLM
;hash and therefore prone to rapid brute force attack.  For the Evaluated
;Configuration LM authentication is not required and can therefore be disabled
;to ensure greater security. The string "bar" is a dummy value name for creating
;the key "NoLMHash" automatically.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash\bar=4,0

;-------------------------------------------------------------------------------
;Disable autorun. Disables autorun capabilities on all drives.
;-------------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255

;-------------------------------------------------------------------------------
;Generate administrative alerts when audit log is full.  Edit this key as
;necessary to specify an appropriate authorized administrative account(s) to
;receive the administrative alerts.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Alerter\Parameters\AlertNames=7,Administrators


;-------------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1


;-------------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```


seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CC
LCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCS
WRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;
CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRR
C;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;SO)"
SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;
CCLCSWRPWPDTLOCRRC;;;SY)"

RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---
;Registry Key Permissions.
;---
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"


```
;-------------------------------------------------------------------------
;File and Folder Permissions.
;-------------------------------------------------------------------------
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;B
U)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;C
I;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;LA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and
Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x120
0a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;
0x1200a9;;;BU)"
"%Systemdirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemroot%\regedit.exe",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%Systemdirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;S
Y)(A;CI;0x1000ae;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;C
O)(A;OICI;0x1300a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;
SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;
;;SY)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;CO)
(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
```


"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1201a9;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OIIO;0x100006;;;BU)(A;;0x100023;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

;---
;Edit default group memberships.
;---
[Group Membership]
;---
;Remove accounts from the Guests group. These settings will not appear in the
;security policy interface.
;---
%SceInfGuests%__Members =

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[Profile Description]
Description=Evaluated Configuration high security policy settings for Windows 2000 Professional computers.

G-7. High Security Windows 2000 Domain Security Policy Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       CC_HiSec_W2K_Domain.inf
; Template Version:    1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[Version]
signature="$CHICAGO$"
Revision=1


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
RequireLogonToChangePassword = 0
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  Rename
Administrator and
;Guest accounts.  This policy setting actually appears in the Security Options
;category of the policy interface.  To set this policy via this template,
;uncomment the pertinent lines below and set an appropriate name in place of the
;sample name shown.  Otherwise, the policy may be edited using the appropriate
;Security Policy interface.  Do not use the names shown below as they are only
;sample placeholders.
;-------------------------------------------------------------------------------
;NewAdministratorName = "NewAdminName"
;NewGuestName = "NewGuestName"

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1

;Note: The following are not configured when No Account Lockout
```



```
;ResetLockoutCount = 30
;LockoutDuration = -1

;-----------------------------------------------------------------------------
;Account Policies - Kerberos Policy.
;-----------------------------------------------------------------------------
[Kerberos Policy]
MaxClockSkew = 5
TicketValidateClient = 1


;-----------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-----------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 1
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 3
AuditAccountLogon = 3

;-----------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-----------------------------------------------------------------------------
;Note: This policy enforces the default Administrator rights on certain
;privileges across the Domain so that they may not be changed.

[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeInteractiveLogonRight = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
SeShutdownPrivilege = *S-1-5-32-547,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeTakeOwnershipPrivilege = *S-1-5-32-544

;-----------------------------------------------------------------------------
;Local Policies - Security Options.
;-----------------------------------------------------------------------------
;-----------------------------------------------------------------------------
;Registry Values.
;-----------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )
```



```
[Registry Values]
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1
;-------------------------------------------------------------------------------
;The following Registry value will shut down the system immediately if it is
;unable to log security audits.  While it is a recommended setting, it should
;only be enabled where there is a strict audit management process in place for
;reviewing, archiving, and clearing the audit log on a regular basis.
;-------------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,5
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=
4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainText
Password=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4
,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserNa
me=4,1
;-------------------------------------------------------------------------------
;NOTICE:  The warning baner title and message shown below are temporary
;placeholders.  The warning banner title and message must be edited to comply
;with local organizational policies and legal requirements.
;-------------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,Pl
aceholder for warning banner title.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=1,This
message is a placeholder!  The local system administrator and security manager must define the
appropriate login warning message, in accordance with local organizational policies, that will
appear here when a user attempts to log in.

;-------------------------------------------------------------------------------
;The following Registry value requires a Domain user to log on to the computer
;before allowing a shutdown.  It is the default on servers.
;-------------------------------------------------------------------------------
```



```
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon
=4,0

;-------------------------------------------------------------------------
;The following Registry values for auditing access of global system objects and
;backup and restore privileges will generate a large amount of audit events.
;While they are recommended settings, they should only be enabled where there is
;a strict audit management process in place for reviewing, archiving, and
;clearing the audit log on a regular basis.  The maximum log size should also be
;edited to support an increase in events being logged.
;-------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,1
;MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1

MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1

;=========================================================================
;EVALUATED CONFIGURATION REQUIRED SECURITY SETTINGS.  The additional Registry
;Value Settings listed below are required in the Common Criteria Evaluated
;Configuration. These settings will not appear in the security policy interface.
;=========================================================================

;-------------------------------------------------------------------------
;Disable DirectDraw.  This edit disables DirectDraw in order to prevent direct
;access to the graphics hardware by the application.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;-------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4

;-------------------------------------------------------------------------
```



```
;Remove OS/2 and POSIX subsystems.  This edit deletes the OS/2 and POSIX default
;values.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Optional=7,""

;-----------------------------------------------------------------------------
;Protect kernel object attributes.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1

;-----------------------------------------------------------------------------
;Restrict Nuss Session Access.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\RestrictNullSessAccess
=4,1

;-----------------------------------------------------------------------------
;Restrict Nuss Session Access over named pipes.  This edit deletes the default
;values.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes=7,""
MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\NullSessionShares=7,""

;-----------------------------------------------------------------------------
;SP3 Edit.  Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not addequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-----------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90


;=============================================================================
;EVALUATED CONFIGURATION RECOMMENDED SECURITY SETTINGS.  The additional
Registry
;Value Settings listed below are recommended for added security in the Common
;Criteria Evaluated Configuration. These settings will not appear in the security
;policy interface.
;=============================================================================

;-----------------------------------------------------------------------------
;Harden the TCP/IP stack against denial of service attacks. The following Registry
;TCP/IP-related values help to increase the resistance of the TCP/IP Stack in
;Windows 2000 against denial of service network attacks.
;-----------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnablePMTUDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\EnableSecurityFilters=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\NetBT\parameters\NoNameReleaseOnDemand=
4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\SynAttackProtect=4,2
```



```
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectResponseRetr
ansmissions=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TcpMaxConnectRetransmission
s=4,3
MACHINE\System\CurrentControlSet\Services\Tcpip\parameters\TCPMaxPortsExhausted=4,5

;-------------------------------------------------------------------------
;Make screensaver password protection immediate.  Sets the value of this key
;entry to 0 in order to make password protection effective immediately.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=1,0

;-------------------------------------------------------------------------
;Disable LMHash creation. The LM hash is relatively weak compared to the NTLM
;hash and therefore prone to rapid brute force attack.  For the Evaluated
;Configuration LM authentication is not required and can therefore be disabled
;to ensure greater security. The string "bar" is a dummy value name for creating
;the key "NoLMHash" automatically.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash\bar=4,0

;-------------------------------------------------------------------------
;Disable autorun. Disables autorun capabilities on all drives.
;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255

;-------------------------------------------------------------------------
;Generate administrative alerts when audit log is full.  Edit this key as
;necessary to specify an appropriate authorized administrative account(s) to
;receive the administrative alerts.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Alerter\Parameters\AlertNames=7,Administrators


;-------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 2
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1
```



```
;-------------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
seclogon,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Schedule,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSW
RPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWD
WO;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:(A;OICI;CCLCSWLORC;;;WD)(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO
;;;BA)(A;OICI;CCLCSWLORC;;;PU)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWRPLO;;;BU)S:(
AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
MSDTC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWP
DTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWR
PWPDTLOCRRC;;;SY)(A;;RP;;;WD)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
LicenseService,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCS
WRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CC
LCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCS
WRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;RPWPDTRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;
CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;DCRPWPDTRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
IISADMIN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRR
C;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;SO)"
SysmonLog,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;
;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
```



```
RSVP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
NtmsSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;
CCLCSWRPWPDTLOCRRC;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRR
C;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SCardSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)"
SCardDrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;A
U)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;
;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOC
RRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLC
SWRPWPDTLOCRRC;;;BU)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(
A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UPS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;
;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;
;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;C
CLCSWRPWPDTLOCRRC;;;SY)"
MSIServer,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;
AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
W3SVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU
)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"


;-------------------------------------------------------------------------
;Registry Key Permissions.
;-------------------------------------------------------------------------
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWR
PSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;
;AU)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout",0,"D:AR(A;CI;KR;;;AU)"
"MACHINE\Software\Microsoft\Windows NT\CurrentVersion",0,"D:AR(A;CI;KR;;;AU)"
```


"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;CCDCLCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;CCDC
LCSWRPSDRC;;;PU)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;CCDCLCSWRPSDRC;;;PU)
(A;CI;KA;;;SY)(A;CI;KR;;;BU)"

;---
;File and Folder Permissions.
;---
[File Security]
"%SystemDrive%\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%SystemDrive%\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x1
00026;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;B
U)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;C
I;0x100026;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;LA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and
Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x120
0a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;
0x1200a9;;;BU)"
"%Systemdirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemroot%\regedit.exe",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%Systemdirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%Systemdirectory%\ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;S
Y)(A;CI;0x1000ae;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;C
O)(A;OICI;0x1300a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1201a9;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OIIO;0x100006;;;BU)(A;;0x100023;;;BU)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

;---
;Edit default group memberships.
;---
[Group Membership]
;---
;Remove accounts from the Guests group. These settings will not appear in the
;security policy interface.
;---
%SceInfGuests%__Members =

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[Profile Description]

Description=Evaluated Configuration high security policy settings for Windows 2000 Domains.

G-8. High Security Windows 2000 Domain Controller Security Policy Template

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:       CC_HiSec_W2K_DC.inf
; Template Version:    1.0
;
;This Security Configuration Template provides settings to support the
;Evaluated Configuration of Windows 2000 under the Common Criteria (CC) for
;Information Technology Security Evaluation.
;
; Revision History
; 0000   -          Original September 17, 2002


[version]
signature="$CHICAGO$"
Revision=1


[System Access]
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1

;-----------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-----------------------------------------------------------------------------
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11
SeInteractiveLogonRight = *S-1-5-32-548,*S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-550,*S-1-5-32-
549
SeMachineAccountPrivilege =
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-1-0,*S-1-5-11,*S-1-5-32-544
SeSystemtimePrivilege = *S-1-5-32-549,*S-1-5-32-544
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-544
SeBatchLogonRight =
SeSecurityPrivilege = *S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeCreateTokenPrivilege =
SeCreatePermanentPrivilege =
SeDenyNetworkLogonRight =
SeDenyBatchLogonRight =
```



```
SeDenyServiceLogonRight =
SeDenyInteractiveLogonRight =
SeAuditPrivilege =
SeTcbPrivilege =
SeLockMemoryPrivilege =
SeServiceLogonRight =
SeAssignPrimaryTokenPrivilege =
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-550,*S-1-5-32-551,*S-1-5-32-544,*S-1-5-32-548
SeSyncAgentPrivilege =
SeTakeOwnershipPrivilege = *S-1-5-32-544

;-------------------------------------------------------------------------
;Local Policies - Security Options.
;-------------------------------------------------------------------------
;-------------------------------------------------------------------------
;Registry Values.
;-------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                  ( 1 )
; REG_EXPAND_SZ           ( 2 )  // with environment variables to expand
; REG_BINARY              ( 3 )
; REG_DWORD               ( 4 )
; REG_MULTI_SZ            ( 7 )
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LdapServerIntegrity=4,2
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignat
ure=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignat
ure=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySi
gnature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecurity
Signature=4,0


;-------------------------------------------------------------------------
;Registry Key Permissions.  Cleans out Power Users references from the Domain
;Controller that are inserted by an Evaluated Configuration Domain Security
;Policy.
;-------------------------------------------------------------------------
[Registry Keys]
"CLASSES_ROOT",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;
KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;
;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\.hlp",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A
;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Classes\helpfile",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;C
O)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\Software\Classes",0,"D:AR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CIIO;KA;;;CO)(A;CI;KA;;;S
Y)(A;CI;KR;;;BU)"
"MACHINE\Software",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
```


[Profile Description]
Description=Evaluated Configuration high security policy (delta) settings for Windows 2000 Domain Controllers.

