Windows Server 2003 with SP2 Security Configuration Guide

Version 3.0

July 19, 2007

Prepared For:

Microsoft Corporation
Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Windows Server 2003 with SP2 Security Configuration Guide

Version 3.0, 07/19/2007

1. Introduction

Welcome to the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*. This document provides guidance to allow for the secure installation and configuration of Windows Server 2003 with Service Pack 2 (SP2) in accordance with the *Microsoft Windows 2003, XP Professional and XP Embedded Security Target*.

The *Microsoft Windows 2003, XP Professional and XP Embedded Security Target*, defines the requirements for Version 3.0 of the Windows Server 2003 with SP2 and XP Professional with SP2 Common Criteria Evaluation and is henceforth referred to as the Windows 2003/XP V3 ST. The Windows 2003/XP V3 ST provides a set of security requirements taken from the Common Criteria (CC) for Information Technology Security Evaluation. The Window Server 2003 products were evaluated against the Windows 2003/XP V3 ST and found to satisfy the security target requirements.

This document is targeted at those responsible for ensuring that the installation and configuration process results in a secure configuration. For the purposes of this document, a secure configuration, henceforth referred to as the Evaluated Configuration, is one that enforces the requirements presented in the Windows 2003/XP V3 ST.

> **Note:** The required configuration settings specified by this document are used explicitly to achieve the Evaluated Configuration. Microsoft also produces the *Windows Server 2003 Security Guide* (http://go.microsoft.com/fwlink/?LinkId=14845) and the "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP" guide (http://go.microsoft.com/fwlink/?LinkId=15159), which can be used to determine the recommended settings that an organization might want to apply. Most of the recommended settings defined in this document were derived from a review of the *Windows Server 2003 Security Guide* and the *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP* document, along with other material identified in the References chapter of this document.

Audience Assumptions

This document assumes the audience is familiar with the general installation process of Windows Server 2003 with SP2 and the configuration tools provided by Windows Server 2003 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 Windows Server 2003 operating system.

Chapter 4, "Windows Firewall Settings," describes the optional configuration of the Windows Internet Connection firewall.

Chapter 5, “Secure Configuration,” describes how to configure Windows Server 2003 into the Evaluated Configuration.

Chapter 6, “Active Directory Federation Services Deployment,” provides the procedures for installing and configuring ADFS.

Chapter 7, “Windows Server Update Services Deployment,” provides the procedures for installing and configuring WSUS.

Chapter 8, “Windows Server 2003 Common Criteria Security Configuration Templates,” describes how to partially automate the configuration of the Evaluated Configuration of Windows Server 2003 with the application of configuration templates.

Chapter 9, “References,” provides the references used to develop this document.

Appendix A, “Windows Server 2003 Default Security Policy Settings,” identifies the Windows Server 2003 default security policy settings (prior to the application of the procedures that result in the Evaluated Configuration of Windows Server 2003).

Appendix B, “Audit Categories and Events,” presents the Windows Server 2003 system audit events that correspond to the events required to be auditable by the Windows 2003/XP V3 ST.

Appendix C, “User Rights and Privileges,” identifies the default user rights assignments in Windows Server 2003, defines their applicability to the Windows 2003/XP V3 ST, and provides change requirements and recommendations necessary to comply with the Windows 2003/XP V3 ST.

Appendix D, “User and Group Accounts”, identifies the default user and group accounts on Windows Server 2003, defines their applicability to the Windows 2003/XP V3 ST, and presents changes to the accounts necessary to comply with the Windows 2003/XP V3 ST.

Appendix E, “Windows Server 2003 Security Configuration Checklist for the Evaluated Configuration,” presents a configuration checklist to ensure that all necessary installation and configuration steps are taken to result in the Evaluated Configuration of Windows Server 2003.

Appendix F, “Windows Server 2003 Security Configuration Templates for the Evaluated Configuration,” contains the security configuration templates that automate changes that the administrator must make to the operating system in order for the system to be in compliance with the Windows Server 2003 Evaluated Configuration .In addition, the appendix contains configuration templates for automating both required and recommended changes to the default settings.

Appendix G, “Device Drivers,” provides a list of all device drivers approved for use in the Evaluated Configuration.

Terminology and Conventions

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

- **Evaluated Configuration:** Used to refer to the configuration of Windows Server 2003 that was evaluated and determined to meet the Windows 2003/XP V3 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.**”
- **Notes:** Text that is important to take notice of is identified with a bolded word “**Note**” or “**Notes**.”
- **Required 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 2003/XP V3 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 2003/XP V3 ST but 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 Server 2003, 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 computers support the ability to start a number of different operating systems. For example, even if users normally start Windows Server 2003 from drive C, someone could boot another operating system from removable media on another drive, such as a floppy disk drive or a Compact Disk-Read Only Memory (CD-ROM) drive. If this happens, any security precautions taken to secure the Windows Server 2003 operating system might be circumvented.

For a secure system, install only one version of Windows Server 2003 on drive C, and do not install any other operating systems on the computer (in other words, do not make the computer multi-boot capable). The central processing unit (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 basic input/output system (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 computer 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 Server 2003 computer with a password. On many hardware platforms, opening the case and clearing the BIOS through a set of jumpers, or removing the motherboard battery, can disable the BIOS password. To prevent this, protect the hardware as described earlier in the Restrict the Boot Process section.

Evaluated Hardware Configuration

Table 2.1 lists the supported hardware platforms and operating system configurations used during the Windows Server 2003 evaluation.

Table 2.1 Evaluated configuration hardware platforms

Manufacturer	Model	Processor(s)	Memory
Dell	PowerEdge SC1420	Intel Xeon (3.6 GHz) (one CPU)	2 GB
Dell	PowerEdge 1800	Intel Xeon (3.2 GHz) (one CPU)	2 GB
Dell	PowerEdge 2850	Intel Xeon (2.8 GHz) (two dual-core CPUs)	4 GB
HP	rx1620 Bundle Solution Server	Intel Itanium (1.3 GHz) (one CPU)	2 GB
HP	Proliant DL385	AMD Opteron Model 252 (2.6 GHz) (one CPU)	2 GB
IBM	eServer 326m Model 796955U	AMD Opteron Model 270 (2.0 GHz) (one CPU)	2 GB
IBM	eServer 326m Model 796975U	AMD Opteron Model 280 (2.4 GHz) (two dual-Core CPUs)	2 GB
Unisys	RASCAL model (ES7000 Real-Time Enterprise Server)	Intel Pentium D (2.50 GHz) (four dual-Core CPUs)	4 GB

Table 2.2 Evaluated hardware and operating system configurations

Evaluated Software Product	Evaluation Hardware
Windows Server 2003 Standard Edition (32-Bit) w/SP2	Dell PowerEdge SC1420 (one CPU)
Windows Server 2003 Standard x64Edition w/SP2	Dell PowerEdge 2850 (two dual-core CPUs) IBM eServer 326m Model 796955U (one CPU)
Windows Server 2003 Enterprise Edition (32-Bit) w/SP2	Dell PowerEdge 1800 (one CPU)
Windows Server 2003 Enterprise x64 Edition w/SP2	Dell PowerEdge 2850 (two dual-Core CPUs) HP Proliant DL385 (one CPU) IBM eServer 326m Model 796975U (two dual-core CPUs)
Windows Server 2003 Enterprise Edition w/SP2 for Itanium-based Systems	HP rx1620 Bundle Solution Server (one CPU)
Windows Server 2003 Datacenter x64Edition w/SP2	Unisys ES7000 Real-Time Enterprise Server (4 dual-core CPUs)

Evaluated Software Configuration

The Windows Server 2003 SP2 Evaluated Configuration includes any one of the roles shown in Table 2.3 configured in accordance with the installation and configuration instructions provided in this document. For further information regarding the specific security requirements met by Windows Server 2003 SP2, see the Windows 2003/XP V3 ST.

Table 2.3 Evaluated Windows Server 2003 SP2 operating systems and applicable roles

Product	Role
Microsoft Windows Server 2003 Standard Edition (32-bit and 64-bit versions)	Domain member server Workgroup member server Stand-alone computer Federation Server host Federation Service Proxy host ADFS Web Agent host Windows Server Update Services (WSUS) host (32-bit only)
Microsoft Windows Server 2003 Enterprise Edition (32-bit and 64-bit versions)	Domain controller Domain member server Workgroup member server Stand-alone computer Federation Server host Federation Service Proxy host ADFS Web Agent host Windows Server Update Services (WSUS) host (32-bit only)
Microsoft Windows Server 2003 Datacenter Edition (32-bit and 64-bit versions)	Domain controller Domain member server Workgroup member server Stand-alone computer Federation Server host Federation Service Proxy host ADFS Web Agent host Windows Server Update Services (WSUS) host (32-bit only)

It is important to understand the difference between a domain and a workgroup environment. The main difference 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 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 require tight security on data should use a domain configuration. Basic definitions are provided here.

- **Domain** — A collection of computers defined by the administrator of a Windows Server 2003 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 Server 2003 computer network from the user account database and Kerberos Key Distribution Center (KDC) perspective.

- **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 Server 2003 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 Server 2003 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 Active Directory and shared resources.
- **Workgroup member** — A computer that is a member of a Windows workgroup, formed as a logical grouping of networked computers for the purpose of sharing resources.
- **Domain member** — A computer that is a joined to a Windows domain.
- **Stand-alone computer (**or **stand-alone workstation)** — A computer that is not connected to any network.
- **Federation Server host** – Federation servers host the Federation Service component of ADFS. They are used to route authentication requests that are made from user accounts in other organizations (in Federated Web Single-Sign-On (SSO) with Forest Trust scenarios) or from external clients that that need to access internal resources (in the Web SSO scenario).
- **Federation Service Proxy host** – Federation server proxies host the Federation Service Proxy component of ADFS. Federation server proxies can be deployed in an organization's perimeter network (also known as a demilitarized zone, extranet, or screened subnet) to forward requests to federation servers that are not accessible from external networks.
- **ADFS Web Agent host** – Within an ADFS supported architecture, Web servers in the resource forest host the ADFS Web Agent component to provide secure access to the Web applications that are hosted on those Web servers. The ADFS Web Agent manages security tokens and authentication cookies that are sent to a Web server. The Web server requires a relationship with a Federation Service so that all authentication tokens come from that Federation Service.
- **Windows Server Update Services (WSUS) host** – WSUS is the server component that is installed on a computer running a Microsoft Windows Server 2003 operating system. WSUS server software enables administrators to manage and distribute updates through a Web-based interface. In addition, one WSUS server can be the update source for other WSUS servers within the TOE.

3. Operating System Installation

This section provides the installation procedures for Windows Server 2003.

Installation Preparation

During installation, Setup prompts for information about how to install and configure Windows Server 2003. Prepare for the Windows Server 2003 installation by collecting hardware information and establishing configuration decisions prior to initiating the installation process. The checklist in Table 3.1 provides some guidelines as to the information that needs to be defined prior to initiating the installation process.

Table 3.1 Windows Server 2003 pre-installation checklist

	Description
❑	**Hardware compatibility:** Review all hardware to ensure compatibility with the Windows Server 2003 operating system and the specified Evaluated Configuration hardware. Hardware components include: Motherboard, network adapters, video card, sound card, CD-ROM drives, etc. For more information about hardware devices supported by the Windows Server 2003 operating systems, see the applicable Windows Catalog at http://www.microsoft.com/whdc/hcl/. The evaluated hardware configurations are described in Tables 2.1 and 2.2.
❑	**Disk space:** Ensure the system has sufficient disk space. The minimum disk space recommended for installation of Windows Server 2003 is 2 GB. The actual requirements vary based on system configuration and the applications and features that are installed.
❑	**Disk partitions:** Determine disk-partitioning requirements, keeping in mind the minimum disk space recommendations for installation of the Windows Server 2003 operating system. It is recommended that the operating system be installed on the primary disk partition.
❑	**File system:** The file system must be configured as New Technology File System (NTFS) in order to allow configuration of the evaluated security mechanisms and conformance to 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 Server 2003 section 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 is to 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 Joining a Domain or Workgroup section provides descriptions for domain and workgroup.
❑	**Service components:** Prior to installation, determine which services are required by the operating system. For server installations, considerations might include Active Directory, Active Directory Federation Services (ADFS), DNS, DHCP, or Internet Information Services (IIS). A list of evaluated services that can be used in an evaluated configuration installation is provided in the Evaluated Configuration System Services section.
❑	**ADFS architecture components:** The following are the software requirements for each ADFS

	Description
	component (Federation Service, Federation Service Proxy, and ADFS Web Service Agent components) in a network environment. ▪ Window Server 2003, R2 product CD (needed to install each of the core ADFS components). ▪ Internet Information Services (IIS), as supported within the TOE. ▪ Microsoft .NET Framework 2.0. ▪ ASP.NET 2.0 enabled (included in Microsoft .NET Framework 2.0). ▪ A default Web site that is configured with Transport Layer Security and Secure Sockets Layer (TLS/SSL). ▪ A Trusted Certification Authority (CA). Since TLS/SSL relies on digital certificates, Microsoft Certificate Services will be necessary within the TOE.
❑	**WSUS components:** The following software components must be installed in order to support the functions of Windows Server Update Services: ▪ Background Intelligent Transfer Service (BITS) 2.0. This service is already available in the operating system, starting with Windows Server 2003 with SP1. ▪ Microsoft .NET Framework 2.0. ▪ ASP.NET 2.0 enabled (included in Microsoft .NET Framework 2.0). ▪ Database software. WSUS requires a database, however, the database is not included in the TOE. It can use several versions of Microsoft SQL. When installed on Windows Server 2003, the Windows Server Update Services download will also install a free version of Microsoft SQL Desktop Engine (MSDE), if no other database is available. For the evaluation of WSUS, the installation of MSDE is sufficient.
❑	**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, DHCP, or IIS. A list of evaluated services that may be used in an Evaluated Configuration installation is provided in the Evaluated Configuration System Services section.

Windows Server 2003 Setup

Installation Methods

Windows Server 2003 can be installed as either an upgrade to an existing Windows operating system or as a new operating system. To ensure a clean installation for the Evaluated Configuration, Windows Server 2003 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 all the hard disk partitions within the computer prior to installing Windows Server 2003.

There are two methods available to install Windows Server 2003:

- CD-ROM
- Over the network, using Remote Installation Service (RIS)

Note: An over the network (RIS) installation shall not be used for the Evaluated Configuration. Procedures for using RIS to install a non-Evaluated Configuration of Windows Server 2003 from the network are described in Microsoft Knowledge Base Article 325862 at http://support.microsoft.com/default.aspx?scid=kb;en-us;325862.

Special Hardware Considerations

Windows Server 2003 Datacenter x64 Edition Installation on Unisys ES7000 Real-Time Enterprise Server Hardware Platform

The installation and configuration of hardware and Service Processors needed to support the initial startup and installation of Windows Server 2003 Datacenter x64 Edition on the Unisys ES7000 Real-Time Enterprise Server hardware platform is not covered in this document. For Unisys ES7000 Real-Time Enterprise Server hardware configuration and Service Processor installation procedures, see the hardware documentation from Unisys.

This document assumes the Unisys Enterprise Server ES7000 hardware and associated Service Processor operating systems are pre-installed and configured prior to initiating the Windows Server 2003 Datacenter Edition installation procedures.

To start the Windows Server 2003 Datacenter x64 Edition installation procedure on the Unisys ES7000:

1. Use an Ethernet (CAT5) cable to connect a Microsoft Windows XP Professional workstation to port 14 of the managed switch mounted in the Unisys rack. This workstation will be used to remotely access the Service Processor for the Unisys ES7000 Real-Time Enterprise Server hardware platform. The Service Processor can only be accessed by way of this direct connection.
2. Log on to the workstation, then use a Web browser to access the Service Processor at http://<*Service Processor IP Address*> (typically http://172.26.3.0).
3. Enter the following logon information for the Service Processor:

   Username: Administrator

   Password: Administer4Me
4. From Server Sentinel, select **Summary** on the system menu.
5. If the system is not powered on, click **Commands** on the system menu, then click the **Power Commands** tab and enable the **State** by clicking the **On** radio buttons. Click the Apply **Selected Power Changes** button to turn on the system.
6. Select **Summary** on the system menu to show a list of partitions.
7. If a partition needs to be created, select **Create Partition** on the **System Commands** pull-down menu and click **Submit**. Name the partition and click **Submit**, then **Close**. Select **Up all cells** and **Submit**, then **Activate and Submit**, and finally **Start and Submit**.

Note: Only leave Compatability Bridge 0 (CPB0) up. Down all other CBPs.

8. If a partition exists, ensure the status shows as active. If the status is not active, stop the partition. Then select **Start** from the **System Commands** pull-down menu and **Submit**. This action might take several minutes to complete.
9. On the **System Summary** of the Server Sentinel window, verify the partition's state is "Initializing."

10. On the **System Summary** of the Server Sentinel window, select the desired partition by clicking the partition name.
11. Open the Console Manager interface by clicking the **Console** icon.
12. Enter the Service Processor administrator user name and password to log on to the Console Manager Partition Desktop.

    Note: The desktop display might state "Video image not available" if the operating system partition has not yet been started.

13. Insert the Windows Server 2003 Datacenter x64 Edition CD-ROM at the Unisys ES7000 Real-Time Enterprise Server hardware platform and follow the installation procedures below. The operating system installation can be completed at the Unisys ES7000 Real-Time Enterprise Server hardware platform console.

The Unisys ES-7000 includes eight network interface cards (NIC). Setup must configure each of the NICs. As a result, during the Microsoft Windows Server 2003 Datacenter installation, Setup appears to hang at the "32 minutes left" mark for approximately one hour as the setup process tries to configure each NIC. In order to drastically decrease this wait time, it is recommended that the number of NICs enabled in the hardware be reduced during Setup. To disable NICs on the Unisys ES7000:

1. In Server Sentinel, on the **Active Partitions** menu, click the desired partition to select it.
2. Under the **Partition: <*PartitionName*>** menu, click **Inventory**.
3. On the Partition Inventory page, scroll down to the bottom, select the **Select All** check box, and then click the **Down Selected** button.
4. On the Partition Inventory page, select the check boxes for the following units only and then click the **Up Selected** button at the bottom of the page. This configuration does not include any of the integrated NICs. The only PCI bus that is up is for the boot adapter.

   IP_0_0

   IP_0_1

   IP_0_2

   IP_0_3

   MEM_0

   CPB_0

   PCI_BUS_0_1

BIOS Modification Requirements for Dell PowerEdge 1800 Computer

The PowerEdge 1800 computer hardware used in the evaluation includes a remote access controller and firmware enabled virtual media. These features need to be disabled for the Evaluated Configuration by following the procedures here.

1. Start the computer. As the computer boots, information will be displayed on the screen showing the Dell Remote Access Controller details, such as that shown below. When this information appears on the screen, press **CRTL+D**.

Dell Remote Access Controller 4/P

Firmware Version 1.33 (Build 08.04)

IP Address: 192.168.0.120

Netmask: 255.255.255.0

Gateway: 192.168.0.1

Press **<CTRL – D>** for DRAC 4/P Setup

2. At the Dell Remote Access Controller 4/P Setup Firmware Version 1.33 (Build 08.04) configuration page, press the **Page Down** key on your keyboard, then press the **E** key to disable Virtual Media under Virtual Media Configuration Options.
3. Press the **R** key to save the changes and then press **Y** to save and continue booting.

Running Setup

This section describes how to begin the operating system installation and describes the phases of the setup process.

Booting from a CD-ROM Disk

The Windows Server 2003 family does not include Setup boot floppy disks, and RIS is not used to install the Windows Server 2003 Evaluated Configuration. This section describes using a bootable CD-ROM to start Setup. The CD-ROM installation method requires configuration of the computer's BIOS to detect and boot from a bootable Windows Server 2003 installation CD-ROM. After the Setup program is started, it works in several stages, prompting for information, copying files, and restarting.

To start Setup from a bootable CD-ROM

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

Initiating the Installation on an Itanium-based Computer

This section explains how to start Setup for a new installation on an Itanium-based computer. In computers with the Itanium processor or the Itanium 2 processor, the Extensible Firmware Interface (EFI) is the interface between a computer's firmware, hardware, and operating system. The EFI defines a new partition style called Globally Unique Identifier (GUID) partition table (GPT). The installation partition on an Itanium-based computer must be on a GPT disk. Setup automatically specifies GPT for the disk used for installation.

The GPT disks cannot be accessed locally from an x86-based computer. To move a disk from an Itanium-based computer to an x86-based computer, use a Master Boot Record (MBR) disk. This is true regardless of whether the disk is basic or dynamic.

Warning: Itanium-based computers require a minimum 100 MB file allocation table (FAT) partition for the operation of the EFI. This EFI system partition is created automatically during Setup, and it stores programs and information files that the EFI uses to start the operating system. Do not delete or reformat this partition.

Setup also creates a Microsoft Reserved Partition (MSR), which is required by the operating system. The size of this partition depends on the size of the hard disk. On drives less than 16 GB in size, the MSR is 32 MB. On drives greater than or equal to 16 GB, the MSR is 128 MB. Do not delete or reformat this partition.

To start Setup on an Itanium-based computer

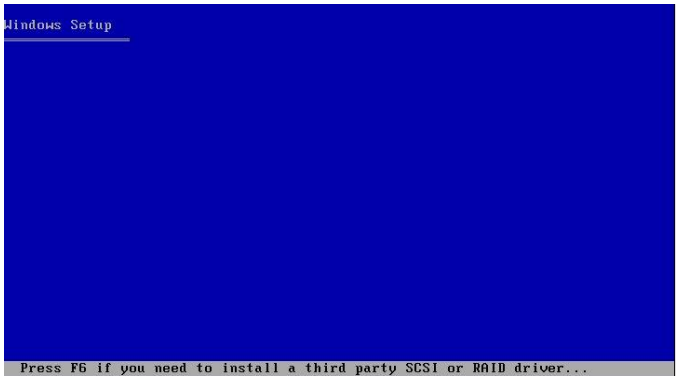
1. Immediately after turning on the computer, insert the Setup CD in the CD-ROM drive.
2. When the EFI Boot Manager menu appears, select the CD-ROM option.
3. When prompted, press any key to start from the CD-ROM.
4. Follow the Setup instructions on the screen. The text mode installation phase that will follow is explained in the Text Mode Installation Phase section next.

Text Mode Installation Phase

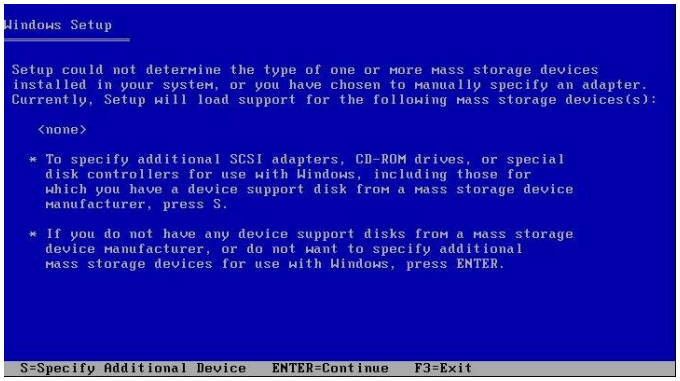
This section provides details for the text mode installation phase of the Windows Server 2003 operating system. After Setup has been initiated, the setup process begins.

1. Setup begins by inspecting the computer's hardware. The screen displays the message "Setup is inspecting your computer's hardware configuration…"
2. Setup then moves on to an interactive stage, where the first interaction depends on whether there are third-party Small Computer System Interface (SCSI) or Redundant Array of Inexpensive Disks (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 7.

Note: Installing Windows Server 2003 Datacenter x64 Edition on the ES7000 Real-Time Enterprise Server hardware platform requires an Adaptec ASC-48300 SAS/SATA Host Adapter driver. In this case, press the **F6** key on the keyboard at this step of Setup and insert the driver disk when prompted.

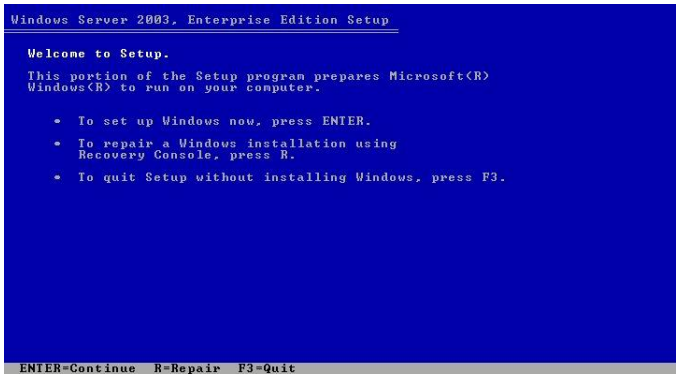


3. If the **F6** (or **F5**) key is pressed, Setup proceeds to load files until it reaches the stage where it requires the third-party driver.
4. When setup reaches the stage where it requires the third-party driver, the is displayed:

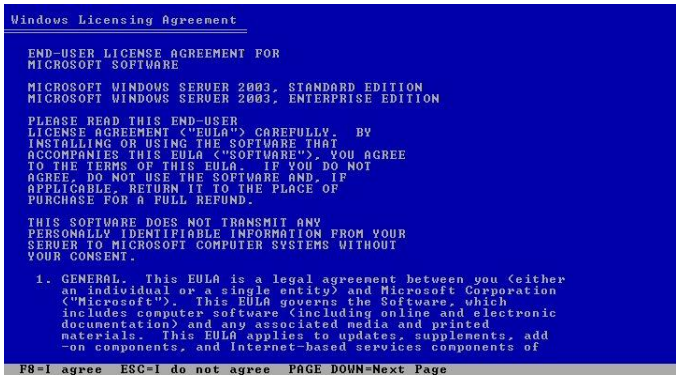


5. Pressing the **S** key on the keyboard causes Setup to search the A: drive for a driver. If there is no disk in the drive, the following interactive display appears:

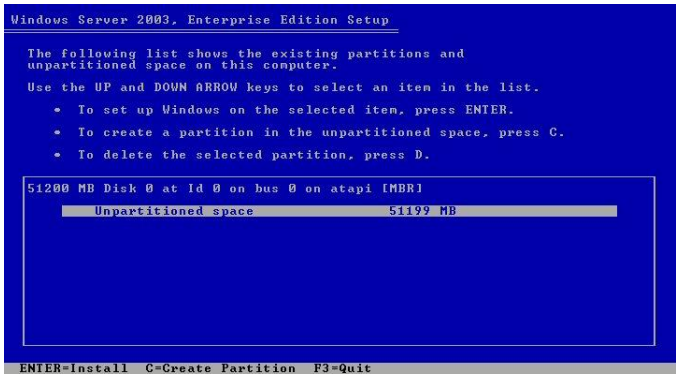
6. Place the disk containing the manufacturer-supplied driver in drive A: and press the **Enter** key on the keyboard to continue. Setup reads the information about the floppy disk and displays the available driver choices.
7. Ensure that the proper driver is selected and press the **Enter** key to continue. Setup begins loading the selected driver. A confirmation of the selected driver is displayed. If additional drivers are required, press the **S** key on the keyboard, otherwise press **Enter** to continue.
8. Setup continues loading files for a short period of time. After the necessary files have been loaded, a message appears briefly: “Setup is starting Windows.” In the interactive display that follows, the user has the option of selecting whether to set up Windows (install), repair an existing installation, or exit Setup. Press **Enter** to continue.



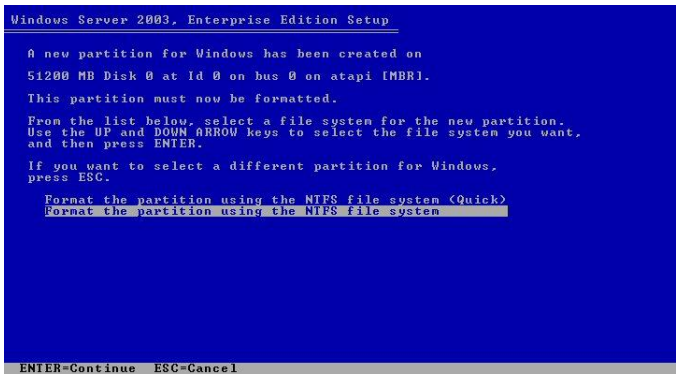
9. The Windows End-user License Agreement is displayed. Use the **Page Down** key on the keyboard to scroll through the text while reading it. After reading the licensing agreement, ensure that the page has been scrolled all the way to the bottom and press **F8** to accept the agreement and continue with the installation.



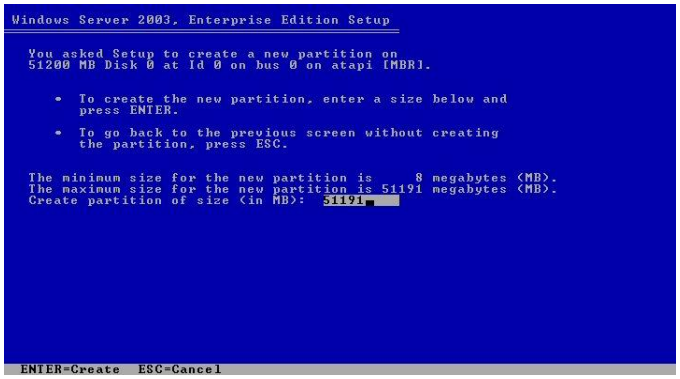
10. The next interactive display shows the existing hard disks and partitions that are available in the computer. If there are multiple partitions or multiple hard disks they are identified here. Any unpartitioned space on the disk must be partitioned and formatted before it can be used. The interactive display example below shows a 50 GB hard disk that is not partitioned. To use all of the existing unpartitioned space as a single partition, press the **Enter** key on the keyboard and proceed to Step 11 of these procedures. In order to partition the disk press the **C** key on the keyboard and proceed to Step 12.



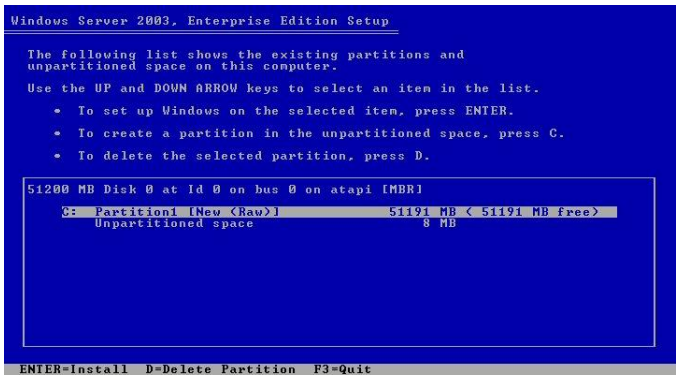
11. The interactive display shows that the new partition was created and must be formatted. To format the partition, select **Format the partition using the NTFS file system**, press the **Enter** key on the keyboard, and proceed to Step 14.



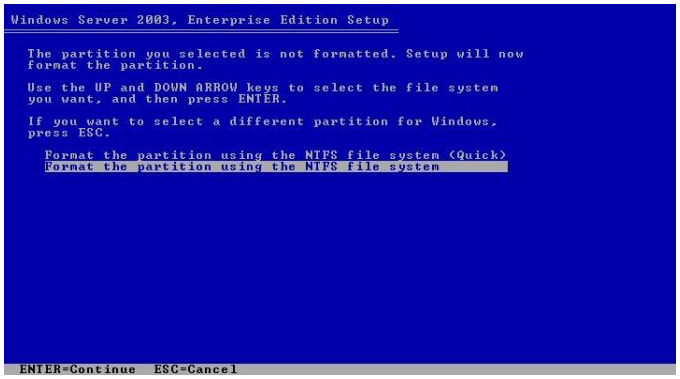
12. If selecting **To create a partition in the unpartitioned space**, the next interactive display provides the ability to define the size of the new partition. The default size selected is the full amount of the unpartitioned space that was previously selected. Either reduce the size for the required 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.



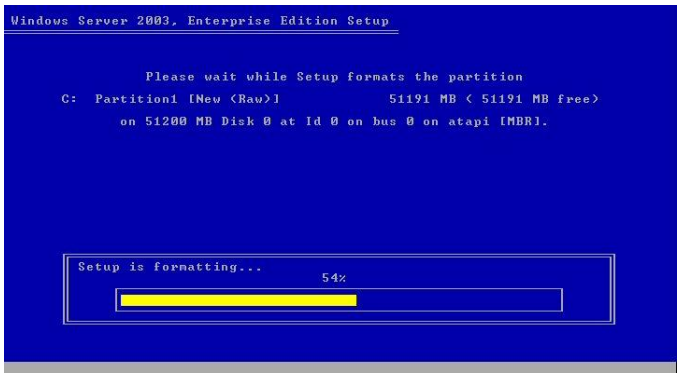
13. The interactive display shows the available disk partitions, displaying the new partition that is available for installation. Select the newly created partition and press **Enter** to proceed.



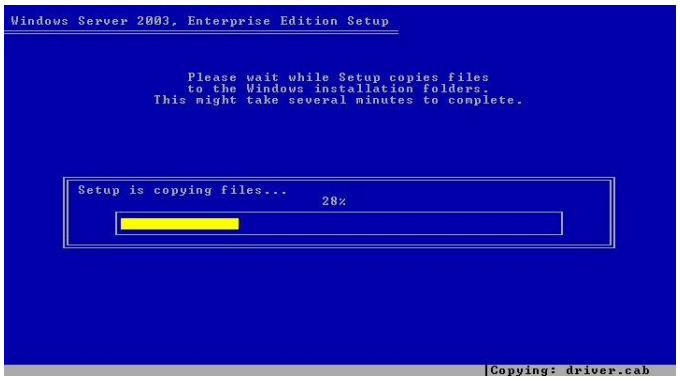
14. The interactive display presents the options for formatting the selected partition. Select **Format the partition using the NTFS file system** and press the **Enter** key on the keyboard to continue.



15. Setup formats the partition.



16. When formatting is completed, Windows Server 2003 Setup examines the disks and then proceeds to copy the necessary operating system files to the hard disk.



17. When all files have been copied to the hard disk, Setup restarts the computer. Remove any disk from the floppy drive. Allow Setup to count down to the restart, or press **Enter** to restart the computer.

18. When the computer reboots, the installation continues in graphical user interface (GUI) mode. The GUI mode installation phase is explained in the next section of this guide.

GUI Mode Installation Phase

This section addresses several of the key installation settings that are configured 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. Windows Server 2003 presents a series of dialog boxes to collect configuration information for setting up the operating system. Most of the sample screen shots and dialog boxes presented in this section are based on a Windows

Server 2003 Enterprise Edition installation. However, the setup process described also applies to Windows Server 2003 Standard Edition installations, unless otherwise specified.

GUI mode startup

After Windows Server 2003 Setup completes the text mode installation phase, the computer reboots and begins the GUI mode phase of the installation.

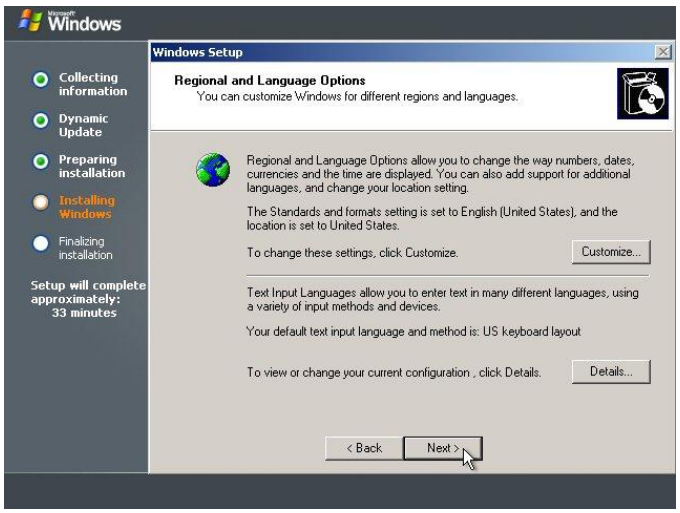
1. The Windows GUI mode begins by displaying the startup background for Windows Server 2003.

2. Setup continues by automatically detecting and installing hardware devices. This might take a few minutes and the screen might flicker during the process. When this process completes, the Regional Settings dialog box appears.

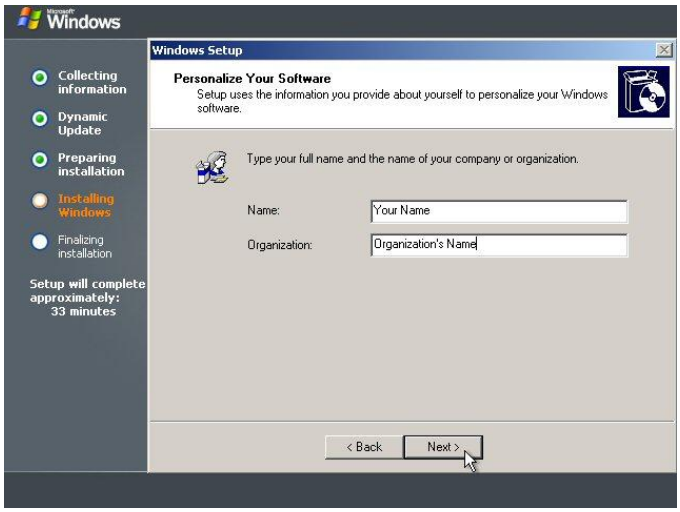
Specify regional options, name, product key, and licensing mode

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

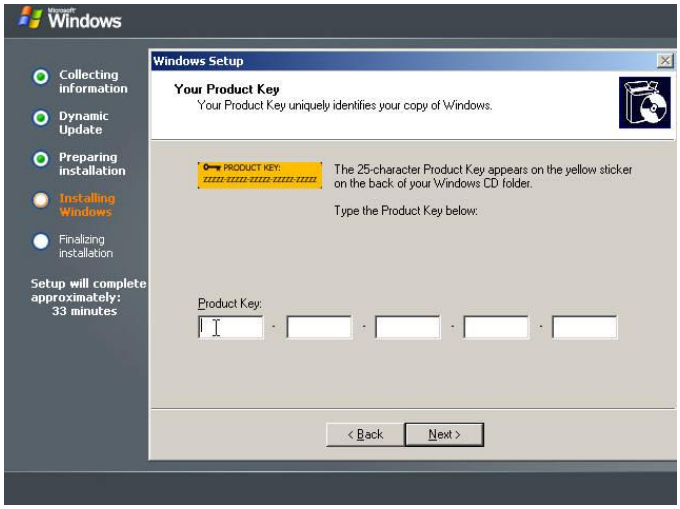
1. In the **Regional and Language Options** page, verify or change the default settings for language, locale, and accessibility options. To make changes to the Regional and Language Options, click the **Customize** button and type any needed changes in the Regional and Language Options interface. The default text input language device is US keyboard layout. To change the text input language device, click the **Details** button and add the new device option in the Text Services and Input Languages interface.
2. Click **Next**.



3. In **Personalize Your Software**, type the user name and, optionally, the name of an organization. Click **Next**.

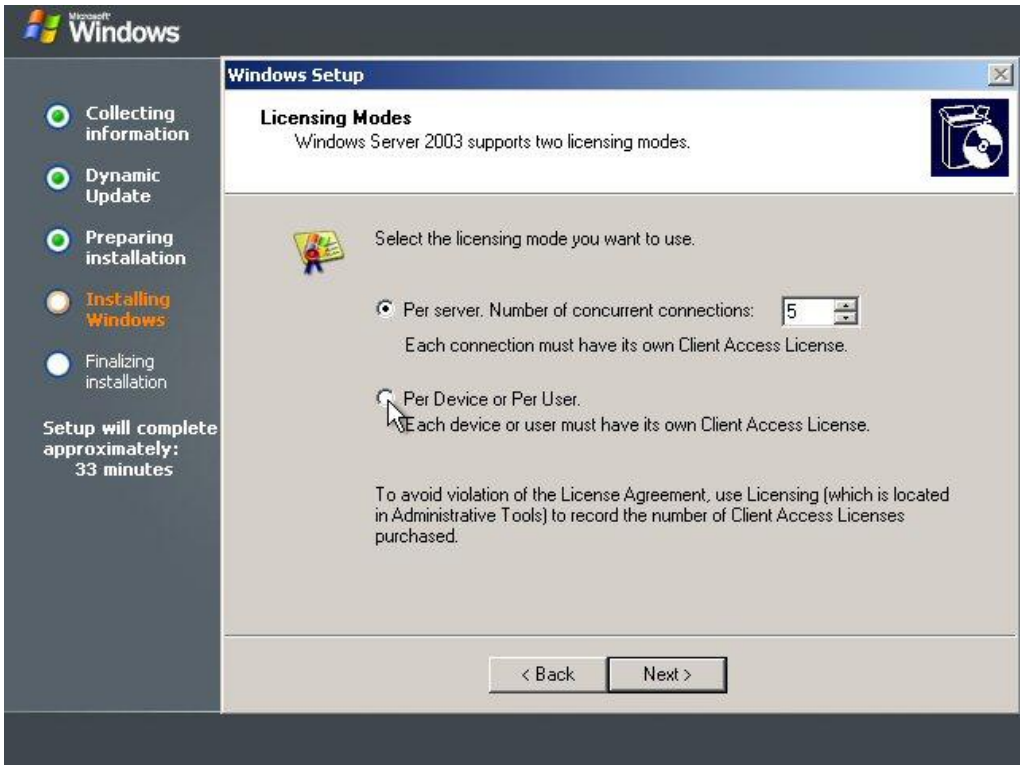


4. For **Product Key**, enter the 25-character product key for the Windows operating system being installed. Click **Next**.



Select a licensing mode for Windows Server 2003

1. In the **Licensing Modes** page, select the client-licensing mode, either **Per server, or Per Device or Per User** (also called Per seat). If unsure of which mode to use, select **Per server** because a change is allowed once from Per server licensing to Per seat licensing at no cost. A description of the licensing modes is provided next.



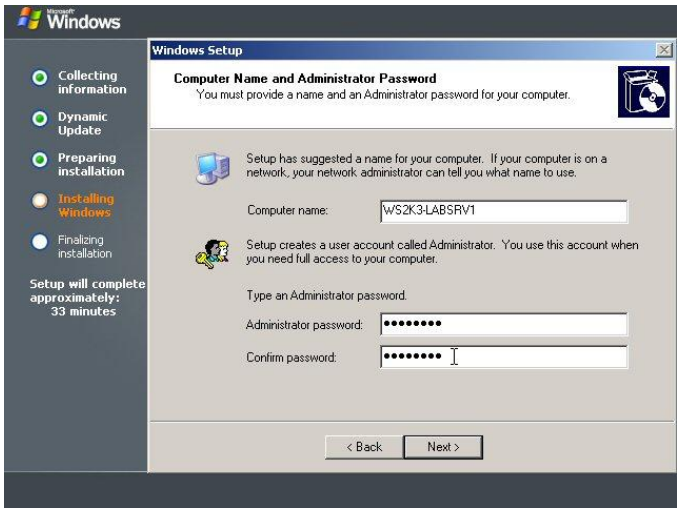
- **Per server** — Per server licensing means that each concurrent connection to the server requires a separate client access license (CAL). This means that at any one time, the server can only support a fixed number of connections. For example, if the Per server licensing mode is selected with five concurrent connections, the server would only be able to have five computers (clients) connected at any one time. Those computers would not need any additional licenses.

- **Per seat** — Per seat licensing means that each computer that accesses the server requires a separate CAL. With one CAL, a particular client computer can connect to any number of servers. This is the most commonly used licensing method for companies with more than one server running Windows Server 2003.

2. When the licensing mode is selected, click **Next** to continue Setup.

Assign a computer name and Administrator account password

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



Computer name

Enter a computer name in the **Computer Name and Administrator Password** page of Windows Setup. 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 the Microsoft Domain Naming System (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, seven characters in some), pre-Windows 2000 computers in the environment will recognize this computer by the first 15 bytes of the name only. 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

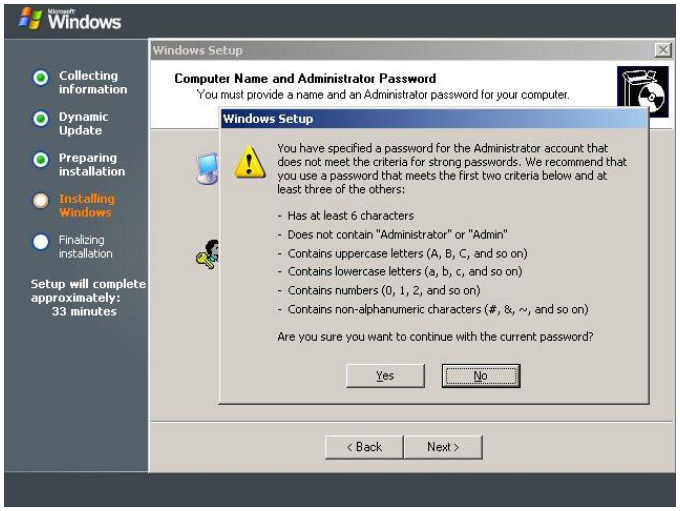
The Windows Server 2003 Setup program creates a user account on the computer called Administrator that has administrative privileges for managing the overall configuration of the computer. The Administrator account is intended for the person who manages the computer.

1. In the **Computer Name and Administrator Password** page, for **Administrator password**, type a password of up to 127 characters. For strong password security, use a password of at least eight 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 eight characters. For security reasons, it is recommended that a strong password be assigned to the Administrator account.

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

The password typed in Confirm password must exactly match the password typed in Administrator password. If the entered password does not meet the criteria for strong passwords, a warning message appears as shown below. Read the message, click No, and re-enter a new password that meets the criteria for strong passwords. Take special care to remember and protect the password.

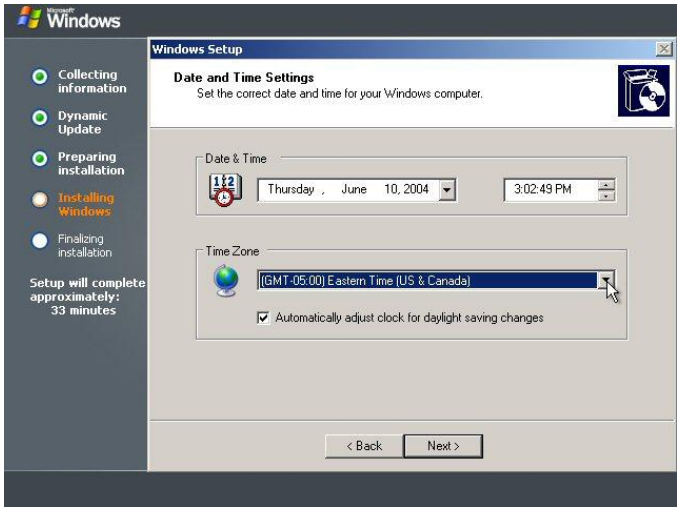


Note: After Setup is completed, it is recommended that the name of the Administrator account be changed (it cannot be deleted). Keep a strong password for the Administrator account at all times.

Set the date and time

The Date and Time Settings view of Windows Setup 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.

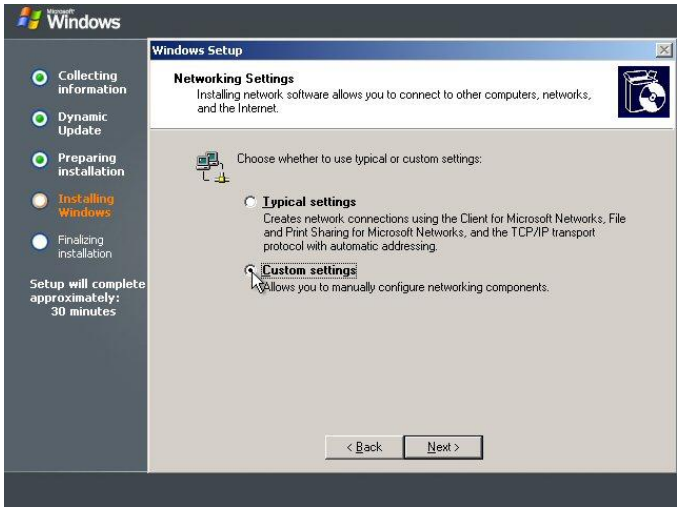


2. Set the system to automatically adjust for daylight saving time by selecting the **Automatically adjust clock for daylight saving changes** check box.
3. Click **Next** to continue Setup. Windows Setup begins installing networking software.

Note: If a driver for the network card is not available on the Setup CD, the system reboots and skips the network settings (describe in the next section of this guide). If this occurs, the network card driver must be installed after the operating system installation is completed.

Configure network settings

The **Networking Settings** page of Windows Setup 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 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 view of Windows Setup, Windows Server 2003 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 Internet Protocol (IP) address. If there is no DHCP server

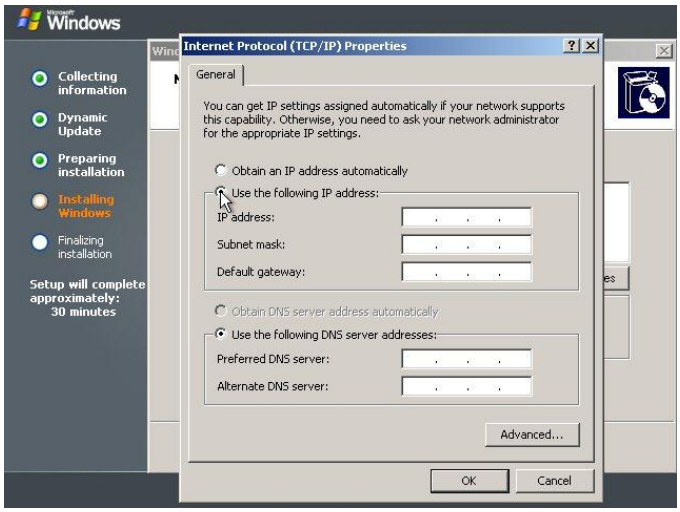
within the domain, Automatic Private IP Addressing (APIPA) assigns an IP address. APIPA provides automatic IP address assignment for computers on networks without a DHCP server. APIPA assigns an internal IP address that is not routable on the Internet.

- **Custom settings** — When the **Custom settings** radio button is selected in the Networking Settings view of Windows Setup, Setup opens the Networking Components interface to allow customized configuration of network components including the selection of dynamic or static IP address and networking information.

For the Windows Server 2003 Evaluated Configuration, in general, either static or dynamic IP addresses can be assigned. It is recommended that all servers have a static IP address. It is important to note that servers that are configured as domain controllers require a static IP address.

To specify a static local IP address and settings needed for DNS and Windows Internet Naming Service (WINS)

1. In the **Networking Settings** page of Windows Setup, select the **Custom settings** radio button and click **Next** to continue.
2. In the **Networking Components** page, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. In the Internet Protocol (TCP/IP) Properties interface, click **Use the following IP address.**



4. For **IP address** and **Subnet mask**, type the appropriate numbers. (If appropriate, specify the **Default gateway** as well.)
5. Type the address of the **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 assigned in the **IP address** field.
6. If a WINS server is required, click **Advanced**, and on the **WINS** tab, click **Add** to type the IP address of one or more WINS servers. If the local server is a WINS server, type the IP address assigned earlier.
7. Click **OK** in each dialog box, and click **Next** in the **Networking Components** page to continue Windows Setup.

Joining a Domain or Workgroup

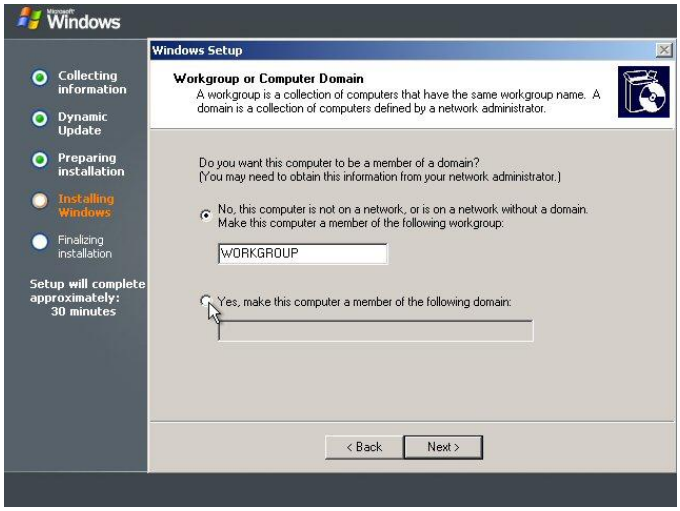
The Workgroup or Computer Domain dialog box allows the option of joining a workgroup or a domain.

1. To join a workgroup or a domain select 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 a Windows Server 2003 to a Domain Controller section.

---

2. Enter the name of the workgroup or domain in the text box and click **Next** to continue Setup.



- **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 is 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 domain administrator to create a computer account in the domain prior to proceeding with Setup. Otherwise, have an authorized administrator, with domain administrator rights, create the account and join the domain during this Setup stage. This requires an authorized administrator to enter an account name and password.

3. Windows Setup installs all the previously defined Windows Server 2003 components.
4. When Setup completes the installation, the computer reboots.
5. After the computer reboots, log on to the computer by pressing **CTRL+ALT+DEL,** entering the Administrator name and password in the Log On to Windows interface, and clicking **OK**.

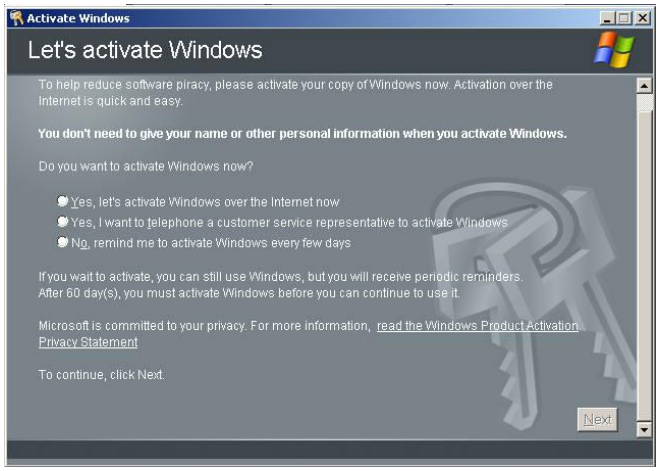
Note: A balloon tip might appear in the system tray indicating that the screen resolution needs to be adjusted. If necessary, click the balloon tip to open the Display Properties interface, click the **Settings** tab, and make the necessary screen resolution adjustments. When finished click **OK** to close Display Properties and save settings.

Activating the Product

Unlike products sold through Microsoft's volume licensing programs, retail boxed versions of Windows Server 2003 software require product activation. As a result, until activation occurs, a balloon tip periodically appears in the system tray indicating the number of days left for activation.

How to Activate Windows Server 2003

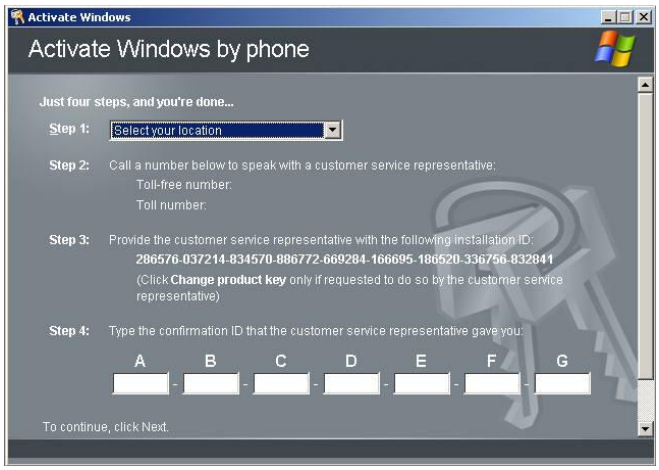
1. Click the balloon tip, or on the activation icon (an image of a set of keys) in the system tray to open the Activate Windows interface.



2. The **Activate Windows** page offers three activation options. Because the Evaluated Configuration is not connected to the Internet, activation must be completed using the telephone. Select the **Yes, I want to telephone a customer service representative to activate Windows** radio button and click **Next**. An installation ID is automatically generated.

3. Follow the steps in the **Activate Windows** pages and click **Next** to complete the product activation process. For more information, see Understanding Product Activation for Retail Boxed Product.

Note: The telephone numbers will differ based on the location selected in Step 1 of the Activate Windows interface.



4. When activation is completed a message appears indicating that the product was successfully activated. Click **OK**.

Understanding product activation for retail boxed product

Product activation works by validating that the software's product key, required as part of product installation, has not been used on more personal computers (PCs) than is allowed by the software's end user license agreement (EULA). Activation is completed either directly by way of the Internet or by a telephone call to a customer service representative. Because the Target of Evaluation (TOE) does not have Internet access, Windows Server 2003 installations that need activation require a telephone call to Microsoft's Customer Service.

Product activation relies on the submission of the installation ID. The installation ID is specifically designed to guarantee anonymity and is only used by Microsoft to deter piracy. The installation ID is comprised of two pieces of information – the product ID and a hardware hash (a hash is a numeric value derived through a mathematical formula and based upon some other, original value). The product ID is unique to the installation of Windows and is created from the product key used during installation. Each product key delivered with retail boxed software is unique, and the product ID it creates is unique. Microsoft uses the product ID for other purposes in addition to product activation such as when requesting product support. The product ID can be found by viewing the Properties of My Computer (an example of a product ID is 12345-123-1234567-12345).

The hardware hash is an eight-byte value that is created by running ten different pieces of information from the PC's hardware components through a one-way mathematical transformation. This means that the resultant hash value cannot be backwards calculated to determine the original values. Further, only a portion of the resulting hash value is used in the hardware hash in order to ensure complete anonymity.

Additionally, whether or not the PC can be put into a docking station or accepts Personal Computer Memory Card International Association (PCMCIA) cards is also determined (the possibility of a docking station or PCMCIA cards existing means that hardware may disappear or seem changed when those devices are not present). Finally, the hardware hash algorithm has a version number. Together with the general nature of the other values used, two different PCs

could actually create the same hardware hash. The 10 different hardware values used to create the hash are outlined in Table 3.2.

Table 3.2 Hardware hash component values

	Component Name	Example Hash Value (bits)
1	Display adapter	00010 (5)
2	SCSI adapter	00011 (5)
3	Integrated Device Electronics (IDE) adapter	0011 (4)
4	Network Adapter Media Access Control (MAC) address	1001011000 (10)
5	Random Access Memory (RAM) amount range (i.e. 0-64 MB, 64-128 MB, etc)	101 (3)
6	Processor type	011 (3)
7	Processor serial number	000000 (6)
8	Hard drive device	1101100 (7)
9	Hard drive volume serial number	1001000001 (10)
10	CD–ROM / CD-RW / DVD-ROM	0101111 (7)
-	Dockable	0 (1)
-	Hardware hash version (version of algorithm used)	001 (3)

The product ID (nine bytes) and hardware hash (eight bytes) are used by Microsoft to process the activation request. When activation is done over the Internet, these two values form the installation ID (in a binary format) and are sent along with request header information directly through secure sockets layer in hyper text transfer protocol (SSL in HTTP) to the Microsoft activation system in a binary format. If Internet activation is successful, the activation confirmation is sent directly back to the user's PC as a digital certificate. This certificate is digitally signed by Microsoft so that it cannot be altered or counterfeited. The confirmation packet returned as part of Internet activation is approximately 9 KB in size (the digital certificate chain accounts for most of the confirmation data packet size).

If activation is done by telephoning a customer service representative, as would be required for an Evaluated Configuration installation, the product ID and hardware hash are automatically displayed to the user as the installation ID; a 50-digit decimal representation. The encoding encrypts the data so that it cannot be altered and provides check digits to help aid in error handling. Telephone activation is a four-step process:

1. Select the country from which the call is being made so that an appropriate phone number can be shown in the product user interface (UI)
2. Dial the phone number
3. Provide the installation ID to the customer service representative
4. Enter the Confirmation ID provided by the customer service representative.

The confirmation ID is a 42-digit integer containing the activation key and check digits that aid in error handling. Both the installation ID and confirmation ID are displayed to the user in easily understandable segments in the product UI.

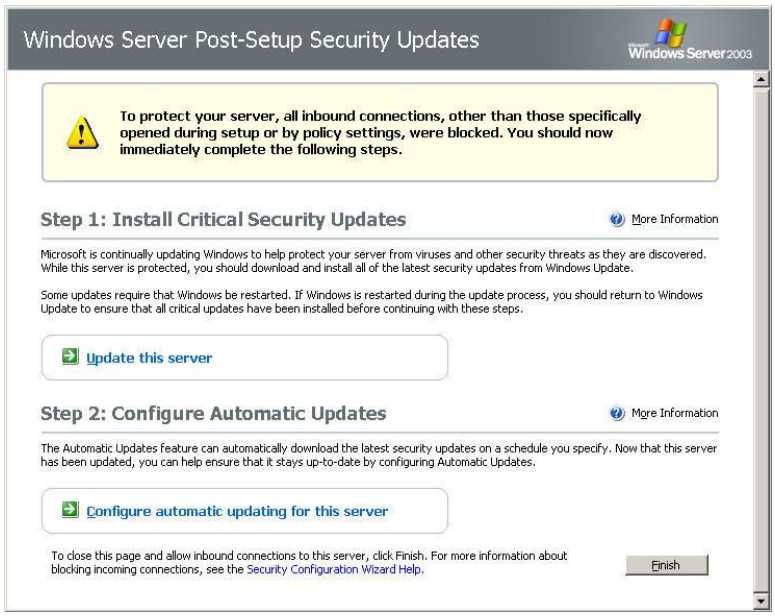
For the Evaluated Configuration, Windows Server 2003 versions requiring activation must be activated during the setup process described in this document. If the product is not activated at this time, the user is reminded about the activation requirement at each logon until the end of the

30-day grace period. An Activation Wizard is available to assist in the activation process. If the product is not activated by the time the grace period ends, the product becomes unusable until activated.

Note: The Activation Wizard is not included in the TOE but can be used during the configuration process.

Configuring Post-Setup Security Updates

For installations of Windows Server 2003 that include SP1 or later (such as a slip-streamed version of Windows Server 2003 with SP2), a Windows Server Post-Setup Security Updates interface appears the first time an administrator logs onto the new server. It provides links to apply updates to the server and to configure automatic update features on the server. The Windows Server Post-Setup Security Updates interface also informs the administrator that all inbound connections other than those specifically opened during setup or by policy settings, are being blocked. The connections are blocked by the Windows Firewall, which is installed with all Service Packs, beginning with SP1 for Windows Server 2003.



Note: If network card drivers were not installed, the Windows Server Post-Setup Security Updates interface does not appear.

For the Evaluated Configuration it is not possible to download updates directly because the TOE is not connected to the Internet. Additionally, automatic update services are not enabled in the Evaluated Configuration. Therefore, do not click the links in Steps 1 and 2 of the Windows Server Post-Setup Security Updates interface. Instead, click **Finish** to close the Windows Server Post-Setup Security Updates interface. A message appears indicating that after the Windows Server Post-Setup Security Updates interface is closed, inbound connections to the server will be allowed. Click **Yes**.

Microsoft Windows Server 2003 R2 Requirement for ADFS and DFS Components

The installation of Microsoft Windows Server 2003 R2 is required for all computers that will be hosting Active Directory Federated Services (ADFS) or Distributed File System (DFS) components within the TOE. The installation of R2 on Windows Server 2003 makes the software packages for ADFS and DFS available for installation on that host. The procedures below describe the installation of the Microsoft Windows Server R2 component on a server that already has Microsoft Windows Server 2003 SP2 installed.

ADFS is a required component of the TOE; therefore procedures for the installing ADFS components are available in the ADFS Installation Preparation section of this document. DFS is an optional component of the TOE; therefore there fore procedures for installing DFS components are available in the Distributed File System (DFS) section of the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

Install Microsoft Windows Server 2003 R2 Component

1. Log on as an authorized administrator.
2. Insert Disc 2 of the R2 operating system disc set into the optical drive. The "Welcome to Microsoft Windows Server 2003 R2" interface will appear.

   Note: If this window does not automatically appear, click the **Start** button, then click on **My Computer** to open the My Computer view of Windows Explorer. Double-click to CDROM drive that the R2 disc is in. This will open up the CDROM drive window and the contents of the CD will be displayed. Double-click the file "R2AUTO.EXE" to begin the R2 installation.
3. On the "Welcome to Microsoft Windows Server 2003 R2" interface, click **Continue Windows Server 2003 R2 Setup**. The Microsoft Windows Server 2003 R2 Setup Wizard will appear.
4. Click **Next**.
5. The Product Key screen will appear. Enter the appropriate Windows Server 2003 R2 product key then click **Next** to continue.
6. The End-User License Agreement interface will appear. Review the Microsoft Software License Terms, select the radio button to accept the terms in the license agreement, and click **Next** to continue.
7. The Setup Summary interface will appear. Click **Next** to continue.
8. The Updating your system interface will appear and the Windows Server 2003 R2 installation will begin.
9. After the installation has finished, the Completing Windows 2003 R2 Setup interface will appear. Click **Finish** to complete the installation process.

10. Click **Exit** on the "Welcome to Microsoft Windows Server 2003 R2" window to close the window.
11. Click **Start**, click **Shut Down**, and then restart the computer for the operating system changes to take effect.
12. Once the computer reboots, ADFS and DFS components will be available for installation.

Registry Modification Required for Windows Server 2003 Datacenter Edition

The installation of SP2 on Widows Server 2003 Datacenter Edition is blocked by default to prevent its installation without the approval of the OEM hardware manufacturer. Typically, once the OEM has verified that the SP does not damage the required configuration of Widows Server 2003 Datacenter Edition on their hardware, they will issue a version of the SP that includes a registry modification to allow installation of the SP. Within the TOE, testing has shown that SP2 does not harm the Widows Server 2003 Datacenter Edition configuration.

When installing Windows Server 2003 Datacenter Edition within the TOE, it is necessary to edit the registry in order to allow the installation of SP2. This will only be necessary if SP2 is not already integrated with the Windows Setup disk and must be installed separately. See procedures for using the Registry Editor in Additional Security Settings. Edit the registry as described in Table 3.3.

Table 3.3 Required registry modification for Windows Server 2003 Datacenter edition

HKLM\SOFTWARE\Microsoft\Updates\		Format	Value
Key: Windows Server 2003	Value Name: DTCUpdate	REG_DWORD	1

Windows Server 2003 Service Packs and Security Updates

Windows Server 2003 service packs provide the latest updates for the Windows Server 2003 operating system. These updates are a collection of fixes in the following areas: application compatibility, operating system reliability, security, and setup. Each service pack is cumulative and includes all of the updates contained in previous Windows Server 2003 service packs.

Windows Server 2003 post-SP security updates provide product updates that address specific security issues that occur between service pack releases. All post-SP security updates are generally rolled into each successive service pack. For example, SP2 for Windows Server 2003 contains all the security updates included in SP1 plus all of the post-SP1 security updates.

The Windows Server 2003 Evaluated Configuration must include Windows Server 2003 SP2 (released on March 12, 2007) for all 32-bit and 64-bit versions of the operating system, along with the all of the required post-SP2 security updates described in the Microsoft Security Bulletins and Knowledge Base Articles listed in Table 3.4. The recommended post-SP2 security updates can be installed as needed.

For information about obtaining SP2, see the Windows Server 2003 Service Pack 2 Web site at http://technet.microsoft.com/en-us/windowsserver/bb229701.aspx. Information about obtaining Windows Server 2003 software updates is available at http://www.microsoft.com/windowsserver2003/downloads/updates/default.mspx

Table 3.4 Windows Server 2003 post-SP2 security updates

Microsoft Security Bulletin	Microsoft Knowledge Base Article	Required Security Update	Recommended Security Update
MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212) **OS Environment:** x86, x64, and ia64 Dated: Jul 10, 2007	KB931212		✓
MS07-039: Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122) **OS Environment:** x86, x64, and ia64 Dated: Jul 10, 2007	KB926122	✓	
MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution (935839) **OS Environment:** x86, x64, and ia64 Dated: Jun 12, 2007	KB935839	✓	
MS07-033: Cumulative Security Update for Internet Explorer (933566) **OS Environment:** x86, x64, and ia64 Dated: Jun 12, 2007	KB933566		✓
MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840) **OS Environment:** x86, x64, and ia64 Dated: Jun 12, 2007	KB935840	✓	
MS07-029: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966) **OS Environment:** x86, x64, and ia64 Dated: May 8, 2007 **Note:** This update only installs on Windows Server 2003 hosts configured with the DNS Server role. See Apply the Domain Name System (DNS) server service Security Update.	KB935966	✓	
MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784) **OS Environment:** x86 Dated: Apr 10, 2007	KB931784	✓	
MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)	KB930178	✓	

Microsoft Security Bulletin	Microsoft Knowledge Base Article	Required Security Update	Recommended Security Update
OS Environment: x86, x64, and ia64 Dated: Apr 10, 2007			
MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168) **OS Environment:** x86, x64, and ia64 Dated: Apr 10, 2007	KB932168		✓
MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902) **OS Environment:** x86, x64, and ia64 Dated: Apr 3, 2007	KB925902	✓	

Software Update for Base Smart Card Cryptographic Service Provider

An update for the Base Smart Card Cryptographic Service Provider (CSP) must be installed in order to use the smart cards specified for the Evaluated Configuration. Microsoft released this update to allow smart card vendors to more easily enable their smart cards on Microsoft Windows by using a lightweight card module instead of a full CSP. This update must be installed to support smart card deployments within the TOE. The Base Smart Card CSP updates for Windows Server 2003 32-bit and 64-bit operating systems can be downloaded from the following Microsoft Web sites:

- **Base Smart Card Cryptographic Service Provider Package: x86**
  http://www.microsoft.com/downloads/details.aspx?familyid=e8095fd5-c7e5-4bee-9577-2ea6b45b41c6&displaylang=en
- **Base Smart Card Cryptographic Service Provider Package: x64**
  http://www.microsoft.com/downloads/details.aspx?familyid=b94e189d-e766-489d-a3e9-b67e896d5ccc&displaylang=en
- **Base Smart Card Cryptographic Service Provider Package: ia64**
  http://www.microsoft.com/downloads/details.aspx?familyid=33d5b229-80fe-4d31-9ca9-9c24015ccb15&displaylang=en

Install Microsoft .NET Framework 2.0

The TOE environment includes the use of Microsoft .NET Framework 2.0. It is a required component which supports the functions of ADFS and WSUS and must be installed as an updated component of the operating system. Microsoft .NET Framework 2.0 for Windows Server 2003 32-bit and 64-bit operating systems can be downloaded from the following Microsoft Web sites:

- **Microsoft .NET Framework 2.0: x86**
  http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en
- **Microsoft .NET Framework 2.0: x64**
  http://www.microsoft.com/downloads/details.aspx?familyid=B44A0000-ACF8-4FA1-AFFB-40E78D788B00&displaylang=en

- **Microsoft .NET Framework 2.0: ia64**
  http://www.microsoft.com/downloads/details.aspx?familyid=53C2548B-BEC7-4AB4-8CBE-33E07CFC83A7&displaylang=en

February 2007 cumulative time zone update for Microsoft Windows operating systems

Starting in the spring of 2007, daylight saving time (DST) start and end dates for the United States transition to comply with the Energy Policy Act of 2005. DST dates in the United States start three weeks earlier, at 2:00 A.M. on the second Sunday in March. DST will end one week later, at 2:00 A.M. on the first Sunday in November. This update changes the time zone data to account for the DST change for the United States. The update can be downloaded at: http://support.microsoft.com/kb/931836/en-us

Apply the Domain Name System (DNS) server service Security Update

An update for the Domain Name System (DNS) Server Service must be installed on all Windows Server 2003 hosts that are configured with the DNS Server role. This update mitigates a remote code execution vulnerability in DNS that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. The following Microsoft Security Bulleting provides details about the vulnerability and links to for downloading the update: MS07-029: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966)

Verifying Hardware Data Execution Prevention Settings on 64-bit Operating Systems

This section defines procedures for using the Windows Management Instrumentation Command-line (WMIC) tool to verify that the hardware enforces DEP for 64-bit processes and to determine if x64 and ia64 editions of Windows Server 2003 are configured to support DEP for 32-bit processes. If the hardware supports DEP, it will be used by default by the 64-bit operating system and all 64-bit processes. Hardware-enforced DEP cannot be disabled for 64-bit operating systems and processes.

To determine if the current hardware supports DEP

1. Click **Start**, and select **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**. A command line interface appears.
3. At the command prompt, type the following command, and then press **Enter**:

   wmic OS Get DataExecutionPrevention_Available

   Note: If this is the first time WMIC is executed on the computer, a brief message is displayed stating “Please wait while wmic is being installed.” Then the results of the command are displayed.
4. If the output is "TRUE," hardware-enforced DEP is available. Type **Exit** and press **Enter** to close the window.

To verify that Windows running with hardware-enforced DEP enabled

1. Click **Start**, and select **Run**.

2. Type **cmd** in the **Open** box, and then click **OK**. A command line interface appears.
3. At the command prompt, type the following command, and then press **Enter**:

   wmic OS Get DataExecutionPrevention_Drivers
4. If the output is "TRUE," Windows is using hardware-enforced DEP. Type **Exit** and press **Enter** to close the window.

To use WMIC to determine if DEP is being used for 32-bit binaries

1. Click **Start**, and select **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**. A command line interface appears.
3. At the command prompt, type the following command, and then press **Enter**:

   wmic OS Get DataExecutionPrevention_SupportPolicy
4. The value returned is 0, 1, 2 or 3. This value corresponds to one of the DEP support policies described in Table 3.7.

Table 3.7 Values ascribed to DEP support policies

Data Execution Prevention Support Policy Property Value	Policy Level	Description
2	OptIn	Only 32-bit Windows core binaries and processes have DEP protection.
3	OptOut	DEP is enabled for all 32-bit processes. Administrators can manually create an exclusion list of specific programs to exclude from DEP protection.
1	AlwaysOn	DEP is enabled system-wide for all 32-bit processes.
0	AlwaysOff	DEP is not enabled for any 32-bit processes.

Modification of hardware-enforced DEP support for 32-bit processes is optional. For procedures about modifying hardware-enforced DEP support for 32-bit processes, see the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

Recommended Actions Before and After Configuration Changes

Before installing any service pack or post-SP security update, it is strongly recommended that the system be backed up to provide a speedy method for restoring the system to a "known good" condition in the event of a problem. After the updates are installed successfully and tested to ensure there are no problems, a new system backup should be created to ensure the latest configuration can be restored in the event of a future problem.

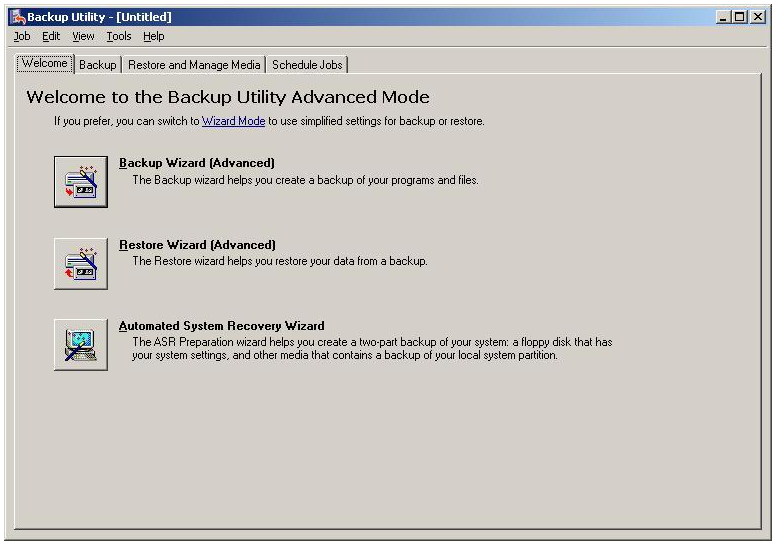
In Windows Server 2000, an Emergency Repair Disk (ERD) can be created to enable administrators to recover the system in the event of damage. In Windows Server 2003, the ERD has been replaced by an Automated System Recovery (ASR) disk. The ASR disk contains the information necessary to fix system files, the boot sector, and the startup environment.

ASR Backup Procedure

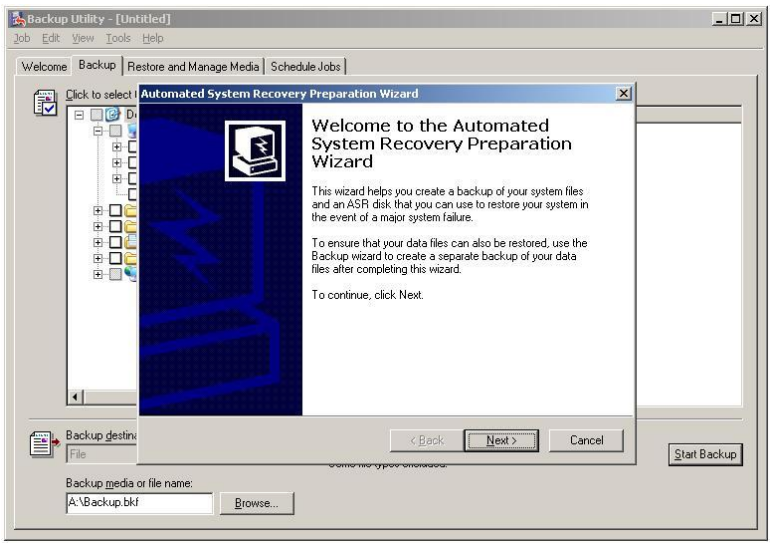
To create a system backup using ASR

1. Close all applications.
2. Click **Start**, point to **All Programs**, point to **Accessories**, click **System Tools**, and then select **Backup**. The Backup or Restore Wizard is displayed.

3. Click the **Advanced Mode** link. The Backup Utility appears.

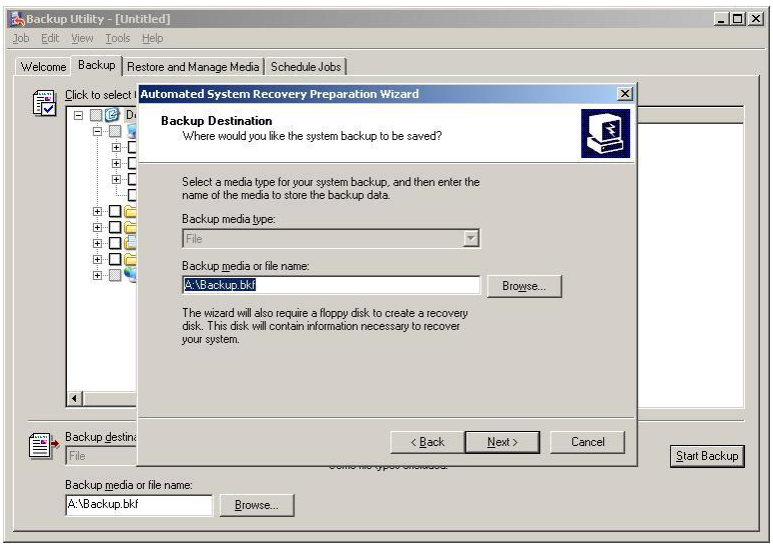


4. On the **Welcome** tab, click **Automated System Recovery Wizard**.

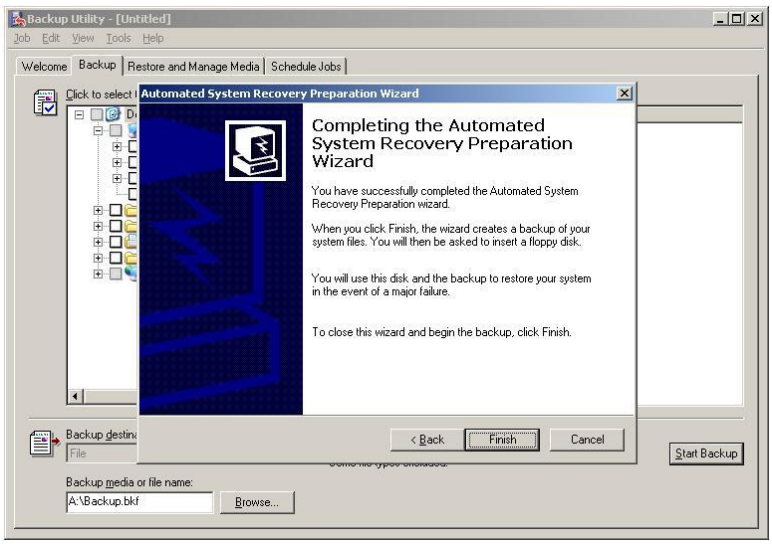


5. Follow the steps prescribed by the wizard to create backup media of critical operating system files and a floppy disk that can be used to restore the system. The wizard first creates a backup of the system partition.

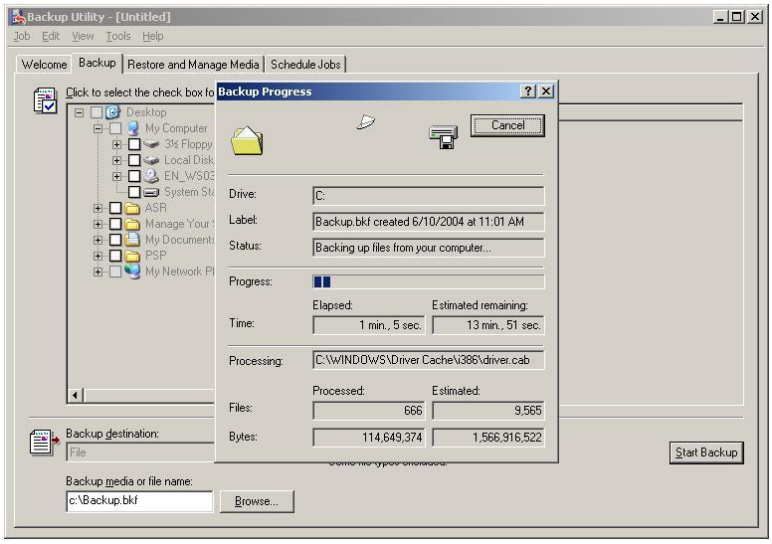
Note: By default, the initial backup destination for the system files is shown as the A: drive. This must be changed to a backup location that provides sufficient space to back up the local system partition. Do not place the backup on the local system partition.



6. After entering a backup location, click **Next**, and then click **Finish**.



7. The system backup begins.



8. After the system backup is complete, a message appears prompting for a formatted floppy disk for storing recovery information. Insert a blank floppy disk and click **OK** to complete the ASR preparation process.

9. Close all windows when the ASR is completed. The files created are described in Table 3.5.

Table 3.5 Windows Server 2003 system recovery files

File Name	Contents
Backup.bkf	File containing a backup of the local system partition.
Asr.sif	Automated system recovery state information file.
Asrpnp.sif	Automated system recovery plug and play devices state information file.
Setup.log	A log of which files were installed and of Cyclic Redundancy Check (CRC) information for use during the emergency repair process.

ASR Restore Procedure

System restoration can be performed by initiating Windows Setup and pressing the **F2** key when prompted during the text mode portion of Setup. ASR reads the disk configurations from the file that it creates and restores all of the disk signatures, volumes and partitions on the disks required to start the computer. (The ASR program attempts to restore all of the disk configurations, but under some circumstances, it might not be able to.) ASR then installs a simple installation of Windows and automatically starts a restoration using the backup created by the ASR wizard.

To recover from a system failure using Automated System Recovery

Ensure that the following items are available before beginning the recovery procedure:

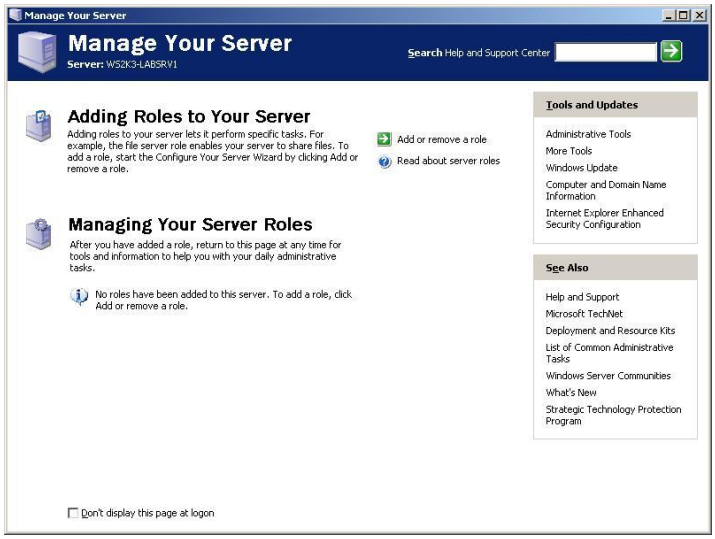
- The previously created ASR floppy disk;
- The previously created backup media (Backup.bkf); and
- The original Windows operating system Setup CD.

1. Insert the Windows Setup CD into the CD-ROM drive.
2. Restart the computer. If prompted to press a key in order to start the computer from CD, press the appropriate key.
3. If a SCSI driver is required, press **F6**. Setup will prompt for the SCSI driver when needed.
4. Press **F2** when prompted during the text–only mode section of Setup. Setup prompts the user to insert the ASR floppy disk previously created.
5. Follow the directions on the screen to complete the system restoration.

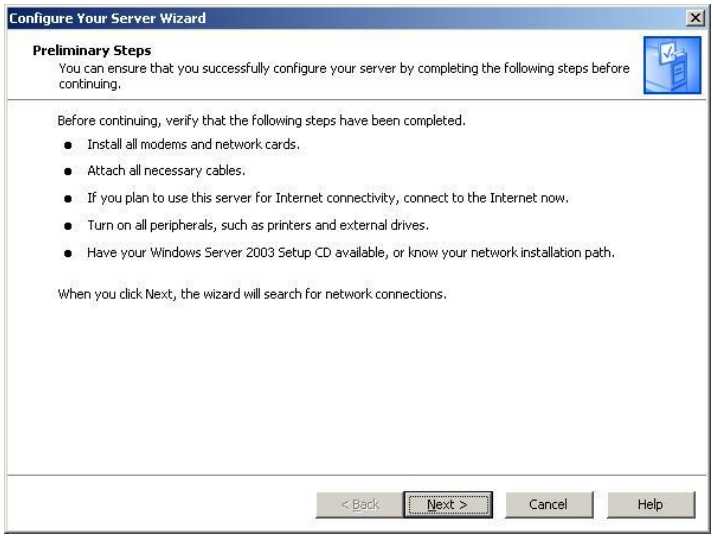
Note: ASR does not restore data files.

Configuring Windows Server 2003 Roles

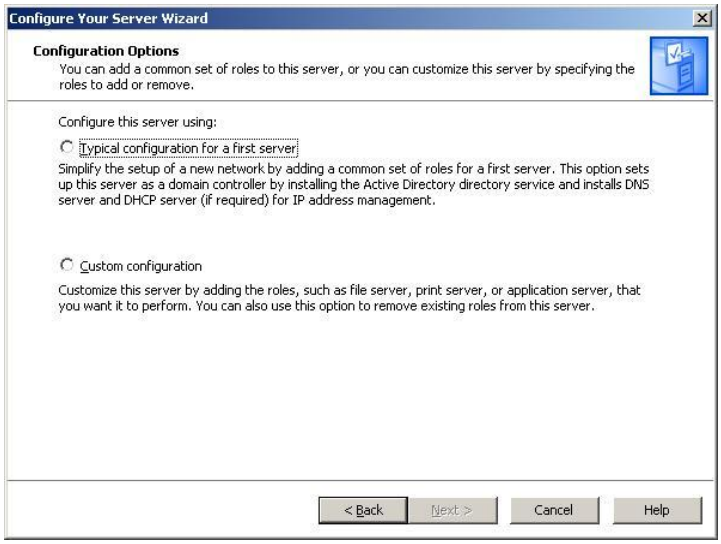
When Setup completes, the computer restarts. Setup has now performed the basic installation. When an administrator logs on, the Manage Your Server interface appears on the screen. This interface is also accessible from the **Administrative Tools** menu. Use it to easily configure the server for specific roles and to manage server roles.



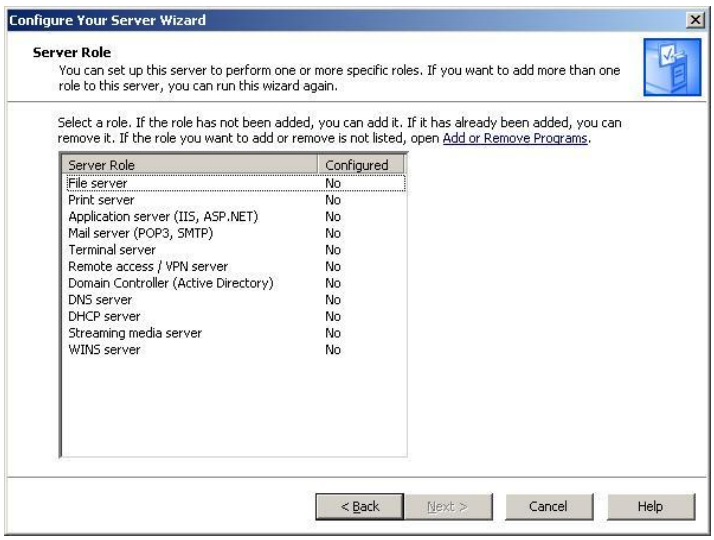
1. If the Manage Your Server interface is not already displayed, click **Start**, point to **Administrative Tools**, and then click **Manage Your Server**.
2. Click the **Add or remove a role** link to open the Configure Your Server Wizard. Simply follow the instructions provided by the wizard to add or remove a server role to the computer.



3. For a first installation, the Configure Your Server Wizard provides two options to configure the server:
   - **Typical configuration for a first server**. Use this option to set up the first domain controller in a network. After the first domain controller has been installed, this option is no longer available.



   - **Custom configuration.** Use this option to configure a specific server role, as described in Table 3.6.
4. Follow the instructions on the screen to configure the server.



Start Manage Your Server at any time by clicking **Start**, pointing to **Administrative Tools**, and then clicking **Manage Your Server**.

Table 3.6 Server role configuration options

Server Role	Description
File Server	File servers provide and manage access to files. Configure this computer as a file server if it will be used to store, manage, and share information such as files and network-accessible applications.
Print Server	Configure this computer as a print server if it will be used to manage printers remotely, manage printers by using Windows Management Instrumentation (WMI), or print from a server or client computer to a print server by using a Uniform Resource Locator (URL) address.
Application Server	An application server provides key infrastructure and services to applications hosted on a system. Typical application servers include the following services: ▪ Resource pooling (for example, database connection pooling and object pooling) ▪ Distributed transaction management ▪ Asynchronous program communication, typically through message queuing ▪ A just-in-time object activation model ▪ Automatic Extensible Markup Language (XML) Web Service interfaces to access business objects ▪ Failover and application health detection services ▪ Integrated security **Note:** Configuring this server as an application server requires installing IIS along with other optional technologies and services such as COM+ and ASP.NET. The verion of ASP.NET installed by the Configure Your Server Wizard is version 1.1, which is not in the TOE. The Wizard provides no options for excluding ASP.NET 1.1 from the installation. Therefore, when installing IIS, do not use the Configure Your Server Wizard. Instead, follow the procedures in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*. The IIS installation procedures in the Administrator's Guide use the Add or Remove Programs interface to install IIS, which allows the option of excluding ASP.NET.

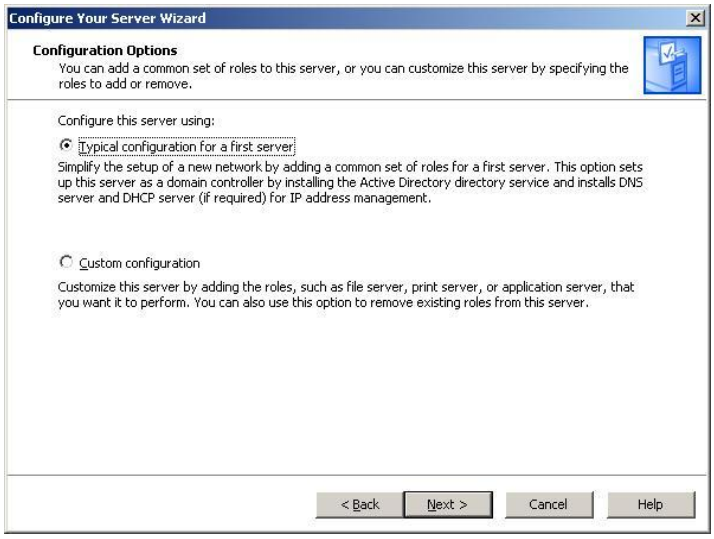
Server Role	Description
Mail Server	To provide e-mail services to users, use the Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) components included with Windows Server 2003. The POP3 service implements the standard POP3 protocol for mail retrieval, and can be paired with the SMTP service to enable mail transfer. **Note:** The Mail Server role is not included in the TOE.
Terminal Server	Terminal Server is used to provide a single point of installation that gives multiple users access to any computer that is running a Windows Server 2003 operating system. Users can run programs, save files, and use network resources all from a remote location, as if these resources were installed on their own computer **Notes:** ▪ The Terminal Server role is not included in the TOE. ▪ If a Terminal Server role is configured, Terminal Server Licensing and Terminal Server License Server must also be configured. Otherwise, the terminal server will stop accepting connections from unlicensed clients when the evaluation period ends 120 days after the first client logon.
Remote Access / VPN Server	Routing and Remote Access provides a full-featured software router and both dial-up and virtual private network (VPN) connectivity for remote computers. It offers routing services for local area network (LAN) and wide area network (WAN) environments and enables remote or mobile workers to access corporate networks either through dial-up connection services or over the Internet by using VPN connections. **Note:** Remote Access / VPN Server roles are not included in the TOE.
Domain Controller (Active Directory)	Configure this server as a domain controller to provide the Active Directory service to manage users and computers. In an Active Directory forest, a domain controller is a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources. Administrators can manage user accounts, network access, shared resources, site topology, and other directory objects from any domain controller in the forest.
DNS Server	The DNS is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database. After setting configuring the DNS Server role, apply the update described in Apply the Domain Name System (DNS) server service Security Update.
DHCP Server	DHCP is an IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on a network. Configure this server as a DHCP server to perform multicast address allocation, and obtain client IP address and related configuration parameters dynamically.
Streaming Media Server	Streaming media servers are used to provide Windows Media Services to organizations. Windows Media Services manages, delivers, and archives Windows Media content, including streaming audio and video, over an intranet or the Internet. **Note:** The Streaming Media Server role is not included in the TOE.
WINS Server	WINS servers map IP addresses to Network Basic Input Output System (NetBIOS) computer names and NetBIOS computer names back to IP addresses. With WINS, servers can be used to search for resources by computer name instead of IP address, which can be easier to remember.

Convert a Windows Server 2003 to a Domain Controller

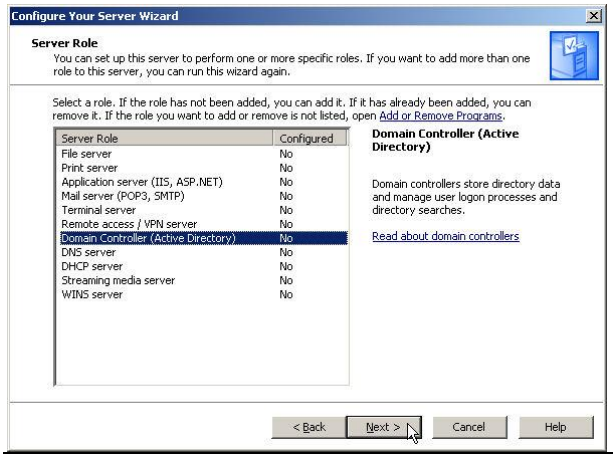
It is possible to convert a Windows Server 2003 computer to domain controller after server installation has been completed.

To promote a server to a domain controller

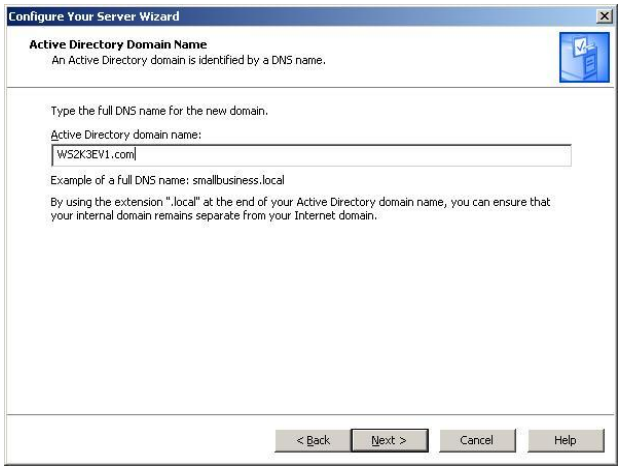
1. Log on as an authorized administrator.
2. If the Manage Your Server interface is not already displayed, click **Start**, point to **Administrative Tools**, and then click **Manage Your Server**.
3. Click the **Add or remove a role** link. When the Configure Your Server Wizard appears, click **Next**. Select the **Typical configuration for a first server** radio button and click **Next**.



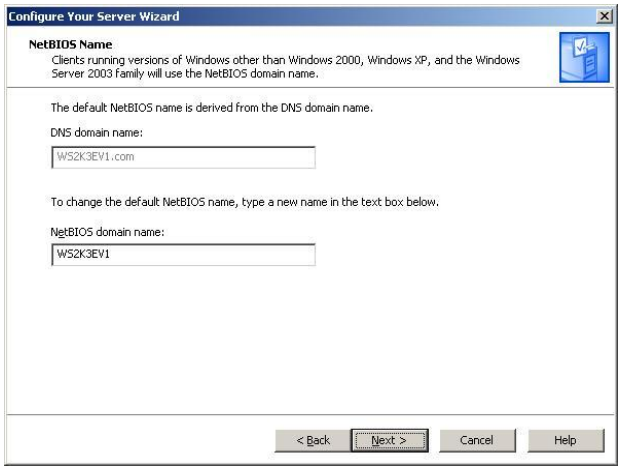
Note: If the wizard detects other servers on the network, the Configuration Options view shown here does not appear. Instead, the **Server Role** view of the wizard appears to enable custom configuration. To install Active Directory, select **Domain Controller (Active Directory)** and click **Next**. Click **Next** on the **Summary of Selections** page. The Active Directory Installation Wizard appears. Follow the directions to install Active Directory. For detailed procedures about using the Active Directory Installation Wizard, see the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.



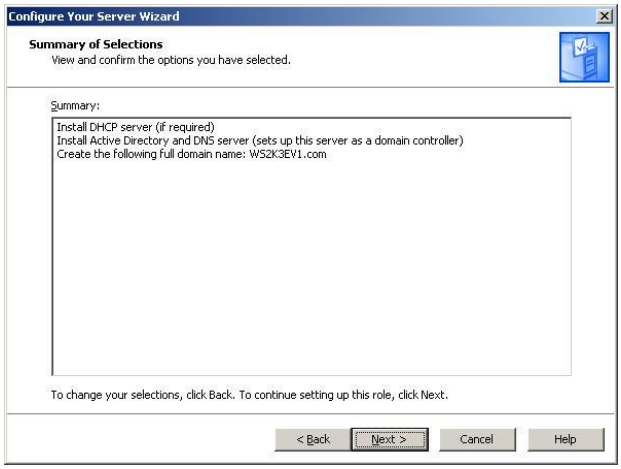
4. Enter a full DNS name for the new domain and click **Next**.



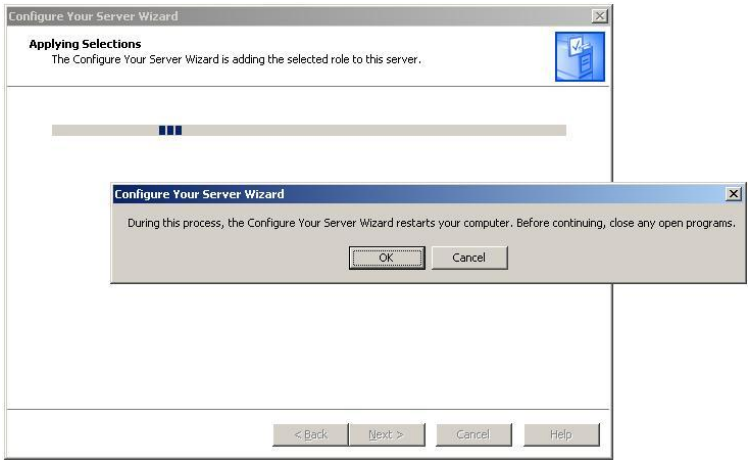
5. Review and accept the default NetBIOS name and click **Next**.



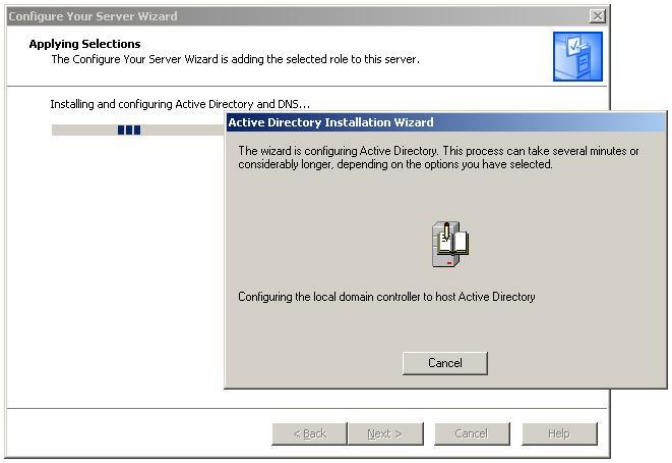
6. A summary of the server roles required to configure the domain controller role on this computer appears. Click **Next** to continue.



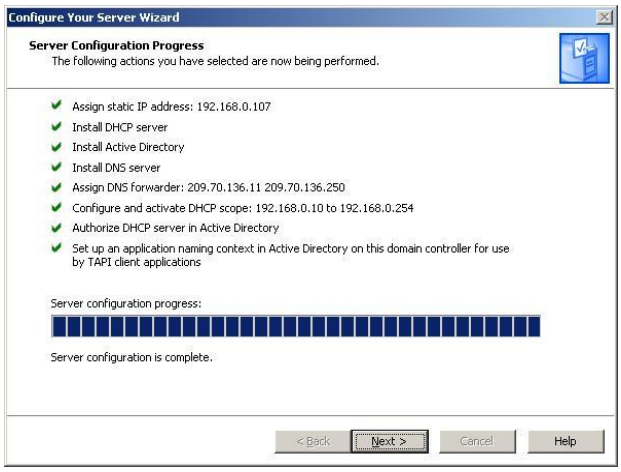
7. The wizard begins applying the selected configuration options to the computer. A message appears stating that the Configure Your Server Wizard will restart the computer and advising that any open programs be closed at this time. Ensure that no other programs are open and click **OK**.



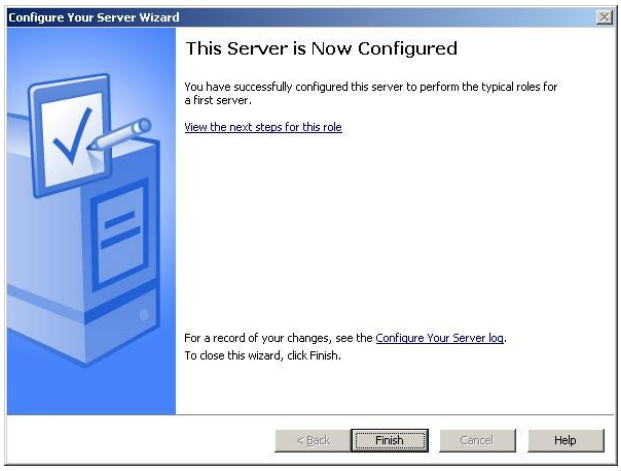
8. During the installation process, the Active Directory Installation Wizard appears. Do not click the Cancel button. When the installation completes, the computer automatically restarts.



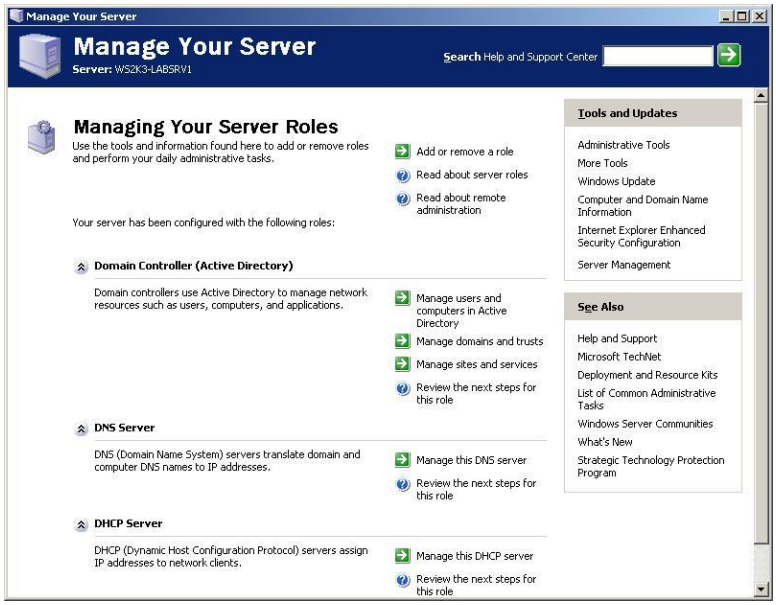
9. After the computer has restarted, log on as an authorized administrator. The Configure Your Server Wizard appears to perform the final configuration of the server. When the server configuration is finished, click **Next**.



10. When the Configure Your Server Wizard indicates that the server is now configured, click **Finish**.



11. The Manage Your Server interface is displayed, and it includes management options for each of the server roles installed during the configuration of the domain controller.



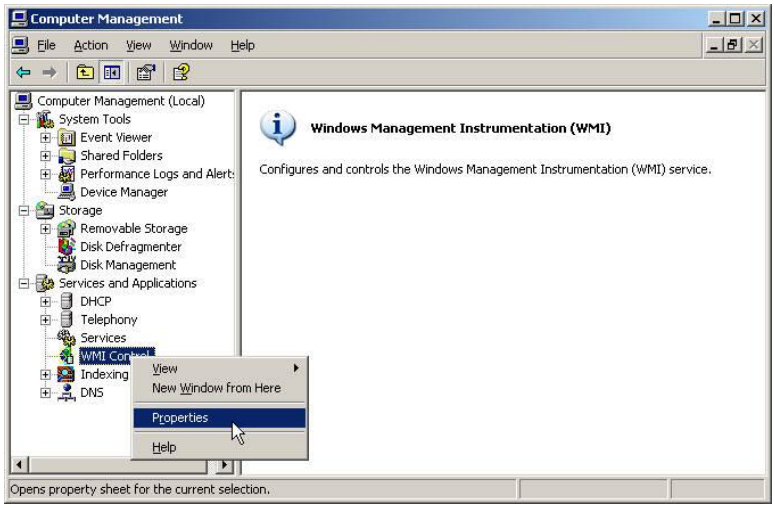
12. By default, DNS is installed on the first domain controller. If the DNS role has been configured on the domain controller, install the DNS Secuirty Update described in Apply the Domain Name System (DNS) server service Security Update.

Installation Modifications

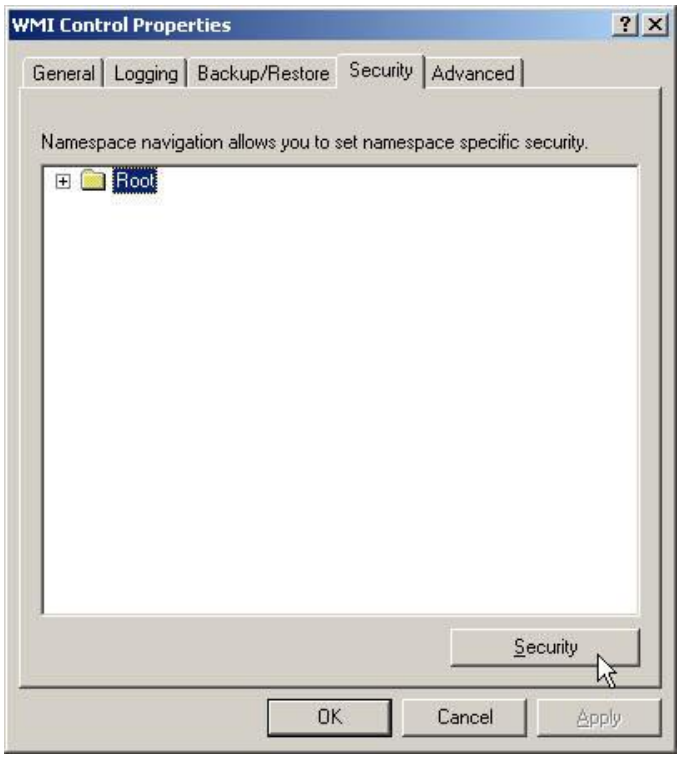
Setting Permissions for WMI Filters

Change Windows Management Instrumentation (WMI) filters permissions to remove access by the Everyone group and to prevent non-administrative accounts from using the Resultant Set of Policy (RSOP) tool as follows:

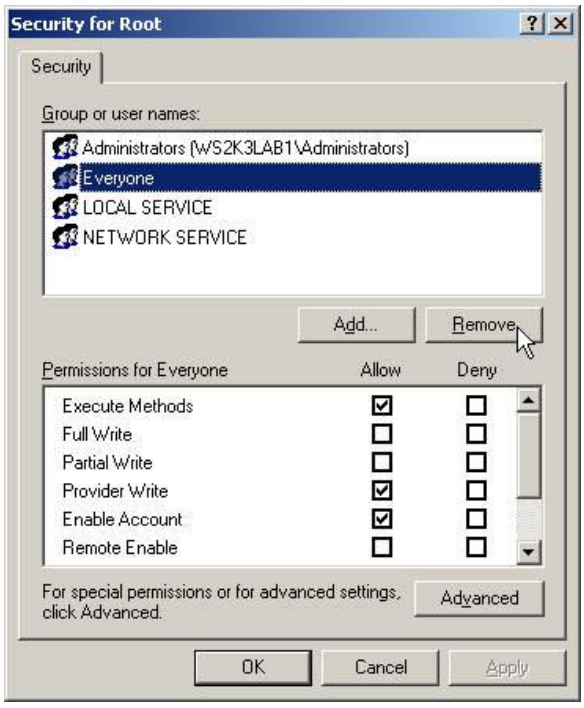
1. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
2. In the Computer Management interface, expand **Services and Applications**.
3. Select and then right-click **WMI Control**. Select **Properties** from the menu.



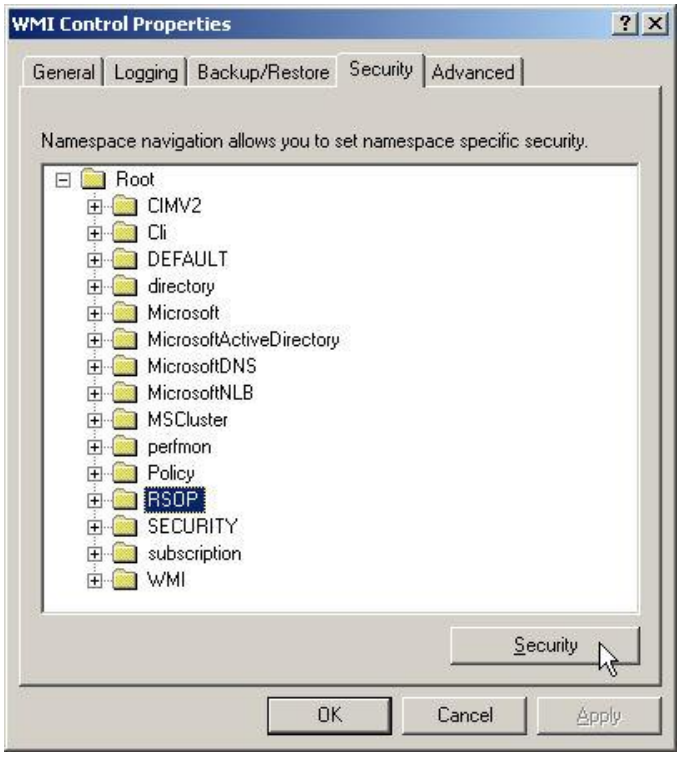
4. Click the **Security** tab on the WMI Control Properties interface.
5. Select the **Root** folder, and then click the **Security** button.



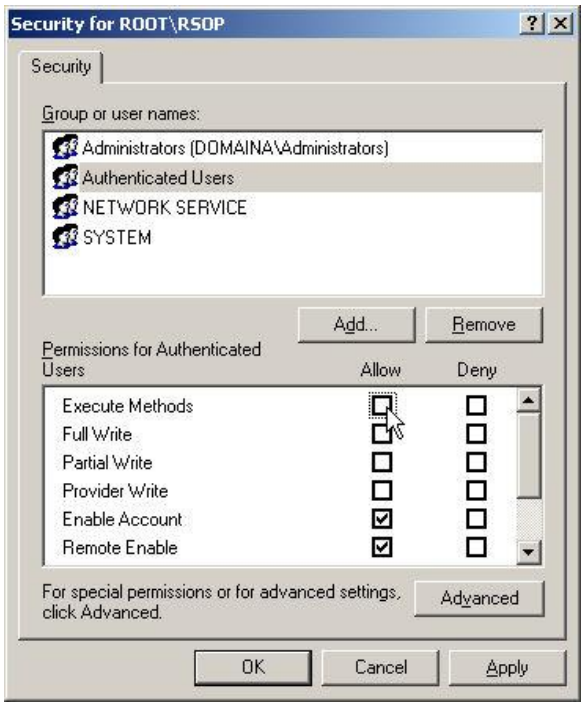
6. Select the **Everyone** group and click the **Remove** button. Click **OK**



7. Expand the **Root** folder on the WMI Control Properties interface. Select the **RSOP** subfolder and then click the **Security** button.



8. Select the **Authenticated Users** group and remove the **Execute Methods** permission for that group by clearing the corresponding check box under the **Allow** column. Click **OK**.

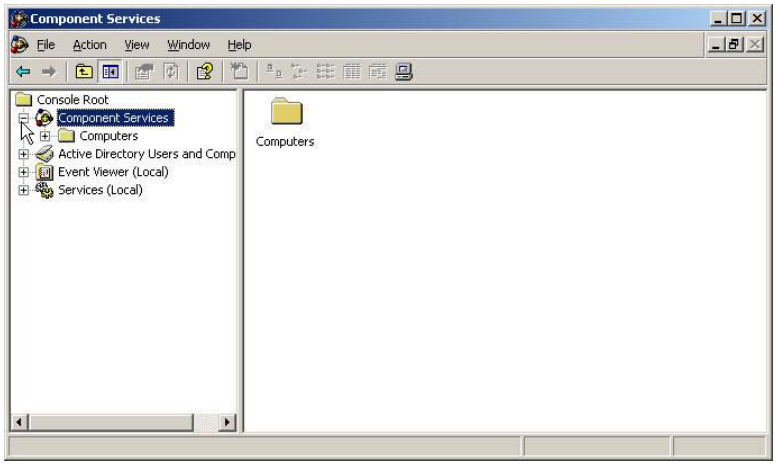


9. Click **OK** to close the WMI Control Properties interface, and then close the Computer Management interface.

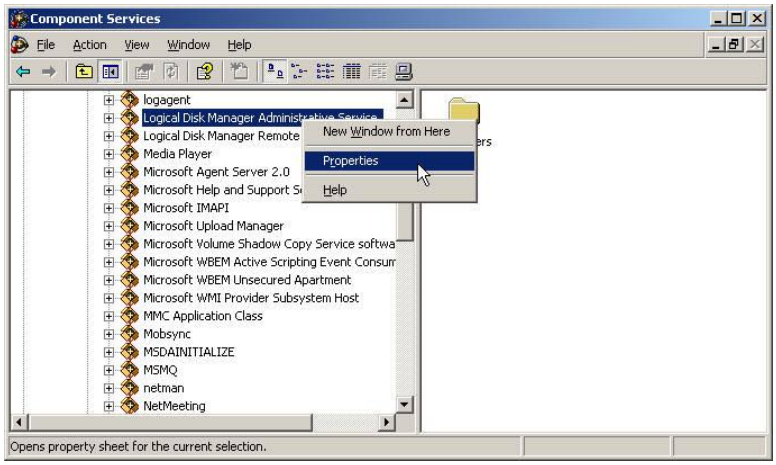
Restricting Launch and Access Permissions for Logical Disk Manager

Restrict Launch and Access permissions for the Logical Disk Manager to administrative and SYSTEM accounts as follows:

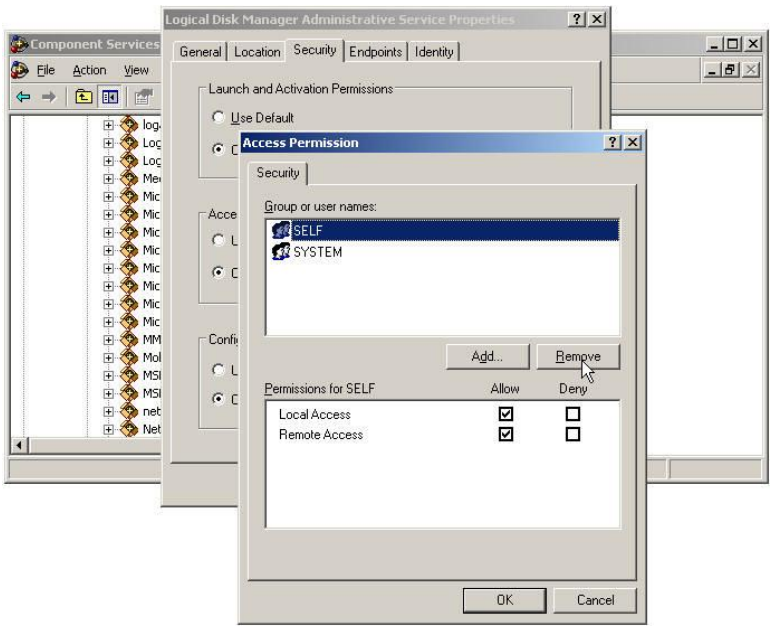
1. Click **Start** and select **Run**.
2. Type **dcomcnfg** and click **OK**.
3. In the Component Services interface, expand the **Component Services** node.



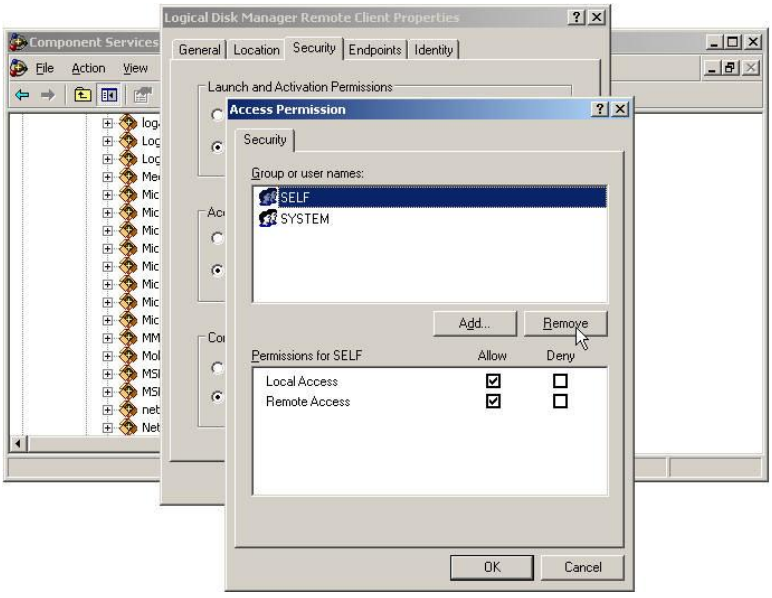
4. Expand the **Computers** folder, expand the **My Computer** node, and expand the **DCOM Config** folder.
5. Right-click **Logical Disk Manager Administrative Service** and select **Properties**.



6. Click the **Security** tab of the Logical Disk Manager Administrative Service Properties interface.
7. In **Access Permissions**, select the **Customize** radio button and click **Edit**.
8. Select the **SELF** account and click **Remove**. Click **OK** twice.



9. Right-click **Logical Disk Manager Remote Client** and select **Properties**.
10. Click the **Security** tab of the Logical Disk Manager Remote Client Properties interface.
11. Under **Access Permissions**, select the **Customize** radio button and click **Edit.**
12. Select the **SELF** account and click **Remove**. Click **OK** twice.

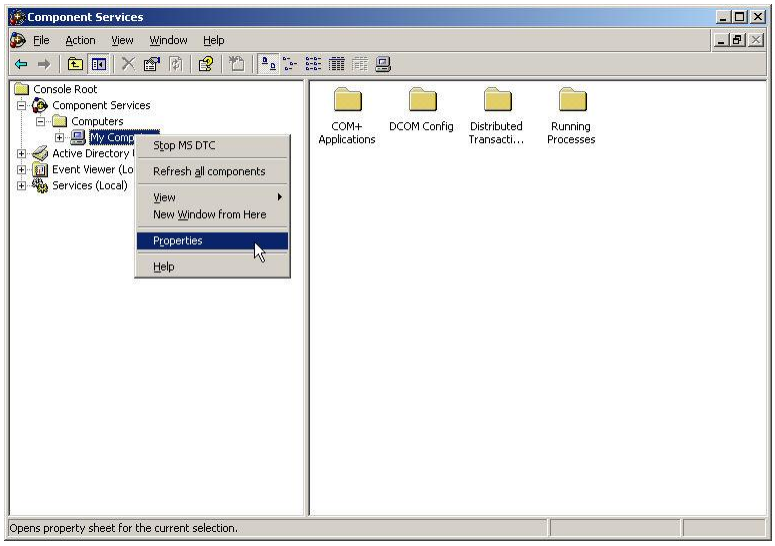


13. Close the Component Services interface.

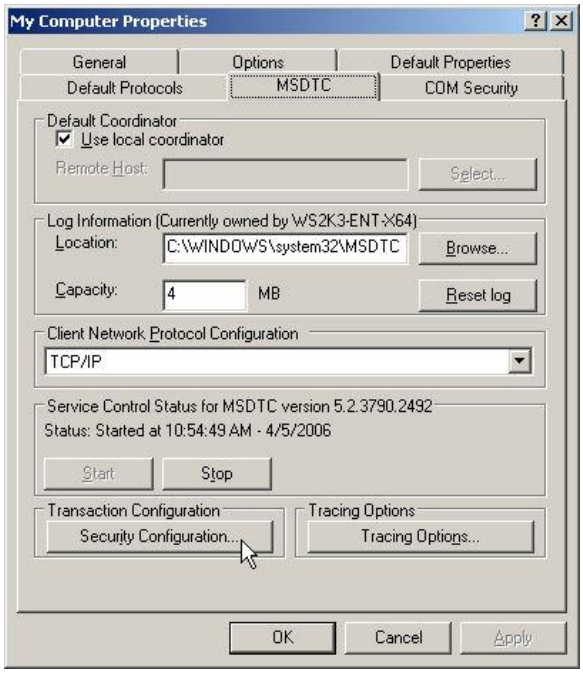
Configuring Distributed Transaction Coordinator Access

To configure the security setting for the Distributed Transaction Coordinator

1. Click **Start** and select **Run**.
2. Type **dcomcnfg** and click **OK**.
3. In the Component Services interface, expand the **Component Services** node.
4. Expand the **Computers** folder, then right-click the **My Computer** node and select **Properties**.

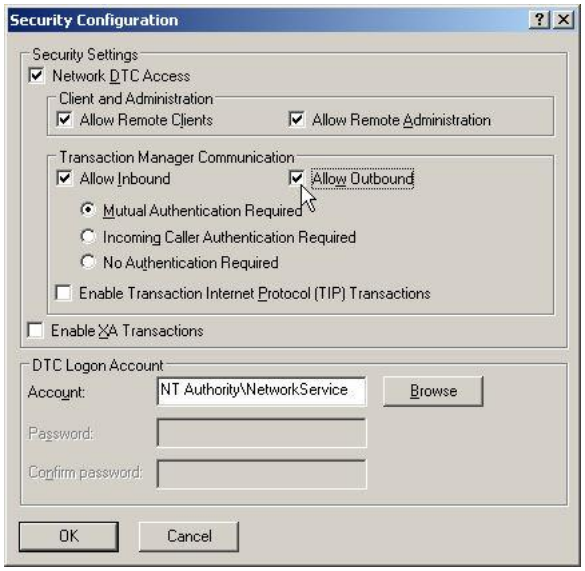


5. On the My Computer Properties interface, click the **MSDTC** tab and then click the **Security Configuration** button.

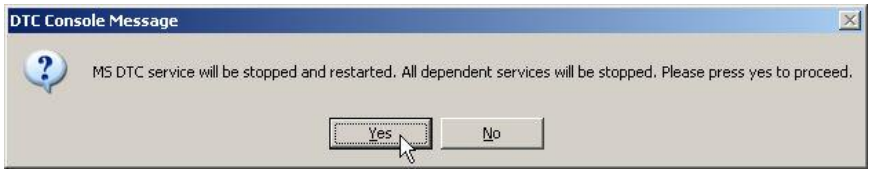


6. In the Security Configuration interface, if Network DTC Access is desired for the Evaluated Configuration, select the **Network DTC Access** check box, and then select the **Allow Remote Client, Allow Remote Administration**, **Allow Inbound**, and **Allow Outbound** check boxes. Select the **Mutual Authentication Required** radio button.
7. The **Enable Transaction Internet Protocol (TIP) Transactions** and **Enable XA Transactions** options **must not be** selected. Click **OK** on the Security Configuration interface.

Note: The Evaluated Configuration does not prohibit Network DTC Access if it is desired for a particular computer on the TOE network. Likewise, the Evaluated Configuration does not mandate Network DTC Access if it is not desired for a particular computer on the TOE network.



8. A message appears indicating that the MS DTC service will be stopped and restarted. Click **Yes**.



9. A message appears indicating that the MS DTC has been restarted. Click **OK**.

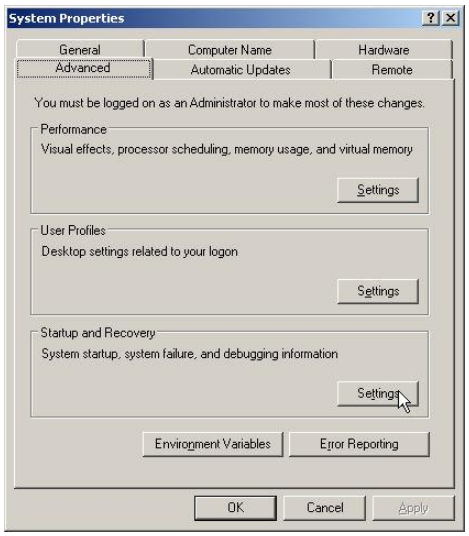
10. Click **OK** on the My Computer Properties interface and close the Component Services interface.

Disabling the Creation of Dump Files

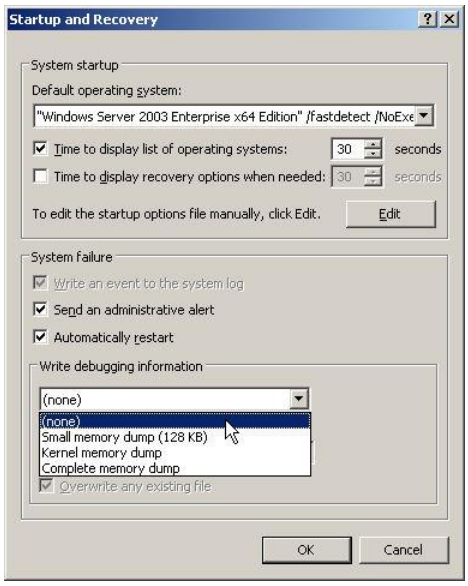
Microsoft Windows Server 2003 writes debugging information to a dump file when the computer stops unexpectedly as a result of a Stop error (also known as a "blue screen", system crash, or bug check). Dump files are useful for troubleshooting. However, there are system memory dumps that might contain sensitive information, such as passwords that can be compromised if the dump file is accessed by an unauthorized user. To prevent the writing of sensitive information to dump files, the creation of dump files must be disabled. This feature can be enabled temporarily by an authorized administrator for troubleshooting purposes, but must be disabled after the issue is resolved in order to remain compliant with the Evaluated Configuration.

To disable the creation of dump files

1. Click **Start**, right-click **My Computer** and select **Properties.**
2. On the **Advanced** tab of the System Properties interface, click the **Settings** button under **Startup and Recovery**.



3. On the **Write debugging information** pull-down menu, select **(none)** and click **OK**. If a message appears indicating that the system needs to be restarted, click **OK**.



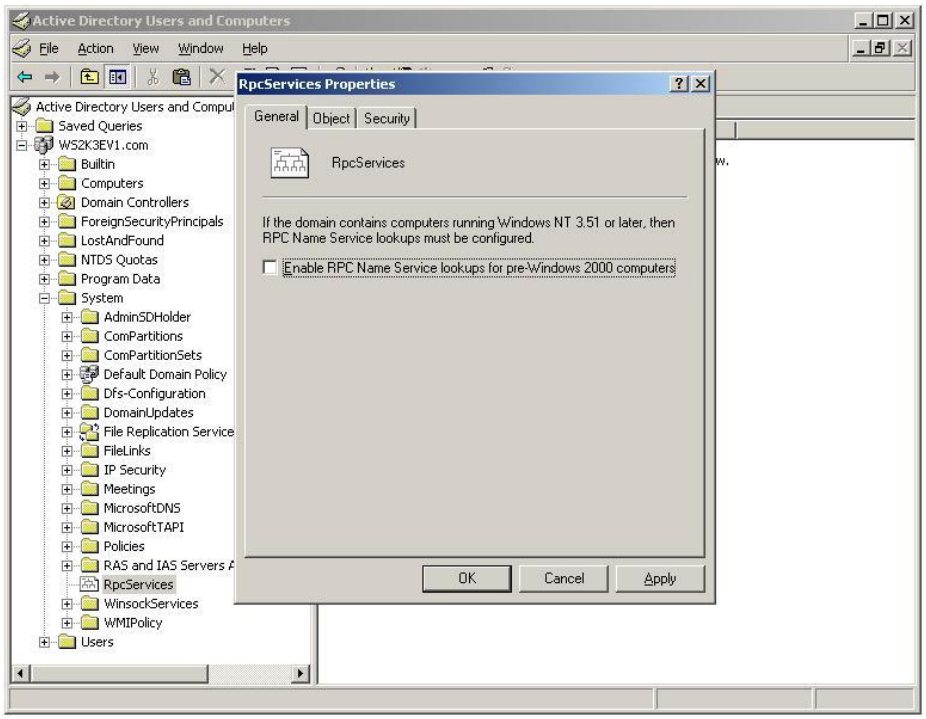
4. Click **OK** on the **Systems Properties** page. Restart the computer.

Disabling RPC Locator Subcomponent in Active Directory

On Windows Server 2003 domain controllers, the Remote Procedure Call (RPC) Locator's ability to optionally support RPC Name Service lookups for pre-Windows 2000 computers must be disabled.

To disable RPC Name Service lookups for pre-Windows 2000 computers

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
2. From the **View** menu, select **Advanced Features**.
3. Expand the **Domain** node and then expand the **System** container.
4. Right-click **RpcServices** and select **Properties**.
5. Under the General tab, clear the check box for **Enable RPC Name Service lookup for pre-**Windows 2000 **computers** and click **OK**.



6. Close all windows and restart the domain controller.

Preventing the Automatic Installation of Device Drivers

By default, Windows Server 2003 stores many driver files in the %SystemDirectory%\drivers (C:\Windows\system32\drivers) folder. The Information files (.inf files), in the %SystemRoot%\inf (C:\Windows\inf) folder, contain instructions for installing the drivers. The availability of these drivers allows for the automatic installation of devices when plugged into a Universal Serial Bus (USB) port.

For the Evaluated Configuration, there are two issues associated with the automatic installation of drivers. First, there is the potential that a device requiring a driver that is not allowed in the Evaluated Configuration might be plugged into a USB port; in this case, the driver is installed automatically by Windows. Second, the Plug and Play service can install drivers using SYSTEM account credentials, thus allowing a driver to be installed when a user with no administrative rights plugs a device into the USB port.

This section provides procedures for moving .inf files to an alternate location in order to prevent the automatic installation of drivers. Because the .inf files contain instructions for installing drivers, the drivers cannot be installed automatically if the Plug and Play service cannot find the .inf files. Instead, the Found New Hardware Wizard, which requires administrator credentials, runs to guide in the installation. The authorized administrator can then point the wizard to the new location of the .inf files and the default %SystemDirectory%\drivers folder to complete the installation. Additionally, procedures are provided to move the Drivers.cab and SP2.cab files to an alternate location because the Plug and Play service might also search these .cab files to find and automatically install drivers.

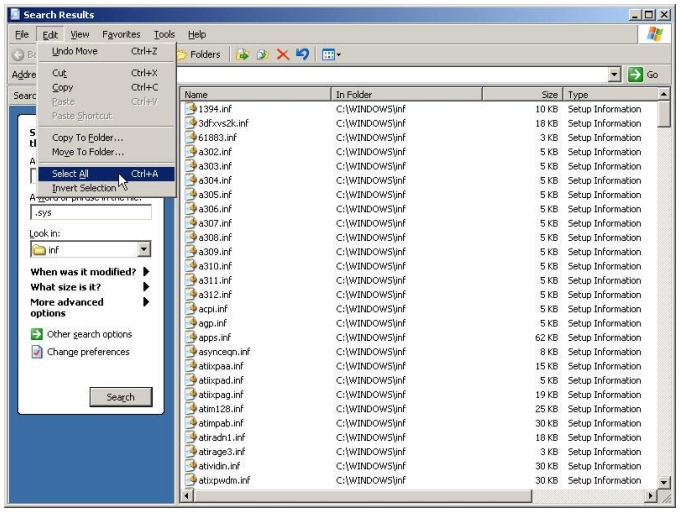
To prevent the automatic installation of drivers and require the use of the New Hardware Found Wizard by an authorized administrator

Notes:

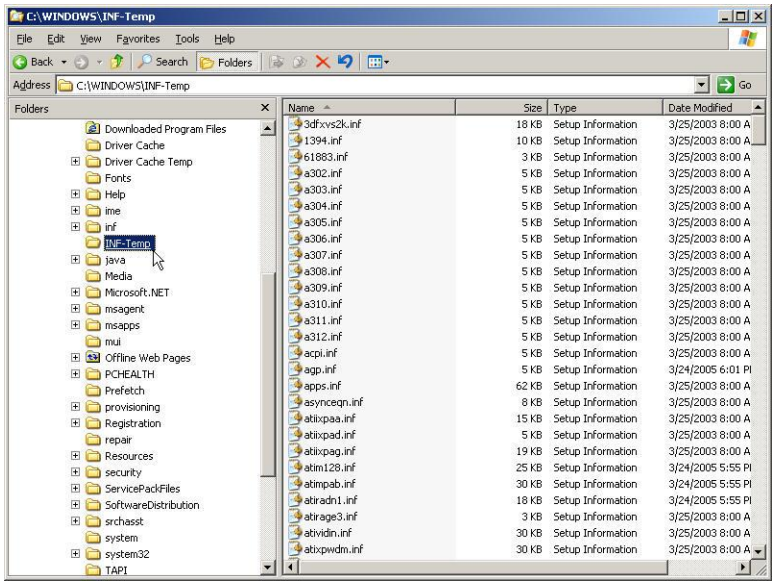
Moving .inf and .cab files might impact the ability of the Windows Components Wizard and the New Hardware Found Wizard to automatically locate necessary files when installing a new Windows component or device. If this occurs, the Wizard might need to be pointed to the location of the drivers and the administrator might need to extract some files from the .cab stores. To prevent this, install and configure all Windows components or devices prior to moving the .inf and .cab files as described in the procedures below.

The recommended procedure for installing a Windows component or device at a later time is to temporarily take the system out of the Evaluated Configuration by moving the .inf and .cab files back to their default location, install the device or component, and then set the system back to the Evaluated Configuration by following the procedures below.

1. Click **Start** and select **Windows Explorer**.
2. Expand **My Computer**, expand the system partition (C:\ by default), and then expand the Windows folder.
3. Select the **Windows** folder to show the contents of the folder in the details pane.
4. From the **File** menu, point to **New** and select **Folder**.
5. Create two folders: name one **INF-Temp**, and name the other **Driver Cache Temp**.
6. Select the %SystemRoot%\Driver Cache folder and move its i386 (also amd64 or ia64 in 64-bit operating systems) subfolder to the new %SystemRoot%\Driver Cache Temp folder. This moves the Drivers.cab and SP2.cab files contained in the i386 folder out of their default location.
7. Right-click the %SystemRoot%\inf folder and select **Search** to open the Search Results tool.
8. In the **A word or phrase in the file** text box, type **.sys**, and then click the **Search** button. The Search Results tool searches for all files in the %SystemRoot%\inf folder that contain a driver reference and lists them in the results pane.
9. From the **Edit** menu, click the **Select All** option. This selects all of the files in the results pane.



10. To move all of the resulting files to the newly created %SystemRoot%\INF-Temp folder, left-click the selected files, drag them to the %SystemRoot%\INF-Temp folder, and release the mouse button to drop them there. All files containing driver references are moved out of the default %SystemRoot%\inf folder and into the to the new %SystemRoot%\INF-Temp folder.



Note: As a result of these procedures, when a user logs on for the first time, a "Failed to install" message might appear. This occurs because the user's profile is being created and the system is attempting to install the Address Book application for the user. The Address Book application cannot be installed because the system cannot find the necessary files. Instruct users to click **OK** on the message to continue. The Address Book application is not included in the TOE.

The following example demonstrates the procedure used to install drivers for a USB-based device after the corresponding .inf files and the driver .cab files have been moved from their default location.

Notes:

Appendix G of this document provides a list of drivers that are allowed in the Evaluated Configuration. Prior to attaching a device to a USB port, administrators can check that any drivers required by the device are identified in the list of allowed drivers.

The recommended procedure for installing a device at a later time is to temporarily take the system out of the Evaluated Configuration by moving the .inf and .cab files back to their default location, installing the device, and then setting the system back to the Evaluated Configuration.

To install drivers for a USB device after the .inf and .cab files have been relocated

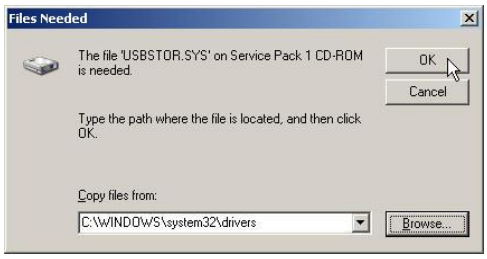
1. Plug the device into a USB port.
2. The Plug and Play Service attempts to find the device drivers by searching the %SystemRoot%\inf folder for a driver reference. It will not find a driver reference and, as a result, the Found New Hardware Wizard appears. Select the **No, not at this time** radio button and click **Next**.

3. Select the **Install from a list or specific location (Advanced)** radio button and click **Next**.
4. If not required, clear the **Search removable media (floppy, CD-ROM…)** check box and select the **Include this location in the search** check box.
5. Enter the path to the %SystemRoot%\INF-Temp folder or click the **Browse** button to find and select the %SystemRoot%\INF-Temp folder. Click **Next**.

6. The Found New Hardware Wizard searches the %SystemRoot%\INF-Temp folder for an INF file containing a driver reference. When a file is found, a message might appear indicating that the driver has not passed Windows Logo testing. This occurs because the .inf files were moved from their default location and the Plug and Play Service cannot find the matching Windows Logo certificate. Click **Continue Anyway**.

7. The Files Needed interface might appear, requesting the location of the driver files. Enter the path to the %SystemDirectory%\drivers folder or click the **Browse** button to find and select the %SystemDirectory%\drivers folder. Click **OK**.

Note: It might be necessary to search for the drivers in a different location and point the wizard to that location.



8. The Found New Hardware Wizard interface indicates when the driver installation is finished. Click **Finish** to close the wizard. Restart the computer if necessary.

Note: Unless a second device is being installed, click **Cancel** if the Found New Hardware Wizard appears a second time.

4. Windows Firewall Settings

Windows Firewall is a stateful filtering firewall for Windows Server 2003. It provides protection for PCs connected to a network by rejecting unsolicited inbound connections through TCP/IP version 4 (IPv4) and Internet Protocol version 6 (IPv6). In Windows Server 2003, the Windows Firewall is disabled by default.

For enterprise networks, enabling Windows Firewall on all network connections on servers can have a significant impact on the types of communication that can occur. If the Windows Server 2003 computers are only running client-based programs, then the Windows Firewall cannot impair communications. Web access, email, Group Policy, and management agents that request updates from a management server are examples of client-based programs. For client-based programs, the client computer always initiates the communication and all response traffic from a server is allowed by Windows Firewall because it is solicited incoming traffic.

However, the consequences to blocking all unsolicited incoming traffic by default can affect network services if the computers running Windows Server 2003 are managed, and are providing network services that require clients to initiate contact with the server such as file services, application hosting, print services, etc. To prevent this from happening, a Windows Server 2003 server that has the Windows Firewall enabled must be configured with the appropriate Windows Firewall exception settings to allow the computer to act as a managed computer and provide access to the services it is providing for the network.

Windows Server 2003, SP2 includes a Security Configuration Wizard (SCW) that facilitates configuration of Windows Firewall to allow support for specific types of network services hosted by the server. For procedures to enable and configure the Windows Firewall on Windows Server 2003 and procedures for using SCW to configure Windows Firewall to support specific server roles, see the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

5. Secure Configuration

This section provides detailed procedures for making security configuration changes to the standard install base of Windows Server 2003 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 Server 2003 (both as a stand-alone computer and as a domain member), IIS 6.0, and domain controller configurations. The domain controller settings defined in the document tables apply only to a Domain Controller Security Policy.

Chapter 8 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 Server 2003 Security Configuration Checklist is provided in Appendix E of this document.

Windows Server 2003 Security Policies

This section explains the various security policy tools and their order of precedence regarding application of security policies. By default, Group Policies are inherited and cumulative, and they 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 are applied in a standard order: LSDOU, which stands for (1) local, (2) site, (3) domain, (4) organizational unit, with the later policies being superior to the earlier applied policies. Local Group Policy Objects are processed first, and then level domain policies. If a computer is participating in a domain and a conflict occurs between the domain and local computer policies, the domain policy prevails. However, if a computer is no longer participating in a domain, the local Group Policy Object is applied.

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 if the default DC GPO has the same privilege configured differently. Because Group Policies are inherited cumulatively, the effective settings of domain controllers would include those specified by the default Domain GPO plus any overriding settings specified in the default DC GPO.

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.

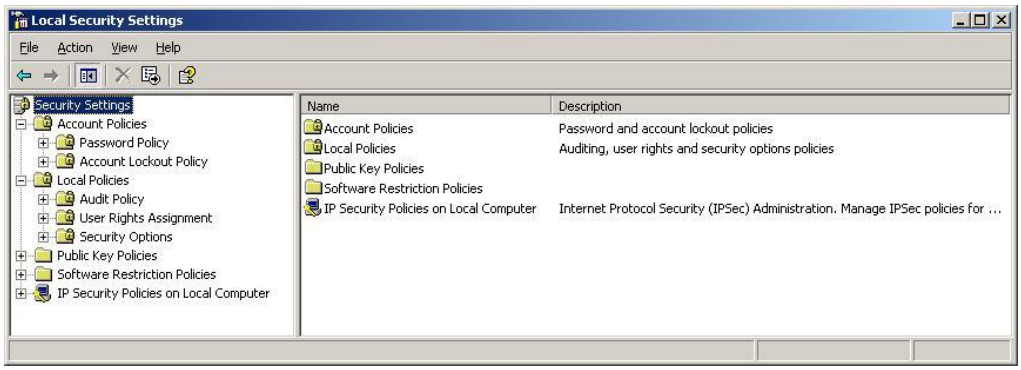
Local Security Settings Interface

The Local Security Settings interface 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 that does not receive a full set of policies from the domain. Within an Active Directory-managed network the Local Security Policy applied by the Local Security Settings interface has the least precedence with respect to policy. Therefore, if the computer is a member

of a domain, the settings within the Local Security Settings interface can be overridden by policies received from the domain.

To open the Local Security Settings interface

1. Log on to the computer as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the Local Security Settings interface.



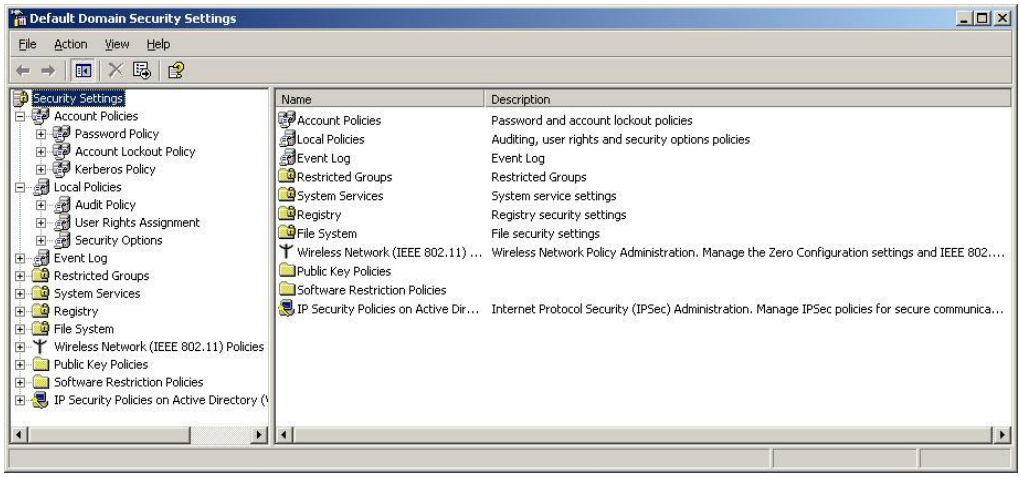
Note: On a domain controller, the Local Security Policy interface is not accessible from the Administrative Tools menu. To apply a security policy locally to a domain controller, it is recommended that the Default Domain Controller Security Settings interface be used in order to ensure consistent security policy settings across all domain controllers.

Default Domain Security Settings Interface

The Default Domain Security Settings interface is used to set and propagate Domain Security Policy requirements for all computers in the domain. Domain Security Policy overrides Local Security Policy settings for all computers within the domain.

To open the Default Domain Security Settings interface

1. Log on to the domain controller as an authorized administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Security Policy**. This opens the Default Domain Security Settings interface.

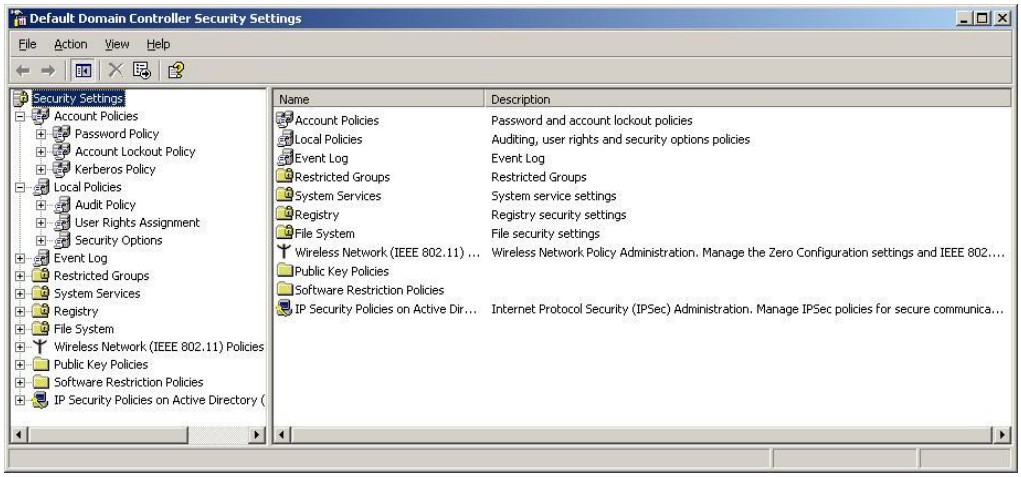


Default Domain Controller Security Settings Interface

The Default Domain Controller Security Settings interface is used to set and propagate security requirements for domain controllers. Domain Controller Security Policies apply strictly to all domain controllers within the applicable domain and take precedence over Domain Security Policies.

To open the Default Domain Controller Security Settings interface

1. Log on to the domain controller as an authorized administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Controller Security Policy**. This opens the Default Domain Controller Security Settings interface.



Organizational Unit Group Policy Objects

This document does not describe the implementation of OU GPOs. However, it should be noted that an OU GPO can 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. To access the **No Override** check box, click the **Options** button in the GPO's **Properties** dialog box.

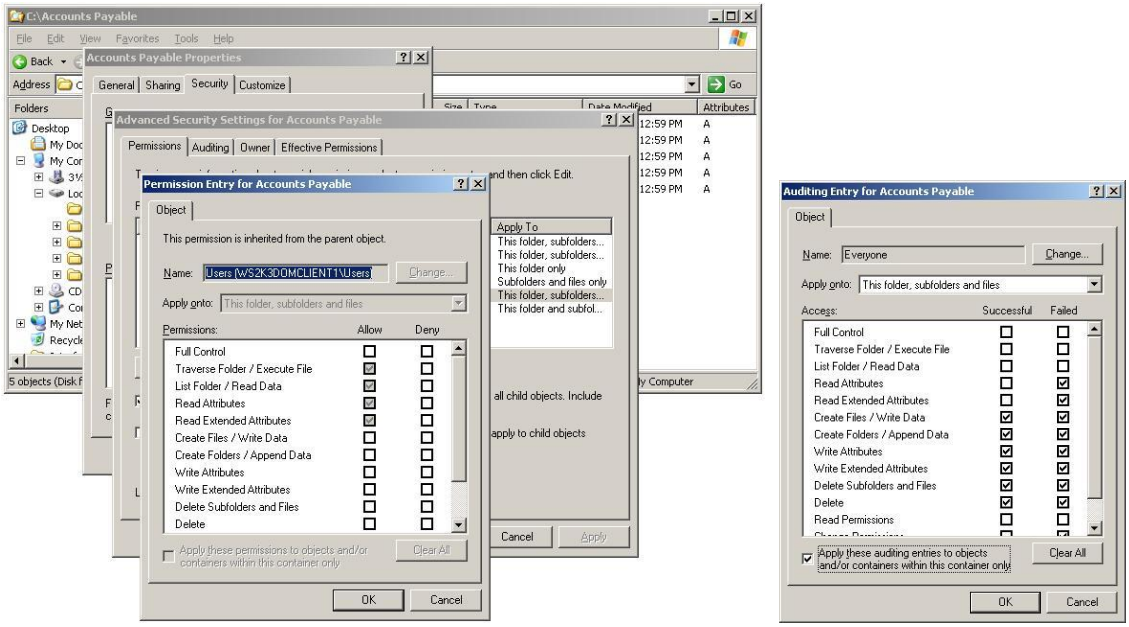
Additional Security Configuration Interfaces

For ease of discussion and implementation, this document focuses on managing security settings through the Windows Server 2003 Security Policies interfaces describe in the previous section. However, additional tools are available, and can 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 Server 2003 management interfaces, as well as the Security Configuration Tool Set. The tool set can be used to apply specific security policy settings and can be used to test the operating system for compliance with established policy requirements. Details about using each of these interfaces can be found in the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

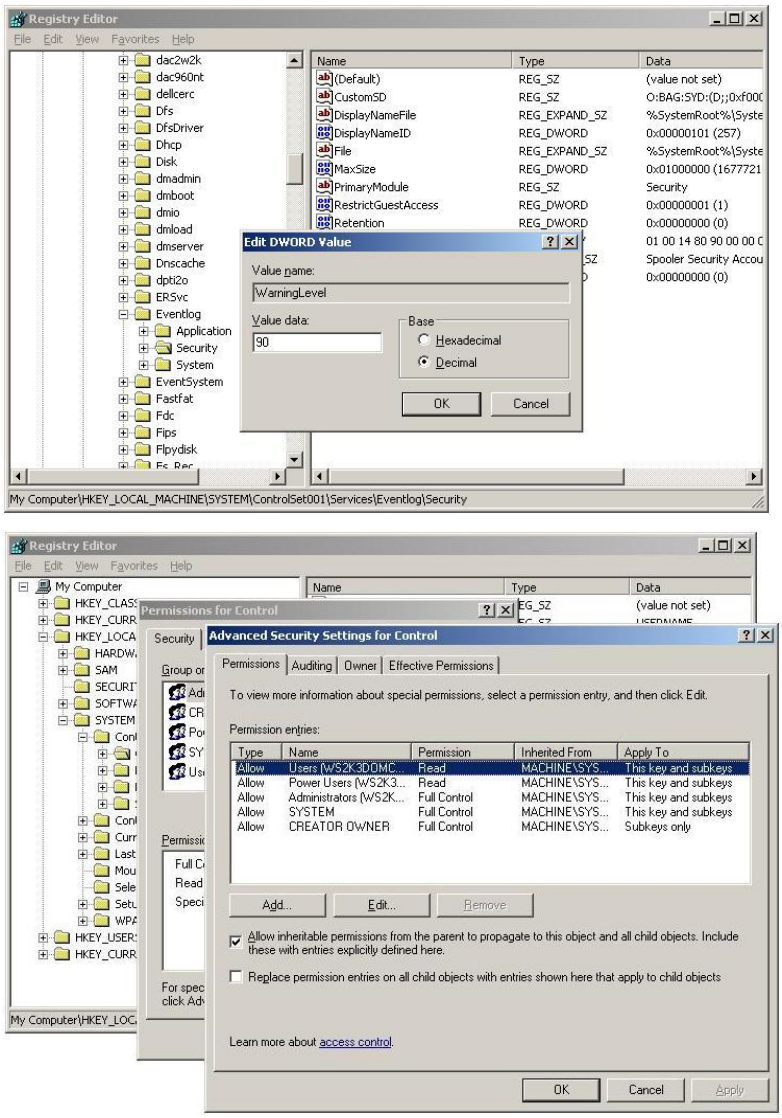
Windows Explorer

Windows Explorer can be used to configure permission and audit settings for specific files and folders. Shared folders and shared folder permissions can also be set through the Windows Explorer interface, as illustrated here.



Registry Editor

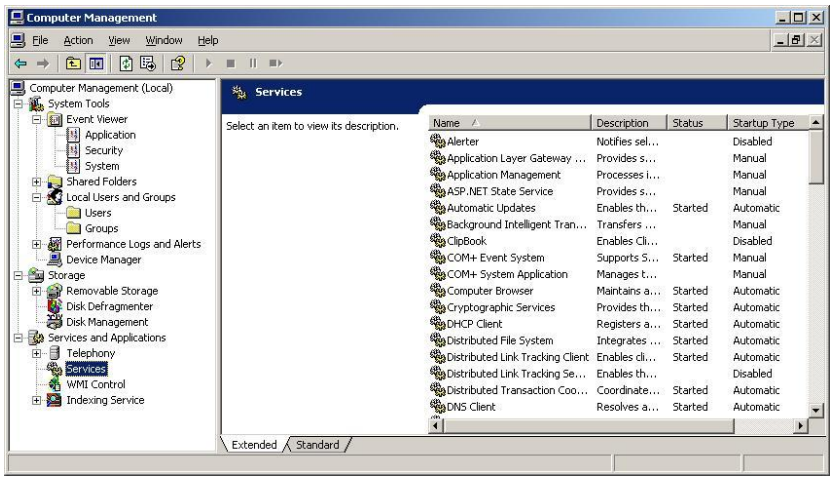
Windows Server 2003 includes a Registry Editor (Regedit.exe) that can be used to set specific values within the system registry. The Registry Editor also supports editing permissions and audit settings for registry key objects.



Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

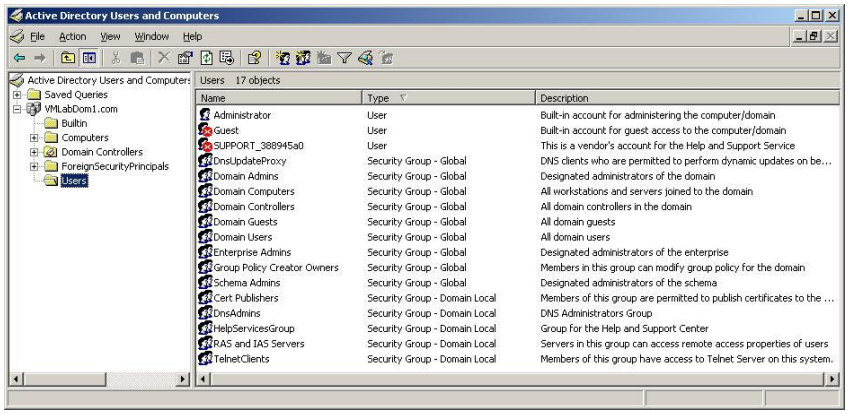
Computer Management Interface

The Computer Management interface is available on all Windows Server 2003 operating system editions. It supports management of audit logs, shared folder assignments and permissions, system services, as well as user and group accounts. On domain controllers the user and group accounts are managed from Active Directory Users and Computers interface instead of the Computer Management interface.



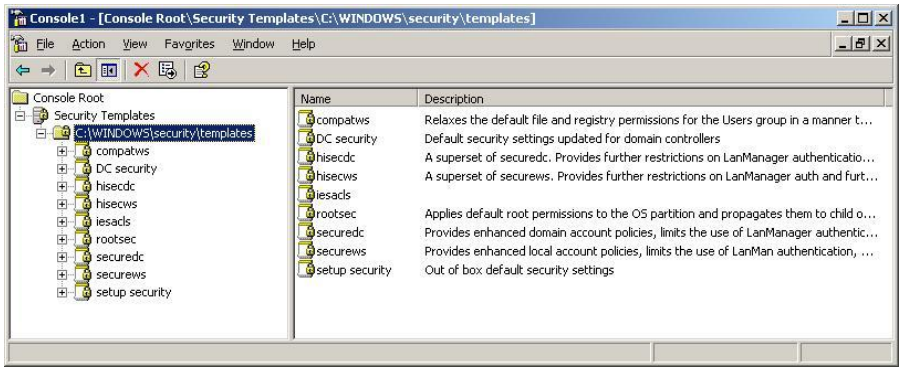
Active Directory Users and Computers

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.

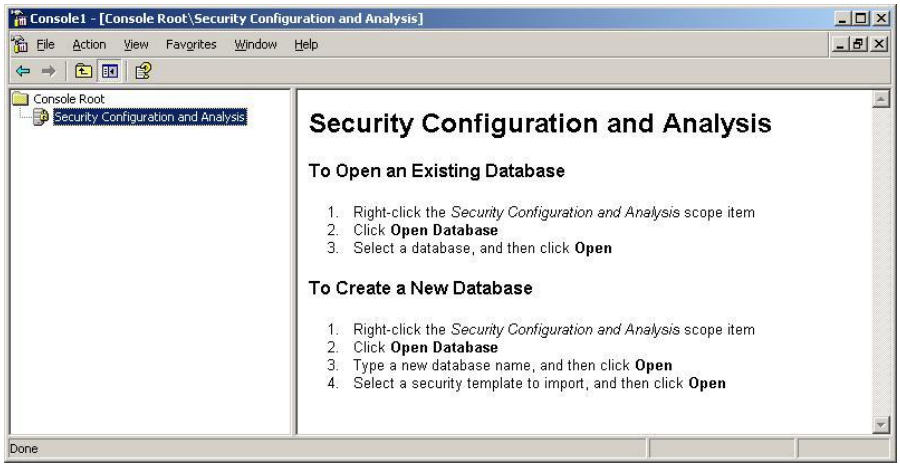


Microsoft Security Configuration Templates

The **Security Templates** and the **Security Configuration and Analysis** tools are a set of Microsoft Management Console (MMC) snap-ins that enable administrators to create and configure security templates and to conduct security configuration and analysis of Windows Server 2003. The **Security Templates** snap-in allows for the creation and modification of security templates.



The **Security Configuration and Analysis** snap-in allows administrators to import security templates to configure Local Security Policy on Windows Server 2003, and then perform periodic analysis of the systems to ensure that the configuration remains intact. The **Security Configuration and Analysis** snap-in can only be used to analyze and apply security configuration templates locally on a Windows Server 2003 computer. To apply a security configuration template to computers across a domain, the template must be imported into the Default Domain Security Settings interface.



Account Policies

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

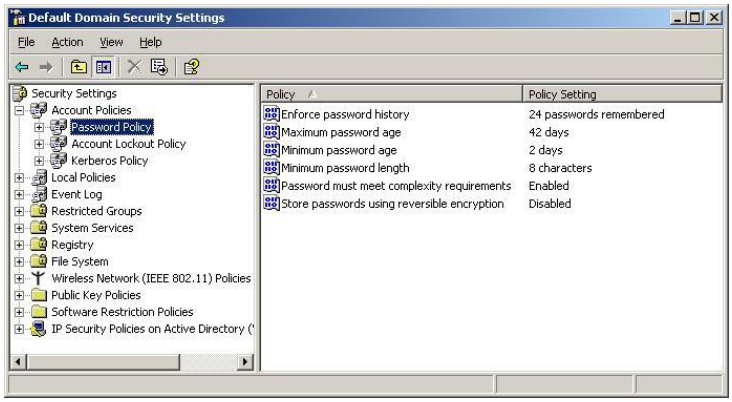
- **Password policy**. For local user accounts, this policy determines settings for passwords such as enforcement, and lifetimes.
- **Account lockout policy**. For local user accounts, this policy determines when and for whom an account is locked out of the system.
- **Kerberos policy**. Kerberos authentication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

See the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0* for additional information about setting account policies.

Password Policy

To view and edit current Password Policy settings

1. Open the applicable Security Policy interface.
2. Expand **Security Settings**.
3. Within Security Settings, expand **Account Policies** to reveal the Password, Account Lockout, and Kerberos policies.
4. Select the **Password Policy** object. The configurable Password Policy settings appear in the details pane.



5. Set the Password Policy as recommended or required in Table 5.1.

Table 5.1 Password policy settings

Password Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Set the Password History Requirements **Security Objective:** Limit how often passwords can be reused. The default setting on stand-alone servers is **0**. The default Domain Security Policy setting is **24**. **Procedure:** 1. Double-click the **Enforce password history** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number in the **passwords remembered** field (maximum is 24) to reflect the number of passwords the system can store. A recommended setting is 24.0.	✓	✓			✓

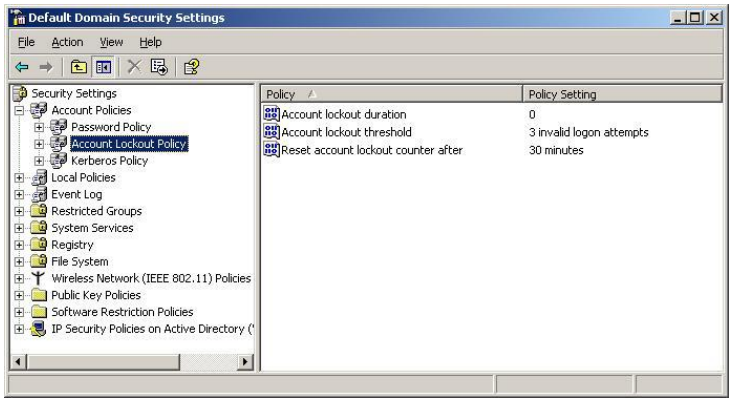
Password Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Set the Maximum Password Age **Security Objective:** Set the length of time users can keep their passwords before they have to change it. **Procedure:** 1. Double-click the **Maximum password age** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number of **days** to the desired number. A recommended setting is 42 days. **Note:** The ST requires that the administrator be able to set a password expiration time, 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:** 1. Double-click the **Minimum password age policy** object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number of **days** 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 of characters required for user passwords.	✓	✓		✓	

Password Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Procedure: 1. Double-click the **Minimum password length** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number of **characters** to **8**. **Note:** The ST requires that passwords be set to a minimum of eight characters.					
Set the Password Complexity Requirements **Security Objective:** Requires the use of a complex (strong) password. This policy imposes a requirement for a combination of alphanumeric, special, and upper and lower case characters in a password. **Procedure:** 1. Double-click the **Passwords must meet complexity requirements** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Select the **Enabled** radio button. **Note:** The ST does not specify password complexity requirements.	✓	✓			✓
Do Not Enable Reversible Encryption for Passwords **Security Objective:** Not recommended. **Procedure:** Review the **Store passwords using reversible encryption** policy setting and verify that the default setting of **Disabled** is set.	✓	✓		✓	

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. Select the **Account Lockout Policy** object. The configurable Account Lockout Policy settings are displayed in the details pane.



5. Set the Account Lockout Policy as recommended or required in Table 5.2.

Table 5.2 Account lockout policy settings

Account Lockout Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Account Lockout Duration **Security Objective:** When 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:** 1. Double-click the Account lockout duration policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. For the Evaluated Configuration, an account lockout policy must be set. It is recommended that the policy be set to lock the account indefinitely by changing the number in the **minutes**	✓	✓		✓	

Account Lockout Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
field to zero. This provides the most security by requiring an administrator to review the settings and unlock the account. **Notes:** ▪ The ST requires that an account lockout duration be set. To meet the strength of function requirement, the value must be set to one minute or greater. The value can also be set to zero, which then requires the administrator to unlock the account. ▪ The **Account lockout duration** policy can only be applied after an **Account lockout threshold** policy greater than zero has been set. ▪ The **Account lockout duration** policy is linked to the **Reset account lockout counter after** policy. If the **Account lockout duration** policy is set to zero, 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 zero, the **Reset account lockout counter after** policy is automatically set to an equal value by default.					
Account Lockout Threshold **Security Objective:** Set the number of invalid logon attempts that are allowed before an account is locked out. **Procedure:** 1. Double-click the **Account lockout threshold** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number of **invalid logon attempts** to the desired number. It is required that it not be set to a value greater than five. **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 five. Setting the **Account lockout threshold** requires that the **Reset account lockout counter after** and **the Account lockout duration value** settings be set. By default, they are set to **30**.	✓	✓		✓	

Account Lockout Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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 increased. This policy determines how long the lockout threshold is maintained before being reset. **Procedure:** 1. Double-click the **Reset account lockout counter after** policy object in the details pane to open the corresponding Security Policy Setting dialog box. 2. For domain-level policies, select the **Define this policy setting box**. 3. Change the number of **minutes** to the desired number. It is recommended that the reset counter be set to a minimum of 30 minutes. **Notes:** The **Reset account lockout counter after** policy can only be applied after an **Account lockout threshold** policy greater than zero has been set. The **Reset account lockout counter after** policy 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 is 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** is automatically set to an equal value by default.		✓	✓		✓	

Kerberos Policy Settings

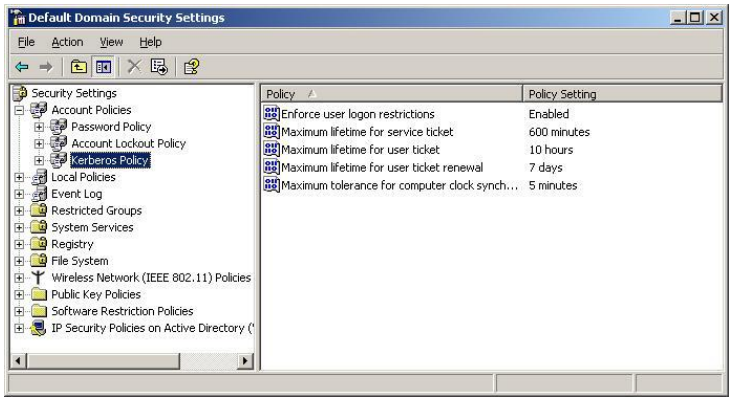
To view and edit current Kerberos Policy settings

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. Expand **Account Policies** to reveal the **Password**, **Account Lockout**, and **Kerberos** policies.
4. Select the **Kerberos Policy** object. The configurable Kerberos Policy settings are displayed in the details pane.



5. Set the Kerberos Policy as recommended or required in Table 5.3.

Table 5.3 Kerberos policy settings

Kerberos Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	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**.		✓		✓	
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**.		✓			✓
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**.		✓			✓

Kerberos Policies	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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**.		✓			✓
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:

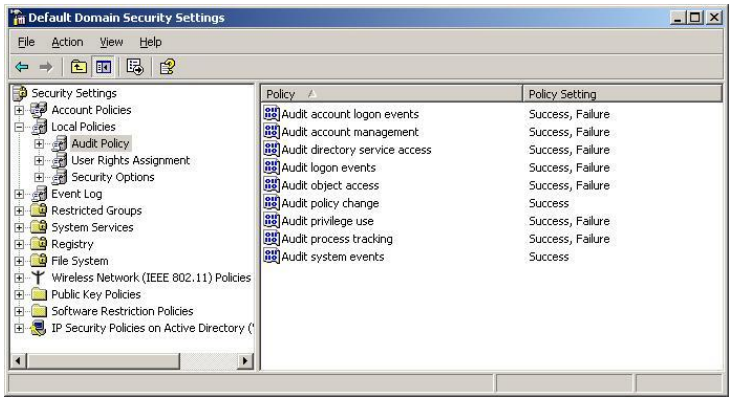
- **Audit policy.** Determines which security events are logged into the Security log on the computer (i.e., successful attempts, failed attempts or both). The Security log is part of Event Viewer.
- **User rights assignment.** Determines which users or groups have logon or task privileges on the computer.
- **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 applied to the computer where they are set – the *local computer*. When these settings are imported to a Group Policy object in Active Directory, they affect the local security settings of any computer accounts to which that Group Policy object is applied. For example, password policies that are configured for the Domain Security Policy (as they are by default) affect every computer member of the domain. This means that the local account databases (on individual workstations in the domain) have the same password policy as the domain itself. Therefore, local user accounts must follow the same policy as domain accounts.

Event Audit

To 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 the **Audit Policy** object. The configurable Audit Policy settings are displayed in the details pane.



5. To set auditing of a security event, double-click the desired audit policy in the details pane. The Security Policy Setting interface opens.
6. For domain-level policies, select the **Define these policy settings** box, and select the **Success** check box and/or **Failure** check box of the event as shown. To disable the auditing of a **Success** or **Failure** event in any of the audit categories, simply clear the corresponding check box.

7. Follow these procedures to set auditing of event categories as defined in Table 5.4.

Table 5.4 Audit policy settings

Audit Policies			Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Audit Event Category	**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	✓	✓	✓	✓	✓		✓

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

Notes:

Setting an Audit Object Access policy only enables the capability to audit objects. To collect object access audit events, an auditing System Access Control List (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.

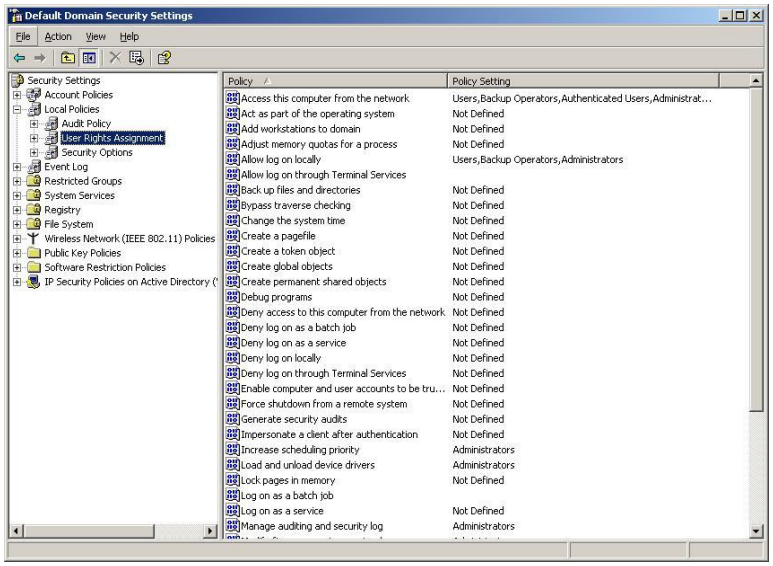
Account logon events are generated where the account resides, such as on a Domain. Logon events are generated where the logon attempt occurs.

See Appendix B – Audit Categories and Events for a matrix of Windows Server 2003 audit events, applicable ST requirements, and recommended audit settings.

Logon Rights and Privileges

To modify logon rights and privileges for user accounts and services

1. Open the applicable Security Policy.
2. Expand **Security Settings**.
3. Expand **Local Policies** to reveal the **Audit**, **User Rights Assignment**, and **Security Options** policies.
4. Click the **User Rights Assignment** object. The configurable user rights policy settings are displayed in the details pane.



5. To set a user Logon Right or Privilege, double-click the desired policy in the details pane. This opens the Security Policy Setting interface.
6. For domain-level policies, select the **Define these policy settings** box.
7. To remove a Logon Right or Privilege for an account, click the account name to highlight it and then click the **Remove** button.
8. To add a Logon Right or Privilege to an account, click the **Add User or Group** button and browse to the desired account.

9. There are several default assignments of user rights and privileges that the administrator must change or retain to support the Evaluated Configuration. Table 5.5 lists user rights and privileges for which there are required settings or recommended changes. For a complete list of Windows Server 2003 user rights and privileges, see Appendix C – User Rights and Privileges.

Note: The Power Users group 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 Security Policy. However, a Domain Security Policy template can include the Power Users SID (*S-1-5-32-547), which the policy then pushes out to the clients.

Table 5.5 User rights and privileges

User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
Access this computer from the network **Note:** The IUSR_ComputerName and IWAM_ComputerName accounts pertain to IIS Web Server hosts only.	Administrators Backup Operators Everyone IUSR_ComputerName IWAM_ComputerName Power Users Users	Administrators Authenticated Users Backup Operators IUSR_ComputerName IWAM_ComputerName Power Users Users	✓			✓	
	Not Defined	Administrators Authenticated Users Backup Operators Power Users (Can be applied by including the *S-1-5-32-547 SID when using a Policy Template) Users		✓		✓	
	Administrators Authenticated Users ENTERPRISE DOMAIN CONTROLLERS Everyone Pre-Windows 2000 Compatible Access	Administrators Authenticated Users ENTERPRISE DOMAIN CONTROLLERS			✓	✓	

User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
Act as part of the operating system	(blank)	Retain the defaults	✓		✓	✓	
	Not Defined	(blank)		✓		✓	
Add Workstations to domain	(blank)	Retain the defaults	✓			✓	
	Not Defined	(blank)		✓		✓	
	Authenticated Users	Domain Admins (or leave blank) **Note:** Domain Administrators already have this privilege by default.			✓	✓	
Adjust memory quotas for a process **Note:** The IWAM_ComputerName account pertain to IIS Web Server hosts only.	Administrators IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE	Retain the defaults	✓		✓	✓	
	Not Defined	Administrators LOCAL SERVICE NETWORK SERVICE		✓		✓	
Allow log on locally **Note:** The IUSR_ComputerName account pertains to IIS Web Server hosts only.	Administrators Backup Operators IUSR_ComputerName Power Users Users	Retain the defaults	✓			✓	
	Not Defined	Retain the defaults		✓		✓	

User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
	Account Operators Administrators Backup Operators Print Operators Server Operators	Retain the defaults			✓	✓	
Allow log on through Terminal Services	Administrators Remote Desktop Users	(blank)	✓			✓	
	Not Defined	(blank)		✓	✓	✓	
Backup files and directories	Administrators Backup Operators	Retain the defaults	✓			✓	
	Not Defined	Administrators Backup Operators		✓		✓	
	Administrators Backup Operators Server Operators	Retain the defaults			✓	✓	
Bypass traverse checking	Administrators Authenticated Users Everyone Pre-Windows 2000 Compatible Access	Administrators Authenticated Users Everyone			✓		✓
Change the system time	Administrators LOCAL SERVICE Power Users	Retain the defaults	✓			✓	
	Not Defined	Retain the defaults		✓		✓	
	Administrators LOCAL SERVICE Server Operators	Retain the defaults			✓		
Create a pagefile	Administrators	Retain the defaults	✓		✓	✓	

User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
	Not Defined	Administrators		✓		✓	
Create a token object	(blank)	Retain the defaults	✓		✓	✓	
	Not Defined	(blank)		✓		✓	
Debug programs	Administrators	(blank)	✓		✓	✓	
	Not Defined	(blank)		✓		✓	
Deny access to this computer from the network	SUPPORT_388945a0	Retain the defaults Organizations may add other accounts as required.	✓		✓	✓	
	Not Defined	If default is changed, the following must also be included: Guest SUPPORT_388945a0		✓		✓	
Deny log on locally	SUPPORT_388945a0	Retain the defaults Organizations may add other accounts as required.	✓		✓	✓	
	Not Defined	If default is changed, the following must also be included: Guest SUPPORT_388945a0		✓		✓	
Enable computer and user accounts to be trusted for delegation	(blank)	Retain the defaults	✓			✓	
	Not Defined	(blank)		✓		✓	
	Administrators	Retain the defaults			✓	✓	
Force shutdown from a remote system	Not Defined	Administrators		✓			✓

User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
Generate security audits	LOCAL SERVICE NETWORK SERVICE	Retain the defaults	✓		✓	✓	
	Not Defined	LOCAL SERVICE NETWORK SERVICE		✓		✓	
Impersonate client after authentication **Note:** The IIS_WPG account pertains to IIS Web Server hosts only.	Administrators IIS_WPG SERVICE	Retain the defaults	✓			✓	
	Not Defined	Retain the defaults		✓	✓	✓	
Increase Scheduling Priority	Not Defined	Administrators		✓			✓
Load and Unload Device Drivers	Administrators	Retain the defaults	✓			✓	
	Not Defined	Administrators		✓		✓	
	Administrators Print Operators	Retain the defaults			✓	✓	
Logon as a batch job **Note:** The IUSR_ComputerName, IWAM_ComputerName and IIS_WPG accounts pertain to IIS Web Server hosts only.	IUSR_ComputerName IWAM_ComputerName IIS_WPG SUPPORT_388945a0 LOCAL SERVICE	IUSR_ComputerName IWAM_ComputerName IIS_WPG LOCAL SERVICE	✓				✓
	Not Defined	LOCAL SERVICE		✓			✓
	<*DomainName*>\ SUPPORT_388945a0 LOCAL SERVICE	LOCAL SERVICE			✓		✓
Manage auditing and Security log	Administrators	Retain the defaults	✓		✓	✓	

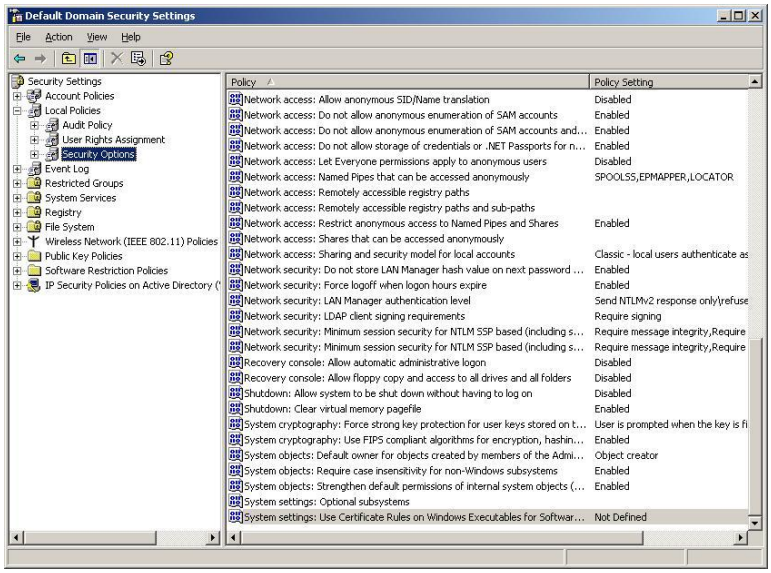
User Rights Assignment			Stand-alone \ Member Server	Domain Policy	Domain Controller	Required	Recommended
Logon Right / Privilege	**Default**	**Modified**					
	Not Defined	Administrators		✓		✓	
Modify firmware environment	Administrators	Retain the defaults	✓		✓	✓	
	Not Defined	Administrators		✓		✓	
Perform volume maintenance tasks	Administrators	Retain the defaults	✓			✓	
	Not Defined	Administrators		✓		✓	
	Not Defined	Retain the defaults			✓	✓	
Profile system performance	Administrators	Retain the defaults	✓		✓	✓	
	Not Defined	Administrators		✓		✓	
Replace a process-level token **Note:** The IWAM_ComputerName account pertains to IIS Web Server hosts only.	IWAM_ ComputerName LOCAL SERVICE NETWORK SERVICE	Retain the defaults	✓		✓	✓	
	Not Defined	Retain the defaults		✓		✓	
Restore files and directories	Administrators Backup Operators	Retain the defaults	✓			✓	
	Not Defined	Administrators Backup Operators		✓		✓	
	Administrators Backup Operators Server Operators	Retain the defaults			✓	✓	
Take ownership of files or other objects	Administrators	Retain the defaults	✓		✓	✓	
	Not Defined	Administrators		✓		✓	

See Appendix C – User Rights and Privileges for a matrix of Windows Server 2003 user rights and privileges, applicable ST requirements, and the recommended/required modifications.

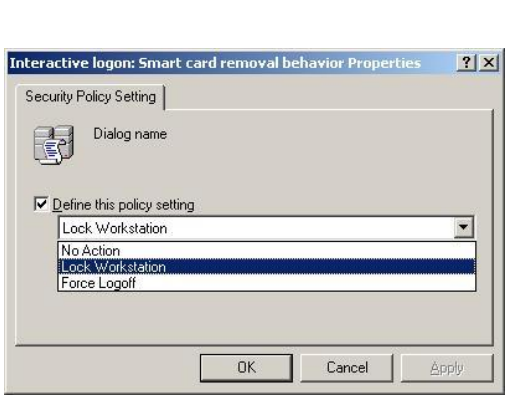
Security Options

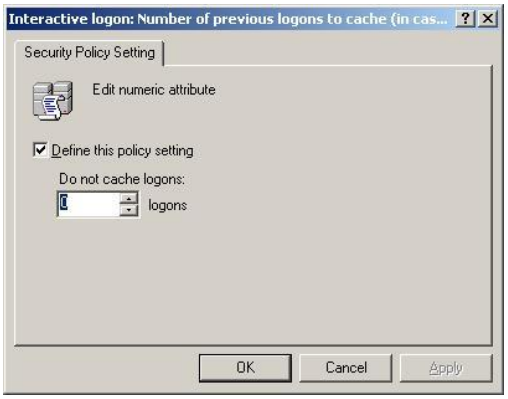
To modify predefined security-related registry settings

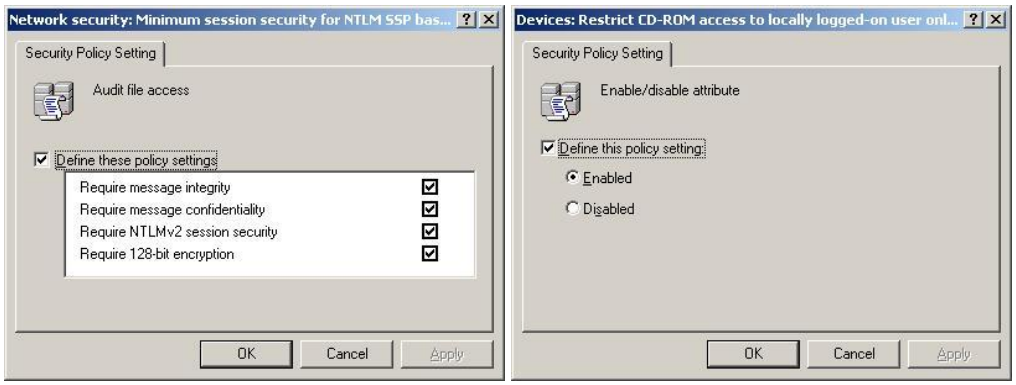
1. Open the applicable Security Policy.
2. Expand **Security Settings**.
3. Expand **Local Policies** to reveal the **Audit**, **User Rights Assignment**, and **Security Options** policies.
4. Click the **Security Options** object. The configurable security options are displayed in the details pane.



5. To set a Security Option, double-click the desired policy in the details pane. This opens the Security Policy Setting dialog box.
6. For domain-level policies, select the **Define these policy settings** check box.
7. How to configure the Security Policy Setting dialog boxes for selected security options varies depending on the configuration requirements of the option. For example, some security options might require selection from a drop-down list, a text input, a check box selection, or a radio button selection as shown in the screenshots here.

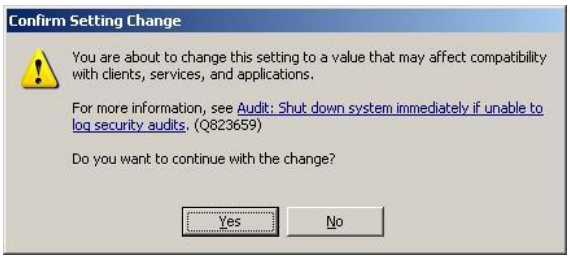






8. Modify the Security Options as shown in Table 5.6.

Note: Some Security Option changes might have an impact on the compatibility between clients, services, and applications. Attempting to make changes to these Security Options might result in a confirmation notice such as the one shown here.



Review the information provided by the notice and proceed as necessary.

Table 5.6 Security option settings

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Accounts: Administrator account status **Security Objective:** Determines whether the Administrator account is enabled or disabled under normal operation. When a computer is booted in Safe Mode, the Administrator account is always enabled, regardless of this policy setting. By default, this policy is **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Enabled**. 1. Double-click **Accounts: Administrator account status** in	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** This setting may not be picked up immediately by the Local Security Policy interface. If this setting is shown as Not Applicable in the Local Security Policy, it may be necessary to right-click the Security Settings node and select Reload in order to refresh the policy settings.					
Accounts: Guest account status **Security Objective:** Determines whether the Guest account is enabled or disabled. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must remain **Disabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Disabled**. 1. Double-click **Accounts: Guest account status** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Note:** This setting may not be picked up immediately by the Local Security Policy interface. If this setting is shown as Not Applicable in the Local Security Policy, it may be necessary to right-click the Security Settings node and select Reload in order to refresh the policy settings.	✓	✓		✓	
Accounts: Limit local account use of blank passwords to console logon only **Security Objective:** Determines whether remote interactive logons by network services such as Terminal Services, Telnet, and FTP are allowed for local accounts that have blank passwords. If this setting is enabled, a local account must have a nonblank password to be used to perform an interactive logon from a remote client.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
By default, this policy is **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Accounts: Limit local account use of blank passwords to console logon only** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** Terminal Services, Telnet, and FTP are not included in the Evaluated Configuration.					
Accounts: Rename administrator account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the Administrator account. 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 default Administrator account. By default, this policy is set to **Administrator** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Renaming the Administrator account is recommended. 1. Double-click **Accounts: Rename administrator account** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. In the text box, enter the new name for the Administrator account and click the **OK** button.	✓	✓			✓
Accounts: Rename guest account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the Guest account. 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	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
associated with the Guest account. By default, this policy is set to **Guest** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Renaming the Guest account is recommended. 1. Double-click **Accounts: Rename Guest Account** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. In the text box, enter the new name for the Guest account and click **OK**. **Note:** The Guest account must be disabled in the Evaluated Configuration (see Table 4-10).					
Audit: 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 Disk Operating System (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 is audited. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Enabling this policy setting is recommended, but requires that a strict audit management process be in place for reviewing, archiving, and clearing the audit logs on a regular basis. 1. Double-click **Audit: Audit the access of global system objects** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** In the Evaluated Configuration, these objects must have the ability to be audited; however, enforcing this audit capability is optional. To audit these objects, the administrator must set this option. This setting generates a large amount of audit information. Therefore, it should only be enabled where there is a strict audit	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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: 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 are audited. By default, this policy is **Disabled** in Windows Server 2003, **Not defin**ed in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Enabling this policy setting is recommended, but requires that a strict audit management process be in place for reviewing, archiving, and clearing the audit logs on a regular basis. 1. Double-click **Audit: Audit the use of Backup and Restore privilege** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** In the Evaluated Configuration, these objects must have the ability to be audited; however, enforcing this audit capability is optional. To audit these objects, the administrator must set this option. This setting generates 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: 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. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the security audit log is full and the retention method specified for the Security log is	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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 occurs: **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** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Enabling this policy setting is recommended, but requires that a strict audit management process be in place for reviewing, archiving, and clearing the audit logs on a regular basis. 1. Double-click **Audit: Shut down system immediately if unable to log security audits** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **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 becomes full. If the administrator desires this functionality, this option must be enabled. This setting 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. **Warning:** The administrative burden of enabling this setting can be very high, especially if the **Retention method** for Security log is configured to **Do not overwrite events (clear log manually)**. This setting turns a repudiation threat (a backup operator could deny that she backed up or restored data) into a denial of service (DoS) vulnerability because a server could be forced to shut down by overwhelming it with logon events and other security events that are written to the Security log. Additionally, since the shut down is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. While NTFS guarantees that the file system's integrity is maintained during an ungraceful system shutdown, it cannot guarantee that every data file for every application will still be in a usable form when the system restarts. Recovery procedures are defined in the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.					

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax **Security Objective:** Distributed Component Object Model (DCOM) access permissions control authorization to call a running COM server. These permissions are defined as security descriptors provided to the COM infrastructure through the CoInitializeSecurity API, or using registry settings. The default DCOM security changes supported by this policy setting include: ▪ By default, the Everyone group is granted local launch, local activation, and local access permissions. This enables all local scenarios to work without modification to the software or the operating system. ▪ By default, the Everyone and Anonymous groups are granted remote access permissions. This enables most COM client scenarios, including the common case where a COM client passes a local reference to a remote server, in effect turning the client into a server. ▪ Also by default, only members of the Administrators group are granted remote activation and launch permissions. This disables remote activations by non-administrators to installed COM servers. **Procedure:** It is recommended that the default setting not be changed.	✓	✓			✓
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax **Security Objective:** DCOM launch permissions control authorization to start a COM server during COM activation if the server is not already running. These permissions are defined as security descriptors that are specified in registry settings. The default DCOM security changes supported by this policy setting include: ▪ By default, the Everyone group is granted local launch, local activation, and local access permissions. This enables all local scenarios to work without modification to the software or the operating system. ▪ By default, the Everyone and Anonymous groups are granted remote access permissions. This enables most COM client scenarios, including the common case where a COM client passes a local reference to a remote server, in effect turning the client into a server. ▪ Also by default, only members of the Administrators group are granted remote activation and launch permissions. This	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
disables remote activations by non-administrators to installed COM servers. **Procedure:** It is recommended that the default setting not be changed.					
Devices: Allow undock without having to log on **Security Objective:** Determines whether a user must log on to request that a portable computer be removed from a docking station. If this setting is disabled, the user must log on to request removal from the docking station, at which time the user must have been granted the **Remove Computer from Docking Station** privilege. If this setting is enabled, a user can request removal from the docking station by pressing the portable computer's physical eject button. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Disabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Disabled**. 4. Double-click **Audit Devices: Allow undock without having to log on** in the details pane. 5. For domain-level policies, select the **Define these policy settings** check box. 6. Select the **Disabled** radio button and click the **OK** button. **Note:** In general, laptop computers should not be used for operating systems that are to function as network servers.	✓	✓			✓
Devices: Allowed to format and eject removable media **Security Objective:** Determines who is allowed to format and eject removable NTFS media. This capability can be given to Administrators, Administrators and Power Users, or Administrators and Interactive Users as defined by the drop-down menu options. By default, this policy is set to **Administrators** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Administrators** setting be maintained in the Windows Server 2003 Local Security	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Policy and that the default setting in the domain-level policies be changed to **Administrators**. 1. Double-click **Devices: Allowed to format and eject removable media** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select **Administrators** from the drop-down list and click **OK**.					
Devices: Prevent users from installing printer 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 computer. This prevents users from adding printers when the device driver does not exist on the local computer. If this policy is disabled, then a member of the Users group can install printer drivers on the computer. By default, this setting is disabled on Windows XP Professional domain clients and enabled on Windows Server 2003. By default, this policy is **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Devices: Prevent users from installing printer drivers** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** If this setting is enabled, only users with Administrative, Power User, or Server Operator privileges will be able to install printers on the servers. If this setting is enabled, but the driver for a network printer already exists on the local computer, users can still add the network printer. This setting does not affect the ability to add a local printer.	✓	✓		✓	
Devices: Restrict CD-ROM access to locally logged-on user only	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Devices: Restrict CD-ROM access to locally logged-on user only** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.					
Devices: 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. By default, this policy is **Di**sabled in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Devices: Restrict floppy access to locally logged-on user only** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
3. Select the **Enabled** radio button and click the **OK** button.					
Devices: 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 (WHQL). The options are: ▪ Silently succeed ▪ Warn but allow installation ▪ Do not allow installation By default, this policy is set to **Warn but allow installation** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Warn but allow installation** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Warn but allow installation**. 1. Double-click **Devices: Unsigned driver installation behavior** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select **Warn but allow installation** from the drop-down list and click the **OK** button.		✓	✓			✓
Domain controller: Allow server operators to schedule tasks **Security Objective:** Determines if Server Operators are allowed to submit jobs by means of the AT schedule facility. By default, this setting is disabled. Therefore, 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. The default setting on Windows 2003 Servers is **Not defined**, which has the same effect as **Disabled**. The default setting in the Domain Controller Security Policy is **Not defined**. **Procedure:** This policy setting is only applicable to domain controllers and does not impact clients in a Windows Server 2003			✓		✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Domain. It is recommended that the default setting not be changed.					
Domain controller: LDAP server signing requirements **Security Objective:** This security setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. The possible values for this Group Policy setting are: ▪ **None** – Data signing is not required in order to bind with the server. If the client requests data signing, the server supports it. ▪ **Require signing** – The LDAP data – signing option must be negotiated unless Transport Layer Security/Secure Socket Layer (TLS/SSL) is being used. The default setting on Windows 2003 Servers is **Not defined**, which has the same effect as **None**. The default setting in the Domain Controller Security Policy is **None**. **Procedure:** It is recommended that the **Require signing** option be set in the Default Domain Controller Security Policy. 1. In the **Default Domain Controller Security Policy**, Double-click **Domain controller: LDAP server signing requirements** in the details pane. 2. The **Define these policy settings** check box should already be selected. If not, check the box to enable the setting. 3. Select **Require signature** from the drop-down list and click the **OK** button. **Note:** This policy setting is only applicable to domain controllers. **Warning:** If the domain controller is set to **Require signing**, the domain clients must also be set by way of the **Network security: LDAP client signing requirements** security option. Not setting the client results in loss of connection with the server.			✓		✓
Domain controller: Refuse machine account password changes **Security Objective:** Determines whether or not a domain controller will accept password change requests for computer accounts. If enabled on all domain controllers in a domain, then domain members will not be able to change their computer account passwords. The default setting on Windows 2003 Servers is **Not defined**, which has the same effect as the **Disabled** setting. The default			✓		✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
setting in the Domain Controller Security Policy is **Not defined**. **Procedure:** It is recommended that the default setting not be changed. Changing the default setting to **Enabled** would leave computer account passwords susceptible to potential compromise. **Note:** This policy setting is only applicable to domain controllers.					
Domain member: Digitally encrypt or sign secure channel data (always) **Security Objective:** Determines whether a secure channel can be established with a domain controller that is not capable of signing or encrypting all secure channel traffic. If this setting is **Enabled**, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data. If this setting is **Disabled**, a secure channel can be established, but the level of encryption and signing is negotiated. By default, this policy is **Enabled** in Windows Server 2003, **Not** defined in the Default Domain Security Policy, and **Enabled** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** settings be maintained and that the default setting in the domain-level policies be changed to **Enabled**. 1. In the **Default Domain Controller Security Policy**, Double-click **Domain member: Digitally encrypt or sign secure channel data (always)** in the details pane. 2. The **Define these policy settings** check box should already be selected. If not, select the box to enable the setting. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** When this policy is enabled, the policy **Domain member: Digitally sign secure channel data (when possible)** is automatically **Enabled**.		✓	✓			✓
Domain member: Digitally encrypt secure channel data (when possible) **Security Objective:** If this setting is enabled, it ensures that all secure channel traffic is encrypted if the partner domain controller is also capable of encrypting all secure channel traffic. By default, this policy is **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in		✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Enabled**. 1. In the **Default Domain Controller Security Policy**, Double-click **Domain member: Digitally encrypt or sign secure channel data (always)** in the details pane. 2. The **Define these policy settings** check box should already be selected. If not, select the box to enable the setting. 3. Select the **Enabled** radio button and click the **OK** button.					
Domain member: Digitally sign secure channel data (when possible) **Security Objective:** If this setting is enabled, it ensures that all secure channel traffic is signed if the partner domain controller is also capable of signing all secure channel traffic. By default, this policy is **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Enabled**.0. 1. In the **Default Domain Controller Security Policy**, Double-click **Domain member: Digitally encrypt or sign secure channel data (always)** in the details pane. 2. The **Define these policy settings** check box should already be selected. If not, select the box to enable the setting. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** If the policy **Domain member: Digitally encrypt or sign secure channel data (always)** is enabled, this setting is implicitly **Enabled**.	✓	✓			✓
Domain member: Disable machine account password changes **Security Objective:** Determines whether a domain member periodically changes its computer account password. If this setting is enabled, the domain member does not attempt to change its	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
computer account password. If this setting is disabled, the domain member attempts to change its computer account password as specified by the setting for **Domain Member: Maximum age for machine account password**, which by default is every 30 days. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default setting not be changed. **Note:** This setting should not be enabled. Computer account passwords are used to establish secure channel communications between members and domain controllers and, within the domain, between the domain controllers themselves. After it is established, the secure channel is used to transmit sensitive information that is necessary for making authentication and authorization decisions. **Warning:** Disabling this feature causes computers running Windows Server 2003 to retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk of an attacker determining the password for the system's domain account.					
Domain member: Maximum machine account password age **Security Objective:** Determines the maximum allowable age for a computer account password. By default, this policy is set to **30 days** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default setting not be changed.	✓	✓			✓
Domain member: Require strong (Windows 2000 or later) session key **Security Objective:** Determines whether a secure channel can be established with a domain controller that is not capable of encrypting secure channel traffic with a strong (128-bit) session key. If this setting is enabled, a secure channel is not established with any domain controller that cannot encrypt secure channel data with a strong key. If this setting is disabled, 64-bit session keys are tolerated. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and enforced through the Domain Security Policy. 0. 1. Double-click **Domain member**: Require strong (Windows 2000 or later) session key in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** When this setting is **En**abled, all domain controllers must be capable of encrypting secure channel data with a strong 128 bit encryption key. This requires Windows 2000 servers or higher as domain controllers. For the Evaluated Configuration, the target environment consists of Windows Server 2003 domain controllers.					
Interactive logon: Display user information when the session is locked **Security Objective:** By default, when a Windows Server 2003 session is locked, the currently logged on user's domain and account name are displayed in the Computer Locked interface. This security setting allows selection of the following three information display modes: ▪ User display name, domain and user names ▪ User display name only ▪ Do not display user information **Procedure:** It is recommended that the default setting be changed to Do not display user information in the Windows Server 2003 Local Security Policy and enforced through the domain-level policies. 1. Double-click **Interactive logon: Display user information when t**he session is locked in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select **Do not display user information** from the drop-down menu and click the **OK** button. **Note:** This setting does not appear in the Windows XP Professional (32-bit operating system) Local Security Policy, but may be applied from a Windows Server 2003 Domain Security Policy.	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Interactive logon: Do not display last user name **Security Objective:** By default, the Windows Server 2003 logon 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 logon 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. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure**: It is recommended that the default setting be changed to **Enabled** in the Windows Server 2003 Local Security Policy and enforced through the domain-level policies. 1. Double-click **Interactive logon: Do not display last user name** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.	✓	✓			✓
Interactive logon: Do not require CTRL+ALT+DEL **Security Objective:** **DO NOT ENABLE THIS OPTION** Enabling this option disables the trusted path mechanism. The purpose of the trusted path mechanism is to prevent spoofing of user logon sessions. By default, this policy is **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** Ensure that this option is set to **Disabled** in the Windows Server 2003 Local Security Policy and enforced through the Domain Security Policy.0. 1. Double-click **Intera**ctive logon: Do not require **CTRL+ALT+DEL** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Interactive logon: Message text for users attempting to log on **Security Objective:** Configure the interactive logon screen to display a logon banner with a warning message. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. By default, this policy is **Not defined** in all Security Policies. **Procedure:** 1. To set a message title, Double-click **Interactive logon: Message text for users attempting to log on** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Enter the message text and click **OK**. **Note:** The Evaluated Configuration requires that a logon banner is set. The message and title text will differ for each organization and must therefore be explicitly defined by the implementing organization.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Interactive logon: Message title for users attempting to log on **Security Objective:** Allows the specification of a title to appear in the title bar of the window that contains the **Interactive logon: Message text for users attempting to log on**. By default, this policy is **Not defined** in all Security Policies. **Procedure:** 1. To set the message, Double-click **Interactive logon: Message title for users attempting to** log on in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Enter the title for the logon message (for example, *Warning*) and click **OK**. **Note:** The Evaluated Configuration requires that a logon banner is set. The message and title text will differ for each organization and must therefore be explicitly defined by the implementing organization.	✓	✓		✓	
Interactive logon: Number of previous logons to cache (in case domain controller is not available) **Security Objective:** Windows Server 2003 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, cached credentials can be used. The **CachedLogonsCount** registry value determines how many user account entries Windows saves in the logon cache on the local computer. If the value of this entry is **0**, Windows 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 displays the following message: **The system cannot log you on now because the domain <DomainName> is not available.** Otherwise, if a domain controller is unavailable and a user's logon information is cached, the user is still allowed to log on after being prompted with the following message: **A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available.**	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Additionally, if the Administrator disables a user's domain account, the user could still use the cache to log on by disconnecting the network cable. To prevent this, 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. By default, this policy is set to 10 logons in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** 1. Double-click **Interactive Logon: Number of previous logons to cache** (in case domain controller is not available in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. In the **Cache** text box, set the number of logons to **0** and click the **OK** button. **Note:** The required setting is not recommended for mobile computers (laptops) that are used out of the organization's network environment because the user would not be able to log on unless the computer is directly connected to the network.					
Interactive logon: Prompt user to change password before expiration **Security Objective:** Determines how far in advance Windows Server 2003 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** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** The default setting of **14 days** is adequate. It is recommended that the default setting not be changed.	✓	✓			✓
Interactive logon: Require Domain Controller authentication to unlock **Security Objective:** Logon information must be provided to unlock a locked computer. For domain accounts, this setting determines whether a domain controller must be contacted to unlock	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
a computer. If this setting is disabled, a user can unlock the computer using cached credentials. If this setting is enabled, a domain controller must authenticate the domain account that is being used to unlock the computer. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. Windows XP Professional domain clients have this policy **Disabled** by default in their Local Security Policy. **Procedure:** It is recommended that the default setting not be changed. **Note:** The required setting is not recommended for mobile computers (laptops) that are used out of the organization's network environment because the user would not be able to log on unless the computer is directly connected to the network. **Warning:** If the domain controller goes offline after a user's computer has been locked, the user is unable to log on to the computer if this setting is enabled.					
Interactive logon: Require smart card **Security Objective:** Controls whether users have to use a smart card to log on to the computer. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default setting not be changed if the organization is not using smart cards for user log on. The policy may be enabled as needed. **Notes:** ▪ In order to use a smart card to log on, the computer must be a member of a domain. ▪ The integration of smart card technology is a configurable option for the Windows Server 2003 Evaluated Configuration.	✓	✓			✓
Interactive logon: 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:	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
▪ No action ▪ Lock workstation ▪ Force logoff By default, this policy is set to **No Action** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. If **Lock Workstation** is specified, then the workstation is locked when the smart card is removed allowing users to leave 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:** In the event an organization decides to use smart cards to control computer access, it is recommended that the default setting be changed to Lock Workstation. 1. Double-click **Interactive logon: Smart card removal behavior** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. From the drop-down menu, select **Lock Workstation** and click the **OK** button. **Notes:** ▪ If the default setting is changed to **Lock Workstation** or **Force Logoff**, the **Interactive logon: Require smart card** Security Option should be set to **Enabled**. ▪ In order to use a smart card to log on, the computer must be a member of a Domain. ▪ The integration of smart card technology is a configurable option for the Windows Server 2003 Evaluated Configuration.					
Microsoft network client: Digitally sign communications (always) **Security Objective:** Determines whether the computer always digitally signs client communications. The Windows Server 2003 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.	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Enabling this option requires the Windows Server 2003 SMB client to perform SMB packet signing. If this policy is disabled, it does not require the SMB client to sign packets. For the Evaluated Configuration, this policy option may be **Disabled** and the following security option, **Microsoft network client: Digitally sign client communications (if server agrees)** can be **Enabled**. Since the Evaluated Configuration operating environment is a closed network with all computers configured to the same requirements, communications use SMB signing (see note below). By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:**It is recommended that the default **Disabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Disabled**. 1. Double-click **Microsoft network client: Digitally sign communications (always)** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Notes:** ▪ In order to use SMB signing, it must be either enabled (if client/server agrees) or required (always) 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 use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, then a client is unable to establish a session unless it is at least enabled for SMB signing. ▪ SMB signing imposes a performance penalty on the computer system. Although it does not consume any more network bandwidth, it does use more CPU cycles on the client and server side. Therefore changing the default setting to **Enabled** would impose a performance penalty on the computer system, but would have no functional effect within the Evaluated Configuration operating environment (see Security Objective discussion earlier).					
Microsoft network client: Digitally sign communications (if server agrees) **Security Objective:** If this policy is enabled, it causes the Windows Server 2003 Server Message Block (SMB) client to	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing. See **Microsoft network client: Digitally sign communications (always)** for additional details. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the Default Domain Security Policy must be changed to **Enabled**. 4. Double-click **Microsoft network client: Digitally sign communications (if server agrees)** in the details pane. 5. For domain-level policies, select the **Define these policy settings** check box. 6. Select the **Enabled** radio button and click the **OK** button. **Note:** See notes for **Microsoft network client: Digitally sign communications (always)**.					
Microsoft network client: 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 policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default setting not be changed. **Note:** The target environment for the Evaluated Configuration does not include third-party SMB servers.	✓	✓			✓
Microsoft network server: Amount of idle time required before suspending 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	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
inactive SMB session. If client activity resumes, the session is automatically reestablished. For this policy setting, a value of **0** means to disconnect an idle session as quickly as reasonably possible. The maximum value is 99999, which is 208 days; in effect, this value disables the policy. By default, this policy is set to **15** minutes in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default setting not be changed.					
Microsoft network server: Digitally sign communications (always) **Security Objective:** If this policy is enabled, it requires the Windows Server 2003 Server Message Block (SMB) server to perform SMB packet signing. See **Microsoft network client: Digitally sign communications (always)** for additional details. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Enabled** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Disabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Disabled**. 1. Double-click **Microsoft network server: Digitally sign communications (always)** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Note:** See notes for **Microsoft network client: Digitally sign communica**tions (always).	✓	✓			✓
Microsoft network server: Digitally sign communications (if client agrees) **Security Objective:** If this policy is enabled, the Windows Server 2003 Server Message Block (SMB) server negotiates SMB packet signing with clients that request it. This policy is disabled by default on Windows Server 2003. This policy is enabled by default on domain controllers. See **Microsoft network client: Digitally**	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
sign communications (always) for additional details. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Enabled** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the Default Domain Security Policy must be changed to **Enabled**. 1. Double-click **Microsoft network server: Digitally sign communications (if client agrees)** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** See notes for **Microsoft network client: Digitally sign communications (always)**.					
Microsoft network server: Disconnect clients when logon hours expire **Security Objective:** Determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. The allowed logon hour range for users is set at the domain controller. This setting affects the SMB component. Enabling this setting causes client sessions with the SMB service to be forcibly disconnected when the client's logon hours expire. Disabling this setting maintains an established client session after the client's logon hours have expired. When enabling this setting you should also enable **Network security: Force logoff when logon hours expire**. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Enabled**. 1. Double-click **Microsoft network server: Disconnect clients when logon hours expire** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box.	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
3. Select the **Enabled** radio button and click the **OK** button. **Note:** When this setting is enabled, the **Network security: Force logoff when logon hours expire** setting should also be enabled.					
Network access: Allow anonymous SID/Name translation **Security Objective:** Determines if an anonymous user can request security identifier (SID) attributes for another user. If this policy is enabled, a user with knowledge of an administrator's SID could contact a computer that has this policy enabled and use the SID to get the administrator's name. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. This policy is set to **Enabled** by default in a domain controller's Local Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Disabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Disabled**. 1. Double-click **Network access: Allow anonymous SID/Name translation** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Note:** Disabling this policy setting on domain controllers means that legacy systems might be unable to communicate with Windows Server 2003-based domains. However, legacy systems are not included in the Windows Server 2003 Evaluated Configuration operating environment.	✓	✓		✓	
Network access: Do not allow anonymous enumeration of SAM accounts **Security Objective:** Controls the ability of anonymous users to enumerate the accounts contained within the Security Accounts Manager (SAM) database by determining which additional permissions will be granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerating the names of domain SAM accounts and of network shares. This is convenient, for example, when an	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. By default, an anonymous user has the same access that is granted to the Everyone group for a particular resource. Enabling this security option allows additional restrictions to be placed on anonymous connections by replacing the Everyone group with Authenticated Users in the security permissions for resources. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the Default Domain Security Policy must be changed to **Enabled**. 1. Double-click **Network access: Do not allow anonymous enumeration of SAM accounts** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** This security policy setting has no impact on domain controllers.					
Network access: Do not allow anonymous enumeration of SAM accounts and shares **Security Objective:** Controls the ability of anonymous users to enumerate Security Accounts Manager (SAM) accounts and shares. Windows Server 2003 allows anonymous users to perform certain activities, such as enumerating the names of domain accounts and network shares. This is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. However, authenticated access is required for the Windows Server 2003 Evaluated Configuration. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Network access: Do not allow anonymous**	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
enumeration of SAM accounts and shares in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** Enabling this security policy setting makes it impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users accessing file and print servers anonymously are unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.					
Network access: Do not allow storage of credentials or .NET Passports for network authentication **Security Objective:** Determines whether the Stored User Names and Passwords tool saves passwords or credentials for later use when it gains domain authentication. This policy setting is **Disabled** by default. If it is **Enabled**, this setting prevents the Stored User Names and Passwords tool from storing passwords and credentials. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **E**nabled in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Network access: Do not allow storage of credentials or .NET Passports for network authentication** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.	✓	✓		✓	
Network access: Let Everyone permissions apply to anonymous users **Security Objective:** Determines if anonymous users are allowed	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
the same permissions as the built-in group Everyone. If this policy is enabled, the Everyone SID is added to the token that is created for anonymous connections. In this case, anonymous users are able to access any resource for which the **Everyone** group has been given permissions. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Disabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Disabled**. 1. Double-click **Network access: Let Everyone permissions apply to anonymous users i**n the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button.					
Network access: Named Pipes that can be accessed anonymously **Security Objective:** Determines which communication sessions (pipes) have attributes and permissions that allow anonymous access. **Procedure:** 1. Double-click **Network access: Named Pipes that can be accessed** anonymously in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. For Stand-alone Server and Domain Security Policies, delete all entries from the text box (see Appendix A for default settings), with the exception of the Print Spooler named pipe (**SPOOLSS**). 4. For Domain Controller Security Policies, delete all entries from the text box (see Appendix A for default settings), with the exception of the Print Spooler named pipe (**SPOOLSS**) and the Local Security Authority Remote Protocol (**LSARPC**). 5. Click the **OK** button. **Notes:**	✓	✓	✓	✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
▪ **SPOOLSS** and **LSARPC** named pipes are used in the Windows Server 2003 Evaluated Configuration. ▪ This setting might impact some services that need to use null session access. For example, Microsoft Commercial Internet System 1.0, which uses the Internet Mail Service, requires the SQL\QUERY pipe on the Structured Query Language (SQL) server in order to work.					
Network access: Remotely accessible registry paths **Security Objective:** This security setting determines which registry paths are accessible after referencing the access control list (ACL) of the **WinReg** key to determine access permissions to those paths. **Procedure:** 6. Double-click **Network access: Remotely accessible registry paths** in the details pane. 7. For domain-level policies, select the **Define these policy settings** check box. 8. Delete all entries from the text box (see Appendix A for default settings) and click the **OK** button. **Note:** Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry in order to properly monitor and manage those systems. Removing the default registry paths from the list of accessible ones could cause those and other management tools to fail.	✓	✓			✓
Network access: Remotely accessible registry paths and subpaths **Security Objective:** This security setting determines which registry paths are accessible after referencing the access control list (ACL) of the **WinReg** key to determine access permissions to those paths. **Procedure:** 1. Double-click **Network access: Remotely accessible registry paths** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box.	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
3. Delete all entries from the text box (see Appendix A for default settings) and click the **OK** button. **Note:** Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry in order to properly monitor and manage those systems. Removing the default registry paths from the list of accessible ones could cause those and other management tools to fail.					
Network access: Restrict anonymous access to named pipes and shares **Security Objective:** Enabling this security setting restricts anonymous access to shares and pipes to the settings for **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously**. This setting controls null session access to shares by adding **RestrictNullSessAccess** with the value 1 in the registry key HKLM\System\CurrentControlSet\Services\LanManServer\Parameters, which is a registry value that toggles null session shares on or off to determine whether the server service restricts access to client's logged on to the system account without user name and password authentication. Enabling this setting restricts null session access to unauthenticated users to all server pipes and shares except those listed in the **NullSessionPipes** and **NullSessionShares** registry entries. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Network access: Restrict anonymous access to named pipes and shares** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.	✓	✓		✓	
Network access: Shares that can be accessed anonymously **Security Objective:** This security setting determines which	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
network shares can be accessed by anonymous users. **Procedure:** 1. Double-click **Network access: Shares that can be accessed anonymously** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Delete all entries from the text box (see Appendix A for default settings) and click the **OK** button.					
Network access: Sharing and security model for local accounts **Security Objective:** This security setting determines how network logons using local accounts are authenticated. If this setting is set to **Classic**, network logons that use local account credentials authenticate by using those credentials. If this setting is set to **Guest only**, network logons that use local accounts are automatically mapped to the Guest account. The Classic model allows fine control over access to resources. By using the **Classic** model, you can grant different types of access to different users for the same resource. By using the **Guest o**nly model, you can have all users treated equally. All users authenticate as Guest, and they all receive the same level of access to a given resource, which can be either Read Only or Modify. There are two models available: ▪ **Classic:** Local users authenticate as themselves ▪ **Guest only:** Local users authenticate as Guest By default, this policy is set to **Classic: Local users authenticate as themselves** on the Windows Server 2003 family and Windows XP Professional computers joined to a domain, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy **Procedure:** For the Evaluated Configuration, the default setting must remain set in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Classic: Local users authenticate as themselves**. 1. Double-click **Network access: Sharing and security model for local accounts** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
3. From the drop-down menu, select **Classic-local users authenticate as themselves** and click the **OK** button. **Note:** When the computer is not joined to a domain, this setting also tailors the **Sharing** and **Security** tabs in Windows Explorer to correspond to the sharing and security model that is being used.					
Network security: Do not store LAN Manager hash value on next password change **Security Objective:** This security setting determines if, at the next password change, the Local Area Network (LAN) Manager hash value for the new password is stored. The LAN Manager (LM) hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT hash. Since the LM hash is stored on the local computer in the security database the passwords can be compromised if the security database is attacked. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Network security: Do not store LAN Manager hash value on next password change** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.	✓	✓		✓	
Network security: Force logoff when logon hours expire **Security Objective:** This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the SMB component. When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's logon hours expire. If this policy is disabled, an established client session is allowed to be maintained after the client's logon hours have expired. By default, this policy is set to **Disabled** in Windows Server 2003, **Disabled** in the Default Domain Security Policy, and **Not defined**	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Network security: Force logoff when logon hours expire** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Notes:** ▪ This security setting behaves as an account policy. For Domain accounts, there can be only one account policy. The account policy must be defined in the Default Domain Security Policy, and it is enforced by the domain controllers that make up the domain. By default, workstations and servers that are joined to a domain (for example, member computers) also receive the same account policy for their local accounts. However, local account policies for member computers can be different from the domain account policy by defining an account policy for the organizational unit that contains the member computers. ▪ This setting does not apply to administrator accounts. ▪ This setting should only be applied from the Default Domain Security Policy.					
Network security: 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 LAN Manager (LM) and New Technology LAN Manager (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,	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
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). By default, this policy is set to **Send NTLM response only** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Send NTLM response only** in the Default Domain Controller Security Policy. 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. Thus, a captured session key serves 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 data**. The key that is used for the encryption of data from the client to the server is different from the one that is used for the encryption of data from the server to the client. **Procedure:** For the Evaluated Configuration, it is recommended that this setting be changed to **Send NTLMv2 response only\refuse LM & NTLM** in the Windows Server 2003 Local Security Policy and in the domain-level policies. 1. Double-click **Network security: LAN Manager**					

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Authentication level in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. From the drop-down menu, select **Send NTLMv2 response only\refuse LM & NTLM** and click the **OK** button.					
Network security: LDAP client signing requirements **Security Objective:** This security setting determines the level of data signing that is requested on behalf of clients issuing Lightweight Directory Access Protocol (LDAP) BIND requests, as follows: ▪ **None:** The LDAP BIND request is issued with the options that are specified by the caller. ▪ **Negotiate signing:** If Transport Layer Security/Secure Sockets Layer (TLS\SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the options specified by the caller. If TLS\SSL has been started, the LDAP BIND request is initiated with the options that are specified by the caller. ▪ **Require signature:** This is the same as Negotiate signing. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. By default, this policy is set to **Negotiate signing** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the **Require signing** option be set in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Require signing**. 1. Double-click **Network security: LDAP client signing requirements** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. From the drop-down menu, select **Require signing** and click the **OK** button. **Note:** If the setting is changed to **Require signing**, it must also be changed on the LDAP server (domain controller) by way of the **Domain controller: LDAP server signing requirements**	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
security option, otherwise there will be a loss of connection with the server.					
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients **Security Objective:** This security setting allows a client to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value. ▪ **Require message integrity**: The connection fails if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with by attaching a cryptographic signature which identifies the sender and is a numeric representation of the contents of the message. This signature ensures that the message has not been tampered with. ▪ **Require message confidentiality**: The connection fails if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted. ▪ **Require NTLMv2 session security**: The connection fails if the NTLMv2 protocol is not negotiated. ▪ **Require 128-bit encryption**: The connection fails if strong encryption (128-bit) is not negotiated. By default, this policy is set to **No minimum** (no options selected) in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to select all options listed earlier in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to select all options listed earlier. 1. Double-click **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select all of the options by checking the selection box for each of the options presented and click the **OK** button.		✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers **Security Objective:** This security setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value. ▪ **Require message integrity**: The connection fails if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with by attaching a cryptographic signature which identifies the sender and is a numeric representation of the contents of the message. This signature ensures that the message has not been tampered with. ▪ **Require message confidentiality**: The connection fails if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted. ▪ **Require NTLMv2 session security**: The connection fails if the NTLMv2 protocol is not negotiated. ▪ **Require 128-bit encryption**: The connection fails if strong encryption (128-bit) is not negotiated. By default, this policy is set to **No minimum** (no options selected) in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to select all options listed earlier in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to select all options listed earlier. 1. Double-click **Network security: Minimum session security for NTLM SSP-based (including secure RPC) servers** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select all of the options by checking the selection box for each of the options presented and click the **OK** button.	✓	✓		✓	
Recovery console: Allow automatic administrative logon **Security Objective:** By default, the Recovery Console requires that a password be provided the for the Administrator account before	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
accessing the system. If this option is enabled, the Recovery Console does not require a password and automatically logs on to the system. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Disabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Disabled**. 1. Double-click **Recovery console:** Allow automatic administrative logon in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Note:** The Windows Recovery Console is not part of the Evaluated Configuration.					
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 in Windows Server 2003. By default, this policy is set to **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Disabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Disabled. 1. Double-click **Recovery Console: Allow Floppy Copy and Access to All Drives and Folders** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button. **Note:** The Windows Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.					
Shutdown: Allow system to be shut down without having to log on **Security Objective:** This security setting determines whether a computer can be shut down without having to log on to Windows. When this policy is enabled, the **Shut Down** command is available on the Windows logon screen. When this policy is disabled, the option to shut down the computer does not appear on the Windows logon screen. In this case, users must be able to log on to the computer successfully and have the **Shut down the system** user right before they can perform a system shutdown. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain Disabled in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Disabled**. 1. Double-click **Shutdown: Allow system to be shut down without having to log on** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Disabled** radio button and click the **OK** button.	✓	✓		✓	
Shutdown: Clear virtual memory pagefile **Security Objective:** This security setting determines whether the virtual memory pagefile is cleared when the system is shut down. Virtual memory support uses a system pagefile to swap pages of memory to disk when they are not used. On a running system, this	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
pagefile is opened exclusively by the operating system, and it is well protected. However, when a file is encrypted or decrypted, plaintext data can be paged. This can be a security problem if an attacker boots the system by using another operating system and opens the paging file. To avoid this problem ensure that the system pagefile is wiped clean when this system shuts down. This ensures that sensitive information from process memory that might go into the pagefile is not available to an unauthorized user who manages to directly access the pagefile. When this policy is enabled, it causes the system pagefile to be cleared upon clean shutdown. If this security option is enabled, the hibernation file (hiberfil.sys) is also zeroed out when hibernation is disabled on a portable computer system. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **Shutdown: Clear virtual memory pagefile** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** Shutting down and restarting the server will take longer and will be especially noticeable on servers with large paging files. For a server with 2 GB of RAM and a 2 GB paging file, this setting may add 20 to 30 minutes, or more time, to the shutdown process. For some organizations, this downtime violates their internal service level agreements. Therefore, use caution when implementing this countermeasure in your environment.					

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
System cryptography: Force strong key protection for user keys stored on the computer **Security Objective:** This security setting determines whether users can use private keys, such as their S-MIME key, without a password. The possible values for this Group Policy setting are: ▪ User input is not required when new keys are stored and used ▪ User is prompted when the key is first used ▪ User must enter a password each time they use a key By default, this policy is set to **Not defined** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that, at a minimum, the **User is prompte**d when the key is first used option be set in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **User is prompted when the key is first used**. 1. Double-click **System cryptography: Force strong key protection for user keys stored on the computer** in the details pane. 2. For domain-level policies, select **the Define these policy settings** check box. 3. From the drop-down menu, select **User is prompted when the key is first used** and click the **OK** button. **Note:** If the **User must enter a password each time they use a key** option is selected, users have to enter their password every time they access a key stored on their computer. For example, if users use an S-MIME certificate to digitally sign their e-mail they are forced to enter the password for that certificate every time they send a signed e- mail message. For some organizations the overhead involved using this configuration may be too extensive, at a minimum they should set it to **User is prompted when the key is first used**.	✓	✓			✓
System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing **Security Objective:** This security setting determines if the Transport Layer Security/Secure Sockets Layer (TL/SS) Security	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, this means that the provider only supports the Transport Layer Security (TLS) protocol as a client and as a server (if applicable). It uses only the Triple DES encryption algorithm for the TLS traffic encryption, only the Rivest, Shamir, and Adleman (RSA) public key algorithm for the TLS key exchange and authentication, and only the Secure Hashing Algorithm 1 (SHA-1) for the TLS hashing requirements. For Encrypting File System Service (EFS), it supports only the Triple Data Encryption Standard (DES) encryption algorithm for encrypting file data supported by the NTFS file system. By default, EFS uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key in the Windows Server 2003 family and DESX algorithm in Windows XP for encrypting file data. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button. **Note:** Enabling this Security Option could result in an inability to connect to Web sites using SSL, depending on the encryption algorithm used at the site(Ref: National Security Agency (NSA) Guide to Securing Windows XP, Version 1.1). Clients with this setting enabled are unable to communicate by way of digitally encrypted or signed protocols with servers that do not support these algorithms. Network clients that do not support these algorithms are unable to use servers that require them for network communications.					
System Objects: Default owner for objects created by members of the Administrators group **Security Objective:** This security setting determines whether the Administrators group or an object creator will be the default owner of any system objects created.	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
By default, this policy is set to **Administrators group** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must be changed to **Object creator** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Object creator**. 1. Double-click **System Objects: Default owner for objects created by members of the Administrators group** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. From the drop-down menu, select **Object creator** and click the **OK** button. **Note:** To ensure accountability, object creators should be the default owners. Administrators can always take ownership if needed. Taking ownership will create a privilege use audit event.					
System Objects: Require case insensitivity for non-Windows subsystems **Security Objective:** This security setting determines whether case insensitivity is enforced for all subsystems. The Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as such as Portable Operating System Interface for UNIX (POSIX). If this setting is enabled, case insensitivity is enforced for all directory objects, symbolic links, and IO objects, including file objects. Disabling this setting does not allow the Win32 subsystem to become case sensitive. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** It is recommended that the default **Enabled** setting be maintained in the Windows Server 2003 Local Security Policy and that the default setting in the domain-level policies be changed to **Enabled**. 1. Double-click **System Objects: Require case insensitivity for non-Windows subsystems** in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box.	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
3. Select the **Enabled** radio button and click the **OK** button.					
System Objects: ***Strengthen default permissions of internal system objects (e.g., Symbolic Links)*** **Security Objective:** This security setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as Disk Operating System (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 and what permissions are granted. If this policy is enabled, the default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create. By default, this policy is set to **Enabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, this setting must remain **Enabled** in the Windows Server 2003 Local Security Policy and the default setting in the domain-level policies must be changed to **Enabled**. 1. Double-click **System Objects:** Strengthen default permissions of internal system objects (e.g., Symbolic Links) in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Select the **Enabled** radio button and click the **OK** button.	✓	✓		✓	
System Settings: Optional Subsystems **Security Objective:** This security setting determines which subsystems support local applications. With this security setting, administrators can specify as many support subsystems as the environment demands. By default, this policy only includes the **POSIX** subsystem in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** For the Evaluated Configuration, all optional subsystems must be removed from the Windows Server 2003 Local	✓	✓		✓	

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Security Policy and the default setting in the domain-level policies. 1. Double-click System Settings: Optional Subsystems in the details pane. 2. For domain-level policies, select the **Define these policy settings** check box. 3. Delete all entries from the text box and click the **OK** button. **Notes:** ▪ The POSIX subsystem is not included in the Evaluated Configuration. ▪ The POSIX subsystem is an Institute of Electrical and Electronic Engineers (IEEE) standard that defines a set of operating system services. The POSIX subsystem is required if the server supports applications that use that subsystem. The POSIX subsystem introduces a security risk relating to processes that can potentially persist across logons. That is, if a user starts a process and then logs out, there is a potential that the next user who logs in to the system could access the previous user's process. This is dangerous because the process started by the first user may retain that users system privileges; anything the second user does with that process is performed with the privileges of the first user.					
System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies **Security Objective:** This security setting determines if digital certificates are processed when a user or process attempts to run software with an.exe file name extension. This security setting enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, authorized administrators can create a certificate rule that will allow or disallow the running of Authenticode® – signed software, based on the digital certificate that is associated with the software. In order for certificate rules to take effect, authorized administrators must enable this security setting. By default, this policy is set to **Disabled** in Windows Server 2003, **Not defined** in the Default Domain Security Policy, and **Not defined** in the Default Domain Controller Security Policy. **Procedure:** The Verification of Authenticode® – signatures is not included in the Evaluated Configuration. It is recommended that the default security policy setting not be changed. **Note:** Enabling certificate rules results in software restriction policies	✓	✓			✓

Security Options	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
checking a certificate revocation list (CRL) to ensure the software's certificate and signature are valid. This may decrease performance when starting signed programs.					

Additional Security Settings

The additional security settings described in this section 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 Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

Information about how to edit the registry is also available in the online Help of the Registry Editor..

For instructions about how to add a key to the registry

1. Click **Start** and select **Run**.
2. Type **regedit** and click **OK** to open the Registry Editor.
3. From the **Help** menu, select **Help Topics**.
4. In the **Contents** tab, click the **Registry Edit**or document object.
5. Click the **How to** submenu, and then select the **Change Keys and Values** link. The left pane provides a list of help topics (shown as hyperlinks) for adding, deleting, or modifying information in the registry. Click the desired hyperlink to obtain the detailed instructions.

Warning: Using the Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from use of the Registry Editor can be solved.

Required Registry Settings

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

Disabling DirectDraw Acceleration

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

Disable DirectDraw acceleration by editing the registry and changing the **Timeout** value to **0** as shown in Table 5.7.

Table 5.7 Disabling DirectDraw acceleration

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

Disabling Unnecessary Devices

For the Evaluated Configuration, it is necessary to disable all of the devices listed in Table 5.8 by editing the registry and changing the **Start** value to **4** as shown in Table 5.8. Some of the registry keys and values might need to be created.

Table 5.8 Disabling unnecessary devices

HKLM\SYSTEM\CurrentControlSet\Services		Format	Value
Key: arp1394	**Value Name:** Start	REG_DWORD	4
Key: Atmarpc	**Value Name:** Start	REG_DWORD	4
Key: audstub	**Value Name:** Start	REG_DWORD	4
Key: cdac15ba	**Value Name:** Start	REG_DWORD	4
Key: cdad10ba	**Value Name:** Start	REG_DWORD	4
Key: crcdisk	**Value Name:** Start	REG_DWORD	4
Key: IRENUM	**Value Name:** Start	REG_DWORD	4
Key: mnmdd	**Value Name:** Start	REG_DWORD	4
Key: mssmbios	**Value Name:** Start	REG_DWORD	4
Key: ndproxy	**Value Name:** Start	REG_DWORD	4
Key: nic1394	**Value Name:** Start	REG_DWORD	4
Key: NwlnkFlt	**Value Name:** Start	REG_DWORD	4
Key: NwlnkFwd	**Value Name:** Start	REG_DWORD	4
Key: Ohci1394	**Value Name:** Start	REG_DWORD	4
Key: parvdm	**Value Name:** Start	REG_DWORD	4
Key: PDCOMP	**Value Name:** Start	REG_DWORD	4
Key: PDFRAME	**Value Name:** Start	REG_DWORD	4
Key: PDRELI	**Value Name:** Start	REG_DWORD	4
Key: PDRFRAME	**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

HKLM\SYSTEM\CurrentControlSet\Services		Format	Value
Key: RDPCDD	**Value Name:** Start	REG_DWORD	4
Key: rdpdr	**Value Name:** Start	REG_DWORD	4
Key: rdpwd	**Value Name:** Start	REG_DWORD	4
Key: sacdrv	**Value Name:** Start	REG_DWORD	4
Key: secdrv	**Value Name:** Start	REG_DWORD	4
Key: tdpipe	**Value Name:** Start	REG_DWORD	4
Key: tdtcp	**Value Name:** Start	REG_DWORD	4
Key: TermDD	**Value Name:** Start	REG_DWORD	4
Key: wanarp	**Value Name:** Start	REG_DWORD	4
Key: wdica	**Value Name:** Start	REG_DWORD	4
Key: wlbs	**Value Name:** Start	REG_DWORD	4

Preventing Interference of the Session Lock from Application-generated Input

Windows Server 2003 includes a registry key value that can be used to prevent application-generated keyboard/mouse input messages from interfering with the session lock. The key name is **BlockSendInputResets** and resides in the following subkey:

HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop
Policy takes precedence over the user-applied setting. The data type is REG_SZ, and is interpreted as a Boolean value. A non–zero value means the key is enabled and the feature is active. A zero value (or nonexistent key) means that the current functionality is maintained.

When this key is set, only real (user-invoked) mouse or keyboard input will reset the screen saver's timer. Currently there are three cases where injected inputs will reset the time.

- **Input injected using SendInput** – This is the case where an application is intentionally trying to simulate input and is blocked.
- **Window activation** – When a new window becomes active the counter is reset. This is blocked unless the screen saver is already active.
- **Calls to SystemParametersInfo()** that set SPI_SETSCREENSAVETIMEOUT, SPI_SETSCREENSAVEACTIVE, SPI_SETLOWPOWERTIMEOUT, SPI_SETLOWPOWERACTIVE, SPI_SETPOWEROFFTIMEOUT, or SPI_SETPOWEROFFACTIVE. These no longer result in the timer being reset if **BlockSendInputResets** is enabled. This should not have an effect on user experience, because setting these values results in real input from the user's mouse movement and keystrokes.

To enable this capability, edit the registry key value as shown in Table 5.9. The subkey must be created under the HKCU\Software\Policies \Microsoft key, along with the necessary value.

Table 5.9 Preventing session-lock interference from application-generated input

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

It is important to note that, for this feature to work effectively, the appropriate screen saver settings must be set in conjunction with this registry key. The necessary screen saver settings are:

- A selected screen saver
- Enabled password protection
- A configured screen saver timeout period

If the screen saver is not properly configured, this feature has no effect on the computer's overall security. See Automatic Screen Lock Protection for procedures for setting a password-protected screen saver.

Generating an Audit Event when the Audit Log Reaches a Percentage Full Threshold

Windows Server 2003 supports a feature for generating a security audit in the security event log when the size of the Security log reaches a configurable threshold. To enable this capability, create the subkey shown in Table 5.10 with a value setting that designates the percentage full amount that generates the event in the Security log. The value shown in the table is a recommendation and can be configured to an appropriate value based on local operational needs.

For example, if set to 90 as shown, when the Security log size reaches 90%, the Security log generates event ID 523: "The security event log is 90 percent full."

Table 5.10 Enabling audit events for percentage full threshold

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

Note: This setting is not effective if the log retention method is set to **Overwrite events as needed**.

Generating Administrative Alert Message when the Audit Log is Full

When an audit log percentage full threshold is set, an event is written to the log when the specified threshold value is reached. However, authorized administrators are not made aware of the event until they review the audit log, unless an administrator enables an alert. Alert messages appear in a message box on the specified desktop specified. To enable the system to send popup alert messages to a specific authorized administrator's user or computer account, edit the subkey value shown in Table 5.11 by entering a list of user and/or computer names. When entering the list of names via a security template, use a comma-separated list; when the names are entered into the registry manually, use a return separated list. If a computer name is entered, the system sends the message to the current user of that computer. If the value of this entry is blank, the system does not send a message.

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.

Table 5.11 Enabling administrative alert messages for percentage full threshold

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

Note: The security templates provided with this document have this registry value set to send alerts to the Administrator account. To send the alerts to other user or computer accounts when a security template is applied, modify this setting in the template prior to applying it to a local or domain level security policy. Note also that the settings in a domain security policy will override corresponding policy settings on a local security policy.

Removing the Default IPSec Exemptions

Some types of traffic are exempted from being secured by Internet Protocol Security (IPSec), even when the IPSec policy specifies that all IP traffic should be secured. This is by design. The IPSec exemptions apply to Broadcast, Multicast, Resource Reservation Setup Protocol (RSVP), Internet Key Exchange (IKE), and Kerberos traffic. For details about these exemptions, please refer to the following Microsoft Knowledge Base articles:

- 254949 — IPSec support for client-to-domain controller traffic and domain controller-to-domain controller traffic (http://support.microsoft.com/kb/254949)
- 810207 — IPSec default exemptions are removed in Windows Server 2003 (http://support.microsoft.com/kb/810207)

Because exemption can be used by an attacker to circumvent IPSec restrictions, it is important to remove it. On systems that do not use IPSec, this setting has no effect. To remove the default IPSec exemptions, edit the registry value shown in Table 5.12. For more information about this setting, please refer to Microsoft Knowledge Base article 811832: IPSec Default Exemptions Can Be Used to Bypass IPSec Protection in Some Scenarios (http://support.microsoft.com/kb/811832).

Table 5.12 Removing default IPSec exemptions

HKLM\SYSTEM\CurrentControlSet\Services		Type	Value
Key: IPSEC	**Value Name:** NoDefaultExempt	REG_DWORD	1

Raw TCP/IP Sockets

Review the registry key shown in Table 5.13 to ensure the **AllowUserRawAccess** value is either not present or is set to **0** (where **0** = false, **1** = true). This parameter controls access to raw Transmission Control Protocol/Internet Protocol (TCP/IP) sockets. If true, non-administrative users have access to raw sockets. By default, the system responds as if the value is false so that only administrators have access to raw sockets. To ensure compliance with the Evaluated Configuration, it is required that only administrators have access to raw sockets.

Table 5.13 Disabling user access to raw TCP/IP sockets

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip		Format	Value
Key: Parameters	**Value Name:** AllowUserRawAccess	REG_DWORD	0

Disabling Remote Assistance

The Remote Assistance feature available through Help and Support allows control of the computer to be shared with someone else over a network. For the Evaluated Configuration, this capability must not be allowed. Disable the Remote Assistance feature by editing the registry and changing the values shown in Table 5.14 to **0**.

Table 5.14 Disabling remote assistance

HKLM\SYSTEM\CurrentControlSet\Control		Type	Value
Key: Terminal Server	**Value Name:** fEnableSalem	REG_DWORD	0
Key: Terminal Server	**Value Name:** fAllowToGetHelp	REG_DWORD	0
Key: Terminal Server	**Value Name:** fAllowUnsolicited	REG_DWORD	0
Key: Terminal Server	**Value Name:** fAllowUnsolicitedFullControl	REG_DWORD	0
Key: Terminal Server	**Value Name:** RAUnsolicited	REG_DWORD	0

Disable Remote Mmanagement of DNS Servers over RPC

Disable the ability to access and manage DNS servers remotely by using the RPC protocol. To set this value, edit the registry as shown in Table 5.15 and create the value name **RpcProtocol** with a value of **4**.

Table 5.15 Disable remote management of DNS over RPC

HKLM\SYSTEM\CurrentControlSet\Services\DNS\		Format	Value
Key: Parameters	**Value Name:** RpcProtocol	REG_DWORD	4

Recommended Registry Settings

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

Screen Saver Password Protection

The grace period allowed for user movement before screen saver 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 as shown in Table 5.16 and create the value name **ScreenSaverGracePeriod** with a value of **0**.

Table 5.16 Setting screen saver grace period

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

Time Service Authentication

Review the key shown in Table 5.17 to ensure that the data type is set to **Nt5DS**. This ensures the Evaluated Configuration is operating with authenticated time service.

Table 5.17 Setting time service authentication

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

Disabling Autorun

Autorun begins reading from a drive as soon as media is inserted in it. As a result, the setup files on program disks and the sounds on audio media start immediately. To prevent a possible malicious program from starting when media is inserted, create the registry value shown in Table 5.18 to disable autorun on all drives.

Table 5.18 Disabling autorun

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

Audit Log Management

Management options for event logs, including the Security log, can be configured for all computers in a domain by using the Event Log folder within the Domain Security Policy or a specific Group Policy object associated with domains, Organizational Units (OUs), and sites. 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.

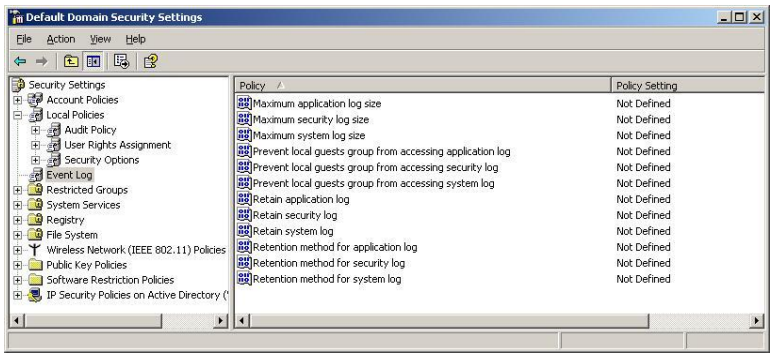
These interfaces allow for viewing, sorting, filtering, and searching the event logs as well as setting the maximum log size or clearing the log. The user must have access to the event log file in order to successfully view it. To view the contents of the Security log, the user must be logged on as a 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.

Event Log Settings

View and edit current settings for event logs.

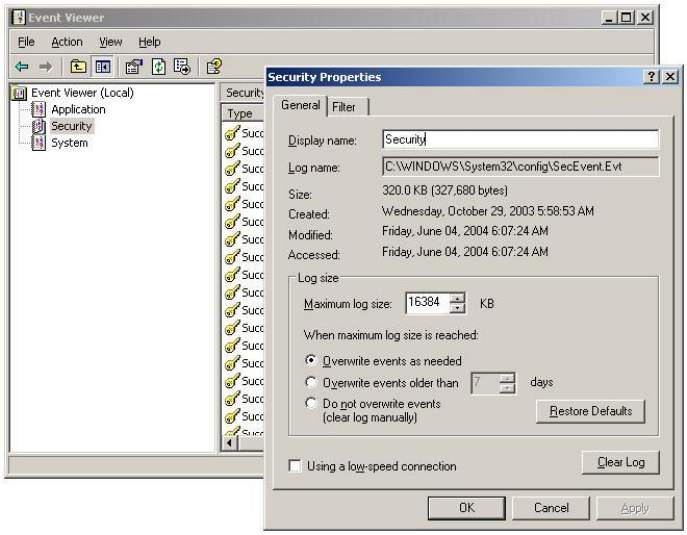
Procedure for domain and domain controller policies

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand **Security Settings**.
3. Expand **Event Log** to reveal the Settings for Event Logs policy.
4. Click the **Settings for Event Logs** object. The configurable audit log management settings are displayed in the details pane.



Procedure for stand-alone workstations and servers

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



3. Set the **Audit Policies** as required or recommended in Table 5.19.

Table 5.19 Audit management settings

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Maximum Application log size **Security Objective:** Specifies the maximum size for the Application event log. The default is 16,384 KB, and the maximum size is 4 GB (4,194,240 KB). Requirements for the Application log size vary depending on the function of the platform and the need for historical records of application related events. **Procedure for domain and domain controller policies:** 4. Double-click **Maximum Application log size** in the details pane. 5. Select the **Define this policy setting box**. 6. 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 are manually reviewed, archived, and cleared, including the amount of disk space that is available. 7. Click the **OK** button.		✓	✓		✓
Procedure for Stand-alone Windows Server 2003: 0. 1. In the Application Log Properties interface, 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 are manually reviewed, archived, and cleared, including the amount of disk space that is available. 2. Click the **OK** button.	✓				✓
Maximum Security log size **Security Objective:** Specifies the maximum size for the Security event log. The default is 16,384 KB on Windows Server 2003 stand-alone and domain member servers and 13,1072 KB on Windows Server 2003 domain controllers, and the maximum size is 4 GB. **Procedure for domain and domain controller policies:** 1. Double-click Maximum Security log size in the details pane.		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
2. Select the **Define this policy setting box**. 3. 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 are manually reviewed, archived, and cleared, including the amount of disk space that is available. 4. Click the **OK** button.					
Procedure for stand-alone Windows Server 2003: 1. In the Security Log Properties interface, 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 are manually reviewed, archived, and cleared, including the amount of disk space that is available. 2. Click the **OK** button.	✓				✓
Maximum System log size **Security Objective:** Specifies the maximum size for the System event log. The default is 16,384 KB, and the maximum size is 4 GB. **Procedure for domain and domain controller policies:** 1. Double-click **Maximum System log size** in the details pane. 2. Select the **Define this policy setting box**. 3. 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 are manually reviewed, archived, and cleared, including the amount of disk space that is available. 4. Click the **OK** button.		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Procedure for stand-alone Windows Server 2003: 1. In the System Log Properties interface, on 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 are manually reviewed, archived, and cleared. 2. Click the **OK** button.	✓				✓
Prevent local guests group from accessing 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 Enabled on all Windows Server 2003 operating systems. **Procedure:** It is recommended that the default settings be maintained in all domain-level policies. This policy setting is not available in the Windows Server 2003 Local Security Policy. **Note:** All Windows Server 2003 and Windows XP Professional operating systems (including domain members) enforce restrictions on guest access to the application event logs by default through a value of **1** set on the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess		✓	✓		✓
Prevent local guests group from accessing 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 enabled on all Windows Server 2003 editions. A user must possess the Manage auditing and Security log user right in order to access the Security log. **Procedure:** It is recommended that the default settings be maintained in all domain-level policies. This policy setting is not available in the Windows Server 2003 Local Security Policy. **Note:** All Windows Server 2003 and Windows XP Professional operating systems (including domain members) enforce restrictions on guest access to the application event logs by default through a value of **1** set on the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Security\Application\RestrictGuestAccess		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Prevent local guests group from accessing 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 enabled on all Windows Server 2003 editions. **Procedure:** It is recommended that the default settings be maintained in all domain-level policies. This policy setting is not available in the Windows Server 2003 Local Security Policy. **Note:** All Windows Server 2003 and Windows XP Professional operating systems (including domain members) enforce restrictions on guest access to the application event logs by default through a value of **1** set on the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System\RestrictGuestAccess		✓	✓		✓
Retain application log **Security Objective:** Determines the number of days that events should be retained in the Application log if the **Retention Method for Application Log** is set to **Overwrite events by days i**n a domain policy, or if the **Overwrite events older than** option is selected in the **Application Log Properties** of a stand-alone server. Set this value only if the log is archived at scheduled intervals and ensure that the maximum Application log size is large enough to accommodate the interval. By default, Windows Server 2003 operating systems have a retention method set to **Overwrite events as needed**, which does not require this policy setting. **Procedure for domain and domain controller policies:** It is recommended that the default setting of **Not defined** be maintained in all domain-level policies.		✓	✓		✓
Procedure for stand-alone Windows Server 2003: See ***Retention method for Application log*** later in this table	✓				✓
Retain security log **Security Objective:** Determines the number of days of events that should be retained for the Security log if the retention method for Security 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** of a stand-alone workstation or		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
server. Set this value only if the log is archived at scheduled intervals and ensure that the maximum Security log size is large enough to accommodate the interval. By default, Windows Server 2003 operating systems have a retention method set to **Overwrite events as needed**, which does not require this policy setting. **Procedure for domain and domain controller policies:** It is recommended that the default setting of **Not defined** be maintained in all domain-level policies.					
Procedure for stand-alone Windows Server 2003: See ***Retention method for Security log*** later in this table.	✓				✓
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 System 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** of a stand-alone workstation or server. Set this value only if the log is archived at scheduled intervals and ensure that the maximum System log size is large enough to accommodate the interval. By default, Windows Server 2003 operating systems have a retention method set to Overwrite events as needed, which does not require this policy setting. **Procedure for domain and domain controller policies:** It is recommended that the default setting of **Not defined** be maintained in all domain-level policies.		✓	✓		✓
Procedure for Stand-alone Windows Server 2003: See ***Retention method for System log*** later in this table.	✓				✓
Retention method for Application log **Security Objective:** Determines how Application logs that have reached their maximum size are handled by the operating system. By default, Windows Server 2003 editions have a retention method set to **Overwrite events as needed**.		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Procedure for domain and domain controller policies: It is recommended that the default setting of **Not defined** be maintained in all domain-level policies.					
Procedure for stand-alone Windows Server 2003: Do not change the **Overwrite events as needed** option in the Application Log Properties interface.	✓				✓
Retention method for Security log **Security Objective:** Determines how Security logs that have reached their maximum size are handled by the operating system. By default, Windows Server 2003 editions have a retention method set to **Overwrite events as needed**. **Procedure for domain and domain controller policies:** It is recommended that the default setting of **Not defined** be maintained in all domain-level policies.		✓	✓		✓
Procedure for stand-alone Windows Server 2003: Setting this policy to **Do not overwrite events (clear log manually)** is recommended at the Local Policy level for critical systems, but requires that a strict audit management process be in place for reviewing, archiving, and clearing the audit logs on a regular basis. Otherwise retain the default setting. 1. In the Security Log Properties interface, on the **General** tab, select the **Do not overwrite events (clear log manually)** radio button. 2. Click the **OK** button.	✓				✓
Retention method for System log **Security Objective:** Determines how System logs that have reached their maximum size are handled by the operating system. By default, Windows Server 2003 editions have a retention method set to **Overwrite events as needed**. **Procedure for domain and domain controller policies:** It is recommended that the default setting of Not defined be maintained in all domain-level policies.		✓	✓		✓

Audit Management and Configuration	Stand-alone Server	Domain Security Policy	DC Security Policy	Required	Recommended
Procedure for stand-alone Windows Server 2003: Do not change the **Overwrite events as needed** option in the System Log Properties interface.	✓				✓

Default Group Accounts

This section discusses required and recommended changes to default group memberships for the built-in groups found in default Windows Server 2003 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:

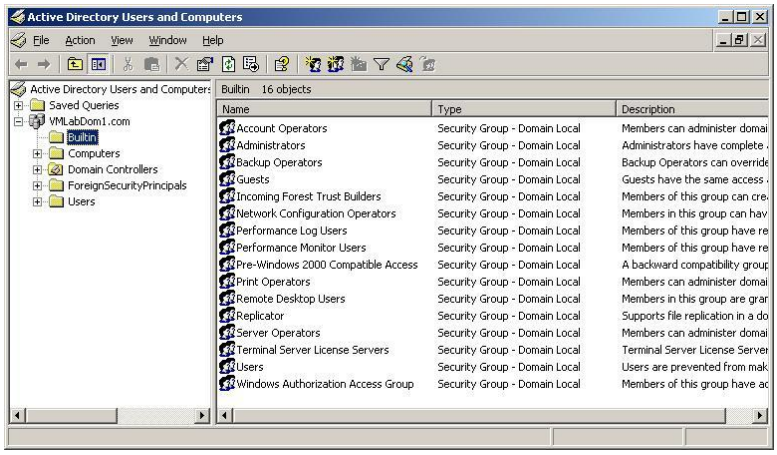
- **Global Groups.** When a Windows Server 2003 domain is established, built-in global groups are created in the Active Directory store. Global groups are used to group common types of user and group accounts for use throughout the entire domain.
- **Domain Local Groups.** Domain local groups provide users with privileges and permissions to perform tasks specifically on the domain controller and in the Active Directory store.
- **Local Groups.** Stand-alone Windows Server 2003, member servers, and Windows XP Professional domain members 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 Server 2003 operating systems automatically, but are not shown in the group administration graphical user interfaces (GUI).

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.

Group Account Memberships for a Domain

To access group accounts within a domain

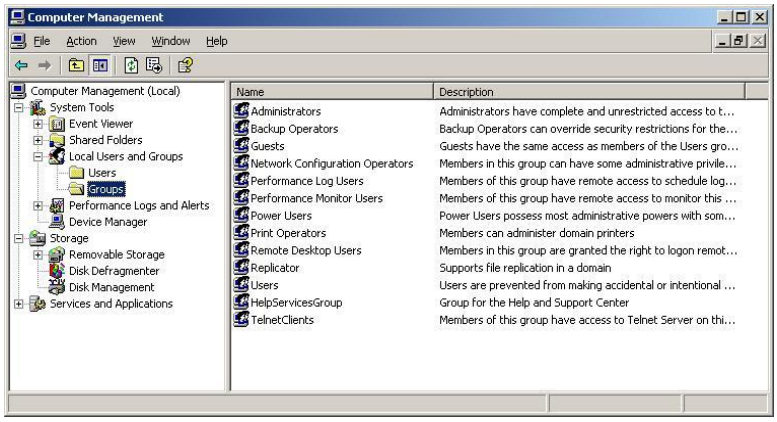
1. Log on to the domain controller as an authorized administrator.
2. Open **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, double-click the domain node.
4. Group accounts are found in the **Builtin and Users** containers.



Group Account Memberships for a Stand-alone Computer

To access group accounts within a stand-alone or individual domain member computer

1. Log on as an authorized administrator.
2. Open **Start**, point to **Administrative Tools**, and then click **Computer Management**.
3. In the console tree, double-click **Local Users and Groups**.
4. Group accounts are found in the **Groups** container.



5. Set up group memberships as required or recommended in Table 5.20.

Table 5.20 Windows Server 2003 group account modifications

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Global Groups	**Default Members**	**Modification / Verification**				
DnsUpdateProxy	None	Do not add accounts to this group.		✓	✓	
Domain Admins	Administrator	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Domain Guests	Guest	Do not add accounts to this group. This is the primary group for the Guest account on a domain controller. Ensure the Guest account is disabled.		✓	✓	
Domain Users	Administrator Krbtgt SUPPORT_388945a0 (All new domain user accounts are added by default)	The SUPPORT_388945a0 account is disabled by default, but may be removed from this group if desired. This may require changing its default primary group (create a new group, make the user a member of that new group, and then change the user's primary group to the new group account), or by deleting the account from the computer. Do not add accounts that allow unauthenticated access to this group.		✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Enterprise Admins	Administrator (domain controller Administrator account)	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Group Policy Creator Owner	Administrator	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Schema Admins	Administrator	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Domain Local Groups	**Default Members**	**Modification / Verification**				
Account Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Administrators	Administrator Domain Admins Enterprise Admins	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Backup Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Cert Publishers	Certification Authority hosts.	Do not add users to this group. Ensure that only authorized Certification Authority hosts are added to this group.		✓	✓	
DnsAdmins	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Guests	Guest (local) Domain Guests	Do not use this group.		✓	✓	
HelpServicesGroup	SUPPORT_388945a0	Do not grant resource permissions or add user accounts to this group. Ensure the SUPPORT_388945a0 account is disabled or deleted from the system.		✓	✓	
Incoming Forest Trust Builders	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Network Configuration Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Performance Log Users	NETWORK SERVICE	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Performance Monitor users	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Pre-Windows 2000 Compatible Access	Authenticated Users	Provides backward compatibility with pre-Windows 2000 operating systems. Does not meet objectives of the TOE, therefore, remove Authenticated Users and do not add other accounts to this group.		✓	✓	
Print Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Remote Desktop Users	None	Do not grant resource permissions or add user accounts to this group.		✓	✓	
Replicator	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	
Server Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.		✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	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.		✓	✓	
Windows Authorization Access Group	ENTERPRISE DOMAIN CONTROLLERS	Maintain the default memberships and do not add accounts to this group.		✓	✓	
Local Groups	**Default Members**	**Modification / Verification**				
Administrators	**Stand-alone:** Administrator **Domain member:** Administrator Domain Admins	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Backup Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
DHCP Administrators (installed with the DHCP Server service)	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
DHCP Users (installed with the DHCP Server service)	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Guests	**Stand-alone:** Guest **Domain member:** Guest Domain Guests	Do not use this group. Remove all accounts, including Guest, from this group.	✓		✓	
HelpServicesGroup	**Stand-alone:** SUPPORT_388945a0 **Domain member:** SUPPORT_388945a0	Do not grant resource permissions or add user accounts to this group. Ensure the SUPPORT_388945a0 account is disabled or deleted from the system.	✓		✓	
IIS_WPG (installed with IIS 6.0)	**Stand-alone:** IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE SYSTEM **Domain member:** IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE SYSTEM	This is a group account for IIS services. Do not add users to this group.	✓		✓	
Network Configuration Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Performance Log Users	NETWORK SERVICE	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Performance Monitor users	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Power Users	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Print Operators	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Remote Desktop Users	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	
Replicator	None	Only add accounts that have been authorized to perform the administrative functions supported by this group.	✓		✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
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 group to prevent the potential for anonymous access to a resource.	✓	✓	✓	
BATCH	All users that have logged on through a batch queue facility.	Do not use this group. Do not grant resource permissions or user rights to this group.	✓	✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
CREATOR GROUP	A placeholder in an inheritable Access Control Entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's current owner.	Improper use may allow all members of a group access to an object creator's resources. Use the CREATOR GROUP placeholder only in cases where all members of a group are to be allowed access to an object creator's resources. Otherwise, use the CREATOR OWNER placeholder instead to ensure that only the object creator is granted access.	✓	✓	✓	
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.	✓	✓	✓	
Everyone	All users accessing the computer, either locally, through the network, or through Remote Access Service (RAS). By default, Everyone includes Authenticated Users and Guests, but not ANONYMOUS LOGON.	Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.	✓	✓	✓	
INTERACTIVE	This group includes all users who log on to Windows Server 2003 locally.	Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.	✓	✓	✓	
NETWORK	This group includes all users who are connected to resources across a network, but does not include those who are connected interactively.	Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.	✓	✓	✓	

Windows Server 2003 Group Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
REMOTE INTERACTIVE LOGON	This group includes all users who log on to the computer by using a Remote Desktop connection.	Do not assign resource permissions or user rights to this account.	✓	✓	✓	
SERVICE	All security principals logged on as a service.	This is a service account. Instead of this account, use the more explicit NETWORK SERVICE or LOCAL SERVICE accounts in order to better control service rights.	✓	✓	✓	
SYSTEM	An identity that is used locally by the operating system and by services configured to log on as LocalSystem. SYSTEM is a hidden member of Administrators. That is, any process running as SYSTEM has the SID for the built-in Administrators group in its access token.	Where specific service rights need to be granted, use the NETWORK SERVICE or LOCAL SERVICE accounts in order to avoid granting full SYSTEM rights to the service.	✓	✓	✓	
TERMINAL SERVER USER	All users who log on to a Terminal Services server.	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 section describes required and recommended changes to built-in user accounts found in default Windows Server 2003 installations.

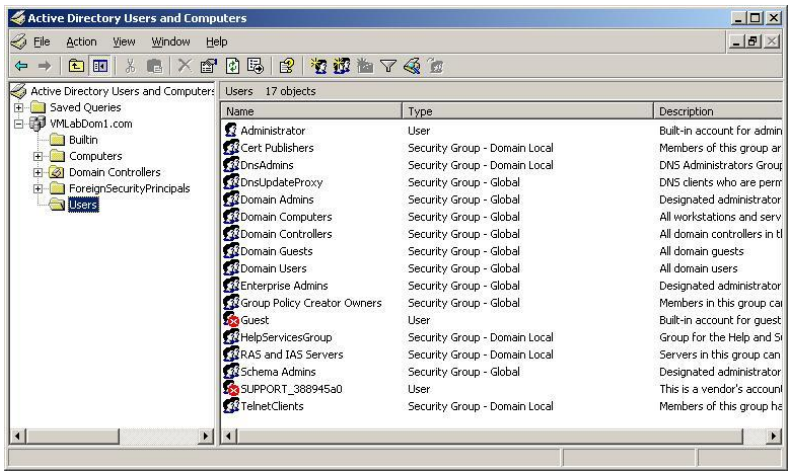
Note: Appendix D – User and Group Accounts, provides a complete description of the default group account settings to be maintained in the Evaluated Configuration, including additional details, applicable ST requirements, and recommended changes.

Default User Accounts for a Domain

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

To access user accounts within a domain

1. Log on to the domain controller as an authorized administrator.
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.

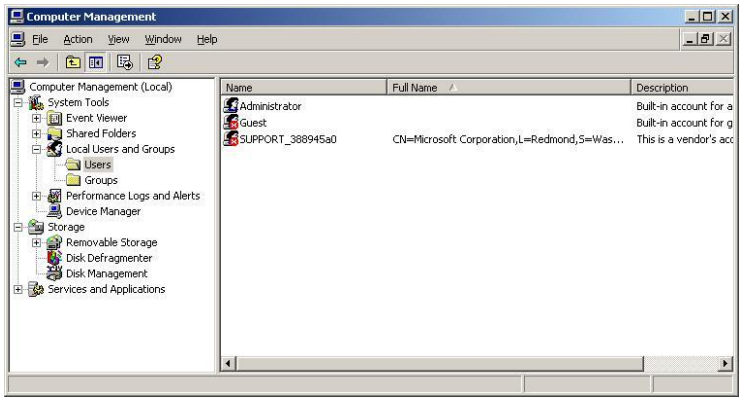


5. Modify User Accounts as required or recommended in Table 5.20.

Default Local User Accounts

Review or modify user accounts within a stand-alone or 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.



4. Modify User Accounts as required or recommended in Table 5.21.

Table 5.21 Default user accounts

User Account Modifications			Stand Alone Server	Domain Controller	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.	✓	✓	✓	
ASPNET	This account is used for running the ASP.NET worker process in IIS 5.0 isolation mode. It is used when doing ASP.NET development on the local computer.	This account should not exist in the Evaluated Configuration. If it does, the account must be disabled or deleted.	✓	✓	✓	

User Account Modifications			Stand Alone Server	Domain Controller	Required	Recommended
Local User Accounts	**Description**	**Modification / Verification**				
Guest	Built-in account for guest access to the computer/Domain.	This account must remain disabled.	✓	✓	✓	
HelpAssistant	Account used by remote help desk personnel to logon to a computer during the Remote Assistance session. This account is created automatically when a request for a Remote Assistance session is made and has limited access to the computer.	Remote Assistance is not used in the Evaluated Configuration; therefore this account should not exist. If it does, the account must remain disabled or be deleted.	✓	✓	✓	
SUPPORT_388945a0	Account used to control access to signed scripts that are accessible from within Help and Support Services. Administrators can use this account to delegate the ability for an ordinary user, who does not have administrative access over a computer, to run signed scripts from links embedded within Help and Support Services.	This account must remain disabled or may be deleted.	✓	✓	✓	

System Services

Table 5.21 lists the system services that can be enabled in an Evaluated Configuration. To remain in the Evaluated Configuration, it is acceptable to have all or any of the listed services enabled and running.

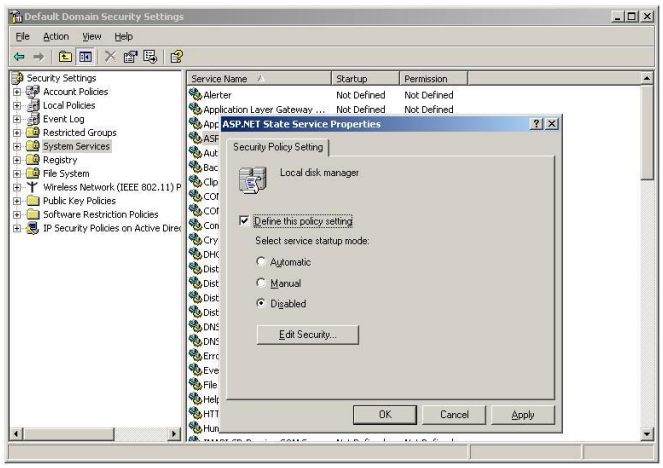
To enable or disable services on all or a group of Windows Server 2003 platforms in a domain, set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local settings on individual Windows Server 2003 computers can be set through the Computer Management interface.

Note: Enabling or installing any new service that is not identified in Table 5.22 is outside the scope of Common Criteria Evaluated Configuration. The 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 must be reestablished subsequently.

Unnecessary System Services on Domain Computers

Set a policy to disable unnecessary services on all computers within a domain, or specifically on domain controllers.

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

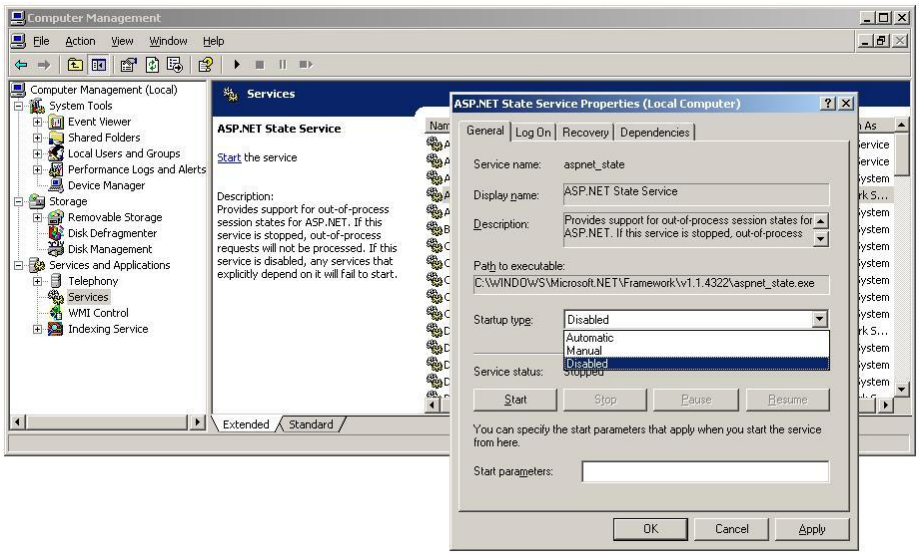


5. Click the **OK** button.

Unnecessary System Services on Workstations

To disable unnecessary services locally on Windows Server 2003 computers

1. Click **Start**, point to **Administrative Tools**, and click **Computer Management**.
2. In the console tree, expand **Services and Applications** and select **Services**.
3. In the right pane, select a service to disable. Right-click the selected service and click **Properties**. The **Properties** dialog box for the selected services appears.
4. In the **Startup type** drop-down list, click **Disabled**.



5. In the **Service status** area, click the **Stop** button (the **Stop** button is grayed out if the service is already stopped).
6. Click the **OK** button.

Table 5.22 Acceptable services for the Evaluated Configuration

List of Evaluated Services		
Alerter Service	Intersite Messaging	Server
Application Experience Lookup Service	IP Version 6 Helper Service	Single Instance Storage Groveler
Application Layer Gateway Service (ALG)	IPSEC Services	Smart Card
Certificate Services	Kerberos Key Distribution Center	System Event Notification
COM+ Event System	License Logging	Task Scheduler
COM+ System Application	Logical Disk Manager	TCP/IP NetBIOS Helper Service
Computer Browser	Logical Disk Manager Administrative Service	Uninterruptible Power Supply
Cryptographic Services	Messenger	Virtual Disk Service
DCOM Server Process Launcher	Microsoft Software Shadow Copy Provider	Volume Shadow Copy
DHCP Client	Net Logon	WebClient
DHCP Server	Network Connections	Windows Firewall (ICF) / Internet Connection Sharing (ICS)
Distributed File System (DFS)	Network Location Awareness (NLA)	Windows Installer
Distributed Transaction Coordinator	NTLM Security Support Provider	Windows Internet Name Service (WINS)
DNS Client	Performance Logs and Alerts	Windows Management Instrumentation
DNS Server	Plug and Play	Windows Management Instrumentation Driver Extensions
Error Reporting Service	Print Spooler	Windows Time
Event Log	Protected Storage	WinHTTP Web Proxy Auto-Discovery Service
File Replication Service	Remote Procedure Call (RPC)	WMI Performance Adapter
Help and Support	Remote Procedure Call (RPC) Locator	Workstation
HTTP SSL	Remote Registry Service	World Wide Web Publishing Service
Human Interface Device Service	Removable Storage	
IIS Admin Service	Resultant Set of Policy Provider	
IMAPI CD-Burning COM Service	Secondary Logon	
Indexing Service	Security Accounts Manager	
Internet Authentication Service		

Note: If the Certificate Services Windows component is installed on the server, it must be configured in accordance with the *Windows Server 2003 Certificate Server Security Configuration Guide*, which is located in Appendix A of the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0.*

File System Security

Among the files and folders to be protected are those that make up the Windows Server 2003 operating system itself. The default file and folder permissions that are applied to servers and domain controllers are found in the following files, respectively:

%SystemRoot%\inf\defltsv.inf

%SystemRoot%\inf\defltdc.inf

Windows Server 2003 file and folder permissions are significantly improved over previous Windows versions. This has been accomplished by changing default permissions on files and folders to place more restrictive ACLs on the group Everyone. The group Everyone has been restricted to only Read and Execute permissions on the root of each system partition and is no longer given Full Control permissions by default on newly created files and folders. Additionally, the group Everyone no longer includes the ANONYMOUS LOGON account. Permissions for anonymous access have to be applied explicitly. The new default permission settings on Windows Server 2003 meet the requirements for the Evaluated Configuration, therefore no changes are necessary.

As required, organizations can set permissions on data files and folders to enforce access restrictions. Detailed instructions for setting individual permissions using the Windows Explorer interface are provided in the Data Protection section of the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

Shared Folder Permissions

The native Windows Server 2003 file sharing service is provided using the SMB-based server and redirector services. In Windows Server 2003 the default permissions assigned to shared folders have been significantly improved by allowing only Read permission to the group Everyone, instead of the Full Control permissions granted in previous Windows versions.

Access to the files and subfolders displayed through shared folders is controlled by the NTFS permissions that are set on the underlying folder that a shared resource is mapped to. It is therefore recommended that proper security be applied using NTFS permissions to any files and folders mapped by a shared resource. Detailed procedures for setting shared folder permissions are provided in the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*. However, the Evaluated Configuration must not include any shared folders other than the administrative shares that are set by default during installation. See the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0* for a description of administrative shares.

Allow auditing of Task Scheduler object creation and management

Within the TOE, an authorized administrator must have the ability to audit task scheduling and scheduled task modification activities, if desired. Verify that the necessary audit settings are configured for the %SystemRoot%\Tasks folder, and modify them as shown in Table 5.23 if needed.

Table 5.23 Auditing of Task Scheduler objects

File Path	Audit Type	Audit Setting
%SystemRoot%\Tasks	Success, Fail	Everyone (Create Files/Write Data, Create Folders/Append Data, Delete Subfolders and Files, Delete, Change

File Path	Audit Type	Audit Setting
		Permissions, Take Ownership)
%SystemRoot%\Tasks	Success, Fail	ANONYMOUS LOGON (Create Files/Write Data, Create Folders/Append Data, Delete Subfolders and Files, Delete, Change Permissions, Take Ownership)

The effect of these settings is to audit any type of failed or successful creation or modification of Task Scheduler objects by any user.

Set auditing on the %SystemRoot%\Tasks folder through Windows Explorer

By default, the System attribute is set on the Tasks folder. This attribute does not allow access to the folder security settings and must therefore be temporarily removed. Once audit is set, the System attribute is reset on the Tasks folder.

Note: For these settings to be effective, the Audit Object Access policy must also be set in the local or domain security policy.

1. Log on with an account that has administrative privileges for the host operating system.
2. Click **Start** and select **Run**.
3. Type cmd in the **Run** interface and click **OK**.
4. At the Command Prompt, enter the command **attrib –S C:\Windows\Tasks**.
5. Open **Windows Explorer**.
6. Navigate to and select the **C:\Windows\Tasks** folder.
7. Right-click on the folder and select **Properties**.
8. In the Properties interface, select the **Security** tab. Click **Advanced** for more detailed permission settings.
9. Select the **Auditing** tab.
10. Click the **Add** button. The **Select Users, Computers, or Groups** dialog box will appear. Enter the name of the account that is to be audited, which is the group **Everyone** and the **ANONYMOUS LOGON** account as defined in Table 5.23. If necessary, click the **Check Names** button to verify the account. Click **OK**.
11. The **Auditing Entry for Tasks** interface will appear. Set auditing for each of the permissions listed in Table 5.23 by selecting the corresponding check boxes under Successful and Failed in the **Access** dialog box.
12. Once audit has been set, click **OK** on the **Auditing Entry for Tasks** interface, the **Advanced Security Settings** interface, and the **Tasks Properties** interface.
13. Go back to the Command Prompt, or open a new one if needed, and enter the command **attrib –S C:\Windows\Tasks** to reset the System attribute on the Tasks folder.

Registry Security

In addition to the considerations for standard security described in this document, security administrators might want to increase protections on certain keys within the Windows Server 2003 registry. By default, protections are set on various components of the registry that allow work to be done while providing standard-level security. The default registry key permissions that are applied to servers and domain controllers are found in the following files, respectively:

%SystemRoot%\inf\defltsv.inf

%SystemRoot%\inf\defltdc.inf

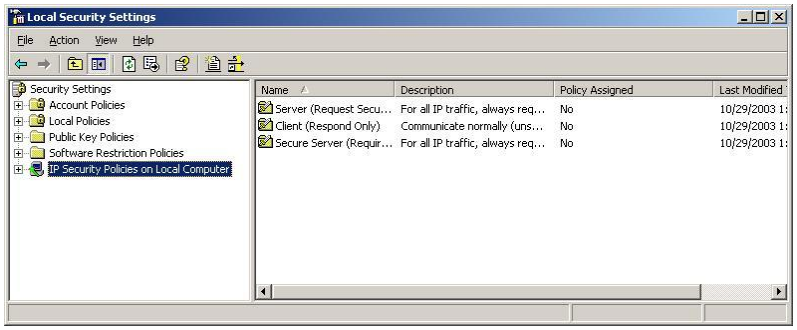
As stated in the File System Security section, Windows Server 2003 permissions are significantly improved over previous Windows versions. This has been accomplished by changing default permissions to place more restrictive ACLs on the group Everyone.

As required, organizations can set registry permissions to enforce access restrictions. Detailed instructions for setting registry permissions are provided in the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

IPSec Policy

IPSec policies, rather than application programming interfaces (API), 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 Server 2003 provides an IP Security Policies interface to define IPSec policies for computers at the Active Directory level for any domain members, or on the local computer for non–domain members. At the Active Directory level, the policy can be accessed from the Group Policy interface or the Default Domain Security Policy interface. At the local computer level it can be accessed from the Local Security Policy interface, as shown here.



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 that are not joined to the domain. When the computer is temporarily not joined to a trusted Microsoft Windows Server 2003 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 Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*. There are no specific IPSec setting requirements for the Evaluated Configuration.

Encrypting File System

Windows Server 2003 provides 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 NTFS file system. EFS runs as a service and uses both private key decryption and public key encryption.

The ST requires the ability to enable, disable, and control EFS on NTFS-formatted 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 Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

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.

Notes:

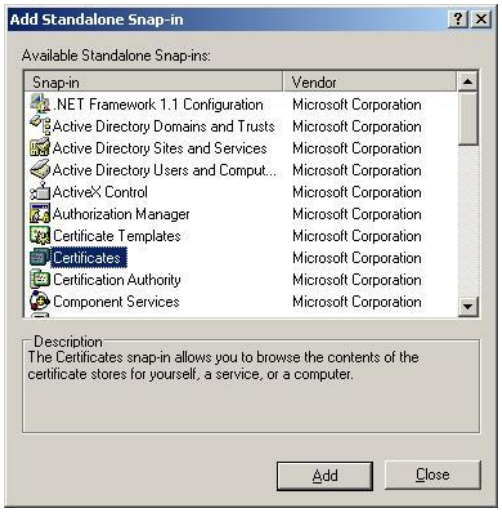
If EFS has not been used by the Administrator since the installation of the operating system, there might not be an EFS certificate for the Administrator. To create an EFS certificate, simply encrypt a file. An EFS certificate for the user is created automatically after the first file encryption attempt. See the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0* for file encryption procedures.

On a domain controller, a Data Recovery Agent (DRA) certificate is created by default for the default domain administrator account. See the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0* for procedures on exporting the DRA certificate.

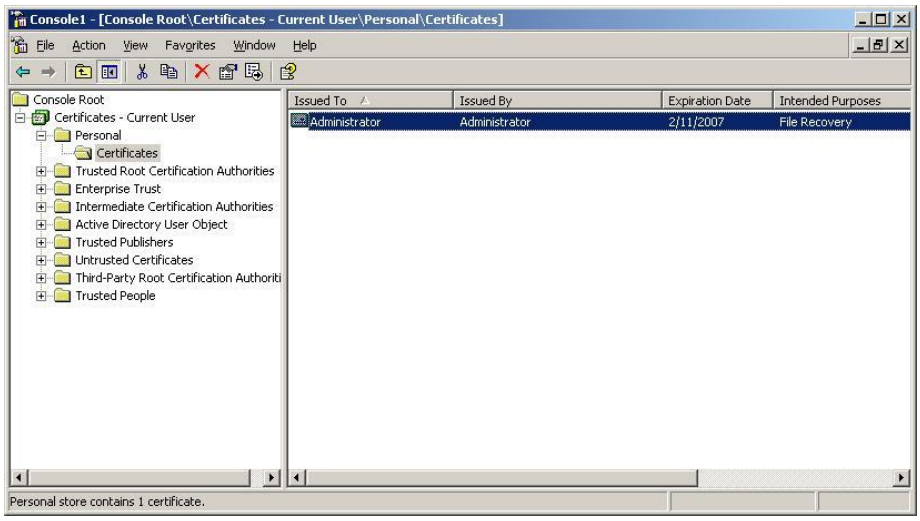
If a Certificate Authority is available, users can request an EFS certificate from it. See the *Windows XP Professional User's Guide, Version 3.0* for user certificate request procedures.

To back up the Administrator's encryption certificate and private key

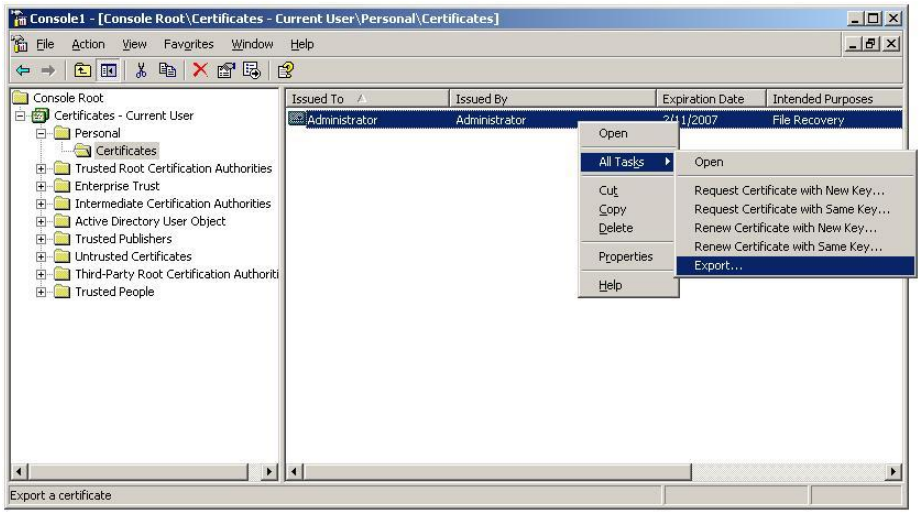
1. Click **Start**, click **Run**, type **mmc**, and click **OK**.
2. On the menu, click **File**, select **Add/Remove Snap-in**, and click **Add**.
3. Locate and click the **Certificates** snap-in, and click **Add**.



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. Expand **Certificates–Current User**. Expand the **Personal** folder. Select **Certificates**.



6. Right-click the Administrator certificate, point to **All Tasks**, and select **Export**. This starts the Certificate Manager Export Wizard.



7. 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 (.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\<*FileName*>. Click **Next**. A list of certificates and keys to be exported is displayed.

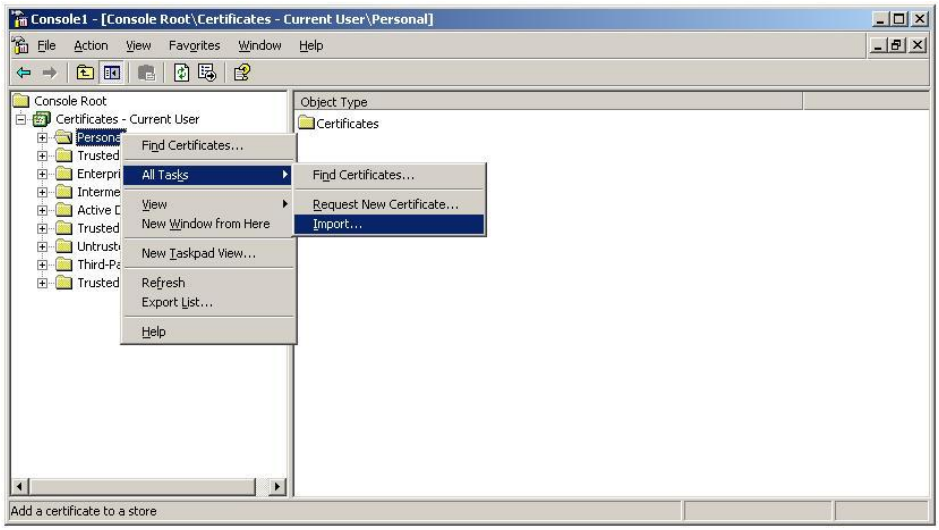
12. Click **Finish** to confirm.

13. Click **OK** to close the wizard. 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

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.
2. Click **Start**, click **Run**, type **mmc**, and click **OK**.
3. On the menu, click **File**, select **Add/Remove Snap-in**, and click **Add**.
4. Locate and click the **Certificates** snap-in, and click **Add**.
5. Select **My user account** and click **Finish**. Click **Close**. Click **OK**.
6. Right-click the **Personal** store, point to **All Tasks**, and select **Import**.



7. This starts the Certificate Manager Import Wizard. Click **Next** and follow the instructions to successfully import the certificate and private key.

8. Provide the path to the .pfx file and type the password to unwrap the .pfx data.

9. Click **Place all certificates in the following store**, and accept browse to the **Personal** certificate store if it is not already displayed in the **Certificate store** box. 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.

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

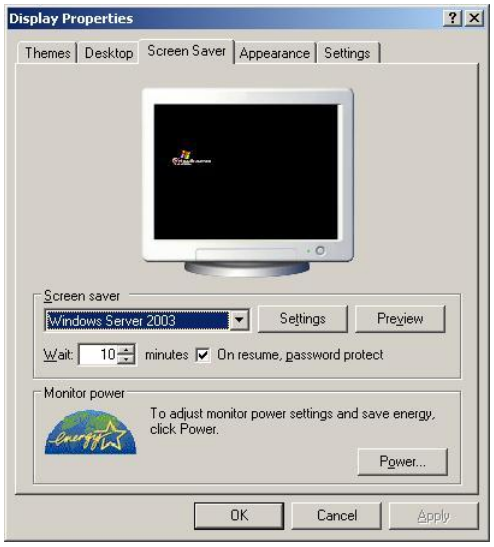
Automatic Screen Lock Protection

By default, Windows Server 2003 has automatic screen lock protection enabled. This enables the server desktop to be locked for security reasons by setting an automatic screen lock that is initiated by the screen saver after a set period of inactivity. After the computer screen lock is invoked, access to the computer is allowed only after authentication by the user whose account is currently logged on to the computer or by an authorized administrator.

For the Evaluated Configuration, screen lock protection must be enabled.

To re-enable a password-protected screen saver

1. Right-click the desktop and select **Properties** to open **Display Properties**.
2. Click the **Screen Saver** tab.
3. Select a screen saver from the **Screen saver** drop-down list.
4. In the **Wait** box enter the number of minutes of inactivity that the system must wait before initiating the screen saver (the server default of 10 minutes is recommended).
5. Select the **On resume, password protect** check box.



6. Click **OK** to enable the password-protected screen saver.

System Recovery

Back up the system and update the ASR disk to reflect all the changes made. For instructions, see Recommended Actions Before and After Configuration Changes earlier in this guide.

6. Active Directory Federation Services Deployment

This section provides a brief overview of Active Directory Federation Services (ADFS) and how to use this guide to prepare for, install, and configure ADFS securely in a Windows Server 2003 R2 with SP2 environment. It is important that administrators are familiar with ADFS concepts prior to embarking upon an ADFS implementation. Although the basic concepts and the scenarios included in the evaluated configuration are described here, more detailed information about ADFS concepts is provided in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0.*

ADFS Overview

Active Directory Federation Services (ADFS) is an add-on component introduced in Windows Server 2003 R2 with SP2 that provides Web single sign-on (SSO) technologies to authenticate a user to multiple Web applications over the life of a single browser session. ADFS enables SSO technologies through distributed identification, authentication, and authorization across organizational and platform boundaries. This technology is known as federated identity management. The ADFS solution in Windows Server 2003 R2 with SP2 enables organizations to securely share a user's identity information over *federation*[1] trusts.

ADFS supports federated identity scenarios that use Web Services Federation (WS-Federation[2]), WS-Federation Passive Requestor Profile (WS-F PRP[3]), and WS-Federation Passive Requestor Interoperability Profile specifications.

Identity federation—the term for linking identities of users across multiple accounts without storing the information centrally—can be used to enable federated identity management in a variety of scenarios. The scenario that an organization employs for federated identity is dependent upon a variety of factors, including network infrastructure design, the type of federated identity needed (i.e., business-to-business, business-to-consumer, or business-to-employee), and other business needs.

This security configuration guide describes the following ADFS implementation scenarios and describes how to securely deploy and configure each:

- Federated Web SSO
- Web SSO

Use the descriptions of the two scenarios here to determine which is appropriate for a particular organization’s environment.

---

1 A pair of realms or domains that have established a federation trust.

2 A specification that defines a model and set of messages for brokering trust and the federation of identity and authentication information across different trust realms.

3 An implementation of the WS-Federation specification that proposes a standard protocol for how passive clients (such as Web browsers) apply the federation framework. Within this protocol, Web service requestors are expected to understand the new security mechanisms and be capable of interacting with Web service providers.

Note: There is a third possible ADFS scenario called Federated Web SSO with forest trust, which allows the administrator to restrict access to a Windows NT token-based application to specific domains in the account realm's forest when that forest contains multiple domains. However, the only ADFS scenarios included within the TOE are the Federated Web SSO and Web SSO scenarios.

Federated Web SSO

The ADFS Federated Web SSO scenario involves two partner organizations, each with its own Active Directory forest. If there is a business need for users in a partner organization to access Web resources in the local organization's forest, then consider implementing this scenario.

An example of this type of scenario is illustrated in Figure 6.1. For the sake of simplicity, in the evaluated configuration, each forest contains only one domain. The forest in the local network comprises the *protected network* (depicted here as *Domain A*); the other forest is located in a separate "partner" network (depicted as *Domain B*). Domain A contains the Web server resources being accessed by a user who has an account in Domain B. Domain A comprises the *resource realm* in this ADFS scenario. Domain B contains the partner user accounts that access the resources in Domain A and comprises the *account realm*.

Federation servers are deployed in both domains, and there is network accessibility between the two domains. A federation server called the *resource federation server* is installed in the protected network of the primary organization (Domain A). A federation server called the *account federation server* is deployed in the partner organization (Domain B). By implementing ADFS, a federation trust is established between these two entities so that accounts in Domain B can be used to access claims-aware and Windows NT token-based[4] Web applications in Domain A.

[4] The types of ADFS-enabled applications supported are described later in this section.

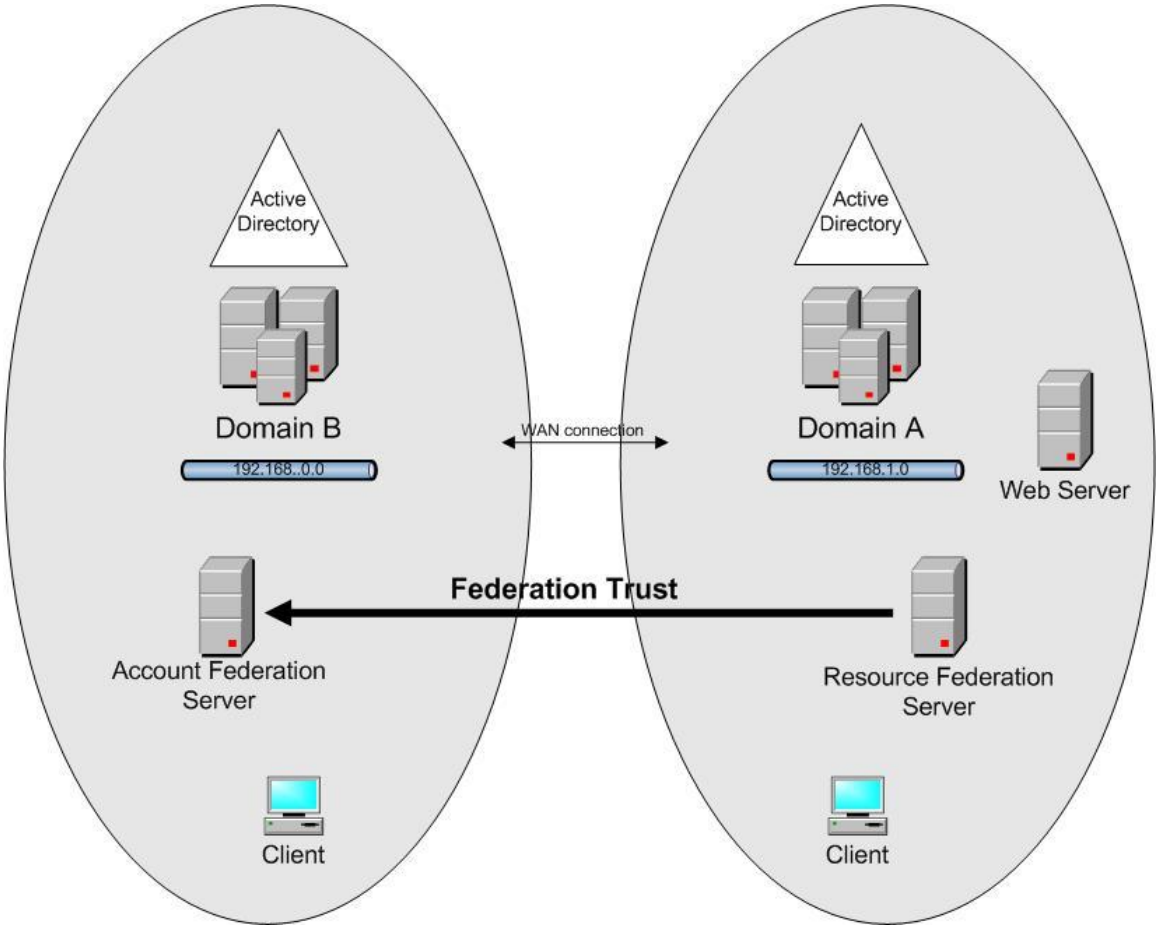


Figure 6.1 Overview of typical Federated Web SSO scenario

In the Federated Web SSO scenario, users in Domain B can access the Web application hosted in Domain A by authenticating to the account federation server in Domain B. Domain A users can also access the Web application by authenticating to the Domain A resource federation server.

Deploying a Federated Web SSO scenario requires installing and configuring the following components in the protected network: the Federation Service and at least one ADFS Web Agent. When the Federation Service is installed on a computer in the protected network, that computer becomes a resource federation server. The ADFS Web Agents are installed on the Web server used to host ADFS-enabled applications. The Federation Service must also be deployed to a server in the partner network. When the Federation Service is installed on a computer in the partner network, that computer becomes an account federation server.

Each server that runs an ADFS component must have Microsoft Internet Information Services (IIS) 6.0 installed. This includes the resource federation server, the account federation server, and the Web server. Also required on each ADFS computer[5] are server authentication certificates (in conjunction with the root certificate of the trusted root certification authority that

[5] In this guide, computers running an ADFS component are sometimes referred to as "ADFS computers." These include federation servers, federation server proxies, and Web servers running an ADFS Web Agent.

issues the certificates). These certificates must be installed on each server running an ADFS component.

Web SSO

In the ADFS Web SSO scenario, as seen in the example illustrated in Figure 6.2, users from an external network authenticate only once to access multiple Web-based applications in the internal network hosting ADFS-enabled resources. Typically, in this scenario external clients (i.e., they are not joined to the internal domain) are allowed access to ADFS-enabled resources, and no federation trust exists between entities. If there is a business need for users with external client computers (that do not have computer accounts on the internal domain) to access Web resources on the internal network, consider implementing this scenario.

Because the Web server must be accessible from the external network and also joined to the internal Active Directory domain, the Web server host is dual-homed to allow connectivity to two networks. The first network—known as the *protected network* or *internal network*—contains an Active Directory forest that is not directly accessible to external clients. The other network is the *perimeter network* or *external network*; it provides the needed connectivity for external clients.

A proxy server called *the federation service proxy* is used to route Web requests initiated at the external client computer to the internal federation server. The federation service proxy runs the Federation Service Proxy component of ADFS on a dual-homed host computer. As with the Web server, dual network adapters provide the necessary connectivity to the federation server and accessibility to external clients. In this scenario, placing the federation server on a network that is not directly accessible by external clients greatly reduces the risk to the federation server.

Note: Routing must not be enabled on any of the dual-homed computers.

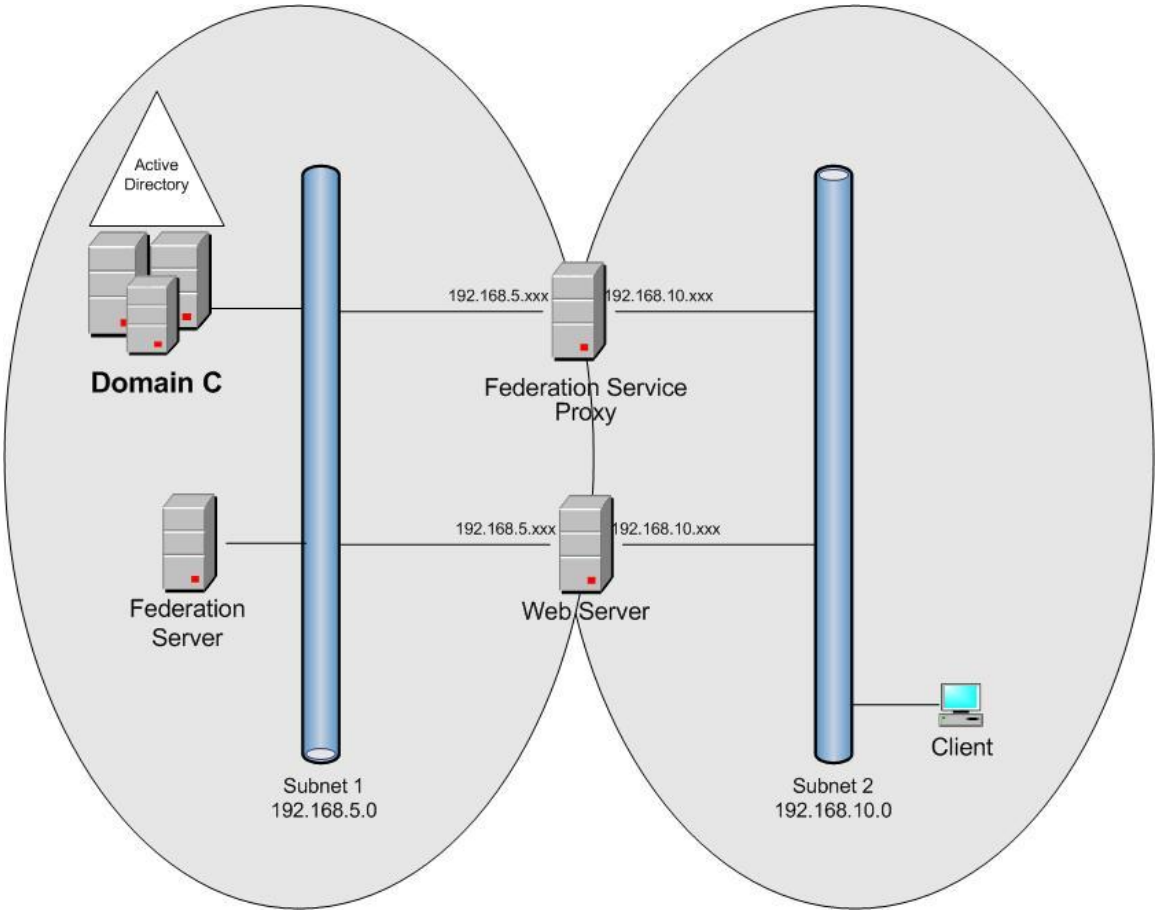


Figure 6.2 Overview of typical Web SSO scenario.

Deploying a Federated Web SSO scenario requires installing and configuring the Federation Service in the protected network and the following components in the perimeter network: the Federation Service Proxy and at least one ADFS Web Agent.

Each server that runs an ADFS component must have Microsoft Internet Information Services (IIS) 6.0 installed. This includes the federation server, the federation service proxy, and the Web server. Also required on each ADFS computer are server authentication certificates (in conjunction with the root certificate of the trusted root certification authority). These certificates must be installed on each server running an ADFS component. As an additional requirement, the federation service proxy must be issued a client authentication certificate for authenticating a connection with the federation server.

For more information about ADFS functionality, see the “Implementing Active Directory Federation Services” section of the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

ADFS Applications

The two types of ADFS-aware Web-based applications are claims-aware applications and Windows NT token-based applications. This guide briefly describes the application types and includes procedures for configuring ADFS in an evaluated configuration using both types of applications. For more conceptual information about these application types, see the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

Claims-aware Applications

Claims-aware applications are Microsoft ASP.NET 2.0 applications that are written so that they can query ADFS security token claims. When the Web-based application used within the TOE is a claims-aware application, the ADFS Web Agent that is running on the Web server does not have to create Windows NT security tokens for the user. Federated applications that are claims-aware are developed specifically to use the claims that are produced by ADFS.

When an application is presented with a valid token, the claims-aware application can make authorization decisions based on the claims in the token, which stores all the information about a given identity. The application might store additional information that links to the identity that is presented in the token, but a user account in Active Directory on the local domain is not required to access a claims-aware application.

In the Federated Web SSO scenario, when incoming claims are received by the resource federation server from the account federation server, they are mapped to organization claims on the resource federation server. In the procedures provided by this guide, security groups in Active Directory are used to map claims in ADFS.

Windows NT Token-based Applications

Windows NT token–based applications are IIS applications that are written to use Windows-based authorization mechanisms. These applications require Windows NT security tokens to make authorization decisions. ADFS can enable the transition of an ADFS security token to an impersonation-level Windows NT access token.

When the Web-based application used in the evaluated configuration is a Windows NT token–based application, the organization claims on the resource federation server must be mapped to either a user or a group in the local Active Directory account store. The user accounts or groups are also known as *resource accounts* or *resource groups*. The application then uses the resource accounts or groups to perform authorization.

Resource account mapping is required with federated Windows NT token-based applications because the ADFS Web Agent must reference an Active Directory security principal in the resource partner forest to build the Windows NT access token and thereby enforce access control on the application. When a client makes a request to a Windows NT token-based application, the ADFS Web Agent that is running on the Web server intercepts the request and creates Windows NT security tokens, which are required by the Web application to make authorization decisions. For users in the resource realm, this is possible because the Web server that hosts the Windows NT token-based application is joined to the resource domain. For users in the account realm (or for external users in the Web SSO scenario), this is enabled through mapped resource groups.

Using this Guide to Deploy ADFS

It is assumed that administrators are familiar with ADFS and understand the ADFS concepts and scenarios that are presented in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

This guide demonstrates how to implement both the Web SSO and the Federated Web SSO scenarios that are included in the TOE. Use this guide to prepare the TOE environment for an ADFS deployment, to install and configure ADFS, and to access ADFS-enabled Web applications. This guide provides sample applications for the purposes of demonstrating an ADFS implementation. It is important to understand that the sample applications are referenced here for the purpose of demonstrating an ADFS implementation according to the secure procedures described in this guide. In the actual implementation, administrators can use this

guide to configure ADFS for their organization's specific ADFS-enabled applications, rather than actually deploying the sample applications provided here.

Note that this guide cannot provide the naming conventions that are required for a particular organization's ADFS implementation. Rather, placeholders are used throughout the procedures provided here for items such as organization names, domain names, computer names, and user and security group account names. Placeholders are represented using brackets, as follows: <PlaceholderName>.

During a production implementation of ADFS, it is the responsibility of the administrator to input the appropriate name in place of the placeholder string in brackets (< >) represented in this guide when configuring ADFS. To aid in this process, Tables 6.1 and 6.2 are provided. These tables describe the terminology used to represent the various computer names of the server and client components that have a role in the ADFS implementations.

Table 6.1 is for use with the Federated Web SSO scenario. Table 6.2 is for use with the Web SSO scenario. It is necessary to refer back to Tables 6.1 and 6.2 when following the procedures provided here for installing and configuring ADFS. Administrators using this guide should consider printing the tables and using them to identify the actual names used in their particular environment. A separate, blank column is provided in the table for administrators to write the appropriate names for their environment to refer to when configuring ADFS.

Table 6.1 Placeholder names used in the ADFS procedures for the Federated Web SSO scenario

Role or description	Placeholder name	Actual name (to be filled in by administrator)
NetBIOS name of account realm domain	<AccountDomain>	
FQDN of account realm domain	<AcctDomainFQDN>	
NetBIOS name of resource realm	<ResourceDomain>	
FQDN of resource realm domain	<ResDomainFQDN>	
NetBIOS name of resource realm domain controller	<ResourceDC>	
NetBIOS name of account realm domain controller	<AccountDC>	
NetBIOS name of resource federation server	<ResFedSvr>	
FQDN of resource federation server	<ResFedSvrFQDN>	
NetBIOS name of account federation server	<AcctFedSvr>	
FQDN of account federation server	<AcctFedSvrFQDN>	
NetBIOS name of ADFS-enabled Web server	<WebSvr>	
FQDN of ADFS-enabled Web server	<WebSvrFQDN>	
ADFS user account name in account realm	<AcctUser>	
ADFS user account name in resource realm	<ResUser>	
NetBIOS name of ADFS client computer in resource realm	<ResClient>	
NetBIOS name of ADFS client computer in account realm	<AcctClient>	
Security group name for resource domain claims-aware application users	<ResClaimAppUsers>	
Security group name for resource domain Windows NT token-based application users	<ResTokenAppUsers>	
Resource group for Windows NT token-based application mapping	<AcctTokenAppUsers>	
NetBIOS name of Certification Authority server	<CASvr>	
FQDN of Certification Authority server	<CASvrFQDN>	

Table 6.2 Placeholder names used in the ADFS procedures for the Web SSO scenario

Role or description	Placeholder name	Actual name (to be filled in by administrator)
NetBIOS name of Certification Authority server	<CASvr>	
FQDN of Certification Authority server	<CASvrFQDN>	
NetBIOS name of internal domain	<InternalDomain>	
NetBIOS name of internal domain controller	<InternalDC>	
NetBIOS name of federation server	<FedSvr>	
FQDN of federation server	<FedSvrFQDN>	
IP address of federation server	<FedSvrIPAddress>	
NetBIOS name of ADFS-enabled Web server	<WebServer>	
FQDN of ADFS-enabled Web server	<WebServerFQDN>	
External IP address of ADFS-enabled Web server	<WebServerIPAddress>	
NetBIOS name of federation service proxy	<FedProxy>	
External IP address of federation service proxy	<FedProxyIPAddress>	
ADFS user account name in internal domain	<ExtUser>	
Local user account on external client computer	<LocalUser>	
NetBIOS name of ADFS client computer in external network	<ExtClient>	
Organizational unit in the internal domain	<FederatedUsers>	
Security group name for claims-aware application users	<ClaimAppUsers>	
Security group name for resource domain Windows NT token-based application users	<TokenAppUsers>	

To further help in installing and configuring ADFS for the TOE, administrators should consider creating diagrams similar to those shown in Figures 1 and 2 for mapping out an ADFS scenario.

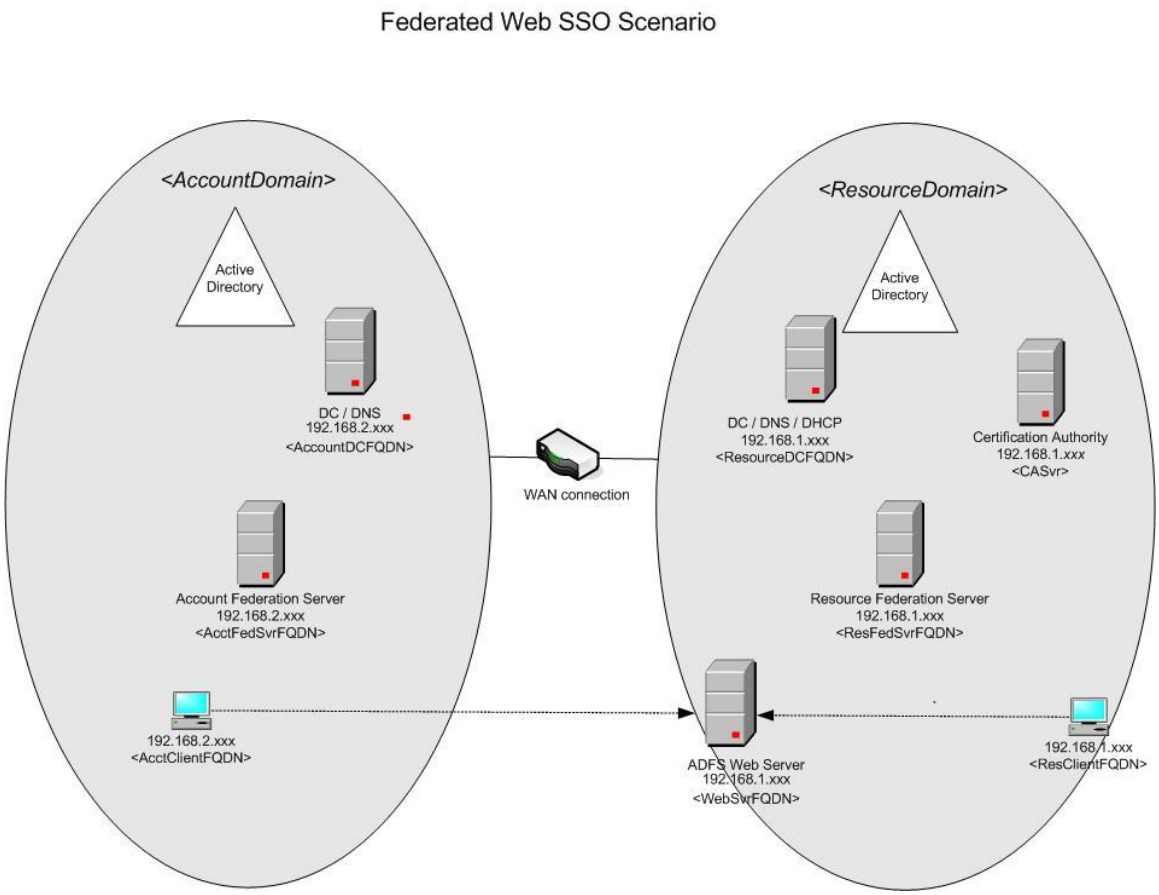


Figure 6.3 Sample diagram for a Federated Web SSO scenario

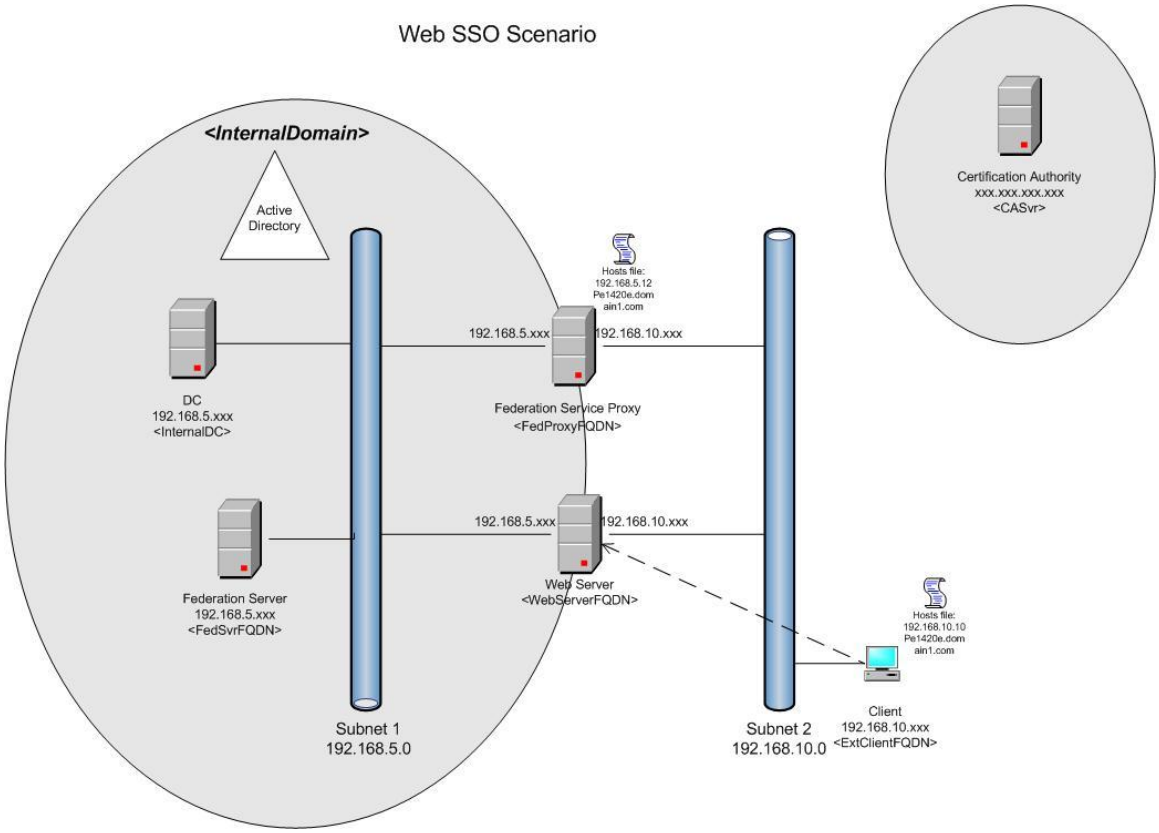


Figure 6.4 Sample diagram for a Web SSO scenario

ADFS Installation Preparation

ADFS components are supported only on specific editions of Windows Server 2003. See Table 6.3 for information about which server operating system editions are included in the ADFS evaluated configuration and which components of ADFS they support. Although other operating system editions are included as part of the TOE (such as Enterprise Itanium and non-R2 versions of Windows Server 2003), they do not appear in Table 6.3 because they do not support ADFS components.

Table 6.3 Windows Server 2003 operating system editions and the ADFS components they support

	Federation Service	ADFS Web Agents	Federation Service Proxy
Standard R2 with SP2		X	
Enterprise R2 with SP2	X	X	X
Datacenter R2 with SP2	X	X	X
Standard x64 R2 with SP2		X	
Enterprise x64 R2 with SP2	X	X	X
Datacenter x64 R2 with SP2	X	X	X

Regardless of which ADFS scenario is being implemented, prior to installing ADFS in the TOE environment, Windows Server 2003 R2 with SP2 and Internet Information Services (IIS) 6.0 must be installed on each ADFS host. Also, ASP.NET 2.0 (a component of Microsoft .NET Framework 2.0) must be enabled on all ADFS computers. This includes federation servers (computers that are running the Federation Service), federation server proxies (computers running the Federation Service Proxy component), and Web servers that host ADFS-enabled applications (computers running one or both ADFS Web Agents).

Client computers accessing ADFS applications[6] must have a Web browser for accessing ADFS-enabled applications. There are no additional software components installed on computers acting as ADFS clients.

A summary of the software components that must be installed in the ADFS environment prior to installing ADFS components is provided in Table 6.4.

Table 6.4 ADFS components and pre-installation software requirements

	Federation Service	ADFS Web Agent(s)	Federation Service Proxy	ADFS Client Computer
IIS 6.0	**X**	**X**	**X**	
Microsoft .NET Framework 2.0	**X**	**X**	**X**	
ASP.NET 2.0 enabled for Default Web site in IIS	**X**	**X**	**X**	
Server authentication certificate	**X**	**X**	**X**	
Client authentication certificate			**X**	

In addition, a Secure Sockets Layer (SSL) server authentication certificate must be assigned to the Default Web Site on each of the ADFS computers before ADFS component setup can be run. Also, for the Federated Web SSO scenario, it is important to verify that TCP/IP settings are configured properly on all of the computers in the ADFS environment, including clients and servers. Lastly, user accounts and security groups should be in place in Active Directory for verifying ADFS functionality after setting up and configuring ADFS.

The ADFS pre-installation tasks are summarized as follows and are described in the rest of this section:

- Install Windows Server 2003 R2 on the ADFS computers.
- Install and configure Internet Information Services (IIS) 6.0, install Microsoft .NET Framework 2.0, and configure ASP.NET 2.0 on the ADFS computers.

Additional pre-installation tasks for the Federated Web SSO scenario are:

- Verify TCP/IP settings are correct on all computers in the ADFS environment.
- Create and apply server authentication certificates on the ADFS computers.

---

[6] Client computers used to access ADFS-enabled applications are sometimes referred to as “ADFS clients” in this document.

- Configure Group Policy to distribute the root certificate to computers in the account realm.
- Create user and security group accounts in the account domain and in the resource domain.

Additional pre-installation tasks for the Federated Web SSO scenario are:

- Create and apply client and server authentication certificates on the ADFS computers.
- Configure Group Policy to distribute the root certificate to computers in the ADFS environment.
- Create user and security group accounts in the internal domain.

Note: For the Web SSO scenario, the Certification Authority (CA) used in the certificate tasks is external and therefore is not part of the TOE. Because the CA is outside of the TOE, instructions for using it are not included in this guide. Consult the CA software vendor's guidance for information about making certificate requests to the external CA.

Before proceeding with the installation preparation procedures, administrators should ensure that a removable media device (such as a portable USB flash drive) is available for copying certificate files created during various installation and configuration procedures. The most important factor in implementing ADFS is creating and configuring the required certificates appropriately.

Installing Windows Server 2003 R2

If Windows Server 2003 R2 has not already been installed, follow the Microsoft Windows Server 2003 R2 Requirement for ADFS and DFS Components section of this document to install Windows Server 2003 R2 from the Windows Server 2003 R2 product CD set.

Installing and Configuring Internet Information Services and .NET Framework 2.0

IIS 6.0 is required in order to support the administrative and service capabilities of ADFS. Prior to initiating an ADFS component on a computer running Windows Server 2003 R2 with SP2, IIS 6.0 must be installed in a manner that is consistent with the TOE requirements on each of the ADFS computers in the environment, including federation servers, federation server proxies, and Web servers.

Federated Web SSO scenario. Use the procedures outlined here to install IIS and verify .NET Framework 2.0 installation and ASP.NET configuration on each of the following ADFS computers in the Federated Web SSO scenario:

- Resource federation server (<ResFedSvr>)
- Account federation server (<AcctFedSvr>)
- Web server (<WebSvr>)

Web SSO scenario. Use the procedures outlined here to install IIS and verify .NET Framework 2.0 installation and ASP.NET configuration on each of the following ADFS computers in the Web SSO scenario:

- Federation server (<FedSvr>)
- Federation service proxy (<FedProxy>)
- Web server (<WebServer>)

Note: When installing any Windows component (such as IIS 6.0 or .NET Framework 2.0) using the procedures outlined in this guide, if prompted for files needed during the procedure, insert the appropriate Windows Server 2003 CD into the CD-ROM drive, and follow instructions displayed to locate and install the file(s) needed.

For each of the procedures in this section, the authorized administrator must be logged on using an account that is a member of the Domain Admins group of the domain that the computer is joined to.

Install IIS

On each ADFS computer:

Warning: When installing IIS to support an ADFS computer, do not select the check box for ASP.NET on the Application Server page because this will cause an older version of .NET Framework (which includes an earlier version of ASP.NET) to be installed. Without the appropriate version of ASP.NET installed, ADFS does not work.

1. Log on using an authorized administrator.
2. Insert the Windows Server 2003 product CD in the CD-ROM drive. If a Welcome to Microsoft Windows Server 2003 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In Add or Remove Programs, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, select **Application Server** (do not click the check box next to Application Server) and then click the **Details** button.
6. Select the check box for **Internet Information Services (IIS)**. This automatically selects the check box for both Enable network COM+ access and Internet Information Services (IIS).

   Warning: Do not select the check box for ASP.NET on the Application Server page.
7. Click **OK**, and then click **Next** in the Windows Components interface.
8. If prompted for Setup files, ensure that the Windows Server 2003 product CD is inserted, click **Browse**, click **My Computer**, double-click the CD-ROM drive letter displayed in the Files Needed interface, navigate to the folder containing the file needed by Setup (for example, **<CDROMDriveLetter>:\\i386, or <CDROMDriveLetter>:\AMD64\i386**). Highlight that folder and click **Open**. Click **OK**.
9. In the Completing the Windows Components Wizard, click **Finish**.
10. Leave the Add or Remove Programs interface open to verify that .NET Framework 2.0 is installed.

After installing IIS, verify that .NET Framework 2.0 is installed on the operating system and that ASP.NET 2.0 is enabled for the Default Web Site in IIS.

Verify the installation of .NET Framework 2.0

On each ADFS computer:

In Add or Remove Programs, in the **Currently Installed Programs** box, verify that **Microsoft .NET Framework 2.0** (or **Microsoft .NET Framework 2.0 (x64)**) is listed.

- If Microsoft .NET Framework 2.0 (or **Microsoft .NET Framework 2.0 (x64)**) is listed, close the Add or Remove Programs interface and proceed to the procedure entitled **Verify that ASP.NET 2.0 is allowed**.
- If Microsoft .NET Framework 2.0 (or **Microsoft .NET Framework 2.0 (x64)**) is not listed, continue to the procedure entitled **Install .NET Framework 2.0 on Windows Server 2003 R2 with SP2 (if necessary)**.

Install .NET Framework 2.0 on Windows Server 2003 R2 with SP2 (if necessary)

Follow the procedure here to install Microsoft .NET Framework 2.0 from the Windows Server 2003 R2 product CD, if it is not already installed.

On each ADFS computer:

1. Insert the Windows Server 2003 R2 product CD in the CD-ROM drive. If a Welcome to Microsoft Windows Server 2003 screen appears, click **Exit**.
2. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
3. In the Add or Remove Programs interface, click **Add/Remove Windows Components** in the left pane.
4. In the Windows Components page, select the check the box for **Microsoft .NET Framework 2.0**, and then click **Next**.
5. When the installation is complete, click **Finish**.
6. Close the Add or Remove Programs interface.

Verify that ASP.NET 2.0 is allowed

1. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
2. In the console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
3. Click the **Web Service Extensions** node in the console tree.
4. At the bottom of the details pane, click the **Standard** tab. All versions of ASP.NET that are currently enabled appear under **Web Server Extension**.
5. Verify that **ASP.NET v2.0.50727** appears in the Web Service Extension column and that the status is set to **Allowed**.
   - If ASP.NET v2.0.50727 is listed and allowed in the Web service extensions, proceed to the procedure entitled **Verify that the Default Web Sites use ASP.NET 2.0**.
   - If ASP.NET is either not listed, or is listed and marked as **Prohibited**, perform the next procedure **Enable ASP.NET 2.0 in the Web service extensions (if necessary)** first and then proceed to the procedure **Verify that the Default Web Sites use ASP.NET 2.0**.

Enable ASP.NET 2.0 in the Web Service Extensions (if necessary)

This procedure enables ASP.NET 2.0 in the Web service extensions without changing the configuration of the virtual servers.

1. Click **Start**, and then select **Command Prompt**.

2. Change directories as specified below.
   - If running a 32-bit Windows Server 2003 R2 with SP2 operating system, change directories to: **C:\Windows\Microsoft.NET\Framework\v2.0.50727**. For example, type the following command and press **Enter**:

     cd c:\windows\microsoft.net\framework\v2.0.50727
   - If running an x64 Windows Server 2003 R2 with SP2 operating system, change directories to: **C:\Windows\Microsoft.NET\Framework64\v2.0.50727**. For example, type the following command and press **Enter**:

     cd c:\windows\microsoft.net\framework64\v2.0.50727
3. Run the following command at the command prompt:

   aspnet_regiis -iru -enable
4. When screen displays "Finished installing ASP.NET (2.0.50727)," type **exit** and press **Enter** to close the Command Prompt interface.
5. In Internet Information Services (IIS) Manager click once anywhere in the white space of the details pane and then press the **F5** key on the keyboard to refresh.
6. Verify that **ASP.NET v2.0.50727** is listed in the **Web Service Extension** column and that the status is **Allowed**. If the status is **Prohibited**, it can be changed by right-clicking **ASP.NET 2.0.50727** in the details pane and then clicking **Allow**.

After verifying that ASP.NET is installed and allowed in Web service extensions, the next step is to verify that the Default Web Site is using ASP.NET 2.0.

Verify that the Default Web Site uses ASP.NET 2.0

ADFS requires that the Default Web Site on the federation servers and the Web server are configured to use ASP.NET 2.0. On each ADFS computer:

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In Internet Information Services (IIS) Manager, under the local computer node, expand the **Web Sites** folder.
3. Right-click **Default Web Site** and click **Properties**.
4. In the Default Web Site Properties interface, click the **ASP.NET** tab.
   - If the **ASP.NET version** is 2.0.50727, click **OK** and then exit Internet Information Services (IIS) Manager.
   - If the **ASP.NET version** is not listed as 2.0.50727, use the drop-down arrow to select **2.0.50727**, click **OK**, and then exit Internet Information Services (IIS) Manager.

After completing the IIS and ASP.NET procedures on the ADFS computers for the ADFS scenario being implemented, complete the procedures in the additional pre-installation tasks topic that is relevant to the scenario being deployed:

- Additional Pre-installation Tasks: Federated Web SSO Scenario, or
- Additional Pre-installation Tasks: Web SSO Scenario.

Additional Pre-installation Tasks: Federated Web SSO Scenario

Follow the procedures in this section to verify TCP/IP settings, create and assign server authentication certificates, distribute the root certificate, and create user accounts and groups for the Federated Web SSO scenario.

Verifying TCP/IP Settings

Each computer in the ADFS environment in the Federated Web SSO scenario must be configured with appropriate TCP/IP configuration settings. Verify that these settings are correct on the ADFS computers, domain controllers, and client computers in the ADFS environment.

Each of those computers should be configured with a primary and secondary DNS server. The primary DNS server should be the domain controller in the local domain (that is, local to the computer where TCP/IP is being configured), and the secondary DNS server is the domain controller of the external domain. The computers should also be configured with a default gateway.

> **Note:** The router used in the Federated Web SSO scenario is an IT environment component that is outside the TOE.

For information about accessing the Windows user interface to verify these settings, see the procedure entitled "Setting IP address information and host security" in the Routine Operations section of the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0.*

Creating Certificates

The most important factor in implementing ADFS is creating and configuring the required certificates appropriately. This section includes procedures for the following tasks:

- Create server authentication certificates for:
  - Resource federation server and Web server
  - Account federation server
- Import and assign server authentication certificates for the account federation server

The first procedure describes how to request a certificate from a Certification Authority (CA) server (<CASvr>) that is in the resource domain; this procedure must be performed on both the resource federation server (<ResFedSvr>) and the Web server (<WebSvr>). The second procedure describes how to request a certificate for the account federation server (<AcctFedSvr>) from the CA server (<CASvr>) in the resource domain.

Table 6.5 indicates the certificate names to use when creating the server authentication certificates for each federation server and the Web server. It is important to use the fully qualified domain name (FQDN) where indicated. Improperly named certificates can cause ADFS operations to fail.

Table 6.5 Computer and certificate names used in Federated Web SSO scenario procedures

Computer role	Computer name	Default Web site certificate name
Resource federation server	<ResFedSvr>	<ResFedSvrFQDN>
Web server	<WebSvr>	<WebSvrFQDN>
Account federation server	<AcctFedSvr>	<AcctFedSvrFQDN>

In order to perform the procedures in this section, the user must be logged on to each of the following computers using an administrative account that is a member of the Domain Admins group in the domain that the computer is joined to:

- Resource federation server (<ResFedSvr>)
- Account federation server (<AcctFedSvr>)
- Web server (<WebSvr>)
- Certification Authority server (<CASvr>)

Creating server authentication certificates for the resource federation server and the Web server

The following procedure is performed on both the federation server and on the Web server. The steps here describe how to request as well as install a server authentication certificate from an online CA.

Create a server authentication certificate for the resource federation server and Web server

On the resource federation server (<ResFedSvr>) and on the Web server (<WebSvr>):

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. In Internet Information Services (IIS) Manager, expand the local computer node, and then expand the **Web Sites** folder.
4. Right-click **Default Web Site** and then click **Properties**.
5. Click the **Directory Security** tab. In the Secure communications area of the Default Web Site Properties page, click the **Server Certificate** button.
6. In the Web Server Certificate Wizard, click **Next**, ensure that the **Create a new certificate** radio button is selected, and click **Next**.
7. In the Delayed or Immediate Request interface, select the radio button for **Send the request immediately to an online certification authority**, and click **Next**.

   Note: If the **Send the request immediately to an online certification authority** option is grayed out, ensure that the logged-on user has administrative credentials and that the computer has access to the <ResourceDomain>.

8. In the Name and Security Settings page, do the following:

- In the **Name** box, type a name for the certificate. Use the fully qualified domain name of the computer (as shown in Table 6.5). For example, on the resource federation server computer, type **<ResFedSvrFQDN>** in the **Name** field; on the Web server, type **<WebSvrFQDN>** in the **Name** field. Verify that every character of the FQDN is typed correctly before proceeding.
- In the **Bit length** list, accept the default of **1024**.
- Click **Next**.

9. In the Organization Information page, do the following:
   - In the **Organization** box, type the organization's name (for example, **Microsoft**).
   - In the **Organizational unit** box, type the name of the organizational unit (for example, **Sales**).
   - Click **Next**.
10. In the Your Site's Common Name page, in the **Common name** box, type the fully qualified name of the computer. For example, for the resource federation server type **<ResFedSvrFQDN>**; for the Web server type **<WebSvrFQDN>**. Verify that every character of the FQDN is typed correctly before proceeding.
11. Click **Next**.
12. In the Geographical Information page, do the following:
    - In the **Country/Region** drop-down list, if not already selected, use the drop-down arrow to select the organization's country or region (for example, **U.S.**).
    - In the **State/Province** drop-down box, type the name of the organization's state or province (for example, **WA**).
    - In the **City/Locality** drop-down box, type the name of the organization's city or locality (for example, **Redmond**).
    - Click **Next**.
13. In the SSL Port interface, ensure that the **SSL port** displayed is **443**, and click **Next**.
14. For **Certification authorities**, select the default CA (**<CASvrFQDN>\CASvr>**) in the list if not already selected, and click **Next**.
15. Verify that the information displayed in the Certificate Request Submission page is correct, and then click **Next**.
16. Click **Finish**. The certificate is installed.

Note: If the certificate installed properly, the **View Certificate** button is no longer grayed out in the Directory Security tab of the Default Web Site Properties page. If the **View Certificate** button is still grayed out, verify that the logged-on user is a member of the Domain Admins group in the domain that the computer is joined to, and repeat the procedure to create the server authentication certificate.

17. Click the **View Certificate** button, verify that the name on the certificate matches the FQDN of the computer exactly, and then exit the Certificate page.
18. Click **OK** to exit Default Web Site Properties.

Ensure that this procedure is repeated on the Web server (<WebSvr>). After performing this procedure on both the federation server and the Web server, proceed to the next procedure to request and create the server authentication certificate for the account federation server, which does not have access to an online CA.

Creating a server authentication certificate for the account federation server

Creating a server authentication certificate for the account federation server is a two-step process. First, request the certificate from the account federation server. Then, use the Certificate Authority (CA) server to create a certificate file that can later be imported to the account federation server's certificate store.

Request a server authentication certificate for the account federation server

On the account federation server (<AcctFedSvr>):

1. Log on as an authorized administrator.
2. Insert a removable media device.
3. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
4. In Internet Information Services (IIS) Manager, expand the local computer node, and then expand the **Web Sites** folder.
5. Right-click **Default Web Site** and then click **Properties**.
6. Click the **Directory Security** tab. In the Secure communications area, click the **Server Certificate** button.
7. In the Web Server Certificate Wizard, click **Next**, ensure that **Create a new certificate** is selected, and click **Next**.
8. In the Delayed or Immediate Request interface, ensure that the radio button for **Prepare the request now, but send it later** is selected, and click **Next**.
9. In the Name and Security Settings page, do the following:
    - In the **Name** box, type a name for the certificate. Use the fully qualified domain name (as shown in Table 6.5). For example, on the resource federation server computer, type **<AcctFedSvrFQDN>** in the **Name** field. Verify that every character of the FQDN is typed correctly before proceeding.
    - In the **Bit length** list, accept the default of **1024**.
    - Click **Next**.
10. In the Organization Information page, do the following:
    - In the **Organization** box, type the organization's name (for example, **Microsoft**).
    - In the **Organizational unit** box, type the name of the organizational unit (for example, **Sales**).
    - Click **Next**.
11. In the Your Site's Common Name page, in the **Common name** box, type the fully qualified name of the computer (**<AcctFedSvrFQDN>**). Verify that every character of the FQDN is typed correctly, and click **Next**.
12. In the Geographical Information page, do the following:
    - In the **Country/Region** drop-down list, if not already selected, use the drop-down arrow to select the organization's country or region (for example, **US**).
    - In the **State/Province** drop-down box, type the name of the organization's state or province (for example, **WA**).

- In the **City/Locality** drop-down box, type the name of the organization's city or locality (for example, **Redmond**).
- Click **Next**.

13. For **File name**, ensure that **c:\certreq.txt** is displayed (if not, type **certreq.txt** for the file name), and click **Next**.
14. Verify that the information displayed in the Request File Summary page is correct and click **Next**.
15. In the Completing the Web Server Certificate Wizard page, click **Finish**.
16. Click **OK** to exit Default Web Site Properties.
17. In Windows explorer, copy the **C:\certreq.txt** file to removable media using these steps:
    - Click **Start**, click **My Computer**, navigate to and double-click the root folder of the local disk (**C:**).
    - Right-click the **certreq.txt** file and click **Copy**.

      In Windows explorer, navigate to and double-click the removable disk drive letter. Right-click the folder to copy the file to and use the **Paste** command to copy the file to the root folder.
18. Close Windows explorer and remove the removable media device from the computer for use in the next procedure.

Leave Internet Information Services (IIS) Manager open for use in a later procedure.

Create a server certificate for the account federation server

On the CA server (<CASvr>):

1. Log on to the CA server (<CASvr>) as an authorized administrator.
2. Insert the removable media containing the **certreq.txt** file created earlier on the account federation server.
3. Click **Start** and then select **Command Prompt**.
4. Change drive letters to the drive letter representing the removable media drive. For example, if the removable media is attached to drive letter F:, type **F:** at the command prompt and press **Enter**.

   Note: If unsure which drive letter to use, click **Start** and then click **My Computer** to determine which drive letter is assigned to the removable media device. Then close Windows Explorer.
5. At the command prompt, if appropriate, type the **CD\<FolderName>** command and press **Enter** to change folders to the folder on the removable media containing certreq.txt.
6. Type the following command, and then press **Enter**:

   certreq –attrib CertificateTemplate:WebServer certreq.txt <AcctFedSvr>_SSL.pfx
7. The Select Certification Authority interface pops up with the local CA listed. Click **OK**.
8. A message is displayed in the command console stating "Certificate retrieved (Issued) Issued."
9. Type **exit** and press **Enter** to exit the command console.
10. Remove the removable media device from the CA server.

Importing and assigning the server authentication certificate on the account federation server

The procedure in this section imports the server authentication certificate to the account federation server's Personal certificate store while assigning it to the Default Web Site in IIS.

Import and assign the server certificate to the account federation server's Default Web Site

On the account federation server (<AcctFedSvr>):

1. Log on as an authorized administrator.
2. Insert the removable media device that contains the <AcctFedSvr>_SSL.pfx file.
3. In the Internet Information Services (IIS) Manager console tree, under the local computer node, ensure that the **Web Sites** folder is expanded.
4. Right-click the **Default Web Site** and select **Properties**.
5. Click the **Directory Security** tab. On the **Directory Security** tab, under Secure communications, click **Server Certificate**.
6. In the Welcome to the Web Server Certificate Wizard, click **Next**.
7. Ensure that **Process the pending request and install the certificate** is selected, and click **Next**.
8. In the Process a Pending Request interface, click **Browse**, click **My Computer**, and for **Files of type** select **All files (*.*)** from the drop-down list.
9. In Windows explorer, navigate to and click once to highlight the **<AcctFedSvr>_SSL.pfx** file located on the removable media, click **Open**, and then (with the correct path and file specified in the Process a Pending Request interface), click **Next**.

   Note: If the removable media disk drive does not appear in the window, press the **F5** function key on the keyboard to refresh the contents of the window.
10. In the SSL Port page, accept the default port number of **443**, and click **Next**.
11. In the Certificate Summary page, verify the details, click **Next**, and then click **Finish**.
12. In the Default Web Site Properties interface, click **OK**, and close Internet Information Services (IIS) Manager.

Distributing the Root Certificate

The computers joined to the resource domain automatically receive the root certificate of the CA through Group Policy. No further configuration is required for this to happen.

The computers joined to the account domain can also receive the root certificate of the CA through Group Policy. This must be configured in the domain security policy for the account domain. Administrators must use removable media to transport the root certificate from the CA to the Trusted Root Certificates store on the account federation server.

This section describes how to configure group policy to distribute the CA root certificate to computers in the account domain. See the CA software operations manual for information about exporting the root certificate to removable media.

Copy the root certificate to removable media

Follow instructions provided with the CA software to locate and copy the root authority certificate to a file. This file typically has a .crt extension and is frequently named using the fully qualified domain name of the CA (i.e., <CASvrFQDN>.crt). Copy the file to a removable media device for use in the ADFS environment.

Configure group policy to distribute the CA's root certificate

Perform this procedure on the <AccountDC>:

1. Log on to the domain controller as a member of the Domain Admins group for that domain.
2. Insert the removable media device that contains the root certificate file from the CA (<CASvrFQDN>.crt).
3. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**.
4. In the console tree, expand the **Public Key Policies** node, right-click **Trusted Root Certification Authorities**, and then click **Import**.
5. On the Welcome to the Certificate Import Wizard, click **Next**.
6. On the File to Import page, browse to the removable media drive, select the root certificate file (**<CASvrFQDN>.crt**), click **Open**, and then click **Next**.
7. On the Certificate Store page, click **Place all certificates in the following store**, and then click **Next**.
8. On the Completing the Certificate Import Wizard, verify that the information provided is accurate, and then click **Finish**.
9. When a pop-up window is displayed indicating "The import was successful," click **OK**. Close the Default Domain Security Settings interface.
10. Remove the removable media device from the computer.

Enforce group policy on account realm computers to distribute the CA's root certificate immediately

On the <AcctFedSvr> and the <AcctClient> computers:

1. Log on as an authorized administrator.
2. Open a Command Prompt interface.
   - On Windows server 2003 operating systems, click **Start** and then select **Command Prompt**.
   - On Windows XP Professional operating systems, click **Start,** click **Run**, type **cmd** in the **Open** box, and click **OK**.
3. In the Command Prompt interface, type **gpupdate /force** and press **Enter**. "Refreshing policy..." is displayed.
4. When the display indicates that the "Refresh has completed," type **exit** and press **Enter** to exit the Command Prompt interface.

Creating User Accounts and Security Groups

Create user and security groups in Active Directory to support claim mappings and user access to the ADFS-enabled applications.

Create User and Group Accounts in the Account Domain

Using the instructions found in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*, create users and security groups on the domain controller in the account domain (<AccountDC>) to support application access and claim mappings. The following chart provides and example of the types of user and security group accounts that must exist to implement and verify the Federated Web SSO scenario:

Active Directory object to create on <AccountDC>	Name	Description
Security global group	<ResClaimAppUsers>	Contains members who can use the claims-aware application hosted in the <ResourceDomain>
Security global group	<ResTokenAppUsers>	Contains members who can use the Windows NT token-based application hosted in the <ResourceDomain>
User	<AcctUser>	Acts as a federated user accessing the claims-aware application and the Windows NT token-based application hosted in the <ResourceDomain>

Add user(s) as members of security group(s) as specified in the following example:

User in account realm	Groups
<AcctUser>	<ResClaimAppUsers> <ResTokenAppUsers>

Create User and Group Accounts in the Resource Domain

Using the instructions found in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*, add a user as specified in the following example:

Active Directory object to create on <ResourceDC>	Name	Description
User	<ResUser>	Acts as an internal user accessing the claims-aware application hosted in the <ResourceDomain>

There is no need to add <ResUser> to any security groups because this user is a member of the resource domain and only accesses the ADFS-enabled claims-aware application internally.

Also, for the purposes of Windows NT token application resource group mapping, create a security group in the <ResourceDomain> as follows:

Active Directory object to create on <ResourceDC>	Name	Description
Security global group	<AcctTokenAppUsers>	Resource group for ADFS resource group mapping

Additional Pre-installation Tasks: Web SSO Scenario

These procedures must be completed prior to installing ADFS; otherwise, the ADFS Setup program fails. This section includes certificate procedures and procedures surrounding creating user accounts and security groups. Topics include:

- Creating Certificates
- Configuring Certificates (and Other Certificate Files)
- Distributing the Root Certificate
- Creating User Accounts and Security Groups

Creating Certificates

The most important factor in implementing ADFS is creating and configuring the required certificates appropriately. The procedures in this section for creating certificates that are used to support federated trust functionality in the evaluated configuration are conducted outside of the TOE.

The following tasks are performed by the Certification Authority (CA) administrator at the computer that serves as the CA (which is outside of the TOE) in the Web SSO scenario implementation:

- Copy certificate revocation list (CRL) and CA root certificate to a removable media device
- Create server authentication certificates for:
    - Federation server
    - Web server
    - Federation service proxy
- Create a client authentication certificate for:
    - Federation service proxy

Table 6.6 shows the naming conventions that the CA administrator must use for each of the ADFS computers used in the Web SSO scenario, along with the certificate names used in the server authentication certificate procedures discussed here. It is important that the ADFS administrator communicate the certificate naming requirements correctly to the CA administrator so that the certificates are configured correctly during creation.

Table 6.6 Computer and server authentication certificate names used in Web SSO procedures

Computer role	Computer name	Certificate name	File name	Certificate Friendly Name
Federation server	<FedSvr>	<FedSvrFQDN>	<FedSvr>_SSL.pfx	FS_SSL
Web server	<WebServer>	<WebServerFQDN>	<WebServer>_SSL.pfx	WS_SSL
Federation service proxy	<FedProxy>	<FedSvrFQDN>[7]	<FedProxy>_SSL.pfx	FSP_SSL

For the client authentication certificate, the CA administrator must use the fully qualified domain name of the federation service proxy (<FedProxyFQDN>) when naming the certificate (<FedProxyFQDN>_cli.pfx).

Copying the certificate revocation list (CRL) and CA root certificate from the CA to a removable media device

It is important to ensure that an up-to-date certificate revocation list (CRL) from the CA is available to the ADFS computers in this scenario at all times. This means that the CA administrator must have a system of updating the CRL at each pre-defined publish date in place in the Web SSO environment. If not, ADFS will malfunction and potentially produce errors that indicate there are problems with the certificate chain or revocation list.

> **Note:** The external CA used in support of the Web SSO scenario is not included in the TOE. Therefore, instructions are not provided in this guide for configuring or using the external CA to publish a CRL.

It is also necessary to distribute the certification authority's root certificate to the computers in the internal domain in the Web SSO scenario. The CA administrator must perform these two tasks:

- **Copy the CRL to removable media**. Follow instructions provided with the CA software to locate and export the CRL to a file. This exported file typically has a .crl extension. Copy the file to the removable media device for use in the ADFS environment, saving it as **<CASvr>.crl**.
- **Copy the root certificate to removable media**. Follow instructions provided with the CA software to locate and copy the root authority certificate to a file. This exported file typically has a .crt extension (although, when exported instead of copied, it can be given a .cer extension.). Copy this file to the removable media device for use in the ADFS environment.

Creating server authentication certificates for the ADFS computers

In order to create the necessary server authentication certificates, the CA administrator must follow instructions provided with the CA server software and copy the certificates created (in the

[7] When naming the server authentication certificate on the federation service proxy, use the fully qualified domain name of the internal federation server (<FedSvrFQDN>), not the fully qualified domain name of the federation service proxy.

form of .pfx files) at the CA to removable media that can be used to transport the certificates to the ADFS computers.

Create server authentication certificates for the federation server, Web server, and federation service proxy

Create server certificates at the CA for each of the ADFS computers. When requesting certificates from the external CA server for the federation server (<FedSvr>), the federation proxy (<FedProxy>), and the Web server (<WebServer>), ensure that the names provided in Table 6.6 are used on the certificates during the certificate request and creation process.

Creating a client authentication certificate for the federation service proxy

Before installing the Federation Service Proxy component of ADFS on the <FedProxy> computer, a client authentication certificate must be installed on the <FedProxy> computer. This is the only server in both ADFS scenarios described in this guide that requires a client authentication certificate. This procedure must be performed by the CA administrator:

Create a client authentication certificate for the Federation Service Proxy computer

In order to create the necessary client authentication certificate, follow instructions provided with the CA software and export the certificate in the form of a .pfx file (named **<FedProxy>_cli.pfx**) created at the CA to removable media. This file will later be transported to the federation service proxy. Ensure that the password used at certificate creation time is accessible to the ADFS administrator implementing the Web SSO scenario.

> **Note:** As a reminder, for the federation service proxy client authentication certificate, do not type the fully qualified domain name of the federation server. Use the federation proxy server's FQDN as the certificate name on the client authentication certificate.

Configuring Certificates (and Other Certificate Files)

After the CA administrator has finished storing the appropriate files on removable media, the ADFS implementation for the evaluated configuration can continue. This section includes procedures for the following tasks:

- Importing and assigning the server authentication certificates for:
  - Federation server
  - Web server
  - Federation service proxy
- Importing the client authentication certificate for:
  - Federation service proxy
- Installing the CRL to a shared network folder
- Distributing the root certificate

Import and assign server authentication certificates for the federation server, Web server, and federation service proxy

Note: When performing the next procedure on the federation service proxy, remember that the file name of the certificate file created at the CA is named for the federation service proxy, even though the common name (CN) of the certificate is named for the federation server. See Table 6.6.

On the federation server (<FedSvr>), Web server (<WebServer>), and federation service proxy (<FedProxy>):

1. Log on as an authorized administrator.
2. Insert the removable media device containing the server authentication certificates in the computer.
3. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
4. In Internet Information Services (IIS) Manager, expand the local computer node, and then expand the **Web Sites** folder.
5. Right-click **Default Web Site** and select **Properties**.
6. Click the **Directory Security** tab.
7. On the **Directory Security** tab, under Secure communications, click **Server Certificate**.
8. In the Welcome to the Web Server Certificate Wizard, click **Next**.
9. Select **Import a certificate from a .pfx file** and click **Next**.
10. In the Import Certificate interface, click **Browse**, click **My Computer**, navigate to and double-click the removable disk drive letter; select the .pfx file (e.g., **<FedSvr>_SSL.pfx** on the federation server, **<WebServer>_SSL.pfx** on the Web server, or **<FedProxy>_SSL.pfx** on the federation service proxy), and then click **Open**.

Note: If the removable media device does not appear in the window, press the **F5** function key on the keyboard to refresh.

11. In the Import Certificate interface, verify that the filename and location is correct and click **Next**.

Note: In the Import Certificate interface, do not select the check box to **Mark certificate as exportable**.

12. In the Import Certificate Password interface, type the password identified when the certificate was created on the external CA. Click **Next**.
13. In the SSL Port page, accept the default port number of **443**, and click **Next**.
14. In the Imported Certificate Summary page, verify the details and click **Next**.
15. Click **Finish**. The certificate is installed.

Note: If the certificate installed properly, the **View Certificate** button is no longer grayed out in the Directory Security tab of the Default Web Site Properties page.

16. Click **OK** in Default Web Site Properties interface to exit.0.

After completing this procedure on the federation server (<FedSvr>), ensure that the procedure is repeated on the Web server (<WebServer>) and on the federation proxy server (<FedProxy>).

Import the client authentication certificate to the federation service proxy

On the federation service proxy (<FedProxy>):

1. Log on as an authorized administrator.
2. Insert the removable media containing the certificate files created on the external CA.
3. Click **Start**, click **Run**, type **mmc**, and press **Enter**.
4. On the **File** menu, click **Add/Remove Snap-in**, click **Add**, click **Certificates**, and click the **Add** button
5. In the Certificates snap-in page, select the **Computer account** radio button and click **Next**.
6. In the Select Computer page, ensure that **Local Computer** is selected, and click **Finish**.
7. Click **Close**, and then click **OK**.
8. In the console tree of the management console, expand the **Certificates (Local Computer)** node, right-click the **Personal** Certificates subfolder, point to **All Tasks**, and click **Import**.
9. In the Welcome to the Certificate Import Wizard, click **Next**.
10. In the File to Import page, click **Browse**, click **My Computer**, then navigate to and double-click the removable media device drive letter. In the Open interface, click the drop-down arrow next to **Files of type**, and select **Personal Information Exchange (*.pfx, *.p12)**. Select the **<FedProxy>_cli.pfx** file, and then click **Open**.

    Note: If the removable media device does not appear in the window, press the **F5** function key on the keyboard to refresh.

11. In the File to Import page, ensure that the path and file name are correct, then click **Next**.
12. When prompted, type the password for the private key that was identified when the certificate was created at the CA, and click **Next**.

    Note: Do not select the check box to **Mark this key as exportable**.

13. In the Certificate Store interface, accept the default to place the certificate in the **Personal** store, and click **Next**. Click **Finish**.
14. Click **OK**.

    Note: The new client authentication certificate displayed in the details pane of the management console should be named for the proxy federation server (i.e., **<FedProxyFQDN>**). (To see this detail, in the console tree expand the **Personal** store and expand **Certificates** beneath it.)

15. Close the management console. When prompted to save the console settings, click **No**.

Installing the certificate revocation list (CRL) to a shared network folder

In the Web SSO scenario procedures described here, because the CA is external to the <InternalDomain> domain hosting the federation server, it is necessary to install the CRL in a shared network folder that is accessible to the ADFS computers. This requires creating the shared folder, assigning permissions to it, and maintaining an updated CRL in that folder. Within the Web SSO architecture of the TOE, the federation service proxy is used to host the CRL.

Copy the CRL to the shared folder

On the federation service proxy (<FedProxy>):

1. Log on as an authorized administrator.
2. Insert the removable media device that contains the **<CASvr>.crl** file from the external CA.
3. On the **Start** menu, click **Run**, type **c:**, and press **Enter**. This opens Windows explorer to the root of the local system disk (C:\).
4. In Windows explorer, click **File**, point to **New**, and select **Folder**. For the name of the folder, type **CRL**, and press **Enter**.
5. Right-click the **CRL** folder, select **Properties**, and then click the **Sharing** tab in the CRL Properties interface.
6. Select the **Share this folder** radio button. Leave the default share name as **CRL**, and leave the rest of the settings at their defaults. Click **OK**.
7. In Windows explorer, navigate to the removable disk drive letter. Right-click the **<CASvr>.crl** file from the external CA, and select **Copy** to copy the file to the Windows clipboard.
8. In Windows explorer, navigate to the root of the local system disk (C:\) and double-click the **CRL** folder to open it. Click **Edit** and then **Paste** to paste the **<CASvr>.crl** file from the clipboard into the CRL folder.
9. Exit Windows explorer.

Distributing the Root Certificate

The computers joined to the internal domain can automatically receive the root certificate of the external CA through Group Policy. This must be configured in the domain security policy for the internal domain (<InternalDomain>). Administrators must use removable media to transport the root certificate from the CA to the Trusted Root Certificates store on the <InternalDC>.

The external client computer, which is not domain-joined, can be configured with the root certificate too. This must be done manually by importing the root certificate from a removable media device.

The procedures here describe how to configure group policy to distribute the CA root certificate to computers in the internal domain and how to import the root certificate to the local certificate store on the external client computer (<ExtClient>). See the CA software operations manual for information about exporting the root certificate to removable media.

Configure group policy to distribute the CA's root certificate

Perform this procedure on the <InternalDC>:

1. Log on to the domain controller as a member of the Domain Admins group.
2. Insert the removable media device containing the root certificate from the CA.
3. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**.

   Note: Be careful not to select the **Domain Controller Security Policy** in this step.

4. In the console tree, expand **Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then click **Import**.
5. In the Welcome to the Certificate Import Wizard, click **Next**.

6. On the File to Import page, click **Browse**, click **My Computer**, and navigate to the removable media drive. Select the root certificate file, click **Open**, verify that the correct file and location is displayed in the **File to Import** page, and then click **Next**.
7. On the Certificate Store page, for **Certificate Store**, accept the default to place all certificates in the Trusted Root Certification Authorities store and click **Next**.
8. On the Completing the Certificate Import Wizard, verify that the information provided is accurate, and then click **Finish**.
9. Click **OK**.
10. Close the Default Domain Security Settings console and remove the removable media device from the computer.

Enforce group policy on the domain-joined computers to distribute the CA's root certificate immediately

On the <FedSvr>, the <WebServer>, and the <FedProxy> computers:

1. Log on as an authorized administrator.
2. Click **Start** and then select **Command Prompt**.
3. In the Command Prompt interface, type **gpupdate /force** and press **Enter**. A message stating "Refreshing policy..." is displayed.
4. When the display indicates that the "Refresh has completed," type **exit** and press **Enter** to exit the Command Prompt interface.

After the ADFS computers are configured with IIS, ASP.NET 2.0, and the required certificates, ADFS components can be successfully installed.

Import the root certificate on the external client computer

On the <ExtClient>:

1. Log on as an authorized administrator (for example, <ExtClient>\Administrator).
2. Insert the removable media device containing the root certificate from the CA.
3. Click **Start**, click **Run**, type **mmc**, and press **Enter**.
4. On the **File** menu, click **Add/Remove Snap-in**, click **Add**, click **Certificates**, and click the **Add** button
5. In the Certificates snap-in page, select the **Computer account** radio button and click **Next**.
6. In the Select Computer page, ensure that **Local Computer** is selected, and click **Finish**.
7. Click **Close**, and then click **OK**.
8. In the console tree of the management console, expand the **Certificates (Local Computer)** node, right-click the **Trusted Root Certificate Authorities** subfolder, point to **All Tasks**, and click **Import**.
9. In the Welcome to the Certificate Import Wizard, click **Next**.
10. In the File to Import page, click **Browse**, click **My Computer**, then navigate to and double-click the removable media device drive letter. Select the CA root certificate file stored on the removable media device, and then click **Open**.

Note: If the removable media device does not appear in the window, press the **F5** function key on the keyboard to refresh.

11. In the File to Import page, ensure that the path and file name are correct, then click **Next**.
12. In the Certificate Store interface, accept the default to place the certificate in the **Trusted Root Certification Authorities** store, and click **Next**. Click **Finish**.
13. Click **OK**.
14. Close the management console. When prompted to save the console settings, click **No**.
15. Remove the removable media disk.

Creating User Accounts and Security Groups

Using the instructions found in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0* and the example accounts provided here, create an organizational unit (OU), users, and security groups on the domain controller in the internal domain to support application access and claim mappings.

First, create an OU called <FederatedUsers> on the domain controller computer in the internal domain. This OU will be used for storing the users and groups needed to support ADFS functionality. Then, using the following chart as a guide, create user and security group accounts required to ADFS-enabled application access.

Active Directory object to create on <InternalDC>	Name	Organizational unit
Security global groups	<TokenAppUsers> <ClaimAppUsers>	<FederatedUsers> Users
User	<ExtUser>	Users

Add group as member of the <FederatedUsers> OU according to the following example:

Group in resource realm	Organizational unit
<TokenAppUsers>	<FederatedUsers>

Add user to security groups as in this example:

User account	Organizational unit \ group accounts
<ExtUser>	<FederatedUsers>\<TokenAppUsers> Users\<ClaimAppUsers>

Also, create a local user account (<LocalUser>) on the external client computer (<ExtClient>). When these tasks are completed, proceed to the ADFS Installation and Configuration: Web SSO Scenario topic.

ADFS Installation and Configuration: Federated Web SSO Scenario

This section describes the procedures for installing and configuring ADFS in a Federated Web SSO scenario. After ADFS components are installed, several steps are required to configure ADFS for the Federated Web SSO scenario implementation described in this guide. Instructions for accessing the federated applications from client computers in the ADFS environment are also included at the end of this section.

This section describes the following processes in detail:

- Installing the Federation Service
- Installing the Web Agents
- Exporting the token-signing certificate from the account federation server to a file
- Creating the claims-aware applications
- Creating the Windows NT token-based application
- Configuring the Web server
- Configuring auditing, event logging, and debug logging on the federation servers
- Configuring the Federation Service on the federation servers
- Accessing federated applications from a client computer

Installing the Federation Service

Use the following procedure to install the Federation Service component on the resource federation server in a Federated Web SSO scenario. There is a separate procedure for installing the Federation Service on the account federation server. In order to perform all of the procedures in this section, the administrator conducting these procedures must be logged on to the ADFS computers with an account that is a member of the Domain Admins group for the domain that the computer is joined to.

Note: After completing the installation and configuration of the Federated Web SSO Scenario, as described in this section, it is important to apply the ADFS FIPS update on all federation servers and ADFS Web servers in order to mitigate a conflict between the ADFS and FIPS security policy setting as described in Microsoft Knowledge Base article KB935449. To apply the ADFS FIPS update, follow the procedures in Apply ADFS FIPS Update.

Install the Federation Service on the resource federation server

On the resource federation server (<ResFedSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In Add or Remove Programs, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, select **Active Directory Services** to highlight it.

   Note: Do not click the check box next to **Active Directory Services** in this step.
6. Click the **Details** button.

7. In the Active Directory Services interface, select **Active Directory Federation Services (ADFS)** to highlight it.

   Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. Click the **Details** button.
9. In the Active Directory Federation Services (ADFS) interface, select only the **Federation Service** check box and click **OK**.

   Note: If prompted, "Do you want to enable ASP.NET 2.0?" click **Yes** to enable it, and then click **OK**. If .NET Framework 2.0 was installed correctly as described earlier in this guide, this prompt is not displayed.

10. In the Active Directory Services interface, click **OK**.

    Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs, despite the fact that ADFS functionality relies on ASP.NET 2.0, not ASP.NET 1.1. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

11. In the Windows Components Wizard, click **Next**.
12. In the Federation Service page, click **Select token-signing certificate**.
13. Click the **Select** button.
14. In the Select Certificate page, ensure that the resource federation server authentication certificate it highlighted, and click **OK**.
15. In the Federation Service page, for Trust Policy, ensure that **Create a new trust policy** is selected, and then click **Next**.

    Note: If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate, click the **Open** button, and click **OK**.

16. In the Completing the Windows Components Wizard, click **Finish**.
17. Close Add or Remove Programs.
18. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

    Note: For 64-bit operating systems, skip the rest of this procedure.

19. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
20. Click the **Web Service Extensions** node in the console tree.
21. At the bottom of the details pane, click the **Standard** tab.
22. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Use the following procedure to install the Federation Service component of ADFS on the account federation server (<AcctFedSvr>).

Install the Federation Service on the account federation server

On the account federation server (<AcctFedSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD. If a Welcome to Microsoft Windows Server 2003 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In Add or Remove Programs, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, click **Active Directory Services** to highlight it.

   Note: Do not click the check box next to **Active Directory Services** in this step.

6. Click the **Details** button.
7. In the Active Directory Services interface, click **Active Directory Federation Services (ADFS)** to highlight it.

   Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. Click the **Details** button.
9. In the Active Directory Federation Services (ADFS) interface, select the **Federation Service** check box, and click **OK**.

   Note: If prompted, “Do you want to enable ASP.NET 2.0?” click **Yes** to enable it, and then click **OK**. If .NET Framework 2.0 was installed correctly as described earlier, this prompt is not displayed.

10. In the Active Directory Services interface, click **OK**.

    Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

11. In the Windows Components Wizard, click **Next**.
12. In the Federation Service page, click **Create a self-signed token-signing certificate**. Ensure that **Create a new trust policy** is selected, and then click **Next**.

    Note: If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate, click the **Open** button, and click **OK**.

13. In the Completing the Windows Components Wizard, click **Finish**.
14. Close Add or Remove Programs.

15. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

Note: For 64-bit operating systems, skip the rest of this procedure and proceed to the Installing the Web Agents section.

16. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
17. Click the **Web Service Extensions** node in the console tree.
18. At the bottom of the details pane, click the **Standard** tab.
19. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Installing the Web Agents

The ADFS component that is installed on the Web server that hosts ADFS-enabled Web applications is called the Web Agent. There are two Web Agents—one for claims-aware applications, and another for Windows NT token-based applications. In this procedure, both Web Agents are installed.

Install the ADFS Web Agents

On the Web server (<WebSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD. If a Welcome to Microsoft Windows Server 2003 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In **Add or Remove Programs**, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, click **Active Directory Services** to highlight it.

Note: Do not click the check box next to **Active Directory Services** in this step.

6. Click the **Details** button.
7. In the Active Directory Services interface, click **Active Directory Federation Services (ADFS)** to highlight it.

Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. Click the **Details** button.
9. In the **Active Directory Federation Services (ADFS)** interface, if any check boxes are pre-selected, clear them. Select the check box for **ADFS Web Agents,** and then click **Details**.
10. In the **ADFS Web Agents** interface, ensure that both the **Claims-aware applications** and **Windows NT token-based applications** check boxes are selected, and then click **OK**.
11. In the **Active Directory Federation Services (ADFS)** interface, ensure that the **ADFS Web Agents** check box is the only check box selected, and click **OK**.
12. In the Active Directory Services interface, click **OK**.

Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs, not ASP.NET 1.1. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

13. In the Windows Components Wizard, click **Next**.

Note: If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate, click the **Open** button, and click **OK**.

14. In the Completing the Windows Components Wizard, click **Finish**.
15. Close Add or Remove Programs.
16. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

Note: For 64-bit operating systems, skip the rest of this procedure.

17. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
18. Click the **Web Service Extensions** node in the console tree.
19. At the bottom of the details pane, click the **Standard** tab.
20. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Exporting the Token-signing Certificate from the Account Federation Server to a File

In the procedure described here, export the token-signing certificate created during ADFS setup on the account federation server to a file stored on the system drive of the local disk. This file will be accessed in a later procedure to add and configure an account partner on the resource federation server.

Export the token-signing certificate to a file

On the <AcctFedSvr>:

1. Insert a removable media device and log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
3. Expand the **Federation Services** node in the console tree, right-click the **Trust Policy** node, and then click **Properties**.
4. Click the **Verification Certificates** tab.

5. Click once to highlight the **Federation Server <AcctFedSvr>** certificate that appears in the Verification Certificates interface, and then click the **View** button. The certificate is displayed in a new window.
6. In the Certificate page, click the **Details** tab, and then click the **Copy to File** button.
7. In the Welcome to the Certificate Export Wizard, click **Next**.
8. In the Export File Format page, ensure that the radio button for **DER encoded binary X.509 (.CER)** is selected, and click **Next**.
9. In the File to Export page, click the **Browse** button, click **My Computer**, navigate to and double-click the removable disk drive letter. For **File name** type **<AcctFedSvr>_ts.cer**, click **Save**, and then click **Next** in the File to Export page.
10. Click **Finish** to complete the export.
11. At the interface indicating the export was successful, click **OK**.
12. Click **OK** in the Certificate page, and then click **OK** in the Trust Policy Properties page to return to the ADFS management console.
13. Remove the removable media device from the computer.

Creating the Claims-aware Applications

This guide employs the sample claims-aware applications that are provided in this section. At this point in a production deployment of ADFS, administrators can substitute their own claims-aware applications. Each of the two claims-aware applications (called “Claimapp” and “Claimapp2”) are made up of three files that can be created from the instructions included here:

- Default.aspx
- Web.config
- Default.aspx.cs

Use the procedures here to create these three files and copy them to the Web server. Later in this guide instructions are provided for modifying these files for use in the ADFS environment. In order to complete the procedures in this section, access to a soft copy of this guide on a removable media device is required.

Note: Use any ADFS computer in the evaluated configuration to perform these procedures for creating the claims-aware applications and the Windows NT token-based application.

Open this guide in WordPad

1. On the computer used to create the claims-aware application files, insert the removable media device containing a copy of this guide into the computer.
2. Click **Start**, click **My Computer**, and double-click the removable disk drive letter that is displayed.
3. In Windows explorer, navigate to and double-click the file representing this document.
4. A pop-up window appears, entitled **Microsoft Word 97 Conversion**, stating, “Unable to load graphics conversion filter. Continue with document conversion?” Click **Yes**.

Note: This pop-up window might appear multiple times. If so, continue to click **Yes** in that window until no more pop-ups are displayed and the document is displayed in WordPad.

5. This file opens in WordPad.

Create the folder on the removable media device

1. Insert a removable media device into the computer. Click **Start**, click **My Computer**, and double-click the removable disk drive letter that is displayed.
2. In Windows explorer, click **File**, point to **New**, and click **Folder**. Type **claimapp** as the New Folder name, and press Enter.
3. Repeat Step 2, typing **claimapp2** as the New Folder name.
4. Repeat Step 2 again, typing **tokenapp** as the New Folder name.
5. Close Windows explorer.

Creating the Default.aspx file for Claimapp

On the same computer, use the following procedure to create the Default.aspx file for use in the first claims-aware application (Claimapp).

Create the Default.aspx file

1. Click **Start**, click **Run**, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code text from WordPad into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<%@ Page Language="C#" AutoEventWireup="true" CodeFile="Default.aspx.cs"
Inherits="_Default" %>

<%@ OutputCache Location="None" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >

<head>

<meta http-equiv="Content-Language" content="en-us">

<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">

<title>Claims-aware Sample Application</title>

<style>

<!--
```

```
.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}

.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}

.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-weight: bold;
background-color: #cccccc ; text-align: left }

.propertyTable { border-collapse: collapse;}

td.l{ width: 200px }

tr.s{ background-color: #eeeeee }

.banner      { margin-bottom: 18px }

.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial; font-weight:
bold; margin-top: 18}

.abbrev { color: #0066FF; font-style: italic }

-->

</style>

</head>


<body>

<form ID="Form1" runat=server>

<div class=banner>

<div class=pagetitle>SSO Sample</div>

[ <asp:HyperLink ID=SignOutUrl runat=server>Sign Out</asp:HyperLink> | <a
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refresh without viewstate
data</a>]

</div>

<div class=propertyHead>Page Information</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table runat=server ID=PageTable CssClass=propertyTable>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>

    </asp:TableHeaderRow>

</asp:Table>

</div>

<div class=propertyHead>User.Identity</div>

<div style="padding-left: 10px; padding-top: 10px">

<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>

    <asp:TableHeaderRow>

        <asp:TableHeaderCell>Name</asp:TableHeaderCell>

        <asp:TableHeaderCell>Value</asp:TableHeaderCell>

        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
```

```
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>(SingleSignOnIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SSOIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>SingleSignOnIdentity.SecurityPropertyCollection</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SecurityPropertyTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Uri</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Type</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Value</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>(IPrincipal)User.IsInRole(...)</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=RolesTable runat=server>
</asp:Table>
```

```
<div style="padding-top: 10px">

<table>

<tr><td>Roles to check (semicolon separated):</td></tr>

<tr><td><asp:TextBox ID=Roles Columns=55 runat=server/></td><td align=right><asp:Button
UseSubmitBehavior=true ID=GetRoles runat=server Text="Check Roles"
OnClick="GoGetRoles"/></td></tr>

</table>

</div>

</div>

</form>

</body>

</html>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, click **My Computer**, navigate to and double-click the removable disk drive letter and then double-click the **claimapp** folder that was created in the previous procedure.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.aspx** exactly.

5. Exit Notepad.

Creating the Default.aspx file for Claimapp2

On the same computer, use the following procedure to create the Default.aspx file for use in the secondary claims-aware application (Claimapp2).

Create the Default.aspx file

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<%@ Page Language="C#" AutoEventWireup="true"  CodeFile="Default.aspx.cs"
Inherits="_Default" %>

<%@ OutputCache Location="None" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
```

```
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Claims-aware Sample Application #2</title>
<style>
<!--
.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}
.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}
.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-weight: bold;
text-align: left }
.propertyTable { border-collapse: collapse;}
td.l{ width: 200px }
tr.s{ background-color: #eeeeee }
.banner      { margin-bottom: 18px }
.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial; font-weight:
bold; margin-top: 18}
.abbrev { color: #0066FF; font-style: italic }
-->
</style>
</head>

<body bgcolor=99ccff; font=arial>

<form ID="Form1" runat=server>

<div class=banner>
<div class=pagetitle>SSO Sample for Claimapp #2</div>
[ <asp:HyperLink ID=SignOutUrl runat=server>Sign Out</asp:HyperLink> | <a
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refresh without viewstate
data</a>]
</div>

<div class=propertyHead>Page Information</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table runat=server ID=PageTable CssClass=propertyTable>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
```

```
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(SingleSignOnIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SSOIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>SingleSignOnIdentity.SecurityPropertyCollection</div>
```

```
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SecurityPropertyTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Uri</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Type</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Value</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IPrincipal)User.IsInRole(...)</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=RolesTable runat=server>
</asp:Table>

<div style="padding-top: 10px">
<table>
<tr><td>Roles to check (semicolon separated):</td></tr>
<tr><td><asp:TextBox ID=Roles Columns=55 runat=server/></td><td align=right><asp:Button
UseSubmitBehavior=true ID=GetRoles runat=server Text="Check Roles"
OnClick="GoGetRoles"/></td></tr>
</table>
</div>

</div>
</form>
</body>

</html>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp2** folder that was created in the previous procedure.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.aspx** exactly.

5. Exit Notepad.

Creating the Web.config file for Claimapp

Use the following procedure to create the Web.config file for the first claims-aware application (Claimapp).

Create the Web.config file

1. Click **Start**, click **Run**, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
   <configSections>
      <sectionGroup name="system.web">
              <section name="websso"

type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
      </sectionGroup>
   </configSections>
   <system.web>
    <machineKey validationKey="AutoGenerate,IsolateApps"
decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
    <sessionState mode="Off" />
    <compilation defaultLanguage="c#">
       <assemblies>
          <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
          <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
       </assemblies>
    </compilation>
    <customErrors mode="Off"/>
    <authentication mode="None" />
    <httpModules>
        <add
            name="Identity Federation Services Application Authentication Module"
```

```
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
    </httpModules>


       <websso>
        <auditlevel>247</auditlevel>
        <authenticationrequired />
        <eventloglevel>55</eventloglevel>
        <auditsuccess>2</auditsuccess>
        <urls>
          <returnurl>https://pe1420.lab.domain.tld:8081/claimapp/</returnurl>
        </urls>
        <cookies writecookies="true">
          <path>/claimapp</path>
          <lifetime>240</lifetime>
        </cookies>
    <fs>https://326m2.lab.domain.tld/adfs/fs/federationserverservice.asmx</fs>
      </websso>
</system.web>
   <system.diagnostics>
      <switches>
  <add name="WebSsoDebugLevel" value="0" /> <!-- Change to 255 to enable full debug
logging -->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
            <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData="c:\logdir\claimapp.log" />
         </listeners>
      </trace>
   </system.diagnostics>
</configuration>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Web.config** and then click the **Save** button.

Note: Be sure not to append the file name with .txt. The filename needs to be **Web.config** exactly.

5. Exit Notepad.

Creating the Web.config file for Claimapp2

Use the following procedure to create the Web.config file for the secondary claims-aware application (Claimapp2).

Create the Web.config file

1. Click **Start**, click **Run**, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
   <configSections>
      <sectionGroup name="system.web">
              <section name="websso"

type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
      </sectionGroup>
   </configSections>
   <system.web>
    <machineKey validationKey="AutoGenerate,IsolateApps"
decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
    <sessionState mode="Off" />
    <compilation defaultLanguage="c#">
       <assemblies>
          <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
          <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
       </assemblies>
    </compilation>
    <customErrors mode="Off"/>
```

```
    <authentication mode="None" />
    <httpModules>
        <add
            name="Identity Federation Services Application Authentication Module"
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
    </httpModules>


       <websso>
        <auditlevel>247</auditlevel>
        <authenticationrequired />
        <eventloglevel>55</eventloglevel>
        <auditsuccess>2</auditsuccess>
        <urls>
          <returnurl>https://pe1420.lab.domain.tld:8083/claimapp2/</returnurl>
        </urls>
        <cookies writecookies="true">
          <path>/claimapp2</path>
          <lifetime>240</lifetime>
        </cookies>
    <fs>https://326m2.lab.domain.tld/adfs/fs/federationserverservice.asmx</fs>
      </websso>
</system.web>
   <system.diagnostics>
      <switches>
  <add name="WebSsoDebugLevel" value="0" /> <!-- Change to 255 to enable full debug
logging -->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
            <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData="c:\logdir\claimapp2.log" />
         </listeners>
      </trace>
   </system.diagnostics>
</configuration>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp2** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Web.config** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Web.config** exactly.

5. Exit Notepad.

Creating the Default.aspx.cs file

Use the following procedure to create the Default.aspx.cs file. This file will be used in both Claimapp and Claimapp2.

Create the Default.aspx.cs file

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
using System;
using System.IO;
using System.Text;
using System.Data;
using System.Collections.Generic;
using System.Configuration;
using System.Reflection;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Web.UI.HtmlControls;
using System.Security;
using System.Security.Principal;
```

```
using System.Web.Security.SingleSignOn;
using System.Web.Security.SingleSignOn.Authorization;


public partial class _Default : System.Web.UI.Page
{
    const string NullValue = "<span class=\"abbrev\" title=\"Null Reference, or not
applicable\"><b>null</b></span>";


    static Dictionary<string, string> s_abbreviationMap;


    static _Default()
    {
        s_abbreviationMap = new Dictionary<string, string>();
        //
        // Add any abbreviations here.  Make sure that prefixes of
        // replacements occur *after* the longer replacement key.
        //
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn.Authorization",
"SSO.Auth");
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn", "SSO");
        s_abbreviationMap.Add("System", "S");
    }


    protected void Page_Load(object sender, EventArgs e)
    {
        SingleSignOnIdentity ssoId = User.Identity as SingleSignOnIdentity;


        //
        // Get some property tables initialized.
        //
        PagePropertyLoad();
        IdentityLoad();
        BaseIdentityLoad();
        SSOIdentityLoad(ssoId);
        SecurityPropertyTableLoad(ssoId);


        //
        // Filling in the roles table
        // requires a peek at the viewstate
```

```
        // since we have a text box driving this.
        //
        if (!IsPostBack)
        {
            UpdateRolesTable(new string[] { });
        }
        else
        {
            GoGetRoles(null, null);
        }

        //
        // Get the right links for SSO
        //
        if (ssoId == null)
        {
            SignOutUrl.Text = "Single Sign On isn't installed...";
            SignOutUrl.Enabled = false;
        }
        else
        {
            if (ssoId.IsAuthenticated == false)
            {
                SignOutUrl.Text = "Sign In (you aren't authenticated)";
                SignOutUrl.NavigateUrl = ssoId.SignInUrl;
            }
            else
                SignOutUrl.NavigateUrl = ssoId.SignOutUrl;
        }
    }

    void SecurityPropertyTableLoad(SingleSignOnIdentity ssoId)
    {
        Table t = SecurityPropertyTable;

        if (ssoId == null)
        {
            AddNullValueRow(t);
```

```
            return;
        }

        //
        // Go through each of the security properties provided.
        //
        bool alternating = false;
        foreach (SecurityProperty securityProperty in ssoId.SecurityPropertyCollection)
        {
            t.Rows.Add(CreateRow(securityProperty.Uri, securityProperty.Name,
securityProperty.Value, alternating));
            alternating = !alternating;
        }
    }

    void UpdateRolesTable(string[] roles)
    {
        Table t = RolesTable;

        t.Rows.Clear();

        bool alternating = false;
        foreach (string s in roles)
        {
            string role = s.Trim();
            t.Rows.Add(CreatePropertyRow(role, User.IsInRole(role), alternating));

            alternating = !alternating;
        }
    }

    void IdentityLoad()
    {
        Table propertyTable = IdentityTable;

        if (User.Identity == null)
        {
            AddNullValueRow(propertyTable);
        }
```

```
        else
        {
            propertyTable.Rows.Add(CreatePropertyRow("Type name",
User.Identity.GetType().FullName));
        }
    }

    void SSOIdentityLoad(SingleSignOnIdentity ssoId)
    {
        Table propertyTable = SSOIdentityTable;

        if (ssoId != null)
        {
            PropertyInfo[] props = ssoId.GetType().GetProperties(BindingFlags.Instance |
BindingFlags.Public | BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, ssoId, props);
        }
        else
        {
            AddNullValueRow(propertyTable);
        }
    }

    void PagePropertyLoad()
    {
        Table propertyTable = PageTable;

        string leftSidePath = Request.Url.GetLeftPart(UriPartial.Path);

        propertyTable.Rows.Add(CreatePropertyRow("Simplified Path", leftSidePath));
    }

    void BaseIdentityLoad()
    {
        Table propertyTable = BaseIdentityTable;
        IIdentity identity = User.Identity;

        if (identity != null)
        {
```

```
            PropertyInfo[] props = typeof(IIdentity).GetProperties(BindingFlags.Instance
| BindingFlags.Public | BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, identity, props);
        }
        else
        {
            AddNullValueRow(propertyTable);
        }
    }

    void AddNullValueRow(Table table)
    {
        TableCell cell = new TableCell();
        cell.Text = NullValue;

        TableRow row = new TableRow();
        row.CssClass = "s";
        row.Cells.Add(cell);

        table.Rows.Clear();
        table.Rows.Add(row);
    }

    void AddPropertyRows(Table propertyTable, object obj, PropertyInfo[] props)
    {
        bool alternating = false;

        foreach (PropertyInfo p in props)
        {
            string name = p.Name;
            object val = p.GetValue(obj, null);

            propertyTable.Rows.Add(CreatePropertyRow(name, val, alternating));
            alternating = !alternating;
        }
    }

    TableRow CreatePropertyRow(string propertyName, object propertyValue)
    {
```

```
        return CreatePropertyRow(propertyName, propertyValue, false);
    }

    TableRow CreatePropertyRow(string propertyName, object value, bool alternating)
    {
        if (value == null)
            return CreateRow(propertyName, null, null, alternating);
        else
            return CreateRow(propertyName, value.ToString(), value.GetType().FullName ,
alternating);
    }

    TableRow CreateRow(string s1, string s2, string s3, bool alternating)
    {
        TableCell first = new TableCell();
        first.CssClass = "l";
        first.Text = Abbreviate(s1);

        TableCell second = new TableCell();
        second.Text = Abbreviate(s2);

        TableCell third = new TableCell();
        third.Text = Abbreviate(s3);

        TableRow row = new TableRow();
        if (alternating)
            row.CssClass = "s";
        row.Cells.Add(first);
        row.Cells.Add(second);
        row.Cells.Add(third);

        return row;
    }

    private string Abbreviate(string s)
    {
        if (s == null)
            return NullValue;
```

```
        string retVal = s;
        foreach (KeyValuePair<string, string> pair in s_abbreviationMap)
        {
            //
            // We only get one replacement per abbreviation call.
            // First one wins.
            //
            if (retVal.IndexOf(pair.Key) != -1)
            {
                string replacedValue = string.Format("<span class=\"abbrev\"
title=\"{0}\">{1}</span>", pair.Key, pair.Value);
                retVal = retVal.Replace(pair.Key, replacedValue);
                break;
            }
        }
        return retVal;
    }

    //
    // ASP.NET server side callback
    //
    protected void GoGetRoles(object sender, EventArgs ea)
    {
        string[] roles = Roles.Text.Split(';');
        UpdateRolesTable(roles);
    }

private void save_request()
{
        int loop1, loop2, strLen;
        HttpCookieCollection MyCookieColl;
        HttpCookie MyCookie;

          string strFilePath = Request.PhysicalApplicationPath +
              "Default_WebA_" + DateTime.Now.ToFileTimeUtc() + ".dat";

        StreamWriter sw = File.CreateText(strFilePath);

        try
```

```
        {

sw.WriteLine("================================================================================
===============");
            sw.WriteLine("Log File: " + strFilePath);
            sw.WriteLine("Created: " + Server.HtmlEncode(DateTime.Now.ToString()));
            sw.WriteLine("CurrentExecutionFilePath: " +
Server.HtmlEncode(Request.CurrentExecutionFilePath));
            sw.WriteLine("ApplicationPath: " +
Server.HtmlEncode(Request.ApplicationPath));
            sw.WriteLine("FilePath: " + Server.HtmlEncode(Request.FilePath));
            sw.WriteLine("Path: " + Server.HtmlEncode(Request.Path));

            // Iterate through the Form collection and write
            // the values to the file with HTML encoding.
            // String[] formArray = Request.Form.AllKeys;
            foreach (string s in Request.Form)
            {
                sw.WriteLine("Form: " + Server.HtmlEncode(s));
            }

            if (Request.PathInfo == String.Empty)
            {
                sw.WriteLine("The PathInfo property contains no information.");
            }
            else
            {
                sw.WriteLine("PathInfo: " + Server.HtmlEncode(Request.PathInfo));
            }

            // Write request information to the file with HTML encoding.
            sw.WriteLine("PhysicalApplicationPath: " +
Server.HtmlEncode(Request.PhysicalApplicationPath));
            sw.WriteLine("PhysicalPath: " + Server.HtmlEncode(Request.PhysicalPath));
            sw.WriteLine("RawUrl: " + Server.HtmlEncode(Request.RawUrl));
            sw.WriteLine("TotalBytes: " + Convert.ToString(Request.TotalBytes,10));

            // Write request information to the file with HTML encoding.
            sw.WriteLine("RequestType: " + Server.HtmlEncode(Request.RequestType));
            sw.WriteLine("UserHostAddress: " +
Server.HtmlEncode(Request.UserHostAddress));
```

```
            sw.WriteLine("UserHostName: " + Server.HtmlEncode(Request.UserHostName));
            sw.WriteLine("HttpMethod: " + Server.HtmlEncode(Request.HttpMethod));

            // Write cookie information to the file.

            MyCookieColl = Request.Cookies;

            // Capture all cookie names into a string array.
            String[] arr1 = MyCookieColl.AllKeys;

            // Grab individual cookie objects by cookie name.
            for (loop1 = 0; loop1 < arr1.Length; loop1++)
            {
                MyCookie = MyCookieColl[arr1[loop1]];
                sw.WriteLine("Cookie: " + MyCookie.Name.ToString());
                sw.WriteLine("Path: " + MyCookie.Path.ToString());
                //sw.WriteLine("Domain: " + MyCookie.Domain.ToString());
                sw.WriteLine("Expires: " + MyCookie.Expires.ToString());
                sw.WriteLine("Secure:" + MyCookie.Secure.ToString());

                //Grab all values for single cookie into an object array.
                String[] arr2 = MyCookie.Values.AllKeys;

                //Loop through cookie Value collection and print all values.
                for (loop2 = 0; loop2 < arr2.Length; loop2++)
                {
                    sw.WriteLine("Value " + Convert.ToString(loop2) + ": " +
Server.HtmlEncode(arr2[loop2]));
                }
            }

            // Iterate through the UserLanguages collection and
            // write its HTML encoded values to the file.
            for (loop1 = 0; loop1 < Request.UserLanguages.Length; loop1++)
            {
                sw.WriteLine(@"User Language " + loop1 + ": " +
Server.HtmlEncode(Request.UserLanguages[loop1]));
            }
```

```
        Stream str = Request.InputStream;
        strLen = (int)str.Length;
        if (strLen > 0 )
        {
               Byte[] strArr = new Byte[strLen];
               int strRead = str.Read(strArr, 0, strLen);

               StringBuilder sb = new StringBuilder();
               // Convert Byte array to a text string.
               for(loop1=0; loop1 < strLen; loop1++)
               {
                 sb.Append(strArr[loop1].ToString());
               }
sw.WriteLine("==========================================================================
==============");
               sw.WriteLine("Request.InputStream: ");
                sw.WriteLine(sb.ToString());
        }
        else
        {
sw.WriteLine("==========================================================================
==============");
               sw.WriteLine("Request.InputStream: Empty");
        }

        HttpClientCertificate ccrt = Request.ClientCertificate;

sw.WriteLine("==========================================================================
==============");
               sw.WriteLine("ClientCertificate Settings: ");
               sw.WriteLine("Certificate: " + ccrt.Certificate);
        sw.WriteLine("Cookie: " + ccrt.Cookie);
        sw.WriteLine("Flags: " + ccrt.Flags);
        sw.WriteLine("IsPresent: " + ccrt.IsPresent);
        sw.WriteLine("Issuer: " + ccrt.Issuer);
        sw.WriteLine("IsValid: " + ccrt.IsValid);
        sw.WriteLine("KeySize: " + ccrt.KeySize);
        sw.WriteLine("SecretKeySize: " + ccrt.SecretKeySize);
```

```
        sw.WriteLine("SerialNumber: " + ccrt.SerialNumber);
        sw.WriteLine("ServerIssuer: " + ccrt.ServerIssuer);
        sw.WriteLine("ServerSubject: " + ccrt.ServerSubject);
        sw.WriteLine("Subject: " + ccrt.Subject);
        sw.WriteLine("ValidFrom: " + ccrt.ValidFrom);
        sw.WriteLine("ValidUntil: " + ccrt.ValidUntil);
        sw.WriteLine("ToString: " + ccrt.ToString());
       }

       finally
       {
            // Close the stream to the file.
            sw.Close();
       }

}
}
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx.cs** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.aspx.cs** exactly.

5. In Notepad, click **File**, click **Save As** again. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp2** folder that was created in the previous procedure.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx.cs** and then click the **Save** button.
6. Exit Notepad.

Creating the Windows NT Token-based Application

Perform this procedure on the same computer where the removable media device is inserted. Only one file must be created for the Windows NT token-based application.

Create the Default.htm file

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.

3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<html>
<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">

<title ID=titletext>ADFS Token-based Application</title>
</head>

<body bgcolor=cccccc>
This is an ADFS token-based application.

</body>
</html>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **tokenapp** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.htm** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.htm** exactly.

5. Exit Notepad and WordPad, close Windows Explorer, and remove the removable media device for use in later procedures.

Configuring the Web Server

This section includes procedures for installing and configuring the ADFS-enabled applications on the Web server in the resource realm. Clients will use ADFS to authorize access to these applications.

Installing and Configuring a Claims-aware Application

This section describes the procedures that must be performed on the Web server to install and configure a sample ADFS-enabled claims-aware application, “Claimapp.”

Create the sampleapp Web site for the claims-aware application

On the Web server (<WebSvr>):

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. In Internet Information Services (IIS) Manager, expand the local computer node, right-click **Web Sites**, point to **New**, and select **Web Site**.
4. In the Welcome to the Web Site Creation Wizard click **Next**.
5. For **Description**, type **sampleapp** and click **Next**.
6. For **TCP Port this Web site should use**, type **8080**. Accept the defaults for the rest of the settings in this page and click **Next**.

   Note: Do not modify the values listed for **Enter the IP address to use for this Web site** ([All Unassigned]) and for **Host header for this Web site** (blank).
7. In the Web Site Home Directory page, click the **Browse** button. Expand the local system disk (C:). Click the **C:\Inetpub** folder to highlight it.
8. With the **C:\Inetpub** folder selected, click the **Make New Folder** button. Type **sampleapp** as the New Folder name and click **OK**.
9. In the Web Site Home Directory page, verify the path is **C:\Inetpub\sampleapp**, leave **Allow anonymous access to this Web site** selected, and click **Next**.
10. In the Web Site Access Permissions page, ensure that only the **Read** check box is selected, and click **Next**.
11. Click **Finish**.

Configure the sampleapp Web site and assign the server authentication certificate

On the Web server (<WebSvr>):

1. In **Internet Information Services (IIS) Manager**, under the **Web Sites** folder, right-click **sampleapp**, and then select **Properties**.
2. In the Web Site tab, in **the SSL port** text box, type **8081**.
3. Click the **ASP.NET** tab. For **ASP.NET version**, ensure that **2.0.50727** is selected. (If not, click the drop-down arrow for **ASP.NET version**, and click **2.0.50727**.) Click **Apply**.
4. Click the **Directory Security** tab and, in the **Authentication and access control** area, click **Edit**.
5. In the Authentication Methods interface, in the **Authenticated access** area, clear the check box for **Integrated Windows authentication** and click **OK**.
6. On the **Directory Security** tab, click **Server Certificate**.
7. In the Welcome to the Web Server Certificate Wizard, click **Next**.
8. In the Server Certificate page, select **Assign an existing certificate**, and then click **Next**.
9. In the Available Certificates page, click the **<WebSvrFQDN>** server authentication certificate to select it, and then click **Next**.
10. In the SSL Port page, type **8081** for the **SSL port this web site should use**, and then click **Next**.

11. In the Certificate Summary page, verify the details, and then click **Next**.
12. In the Completing the Web Server Certificate Wizard, click **Finish**.
13. Click **OK** to exit the sampleapp Properties page.
14. Under the **Web Sites** folder in the console tree, right-click **sampleapp**, point to **New**, and select **Virtual Directory**.
15. In the Welcome to the Virtual Directory Creation Wizard, click **Next**.
16. In the Virtual Directory Alias interface, for **Alias**, type **claimapp**, and then click **Next**.
17. In the Web Site Content Directory interface, click **Browse**, navigate to and expand the **Inetpub** folder on the local disk (C:) and click the **sampleapp** subfolder once to highlight it. Click the **Make New Folder** button. This creates a subfolder called New Folder beneath the sampleapp folder.
18. Right-click **New Folder**, select **Rename** from the menu, type the name **claimapp** (exactly as it appears here) and press the **Enter** key.

    Warning: Do not use capital letters in the **claimapp** folder name. If this folder name contains capital letters, users must also use capital letters when they type the address of the Web site.
19. With the new **claimapp** folder selected, click **OK**.
20. Verify that the **Path** specified in the Virtual Directory Creation Wizard is **C:\Inetpub\sampleapp\claimapp**, and then click **Next**.
21. In the **Virtual Directory Access Permissions** page, select both the **Read** and **Run scripts (such as ASP)** check boxes, and then click **Next**.
22. In the You have successfully completed the Virtual Directory Creation Wizard, click **Finish**.
23. In the **Internet Information Services (IIS) Manager** console tree, under **sampleapp** Web site, right-click the **claimapp** item, and then click **Properties**.
24. On the **Documents** tab, verify that **Default.aspx** is in the list of files displayed.

    Otherwise, if Default.aspx is not listed, click **Add**, type **Default.aspx**, click **OK**.
25. Click **OK** again to close the claimapp Properties interface.

The next procedure requires access to the removable media device used earlier to store the application files created for Claimapp.

Copy the claims-aware application (Claimapp) files to the Web server

On the Web server (<WebSvr>):

1. Insert the removable media device that contains the Claimapp and Claimapp2 files created earlier.
2. Click **Start** and select **My Computer**. Use Windows explorer to navigate to and double-click the **claimapp** folder on the removable disk. The three follows should be displayed in the claimapp folder:
   - Default.aspx
   - Web.config
   - Default.aspx.cs
3. Select all three files, click the **Edit** menu, and select **Copy** to copy the files to the Windows clipboard.

4. In Windows explorer, navigate to the local disk (C:), double-click the **Inetpub** folder, double-click the **sampleapp** subfolder, and double-click the **claimapp** subfolder.
5. Click the **Edit** menu and then select **Paste** to copy the three files from the Windows clipboard to the C:\Inetpub\sampleapp\claimapp folder.
6. Leave Windows explorer open for the next procedure.

Edit Claimapp for use in the ADFS environment

On the Web server (<WebSvr>):

1. With Windows explorer still open to the C:\Inetpub\sampleapp\claimapp folder from the previous procedure, right-click the **Web.config** file, click **Open**, click the **Select the program from a list** radio button and click **OK**. In the Open With interface, click **WordPad**, and then click **OK**.
2. Scroll down and locate the <websso> section of the file, and then find the <returnurl> line within that section. Between the left and right brackets, ensure that the URL is modified to point to the claimapp URL, using the fully qualified domain name (FQDN) of the Web server, as follows:

```
<returnurl>https://<WebSvrFQDN>:8081/claimapp/</returnurl>
```

3. In the <websso> section, locate the <fs> entry for the federation server. Between the left and right brackets, ensure that the URL is modified to point to the FQDN of the resource federation server URL, as follows:

```
<fs>https://<ResFedSvrFQDN>/adfs/fs/federationserverservice.asmx</fs>
```

4. Before exiting, ensure that every character of both URLs is typed correctly.
5. Click **File**, choose **Save**, and then exit WordPad and exit Windows explorer.

Installing and Configuring a Secondary Claims-aware Application

This section includes instructions for installing and configuring a second claims-aware application, “Claimapp2,” which will also be accessed by ADFS clients.

Create the sampleapp2 Web site for Claimapp2

On the Web server (<WebSvr>):

1. Switch to the **Internet Information Services (IIS) Manager** interface.
2. Expand the local computer node, right-click **Web Sites**, point to **New**, and select **Web Site**.
3. In the Welcome to the Web Site Creation Wizard click **Next**.
4. For **Description**, type **sampleapp2** and click **Next**.
5. For **TCP Port this Web site should use**, type **8082**. Accept the defaults for the rest of the settings in this page and click **Next**.

Note: Do not modify the values listed for **Enter the IP address to use for this Web site** ([All Unassigned]) and for **Host header for this Web site** (blank).

---

6. In the Web Site Home Directory page, click the **Browse** button. On the local disk (C:), navigate to and select the **C:\Inetpub** folder.

7. With the **C:\Inetpub** folder selected, click the **Make New Folder** button. Type **sampleapp2**, and press the **Enter** key.
8. With the **sampleapp2** folder selected, click **OK**.
9. In the Web Site Home Directory page, verify the path is **C:\Inetpub\sampleapp2**, leave **Allow anonymous access to this Web site** selected, and click **Next**. and click **Next**.
10. In the Web Site Access Permissions page, ensure that only the **Read** check box is selected, and click **Next**.
11. Click **Finish**.

Configure the sampleapp2 Web site and assign the server authentication certificate

On the Web server (<WebSvr>):

1. In the **Internet Information Services (IIS) Manager** interface, under the **Web Sites** node, right-click **sampleapp2**, and then select **Properties**.
2. Click the **ASP.NET** tab. On the **ASP.NET** tab, for **ASP.NET version**, ensure that **2.0.50727** is selected. (If not, click the drop-down arrow for **ASP.NET version**, and click **2.0.50727**.) Click **Apply**.
3. Click the **Directory Security** tab and, in the **Authentication and access control** area, click **Edit**.
4. In the Authentication Methods interface, clear the **Integrated Windows authentication** check box, and then click **OK**.
5. On the **Directory Security** tab, click **Server Certificate**.
6. In the Welcome to the Web Server Certificate Wizard, click **Next**.
7. In the Server Certificate page, click **Assign an existing certificate**, and then click **Next**.
8. In the Available Certificates page, click the **<WebSvrFQDN>** server authentication certificate to select it, and then click **Next**.
9. In the SSL Port page, type **8083** for the **SSL port this web site should use**, and then click **Next**.
10. In the Certificate Summary page, verify the details, and then click **Next**.
11. In the Completing the Web Server Certificate Wizard, click **Finish**.
12. Click **OK** to exit the sampleapp2 Properties page.
13. Under the Web Sites node in the console tree, right-click **sampleapp2**, point to **New**, and then click **Virtual Directory**.
14. In the Welcome to the Virtual Directory Creation Wizard, click **Next**.
15. In the Virtual Directory Alias page, for **Alias**, type **claimapp2**, and then click **Next**.
16. In the **Web Site Content Directory** page, click **Browse**, navigate to and select the **C:\Inetpub\sampleapp2** folder, click the **Make New Folder** button. This creates a subfolder called New Folder beneath the sampleapp2 folder.
17. Right-click **New Folder**, select **Rename** from the menu, type the name **claimapp2** (exactly as it appears here) and press the **Enter** key.

Warning: Do not use capital letters in the **claimapp2** folder name. If this folder name contains capital letters, users must also use capital letters when they type the address of the Web site.

18. With the new **claimapp2** folder selected, click **OK**.
19. Verify that the **Path** specified in the Virtual Directory Creation Wizard is **C:\Inetpub\sampleapp2\claimapp2**, and then click **Next**.
20. In the **Virtual Directory Access Permissions** page, select both the **Read** and **Run scripts (such as ASP)** check boxes, and then click **Next**.
21. In the You have successfully completed the Virtual Directory Creation Wizard, click **Finish**.
22. In the console tree, under the **sampleapp2** Web site, right-click the **claimapp2** folder, and then click **Properties**.
23. On the **Documents** tab, verify that **Default.aspx** is in the list of files displayed. Otherwise, if Default.aspx is not listed, click **Add**, type **Default.aspx**, click **OK**.
24. Click **OK** again to close the claimapp Properties interface.

Copy the claims-aware application (Claimapp2) files to the Web server

On the Web server (<WebSvr>):

1. Insert the removable media device that contains the Claimapp and Claimapp2 files created earlier.
2. Click **Start** and select **My Computer**. Use Windows explorer to navigate to and double-click the **claimapp2** folder on the removable disk. The three files should be displayed in the claimapp2 folder:
   - Default.aspx
   - Web.config
   - Default.aspx.cs
3. To select all three files, choose **Select All** on the **Edit** menu, click **Edit** again, and then select **Copy** to copy the files to the Windows clipboard.
4. In Windows explorer, navigate to the local disk (C:), double-click the **Inetpub** folder, double-click the **sampleapp2** subfolder, and double-click the **claimapp2** subfolder.
5. Click the **Edit** menu and then select **Paste** to copy the three files from the Windows clipboard to the C:\Inetpub\sampleapp2\claimapp2 folder.

Edit Claimapp2 for use in the ADFS environment

1. With Windows explorer still open to the C:\Inetpub\sampleapp2\claimapp2 folder from the previous procedure, right-click the **Web.config** file, click **Open With**, and double-click **WordPad**.
2. Locate the `<websso>` section of the file, and then find the `<returnurl>` line within that section. Between the left and right brackets, ensure that the URL is modified to point to the fully qualified domain name (FQDN) of the Web server and correct SSL port number, as follows:

```
<returnurl>https://<WebSvrFQDN>:8083/claimapp2/</returnurl>
```

3. In the <websso> section, locate the <path> entry under <cookies...>. Between the left and right brackets, ensure that the path points to claimapp2, as follows:

```
<path>/claimapp2</path>
```

4. In the <websso> section, locate the <fs> entry for the federation server. Between the left and right brackets, ensure that the URL points to the FQDN of the resource federation server URL, as follows:

```
<fs>https://<ResFedSvrFQDN>/adfs/fs/federationserverservice.asmx</fs>
```

5. In the <system.diagnostics> section, locate the <add name...> entry under <listeners>. Between the left and right brackets, ensure that the path for the claimapp2 log file points to c:\logdir\claimapp2.log, as follows:

```
<add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" initializeData="c:\logdir\claimapp2.log"
/>
```

6. Before exiting, ensure that every character in the modified settings is typed correctly.
7. Click **File**, choose **Save**, and then exit WordPad.

Installing and Configuring a Windows NT Token-based Application

In this example, the token-based application is hosted on its own Web site, so a new Web site must be created (as with the claims-aware applications).

Configure Web Sites for the Federation Service

On the Web server (<WebSvr>):

1. In the **Internet Information Services (IIS) Manager** console, under the local computer node, right-click **Web Sites**, and then click **Properties**.
2. Click the **ADFS Web Agent** tab.
3. For **Federation Service URL**, type the following:

   https://<ResFedSvrFQDN>/adfs/fs/FederationServerService.asmx

4. Verify that every character in the URL is typed correctly, and then click **OK**.

Create a Web site for the Windows NT token-based application (Tokenapp)

1. In the **Internet Information Services (IIS) Manager** console, under the local computer node, right-click **Web Sites**, click **New** and select **Web Site**.
2. In the Welcome to the Web Site Creation Wizard click **Next**.
3. For **Description**, type **tokenapp** and click **Next**.
4. For **TCP Port this Web site should use**, type **8090**. Accept the defaults for the rest of the settings in this page and click **Next**.

Note: Do not modify the values listed for **Enter the IP address to use for this Web site** ([All Unassigned]) and for **Host header for this Web site** (blank).

5. In the Web Site Home Directory page, click the **Browse** button. On the local disk (C:), navigate to and select the **C:\Inetpub** folder.
6. With the **C:\Inetpub** folder selected, click the **Make New Folder** button. Type **tokenapp**, and press the **Enter** key.
7. With the **tokenapp** folder selected, click **OK**.
8. In the Web Site Home Directory page, verify the path is **C:\Inetpub\tokenapp**, leave **Allow anonymous access to this Web site** selected, and click **Next**.
9. In the Web Site Access Permissions page, ensure that only the **Read** check box is selected, and click **Next**.
10. Click **Finish** to exit the Web Site Creation Wizard.
11. Under the **Web Sites** folder in the console tree, right-click the **tokenapp** Web site node, point to **New**, and then click **Virtual Directory**.
12. In the Welcome to the Virtual Directory Creation Wizard, click **Next**.
13. In the Virtual Directory Alias interface, for **Alias**, type **tokenapp**, and then click **Next**.
14. In the **Web Site Content Directory** interface, click **Browse**, navigate to and expand the **Inetpub** folder on the local disk (C:), click the **tokenapp** subfolder once to highlight it, and click **OK**.
15. Verify that the **Path** specified in the Virtual Directory Creation Wizard is **C:\Inetpub\tokenapp**, and then click **Next**.
16. In the **Virtual Directory Access Permissions** page, select both the **Read** and **Run scripts (such as ASP)** check boxes, and then click **Next**.
17. In the You have successfully completed the Virtual Directory Creation Wizard, click **Finish**.

Configure the Windows NT token-based application Web Site and assign the <WebSvr> server authentication certificate

On the Web server (<WebSvr>):

1. In the **Internet Information Services (IIS) Manager** console, under **Web Sites**, right-click the **tokenapp** Web site node, and then click **Properties**.

Warning: To open the tokenapp Web site properties page, ensure that this action is performed on the tokenapp Web site that exists in the console tree one level below the Web Sites node. Do not right-click the tokenapp virtual directory that exists in the console tree one level below the tokenapp Web site.

2. Click the **Directory Security** tab.
3. On the **Directory Security** tab, in the **Secure communications** area, click the **Server Certificate** button.
4. In the Welcome to the Web Server Certificate Wizard, click **Next**.
5. In the Server Certificate page, click **Assign an existing certificate**, and then click **Next**.
6. In the Available Certificates page, click the **<WebSvrFQDN>** server authentication certificate to select it, and then click **Next**.

7. In the SSL Port page, for the **SSL port this web site should use**, type **8091** and then click **Next**.
8. In the Certificate Summary page, verify the details, and then click **Next**.
9. In the Completing the Web Server Certificate Wizard, click **Finish**.
10. In the tokenapp Properties page, click the **ASP.NET** tab.
11. On the **ASP.NET** tab, for **ASP.NET version**, ensure that 2.0.50727 is selected. (If not, click the drop-down arrow for **ASP.NET version**, and click **2.0.50727**.) Click **Apply**.
12. Click the **ADFS Web Agent** tab.
13. Select the check box next to **Enable the ADFS Web Agent for Windows NT token-based applications**. Modify the **Return URL** as follows:

    https://<WebSvrFQDN>:8091/tokenapp/

14. Verify that ever character in the URL is typed correctly, and then click **OK**. If prompted, "The current cookie path does not match a prefix of the application path and/or the Return URL" click **Yes** to continue.
15. If an ADFS Web Agent pop-up window is displayed indicating "You are about to change the authentication method for this resource, which may break other applications. If you want to continue, press OK," click **OK**.
16. Click **OK** to exit the tokenapp Properties interface.

Copy the Windows NT token-based application file to the Web server

On the Web server (<WebSvr>):

1. Insert the removable media device that contains the application files created earlier.
2. Click **Start** and select **My Computer**. Use Windows explorer to navigate to and double-click the **tokenapp** folder on the removable disk. The following file should be displayed in \tokenapp:
   - Default.htm
3. Select the **Default.htm** file, click the **Edit** menu, and select **Copy** to copy the files to the Windows clipboard.
4. In Windows explorer, navigate to the local disk (C:), double-click the **Inetpub** folder, and double-click the **tokenapp** subfolder.
5. Click the **Edit** menu and then select **Paste** to copy the file from the Windows clipboard to the C:\Inetpub\tokenapp folder and close Windows explorer.

Configuring Debug Logging on the Web Server

Debug logging can be enabled for the Web server components described here.

- The ADFS Web Agent running on ADFS Web servers has two components:
  - ADFS Token Authentication service (ifssvc.exe), which validates incoming tokens and cookies. Debug logging creates **ifssvc.log** in the **C:\ADFS\Logs** folder.
  - ADFS Web Agent Internet Server Application Programming Interface (ISAPI) extension (ifsext.dll), which handles the protocols that are used by ADFS to authenticate requests; and the ADFS Web Agent ISAPI filter (ifsfilt.dll), which assists the extension and enables

user name logging in the Internet Information Services (IIS) log files. Debug logging creates the **ifsext_StsAppPool1.log** and **ifsfilt_StsAppPool1.log**, respectively in the **C:\ADFS\Logs** folder.

- In addition, the ADFS Web Agent authentication package (ifsAp.dll) is used by Windows NT token-based applications for generating tokens when Service-for-User (S4U) is not available. Debug logging creates **ifsap.log** in the **C:\ADFS\Logs** folder.

Enable debug logging for each of these components in the registry on the Web server.

Enable debug logging for the ADFS ISAPI extension and filter

On the Web server (<WebSvr>):

1. Click **Start**, click **Run**, type **Regedit**, and click **OK**.
2. In Registry Editor, expand the nodes in the console tree to navigate to:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ADFS\WebServerAgent
3. Right-click **WebServerAgent**, click **New**, and then select **DWORD Value**.
4. In the new value file name box, type **DebugPrintLevel**, and then press **Enter**.
5. Double-click the new entry and then, in **Value data**, type **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295).

   Note: The value “FFFFFFFF” is not case-sensitive.
6. Leave Registry Editor open for the next procedure.

Enable debug logging for the ADFS Web Agent authentication package (for Windows NT token-based applications)

On the Web server (<WebSvr>):

1. In Registry Editor, navigate to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\WebSso\Parameters
2. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
3. In the new value file name box, type **DebugLevel**, and then press **Enter**.
4. Double-click the new entry and then, in **Value data**, **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295).

   Note: The value “FFFFFFFF” is not case-sensitive.
5. Leave Registry Editor open for the next procedure.

Enable debug logging for the ADFS Token Authentication service

On the Web server (<WebSvr>):

1. In Registry Editor, navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ifssvc\Parameters

2. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
3. In the new value file name box, type **DebugPrintLevel**, and then press **Enter**.
4. Double-click the new entry and then, in **Value data**, **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295)..

   Note: The value “FFFFFFFF” is not case-sensitive.

5. Leave Registry Editor open for another procedure to be completed later.

Configuring Event Logging on the Web Server

Events logged on Web servers that are running an ADFS Web Agent are configured according to the application type that the enabled agent supports. Event logging is configured differently for Windows NT token-based applications and claims-aware applications.

Event logging for claims-aware applications

On Web servers that are running the ADFS Web Agent for claims-aware applications, event logging for these applications is set in the Web.config file for the ADFS-enabled application. Use the following procedure to specify the level of events to be logged for claims-aware applications in the Application event log on the Web server. Set event logging for claims-aware applications in the Web.config file for the application.

The procedure in this section describes how to use a summation value of **247** to enable all of the following debug logging levels in the Web.config file, and is recommended for troubleshooting ADFS problems only:

- **DetailedFailure (0x80)**: A failure audit event that provides detailed information about each token involved in the transaction, including claims information.
- **DetailedSuccess (0x40)**: A success audit event that provides detailed information about each token involved in the transaction, including claims information.
- **Error (0x01)**: Provides information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **FailureAudit (0x20)**: Indicates a security event that occurs when an audited access attempt fails; for example, a failed attempt to open a file.
- **Info (0x04)**: Provides information about a significant, successful operation.
- **SuccessAudit (0x10)**: Indicates an audited security event that when an audited access attempt is successful; for example, a successful logon attempt.
- **Warning (0x02)**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Everything (0xf7** (or **247** in decimal)**)**: Enables all logging levels.

Note: To reduce the number of events generated by ADFS, change this value to a lesser level of debug logging after reaching a resolution following any troubleshooting steps.

Verify that event logging for the claims-aware application is configured in the Web.config file

On the Web server (<WebSvr>):

1. From the **Start** menu click **My Computer**.
2. In Windows explorer, navigate to the Web.config file in the folder that stores the claims-aware application (**C:\Inetpub\sampleapp\claimapp**). Right-click the **Web.config** file, select **Open With**, and select **WordPad** from the list of applications.

   Note: If the **Open With** command is not available on the menu, exit the menu, and double-click the Web.config file. In the interface displayed, select the radio button to **Select the program from a list**, and click **OK**. In the **Open With** interface select **WordPad** from the list of applications, and click **OK**.
3. In WordPad, scroll down and locate the <websso> section of the file.
4. Verify or edit the <auditlevel> entry in the <websso> section to appear as follows:

```
<auditlevel>247</auditlevel>
```

5. Click **File**, click **Save**, close WordPad, and exit Windows explorer.

Repeat this procedure for the secondary claims-aware application, sampleapp2 by verifying the same <auditlevel> entry exisis in the <websso> section of the C:\Inetpub\sampleapp2\claimapp2\Web.config file.

Event logging for Windows NT token-based applications

On Web servers that are running the ADFS Web Agent for Windows NT token-based applications, event logging for these applications is set in the registry on the Web server. Use the following procedure to specify the types of events to be logged for Windows NT token-based applications on the Web server.

The procedure in this section describes how to use a summation value of **0f** to enable all of the following debug logging levels, and is recommended for troubleshooting only:

- Warning: **0x01**
- Information: **0x02**
- Success: **0x04**
- Failure: **0x08**
- (All of the above: **0f**)

Note: To reduce the number of events generated by ADFS, change this value to a lesser level of debug logging when after reaching a resolution following any troubleshooting steps.

Configure event logging for the Windows NT token-based application

On the Web server (<WebSvr>):

1. Switch to the Registry Editor.
2. In Registry Editor, navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ifssvc\Parameters

3. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
4. In the new value file name box, type **ADFSEvent**, and then press **Enter**.
5. Double-click the new entry and then, in **Value data**, type **0f**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0x00000000f (15).
6. Exit Registry Editor.

Configuring Auditing, Event Logging, and Debug Logging on the Federation Servers

This section includes procedures for the following:

- Configure federation servers to record auditing of ADFS events to the security log
- Configure event logging on the federation servers
- Configure debug logging on the federation servers
- Enable ADFS authentication package debug logging on the account federation server

The first three procedures should be performed on both the research federation server and the account federation server in the Federated Web SSO scenario. The fourth procedure is performed on the account federation server only.

Configuring ADFS Computers to Record Auditing of ADFS Events to the Security Log

All ADFS-related audits that are made specifically to the security log are considered by the system to be object access–type audits, which by default are ignored by the system. For this reason, to ensure that ADFS-related audits (specifically Success Audits and Failure Audits) appear in the Security log, an administrator must manually configure the Local Security Policy, using the procedure here.

Apply the steps in this procedure to each of the ADFS computers (including the federation servers and the Web server) before enabling success or failure auditing in the Trust Policy properties of the ADFS management console. This allows the Federation Service to log either success or failure errors.

This procedure has no effect on the events that ADFS writes to the application log.

Configure the Windows Security Log to support auditing of ADFS events

Perform this procedure on the resource federation server (<ResFedSvr>), the account federation server (<AcctFedSvr>), and the Web server (<WebSvr>).

1. Click **Start**, point to **Administrative Tools**, and then click **Local Security Policy**.
2. Double-click **Local Policies**, and then click **Audit Policy**.
3. In the details pane, double-click **Audit object access**.

4. On the Audit object access Properties page, select both **Success** and **Failure**, and then click **OK**.
5. Close the Local Security Settings console.
6. Click **Start** and then click **Command Prompt**. At the command prompt, type **gpupdate /force** and then press **Enter** to immediately refresh the local policy.
7. Exit the command prompt.

After performing the previous procedure to enable auditing on both federation servers, configure event logging on each federation server.

Configuring Event Logging on the Federation Servers

Servers that are running the Federation Service component of ADFS log ADFS Federation Service events in the Application event log. These events report information about the operation of the components of the local organization and partner organizations that are covered by a trust policy.

Note: ADFS also can log debug information. Debug logs are located in **C:\ADFS\logs**.

The following types of events are available and enabled by default in ADFS:

- **Error**: Information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **Information**: Information about a significant, successful operation.
- **Success audit**: Indicates an audited security event that when an audited access attempt is successful; for example, a successful logon attempt.
- **Detailed success**: A success audit event with detailed information about each token involved in the transaction, including claims information.
- **Warning**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Failure audit**: Indicates a security event that occurs when an audited access attempt fails; for example, an inbound token was not valid.
- **Detailed failure**: A failure audit event with detailed information about each token involved in the transaction, including claims information.

Note: Audit object access must be turned on for success or failure to allow the Federation Service to log errors.

To complete this procedure, the logged-on account must be a member of the Administrators group on the local computer.

Verify the types of events logged by ADFS

Perform this procedure on both the resource federation server (<ResFedSvr>) and the account federation server (<AcctFedSvr>).

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.
2. Expand the **Federation Services** node, right-click the **Trust Policy** node, and then click **Properties**.

3. Use the right arrow button to scroll to the **Event Log** tab.
4. For **Event log level**, verify that all seven of the event log types are selected, and then click **OK**.

After performing the previous procedure to verify event logging on both federation servers, configure debug logging on each federation server.

Configuring Debug Logging on the Federation Servers

Event logs are generally descriptive, intended to help the administrator understand what is happening. However, the default events do not always provide the level of detail that is needed for effective troubleshooting. In this case, configure ADFS debug logging, as described in the procedures here.

If debug logging is enabled on a federation server, the log filename in the C:\ADFS\logs folder has the following format:

adfsyyyymmdd-hhmmss.log

In the name of the file, the number following "adfs" represents the date of the log and the number following the dash (-) represents the beginning time of the log.

Depending on the level of debug logging enabled, the following tags are displayed in debug logs:

- **[INFO]** - Displays information about events, such as redirects with protocol Uniform Resource Locators (URLs), token validations, or claim mappings.
- **[VERBOSE]** - Displays information about events, such as sign-in requests, responses, token contents, Web method calls, and security identifier (SID) information.
- **[ERROR]** - Displays events for significant problems in the debug log.
- **[WARNING]** - Displays events, which are not necessarily significant but that may cause future problems.
- **[EVENTLOG]** - Displays all ADFS events.

Although all information in the log file could be useful, an administrator can look at the lines that are tagged **[ERROR]** and **[WARNING]** first to quickly assess the problem.

On federation servers, use the Windows interface to enable debug logging and set levels to increase the detail of feedback in the logs.

Set ADFS debug levels on federation servers

Perform the following procedure on both the account federation server (<AcctFedSvr>) and resource federation server (<ResFedSvr>).

1. If the ADFS management console is not already open, click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**.
2. Right-click **Federation Service** and then click **Properties**.
3. On the **Troubleshooting** tab, select the check box for each of the eight debug levels, and then click **OK**.

After performing the previous procedure to set debug levels on both federation servers, configure authentication package debug logging on the account federation server.

Enabling ADFS Authentication Package Debug Logging on the Account Federation Server

The account federation server uses the ADFS authentication package (ifsAp.dll) for mapping client certificates.

Enable debug logging for the ADFS authentication package on an account federation server

On the account federation server (<AcctFedSvr>):

1. Click **Start**, click **Run**, type **Regedit**, and click **OK**.
2. Navigate to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\WebSSO\Parameters
3. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
4. In the new value file name box, type **DebugLevel**, and then press **Enter**.
5. Double-click the new entry and then, in **Value data**, type **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295)..

   Note: The value “FFFFFFFF” is not case-sensitive.
6. Exit Registry Editor.

Configuring Web Error Reporting on the Federation Servers

CustomErrors is an ASP.NET element that provides information about custom error messages for an ASP.NET application. Setting the customErrors mode attribute to “Off” specifies that custom errors are disabled. This results in better error reporting by ADFS.

Configure Web error reporting on the federation servers

Perform the following procedure on both the account federation server (<AcctFedSvr>) and resource federation server (<ResFedSvr>).

1. Click **Start**, click **My Computer**, and navigate to the **Web.config** file located in the **C:\ADFS\sts** folder in Windows Explorer.
2. Right-click the **Web.config** file, click **Open**, click the **Select the program from a list** radio button and click **OK**. In the Open With interface, click **WordPad**, and then click **OK**.
3. With the Web.config file open in WordPad, scroll down to the <system.web> section. Under <system.web>, insert a blank line and type the following text on that line, (preceded by four spaces for text alignment purposes only):

   ```
       <customErrors mode=”Off” />
   ```
4. After verifying the text is typed correctly, click **File**, choose **Save**, exit **WordPad** and close Windows explorer.

Configuring the Federation Service on the Federation Servers

For ADFS authorization methods to be invoked by a Web application, extensive configuration is required on the federation server in the resource realm and on the federation server in the account realm. This section describes in detail how to configure the federation servers in a Federated Web SSO scenario for the sample applications created previously.

> **Warning:** Where text strings are required in the configuration, ensure that the text is typed exactly as described in these procedures. A single missing slash ('/') in a text box or other typographical error can render ADFS non-functional.

Resource Partner: Configuring the Federation Service on the Resource Federation Server

This section includes procedures for performing the following tasks on the resource federation server:

- Configure the federation service trust policy
- Create group claims for the claims-aware applications and the Windows NT token-based application
- Add a resource group to the Windows NT token-based application claim
- Add an Active Directory account store
- Add the claims-aware applications and the Windows NT token-based application
- Enable the claims-aware application claim and the Windows NT token-based application claim
- Add and configure an account partner
- Create incoming group claim mappings for the claims-aware applications and for the Windows NT token-based application

To perform these procedures, an authorized administrator must be logged on to the resource federation server using an account that is a member of the Domain Admins group.

> **Note:** To determine current logon context, press **CTRL+ALT+DEL** to view logon information. Then click **Cancel** to return to the Windows desktop.

Configure the trust policy

On the resource federation server (<ResFedSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. If the ADFS management console is not already open, click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**. The ADFS management console appears.
3. In the console tree, expand the **Federation Service** node by clicking the plus sign (**+**) adjacent to **Federation Service**, right-click **Trust Policy**, and then click **Properties**.
4. On the General tab, in the **Federation Service URI** text box, replace **urn:federation:myOrganization** with **urn:federation:<ResourceDomain>>**, using all upper case letters for <ResourceDomain>.

Warning: This value is case-sensitive and must match the value typed in the Resource Partner properties on the account federation server. For best results, use all lower case letters for <ResourceDomain>.

5. In the **Federation Service endpoint URL** text box, replace **https://<ResFedSvr>/adfs/ls/** with **https://<ResFedSvrFQDN>/adfs/ls/**.
6. Verify that every character in the URL is typed correctly before proceeding to the next step.
7. Click the **Display Name** tab. In the **Display name for this trust policy** field, type the name of the resource realm organization (**<ResourceDomain>**). This name must be typed using the same casing wherever referenced in the ADFS configuration. For best results, use all lower case. Click **OK**.

Note: Except when instructed otherwise throughout these procedures, leave the ADFS management console open on the desktop.

Create a group claim for the claims-aware applications

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, expand **Trust Policy**, expand **My Organization**, right-click **Organization Claims**, point to **New**, and then select **Organization Claim**.
2. In the Create a New Organization Claim interface, in **Claim name**, type **<AccountDomain> ClaimApp Claim**.
3. Ensure that **Group claim** is selected and click **OK**.

Create a group claim for the Windows NT token-based application

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Organization Claims**, point to **New**, and then select **Organization Claim**.
2. In the **Create a New Organization Claim** interface, in **Claim name**, type **<AccountDomain> TokenApp Claim**.

   Ensure that **Group claim** is selected and click **OK**.

Add a resource group to the Windows NT token-based application claim

On the federation server (<ResFedSvr >):

4. In the ADFS management console, under the **My Organization** node, click **Organization Claims**.
5. In the details pane, right-click **<AccountDomain> TokenApp Claim** and select **Properties**.
6. In the Group Claim Properties interface, click the **Resource Group** tab.
7. Select the check box for **Map this claim to the following resource group**. Click the "**. . .**" button to the right of the text box.
8. In the Select Group interface, in the **Enter the object name to select** box, type **<AcctTokenAppUsers>**, and click **OK**.

Note: The object name is not case-sensitive.

9. The Group field in the Group Claim Properties interface is populated with the UPN name **<AcctTokenAppUsers>@<ResDomainFQDN>**.
10. Click **OK** again.

Add an Active Directory account store

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Account Stores**, point to **New**, and then click **Account Store**.
2. In the Welcome to the Add Account Store Wizard, click **Next**.
3. In the Account Store Type page, ensure that **Active Directory** is selected, and then click **Next**.
4. In the Enable this Account Store page, ensure that the **Enable this account store** check box is selected, and then click **Next**.
5. In the Completing the Add Account Store Wizard, click **Finish**.

Note: Sometimes it takes a few moments for the new account store to show up in the management console. If the account store does not appear right away, proceed to Step 6 and then repeat this procedure to add an Active Directory account store.

6. Click **File** and then click **Exit** to close the ADFS management console.

Add the claims-aware application

On the resource federation server (<ResFedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Federation Services**. The ADFS management console appears.
2. In the ADFS management console expand **Federation Service**, expand **Trust Policy**, expand **My Organization**, right-click **Applications**, point to **New**, and then select **Application**.
3. In the Welcome to the Add Application Wizard, click **Next**.
4. In the Application Type page, ensure that **Claims-aware application** is selected and click **Next**.
5. In the Application Details page, in **Application display name**, type **Claimapp**. In **Application URL**, type **https://<WebSvrFQDN>:8081/claimapp/**.

Note: The reference to **8081** in the **Application URL** is necessary to route SSL traffic to port 8081 because the default Web site is using the default SSL port (443).

6. Verify that every character in the URL is typed correctly, and then click **Next**.
7. In the Accepted Identity Claims page, select the **User principal name (UPN)** check box and click **Next**.
8. In the Enable this Application page, ensure that the **Enable this application** check box is selected, and then click **Next**.
9. In the Completing the Add Application Wizard, click **Finish**.

Add a secondary claims-aware application

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Applications**, point to **New**, and then select **Application**.
2. In the Welcome to the Add Application Wizard, click **Next**.
3. In the Application Type page, ensure that **Claims-aware application** is selected and click **Next**.
4. In the Application Details page, in **Application display name**, type **Claimapp2**. In **Application URL**, type **https://<WebSvrFQDN>:8083/claimapp2/**.

   Note: The reference to **8083** in the **Application URL** is necessary to route SSL traffic to port 8083 because the default Web site is using the default SSL port (443).

5. Verify that every character in the URL is typed correctly, and then click **Next**.
6. In the Accepted Identity Claims page, select the **User principal name (UPN)** check box and click **Next**.
7. In the Enable this Application page, ensure that the **Enable this application** check box is selected, and then click **Next**.
8. In the Completing the Add Application Wizard, click **Finish**.

Add a Windows NT token-based application

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Applications**, point to **New**, and then select **Application**.
2. In the Welcome to the Add Application Wizard, click **Next**.
3. In the Application Type page, select **Windows NT token-based application** and click **Next**.
4. In the Application Details page, in **Application display name**, type **TokenApp**. In **Application URL**, type **https://<WebSvrFQDN>:8091/tokenapp/**.
5. Verify that every character in the URL is typed correctly, and then click **Next**.
6. In the Accepted Identity Claims page, select the **User principal name (UPN)** check box and click **Next**.
7. In the Enable this Application page, ensure that the **Enable this application** check box is selected, and then click **Next**.
8. In the Completing the Add Application Wizard, click **Finish**.
9. Close the ADFS management console.

Enable the <AccountDomain> ClaimApp Claim for both claims-aware applications

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **Applications**, click **Claimapp**.
2. In the details pane, right-click the **<AccountDomain> ClaimApp Claim** group claim, and then select **Enable**.

3. Under **Applications**, click **Claimapp2**.
4. In the details pane, right-click the **<AccountDomain> ClaimApp Claim** group claim, and then select **Enable**.

Enable the <AccountDomain> TokenApp Claim

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **Applications**, click **TokenApp**.
2. In the details pane, right-click the **<AccountDomain> TokenApp Claim** group claim, and then select **Enable**.

Add and configure an account partner

On the resource federation server (<ResFedSvr>):

1. Insert the removable media device containing the <AcctFedSvr>_ts.cer file created earlier.
2. In the ADFS management console, under **Partner Organizations**, right-click **Account Partners**, point to **New**, and then select **Account Partner**.
3. In the Welcome to the Add Account Partner Wizard, click **Next**.
4. In the Import Policy File page, ensure that **No** is selected, and then click **Next**.
5. In the Account Partner Details page, in **Display name**, type **<AccountDomain>**.. This name must be typed using the same casing wherever referenced in the ADFS configuration. For best results, use all lower case.
6. In **Federation Service URI**, type **urn:federation:<AccountDomain>**, using all upper case letters for the <AccountDomain> name.

Warning: This value is case-sensitive and must match the value typed in the Trust Policy properties on the account federation server. For best results, use all lower-case when typing <AccountDomain>.

---

7. In **Federation Service endpoint URL**, type **https://<AcctFedSvrFQDN>/adfs/ls/**, and then click **Next**.
8. In the Account Partner Verification Certificate page, click **Browse**, click **My Computer**, and navigate to and double-click the removable media disk drive letter. Locate and click once to highlight the **AcctFedSvr>_ts.cer** file.
9. In the **File name** text box, type the UNC path to the account federation server's administrative C$ share and the name of the token-signing certificate, as follows:

   \\<AcctFedSvrFQDN>\c$\<AcctFedSvr>_ts.cer

Note: If logged on properly as an authorized member of the Domain Admins group, no prompt is generated here for a username and password for the administrative share. If prompted, input **<AccountDomain>\Administrator** as username and type the appropriate password for that domain account.

---

10. Click **Open.** Verify that the path and file name are typed correctly for the verification certificate, and then click **Next**.
11. In the Federation Scenario page, select **Federated Web SSO**, and then click **Next**.

12. In the Account Partner Identity Claims page, select the **UPN Claim** check box is selected, and then click **Next**.
13. In the Accepted UPN Suffixes page, in the text box beneath **Add a new suffix**, type **<AcctDomainFQDN>**, click **Add**, and then click **Next**.
14. In the Enable this Account Partner page, ensure that the **Enable this account partner** check box is selected, and then click **Next**.
15. In the Completing the Add Account Partner Wizard, click **Finish**.
16. Click **File** and then click **Exit** to close the ADFS management console.
17. Remove the removable media device from the computer.

Create an incoming group claim mapping for the claims-aware application

On the resource federation server (<ResFedSvr>):

1. In the ADFS management console, under **Account Partners,** right-click **<AccountDomain>**, point to **New**, and then select **Incoming Group Claim Mapping**.
2. In the Create a New Incoming Group Claim Mapping interface, in **Incoming group claim name**, type **ClaimAppMapping** exactly as it appears here.

   Warning: This value is case-sensitive. It must match exactly with the value that is specified in the outgoing group claim mapping in the account partner organization.
3. In **Organization group claim** list box, ensure that the **<AccountDomain> ClaimApp Claim** group claim is selected, and then click **OK**.

Create an incoming group claim mapping for the Windows NT token-based application

On the resource federation server (<ResFedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. Expand **Federation Service**, expand **Trust Policy**, expand **Partner Organizations**, expand **Account Partners,** right-click **<AccountDomain>**, point to **New**, and then select **Incoming Group Claim Mapping**.
3. In the Create a New Incoming Group Claim Mapping interface, in **Incoming group claim name**, type **TokenAppMapping** exactly as it appears here.

   Warning: This value is case-sensitive. It must match exactly with the value that is specified in the outgoing group claim mapping on the account federation server in the account partner organization.
4. In **Organization group claim** list box, click the drop-down arrow, select the **<AccountDomain> TokenApp Claim** group claim, and then click **OK**.
5. Click **File** and then click **Exit** to close the ADFS management console.

Account Partner: Configuring the Federation Service on the Account Federation Server

This section includes the following procedures:

- Configure the trust policy

- Create a group claim for the claims-aware application
- Create a group claim for the Windows NT token-based application
- Add and configure an Active Directory account store
- Add and configure a resource partner

To perform these procedures, an authorized administrator must be logged on to the account federation server using an account that is a member of the Domain Admins group.

Configure the trust policy

On the account federation server (<AcctFedSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Close any open windows on the desktop. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
3. In the console tree, expand **Federation Service**, right-click **Trust Policy**, and then select **Properties**.
4. On the **General** tab, in **Federation Service URI**, replace **urn:federation:myOrganization** with **urn:federation:<AccountDomain>** (type this text exactly as it appears here).

   Warning: This value is case-sensitive and must match the value typed in the Account Partner properties on the resource federation server. For best results, use all lower case letters.

5. In **Federation Service endpoint URL**, replace **https://<AcctFedSvr>/adfs/ls/** with **https://<AcctFedSvrFQDN>/adfs/ls/**. Verify that every character in the URL is typed correctly before proceeding to the next step.
6. Click the **Display Name** tab. For **Display name for this trust policy**, type **<AccountDomain>**. This name must be typed using the same casing wherever referenced in the ADFS configuration. For best results, use all lower case.
7. Click **OK**.

Create a group claim for the claims-aware applications

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, under **Federation Service**, expand **Trust Policy**, and then expand **My Organization**.
2. Right-click **Organization Claims**, point to **New**, and then select **Organization Claim**.
3. In the Create a New Organization Claim interface, in **Claim name**, type **<ResourceDomain> ClaimApp Claim**.
4. Ensure that **Group claim** is selected, and then click **OK**.

Create a group claim for the token-based application

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Organization Claims**, point to **New**, and then select **Organization Claim**.

2. In the Create a New Organization Claim interface, in **Claim name**, type **<ResourceDomain> TokenApp Claim**.
3. Ensure that **Group claim** is selected, and then click **OK**.

Add an Active Directory account store

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, under **My Organization**, right-click **Account Stores**, point to **New**, and then select **Account Store**.
2. On the Welcome to the Add Account Store Wizard, click **Next**.
3. On the Account Store Type page, ensure that **Active Directory** is selected, and then click **Next**.

Note: There can be only one Active Directory store that is associated with a Federation Service. If the Active Directory option is not available, it is because an Active Directory store has already been created for this Federation Service.

4. On the Enable this Account Store page, ensure that the **Enable this account store** check box is selected, and then click **Next**.
5. On the Completing the Add Account Store Wizard, click **Finish**.

Note: Sometimes it takes a few moments for the new account store to show up in the management console. If the account store does not appear right away, proceed to Step 6 and then repeat this procedure to add an Active Directory account store.

6. Click **File** and then click **Exit** to close the ADFS management console.

Map a global group to the group claim for the claims-aware application

On the account federation server (<AcctFedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. Expand **Federation Service**, expand **Trust Policy**, expand **My Organization**, expand **Account Stores**, right-click **Active Directory**, point to **New**, and then select **Group Claim Extraction**.

Note: If the Active Directory account store does not appear in the ADFS management console, repeat the earlier procedure **To add an Active Directory account store**.

3. In the Create a New Group Claim Extraction interface and click the **Add** button.
4. In the **Enter the object names to select box**, type **<ResClaimAppUsers>**, and then click **OK**.

Note: The object name is not case-sensitive.

5. Ensure that the appropriate security group is displayed (i.e., **<ResClaimAppUsers>@<AcctDomainFQDN>**) and that **Map to this Organization Claim** menu displays **<ResourceDomain> ClaimApp Claim**, and then click **OK**.

Map a global group to the group claim for the token-based application

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, under **My Organization**, expand **Account Stores**. The **Active Directory** account store should be displayed.

   Note: If the Active Directory account store does not appear in the ADFS management console, repeat the earlier procedure **To add an Active Directory account store**.

2. Right-click **Active Directory**, point to **New**, and then select **Group Claim Extraction**.
3. In the Create a New Group Claim Extraction interface, click **Add**.
4. In the **Enter the object names to select** box, type **<ResTokenAppUsers>**, and then click **OK**.

   Note: The object name is not case-sensitive.

5. Ensure that the appropriate security group is displayed (i.e., **<ResTokenAppUsers>@<AcctDomainFQDN>**).
6. In the **Map to this Organization Claim** drop-down list, select **<ResourceDomain> TokenApp Claim**, and then click **OK**.

Add a resource partner

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, under **Trust Policy**, expand **Partner Organizations**.
2. Right-click **Resource Partners**, point to **New**, and then select **Resource Partner**.
3. On the Welcome to the Add Resource Partner Wizard, click **Next**.
4. On the Import Policy File page, ensure that **No** is selected, and then click **Next**.
5. On the Resource Partner Details page, in **Display name**, replace the text with resource realm organization name (**<ResourceDomain>**), using all upper case letters for <ResourceDomain>.
6. In **Federation Service URI**, type **urn:federation:<ResourceDomain>**.

   Warning: This value is case-sensitive and must match the value typed in the Trust Policy properties on the resource federation server. For best results, use all lower case letters for **<ResourceDomain>**.

7. In **Federation Service endpoint URL**, type **https://<ResFedSvrFQDN>/adfs/ls/**, and then click **Next**.
8. On the Federation Scenario page, ensure that **Federated Web SSO**, is selected and then click **Next**.
9. On the Resource Partner Identity Claims page, select the **UPN Claim** check box, and then click **Next**.
10. On the Select UPN Suffix page, select the radio button for **Replace all UPN suffixes with the following**, type **<AcctDomainFQDN>** in the text box, and then click **Next**.
11. On the Enable this Resource Partner page, ensure that the **Enable this resource partner** check box is selected, and then click **Next**.
12. On the Completing the Add Resource Partner Wizard, click **Finish**.

13. Click **File** and then click **Exit** to close the ADFS management console.

Create an outgoing group claim mapping for the claims-aware application

On the account federation server (<AcctFedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. Expand **Federation Service**, expand **Trust Policy**, expand **Partner Organizations**, expand **Resource Partners,** right-click the resource realm organization name (**<ResourceDomain>**), point to **New**, and then select **Outgoing Group Claim Mapping**.

   Note: If the resource partner (**<ResourceDomain>**) does not appear as a Resource Partner, repeat the procedure **To add a resource partner**.
3. In the Create a New Outgoing Group Claim Mapping interface, in **Organization group claims**, ensure that **<ResourceDomain> ClaimApp Claim** is selected from the drop-down list. For **Outgoing group claim name**, type **ClaimAppMapping** exactly as it appears here, and then click **OK**.

   Warning: This value is case-sensitive. It must match exactly with the value that is specified in the incoming group claim mapping in the resource partner organization.

Create an outgoing group claim mapping for the token-based application

On the account federation server (<AcctFedSvr>):

1. In the ADFS management console, if not already expanded, expand **Federation Service**, expand **Trust Policy**, expand **Partner Organizations**, and then expand **Resource Partners**.
2. Right-click the resource realm organization name (**<ResourceDomain>**), point to **New**, and then select **Outgoing Group Claim Mapping**.

   Note: If the resource partner (**<ResourceDomain>**) does not appear as a Resource Partner, repeat the procedure **To add a resource partner**.
3. In the Create a New Outgoing Group Claim Mapping interface, in **Organization group claims**, select **<ResourceDomain> TokenApp Claim** from the drop-down list. For **Outgoing group claim name**, type **TokenAppMapping** exactly as it appears here, and then click **OK**.

   Warning: This value is case-sensitive. It must exactly match the the value that is specified in the incoming group claim mapping in the resource partner organization.

Apply ADFS FIPS Update

A conflict exists with the original installation of ADFS and the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** security policy setting that is required in the Evaluated Configuration of Windows Server 2003 with SP2. When the FIPS policy setting is enabled, any attempt to access an ADFS Web site can result in the following exception:

InvalidOperationException: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

To mitigate this issue, Microsoft has made a patch available (KB935449) that can be downloaded from http://support.microsoft.com/kb/935449.

Download and install this patch on all federation servers (including federation service proxies) and ADFS Web servers. Then follow the procedures here to make the necessary changes to the Web.config files and Web browser settings.

Updating Existing Web files

As described in the procedures here, any instance of debug="true" must be removed from Web.config files and *.aspx files on the ADFS computers.

Note: In the <compilation> section of the Web.config, the default debug setting is false. If no debug= instance appears in the compilation section of the Web.config, the file does not need modification because it automatically defaults to false.

Modify debug setting on federation servers

1. On each federation server:Open the C:\ADFS\sts\Web.config file in a text editor such as Notepad or WordPad, and scroll down to the <compilation> section. Look for debug="true." If it exists, change it to debug="false."
2. Add the following line as a new line the <system.web> section (anywhere after <system.web> and before <system.web/>):

   <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
3. Save changes and close the Web.config file.
4. At a command prompt, execute the **iisreset** command.

   Exit the command console.

Modify debug setting on ADFS Web servers

The following procedure must be performed for each claims-aware application that is installed on the Web server.

1. Open the C:\Inetpub\sampleapp\claimapp\Web.config file in a text editor and look for debug="true." If it exists, change it to debug="false."
2. If it does not exist already, add the following line as a new line the <system.web> section (anywhere after <system.web> and before <system.web/>):

   <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
3. Save changes and close the Web.config file.
4. Open the C:\Inetpub\sampleapp\claimapp\Default.aspx file in a text editor and look for debug="true." If it exists, delete debug="true" from the line that it appears in.
5. Save changes and close the Default.aspx file.
6. Open the C:\Inetpub\sampleapp2\claimapp2\Web.config file in a text editor and look for debug="true." If it exists, change it to debug="false."

7. If it does not exist already, add the following line as a new line the <system.web> section (anywhere after <system.web> and before <system.web/>):

   <machineKey validationKey="AutoGenerate,IsolateApps"
   decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>

8. Save changes and close the Web.config file.
9. Open the C:\Inetpub\sampleapp2\claimapp2\Default.aspx file in a text editor and look for debug="true." If it exists, delete debug="true" from the line that it appears in.
10. Save changes and close the Default.aspx file.
11. At a command prompt, execute the **iisreset** command.
12. Exit the command console.

Enabling Transport Layer Security in Web Browsers

Follow the procedure here to enable Transport Layer Security in the Web browsers used in the ADFS environment.

Enable TLS 1.0

On all ADFS computers and ADFS client computers:

1. Click **Start**, click **Control Panel**, navigate to and click **Internet Options**
2. Click the **Advanced** tab in Internet Options, scroll down and select the check box for **Use TLS 1.0**.
3. Click **OK**
4. Exit Control Panel.

Accessing Federated Applications from a Client Computer

This section describes the configuration steps that must be performed on the client computer before accessing ADFS-enabled applications from a client computer that is either in the account realm or the resource realm in the ADFS Federated Web SSO scenario. Also provided are instructions for accessing the ADFS-enabled applications for the purposes of testing the ADFS implementation.

Synchronizing Clocks

The system times on both domains must be synchronized so that all computers in the ADFS environment (including client computers) have the same time.

Synchronize the time on the client with the time on the federation server

1. Log in to the two domain controllers in the ADFS environment (<ResourceDC> and <AccountDC>) as a member of the Domain Admins group. On each computer, double-click the time displayed in the system tray on the Windows desktop to display the Date and Time Properties interface.

2. Adjust the time on the domain controllers so that they are synchronized with each other and click **OK** in the Date and Time Properties interface. The times need to be the same on each domain controller, preferably to within one or two seconds of each other.
3. On each computer in the ADFS environment that is not a domain controller, perform the following:
4. Click **Start** and click **Command Prompt**.
5. In the command console, type the following command and then press the **Enter** key:

   net time /set

6. At the following prompt, press the **Y** key and then press **Enter**:

   The current local clock is <date> <time>

   Do you want to set the local computer's time to match the

   time at \\<TimeServerName>? (Y/N) [Y]:

7. When the command completes successfully, type **exit** and press **Enter** to close the command prompt.

Note: Failure to synchronize clocks to within 20 seconds of each other can cause ADFS to fail.

Configuring Browser Settings

Use the following procedure to manually configure the user's Web browser settings on an ADFS client computer that is in the account realm so that the Web browser settings trust the account federation server.

Configure browser settings to trust the account federation server on the client computer in the account realm

On the account realm client computer (<AcctClient>):

1. Log on to the client computer as <AccountDomain>\<AcctUser>. In Windows XP Professional, click **Start**, click **Control Panel** and, if the folder is not displayed using Windows classic folders, click **Network and Internet Connections**.
2. Click **Internet Options**, and then click the **Security** tab.
3. On the **Security** tab, click the **Local intranet** Web content zone icon, and then click the **Sites** button.
4. Click the **Advanced** button, and in **Add this Web site to the zone**, type **https://<AcctFedSvrFQDN>**, verify that the URL is typed correctly, and then click **Add**.
5. Click **OK** three times and then exit the Control Panel.

Use the following procedure to manually configure the user's Web browser settings so that the Web browser settings trust the resource federation server.

Configure browser settings to trust the resource federation server on the client computer in the resource realm

On the resource realm client computer (<ResClient>):

1. Log on to the client computer using an account from the resource realm (i.e., <ResourceDomain>\<ResUser>). In Windows XP Professional, click **Start**, click **Control Panel** and, if the folder is not displayed using Windows classic folders, click **Network and Internet Connections**.
2. Click **Internet Options**, and then click the **Security** tab.
3. On the **Security** tab, click the **Local intranet** Web content zone icon, and then click the **Sites** button.
4. Click the **Advanced** button, and in **Add this Web site to the zone**, type **https://<ResFedSvrFQDN>**, verify that the URL is typed correctly, and then click **Add**.
5. Click **OK** three times and then exit the Control Panel.

Accessing the Sample Claims-aware Applications from the Account Realm

Use the following procedures to access the sample claims-aware applications from a client in the account realm that is authorized for that application.

Access the claims-aware application from the account realm

On the ADFS client computer (<AcctClient>):

1. Log on to the client computer using an account from the account realm (i.e., <AccountDomain>\<AcctUser>).
2. Click **Start**, click **Run**, type **https://<WebSvrFQDN>:8081/claimapp/**, and press the **Enter** key. A Web browser is launched.
3. If a Security Alert window is displayed indicating "You are about to view pages over a secure connection," select the check box for **In the future do now show this warning**, and click **OK**. Wait for the Web page to open.
4. If prompted with one or more Security Alert windows indicating a potential problem with the security certificate, click **Yes** each time such an alert appears.

Note: To avoid future certificate prompts, instead of choosing yes in the Security Alert interface, the user can choose **View Certificate**, select the **Details** tab, and click **Install Certificate**. In the Welcome to the Certificate Import Wizard, click **Next**, ensure that the radio button for **Automatically select the certificate store based on the type of certificate** is selected, click **Next**, click **Finish**, click **OK** at the "import was successful" message, click **OK** again, and select **Yes** in the Security Alert interface. This procedure can be repeated for each Security Alert interface presented on the client.

---

5. When the sample Web page opens prompting for a home realm, from the drop-down list select the account realm name (**<AccountDomain>**), and then click **Submit**.
6. The **Claims-aware Sample Application** appears in the browser, displaying the claims that were sent to the Web server in the **SingleSignOnIdentity.SecurityPropertyCollection** section.

Without clicking any links in the sample Web page, exit the Web browser and remain logged on as <AcctUser> for the next procedure.

Access the secondary claims-aware application from the account realm

On the ADFS client computer (<AcctClient>):

1. While still logged on to the <AcctClient> computer as <AccountDomain>\<AcctUser>, click **Start**, click **Run**, type **https://<WebSvrFQDN>:8083/claimapp2/**, and press the **Enter** key.
2. When the sample Web page opens, the user should not be prompted for a home realm, because a token was just received when accessing Claimapp in the previous procedure.
3. The secondary **Claims-aware Sample Application** appears in the browser, displaying the claims that were sent to the Web server in the **SingleSignOnIdentity.SecurityPropertyCollection** section.
4. Click the **Sign out** link on the Web page and exit the Web browser.

Accessing the Sample Windows NT Token-based Application from the Account Realm

Use the following procedure to access the sample token-based application from a client in the account realm that is authorized for that application.

Access the token-based application from the account realm

On the ADFS client computer (<AcctClient>):

1. Click **Start**, click **Run**, type **https://<WebSvrFQDN>:8091/tokenapp/**, and press the **Enter** key.
2. If a Security Alert window is displayed indicating "You are about to view pages over a secure connection," select the check box for **In the future do now show this warning**, and click **OK**. Wait for the Web page to open.
3. If prompted with one or more Security Alert windows indicating a potential problem with the security certificate, click **Yes** each time such an alert appears.

Note: To avoid future certificate prompts, instead of choosing yes in the Security Alert interface, the user can choose **View Certificate**, select the **Details** tab, and click **Install Certificate**. In the Welcome to the Certificate Import Wizard, click **Next**, ensure that the radio button for **Automatically select the certificate store based on the type of certificate** is selected, click **Next**, click **Finish**, click **OK** at the "import was successful" message, click **OK** again, and select **Yes** in the Security Alert interface. This procedure can be repeated for each Security Alert interface presented on the client.

---

4. If the Web page opens prompting for a home realm, from the drop-down list select the account realm name (**<AccountDomain>**), and then click **Submit**.
5. At this point the **Token-based Sample Application** appears in the browser, displaying a single line of text indicating the application type on a colored background.
6. In the browser, click **Tools**, click **Internet Options**, and click the **Delete Cookies** button on the **General** tab. Click **OK** twice and then exit the browser.
7. Click **Start**, click **Run**, type **https://<WebSvrFQDN>:8091/tokenapp/**, and press the **Enter** key.
8. If a Security Alert window is displayed indicating "You are about to view pages over a secure connection," select the check box for **In the future do now show this warning**, and click **OK**. Wait for the Web page to open.

9. If prompted with one or more Security Alert windows indicating a potential problem with the security certificate, click **Yes** each time such an alert appears.

Note: To avoid future certificate prompts, instead of choosing yes in the Security Alert interface, the user can choose **View Certificate**, select the **Details** tab, and click **Install Certificate**. In the Welcome to the Certificate Import Wizard, click **Next**, ensure that the radio button for **Automatically select the certificate store based on the type of certificate** is selected, click **Next**, click **Finish**, click **OK** at the "import was successful" message, click **OK** again, and select **Yes** in the Security Alert interface. This procedure can be repeated for each Security Alert interface presented on the client.

10. The token-based application Web page appears without prompting for a username or password.

Note: If a session was not first established with another ADFS-enabled application, or if such a session has since been closed, or if the cookie has expired, a username/password prompt is displayed when accessing the Windows NT token-based application.

11. Exit the Web browser and log off of Windows by clicking **Start**, **Log Off**, and **Log Off** again.

Accessing the Sample Claims-aware Application from the Resource Realm

Use the following procedure to access the sample claims-aware application from a client in the resource realm that is authorized for that application.

Access the claims-aware application from the resource realm

On the resource realm ADFS client computer (<ResClient>):

1. Log on to the <ResClient> computer as <ResourceDomain>\<ResUser>.
2. Click **Start**, click **Run**, type **https://<WebSvrFQDN>:8081/claimapp/**, and press the **Enter** key.
3. If a Security Alert window might be displayed indicating "You are about to view pages over a secure connection," select the check box for **In the future do now show this warning**, and click **OK**. Wait for the page to open.
4. When the Web page opens prompting for a home realm, ensure that the resource realm (**<ResourceDomain>**) is selected in the drop-down list, and then click **Submit**.
5. The **Claims-aware Sample Application** appears in the browser, displaying the claims that were sent to the Web server in the **SingleSignOnIdentity.SecurityPropertyCollection** section.
6. Exit the Web browser, then repeat Step 2 above. Single sign-on prevents the user from being prompted for a home realm again, and the **Claims-aware Sample Application** appears in the browser, displaying the claims that were sent to the Web server in the **SingleSignOnIdentity.SecurityPropertyCollection** section.
7. Click the **Sign out** link on the Web page and exit the Web browser.
8. Log off Windows by clicking **Start**, **Log Off**, and **Log Off** again.0.

If not configuring ADFS for the Web SSO scenario, skip the next section and proceed to Accessing Federated Applications from the Client Computer: Federated Web SSO Scenario.

Note: After completing the installation and configuration of the Federated Web SSO Scenario, as described in this section, it is important to apply the ADFS FIPS update on all federation servers and ADFS Web servers in order to mitigate a conflict between the ADFS and FIPS security policy setting as described in Microsoft Knowledge Base article KB935449. To apply the ADFS FIPS update, follow the procedures in Apply ADFS FIPS update to all ADFS Scenarios.

ADFS Installation and Configuration: Web SSO Scenario

This section describes installing and configuring ADFS in a Web SSO scenario. After ADFS components are installed, several steps are required to configure ADFS for the Web SSO scenario implementation described in this guide. This section describes the following processes in detail:

- Installing the Federation Service
- Installing the Web Agents
- Installing the Federation Service Proxy
- Creating the claims-aware application
- Creating the Windows NT token-based application
- Configuring the Web server
- Configuring the federation server
- Configuring the federation service proxy
- Accessing federated applications from the client computer

Installing the Federation Service

Use the following procedure to install the Federation Service component on the federation server in a Web SSO scenario. In order to perform all of the procedures on the ADFS computers in this installation and configuration section, the administrator must be logged on with an account that is a member of the Domain Admins group for the domain that the computer is joined to. This does not apply to procedures performed on the ADFS client computer.

Note: After completing the installation and configuration of the Web SSO Scenario, as described in this section, it is important to apply the ADFS FIPS update on all federation servers and ADFS Web servers in order to mitigate a conflict between the ADFS and FIPS security policy setting as described in Microsoft Knowledge Base article KB935449. To apply the ADFS FIPS update, follow the procedures in Apply ADFS FIPS Update.

Install the Federation Service

On the federation server (<FedSvr>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD. If a Welcome to Microsoft Windows Server 2003 R2 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In Add or Remove Programs, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, click **Active Directory Services** to highlight it.

Note: Do not click the check box next to **Active Directory Services** in this step.

6. Click the **Details** button.

7. In the Active Directory Services interface, click **Active Directory Federation Services (ADFS)** to highlight it.

   Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. Click the **Details** button.
9. In the Active Directory Federation Services (ADFS) interface, select the Federation Service check box, and click **OK**.

   Note: If prompted, "Do you want to enable ASP.NET 2.0?" click **Yes** to enable it, and then click **OK**. If .NET Framework 2.0 was installed and configured correctly earlier, this prompt is not displayed.

10. In the Active Directory Services interface, click **OK**.

    Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

11. In the Windows Components Wizard, click **Next**.
12. In the Federation Service page, click the radio button for **Select token-signing certificate**, and then click the **Select** button.
13. In the Select Certificate page, ensure that the server authentication certificate is selected (this is the server authentication certificate created earlier). Click **OK**.
14. In the Federation Service interface, for Trust policy, ensure that **Create a new trust policy** is selected, and then click **Next**.
15. If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate subfolder, click the **Open** button, and click **OK**.
16. In the Completing the Windows Components Wizard, click **Finish**, and exit Add or Remove Programs.
17. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

    Note: For 64-bit operating systems, skip the rest of this procedure and proceed to the Installing the Web Agents section.

18. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
19. Click the **Web Service Extensions** node in the console tree.
20. At the bottom of the details pane, click the **Standard** tab.
21. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Installing the Web Agents

The ADFS component that is installed on the Web server that hosts ADFS-enabled Web applications is called the Web Agent. There are two Web Agents—one for claims-aware applications, and another for Windows NT token-based applications. In this procedure, both Web Agents are installed.

Install the ADFS Web Agent

On the Web server (<WebServer>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD. If a Welcome to Microsoft Windows Server 2003 R2 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In **Add or Remove Programs**, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, click **Active Directory Services** to highlight it.

   Note: Do not click the check box next to **Active Directory Services** in this step.

6. Click the **Details** button.
7. In the Active Directory Services interface, click **Active Directory Federation Services (ADFS)** to highlight it.

   Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. Click the **Details** button.
9. In the **Active Directory Federation Services (ADFS)** interface, if any check boxes are pre-selected, clear them. Select the check box for **ADFS Web Agents,** and then click **Details**.
10. In the **ADFS Web Agents** interface, ensure that both the **Claims-aware applications** and **Windows NT token-based applications** check boxes are selected, and then click **OK**.
11. In the **Active Directory Federation Services (ADFS)** interface, ensure that only the **ADFS Web Agents** check box selected, and click **OK**.
12. In the Active Directory Services interface, click **OK**.

    Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

13. In the Windows Components Wizard, click **Next**.
14. If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate subfolder, click the **Open** button, and click **OK**.

15. In the Completing the Windows Components Wizard, click **Finish**. Close Add or Remove Programs.
16. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

Note: For 64-bit operating systems, skip the rest of this procedure.

17. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
18. Click the **Web Service Extensions** node in the console tree.
19. At the bottom of the details pane, click the **Standard** tab.
20. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Installing the Federation Service Proxy

Perform this installation on the federation service proxy (<FedProxy>).

Install the Federation Service Proxy

On the federation service proxy (<FedProxy>):

1. Log on as an authorized administrator that is a member of the Domain Admins group.
2. Insert the Windows Server 2003 R2 product CD. If a Welcome to Microsoft Windows Server 2003 R2 screen appears, click **Exit**.
3. Click **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
4. In Add or Remove Programs, click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, click **Active Directory Services** to highlight it.

Note: Do not click the check box next to **Active Directory Services** in this step.

6. Click the **Details** button.
7. In the Active Directory Services interface, click **Active Directory Federation Services (ADFS)** to highlight it.

Note: Do not click the check box next to **Active Directory Federation Services (ADFS)** in this step.

8. In the Active Directory Federation Services (ADFS) interface, select the **Federation Service Proxy** check box, and click **OK**.

Note: If prompted, “Do you want to enable ASP.NET 2.0?” click **Yes** to enable it, and then click **OK**. If .NET Framework 2.0 was installed and configured correctly earlier, this prompt is not displayed.

9. In the Active Directory Services interface click **OK**.

Note: On 32-bit Windows Server 2003 operating systems only, ADFS component installation causes the check box for ASP.NET in the Application Server details page to be selected automatically. This component is selected and installed by default during ADFS setup, and it cannot be de-selected. (De-selecting the ASP.NET check box in Application Server details prevents ADFS components from installing.) This results in ASP.NET version 1.1 being installed along with the ADFS component(s) selected in Add or Remove Programs. Because ASP.NET 1.1 is not included in the TOE, steps for disabling ASP.NET 1.1 in the Web Service Extensions in IIS on 32-bit operating systems are included later in this procedure.

10. In the Windows Components interface click **Next**.
11. In the Federation Service Proxy page click the **Select** button to choose the client authentication certificate.
12. In the Select Certificate page, ensure the client authentication certificate (which is named for the federation service proxy computer) is selected and click **OK**. Wait several moments until the **Select client authentication certificate** box is populated with the certificate name.
13. In the **Federation Service Domain Name System (DNS) host name** text box, type **<FedSvrFQDN>**.

Warning: Ensure that the fully qualified domain name (FQDN) of the federation server is used here, not the FQDN of the federation service proxy.

14. Verify that every character of the FQDN is typed correctly, and then click **Next**.
15. If prompted for the location of the installation files, click **Browse**, click **My Computer**, navigate to and double-click the CD-ROM drive letter, locate and double-click the appropriate subfolder, click the **Open** button, and click **OK**.
16. In the Completing the Windows Components Wizard, click **Finish**.
17. If the operating system is a 32-bit version of Windows Server 2003, click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

Note: For 64-bit operating systems, skip the rest of this procedure.

18. In the IIS Manager console tree, if the local computer node is not already expanded, click the plus sign (**+**) next to that node to expand it.
19. Click the **Web Service Extensions** node in the console tree.
20. At the bottom of the details pane, click the **Standard** tab.
21. In the Web Service Extension column, right-click **ASP.NET v1.1.4322** and select **Prohibit**. If prompted to confirm modification to this setting, click **Yes**.

Creating the Claims-aware Application

This guide employs the sample claims-aware applications that are provided in this section. At this point in a production deployment of ADFS, administrators can substitute their own claims-aware application. The claims-aware application (called “Claimapp”) is made up of three files that can be created from the instructions included here:

- Default.aspx
- Web.config
- Default.aspx.cs

Use the procedures here to create these three files and copy them to the Web server. Later in this guide instructions are provided for modifying these files for use in the ADFS environment. In order to complete the procedures in this section, access to a soft copy of this guide on a removable media device is required.

The first procedure describes how to open this document using WordPad (wordpad.exe) on the computer used in the evaluated configuration to create these files.

Note: Use any computer in the evaluated configuration to perform these procedures for creating the claims-aware application and the Windows NT token-based application.

Open this guide in WordPad

1. On the computer used to create the claims-aware application files, insert the removable media device containing a copy of this guide into the computer.
2. Click **Start**, click **My Computer**, and double-click the removable disk drive letter that is displayed.
3. In Windows explorer, navigate to and double-click the file representing this document.
4. A pop-up window appears, entitled **Microsoft Word 97 Conversion**, stating, “Unable to load graphics conversion filter. Continue with document conversion?” Click **Yes**.

   Note: This pop-up window might appear multiple times. If so, continue to click **Yes** until no more pop-ups are displayed and the document is displayed in WordPad.
5. This file opens in WordPad.
6. Close Windows explorer.

Create the folder on the removable media device

1. Insert a removable media device into the computer. Click **Start**, click **My Computer**, and double-click the removable disk drive letter that is displayed.
2. In Windows explorer, click **File**, point to **New**, and select **Folder**. Type **claimapp for Web SSO** as the new folder name, and press **Enter**.
3. Close Windows explorer.

Create the Default.aspx file

On the same computer, use the following procedure to create the Default.aspx file. This file will be modified later for use in the claims-aware application (Claimapp).

Create the Default.aspx file

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.

- Click the **Edit** menu in Word, and then click **Copy**.
- Switch applications to Notepad.
- In Notepad, click **File** then **Paste**.

```
<%@ Page Language="C#" AutoEventWireup="true" CodeFile="Default.aspx.cs"
Inherits="_Default" %>

<%@ OutputCache Location="None" %>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >

<head>

<meta http-equiv="Content-Language" content="en-us">

<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">

<title>Claims-aware Sample Application</title>

<style>

<!--

.pagetitle   { font-family: Verdana; font-size: 18pt; font-weight: bold;}

.propertyTable td { border: 1px solid; padding: 0px 4px 0px 4px}

.propertyTable th { border: 1px solid; padding: 0px 4px 0px 4px; font-weight: bold;
background-color: #cccccc ; text-align: left }

.propertyTable { border-collapse: collapse;}

td.l{ width: 200px }

tr.s{ background-color: #eeeeee }

.banner      { margin-bottom: 18px }

.propertyHead { margin-top: 18px; font-size: 12pt; font-family: Arial; font-weight:
bold; margin-top: 18}

.abbrev { color: #0066FF; font-style: italic }

-->

</style>

</head>


<body>

<form ID="Form1" runat=server>

<div class=banner>

<div class=pagetitle>SSO Sample</div>

[ <asp:HyperLink ID=SignOutUrl runat=server>Sign Out</asp:HyperLink> | <a
href="<%=Context.Request.Url.GetLeftPart(UriPartial.Path)%>">Refresh without viewstate
data</a>]

</div>

<div class=propertyHead>Page Information</div>

<div style="padding-left: 10px; padding-top: 10px">
```

```
<asp:Table runat=server ID=PageTable CssClass=propertyTable>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=IdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>

<div class=propertyHead>(IIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=BaseIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>(SingleSignOnIdentity)User.Identity</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SSOIdentityTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Name</asp:TableHeaderCell>
        <asp:TableHeaderCell>Value</asp:TableHeaderCell>
        <asp:TableHeaderCell>Type</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
```

```
</div>
<div class=propertyHead>SingleSignOnIdentity.SecurityPropertyCollection</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=SecurityPropertyTable runat=server>
    <asp:TableHeaderRow>
        <asp:TableHeaderCell>Uri</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Type</asp:TableHeaderCell>
        <asp:TableHeaderCell>Claim Value</asp:TableHeaderCell>
    </asp:TableHeaderRow>
</asp:Table>
</div>
<div class=propertyHead>(IPrincipal)User.IsInRole(...)</div>
<div style="padding-left: 10px; padding-top: 10px">
<asp:Table CssClass="propertyTable" ID=RolesTable runat=server>
</asp:Table>
<div style="padding-top: 10px">
<table>
<tr><td>Roles to check (semicolon separated):</td></tr>
<tr><td><asp:TextBox ID=Roles Columns=55 runat=server/></td><td align=right><asp:Button
UseSubmitBehavior=true ID=GetRoles runat=server Text="Check Roles"
OnClick="GoGetRoles"/></td></tr>
</table>
</div>
</div>
</form>
</body>
</html>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp for Web SSO** folder that was created in the previous procedure.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.aspx** exactly.

5. Exit Notepad.

Create the Web.config file

Use the following procedure to create the Web.config file.

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.

2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following steps:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
   <configSections>
      <sectionGroup name="system.web">
              <section name="websso"

type="System.Web.Security.SingleSignOn.WebSsoConfigurationHandler,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
      </sectionGroup>
   </configSections>
   <system.web>
    <machineKey validationKey="AutoGenerate,IsolateApps"
decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
    <sessionState mode="Off" />
    <compilation defaultLanguage="c#">
       <assemblies>
          <add assembly="System.Web.Security.SingleSignOn, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
          <add assembly="System.Web.Security.SingleSignOn.ClaimTransforms, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35, Custom=null"/>
       </assemblies>
    </compilation>
    <customErrors mode="Off"/>
    <authentication mode="None" />
    <httpModules>
        <add
            name="Identity Federation Services Application Authentication Module"
            type="System.Web.Security.SingleSignOn.WebSsoAuthenticationModule,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null" />
    </httpModules>

       <websso>
        <auditlevel>247</auditlevel>
```

```
        <authenticationrequired />
        <eventloglevel>55</eventloglevel>
        <auditsuccess>2</auditsuccess>
        <urls>
.........<returnurl>https://pe1420d.cmtl.com:8081/claimapp/</returnurl>
        </urls>
        <cookies writecookies="true">
          <path>/claimapp</path>
          <lifetime>240</lifetime>
        </cookies>
    <fs>https://pe1420e.cmtl.com/adfs/fs/federationserverservice.asmx</fs>
      </websso>
</system.web>
   <system.diagnostics>
      <switches>
  <add name="WebSsoDebugLevel" value="0" /> <!-- Change to 255 to enable full debug
logging -->
      </switches>
      <trace autoflush="true" indentsize="3">
         <listeners>
            <add name="LSLogListener"
type="System.Web.Security.SingleSignOn.BoundedSizeLogFileTraceListener,
System.Web.Security.SingleSignOn, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35, Custom=null"
initializeData=”c\logdir\claimapp.log” />
         </listeners>
      </trace>
   </system.diagnostics>
</configuration>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp for Web SSO** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Web.config** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Web.config** exactly.

5. Exit Notepad.

Create the Default.aspx.cs file

Use the following procedure to create the Default.aspx.cs file.

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key
2. Copy and paste the following code into Notepad by performing the following:
   - Highlight all of the text shown below.
   - Click the **Edit** menu in Word, and then click **Copy**.
   - Switch applications to Notepad.
   - In Notepad, click **File** then **Paste**.

```
using System;
using System.Data;
using System.Collections.Generic;
using System.Configuration;
using System.Reflection;
using System.Web;
using System.Web.Security;
using System.Web.UI;
using System.Web.UI.WebControls;
using System.Web.UI.WebControls.WebParts;
using System.Web.UI.HtmlControls;
using System.Security;
using System.Security.Principal;


using System.Web.Security.SingleSignOn;
using System.Web.Security.SingleSignOn.Authorization;


public partial class _Default : System.Web.UI.Page
{
    const string NullValue = "<span class=\"abbrev\" title=\"Null Reference, or not
applicable\"><b>null</b></span>";


    static Dictionary<string, string> s_abbreviationMap;


    static _Default()
    {
        s_abbreviationMap = new Dictionary<string, string>();
        //
        // Add any abbreviations here.  Make sure that prefixes of
        // replacements occur *after* the longer replacement key.
```

```
        //
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn.Authorization",
"SSO.Auth");
        s_abbreviationMap.Add("System.Web.Security.SingleSignOn", "SSO");
        s_abbreviationMap.Add("System", "S");
    }

    protected void Page_Load(object sender, EventArgs e)
    {
        SingleSignOnIdentity ssoId = User.Identity as SingleSignOnIdentity;

        //
        // Get some property tables initialized.
        //
        PagePropertyLoad();
        IdentityLoad();
        BaseIdentityLoad();
        SSOIdentityLoad(ssoId);
        SecurityPropertyTableLoad(ssoId);

        //
        // Filling in the roles table
        // requires a peek at the viewstate
        // since we have a text box driving this.
        //
        if (!IsPostBack)
        {
            UpdateRolesTable(new string[] { });
        }
        else
        {
            GoGetRoles(null, null);
        }

        //
        // Get the right links for SSO
        //
        if (ssoId == null)
        {
```

```
            SignOutUrl.Text = "Single Sign On isn't installed...";
            SignOutUrl.Enabled = false;
        }
        else
        {
            if (ssoId.IsAuthenticated == false)
            {
                SignOutUrl.Text = "Sign In (you aren't authenticated)";
                SignOutUrl.NavigateUrl = ssoId.SignInUrl;
            }
            else
                SignOutUrl.NavigateUrl = ssoId.SignOutUrl;
        }
    }

    void SecurityPropertyTableLoad(SingleSignOnIdentity ssoId)
    {
        Table t = SecurityPropertyTable;

        if (ssoId == null)
        {
            AddNullValueRow(t);
            return;
        }

        //
        // Go through each of the security properties provided.
        //
        bool alternating = false;
        foreach (SecurityProperty securityProperty in ssoId.SecurityPropertyCollection)
        {
            t.Rows.Add(CreateRow(securityProperty.Uri, securityProperty.Name,
securityProperty.Value, alternating));
            alternating = !alternating;
        }
    }

    void UpdateRolesTable(string[] roles)
    {
```

```
        Table t = RolesTable;

        t.Rows.Clear();

        bool alternating = false;
        foreach (string s in roles)
        {
            string role = s.Trim();
            t.Rows.Add(CreatePropertyRow(role, User.IsInRole(role), alternating));

            alternating = !alternating;
        }
    }
    void IdentityLoad()
    {
        Table propertyTable = IdentityTable;

        if (User.Identity == null)
        {
            AddNullValueRow(propertyTable);
        }
        else
        {
            propertyTable.Rows.Add(CreatePropertyRow("Type name",
User.Identity.GetType().FullName));
        }
    }

    void SSOIdentityLoad(SingleSignOnIdentity ssoId)
    {
        Table propertyTable = SSOIdentityTable;

        if (ssoId != null)
        {
            PropertyInfo[] props = ssoId.GetType().GetProperties(BindingFlags.Instance |
BindingFlags.Public | BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, ssoId, props);
        }
        else
```

```
        {
            AddNullValueRow(propertyTable);
        }
    }

    void PagePropertyLoad()
    {
        Table propertyTable = PageTable;

        string leftSidePath = Request.Url.GetLeftPart(UriPartial.Path);

        propertyTable.Rows.Add(CreatePropertyRow("Simplified Path", leftSidePath));
    }

    void BaseIdentityLoad()
    {
        Table propertyTable = BaseIdentityTable;
        IIdentity identity = User.Identity;

        if (identity != null)
        {
            PropertyInfo[] props = typeof(IIdentity).GetProperties(BindingFlags.Instance
| BindingFlags.Public | BindingFlags.DeclaredOnly);
            AddPropertyRows(propertyTable, identity, props);
        }
        else
        {
            AddNullValueRow(propertyTable);
        }
    }

    void AddNullValueRow(Table table)
    {
        TableCell cell = new TableCell();
        cell.Text = NullValue;

        TableRow row = new TableRow();
        row.CssClass = "s";
        row.Cells.Add(cell);
```

```
        table.Rows.Clear();
        table.Rows.Add(row);
    }

    void AddPropertyRows(Table propertyTable, object obj, PropertyInfo[] props)
    {
        bool alternating = false;

        foreach (PropertyInfo p in props)
        {
            string name = p.Name;
            object val = p.GetValue(obj, null);

            propertyTable.Rows.Add(CreatePropertyRow(name, val, alternating));
            alternating = !alternating;
        }
    }

    TableRow CreatePropertyRow(string propertyName, object propertyValue)
    {
        return CreatePropertyRow(propertyName, propertyValue, false);
    }

    TableRow CreatePropertyRow(string propertyName, object value, bool alternating)
    {
        if (value == null)
            return CreateRow(propertyName, null, null, alternating);
        else
            return CreateRow(propertyName, value.ToString(), value.GetType().FullName ,
alternating);
    }

    TableRow CreateRow(string s1, string s2, string s3, bool alternating)
    {
        TableCell first = new TableCell();
        first.CssClass = "l";
        first.Text = Abbreviate(s1);
```

```
        TableCell second = new TableCell();
        second.Text = Abbreviate(s2);

        TableCell third = new TableCell();
        third.Text = Abbreviate(s3);

        TableRow row = new TableRow();
        if (alternating)
            row.CssClass = "s";
        row.Cells.Add(first);
        row.Cells.Add(second);
        row.Cells.Add(third);

        return row;
    }

    private string Abbreviate(string s)
    {
        if (s == null)
            return NullValue;

        string retVal = s;
        foreach (KeyValuePair<string, string> pair in s_abbreviationMap)
        {
            //
            // We only get one replacement per abbreviation call.
            // First one wins.
            //
            if (retVal.IndexOf(pair.Key) != -1)
            {
                string replacedValue = string.Format("<span class=\"abbrev\"
title=\"{0}\">{1}</span>", pair.Key, pair.Value);
                retVal = retVal.Replace(pair.Key, replacedValue);
                break;
            }
        }
        return retVal;
    }
```

```
    //
    // ASP.NET server side callback
    //
    protected void GoGetRoles(object sender, EventArgs ea)
    {
        string[] roles = Roles.Text.Split(';');
        UpdateRolesTable(roles);
    }
}
```

3. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **claimapp for Web SSO** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.aspx.cs** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.aspx.cs** exactly.

4. Exit Notepad.

Creating the Windows NT Token-based Application

Perform this procedure on the same computer where the removable media device is inserted. Only one file must be created for the Windows NT token-based application.

Create the folder on the removable media device

1. Insert a removable media device into the computer. Click **Start**, click **My Computer**, and double-click the removable disk drive letter that is displayed.
2. In Windows explorer, click **File**, point to **New**, and then select **Folder**.
3. Type **tokenapp for Web SSO** as the new folder name, and click **Enter**.

   Note: If the File and Folder Tasks section is not visible in Windows explorer, click **Tools** and select **Folder Options**. In the Tasks section of the Folder Options interface, click the radio button to **Show common tasks in folders**, and click **OK**.

4. Close Windows explorer.

Create the Default.htm file

1. Click **Start**, click Run, type **notepad**, and press the **Enter** key.
2. Switch to the open document in WordPad.
3. Copy and paste the following code into Notepad by performing the following steps:
   - Highlight all of the text shown in the gray box.

- Click the **Edit** menu in Word, and then click **Copy**.
- Switch applications to Notepad.
- In Notepad, click **File** then **Paste**.

```
<html>
<head>
<meta HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">

<title ID=titletext>ADFS Token-based Application</title>
</head>

<body bgcolor=cccccc>
This is an ADFS token-based application.

</body>
</html>
```

4. In Notepad, click **File**, click **Save As**. In the Save As interface, use My Computer to navigate to and double-click the removable disk drive letter and then double-click the **tokenapp for Web SSO** folder that was created earlier.
   - Click the drop-down arrow for **Save as type** and choose **All files**.
   - In the **File name** box, type **Default.htm** and then click the **Save** button.

   Note: Be sure not to append the file name with .txt. The filename needs to be **Default.htm** exactly.
5. Exit Notepad and WordPad.
6. Remove the removable media device for use on the Web server later.

Configuring the Web Server

This section contains procedures for the following:

- Installing and configuring a claims-aware application
- Installing and configuring a Windows NT token-based application
- Configuring debug Logging on the Web Server
- Configuring debug Logging on the Web Server

Installing and Configuring a Claims-aware Application

Use the procedures in this section to install a sample claims-aware application and enable it for ADFS.

Create the sampleapp Web site for the claims-aware application on the Web server

On the Web server (<WebServer>):

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. In the **Internet Information Services (IIS) Manager** console tree, expand the local computer node, expand the Web Sites folder, right-click **Web Sites**, point to **New**, and select **Web Site**.
4. In the Welcome to the Web Site Creation Wizard click **Next**.
5. For **Description**, type **sampleapp** and click **Next**.
6. For **TCP Port this Web site should use**, type **8080**. Accept the defaults for the rest of the settings in the IP Address and Port Settings interface and click **Next**.

   Note: Do not modify the values listed for **Enter the IP address to use for this Web site** ([All Unassigned]) and for **Host header for this Web site** (blank).

7. In the Web Site Home Directory page, click the **Browse** button. Expand the local disk (C:) and navigate to the **C:\Inetpub** folder. Click the **Inetpub** folder once to highlight it.
8. In the Browse For Folder interface, with the **C:\Inetpub** folder selected, click the **Make New Folder** button. Type **sampleapp** for the New Folder name and press the **Enter** key.
9. With the **sampleapp** folder selected, click **OK**.
10. In the Web Site Home Directory page, verify the path is **C:\Inetpub\sampleapp**, leave the **Allow anonymous access to the Web site** check box selected, and click **Next**.
11. In the Web Site Access Permissions page, ensure that only the **Read** check box is selected, and click **Next**.
12. Click **Finish** to close the wizard.

Configure the sampleapp Web site

On the Web server (<WebServer>):

1. In the **Internet Information Services (IIS) Manager** console, under the **Web Sites** folder, right-click **sampleapp**, and then select **Properties**.
2. On the **Web Site** tab, in the **SSL Port** box type **8081**.
3. Click the **ASP.NET** tab. For **ASP.NET version**, ensure that 2.0.50727 is selected. (If not, click the drop-down arrow for **ASP.NET version**, and click **2.0.50727**.) Click **Apply**.
4. Click the **Directory Security** tab and, in the **Authentication and access control** area, click **Edit**.
5. In the Authentication Methods interface, in the **Authenticated access** area, clear the check box for **Integrated Windows authentication**, click **OK**, and then click **OK** again in the sampleapp Properties interface.
6. Under the **Web Sites** folder in the console tree, right-click **sampleapp**, point to **New**, and then select **Virtual Directory**.
7. In the Welcome to the Virtual Directory Creation Wizard, click **Next**.
8. In the Virtual Directory Alias interface, for **Alias**, type **claimapp**, and then click **Next**.

9. In the **Web Site Content Directory** interface, click **Browse**, navigate to and expand the **Inetpub** folder on the local disk (C:) and click the **sampleapp** subfolder once to highlight it. Click the **Make New Folder** button. This creates a subfolder called New Folder beneath the sampleapp folder.
10. Right-click **New Folder**, select **Rename** from the menu, type the name **claimapp** (exactly as it appears here) and press the **Enter** key. Click the new **claimapp** folder once to highlight it and click **OK**.

Warning: Do not use capital letters in the **claimapp** folder name. If this folder name contains capital letters, users must also use capital letters when they type the address of the Web site.

11. Verify that the **Path** specified in the Virtual Directory Creation Wizard is **C:\Inetpub\sampleapp\claimapp**, and then click **Next**.
12. In the **Virtual Directory Access Permissions** page, select both the **Read** and **Run scripts (such as ASP)** check boxes, and then click **Next**.
13. Click **Finish**.
14. In the **Internet Information Services (IIS) Manager** console tree, under **sampleapp** Web site, right-click the **claimapp** folder, and then select **Properties**.
15. On the **Documents** tab, verify that **Default.aspx** is in the list of files displayed. Otherwise, if Default.aspx is not listed, click **Add**, type **Default.aspx**, click **OK**.
16. Click **OK** again to close the claimapp Properties interface.

Assign the Web server's server authentication certificate to the sampleapp Web site

On the Web server (<WebServer>):

1. In **Internet Information Services (IIS) Manager**, under **Web Sites**, right-click **sampleapp**, and then select **Properties**.
2. Click the **Directory Security** tab.
3. On the **Directory Security** tab, click **Server Certificate**.
4. In the Welcome to the Web Server Certificate Wizard, click **Next**.
5. In the Server Certificate page, select **Assign an existing certificate**, and then click **Next**.
6. In the Available Certificates page, click the <WebServerFQDN> certificate to select it, and then click **Next**.
7. In the SSL Port page, accept the default (**8081**) for the **SSL port this web site should use**, and then click **Next**.
8. In the Certificate Summary page, verify the details, and then click **Next**.
9. In the Completing the Web Server Certificate Wizard, click **Finish**.
10. Click **OK** to exit the claimapp Properties page.

The next procedure requires access to the removable media device used earlier to store the application files created for Claimapp.

Copy the claims-aware application (Claimapp) files to the Web server

On the Web server (<WebServer>):

11. Insert the removable media device that contains the Claimapp files created earlier.
12. Click **Start** and select **My Computer**. Use Windows explorer to navigate to and double-click the **claimapp for Web SSO** folder on the removable disk. The three follows should be displayed in the claimapp folder:
    - Default.aspx
    - Web.config
    - Default.aspx.cs
13. To select all three files, choose **Select All** on the **Edit** menu, click **Edit** again, and then select **Copy** to copy the files to the Windows clipboard.
14. In Windows explorer, navigate to the local disk (C:), double-click the **Inetpub** folder, double-click the **sampleapp** subfolder, and double-click the **claimapp** subfolder to open it.
15. Click the **Edit** menu and then select **Paste** to copy the three files from the Windows clipboard to the C:\Inetpub\sampleapp\claimapp folder.
16. Leave Windows explorer open for the next procedure.

Edit Claimapp for use in the ADFS environment

On the Web server (<WebServer>):

1. With Windows explorer still open to the C:\Inetpub\sampleapp\claimapp folder from the previous procedure, right-click the **Web.config** file, click **Open**, click the **Select the program from a list** radio button and click **OK**. In the Open With interface, under **Programs**, click **WordPad** and then click **OK**. The Web.config file is displayed in WordPad.
2. Scroll down and locate the <websso> section of the file, and then find the <returnurl> line within that section. Between the left and right brackets, ensure that the URL is modified to point to the claimapp URL, using the fully qualified domain name (FQDN) of the Web server, as follows:

```
<returnurl>https://<WebServerFQDN>:8081/claimapp/</returnurl>
```

3. In the <websso> section, locate the <fs> entry for the federation server. Between the left and right brackets, ensure that the URL is modified to point to the FQDN of the resource federation server URL, as follows:

```
<fs>https://<FedSvrFQDN>/adfs/fs/federationserverservice.asmx</fs>
```

4. Click **File**, choose **Save**.
5. Exit WordPad and Windows explorer.

Installing and Configuring a Windows NT token-based Application

The token-based application is hosted on its own Web Site, so it is necessary to create a new Web site in IIS (as with sampleapp earlier). These procedures describe how to install a sample token-based application and enable it for ADFS.

Configure Web Sites for the Federation Service

On the Web Server (<WebServer>):

1. In the **Internet Information Services (IIS) Manager** console, under the local computer node, right-click **Web Sites**, and then select **Properties**.
2. Click the **ADFS Web Agent** tab.
3. For **Federation Service URL**, type the following:

   https://<FedSvrFQDN>/adfs/fs/FederationServerService.asmx
4. Verify that every character in the URL is typed correctly, and click **OK**.

Create a Web site for the Windows NT token-based application (Tokenapp)

1. In the **Internet Information Services (IIS) Manager** console, under the local computer node, right-click **Web Sites**, click **New** and select **Web Site**.
2. In the Welcome to the Web Site Creation Wizard click **Next**.
3. For **Description**, type **tokenapp** and click **Next**.
4. For **TCP Port this Web site should use**, type **8090**. Accept the defaults for the rest of the settings in this page and click **Next**.

   Note: Do not modify the values listed for **Enter the IP address to use for this Web site** ([All Unassigned]) and for **Host header for this Web site** (blank).
5. In the Web Site Home Directory page, click the **Browse** button. On the local disk (C:), browse to and click the **C:\Inetpub** folder.
6. With the **C:\Inetpub** folder selected, click the **Make New Folder** button. Type **tokenapp**, and press the **Enter** key.
7. With the **tokenapp** folder selected, click **OK**.
8. In the Web Site Home Directory page, verify the path is **C:\Inetpub\tokenapp**, leave **Allow anonymous access to this Web site** selected, and click **Next**.
9. In the Web Site Access Permissions page, ensure that only the **Read** check box is selected, and click **Next**.
10. Click **Finish** to exit the Web Site Creation Wizard.
11. Under the **Web Sites** folder in the console tree, right-click the **tokenapp** Web site node, point to **New**, and then click **Virtual Directory**.
12. In the Welcome to the Virtual Directory Creation Wizard, click **Next**.
13. In the Virtual Directory Alias interface, for **Alias**, type **tokenapp**, and then click **Next**.
14. In the **Web Site Content Directory** interface, click **Browse**, navigate to and expand the **Inetpub** folder on the local disk (C:) and click the **tokenapp** subfolder once to highlight it, and click **OK**. Verify that the **Path** specified in the Virtual Directory Creation Wizard is **C:\Inetpub\tokenapp**, and then click **Next**.
15. In the **Virtual Directory Access Permissions** page, select both the **Read** and **Run scripts (such as ASP)** check boxes, and then click **Next**.
16. Click **Finish**.

Configure the Windows NT token-based application Web site and assign the certificate

On the Web server (<WebServer>):

1. In the **Internet Information Services (IIS) Manager** console, under **Web Sites**, right-click the **tokenapp** Web site node, and then select **Properties**.
2. On the **Web Site** tab, in the **SSL Port** box type **8091**.

Warning: To open the tokenapp Web site properties page, ensure that this action is performed on the tokenapp Web site that exists in the console tree one level below the Web Sites node. Do not right-click the tokenapp virtual directory that exists in the console tree one level below the tokenapp Web site.

---

3. On the **ASP.NET** tab, for **ASP.NET version**, ensure that 2.0.50727 is selected. (If not, click the drop-down arrow for **ASP.NET version**, and click **2.0.50727**.) Click **Apply**.
4. In the tokenapp properties page, click the **Directory Security** tab. On the **Directory Security** tab, in the **Secure Communications** area, click **Server Certificate**.
5. In the Welcome to the Web Server Certificate Wizard, click **Next**.
6. In the Server Certificate page, click **Assign an existing certificate**, and then click **Next**.
7. In the Available Certificates page, click the **<WebServerFQDN>** certificate to select it, and then click **Next**.
8. In the SSL Port page, for the **SSL port this web site should use**, ensure the port number specified is **8091**, and then click **Next**.
9. In the Certificate Summary page, verify the details, and then click **Next**.
10. In the Completing the Web Server Certificate Wizard, click **Finish**.
11. Click the **ADFS Web Agent** tab.
12. Select the check box next to **Enable the ADFS Web Agent for Windows NT token-based applications**. Modify the **Return URL** as follows:

    https://<WebServerFQDN>:8091/tokenapp/

13. Verify that every character in the URL is typed correctly, and then click **OK**. If prompted, "The current cookie path does not match a prefix of the application path and/or the Return URL," click **Yes** to continue.
14. If an ADFS Web Agent pop-up window is displayed indicating "You are about to change the authentication method for this resource, which may break other applications. If you want to continue, press OK," click **OK**.

Copy the token-based application file to the Web server

On the Web server (<WebServer>):

1. Insert the removable media device that contains the application files created earlier.
2. Click **Start** and select **My Computer**. Use Windows explorer to navigate to and double-click the **tokenapp for Web SSO** folder on the removable disk. The following file should be displayed in the folder:
   - Default.htm
3. Select the **Default.htm** file, click the **Edit** menu, and select **Copy** to copy the files to the Windows clipboard.
4. In Windows explorer, navigate to the local disk (C:), double-click the **Inetpub** folder, and double-click the **tokenapp** subfolder.

5. Click the **Edit** menu and then click the **Paste** command to copy the file from the Windows clipboard to the C:\Inetpub\tokenapp folder.
6. Close Windows explorer.

Configuring Debug Logging on the Web Server

If it is necessary for the ADFS administrator to troubleshoot ADFS problems, debug logging can be configured to report ADFS-related activities that occur on the Web server. This section describes how to configure the Web server for debug logging. When troubleshooting is completed and the problem is resolved, it is recommended that debug logging be disabled if it is necessary to limit the size of the log files generated in the C:\ADFS\Logs folder on the Web server.

It is possible to enable debug logging for the following ADFS components:

- The ADFS Web Agent running on ADFS Web servers has two components:
  - ADFS Token Authentication service (ifssvc.exe), which validates incoming tokens and cookies. Debug logging creates **ifssvc.log** in the **C:\ADFS\Logs** folder.
  - ADFS Web Agent Internet Server Application Programming Interface (ISAPI) extension (ifsext.dll), which handles the protocols that are used by ADFS to authenticate requests; and the ADFS Web Agent ISAPI filter (ifsfilt.dll), which assists the extension and enables user name logging in the Internet Information Services (IIS) log files. Debug logging creates the **ifsext_StsAppPool1.log** and **ifsfilt_StsAppPool1.log**, respectively in the **C:\ADFS\Logs** folder.
- In addition, the ADFS Web Agent authentication package (ifsAp.dll) is used by Windows NT token-based applications for generating tokens when Service-for-User (S4U) is not available. Debug logging creates **ifsap.log** in the **C:\ADFS\Logs** folder.

Enable debug logging for each of these components in the registry on the Web server.

Note: In each of the following procedures, the registry value **FFFFFFFF** is not case-sensitive.

Enable debug logging for the ADFS ISAPI extension and filter

On the Web Server (<WebServer>):

1. Click **Start**, click Run, type **regedit** in the **Open** box, and click **OK**.
2. In **Registry editor** navigate to:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ADFS\WebServerAgent
3. Right-click **WebServerAgent**, click **New**, and then select **DWORD Value**.
4. In the new value file name box, type **DebugPrintLevel**, and then press **Enter**.
5. Double-click the new entry and then, in **Value data**, type **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295).

Enable debug logging for the ADFS Web Agent authentication package (for Windows NT token-based applications)

On the Web Server (<WebServer>):

1. In **Registry editor** navigate to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\WebSso\Parameters
2. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
3. In the new value file name box, type **DebugLevel**, and then press **Enter**.
4. Double-click the new entry and then, in **Value data**, type **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295).

Enable debug logging for the ADFS Token Authentication service

On the Web Server (<WebServer>):

1. In **Registry editor** navigate to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ifssvc\Parameters
2. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
3. In the new value file name box, type **DebugPrintLevel**, and then press **Enter**.
4. Double-click the new entry and then, in **Value data**, type **FFFFFFFF**, and then click **OK**. The details pane displays the following value for the new DWORD Value in the Data column: 0xffffffff (4294967295).
5. Leave Registry Editor open for a later procedure.

Configuring Event Logging on the Web Server

Events logged on Web servers that are running an ADFS Web Agent are configured according to the application type that the agent supports. Event logging is configured differently for Windows NT token-based applications and claims-aware applications.

Event logging for Windows NT token-based applications

On Web servers that are running the ADFS Web Agent for Windows NT token-based applications, event logging for these applications is set in the registry on the Web server. Use the following procedure to specify the types of events to be logged for Windows NT token-based applications on the Web server.

The procedure in this section is recommended for troubleshooting. It describes how to use a summation value of **0f** to enable all of the following debug logging levels:

- Warning: **0x01**
- Information: **0x02**
- Success: **0x04**
- Failure: **0x08**
- (All of the above: **0f)**

Note: To reduce the number of events generated by ADFS, change this value to a lesser level of debug logging after reaching a problem resolution following any troubleshooting steps.

Configure event logging for the Windows NT token-based application

On the Web server (<WebServer>):

1. In Registry Editor, navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ifssvc\Parameters

2. Right-click **Parameters**, click **New**, and then select **DWORD Value**.
3. In the new value file name box, type **ADFSEvent**, and then press **Enter**.
4. Double-click the new entry and then, in **Value data**, type **0f**, and then click **OK**.
5. Exit Registry Editor.

Event logging for claims-aware applications

On Web servers that are running the ADFS Web Agent for claims-aware applications, event logging for these applications is set in the Web.config file for the application. Use the following procedure to specify the level of events to be logged for claims-aware applications in the Application event log on the Web server (<WebServer>).Set event logging for claims-aware applications in the Web.config file for the application.

The procedure in this section describes how to use a summation value of 247 to enable all of the following debug logging levels in the Web.config file, and is recommended for troubleshooting:

- **DetailedFailure (0x80)**: A failure audit event that provides detailed information about each token involved in the transaction, including claims information.
- **DetailedSuccess (0x40)**: A success audit event that provides detailed information about each token involved in the transaction, including claims information.
- **Error (0x01)**: Provides information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **FailureAudit (0x20)**: Indicates a security event that occurs when an audited access attempt fails; for example, a failed attempt to open a file.
- **Info (0x04)**: Provides information about a significant, successful operation.
- **SuccessAudit (0x10)**: Indicates an audited security event that when an audited access attempt is successful; for example, a successful logon attempt.
- **Warning (0x02)**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Everything (0xf7, or 247 in decimal)**: Enables all logging levels.

Use the following procedure to configure the event logging level to record everything (enable all logging levels) for a claims-aware application. To complete this procedure, it is necessary to have read-write access to the application's Web.config file on the Web server.

Note: To reduce the number of events generated by ADFS, change this value to a lesser level of debug logging after reaching a problem resolution following any troubleshooting steps.

Verify that event logging for the claims-aware application is configured in the Web.config file

On the Web server (<WebServer>):

1. From the **Start** menu select **My Computer**.
2. In Windows explorer, navigate to the Web.config file in the folder that stores the claims-aware application (**C:\Inetpub\sampleapp\claimapp**). Right-click the **Web.config** file, select **Open With**, select **WordPad** from the list of applications, and click **OK**.
3. In WordPad, scroll down and locate the <websso> section of the file.
4. Verify or edit the <auditlevel> entry in the <websso> section to appear as follows:

```
<auditlevel>247</auditlevel>
```

5. Click **File**, click **Save**, and close WordPad.

Configuring the Federation Server

In this section, configure the debug logging, and event logging on the federation server. Then configure the Federation Service trust policy, organization claims, partners, and sample applications for use in the ADFS environment.

Configuring Auditing, Event Logging, and Debug Logging on the Federation Server

This section includes procedures for the following:

- Configure federation servers to record auditing of ADFS events to the security log
- Configure event logging on the federation server
- Configure debug logging on the federation server

Configuring ADFS servers to record auditing of ADFS events to the security log

All ADFS-related audits that are made specifically to the security log are considered by the system to be object access–type audits, which by default are ignored by the system. For this reason, to ensure that ADFS-related audits (specifically Success Audits and Failure Audits) appear in the Security log, the Local Security Policy must be configured manually using the procedure included here. The steps in this procedure must be applied to each of the ADFS servers (federation server, federation service proxy, and Web server) before enabling success or failure auditing in the Trust Policy properties of the ADFS management console. This allows the Federation Service to log either success or failure errors.

This procedure has no effect on the events that ADFS writes to the application log.

Configure the Windows security log to support auditing of ADFS events

Perform this procedure on both the federation server (<FedSvr>) and the federation service proxy (<FedProxy>).

1. Click **Start**, point to **Administrative Tools**, and then select **Local Security Policy**.
2. Double-click the **Local Policies** item, and then click **Audit Policy** beneath that in the console tree.
3. In the details pane, double-click **Audit object access**.
4. On the Audit object access Properties interface, select both the **Success** and **Failure** check boxes, and then click **OK**.
5. Close the Local Security Settings console.
6. Click **Start** and select **Command Prompt**. At the command prompt, type **gpupdate /force** and then press **Enter** to refresh local policy immediately.
7. Type **exit** and press **Enter** to close the command prompt.

Configuring event logging on the federation server

Servers that are running the Federation Service component of ADFS log ADFS Federation Service events in the Application event log. These events report information about the operation of the components of the local organization and partner organizations that are covered by a trust policy.

Note: ADFS also can log debug information. Debug logs are located in **C:\ADFS\logs**.

The following types of events are available and enabled by default in ADFS:

- **Error**: Information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **Warning**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Info**: Information about a significant, successful operation.
- **Success audit**: Indicates an audited security event when an audited access attempt is successful; for example, a successful logon attempt.
- **Failure audit**: Indicates a security event that occurs when an audited access attempt fails; for example, an inbound token was not valid.
- **Detailed success**: A success audit event with detailed information about each token involved in the transaction, including claims information.
- **Detailed failure**: A failure audit event with detailed information about each token involved in the transaction, including claims information.

Note: Audit object access must be turned on for success or failure to allow the Federation Service to log errors.

To complete this procedure, the logged-on account must be a member of the Administrators group on the local computer.

Verify the types of events logged by ADFS

On the federation server (<FedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. In the console tree, expand the **Federation Service** node, right-click **Trust Policy**, and select **Properties**.
3. Use the right arrow button to scroll to the **Event Log** tab. Click the **Event Log** tab.
4. For **Event log level**, ensure that each of the eight check boxes for the event log types is selected.
5. Click **OK**.

Configuring debug logging on the federation server

Event logs are generally descriptive, intended to help the administrator understand what is happening. However, the default events do not always provide the level of detail that is needed for effective troubleshooting. In this case, configure ADFS debug logging, as described here.

If debug logging is enabled on a federation server, the log filename in the C:\ADFS\logs directory has the following format:

adfsyyyymmdd-hhmmss.log

In the name of the file, the number following "adfs" represents the date of the log and the number following the dash (-) represents the beginning time of the log.

Depending on the level of debug logging enabled, the following tags are displayed in debug logs:

- **[INFO]** - Displays information about events, such as redirects with protocol Uniform Resource Locators (URLs), token validations, or claim mappings.
- **[VERBOSE]** - Displays information about events, such as sign-in requests, responses, token contents, Web method calls, and security identifier (SID) information.
- **[ERROR]** - Displays events for significant problems in the debug log.
- **[WARNING]** - Displays events, which are not necessarily significant but that may cause future problems.
- **[EVENTLOG]** - Displays all ADFS events.

Although all information in the log file could be useful, an administrator can look at the lines that are tagged **[ERROR]** and **[WARNING]** first to quickly assess the problem.

On federation account, resource, and proxy servers, administrators can use the Windows UI to enable debug logging and set levels to increase the detail of feedback in the logs.

Set ADFS debug levels on the federation server

On the federation server (<FedSvr>):

1. In the ADFS management console, right-click the **Federation Service** node and then select **Properties**.
2. Click the **Troubleshooting** tab.
3. On the **Troubleshooting** tab, select the check box for each of the eight debug levels, and then click **OK**.

Configuring Web Error Reporting on the Federation Servers

CustomErrors is an ASP.NET element that provides information about custom error messages for an ASP.NET application. Setting the customErrors mode attribute to “Off” specifies that custom errors are disabled. This results in better error reporting by ADFS.

Configure Web error reporting on the federation server and federation service proxy

Perform the following procedure on both the federation server (<FedSvr>) and the federation service proxy (<FedProxy>):

1. Click **Start**, click **My Computer**, and navigate to the **Web.config** file located in the **C:\ADFS\sts** folder in Windows Explorer.
2. Right-click the **Web.config** file, click **Open**, click the **Select the program from a list** radio button and click **OK**. In the Open With interface, click **WordPad**, and then click **OK**.
3. With the Web.config file open in WordPad, scroll down to the <system.web> section. Under <system.web>, insert a blank line and type the following text on that line, (preceded by four spaces for text alignment purposes only):

```
    <customErrors mode=”Off” />
```

4. After verifying the text is typed correctly, click **File**, choose **Save**, and exit **WordPad**.
5. Close Windows explorer

Exporting the Client Authentication Certificate Public Key

For the Web SSO scenario, the public portion of the Federation Service Proxy client authentication certificate must be added to the trust policy on a federation server so that the Federation Service can authenticate the federation service proxy. By exporting the public portion of the client authentication certificate, a file is created that can be imported by a federation server into the trust policy. Use the procedure here to export the public portion of the Federation Service Proxy client authentication certificate to a file.

Export the client authentication certificate public key to a file

On the federation service proxy (<FedProxy>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. In the console tree, right-click the **Federation Service Proxy** node, and then select **Properties**.
3. On the **General** tab, under FSP client authentication certificate, click the **View** button. The client authentication certificate is displayed.
4. In the Certificate interface, click the **Details** tab, and then click the **Copy to File** button.
5. In the Welcome to the Certificate Export Wizard page, click **Next**.
6. In the Export Private Key page, ensure that **No, do not export the private key** is selected, and then click **Next**.
7. In the Export File Format page, ensure that **DER encoded binary X.509 (.CER)** is selected, and then click **Next**.

8. In the File to Export page, click **Browse**, and type the location and file name to use for the exported certificate (**c:\<FedProxy>_cli.cer**), and then click **Save**.
9. Click **Next**.
10. In the Completing the Certificate Export Wizard page, verify that the information that was provided is accurate, and then click **Finish**.
11. In the Certificate Export Wizard interface, click **OK**.
12. In the Certificate interface, click **OK**.
13. In the Federation Service Properties interface, click **OK**.

Later in this guide a procedure is used to add the Federation Service Proxy client authentication certificate from the file that was exported.

Configuring the Federation Service

When configuring the Federation Service for the Web SSO scenario, because there is no federation trust involved, there is no need to configure partner organizations. The federation server performs both partner roles. This section describes the procedures that must be followed to configure ADFS in the Web SSO scenario.

This section includes procedures for performing the following:

- Configure the federation service trust policy
- Add the Federation Service Proxy client authentication certificate to the federation server trust policy
- Create group claims for the claims-aware application and the Windows NT token-based application
- Add a resource group to the Windows NT token-based application claim
- Add an Active Directory account store
- Add group claim extractions to the account store for the claims-aware application and for Windows NT token-based application and for the
- Add a claims-aware application and a Windows NT token-based application
- Enable the claims-aware application claim and the Windows NT token-based application claim
- Create incoming group claim mappings for the claims-aware application and for the Windows NT token-based application

As with all of the procedures on the ADFS computers, to perform these procedures, log on to the federation server using an account that is a member of the Domain Admins group.

Configure the federation service trust policy

On the federation server (<FedSvr>):

1. Close any open windows on the desktop. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**. The ADFS management console appears.
2. In the console tree, expand the **Federation Service** node by clicking the plus sign (**+**) adjacent to **Federation Service**, right-click **Trust Policy**, and then select **Properties**.

3. On the General tab, in the **Federation Service URI** text box, replace **urn:federation:myOrganization** with **urn:federation:<InternalDomain>>**, using all upper case letters for the <InternalDomain> name.

   Warning: This value is case-sensitive. Use all upper case when typing the internal domain's NetBIOS name

4. In the **Federation Service endpoint URL** text box, replace **https://<FedSvr>/adfs/ls/** with **https://<FedSvrFQDN>/adfs/ls/**.
5. Click the **Display Name** tab. In the **Display name for this trust policy** field, type a name identifying the organization that is hosting the federation server (<InternalDomain>). This name must be typed using the same casing wherever referenced in the ADFS configuration. For best results, use all lower case.
6. Click **OK**.

Add the Federation Service Proxy client authentication certificate to the federation server trust policy

On the federation server (<FedSvr>):

1. In the left pane of the ADFS management console, under **Federation Service**, right-click **Trust Policy**, and then select **Properties**. Click the **FSP Certificates** tab.
2. On the **FSP Certificates** tab, click the **Add** button.
3. In the Browse for Federation Service Proxy Certificate file interface, in the **File name** box, type the UNC path to the administrative share on the federation service proxy that contains the client authentication certificate file (i.e., **\\<FedProxy>\C$**) and click **Open**. Select the **<FedProxy>_cli.cer** certificate file and click **Open**.

   Note: If logged on properly as an authorized member of the Domain Admins group, no prompt is generated here for a username and password for the administrative share. If prompted, input **<AccountDomain>\Administrator** as username and type the appropriate password for that domain account.

4. Wait several seconds for the certificate to load. After the name of the client authentication certificate is displayed in the Trust Policy Properties interface, click **OK**.

Create a group claim for the claims-aware application

On the federation server (<FedSvr>):

1. In the ADFS management console, navigate to and expand the **Trust Policy** node under **Federation Service**.
2. Expand **My Organization**, right-click **Organization Claims**, point to **New**, and select **Organization Claim**.
3. In the Create a New Organization Claim interface, in **Claim name**, type **ClaimApp Claim**.
4. Ensure that **Group claim** is selected and click **OK**.

Create a group claim for the Windows NT token-based application

On the federation server (<FedSvr>):

1. In the ADFS management console, under the **My Organization** node, right-click **Organization Claims**, point to **New**, and select **Organization Claim**.
2. In the **Create a New Organization Claim** interface, in **Claim name**, type **TokenApp Claim**.
3. Ensure that **Group claim** is selected and click **OK**.

Add a resource group to the Windows NT token-based application claim

On the federation server (<FedSvr>):

1. In the ADFS management console, under the **My Organization** node, click **Organization Claims**.
2. In the details pane, right-click **TokenApp Claim** and select **Properties**.
3. In the Group Claim Properties interface, click the **Resource Group** tab.
4. Select the check box for **Map this claim to the following resource group**. Click the "**. . .**" button to the right of the text box.
5. In the Select Group interface, in the **Enter the object name to select** box, type **<TokenAppUsers>**, and click **OK**.

   Note: The object name is not case-sensitive.
6. The Group field in the Group Claim Properties interface is populated with the UPN name **<TokenAppUsers>@<InternalDomainFQDN>**.
7. Click **OK** again.

Add an Active Directory account store

On the federation server (<FedSvr>):

1. In the ADFS management console, under the **My Organization** node, right-click **Account Stores**, point to **New**, and then select **Account Store**.
2. In the Welcome to the Add Account Store Wizard, click **Next**.
3. In the Account Store Type page, ensure that **Active Directory** is selected, and then click **Next**.
4. In the Enable this Account Store page, ensure that the **Enable this account store** check box is selected, and then click **Next**.
5. In the Completing the Add Account Store Wizard, click **Finish**.
6. Click **File** and then click **Exit** to close the ADFS management console.

Add a group claim extraction to the account store for the Windows NT token-based application

On the federation server (<FedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. In the ADFS management console, navigate to and expand the **Account Stores** node under the **My Organization** node.

Note: The **Active Directory** account store should appear under the Account Stores node. However, sometimes the ADFS management console does not display the account store immediately after creation. If the Active Directory account store does not appear, repeat the entire procedure (**To add an Active Directory account store**) and then continue with Step 1 of the current procedure (**To add a group claim extraction to the account store**).

3. Right-click the **Active Directory** item, point to **New**, and select **Group Claim Extraction**.
4. In the Create a New Group Claim Extraction interface, ensure that **TokenApp Claim** is displayed in the box for **Map to this organization claim**. If not, use the drop-down arrow to select **TokenApp Claim**. Click the **Add** button.
5. In the Select Users or Groups interface, in the **Enter the object name to select** box, type **<TokenAppUsers>**, and click **OK**.

Note: The object name is not case-sensitive.

6. The Create a New Group Claim Extraction interface is populated with the **<TokenAppUsers>@<InternalDomainFQDN>** claim mapping.
7. Click **OK** again.

Add a group claim extraction to the account store for the claims-aware application

On the federation server (<FedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**. The ADFS management console appears. Expand the **Trust Policy** node under **Federation Service**.
2. Navigate to and expand the **Account Stores** node under the **My Organization** node.
3. Right-click the **Active Directory** item, point to **New**, and select **Group Claim Extraction**.
4. In the Create a New Group Claim Extraction interface, click the drop-down arrow for the **Map to this organization claim** menu and select **ClaimApp Claim** from the drop-down list. Click the **Add** button.
5. In the Select Users or Groups interface, in the **Enter the object name to select** box, type **<ClaimAppUsers>**, and click **OK**.

Note: The object name is not case-sensitive.

6. The Create a New Group Claim Extraction interface is populated with the **<ClaimAppUsers>@<InternalDomainFQDN>** claim mapping.
7. Click **OK** again.

Add a claims-aware application

On the federation server (<FedSvr>):

1. In the ADFS management console under **My Organization**, right-click **Applications**, point to **New**, and select **Application**.
2. In the Welcome to the Add Application Wizard, click **Next**.
3. In the Application Type page, ensure that **Claims-aware application** is selected and click **Next**.

4. In the Application Details page, in **Application display name**, type **Claimapp**. In **Application URL**, type **https://<WebServerFQDN>:8081/claimapp/**. Verify that every character in the URL is typed correctly, and then click **Next**.

   Note: The reference to **8081** in the **Application URL** is necessary to route SSL traffic to port 8081 because the default Web site is using the default SSL port (443).

5. In the Accepted Identity Claims page, select the **User principal name (UPN)** check box and click **Next**.
6. In the Enable this Application page, ensure that the **Enable this application** check box is selected, and then click **Next**.
7. In the Completing the Add Application Wizard, click **Finish**.
8. Click **File** and then click **Exit** to close the ADFS management console.

Add a Windows NT token-based application

On the federation server (<FedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. In the ADFS management console, expand **Trust Policy** and **My Organization**, then right-click **Applications**, point to **New**, and select **Application**.
3. In the Welcome to the Add Application Wizard, click **Next**.
4. In the Application Type page, select **Windows NT token-based application** and click **Next**.
5. In the Application Details page, for **Application display name**, type **TokenApp**. In **Application URL**, type **https://<WebServerFQDN>:8091/tokenapp/**. Verify that every character in the URL is typed correctly, and then click **Next**.
6. In the Accepted Identity Claims page, ensure that the **User principal name (UPN)** radio button is selected and click **Next**.
7. In the Enable this Application page, ensure that the **Enable this application** check box is selected, and then click **Next**.
8. In the Completing the Add Application Wizard, click **Finish**.
9. Click **File** and then click **Exit** to close the ADFS management console.

Enable the ClaimApp Claim

On the federation server (<FedSvr>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. Navigate to and expand **Trust Policy** in the ADFS management console. Expand **My Organization**, and expand **Applications**.
3. Under the **Applications** node, click **Claimapp**.
4. In the details pane, right-click the **ClaimApp Claim** group claim, and then select **Enable**.

Enable the TokenApp Claim

On the federation server (<FedSvr>):

1. In the ADFS management console, under the **Applications** node, click **TokenApp**.
2. In the details pane, right-click the **TokenApp Claim** group claim, and then select **Enable**.

Configuring the Federation Service Proxy

Active Directory Federation Services (ADFS) federation servers log ADFS Federation Service events in the Application event log. On a federation service proxy, these events contain additional information about errors regarding contacting the Federation Service. In addition, when a federation service proxy is in effect, the Federation Service events contain information about the proxy certificates that are used.

Federation servers log ADFS Federation Service events in the Application and Security event logs. On a federation service proxy, events in the Application log contain additional information about errors regarding contact with the Federation Service. In addition, when a federation service proxy is in effect, the Federation Service events contain information about the proxy certificates that are used.

Event logging for a federation service proxy is set in the Web.config file. By default, this file is located in <SystemDrive>\ADFS\sts. The following logging types can be specified in the Web.config file:

- **Error (0x01)**: Information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **Warning (0x02)**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Info (0x04)**: Information about a significant, successful operation.
- **SuccessAudit (0x10)**: Indicates an audited security event that occurs when an audited access attempt is successful, for example, a successful logon attempt.
- **FailureAudit (0x20)**: Indicates a security event that occurs when an audited access attempt fails; for example, authentication failed.
- **DetailedSuccess (0x40)**: A success audit event with detailed information about each token involved in the transaction, including claims information.
- **DetailedFailure (0x80)**: A failure audit event with detailed information about each token involved in the transaction, including claims information.
- **Everything (0xf7**, or **247** in decimal**)**: Enables all logging levels.

Use the following procedure to configure event logging levels on a federation service proxy. Perform this procedure on the federation service proxy. To complete this procedure, log on as a member of the Domain Admins group.

Configure event logging for a federation service proxy using the Web.config file

On the federation service proxy (<FedProxy>):

1. From the **Start** menu select **My Computer**.
2. In Windows explorer, navigate to the Web.config file in the **C:\ADFS\sts** folder.
3. Right-click the **Web.config** file, point to **Open With**, click **WordPad**, and click **OK**.

4. In WordPad, scroll down and locate the <logonserver> entry.
5. Under <logonserver>, insert a blank line and type the following text on that line, (preceded by six spaces for text alignment purposes only):

```
<auditlevel>247</auditlevel>
```

6. Click **File**, click **Save**, and close WordPad.
7. Close Windows explorer.

Configuring Debug Logging on the Federation Service Proxy

If debug logging is enabled on a federation service proxy, the log filename in the C:\ADFS\logs folder has the following format:

adfsyyyymmdd-hhmmss.log

In the name of the file, the number following "adfs" represents the date of the log and the number following the dash (-) represents the beginning time of the log.

Depending on the level of debug logging enabled, the following tags are displayed in debug logs:

- **[INFO]** - Displays information about events, such as redirects with protocol Uniform Resource Locators (URLs), token validations, or claim mappings.
- **[VERBOSE]** - Displays information about events, such as sign-in requests, responses, token contents, Web method calls, and security identifier (SID) information.
- **[ERROR]** - Displays events for significant problems in the debug log.
- **[WARNING]** - Displays events, which are not necessarily significant but that may cause future problems.
- **[EVENTLOG]** - Displays all ADFS events.

Although all information in the log file could be useful, an administrator can look at the lines that are tagged **[ERROR]** and **[WARNING]** first to quickly assess the problem.

On federation servers, use the Windows interface to enable debug logging and set levels to increase the detail of feedback in the logs.

Set ADFS debug levels on the federation service proxy

On the federation service proxy (<FedProxy>):

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Federation Services**.
2. Right-click **Federation Service Proxy** and then select **Properties**.
3. On the **Troubleshooting** tab, select the check box for each of the eight debug levels, and then click **OK**.

Accessing Federated Applications from the Client Computer: Web SSO Scenario

This section describes the configuration steps that must be performed on the client computer before accessing ADFS-enabled applications from a computer that is external to the protected network (i.e., is in the perimeter network) in the ADFS Web SSO scenario. Also provided are instructions for accessing the ADFS-enabled applications.

Configuring Hosts Files for Name Resolution

Because the client computer is external to the protected network, it must be able to resolve the internal federation server's fully qualified domain name (FQDN) to the externally-facing IP address of the federation service proxy. It must also be able to resolve the Web server's FQDN to the Web server's external IP address.

In order for these things to happen, a Windows **hosts** file must be edited for name resolution on both the federation service proxy and on the client computer. This file is located in the <SystemDrive>\Windows\System32\Drivers\etc folder on both computers.

Edit the hosts file

On the federation service proxy (<FedProxy>) and external client computer (<ExtClient>):

1. Log on to the federation servcie proxy as an authorized administrator. On the external client computer, log on as an authorized administrator.
2. From the **Start** menu, select **My Computer**. Navigate to and open the following folder:

   C:\Windows\System32\Drivers\etc
3. Double-click the **hosts** file in the etc folder. In the **Open With** interface, click **Notepad,** and then click **OK**. The hosts file opens in Notepad for editing.
4. Locate the following line in the file, which displays the loopback IP address for the local computer:

   127.0.0.1 localhost

   Note: This entry is not case-sensitive.
5. Add new line(s) beneath the local host line as indicated below, then save the hosts file and exit Notepad.
6. Close Windows explorer and log off Windows.

Hosts file configuration on the federation service proxy computer

Edit the hosts file on the federation service proxy computer (<FedProxy>) to include the following entry, so that the DNS name of the federation server resolves to the internal IP address of the federation server, and save changes:

<FedSvrIPAddress> <FedSvrFQDN>

For example:

192.168.5.12 pe1420e.cmtl.com

Note: Use spaces between the IP address and DNS name when adding entries to the hosts file.

Hosts file configuration on the client computer

Edit the hosts file on the external ADFS client computer (<ExtClient>) to include the following entries, so that the external IP address of the federation service proxy resolves to the internal DNS name of the federation server, and the external IP address of the Web server resolves to the internal DNS name of the Web server, and save changes:

<FedProxyIPAddress> <FedSvrFQDN>

<WebServerIPAddress> <WebServerFQDN>

For example:

192.168.10.10 pe1420e.cmtl.com

192.168.10.11 pe1420d.cmtl.com

Accessing the Sample Claims-aware Application and the Windows NT Token-based Application

For the purposes of testing the ADFS implementation, use the procedures here to access the sample applications created for this implementation.

Access the sample claims-aware application

On the external client <ExtClient>:

1. Log on to the computer using a local user account, <ExtClient>\<LocalUser>.
2. Click **Start**, click **Run**, type **https://<WebServerFQDN>:8081/claimapp/**, and press **Enter**.
3. If a Security Alert window is displayed indicating "You are about to view pages over a secure connection," select the check box for **In the future do now show this warning**, and click **OK**. Wait for the page to open.
4. If prompted with one or more Security Alert windows indicating a potential problem with the security certificate, click **Yes** each time such an alert appears.

Note: To avoid future certificate prompts, instead of choosing yes in the Security Alert interface, the user can choose **View Certificate**, select the **Details** tab, and click **Install Certificate**. In the Welcome to the Certificate Import Wizard, click **Next**, ensure that the radio button for **Automatically select the certificate store based on the type of certificate** is selected, click **Next**, click **Finish**, click **OK** at the "import was successful" message, click **OK** again, and select **Yes** in the Security Alert interface. This procedure can be repeated for each Security Alert interface presented on the client.

---

5. When the **CollectInitialCredentials** Active Directory Federation Services Web page opens prompting for a username and password, type **<ExtUser>** for the username, type the user's domain password in the appropriate field, and then click **Submit**.
6. The **Claims-aware Sample Application** appears in the browser, displaying the claims that were sent to the Web server in the **SingleSignOnIdentity.SecurityPropertyCollection** section.

Warning: If the client computer time is out of sync with the time on the ADFS servers, access to an ADFS-enabled application might fail, generating "infinite loop" errors in the federation proxy logs and application event log.

---

7. Leave the sample Web page open in the browser and proceed to accessing the Windows NT token-based application.

Access the sample windows NT token-based application

On the external client <ExtClient>:

1. While logged on to the external client computer as a local user (such as <ExtClient>\<LocalUser>) who has signed in to the claims-aware application, click **Start**, click **Run**, type **https://<WebServerFQDN>:8091/tokenapp/** and press **Enter**.
2. If prompted with one or more Security Alert windows indicating a potential problem with the security certificate, click **Yes** each time such an alert appears.

Note: To avoid future certificate prompts, instead of choosing yes in the Security Alert interface, the user can choose **View Certificate**, select the **Details** tab, and click **Install Certificate**. In the Welcome to the Certificate Import Wizard, click **Next**, ensure that the radio button for **Automatically select the certificate store based on the type of certificate** is selected, click **Next**, click **Finish**, click **OK** at the "import was successful" message, click **OK** again, and select **Yes** in the Security Alert interface. This procedure can be repeated for each Security Alert interface presented on the client.

3. The token-based application Web page appears without prompting for a username or password.

Note: If a session was not first established with another ADFS-enabled application, or if such a session has since been closed, or if the cookie has expired, a username/password prompt is displayed when accessing the Windows NT token-based application.

4. Exit the Web browser.

The next time the user accesses either the claims-aware application or the Windows NT token-based application, the user is required to input a user name and password in order to access the ADFS-enabled application.

Install the ADFS FIPS Update

As stated in the beginning of this section, after completing the installation and configuration of the Web SSO Scenario, it is important to apply the ADFS FIPS update on all federation servers, federation service proxies, and ADFS Web servers in order to mitigate a conflict between the ADFS and FIPS security policy setting as described in Microsoft Knowledge Base article KB935449. To apply the ADFS FIPS update, follow the procedures in Apply ADFS FIPS update.

Apply ADFS FIPS Update

A conflict exists with the original installation of ADFS and the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** security policy setting that is required in the Evaluated Configuration of Windows Server 2003 with SP2. When the FIPS policy setting is enabled, any attempt to access an ADFS Web site can result in the following exception:

InvalidOperationException: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms.

To mitigate this issue, Microsoft has made a patch available (KB935449) that can be downloaded from http://support.microsoft.com/kb/935449.

Download and install this patch on all federation servers (including federation service proxies) and ADFS Web servers. Then follow the procedures here to make the necessary changes to the Web.config files and Web browser settings.

Updating existing Web files

Any instance of debug=”true” must be removed from Web.config files and *.aspx files on the ADFS computers.

Note: In the <compilation> section of the Web.config, the default debug setting is false. If no debug= instance appears in the compilation section of the Web.config, the file does not need modification because it automatically defaults to false.

Modify debug setting on federation servers (including federation service proxies)

On each federation server and federation server proxy:

1. Open the C:\ADFS\sts\Web.config file in a text editor such as Notepad or WordPad, and scroll down to the <compilation> section. Look for debug=”true.” If it exists, change it to debug=”false.”
2. Add the following line as a new line the <system.web> section (anywhere after <system.web> and before <system.web/>):

   <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
3. Save changes and close the Web.config file.
4. At a command prompt, execute the **iisreset** command.
5. Exit the command console.

Modify debug setting on ADFS Web servers

The following procedure must be performed for each claims-aware application that is installed on the Web server.

1. Open the C:\Inetpub\sampleapp\claimapp\Web.config file in a text editor and look for debug=”true.” If it exists, change it to debug=”false.”
2. If it does not exist already, add the following line as a new line the <system.web> section (anywhere after <system.web> and before <system.web/>):

   <machineKey validationKey="AutoGenerate,IsolateApps" decryptionKey="AutoGenerate,IsolateApps" validation="3DES" decryption="3DES"/>
3. Save changes and close the Web.config file.
4. Open the C:\Inetpub\sampleapp\claimapp\Default.aspx file in a text editor and look for debug=”true.” If it exists, delete debug=”true” from the line that it appears in.
5. Save changes and close the Default.aspx file.
6. At a command prompt, execute the **iisreset** command.
7. Exit the command console.

Enabling Transport Layer Security in Web Browsers

Follow the procedure here to enable Transport Layer Security in the Web browsers used in the ADFS environment.

Enable TLS 1.0

On all ADFS computers and ADFS client computers:

1. Click **Start**, click **Control Panel**, navigate to and click **Internet Options**
2. Click the **Advanced** tab in Internet Options, scroll down and select the check box for **Use TLS 1.0**.
3. Click **OK**.
4. Exit Control Panel.

7. Windows Server Update Services Deployment

WSUS 3.0 Overview

Microsoft Windows Server Update Services (WSUS) 3.0 provides administrators with full control over the update management process, eliminating the need for client computers to retrieve updates directly from Microsoft Update. WSUS administrators can specify the types of updates to download, create target groups of computers to receive updates, and determine which computers require updates before deployment. WSUS administrators can also approve updates for automatic deployment, uninstall updates, and generate reports to monitor update activity.

WSUS 3.0 consist of a server and a client portion. WSUS clients are all computers residing within the TOE that are configured to get their updates from a WSUS 3.0 server. The server portion is responsible for collecting and storing the updates, as well as making the updates available to clients within the TOE. The client portion is responsible for downloading and installing updates onto its local host. The server and the client communicate using a protected interface that ensures only privileged users can interact with either interface. Additionally, WSUS 3.0 performs a CRC and certificate check to ensure each update is a Microsoft created update.

A WSUS server within the TOE receives updates from a trusted source; either imported by an authorized administrator from a WSUS 3.0 server outside the TOE, which obtains the updates from the Microsoft Update Web site, or from an upstream WSUS 3.0 server. The server stores its update information, event information about update actions on client machines, and server settings in a Microsoft SQL Server 2005 Embedded Edition database.

> **Note:** The TOE is a protected network with no Internet connectivity; therefore direct access to the Microsoft Update Web site is not possible. However, a WSUS 3.0 server outside the TOE can be used to obtain the updates from the Microsoft Update Web site. The updates can then be exported from the external WSUS 3.0 server and imported to WSUS 3.0 servers within the TOE.

An authorized administrator manages the updates received by the WSUS 3.0 server and has the ability to determine if an update should be approved for installation. If the administrator approves an update, the update can then be either pushed or pulled from the server. In a pull operation, the administrator can let client machines poll the server looking for new updates. In the push operation, WSUS server downloads updates and pushes them to the Auto Update Client on each computer within the TOE. The client then installs the updates. The administrator can configure the server to require all client computers to perform an immediate update. The administrator also has the ability to set a deadline by which time all clients must download an update (i.e., perform a pull operation) or the server will push the update.

WSUS Architecture within the TOE

WSUS 3.0 server software is not included with the Windows Server 2003 operating system, but is installed as a separate add-on product. The IT environment is a protected network with no Internet connectivity. Therefore, to support WSUS 3.0 within the TOE, an external WSUS 3.0 server must first be configured on an external network that has Internet connectivity in order to access the Microsoft Update Web site. After the Microsoft updates are downloaded to the external WSUS 3.0 server, an authorized administrator exports the update metadata and content to removable media, and then imports that update metadata and content to the WSUS servers within the protected network of the TOE. The external WSUS 3.0 server will not be included in the TOE.

Within the protected network, WSUS 3.0 can be deployed in single server architectures directly supporting clients or as multiple internally synchronized WSUS 3.0 servers. Architectures consisting of multiple internally synchronized WSUS servers will include upstream WSUS 3.0 servers and downstream WSUS 3.0 servers. In this architecture, the updates are imported to the upstream WSUS 3.0 server from the external WSUS 3.0 server. Downstream WSUS 3.0 servers then synchronize with the upstream WSUS 3.0 servers to get the new update metadata and content.

Within the TOE, all Windows Server 2003 SP2 computers hosting WSUS also host IIS 6.0 locally to support WSUS 3.0. Each WSUS 3.0 server also requires its own database. Within the TOE, Microsoft SQL Server 2005 Embedded Edition is the database used in the IT environment supporting WSUS 3.0. The WSUS 3.0 server setup software already includes Microsoft SQL Server 2005 Embedded Edition. Within the TOE, SSL will be required for metadata exchange between downstream servers and clients.

WSUS Components

The following WSUS components are included in the TOE:

- **WSUS**. WSUS 3.0 is the server software component that is hosted on computers running the Windows Server 2003 SP2 operating systems (both 32 and 64-bit versions) within the TOE. The Background Intelligent Transfer Service (BITS) 2.0 update must be installed on the host before installing the WSUS server software. WSUS administration interfaces require the use of Internet Explorer, which is not included in the TOE. For this reason, and to mitigate any potential risks associated with the use of IE by an administrator, remote administration of WSUS servers is not be permitted within the TOE.
- **Windows Update Agent**. This is the client side software component, also known as WSUS Client that downloads and installs updates made available by WSUS servers. This client requires BITS 2.0 to efficiently download updates, utilizing available bandwidth. Within the TOE, WSUS client host operating systems include Windows Server 2003 with SP2 and Windows XP Professional with SP2 (both 32 and 64-bit versions).
- **Background Intelligent Transfer Services (BITS) 2.0**. BITS 2.0 provides a file transfer mechanism that uses idle bandwidth on WSUS servers and clients to transfer files. BITS 2.0 is used to support both upload and download operations, as well as scheduling, pausing, and restarting downloads. BITS 2.0 is installed when a Windows XP WSUS client is installed and configured in accordance with the Evaluated Configuration guidance provided in the *Windows XP Professional with SP2 Security Configuration Guide, Version 3.0*. It is installed by default on Windows Server 2003 with SP2.

WSUS 3.0 Installation

WSUS Installation Pre-Requisites

Disk Space Requirements

Use the following guidelines to prepare the disks and partitions on the computer where WSUS will be installed:

- All partitions supporting WSUS must be formatted with the NTFS file system.

- A minimum of 20 GB of free disk space is required for the volume where WSUS stores content; 30 GB is recommended.
- A minimum of 2 GB of free space is required on the volume where WSUS Setup installs Microsoft SQL Server 2005 Embedded Edition.

Software Prerequisites

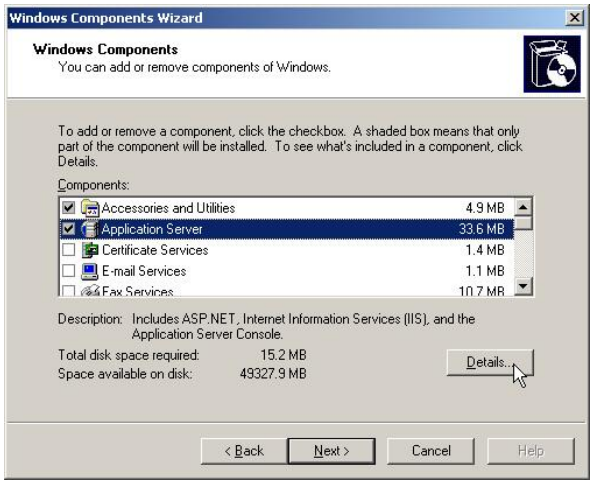
The following is a list of software prerequisites for running WSUS 3.0 on Windows Server 2003. Ensure that the WSUS server host meets this list of requirements prior to initiating the installation of WSUS 3.0.

- Microsoft Internet Information Services (IIS) 6.0. See Install Internet Information Services (IIS) 6.0 for IIS 6.0 installation instructions.
- Background Intelligent Transfer Service (BITS) 2.0 (installed by default on Windows Server 2003 with SP2).
- Microsoft .NET Framework 2.0 for Windows Server 2003. .NET Framework 2.0 is installed when installing and configuring the operating systems in accordance with the Evaluated Configuration guidance provided in this document.
- Microsoft Management Console (MMC) 3.0 for Windows Server 2003 (installed by default on Windows Server 2003 with SP2).
- Microsoft Report Viewer 2005, available from the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=70410.
- Microsoft SQL Server 2005 database. The WSUS server setup software already includes Microsoft SQL Server 2005 Embedded Edition. Additionally, WSUS does not support direct access to data in a database and does not require the use of a full featured database such as Microsoft SQL Server 2005. Therefore, Microsoft SQL Server 2005 Embedded Edition is the database used in the IT environment supporting the TOE.

Follow the procedures below to install IIS 6.0, configure ASP.NET 2.0 for all Web sites, and install Microsoft Report Viewer 2005 on the servers that will be hosting WSUS 3.0.

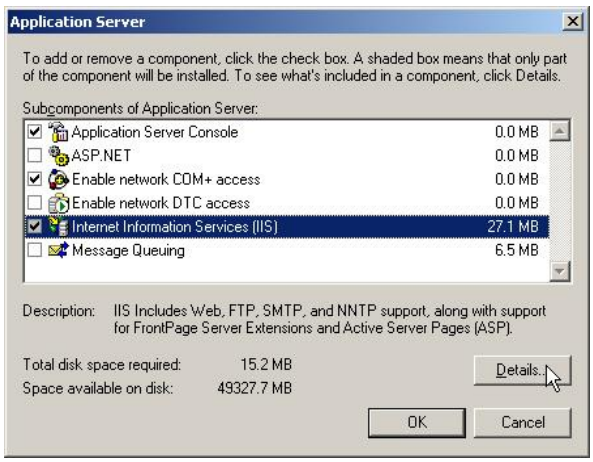
Install Internet Information Services (IIS) 6.0

1. Log on to the server designated to be the WSUS 3.0 server as an authorized administrator.
2. Click the **Start**, point to **Control Panel**, and select **Add or Remove Programs**. The Add or Remove Programs interface will appear.
3. Click the **Add/Remove Windows Components** button. The Windows Components Wizard will appear.
4. In the Windows Components Wizard, select **Application Server** and then click the **Details** button. The Application Server window will appear.



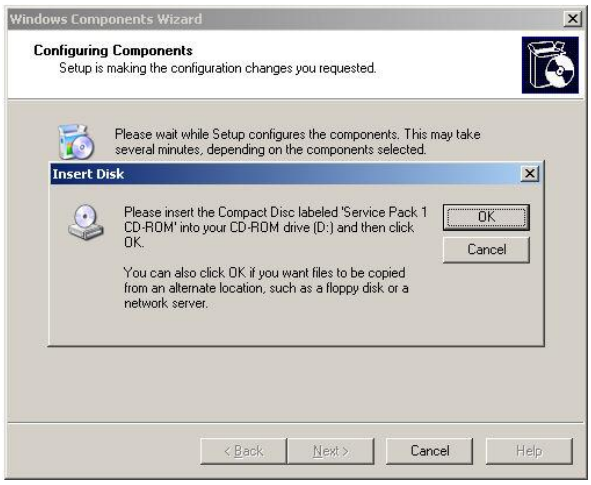
5. Click the checkbox next to **Internet Information Services (IIS)** to select it for installation (a check mark will appear in the checkbox), then click the **Details** button.

Note: Do not select ASP.NET from the Application Server interface. Doing so will install ASP.NET 1.1, which is not included in the TOE. Within the TOE, WSUS uses ASP.NET 2.0, which is configured in the procedures that follow.



6. Verify that **Common Files**, **Internet Information Services Manager**, and **World Wide Web Service** are selected for installation. Click **OK** on the Internet Information Services (IIS) interface, click **OK** on the Application Server interface, then click **Next** on the **Windows Component Wizard**.

7. If the Windows Server 2003 installation disk is not in the CD-ROM drive, a message will appear asking that it be inserted. Insert the installation disk for Windows Server 2003 in the CD-ROM drive to allow the IIS installation to continue.



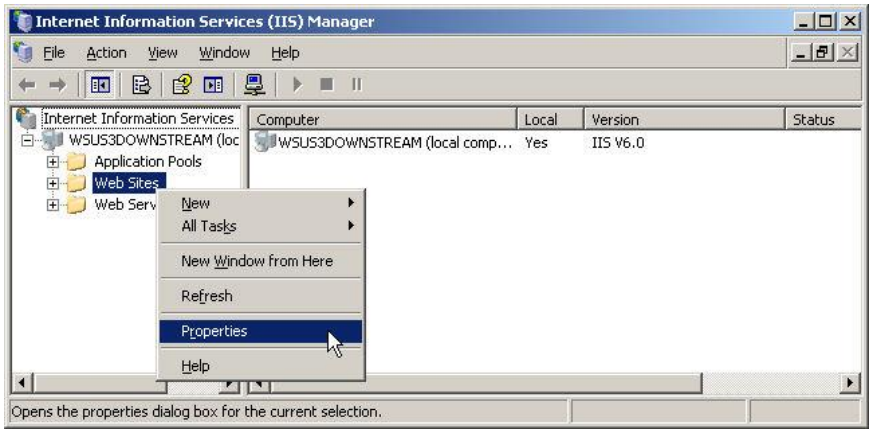
8. When the installation process is complete, click **Finish** on the Windows Component Wizard.

9. Close the Add or Remove Programs interface.
10. Proceed to Configure the IIS Web sites to use ASP,NET 2.0.

Configure IIS Web sites to use ASP.NET 2.0

Continue from the procedures above to ensure that Web sites hosted by IIS are configured to support ASP.NET 2.0.

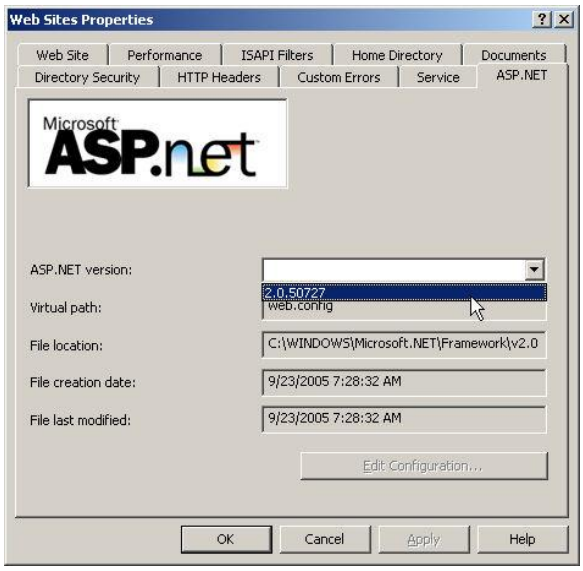
1. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
2. Expand the local computer node, then right click on the **Web Sites** folder and select **Properties**.



3. Click on the **ASP.NET** tab of the Web Sites Properties interface to select it.

4. Select **2.0.50727** from the ASP.NET version drop down menu then click **OK**. This will ensure that the setting requiring the use of ASP.NET 2.0 is automatically inherited by all Web sites created under the Web Sites folder of IIS.

Note: The WSUS 3.0 installer program will automatically register and allow the ASP.NET 2.0 Web Service Extension as part of the WSUS 3.0 installation process.



5. Proceed to the Install Microsoft Report Viewer 2005.

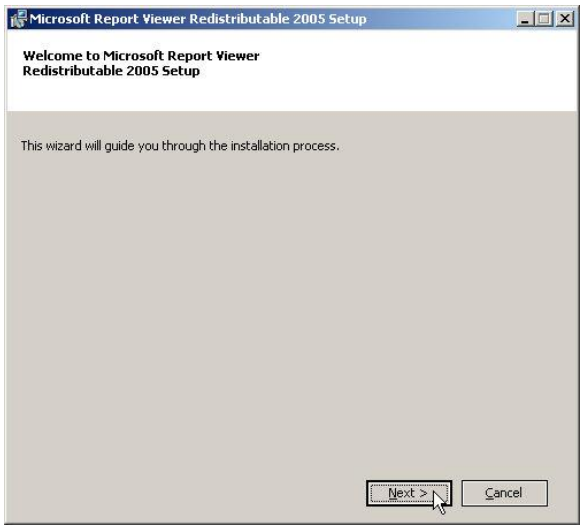
Install Microsoft Report Viewer 2005

The Microsoft Report Viewer 2005 is a prerequisite for the installation WSUS 3.0 and should be installed immediately after the installation of IIS. Use the procedures below to install Microsoft Report Viewer 2005 on the WSUS 3.0 host.

1. Load the media containing the Microsoft Report Viewer 2005 installation software.

2. Double-click the installer file, **ReportViewer.exe**. The Microsoft Report Viewer Redistributable 2005 Setup wizard will appear. Click **Next**.

Note: Microsoft Report Viewer Redistributable 2005 is available for download from the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=70410.



3. After reviewing the license agreement, check the box next to **I accept the terms of the License Agreement** and click **Install**.
4. The Report Viewer will install. Click **Finish** when the Setup Complete page of the wizard appears.

WSUS 3.0 Installation Procedures

Use the procedures in this section to install WSUS 3.0 with its own internal Microsoft SQL Server 2005 Embedded Edition database, storing updates locally, and using its own IIS Web site on port 8530. These procedures can be used to perform the basic WSUS 3.0 installation, which can then be configured to support architectures that include a single WSUS 3.0 server or multiple WSUS 3.0 servers, including upstream and downstream servers. Procedures for converting a WSUS 3.0 server into a downstream server are provided in Configure downstream WSUS 3.0 servers.

Follow the procedures in this order:

1. Install all single (stand-alone) or upstream WSUS 3.0 servers, following the procedures in Install WSUS 3.0.
2. Check the update synchronization settings on the external WSUS 3.0 server, and modify them if needed. Verify that the settings on the external WSUS 3.0 server and the WSUS 3.0 servers in the TOE match and make any necessary adjustments. The procedures are provided in Setting and verifying synchronization options on the external WSUS server.
3. Synchronize the external WSUS 3.0 server with the Microsoft Update Web site, if needed, in order to collect the necessary updates.
4. Export the updates and metadata from the external WSUS 3.0 servers and copy it to exportable media.
5. Import the updates and metadata to the appropriate WSUS 3.0 servers in the TOE.
6. Install downstream WSUS 3.0 servers, if needed, following the procedures in Install WSUS 3.0 and in the Configure downstream WSUS 3.0 servers section of this document.
7. Synchronize the downstream WSUS 3.0 servers with their upstream server.

Install WSUS 3.0

Follow the procedures below to install all WSUS 3.0 servers in the TOE. In an architecture with multiple WSUS 3.0 servers it is recommended that the upstream servers be installed and configured first. After installing and configuring the upstream servers, the downstream servers can be installed and set to synchronize with the upstream servers.

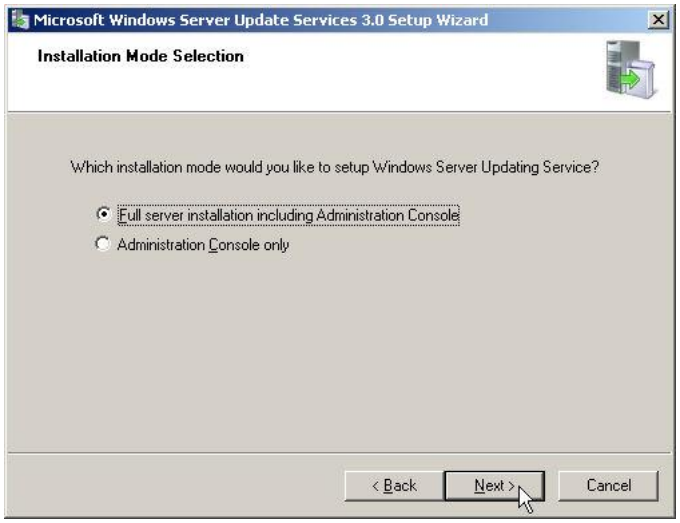
1. Log on using as a member of the local Administrators group.
2. Double-click the installer file (**WSUSSetupx86.exe** for the 32-bit executable or **WSUSSetupx64.exe** for the 64-bit executable).

Note: Windows Server Update Services 3.0 is available for download through the Microsoft Web site for Windows Server Update Services at http://go.microsoft.com/fwlink/?LinkId=47374.

---

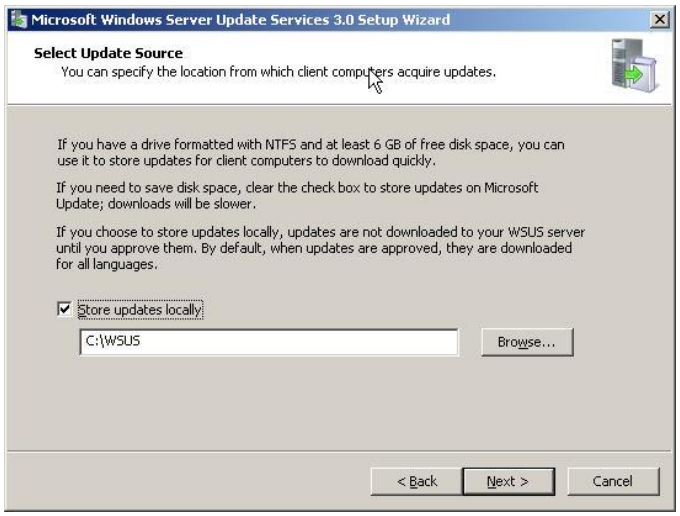
3. On the **Welcome** page of the Microsoft Windows Server Update Services 3.0 Setup Wizard, click **Next**.

4. Click the radio button for **Full server installation including Administration Console** and click **Next**.

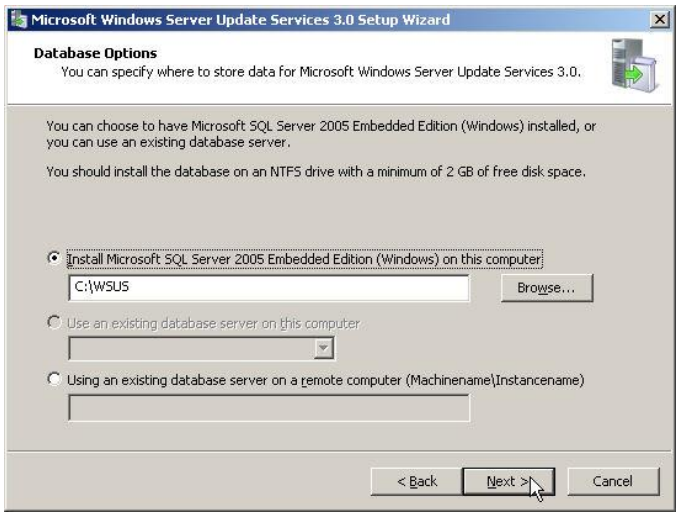


5. Read the terms of the license agreement carefully, click the radio button for **I accept the terms of the License Agreement**, and then click **Next**.

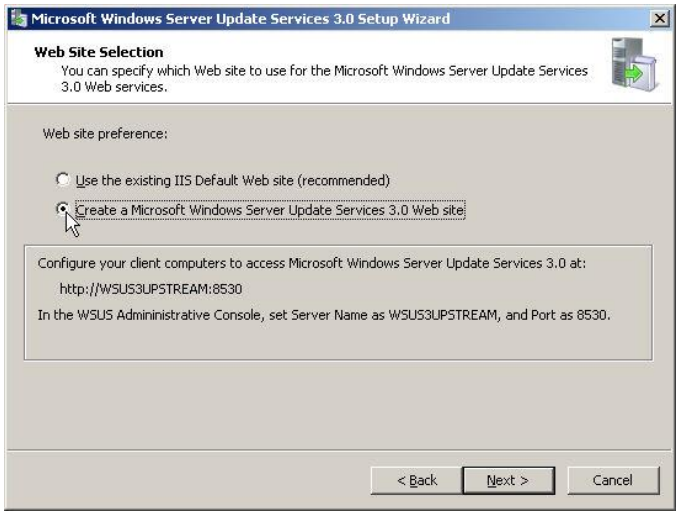
6. On the **Select Update Source** page, specify where clients get updates. If the **Store updates locally** check box is selected, updates are stored on the WSUS server and a location in the file system to store updates will need to be selected. By default, if there are more than one drives or partitions in the computer, the Wizard will automatically avoid using the system partition by selecting an alternate drive or partition. Keep the default options or change the location as needed, and then click **Next**.



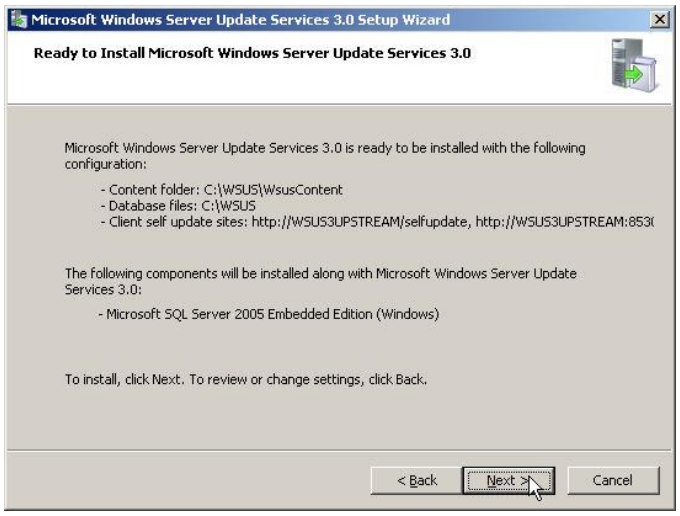
7. On the **Database Options** page, select the software used to manage the WSUS database. By default, WSUS Setup offers to install Microsoft SQL Server 2005 Embedded Edition in the same folder location specified in the **Select Update Source** page from the previous step. Microsoft SQL Server 2005 Embedded Edition is the database used in the IT environment supporting the TOE. Keep the default options, and click **Next**.



8. On the **Web Site Selection** page, specify the Web site that WSUS 3.0 will use. If other Web sites exist or will be installed on this host, it is best to select **Create a Microsoft Windows Server Update Services Web site** radio button to create a separate Web site for WSUS. In the TOE, a separate Web site is selected for WSUS 3.0. As noted in the Web Site Selection page of the Wizard, when WSUS is installed on its own site, clients must be configured to access it via port 8530. Click **Next**.



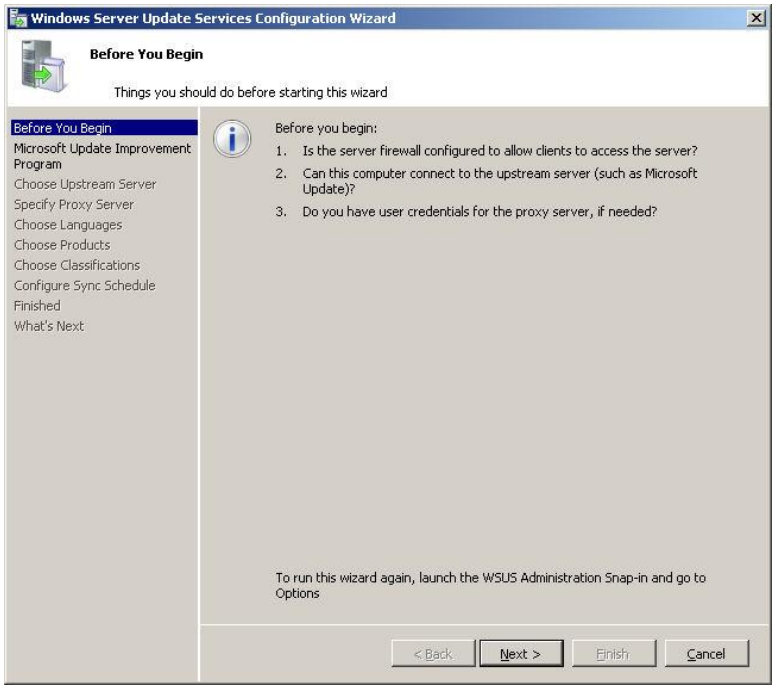
9. On the **Ready to Install Windows Server Update Services** page, review the selections and click **Next**. The installation of WSUS will begin.



10. If the final page of the wizard confirms that WSUS installation was successfully completed, click **Finish**.

11. A Windows Server Update Services Configuration Wizard will appear. If this is the only server in the current TOE architecture, or if it is to be an upstream server with one or more downstream servers, click **Cancel**.

    - If this WSUS server is to be configured as the only WSUS 3.0 server or as an upstream server within a network that is disconnected from the Internet, such as the TOE environment, proceed to Importing updates to WSUS 3.0 servers within a disconnected network.
    - If this WSUS server is to be configured as a downstream server, continue to Configure downstream WSUS 3.0 servers.



Importing updates to WSUS 3.0 servers within a disconnected network

Since the TOE is disconnected from the Internet, it is necessary to export updates and metadata from a WSUS 3.0 server that is external to the TOE and has access to the Microsoft Update Web site via the Internet. The external WSUS 3.0 server is synchronized with the Microsoft Update Web site in order to download the updates that are to be distributed to computers within the TOE. Once exported from the external WSUS 3.0 server, the updates and corresponding metadata are imported to WSUS 3.0 servers within the TOE and their distribution to WSUS clients within the TOE can be managed.

There are three steps to exporting and then importing updates:

12. 1. Make sure that the options for express installation files and update languages on the external WSUS 3.0 server are compatible with the settings on the WSUS 3.0 servers within the TOE. This ensures that the proper updates are collected for distribution.

13. 2. Backup the updates from the file system of the external WSUS server and then restore those updates to the file system of the WSUS 3.0 servers within the TOE. This would be to the upstream or single WSUS 3.0 servers within the TOE. Downstream WSUS 3.0 servers within the TOE will obtain their updates from the upstream WSUS 3.0 server.

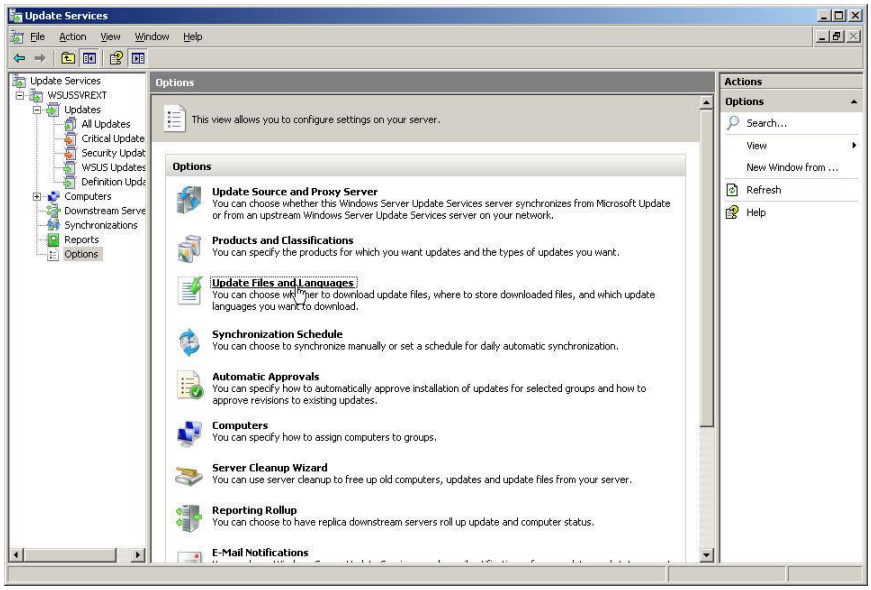
Note: When restoring updates from an externa WSUS server to a WSUS server within the TOE, take note of the location of the **WSUSContent** folder on each computer. The default WSUSContent folder location on the external WSUS server may not be the same as what was established on WSUS servers within the TOE. If it is different, use the Advanced button on the Restore Wizard to point it to the proper restore location.

14. 3. Export update metadata from the database of the external WSUS 3.0 server, and import it into the database of the upstream or single WSUS 3.0 servers within the TOE.

Setting and verifying synchronization options on the external and internal WSUS servers

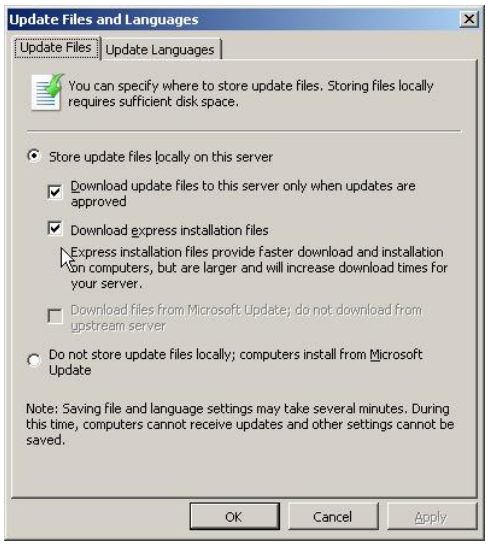
The external WSUS 3.0 server is a server that resides outside of the TOE and has a network connection to the internet. WSUS 3.0 must already be installed on this server. It will be necessary to log on to the external WSUS 3.0 server to verify or modify the synchronization options for express installation files and update languages to ensure they match the settings on the WSUS 3.0 servers within the TOE.

1. Logon to the external WSUS 3.0 server as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Microsoft Windows Server Update Services 3.0**.
3. Click the **Options** node in the left hand pane, and then click the **Update Files and Languages** link in the center pane.



4. In the **Update Files** tab of the Update Files and Languages interface, check the settings for **Download express installation files**. Click **Apply**.

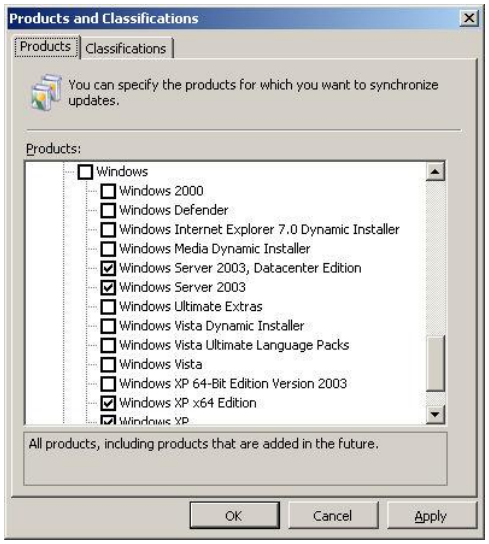
Note: The **Download update files to this server only when updates are approved** setting simply means that files will not be downloaded until they are approved by the upstream server. In the case of the external WSUS 3.0 server, its upstream server is the Microsoft server hosting Microsoft Update Web site. Within the TOE, this has no effect on the upstream servers since they cannot contact the Microsoft Update Web site, but when the downstream WSUS 3.0 servers use this setting, they will only download updates from the upstream WSUS 3.0 server in the TOE after the updates are approved on the upstream server.



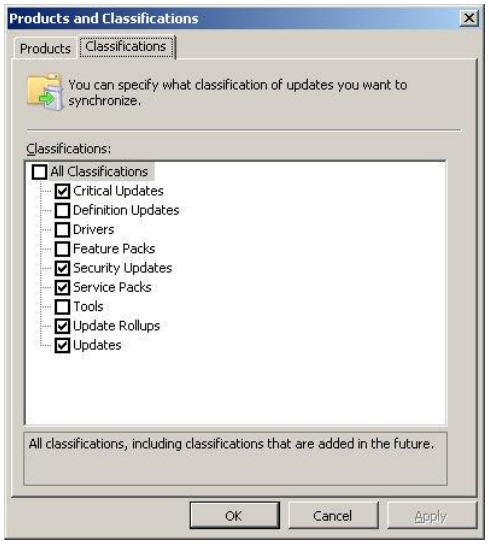
5. In the **Update Languages** tab of the Update Files and Languages interface, make sure the **Download updates only in these languages** radio button is selected and that only the **English** language check box is checked. Click **OK**.

Note: Within the TOE, only English language updates are used.

6. If the external WSUS 3.0 server is set up to only serve the TOE, click the **Products and Classifications** link in the center pane of the Update Services snap-in.
7. In the **Products** tab of the Products and Classifications interface, uncheck any product that is not an operating system within the TOE. Scroll down to the **Windows** section and check to the boxes next to all of the operating system versions within the TOE.



8. In the **Classifications** tab of the Products and Classifications interface, make sure that the **Critical Updates**, **Security Updates**, **Service Packs**, **Update Rollups**, and **Updates** checkboxes are checked. Click **OK**.

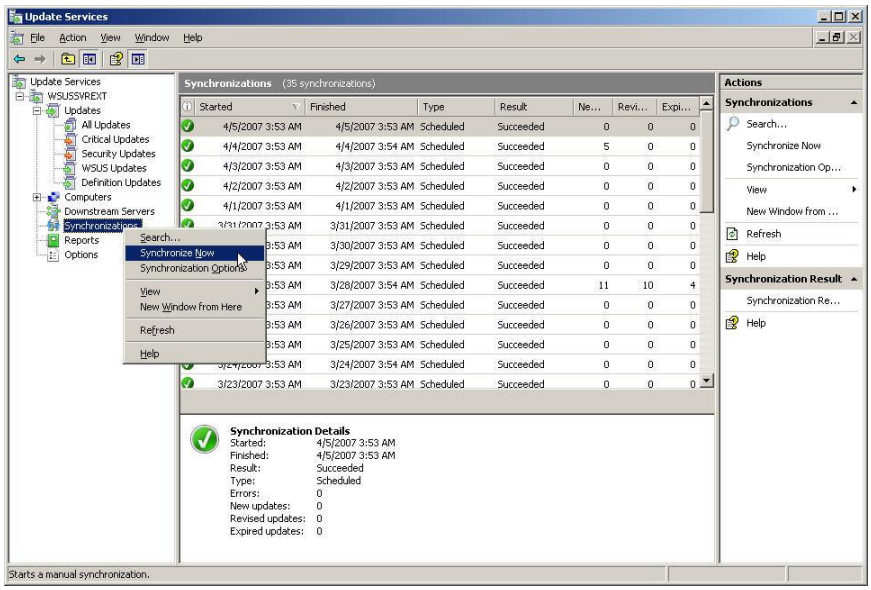


9. Repeat the steps above on the WSUS 3.0 servers within the TOE to ensure their settings match with those of the external WSUS 3.0 server.

Synchronizing the external WSUS 3.0 server with the Microsoft Update Web site

After checking the option settings discussed above, it may be necessary to download the necessary updates to the external WSUS 3.0 server from the Microsoft Update Web site, if the updates have not already been downloaded. Follow the procedures below to synchronize the external WSUS 3.0 server with the Microsoft Update Web site in order to download the complete set of updates that can be distributed within the TOE.

1. Logon to the external WSUS 3.0 server as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Microsoft Windows Server Update Services 3.0**.
3. Right-click on the **Synchronizations** node and select **Synchronize Now**.



4. The WSUS server will contact the Microsoft Update site and will begin downloading new updates, if there are any available.

Importing and Exporting Updates between the External and Internal WSUS 3.0 Servers

As stated earlier, managing WSUS 3.0 on a network that is disconnected from the Internet, such as the TOE, involves exporting updates and metadata from a WSUS 3.0 server that has a connection to the Internet and then importing all that information into the WSUS 3.0 server on the disconnected network. Follow the procedures bellow to export the updates and metadata from the external WSUS 3.0 server and import them to the WSUS 3.0 servers within the TOE. Downstream WSUS 3.0 servers within the TOE will get their updates from their respective upstream servers and do not need to have the updates imported from the external WSUS 3.0 server.

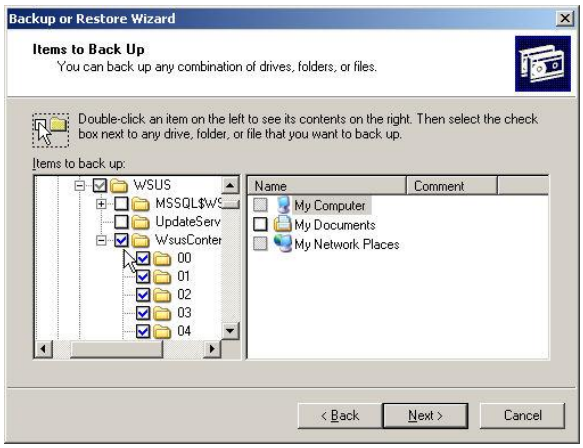
Exporting the update data from the external WSUS 3.0 server

Use the following procedures to create a backup copy of the updates from the file system of the export server. This backup will later be restored onto the file system of the WSUS 3.0 upstream and standalone servers within the TOE. By default, updates are stored in the following folder:

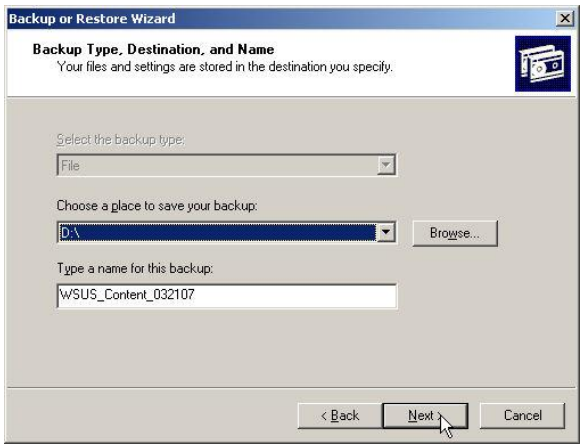
WSUSInstallationDrive:\WSUS\WSUSContent\

1. Log on to the external WSUS 3.0 server as an authorized administrator.
2. Click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **ntbackup**.
4. Click **Next** on the Backup or Restore Wizard.

5. Select the **Back up files and settings** radio button and click **Next**.
6. Select the **Let me choose what to back up** radio button and click **Next.**
7. In the Items to Back Up page of the Wizard, expand the node representing the drive location of the WSUS content folder. Expand the **WSUS** folder and check the box next to the **WsusContent** folder to select it and all of its contents. Click **Next**.

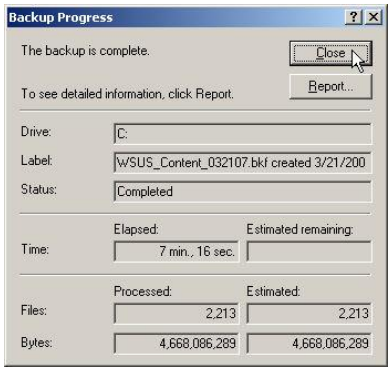


8. Choose a storage location and enter a name for the backup file. Click **Next**.



9. Review the backup settings. If everything is correct, click **Finish**.

10. The Backup Progress interface will appear indicating the backup progress and an estimated time for completion. When the backup is complete, click **Close**.



11. Continue to the procedures for "Exporting update metadata from the external WSUS 3.0 server."

Exporting update metadata from the external WSUS 3.0 server

The update metadata must be exported from the external WSUS 3.0 server so that it can be imported to the WSUS 3.0 servers in the TOE in order to manage the imported updates. The WSUSUTIL.EXE command line tool is used to import and export the metadata. The WSUSutil.exe command can be found in the Tools subfolder where the WSUS 3.0 program files are installed (C:\Program Files\Update Services\Tools). Only members of the local Administrators group on the WSUS 3.0 server can export or import metadata; both operations can only be run from the WSUS 3.0 server itself.

Note: During the import or export process, the Update Service is shut down.

1. Open a command prompt on the external WSUS server. Click **Start**, click **Run**, type **cmd**, and the click **OK**.
2. Change directories to the folder that contains **WSUSutil.exe**.
3. Type and enter the following: **wsusutil export *packagename logfile.*** That is, *wsusutil* followed by the *export* command, the name of an export *.cab* file, a space, and the name of a log file. For example:

   wsusutil export wsusmetadata.cab export.log

Note: The package (.cab file) and log file name must be unique. WSUSutil.exe creates these two files as it exports metadata from the WSUS 3.0 database.

4. Copy the update backup file and the metadata .cab file to removable media for export to the WSUS 3.0 servers within the TOE.

Importing the update data to WSUS 3.0 servers within the TOE

When the exported update backup file and the metadata .cab file are copied to a WSUS 3.0 server in the TOE, the folder structure must be maintained for all folders under \WSUSContent. Verify that the WSUS 3.0 server in the TOE have the same location set for the WSUSContent folder; this designation is made during the WSUS setup process.

1. Within the TOE, log on to the WSUS 3.0 server as a member of the local Administrators group.
2. Load the removable media containing the update backup and metadata .cab files that were exported from the external WSUS 3.0 server.
3. Click **Start**, and then click **Run**.
4. In the **Run** dialog box, type **ntbackup**.
5. Click **Next** on the Backup or Restore Wizard.
6. Select the **Restore files and settings** radio button and click **Next**.
7. On the What to Restore page, click **Browse** to search for the location of the updates backup file. The Open Backup File interface will appear. Type in the path of the backup file in the **Open** text box, or click **Browse** to search for the location, and then click **OK**.
8. Expand the **File** node in the Items to restore pane of the Wizard and traverse the file structure to find the **WsusContent** folder. Check the box next to the **WsusContent** folder to select it for restoration to the local host. Click **Next**.
9. Review the restore settings.
   - If everything is correct, click **Finish**.
   - If the **Restore to** location needs to be changed, click the **Advanced** button. On the Where to Restore page, select **Alternate location** from the drop-down menu, browse to find the alternate resotore location on the local host, and then click **Next**. Choose an existing file replacement option and click **Next**. Leave the defaults and click **Next** on the Advanced Restore Options page. Click **Finish**.
10. The Restore Progress interface will appear indicating the restoration progress and an estimated time for completion. When the restoration is complete, click **Close**.
11. Continue to the procedures for "Importing update metadata to the WSUS 3.0 servers within the TOE."

Importing update metadata to the WSUS 3.0 servers within the TOE

Updates should be imported to the file system of the WSUS 3.0 servers within the TOE before the metadata is imported. If WSUS 3.0 finds metadata for an update that is not in the file system, the WSUS 3.0 console shows that the update failed to be downloaded. This type of problem can be corrected by copying the missing update(s) onto the file system of the TOE server and then again attempting to deploy the update.

Only members of the local Administrators group on the WSUS 3.0 server can export or import metadata; both operations can only be run from the WSUS 3.0 server itself.

Note: During the import or export process, the Update Service is shut down.

1. Open a command prompt on the WSUS server. Click **Start**, click **Run**, type **cmd**, and the click **OK**.
2. Change directories to the folder that contains **WSUSutil.exe** (C:\Program Files\Update Services\Tools).
3. Type and enter the following: **wsusutil import *packagename logfile.*** That is, *wsusutil* followed by the *import* command, the name of an exported *.cab* file, a space, and the name of a log file. For example:

   wsusutil import wsusmetadata.cab export.log

   Note: The exported metadata .cab file can be copied from the removable media to the folder that contains **WSUSutil.exe** or the command above can be modified to include the path of the metadata file.
4. WSUSutil.exe imports the metadata from the external WSUS 3.0 server and creates a log file of the operation.

   Note: It can take from 1 to 4 hours for the database to validate content that has just been imported. Please be patient.

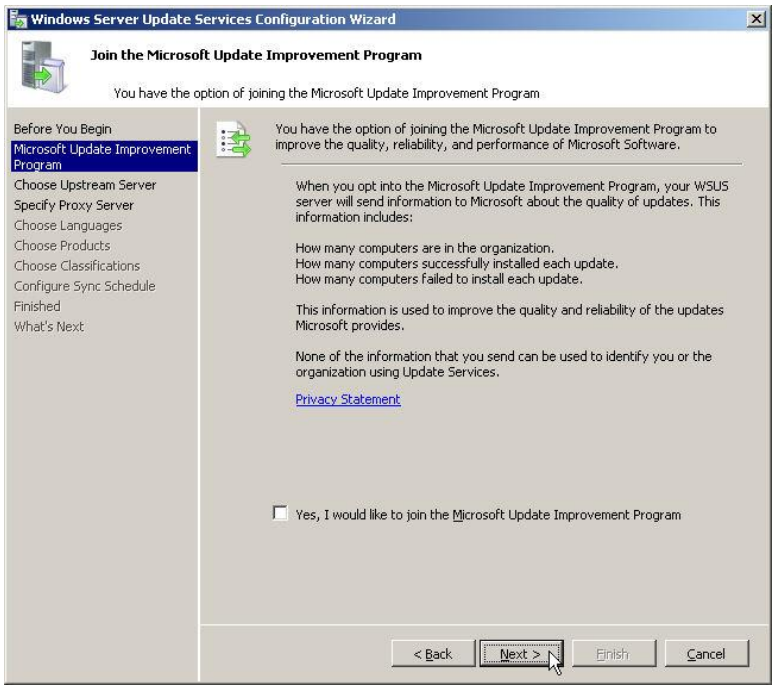
Configure downstream WSUS 3.0 servers

Install a downstream WSUS 3.0 server by following the procedures provided above, in the Install WSUS 3.0 section of this document. Then continue the configuration of the downstream WSUS 3.0 server by following the instructions of the Windows Server Update Services Configuration Wizard, as indicated in the procedures below.

1. After clicking **Finish** on the final page of the Microsoft Windows Server Update Services 3.0 Setup Wizard, the Windows Server Update Services Configuration Wizard will appear.

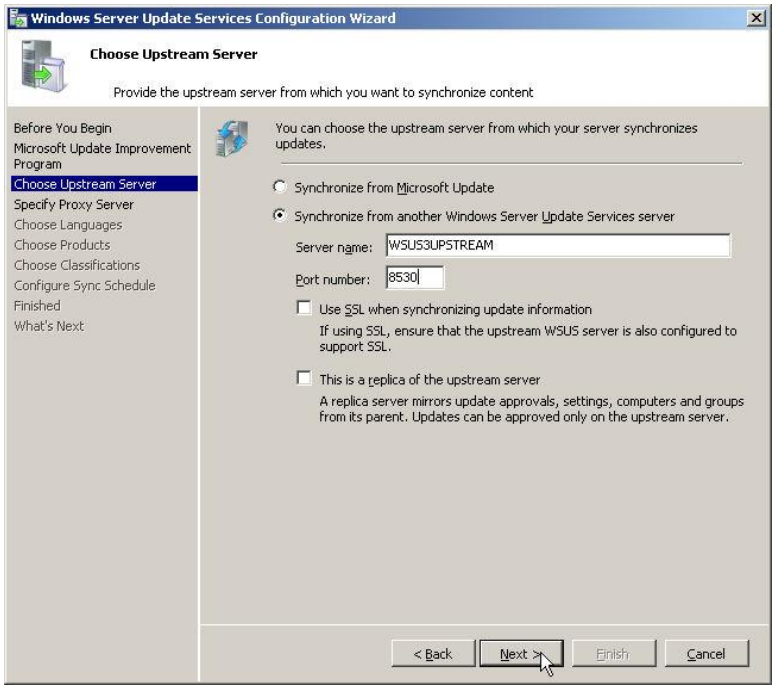
   Note: If the Windows Server Update Services Configuration Wizard has been closed, it may be opened again by clicking on the **WSUS Server Configuration Wizard** link in the **Options** node of the Update Services Snap-in. Click **Start**, point to **Administrative Tools**, and select **Windows Server Update Services 3.0**. Expand the WSUS server node if necessary, click on the **Options** node on the left-hand pane, and then click the **WSUS Server Configuration Wizard** link in the center pane.
2. Click **Next** on the Windows Server Update Services Configuration Wizard.
3. Remove the check mark from the **Yes, I would like to join Microsoft Update Improvement Program** check box. Click **Next**.

Note: The TOE is a closed environment, with no access to the Internet.

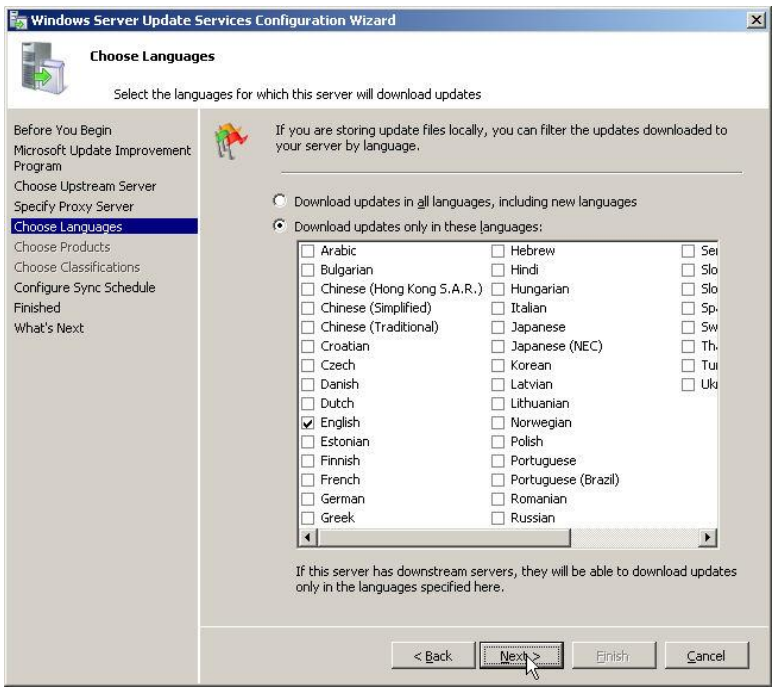


4. Select the **Synchronize from another Windows Server Update Services server** radio button. Then enter the name of the upstream server and the port number (8530) as shown in the screenshot below.

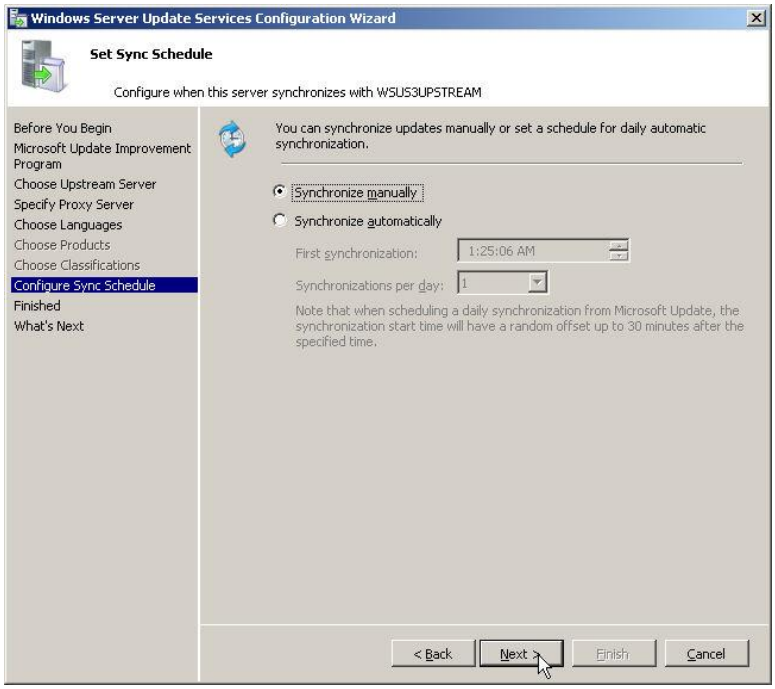
   - The use of SSL will be documented later, after the base TOE configuration has been configured and tested.
   - If the **This is a replica of the upstream server** check box is checked, this WSUS 3.0 server will be configured as another upstream WSUS 3.0 server that mirror the original server for recovery purposes. Do not select this option for this installation.



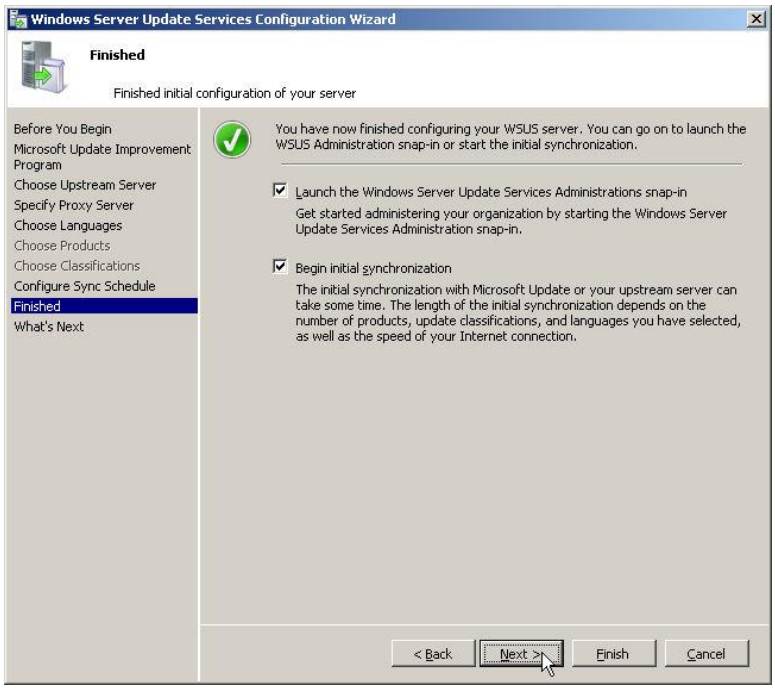
5. Click **Next**.
6. The use of proxy servers for WSUS 3.0 is not included in the TOE, therefore do not make any selections on the Specify Proxy Server page of the Wizard. Click **Next**.
7. Click the **Start Connecting** button on the Connect to Upstream Server page of the Wizard. The Wizard will try to establish contact with the upstream WSUS 3.0 server. When this process completes the **Next** button will become active. Click the **Next** button when ready.
8. On the Choose Languages page of the Wizard, verify that the language settings inherited from the upstream server are correct. For the TOE, **English** should be the only language selected. Click **Next**.



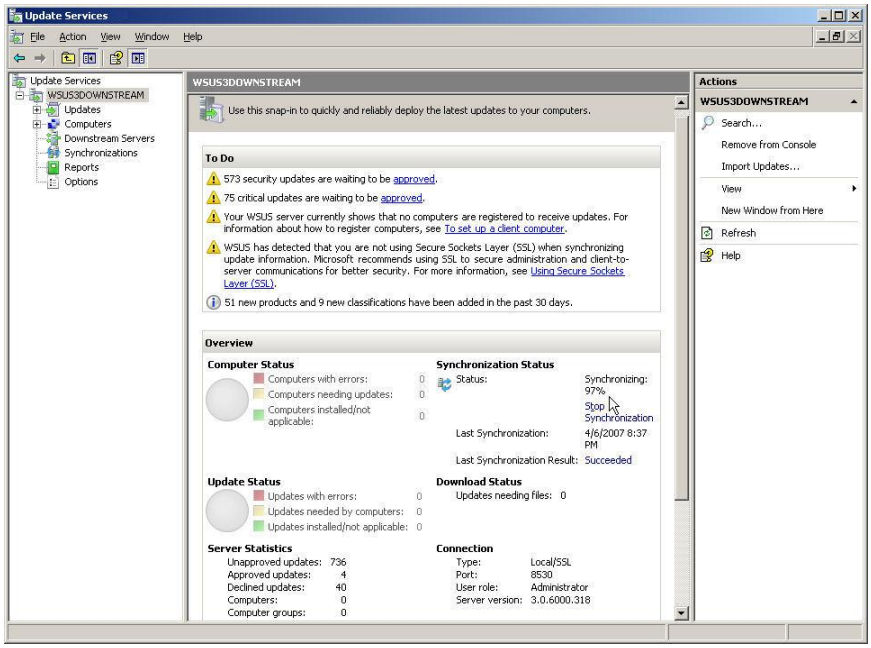
9. On the Set Sync Schedule page of the Wizard, select the method for synchronization and then click **Next.**
   - Select the **Synchronize manually** radio button to allow an administrator the ability to synchronize the upstream and downstream servers manually, as needed.
   - Select the **Synchronize automatically** radio button and then the **First synchronization** time and number of **Synchronizations per day** to allow the downstream server to automatically contact the upstream server and download updates without administrator intervention.



10. On the Finish page of the Wizard, keep the defaults and click **Next**.



11. Click **Finish** on the What's Next page of the Wizard.
12. The Update Services snap-in will appear, showing the current status of updates. It may take a few minutes for the update status information to be updated as the downstream server synchronizes with the upstream server. This progress can be observed by viewing the **Synchronization Status** as it updates.



13. To verify the downstream server's relation to the upstream server, click the **Downstream Servers** node on the left-hand pane of the Update Services snap-in. It may take some time for this information to appear on the downstream server (it may appear on the upstream server first).

Once the initial synchronization is complete, the downstream server is ready to be configured to support client computers. This is first accomplished by creating computer groups in the Update Services snap-in and configuring Windows Update group policy settings to define the Automatic Updates policies for WSUS 3.0 clients in the TOE. Continue to Initial WSUS 3.0 Configuration Procedures.

Initial WSUS 3.0 Configuration Procedures

To configure WSUS for initial use within the TOE, perform the following procedures in the order indicated:

1. Create computer groups in WSUS 3.0. Computer groups must be created regardless of the method used to assign computers to groups.
2. Specify method of assigning computers to groups. Methods include manual assignment via server-side targeting or automatic assignment via client-side targeting.
3. Configure Automatic Updates settings on WSUS 3.0 clients. Within the TOE, Automatic Updates settings are managed by configuring domain-level Group Policies for computers within a domain, or local Group Policies on computers that are not in a domain.
4. Move computers to computer groups in WSUS 3.0.

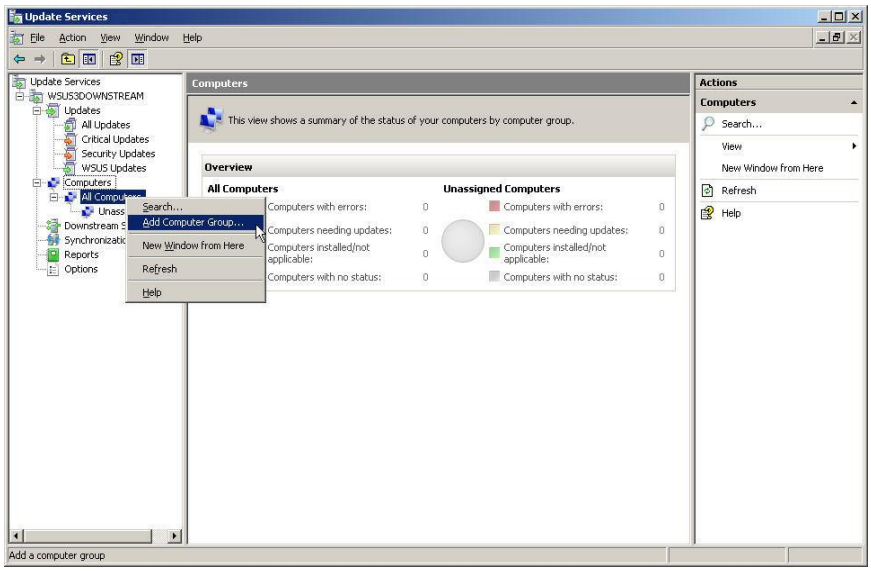
Procedures for day-to-day management of WSUS 3.0 are available in the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

Create computer groups in WSUS 3.0

To manage WSUS 3.0 clients, the client computers must be assigned to computers groups. Computer groups allow the targeting of updates to specific groups of computers. There are two

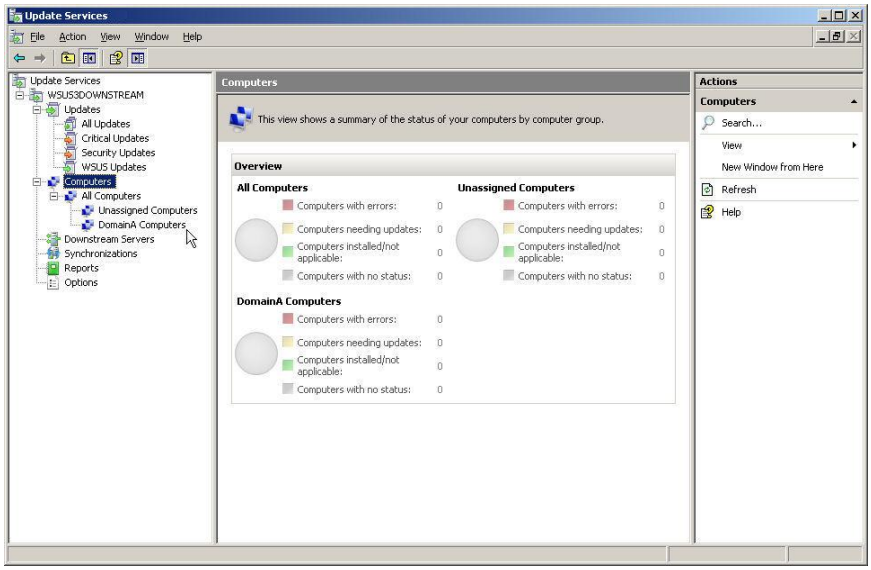
default computer groups: **All Computers** and **Unassigned Computers**. By default, when a client computer contacts the WSUS 3.0 server, it is automatically added to both default computer groups if there is no client-side targeting. An administrator then moves the computer to an appropriate group. If server-side targeting is configured, the first time a client computer contacts the WSUS 3.0 server it will automatically be added to the **All Computers** group as well as the target group specified in by the group policy that is being used by the client. Follow the procedures below to create the necessary WSUS 3.0 computer groups within the TOE.

5. On the left-hand pane of the Update Services snap-in, expand the **Computers** node and then right-click on the **All Computers** node and select **Add Computer Group**.



6. In the Add Computer Group interface, enter a name for the new computer group in the **Name** text box and click **Add**.

7. The new computer group will appear in the right-hand pane of the Update Services snap-in.



8. Continue to complete the next step to Specify the method of assigning computers to groups.

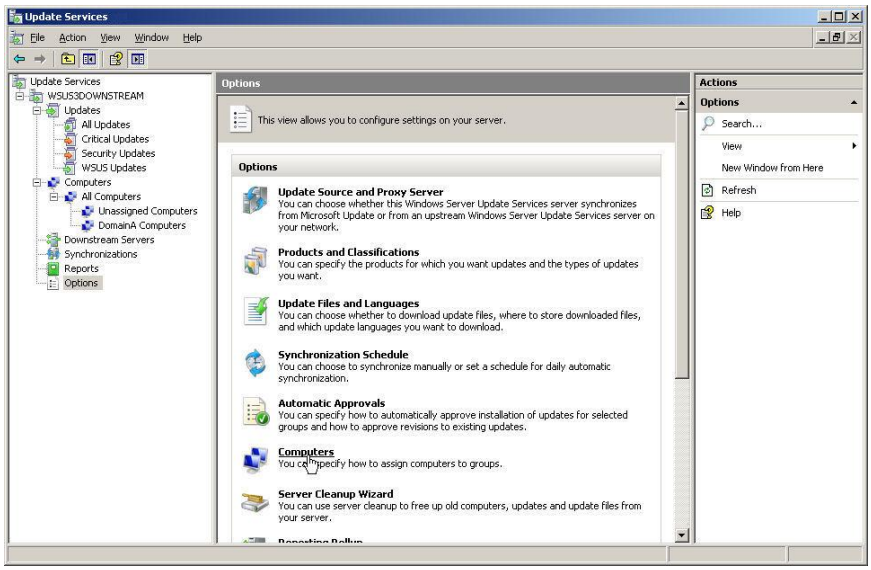
Specify the method of assigning computers to groups

Determine the method that will be used to assign computers to groups for the current deployment.

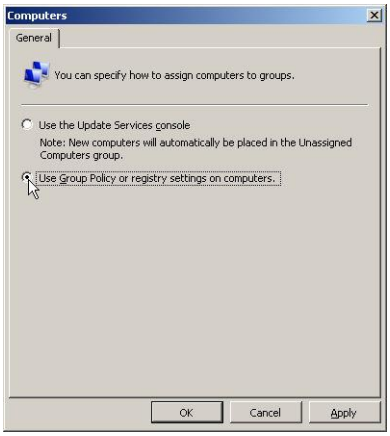
- Server-side targeting of WSUS 3.0 client computers to computer groups requires an administrator to manually move computers to specific computer groups.
- Client-Side targeting allows for automatic assignment of WSUS 3.0 client computers to computer to computer groups defined in a Group Policy.

Follow the procedures below to specify the method of assigning computers to groups for the current WSUS 3.0 implementation.

1. In the left-hand pane of the Update Services snap-in, select the **Options** node.
2. In the center pane of the Update Services snap-in, click on the **Computers** link.



3. On the Computers interface, select one of the following options:
   - **Use the Update Services console**. Select this option to manually assign computers through the Update Services snap-in.
   - **Use Group Policy or registry settings on computers**. Select this option to create groups and assign computers using Group Policy.



4. Click **OK**.
5. Continue to complete the next step to Configure Automatic Updates settings on WSUS 3.0 clients.

Configure Automatic Updates settings on WSUS 3.0 clients

There are two methods to configure Automatic Updates on computers in order to allow the management of updates for those computers through a WSUS 3.0 server:

- Configure Automatic Updates via Group Policy. This method involves configuring domain-level Group Policies for computers within a domain, or local Group Policies on computers that are not in a domain.
- Configure Automatic Updates locally by modifying registry settings on the local computer. This method involves using the Registry Editor and is not used in the TOE. Configuring Automatic Updates via a local Group Policy has the same effect as using the Registry Editor.

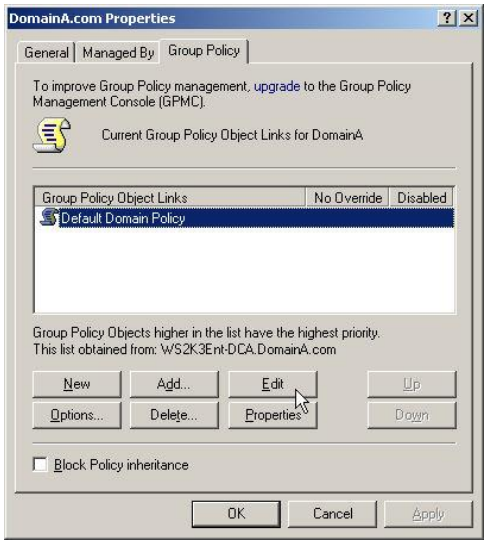
Follow the procedures below to configure Automatic Updates settings for WSUS 3.0 via a Group Policy object (GPO).

Open a GPO in Active Directory

Use the procedures below to open a domain-level GPO used to manage computers within an Active Directory domain.

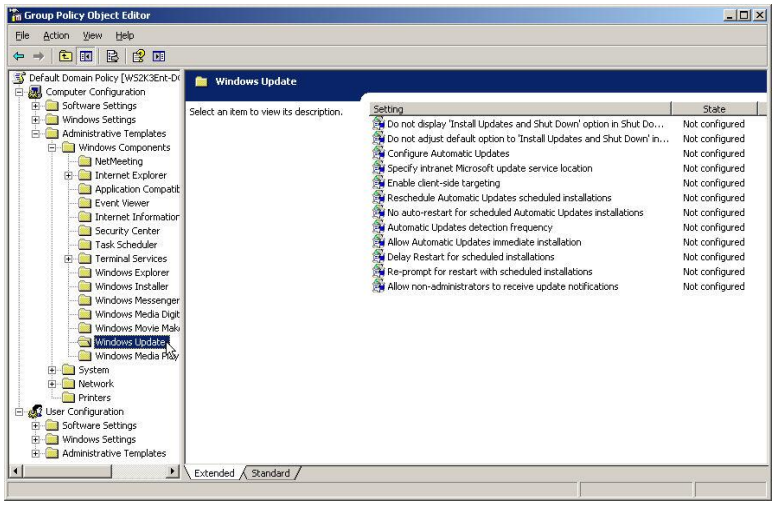
1. Log on to the domain controller as an authorized domain administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Active Directory Users and Computers**. The Active Directory Users and Computers interface will appear.
3. Right-click on the domain node and select **Properties**. The domain Properties interface will appear.

4. Click the **Group Policy** tab. Select the **Default Domain Policy** and click **Edit**. This will open a Group Policy Object Editor interface for a GPO that is applicable to all computers within the domain.



Note: Group policies can also be edited for computers in specific organizational units (OUs). This allows the application of unique Automatic Update policies to computers in specific domain OUs. Procedures for creating new OUs are available in the *Windows Server 2003 with Service Pack 2 Evaluated Configuration Administrator's Guide, Version 3.0*.

5. Under the Computer Configuration node, expand the **Administrative Templates** folder.
6. Expand the **Windows Components** folder and click **Windows Update** to select it. The Windows Update policy settings will be displayed in the right-hand pane.



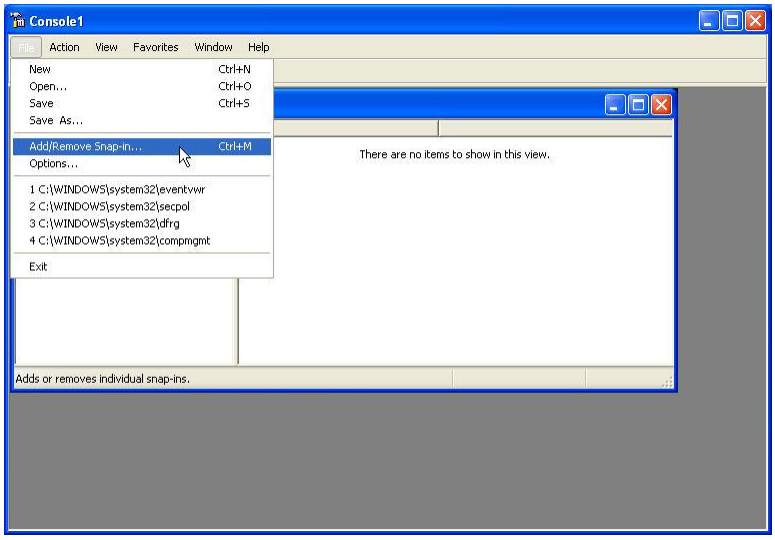
7. Continue with the procedures to Configure Automatic Updates Group Policy settings.

Open a local GPO on a WSUS 3.0 client computer

Use the procedures below to open a local GPO on a WSUS 3.0 client computer that is not a member of an Active Directory domain.

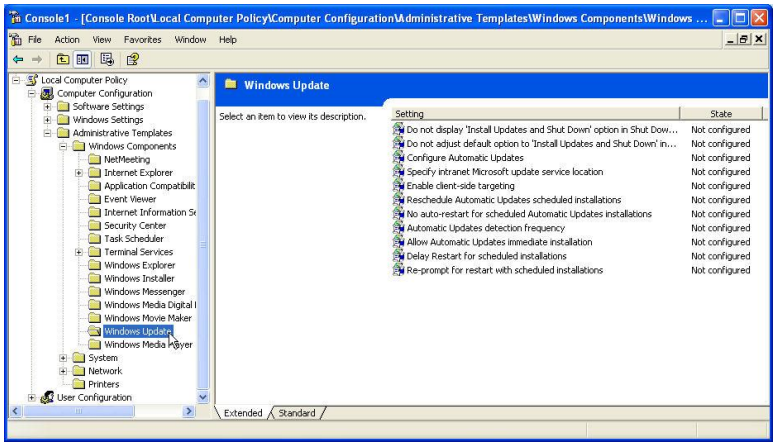
1. Log on to the WSUS 3.0 client computer as a member of the local Administrators group.

2. Click **Start** and select **Run**.
3. In the **Open** text box of the Run interface, type **mmc**. Click **OK**. An MMC console will appear.
4. From the **File** menu, select **Add/Remove Snap-in**.



5. In the Add/Remove Snap-in interface, click **Add**.
6. In the Add Standalone Snap-in interface, select **Group Policy Object Editor** and then click **Add**.

7. Click **Finish** on the Select Group Policy Object Wizard, click **Close** on the Add Standalone Snap-in interface, and then click **OK** on the Add/Remove Snap-in interface.
8. Under Console Root, expand the **Local Computer Policy** node.
9. Expand the **Computer Configuration** node, expand **Administrative Templates**, and then expand **Windows Components**.
10. Select the **Windows Update** folder. The Windows Update policy settings will be displayed in the right-hand pane.



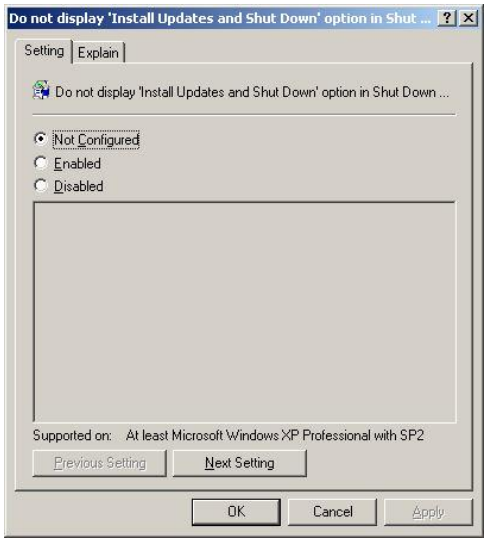
11. Continue to the procedures to Configure Automatic Updates Group Policy settings.

Configure Automatic Updates Group Policy settings

To configure an Automatic Updates Group Policy setting, double-click on the policy setting in the right-hand pane of the GPO interface. The **Configure Automatic Updates** and **Specify intranet Microsoft update service location** policy settings must be **Enabled** in the TOE. All other settings are configurable. Follow the guidance in the steps below to configure Automatic Updates Group Policy settings.

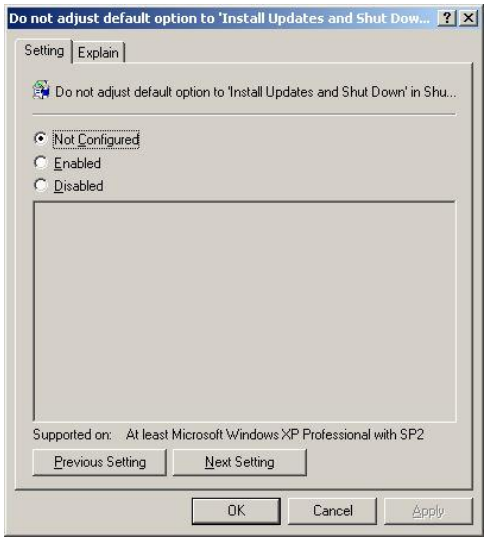
1. **Do not display "Install Updates and Shut Down" option in Shut Down Windows dialog box**. This policy setting allows the option to display the "**Install Updates and Shut Down**" option in the Shut Down Windows dialog box.

   - If this policy setting is **Enabled**, "**Install Updates and Shut Down**" will not appear as a choice in the Shut Down Windows dialog box, even if updates are available for installation when the user selects the Shut Down option in the Start menu.
   - If this policy setting is **Disabled** or **Not Configured**, the "**Install Updates and Shut Down**" option will be available in the Shut Down Windows dialog box if updates are available when the user selects the **Shut Down** option in the **Start** menu.



2. **Do not adjust default option to "Install Updates and Shut Down" in the Shut Down Windows dialog box**. This policy setting allows the option to set the "**Install Updates and Shut Down**" option is allowed as the default choice in the Shut Down Windows dialog.

   - If this policy setting is **Enabled**, the user's last shut down choice is the default option in the Shut Down Windows dialog box, regardless of whether the "**Install Updates and Shut Down**" option is available in the 'What do you want the computer to do?' list.
   - If this policy setting is **Disabled** or **Not Configured**, the "**Install Updates and Shut Down**" option will be the default option in the Shut Down Windows dialog box if updates are available for installation at the time the user selects the **Shut Down** option in the **Start** menu.



Note: This policy setting has no impact if the Computer Configuration\Administrative Templates\Windows Components\Windows Update\Do not display "**Install Updates and Shut Down**" option in Shut Down Windows dialog box policy setting is enabled.

3. **Configure Automatic Updates**. The settings for this policy specify how Automatic Updates is configured to work. Within the TOE, this setting must be **Enabled** With one of the options from the **Configure automatic updating** drop-down menu selected.

   - When this policy setting is **Enabled**, the following options can be selected:

     2-Notify for download and notify for install. This option is available from the **Configure automatic updating** drop-down menu and is used to notify a logged-on administrative user prior to the download and prior to the installation of the updates.

     3-Auto download and notify for install. This option is available from the **Configure automatic updating** drop-down menu and is used to automatically download updates and then notify a logged-on administrative user prior to installing the updates.

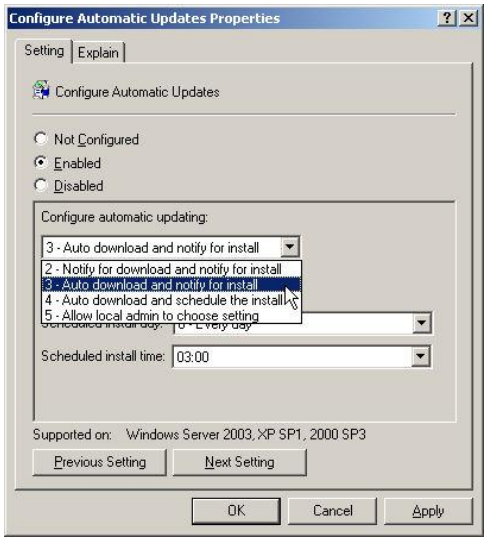
     4-Auto download and schedule the install. This option is available from the **Configure automatic updating** drop-down menu and is used to perform a scheduled installation if Automatic Updates is configured. The day and time must also be set for the recurring scheduled installation.

     5-Allow local admin to choose setting. This option is available from the **Configure automatic updating** drop-down menu and allows local administrators to use Automatic Updates in Control Panel to select a configuration option of their choice. For example, they can choose their own scheduled installation time. Local administrators are not allowed to disable Automatic Updates.

Scheduled install day. This option is used when option 4 above is selected from the **Configure automatic updating** drop-down menu. It allows installations to be scheduled daily or once a week, as selected from the drop-down menu.

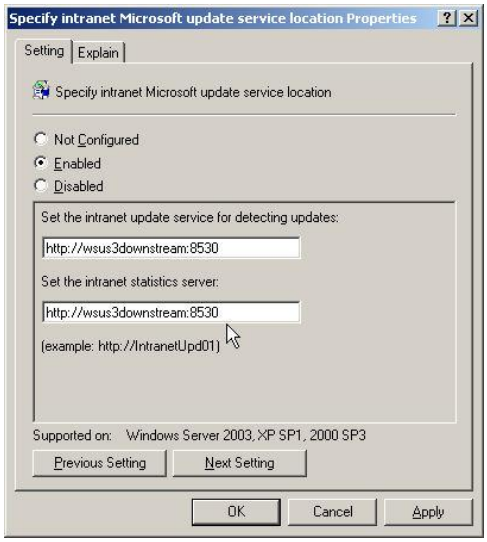
Scheduled install time. This option is used when option 4 above is selected from the **Configure automatic updating** drop-down menu. It is used with the **Scheduled install day** setting and allows the time of the installation to be selected, in hour increments.

- If this policy setting is **Disabled**, updates can only be downloaded manually from the Windows Update site. However, access to the Windows Update site is not possible in the closed environment of the TOE.
- If this policy setting is **Not Configured**, the use of Automatic Updates is not specified at the Group Policy level. However, members of the Administrators group can still configure Automatic Updates locally through the Control Panel interface.



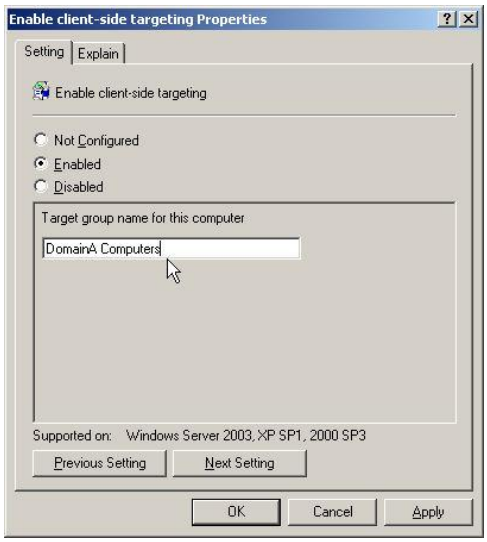
4. **Specify intranet Microsoft update service location**. This policy setting specifies the WSUS 3.0 server that Automatic Updates on WSUS client computers will contact for updates. This policy must be enabled in order for Automatic Updates to download updates from the WSUS 3.0 server and must be **Enabled** in the TOE.

   - When this policy setting is **Enabled**, the WSUS 3.0 client computer will contact the intranet update service site specified in the **Set the intranet update service for detecting updates** and **Set the intranet statistics server** text boxes. Enter the same site in both text boxes so that the server specified for updates is also used for reporting client events. Within the TOE, when WSUS 3.0 is hosted on its own Web site, include the port number (8530) with the site entries. For example, type **http://servername:8530** in both text boxes. Both URLs are required. In an environment where there are downstream servers, this would typically be an entry for one of the downstream WSUS 3.0 server sites.
   - If this policy setting is **Disabled** or **Not Configured**, and if Automatic Updates is not **Disabled** by policy or user preference, Automatic Updates will try to connect to the Windows Update site on the Internet for its updates. However, access to the Windows Update site is not possible in the closed environment of the TOE.



5. **Enable client side targeting**. This policy setting specifies the target group name that the client should use to receive updates from a WSUS 3.0 server.

   - If this policy setting is **Enabled** it allows client computers to self-populate the specified computer group that exists on the WSUS 3.0 server. This setting is only capable of indicating to the WSUS 3.0 server which group the client computer should be placed in. The group must first be manually created on the WSUS 3.0 server as described in Create computer groups in WSUS 3.0.
   - If this policy setting is **Disabled** or **Not Configured**, no computer group information will be sent to the WSUS 3.0 server.

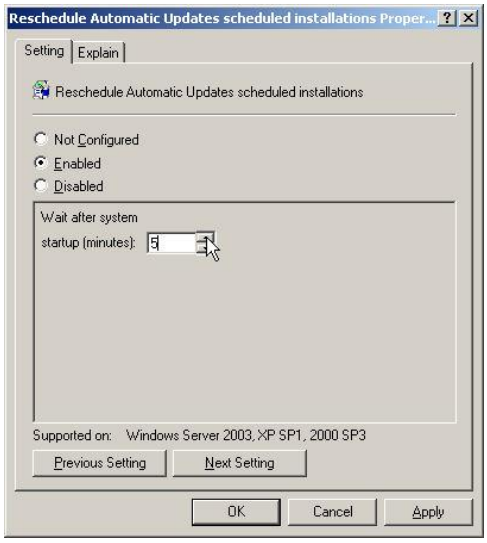


6. **Reschedule Automatic Updates scheduled installations**. This policy specifies the amount of time for Automatic Updates to wait, following system startup, before proceeding with a scheduled installation that was missed previously.

   - If this policy setting is **Enabled** a scheduled installation that did not take place earlier will occur the specified number of minutes after the computer is next started.
   - If this policy setting is **Disabled**, a missed scheduled installation will occur with the next scheduled installation.

- If this policy setting is **Not Configured**, a missed scheduled installation will occur one minute after the computer is next started.

Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the **Configure Automatic Updates** policy is disabled, this policy has no effect.



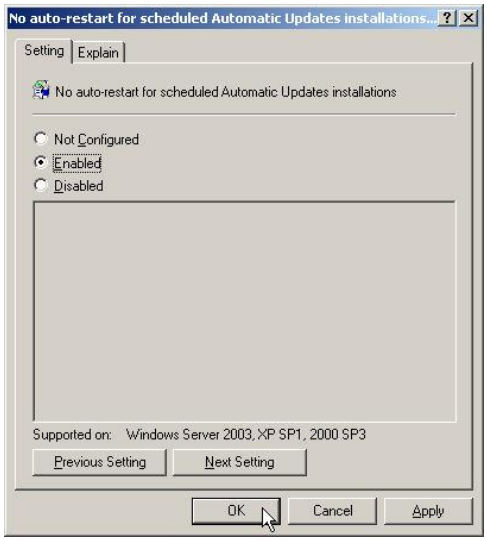
7. **No auto-restart for scheduled Automatic Updates installations**. This policy specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically.

   - If this policy setting is **Enabled**, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged on to the computer. Instead, Automatic Updates will notify the user to restart the computer in order to complete the installation.

   Note: Automatic Updates will not be able to detect future updates until the restart occurs.

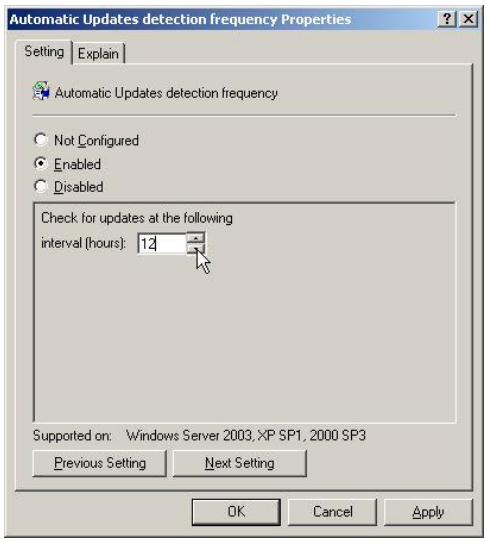
   - If this policy setting is **Disabled** or **Not Configured**, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation.

Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the **Configure Automatic Updates** policy is disabled, this policy has no effect.



8. **Automatic Updates detection frequency**. This policy specifies the hours that the WUS 3.0 client computer will use to determine how long to wait before checking for available updates. The exact wait time is determined by using the hours specified here, minus 0 to 20 percent of the hours specified. For example, if this policy is used to specify a 20-hour detection frequency, then all WSUS clients to which this policy is applied will check for updates anywhere between 16 and 20 hours.

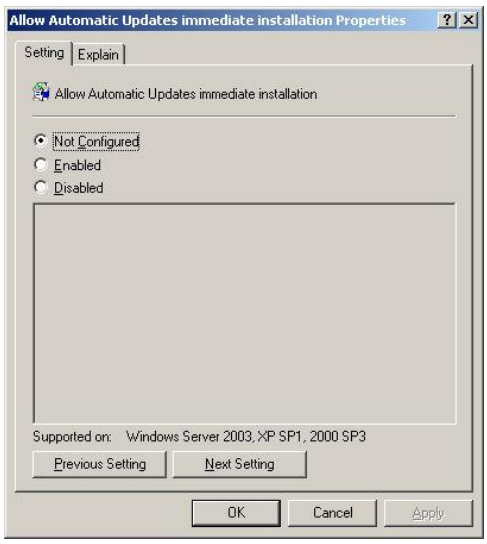
   - If this policy setting is **Enabled**, Automatic Updates will check for available updates at the specified interval.
   - If this policy setting is **Disabled** or **Not Configured**, Automatic Updates will check for available updates at the default interval of 22 hours.



9. **Allow Automatic Updates immediate installation**. This policy specifies whether Automatic Updates should automatically install certain updates that neither interrupt Windows services nor restart Windows.

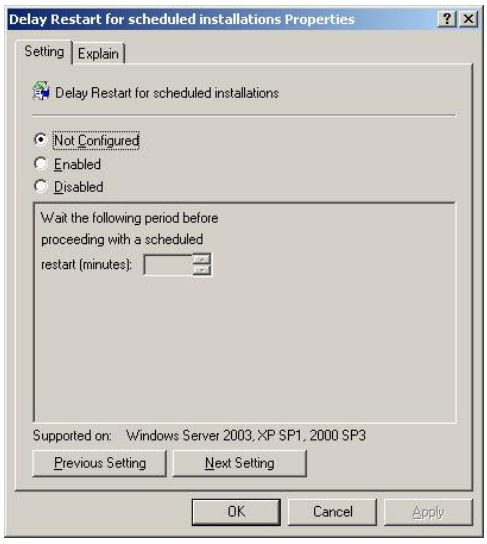
- If this policy setting is **Enabled**, Automatic Updates will immediately install these updates after they have been downloaded and are ready to install.
- If this policy setting is **Disabled** or **Not Configured**, such updates will not be installed immediately.

Note: If the **Configure Automatic Updates** policy is disabled, this policy will have no effect.



10. **Delay restart for scheduled installations**. This policy specifies the amount of time for Automatic Updates to wait before proceeding with a scheduled restart.
    - If this policy setting is **Enabled**, a scheduled restart will occur at the specified number of minutes after the installation is finished.
    - If this policy setting is **Disabled** or **Not Configured**, the default wait time is five minutes.

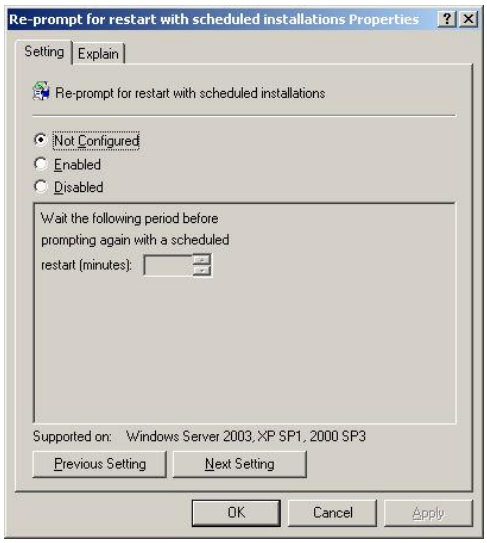
Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the **Configure Automatic Updates** policy is disabled, this policy has no effect.



11. **Re-prompt for restart with scheduled installations**. This policy specifies the amount of time for Automatic Updates to wait before prompting the user again for a scheduled restart.

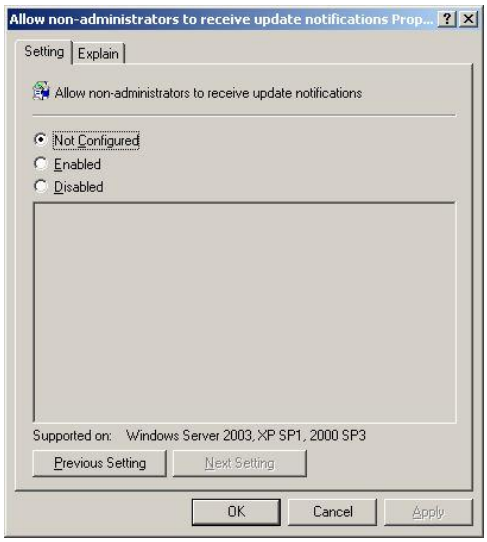
- If this policy setting is **Enabled**, a scheduled restart will occur based on the specified number of minutes after the previous prompt for restart was postponed, as defined in the **restart (minutes)** entry.
- If this policy setting is **Disabled** or **Not Configured**, the default interval is 10 minutes.

Note: This policy applies only when Automatic Updates is configured to perform scheduled installations of updates. If the **Configure Automatic Updates** policy is disabled, this policy has no effect.



12. **Allow non-administrators to receive update notifications**. This policy specifies whether logged-on non-administrative users will receive update notifications based on the configuration settings for Automatic Updates. If Automatic Updates is configured, by policy or locally, to notify the user either before downloading or only before installation, these notifications will be offered to any non-administrator who logs onto the computer.
    - If this policy setting is **Enabled**, Automatic Updates will include non-administrators when determining which logged-on user should receive notification.
    - If this policy setting is **Disabled** or **Not Configured**, Automatic Updates will notify only logged-on administrators.

Note: If the **Configure Automatic Updates** policy is disabled, this policy will have no effect.



13. Once all of the desired Automatic Updates Group settings have been configured close the GPO.
14. Click **Start**, click **Run**, type **cmd**, and the click **OK**.
15. At the command prompt, type **gpupdate /force** and hit the **Enter** key. Do this at the domain controller if a domain-level GPO was used. For all clients, either type **gpupdate /force** at a command prompt to force a refresh of Group Policies, reboot the computer, or wait for the next Group Policy refresh (15 minutes).
16. Continue to the procedures to Configure Automatic Updates Group Policy settings.

Move computers to computer groups in WSUS 3.0

WSUS 3.0 client computers are moved to computer groups based on the settings previously selected in Specify the method of assigning computers to groups.

- If the **Use the Update Services console** option was selected, WSUS 3.0 is configured for server-side targeting of WSUS 3.0 client computers to computer groups and requires an administrator to manually move computers to specific computer groups.
- If the **Use Group Policy or registry settings on computers** option was selected, WSUS 3.0 is configured for client-side targeting and WSUS 3.0 client computers will automatically assigned themselves to the computer group defined in the **Enable client side targeting** Automatic Updates Group Policy setting.

If WSUS 3.0 is configured for server-side targeting, follow the procedures below to move a computer to a different group.

1. Log on as an authorized administrator to the WSUS 3.0 server that will be servicing client computers.
2. Click **Start**, point to **Administrative Tools**, and then select **Windows Server Update Services 3.0**.
3. Expand the **Computers** node in the left-hand pane of the Update Services snap-in, expand **All Computers**, and then select **Unassigned Computers**.
4. In the center pane of the Update Services snap-in, right-click on a computer that is to be moved to an established computer group and select **Change Membership**.

Note: The **Change Membership** menu item will be grayed-out if WSUS 3.0 is not configured for server-side targeting.

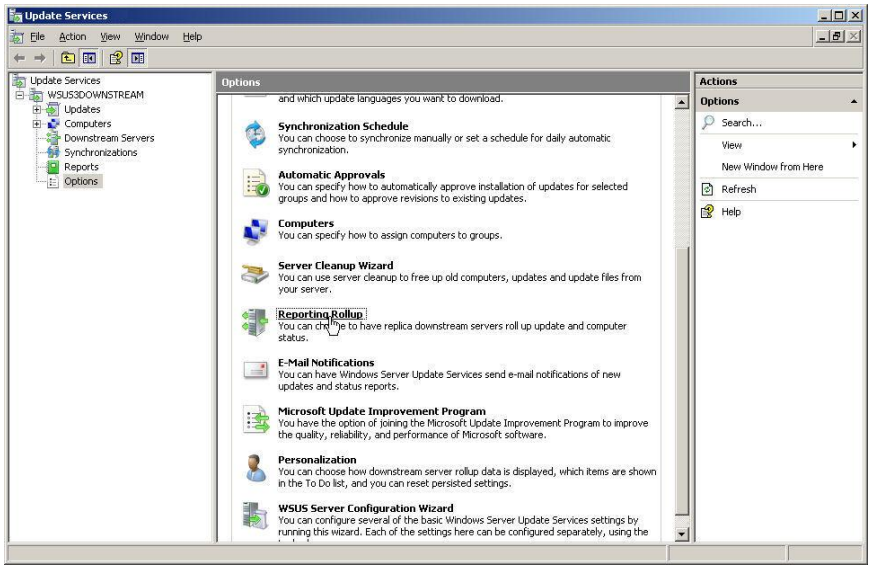
5. In the Set Computer Group Membership interface, check the box next to the name of the computer group that the selected computer is to be made a member of. Click **OK**.

6. The computer will be moved to the desired computer group.

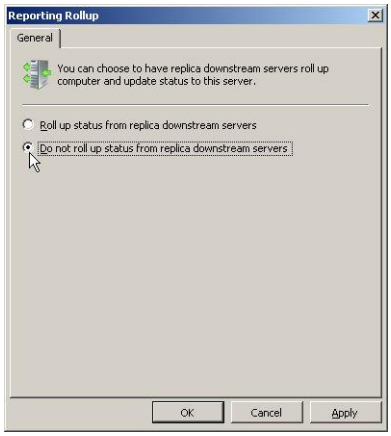
Disable Reporting Rollup

The Reporting Rollup feature of WSUS 3.0, used to roll up status from replica downstream servers, is not included in the TOE and needs to be disabled. Follow the procedures below, on each WSUS 3.0 server, to disable Reporting Rollup.

7. Log on as an authorized administrator.
8. Click **Start**, point to **Administrative Tools**, and then select **Windows Server Update Services 3.0**.
9. Expand the WSUS server node if necessary, click on the **Options** node on the left-hand pane, and then click the **Reporting Rollup** link in the center pane.



10. On the Reporting Rollup interface, click the **Do not roll up status from replica downstream servers** radio button and then click **OK**.



Approve Updates

Once the procedures above have been completed, the WSUS 3.0 server(s) are ready to support clients in the TOE. Within the TOE, the only updates that are allowed to be approved for installation on computers are those listed in Table 3.4 of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* (this document) and Table 3.3 of the *Windows XP Professional with SP2 Security Configuration Guide, Version 3.0*. All computers within the TOE, once installed and configured, will include all of the updates shown under the **Required Security Update** column of Tables 3.3 and 3.4 in the respective Security Configuration Guides. Therefore, the only remaining updates that may be approved for installation WSUS 3.0 clients within the TOE are those shown under the **Recommended Security Update** column of Tables 3.3 and 3.4 in the respective Security Configuration Guides.

There are many options available for deploying updates. For procedures used to manage and approve updates for installation on WSUS 3.0 clients within the TOE, see the *Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*.

Securing WSUS with the Secure Sockets Layer Protocol

Once proper operation of WSUS in the TOE has been verified, SSL can be added to the configuration. WSUS will use SSL to encrypt the metadata passed between clients and downstream WSUS servers. Follow the procedures below to enable the Secure Sockets Layer Protocol.

1. Log on the WSUS server as an authorized administrator.
2. Run the command: wsusutil configuressl *certificateName*

   Where *certificateName* is the DNS name of the WSUS server. For example, if the clients were configured to connect to https://myWSUSServer, then *certificateName* should be myWSUSServer. If clients were connected to https://myWSUSServer.myDomain.com, then *certificateName* should be myWSUSServer.myDomain.com.
3. Import the certificate of the certification authority into the local computer's Trusted Root CA store. The certificate must be imported to all the computers that will communicate with the server, including all clients and downstream servers.
4. Since port 8530 was used for WSUS configuration, be sure to use port 8531 for the HTTPS port when updating the IIS configuration.

5. The next set of changes involves the WSUS client computers. The URL for the listening WSUS Server must be specified with a secure port. In addition to using HTTPS, the port number must also be specified. As an example, if the WSUS server is named myWSUSServer, then the URL must be HTTPS://myWSUSServer:8531.
6. The certificates on the client computers have to be imported into the Local Computer's Trusted Root CA store.
7. The client computers must trust the certificate that was bound to the WSUS server in IIS. Depending upon the type of certificate used, it may be necessary to set up a service to enable the clients to trust the certificate bound to the WSUS server.

Finally, the downstream WSUS servers must be configured to use SSL to allow synchronization with upstream servers configured with SSL. Follow the procedures below to configure the downstream server.

8. Log on the WSUS downstream server as an authorized administrator.
9. In the WSUS Administration snap-in, click **Options**, and then click **Update Source and Proxy Server**.
10. In the **Update Source** box, select **Synchronize from another Windows Server Update Services Server** check box, then type the name of the upstream server and the port number it uses for SSL connections, and then select the **Use SSL when synchronizing update information** check box.
11. Click **OK** to save the settings. This completes the SSL configuration for WSUS.

8. Windows Server 2003 SP2 Common Criteria Security Configuration Templates

For convenience, this guide includes a set of Windows Server 2003 with SP2 Common Criteria security configuration templates. The templates can 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, because an organization's local security policies might require adjustments to the recommended values or security settings defined in the templates.

The templates supporting this document are listed in Table 8.1 and are included in Appendix F - Windows Server 2003 Security Configuration Templates for the Evaluated Configuration. 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 security settings required by the Common Criteria and provide stronger security by also applying the recommended security settings.

Table 8.1 Windows Server 2003 SP2 security configuration templates

Template File Name	Operating System Type/Configuration	Template Description
CC_Baseline_WS2K3_V2.inf	Windows Server 2003	Required Common Criteria Evaluated Configuration security settings for Windows Server 2003 configured as stand-alone or member server.
CC_Baseline_WS2K3_V2_Domain.inf	Windows Server 2003 domain	Required Common Criteria Evaluated Configuration security settings for Windows Server 2003 and Windows XP Professional domain members.
CC_Baseline_WS2K3_V2_DC.inf	Windows Server 2003 domain controller	Required Common Criteria Evaluated Configuration security settings for Windows Server 2003 domain controllers. Used with a Domain template or a Server template if a Domain policy is not used.
CC_HiSec_WS2K3_V2.inf	Windows Server 2003	Required and recommended Common Criteria Evaluated Configuration security settings for Windows Server 2003 Server configured as stand-alone or member server.
CC_HiSec_WS2K3_V2_Domain.inf	Windows Server 2003 domain	Required and recommended Common Criteria Evaluated Configuration security settings for Windows Server 2003 and Windows XP Professional Domain members.
CC_HiSec_WS2K3_V2_DC.inf	Windows Server 2003 domain controller	Required and recommended Common Criteria Evaluated Configuration security settings for Windows Server 2003 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 described in this section are either not included in the Windows Server 2003 Common Criteria security configuration templates, or are commented out of the templates. These settings must either be manually set through a Security Policy interface or can be included in the templates (by removing the comment markers) and edited as appropriate. The Security Templates snap-in tool can also be used as described in the Viewing and editing a security configuration template section later in this guide.

Recommended Modifications

In the Security Options policies section of the template, the following recommended settings should be reviewed and edited as applicable:

- **Accounts: Rename Administrator account.** This setting is commented out in the templates. The policy implementer must select a unique name. See the Security Options section for details.
- **Accounts: Rename Guest account.** This setting is commented out in the templates. The policy implementer must select a unique name. See the Security Options section for details.
- **Audit: Audit the access of global system objects.** This setting 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 Security Options section for details.
- **Audit: Audit the use of Backup and Restore privilege.** This setting is commented out in the templates. It generates a large amount of audit events and should only be implemented when strict audit management practices are in place. See the Security Options section for details.
- **Audit: Shut down the system immediately if unable to log security audits.** This setting 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 a critical system when strict audit management practices are in place. See the Security Options section for details.
- **Interactive logon: 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 Security Options section for details.
- **Interactive logon: 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 Security Options section for details.

Required Modifications

- **Prevent interference of the session lock from application generated input,** see the Additional Security Settings section for details. The security templates cannot create the path necessary to apply this setting. It must therefore be applied manually by using the Registry Editor (Regedit.exe). Procedures for using Regedit.exe are available in the *Windows Server 2003 Evaluated Configuration Administrator's Guide, Version 3.0*.

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

- **Domain Users.** Remove the SUPPORT_388945a0 account from the Domain Users group. See the Default Group Accounts section for details.
- **Pre-Windows 2000 Compatible Access.** This group provides backward compatibility with pre-Windows 2000 operating systems. Pre-Windows 2000 operating systems are not

included in the TOE. Therefore, remove Authenticated Users and do not add other accounts to this group. See the Default Group Accounts section for details.

- **Enable automatic screen lock protection.** The procedures are available in the Automatic Screen Lock Protection section of this document.

Recommended Procedures

- **Update the system backup and ASR Disk.** The procedures are available in the Recommended Actions Prior to Installing Service Pack and Patch Updates section of this document.
- **Back up the Administrator's encryption certificates.** The recommended procedures are available in the Encrypting File System section 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 enables 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 enables the administrator to configure or analyze Windows Server 2003 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 stand-alone computer or a domain member that does not receive security policies from the domain.

At the domain level, the Domain Security Policy and Domain Controller Security Policy templates must be applied by importing them into the domain controller's Domain Security Policy and Domain Controller Security Policy GUIs described in the Windows Server 2003 Security Policies section of this document.

Managing and Applying Common Criteria Security Configuration Templates

This section provides procedures for editing and applying the Common Criteria security configuration templates. The templates are available in Appendix F - Windows Server 2003 Security Configuration Templates for the Evaluated Configuration.

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 in the MMC. It is recommended that Notepad.exe be used to edit the security options that are commented out, or if modifications are to be made to any of the recommended registry settings that are not visible using the Security Templates Snap-in, such as those defined in the Additional Security Settings section of this document.

To edit a template using the Security Templates Snap-in

1. Log on to the computer as an authorized administrator.
2. Copy the desired template to the %SystemRoot%\Security\Templates folder.
3. Next, click **Start**, click **Run**, type **mmc**, and then click **OK**.
4. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
5. Select **Security Templates**, click **Add**, click **Close**, and then click **OK**.
6. To save the snap-in settings, click **Save** on the **File** menu. Type a name, and then click **Save**.
7. In the Security Templates Snap-in, double-click **Security Templates**.
8. 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**).
9. Double-click the security policy that is to be modified.
10. 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**).
11. Modification procedures are the same as those described in the Secure Configuration section of this document.
12. After 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 Server 2003. 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 as an authorized administrator.
2. Copy the desired template to the %SystemRoot%\Security\Templates folder.
3. Next, click **Start**, click **Run**, type **mmc**, and then click **OK**.
4. On the **File** 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 settings, click **Save** on the **File** menu. Type a name, and then click **Save**.
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 an .sdb extension, and click **Open**. Find and select the Common Criteria security configuration template so that it appears in the **File name** text box. Select 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. Select 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 appears showing the path to the error log file; click **OK**. Note that the

security settings are set immediately. Some settings, though applied, do 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 domain clients are to have all settings applied locally), then a Common Criteria server template must 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.

Importing a Common Criteria Domain Security Configuration Template

Use the following procedures to import a Common Criteria template for a domain.

1. Log on to the domain controller with administrative rights.
2. Copy the desired template into the %SystemRoot%\Security\Templates folder.
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. Browse to and select the Common Criteria security configuration template so that it appears in the **File name** text box. Select the **Clear this database** check box and click the **Open** button.
7. Close the Domain Security Policy.

If the server is a domain controller, follow the next procedure to import a Common Criteria template for domain controllers.

Importing a Common Criteria Domain Controller Security Configuration Template

Use the following procedure to import a Common Criteria template for a domain controller.

1. Log on to the domain controller with administrative rights.
2. Copy the desired template into the %SystemRoot%\Security\Templates folder.
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. Browse to and select the Common Criteria security configuration template so that it appears in the **File name** text box. Select the **Clear this database** check box and click the **Open** button.

7. Reboot the domain controller.

9. References

- A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003 http://support.microsoft.com/kb/875352
- Availability of hardware-based Data Execution Prevention on multiprocessor systems that are running Windows Server 2003 with Service Pack 1 http://support.microsoft.com/?kbid=902247
- Common Criteria Evaluated Configuration Guide: Microsoft Windows 2000 Security Configuration Guide http://www.microsoft.com/technet/security/topics/issues/w2kccscg/default.mspx
- How ASR Works http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/sdcbc_sto_axho.asp
- How to determine that hardware DEP is available and configured on your computer http://support.microsoft.com/kb/912923
- How To: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000 http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315669
- How To: Harden the TCP/IP Stack http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTHardTCP.asp
- IIS 6.0 Technical Reference: IIS and Built-in Accounts http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_SEC_23.mspx
- Internet Protocol security (IPSec) http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/sag_IPSECtopnode.asp
- Local Policies http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/techref/en-us/w2k3tr_sepol_local_set.asp
- Logon Rights and Privileges http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/sag_SEconceptsUnPrivs.asp
- Microsoft Home: Windows Server 2003 Security Guide http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en
- Microsoft Knowledge Base Article – 243330: Well Known Security Identifiers in Windows Server Operating Systems http://support.microsoft.com/default.aspx?scid=kb;en-us;243330
- Microsoft Knowledge Base Article – 243330: Well Known Security Identifiers in Windows Server Operating Systems http://support.microsoft.com/default.aspx?scid=kb;en-us;243330
- Microsoft Knowledge Base Article – 254649: Overview of memory dump file options for Windows 2000, for Windows XP, and for Windows Server 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;254649
- Microsoft Knowledge Base Article – 27825: Everyone Group Does Not Include Anonymous Security Identifier http://support.microsoft.com/default.aspx?scid=kb;en-us;278259

- Microsoft Knowledge Base Article – 324270: How To: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;324270
- Microsoft Knowledge Base Article – 325862: HOW TO: Use Remote Installation Service to Install Windows Server 2003 on Remote Computers http://support.microsoft.com/default.aspx?scid=kb;en-us;325862
- Microsoft Knowledge Base Article – 816302: HOW TO: Manage Groups in Windows Server 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;816302
- Microsoft Knowledge Base Article – 817009: The Default Permissions for Home Folders in Windows 2000 and Windows Server 2003 Are Different http://support.microsoft.com/default.aspx?scid=kb;en-us;817009
- Microsoft Knowledge Base Article – 823659: Client, service, and program incompatibilities that may occur when you modify security settings and user rights assignments http://support.microsoft.com/default.aspx?scid=kb;en-us;823659
- Microsoft Knowledge Base Article – 825069: A member of the Power Users group may be able to gain administrator rights and permissions in Windows Server 2003, Windows 2000, or Windows XP http://support.microsoft.com/default.aspx?scid=kb;en-us;825069
- Microsoft TechNet: Active Directory Federation Services (ADFS) http://technet2.microsoft.com/WindowsServer/en/Library/050392bc-c8f5-48b3-b30e-bf310399ff5d1033.mspx
- Microsoft TechNet: ADFS How To http://technet2.microsoft.com/WindowsServer/en/Library/d022ac37-9b74-4ba1-95aa-55868c0ebd8c1033.mspx
- Microsoft TechNet: ADFS Concepts http://technet2.microsoft.com/WindowsServer/en/Library/4147976b-8518-4ae0-804b-8723645f04ae1033.mspx
- Microsoft TechNet: ADFS Operations Guide http://technet2.microsoft.com/WindowsServer/en/Library/ed76b687-7585-421d-ad41-47c21499de001033.mspx
- Microsoft TechNet: Administering Active Directory Federation Services http://technet2.microsoft.com/WindowsServer/en/Library/007d4d62-2e2e-43a9-8652-9108733cbb731033.mspx
- Microsoft TechNet: Encrypting File System in Windows XP and Windows Server 2003 http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx
- Microsoft TechNet: Microsoft Windows Server 2003 TCP/IP Implementation Details (XP&2003) http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx
- Microsoft TechNet: Securing a Windows 2003 Server http://www.microsoft.com/technet/security/guidance/secmod119.mspx
- Microsoft TechNet: Threats and Countermeasures Guide |http://go.microsoft.com/fwlink/?LinkId=15159
- Microsoft TechNet: Troubleshooting Active Directory Federation Services http://technet2.microsoft.com/WindowsServer/en/Library/1eb6840d-3e5e-42d1-b310-41772a8a095a1033.mspx
- Microsoft Windows Security Resource Kit - Chapter 9: Implementing TCP/IP Security http://www.microsoft.com/mspress/books/sampchap/6418.asp

- Microsoft Windows Server 2003 Administrator's Companion (2003), Microsoft Press
- MSDN Home: How To Harden the TCP Stack
  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod109.asp
- Overview of Windows Server 2003 Datacenter Edition
  http://www.microsoft.com/windowsserver2003/evaluation/overview/datacenter.mspx
- Readme for Microsoft Windows Server 2003 Enterprise Edition
- Server roles
  http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/choose_role.asp
- User rights assignment
  http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/URAtopnode.asp
- What's New in Windows Server 2003 Security
  http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/security.mspx
- Windows 2000 Security Hardening Guide
  http://www.microsoft.com/downloads/details.aspx?FamilyID=15e83186-a2c8-4c8f-a9d0-a0201f639a56&displaylang=en

Appendix A Windows Server 2003 Default Security Policy Settings

The Windows Server 2003 Default Security Policy Settings table identifies the default Local Security Policy and Event Viewer Properties settings that are configured on a newly installed Windows Server 2003 operating system.

Table A.1 Default security policy settings

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Account Policies			
Password Policy			
Enforce password history	0 passwords remembered	24 passwords remembered	Not Defined
Maximum password age	42 days	42 days	Not Defined
Minimum password age	0 days	1 days	Not Defined
Minimum password length	0 characters	7 characters	Not Defined
Passwords must meet complexity requirements	Disabled	Enabled	Not Defined
Store passwords using reversible encryption for all users in the domain	Disabled	Disabled	Not Defined
Account Lockout Policy			
Account lockout duration	Not applicable	Not Defined	Not Defined
Account lockout threshold	0 invalid logon attempts	0 invalid logon attempts	Not Defined
Reset account lockout counter after	Not applicable	Not Defined	Not Defined
Kerberos Policy			
Enforce user logon restrictions	N/A	Enabled	Not Defined
Maximum lifetime for service ticket	N/A	600 minutes	Not Defined
Maximum lifetime for user ticket	N/A	10 hours	Not Defined
Maximum lifetime for user ticket renewal	N/A	7 days	Not Defined
Maximum tolerance for computer clock synchronization	N/A	5 minutes	Not Defined
Local Policies			
Audit Policy			
Audit account logon events	Success	Not Defined	Success
Audit account management	No auditing	Not Defined	Success

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Audit directory service access	No auditing	Not Defined	Success
Audit logon events	Success	Not Defined	Success
Audit object access	No auditing	Not Defined	No auditing
Audit policy changes	No auditing	Not Defined	Success
Audit privilege use	No auditing	Not Defined	No auditing
Audit process tracking	No auditing	Not Defined	No auditing
Audit system events	No auditing	Not Defined	Success
User Rights Assignment			
Access this computer from the network	Administrators Backup Operators Everyone Power Users Users	Not Defined	Administrators Authenticated users ENTERPRISE DOMAIN CONTROLLERS Everyone Pre-Windows 2000 Compatible Access
Act as part of the operating system	(Blank)	Not Defined	(Blank)
Add workstations to domain	(Blank)	Not Defined	Authenticated users
Adjust memory quotas for a process	Administrators LOCAL SERVICE NETWORK SERVICE	Not Defined	Administrators LOCAL SERVICE NETWORK SERVICE
Allow Logon Locally	Administrators Backup Operators Power Users Users	Not Defined	Account Operators Administrators Backup Operators Print Operators Server Operators
Allow logon through Terminal Services	Administrators Remote Desktop Users	Not Defined	(Blank)
Back up files and directories	Administrators Backup Operators	Not Defined	Administrators Backup Operators Server Operators

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Bypass traverse checking	Administrators Backup Operators Everyone Power Users Users	Not Defined	Administrators Authenticated users Everyone Pre-Windows 2000 Compatible Access
Change the system time	Administrators LOCAL SERVICE Power Users	Not Defined	Administrators LOCAL SERVICE Server Operators
Create a pagefile	Administrators	Not Defined	Administrators
Create a token object	(Blank)	Not Defined	(Blank)
Create global objects	Administrators INTERACTIVE SERVICE	Not Defined	Not Defined
Create permanent shared objects	(Blank)	Not Defined	(Blank)
Debug programs	Administrators	Not Defined	Administrators
Deny access to this computer from the network	SUPPORT_388945a0	Not Defined	<*DomainName*>\ SUPPORT_388945a0
Deny logon as a batch job	(Blank)	Not Defined	(Blank)
Deny logon as a service	(Blank)	Not Defined	(Blank)
Deny logon locally	SUPPORT_388945a0	Not Defined	<*DomainName*>\ SUPPORT_388945a0
Deny logon through Terminal Services	(Blank)	Not Defined	Not Defined
Enable computer and user accounts to be trusted for delegation	(Blank)	Not Defined	Administrators
Force shutdown from a remote system	Administrators	Not Defined	Administrators Server Operators
Generate security audits	LOCAL SERVICE NETWORK SERVICE	Not Defined	LOCAL SERVICE NETWORK SERVICE
Impersonate a client after authentication	Administrators SERVICE	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Increase security scheduling priority	Administrators	Not Defined	Administrators
Load and unload device drivers	Administrators	Not Defined	Administrators Print Operators
Lock pages in memory	(Blank)	Not Defined	(Blank)
Logon as a batch job	SUPPORT_388945a0 LOCAL SERVICE	Not Defined	<*DomainName*>\ SUPPORT_388945a0 LOCAL SERVICE
Logon as a service	NETWORK SERVICE	Not Defined	NETWORK SERVICE
Manage auditing and Security log	Administrators	Not Defined	Administrators
Modify firmware environment values	Administrators	Not Defined	Administrators
Perform volume maintenance tasks	Administrators	Not Defined	Not Defined
Profile single process	Administrators Power Users	Not Defined	Administrators
Profile system performance	Administrators	Not Defined	Administrators
Remove computer from docking station	Administrators Power Users Users	Not Defined	Administrators
Replace process level token	LOCAL SERVICE NETWORK SERVICE	Not Defined	LOCAL SERVICE NETWORK SERVICE
Restore files and directories	Administrators Backup Operators	Not Defined	Administrators Backup Operators Server Operators
Shut down the computer	Administrators Backup Operators Power Users	Not Defined	Administrators Backup Operators Print Operators Server Operators
Synchronize directory service data	(Blank)	Not Defined	(Blank)
Take ownership of files and other objects	Administrators	Not Defined	Administrators

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Security Options			
Accounts: Administrator account status	Enabled	Not Defined	Not Defined
Accounts: Guest account status	Disabled	Not Defined	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Not Defined	Not Defined
Accounts: Rename Administrator Account	Administrator	Not Defined	Not Defined
Accounts: Rename Guest Account	Guest	Not Defined	Not Defined
Audit: Audit the access of global system objects	Disabled	Not Defined	Not Defined
Audit: Audit the use of Backup and Restore privilege	Disabled	Not Defined	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled	Not Defined	Not Defined
DCOM: Machine Access restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined	Not Defined
DCOM: Machine Launch restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined	Not Defined
Devices: Allow undock without having to log on	Enabled	Not Defined	Not Defined
Devices: Allowed to format and eject removable media	Administrators	Not Defined	Not Defined
Devices: Prevent users from installing printer drivers	Enabled	Not Defined	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	Not Defined	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Disabled	Not Defined	Not Defined
Devices: Unsigned driver installation behavior	Warn but allow installation	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Domain controller: Allow server operators to schedule tasks	Not Defined	Not Defined	Not Defined
Domain controller: LDAP server signing requirement	Not Defined	Not Defined	None
Domain controller: Refuse machine account password changes	Not Defined	Not Defined	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Not Defined	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Not Defined	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Enabled	Not Defined	Not Defined
Domain member: Disable machine account password changes	Disabled	Not Defined	Not Defined
Domain member: Maximum machine account password age	30 days	Not Defined	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Not Defined	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined	Not Defined	Not Defined
Interactive logon: Do not display last user name	Disabled	Not Defined	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Not Defined	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined (or blank)	Not Defined	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined	Not Defined	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Interactive logon: Prompt user to change password before expiration	14 days	Not Defined	Not Defined
Interactive logon: Require domain controller authentication to unlock	Disabled	Not Defined	Not Defined
Interactive logon: Require smart card	Disabled	Not Defined	Not Defined
Interactive logon: Smart card removal behavior	No Action	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled	Not Defined	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Not Defined	Not Defined
Microsoft network client: Send unencrypted password to connect to third-party SMB servers	Disabled	Not Defined	Not Defined
Microsoft network server: Amount of idle time required before suspending session	15 minutes	Not Defined	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled	Not Defined	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Not Defined	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Not Defined	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled	Not Defined	Not Defined (Although Not Defined in this policy, it is Enabled in a domain controller's Local Security Policy)
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Not Defined	Not Defined
Network access: Do not allow anonymous enumeration of	Disabled	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
SAM accounts and shares			
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	Not Defined	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Disabled	Not Defined	Not Defined
Network access: Named Pipes that can be accessed anonymously	COMNAP COMNODE SQL\QUERY SPOOLSS netlogon lsarpc samr browser	Not Defined	Not Defined
Network access: Remotely accessible registry paths	System\CurrentControlSet\ Control\ProductOptions System\CurrentControlSet\ Control\Server Applications Software\Microsoft\Windows NT\ CurrentVersion	Not Defined	Not Defined
Network Access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\ Control\Print\Printers System\CurrentControlSet\ Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\ Control\ContentIndex System\CurrentControlSet\ Control\Terminal Server System\CurrentControlSet\ Control\Terminal Server\UserConfig System\CurrentControlSet\	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
	Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\ Services\SysmonLog		
Network access: Restrict anonymous access to named pipes and shares	Enabled	Not Defined	Not Defined
Network access: Shares that can be accessed anonymously	COMCFG DFS$	Not Defined	Not Defined
Network access: Sharing and security model for local accounts	Classic: Local users authenticate as themselves	Not Defined	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Disabled	Not Defined	Not Defined
Network security: Force logoff when logon hours expire	Disabled	Disabled	Not Defined
Network security: LAN Manager Authentication Level	Send NTLM response only	Not Defined	Send NTLM response only
Network security: LDAP client signing requirements	Negotiate signing	Not Defined	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum	Not Defined	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum	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
Shutdown: Allow system to be shut down without having to log on	Disabled	Not Defined	Not Defined
Shutdown: Clear virtual memory pagefile	Disabled	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	Not Defined	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing	Disabled	Not Defined	Not Defined
System Objects: Default owner for objects created by members of the Administrators group	Administrators group	Not Defined	Not Defined
System Objects: Require case insensitivity for non-Windows subsystems	Enabled	Not Defined	Not Defined
System Objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)	Enabled	Not Defined	Not Defined
System Settings: Optional Subsystems	Posix	Not Defined	Not Defined
System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	Not Defined	Not Defined
Event Log			
Property Settings for Event Logs			
Maximum Application log size	16,384 KB	Not Defined	Not Defined
Maximum Security log size	16,384 KB	Not Defined	Not Defined (Although Not Defined in this policy, the log size is changed to 131,072 KB on domain controllers)
Maximum System log size	16,384 KB	Not Defined	Not Defined
Prevent local guests group from accessing Application log	Not Applicable	Not Defined	Not Defined
Prevent local guests group from accessing Security log	Not Applicable	Not Defined	Not Defined
Prevent local guests group from accessing System log	Not Applicable	Not Defined	Not Defined

Windows Server 2003 Default Security Policy Settings			
Security Policies	**Stand-alone Server**	**Default Domain Security Policy**	**Default Domain Controller Security Policy**
Retain Application log	Overwrite events as needed	Not Defined	Not Defined
Retain Security log	Overwrite events as needed	Not Defined	Not Defined
Retain System log	Overwrite events as needed	Not Defined	Not Defined
Retention method for Application log	Overwrite events as needed	Not Defined	Not Defined
Retention method for Security log	Overwrite events as needed	Not Defined	Not Defined
Retention method for System log	Overwrite events as needed	Not Defined	Not Defined

Appendix B Audit Categories and Events

The Windows Server 2003 Security Target Compliance Matrix for Audit presents a correlation of the audit requirements specified by the Windows 2003/XP Security Target to the specific audit event identifiers which support the stated requirements.

Table B.1 Security target compliance matrix for audit

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
FAU_GEN.1	Startup 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**		✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		578 – Privileged object operation. (Failure should result for SeSecurityPrivilege.)		
FAU_SAR.3(a), (b)	None			
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 **Note:** Event 523 is generated only when the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel key value is set to the percentage that the administrator wants the audit record to be cut upon.	✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
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	None			
FDP_ACF.1	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			

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
FDP_RIP.2. Note 1	None			
FIA_ATD.1	None			
FIA_SOS.1	Rejection or acceptance by the TOE Security Functions (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. **Category: Account logon** 680 – Account used for logon. 681 – The logon account: <*ClientName*> by: <*Source*> from workstation <*Workstation*> failed. The error code was <*Error*>.	✓	✓
FIA_UAU.1	The use of the authentication mechanism.	**Category: Logon**	✓	✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		528 – Successful logon. 529 – Logon failure: Unknown user name or bad password. 531 – A logon attempt was made by using a disabled account. 532 – A logon attempt was made by using an expired account. 534 – The user attempted to log on with a type (such as network, interactive, batch, service, or remote interactive) that is not allowed. 540 – Successful network logon. **Category: Account logon** 681 – The logon account: <*ClientName*> by: <*Source*> from workstation <*Workstation*> failed. The error code was <*Error*>.		✓
FIA_UAU.7	None			
FIA_UID.1	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. 531 – A logon attempt was made by using a disabled account.	✓	✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		532 – A logon attempt was made by using an expired account. 534 – The user attempted to log on with a type (such as network, interactive, batch, service, or remote interactive) that is not allowed. 535 – Logon failure: The specified account's password has expired. 540 – Successful network logon. 545 – IPSec peer authentication failed. **Category: Account logon** 675 – Pre-authentication failed. 681 – The logon account: <*ClientName*> by: <*Source*> from workstation <*Workstation*> failed. The error code was <*Error*>.	✓	✓
FIA_USB.1_EX	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. (For **Description → Accesses**, there should be the following entries; AppendData, ReadAttributes and WriteAttributes.)	✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
FMT_MSA.3	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** (These 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) **Category:** Policy change 612 – Audit policy change.	✓ ✓ ✓ ✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
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. 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.	✓ ✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		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. 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.		

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		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.	✓	✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
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.	✓ ✓	✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		637 – Security enabled Local Group member removed. 638 – Security enabled Local Group deleted. 639 – Security enabled Local Group changed. 640 – General account database changed. 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. 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.		

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		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_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)		✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		Category: Account management 642 – User account changed – account locked. 644 – User account locked.	✓	
FIA_UAU.2	The use of the authentication mechanism.	**Category: Logon** 528 – Successful logon. 529 – Logon failure: Unknown user name or bad password. 531 – A logon attempt was made by using a disabled account. 532 – A logon attempt was made by using an expired account. 534 – The user attempted to log on with a type (such as network, interactive, batch, service, or remote interactive) that is not allowed. 540 – Successful network logon. **Category: Account logon** 681 – The logon account: <*ClientName*> 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	**Category: Logon**	✓	✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
	attempts. Additionally, the origin of the attempt (e.g. terminal identification) is included in the audit event.	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** 675 – Pre-authentication failed. 681 – The logon account: <*ClientName*> 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	**Category: Privilege use**	✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
	privilege to change the TSF Time.	577 – Privileged service called. (Shown as use of SeSystemTimePrivilege.)		
TRANSFER_PROT_EX.1	IPSEC related events.	**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 6 is unlock) 529 – Logon failure (entry 6 is unlock)	✓	✓
FTA_SSL.2	Attempt to unlock.	**Category: Logon** 528 – Logon successful (entry 6 is unlock) 529 – Logon failure (entry 6 is unlock)	✓	✓
FTA_TSE.1	Logon Failure.	**Category: Logon**		✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		535 – Logon failure: The specified account's password has expired.		
FTP_TRP.1	Authentication and locking attempts.	**Category: Account Logon** 680 – Logon attempted by MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 **Category: Logon** 552 – Logon attempt using explicit credentials. 528 – Successful Logon. 529 – Logon Failure. 538 – User Logoff. Logon Type 7 (Locking Attempt)	✓ ✓	✓ ✓
FMT_MTD.1(e)	Lockout duration changes.	**Category: Account management** 643 – Lockout policy modified. Changed attributes: Lockout Observation Window.	✓	
FMT_MTD.1(f)	Modification of minimum password length.	**Category: Account management** 643 – Password policy modified. Changed attributes: Min Password Age.	✓	
FMT_MTD.1(n)	Modification of password complexity policy.	**Category: Account management**	✓	

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
		643 – Password policy modified. Changed attributes: Password properties. (0 = disabled password complexity, 1 = enabled password complexity)		
FMT_MTD.2	Modification of unsuccessful logon attempt threshold.	**Category: Account management** 643 – Password policy modified. Changed attributes: Lockout Threshold	✓	
FMT_SAE.1	Setting of password expiration time.	**Category: Account management** 643 – Password policy modified. Changed attributes: Max Password Age	✓	
TRANSFER_PROT_EX.3	Detection of data integrity violation. **Note:** Requires setting the ReplayIntegrityLogging registry value to 1 (DWORD) in the HKLM\System\CurrentControlSet\Control\Lsa\Audit registry key.	**Category: System** 864 – Received packet from over a security association that failed data integrity verification.		✓
FPT_RPL.1	Replay of TSF data **Note:** Requires setting the ReplayIntegrityLogging registry value to 1 (DWORD) in the HKLM\System\CurrentControlSet\Control\Lsa\Audit	**Category: System** 865 – Received packet from over a security association with a sequence number for a packet already processed by the system. This could be a temporary problem; if it persists it may indicate a replay attack against the system. 866 – IPSec inbound packet replay check failed, inbound packet had too low a sequence		✓

Component	Event	Audit Event	Required Setting: Success	Required Setting: Failure
	registry key.	number to ensure it was not a replay. 867 – IPSec received inbound clear text packet that should have been secured.		
FPT_TRC_EX.1	Directory Replication Audit access to directory service objects and associated properties.	**Category: Object Access** 566 – A generic object operation took place. (This event message is also used to audit directory service access events.) **Category: Directory Service Access** 566 – A generic object operation took place. This is the only directory service access event and is also included in Object Access Events.	✓ ✓	 ✓

Appendix C User Rights and Privileges

The table here identifies the default user rights assignments on Windows Server 2003, defines their applicability to the Windows 2003/XP V3 ST, and provides change requirements and recommendations necessary to comply with the Windows 2003/XP V3 ST objectives.

The table identifies the default user rights assigned to users on stand-alone and member server Windows Server 2003 systems and on a Windows Server 2003 domain controller. It also identifies the default user rights in a Domain Security Policy (all are set to **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 Windows 2003/XP V3 ST requirements.

Settings for Windows XP Professional are described in the *Windows XP Professional Security Configuration Guide, Version 3.0*. The Domain Security Policy settings described in this document also apply to Windows XP Professional systems that are joined to the domain where the Domain Security Policy is applied.

Table C.1 User rights and privileges

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 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 Everyone *IUSR_ComputerName *IWAM_ComputerName Power Users Users **Required:** Administrators Authenticated Users Backup Operators *IUSR_ComputerName *IWAM_ComputerName Power Users Users	**Default:** (Not Defined) **Required:** Administrators Authenticated Users Backup Operators Power Users Users	**Default:** Administrators Authenticated Users ENTERPRISE DOMAIN CONTROLLERS Everyone Pre-Windows 2000 Compatible Access **Required:** Administrators Authenticated Users ENTERPRISE DOMAIN CONTROLLERS	**Supports the following TOE Security Functional Requirement:** FIA_UAU.2.1, Authentication; FIA_UID.2, User Identification before any action; FIA_USB.1_EX, User subject binding. Implements the following TOE Security functions: Para 6.1.4, Identification and Authentication Function. * The IUSR_ComputerName and IWAM_ComputerName accounts are installed with IIS 6.0 and are allowed only on a Windows Server 2003 running IIS 6.0. **Changes:** Replace **Everyone** with **Authenticated User**.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Allow log on locally (SeInteractiveLogonRight)	This logon right determines which users can interactively log on to this computer. Logons initiated by pressing **CTRL+ALT+DEL** sequence on the attached keyboard requires the user to have this logon right. Additionally this logon right may be required by some service or administrative applications that can log on users.	**Default:** Administrators Backup Operators *IUSR_ComputerName Power Users Users **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** Account Operators Administrators Backup Operators Print Operators Server Operators **Required:** No Change	**Supports the following TOE Security Functional Requirement:** FIA_UAU.2.1, Authentication; FIA_UID.2, User Identification before any action; FIA_USB.1_EX, User subject binding. Implements the following TOE Security functions: Para 6.1.4, Identification and Authentication Function. *The IUSR_ComputerName account is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0. **Changes:** Do not allow Guest/anonymous logons. Remove Guest accounts since they allow unauthenticated/anonymous access.
Allow Log on through Terminal Services	This security setting determines which users or groups have permission to	**Default:** Administrators	**Default:** Not Defined	**Default:** Not Defined	Terminal Services is not included in the Evaluated Configuration.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	log on as a Terminal Services client.	Remote Desktop Users **Required:** None	**Required:** None	**Required:** None	**Changes:** Remove default accounts from stand-alone systems. Set the Domain Security Policy and Domain Controller Security Policy to None.
Log on as a batch job (SeBatchLogonRight)	Allows a user to log on by using a batch-queue facility. For example, when a user submits a job by means of the task scheduler, the task scheduler logs that user on as a batch user rather than as an interactive user.	**Default:** * IIS_WPG * IUSR_ComputerName * IWAM__<*ComputerName*> LOCAL SERVICE SUPPORT_388945a0 **Recommended:** * IIS_WPG * IUSR_ComputerName * IWAM__<*ComputerName*> LOCAL SERVICE *For IIS, grant this right to	**Default:** (Not Defined) **Recommended:** LOCAL SERVICE	**Default:** SUPPORT_388945a0 **Recommended:** LOCAL SERVICE	* The IIS_WPG, IUSR_ComputerName, and IWAM__<*ComputerName*> accounts are installed with IIS 6.0 and are allowed only on a Windows Server 2003 running IIS 6.0.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
		IIS accounts through an OU if a Domain Security Policy is being used to enforce settings on domain clients.			
Logon as a service (SeServiceLogonRight)	Allows a security principal to log on as a service.	**Default:** NETWORK SERVICE **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** NETWORK SERVICE **Recommended:** No Change	
Deny Access to this computer from the network (SeDenyNetworkLogonRight)	Prohibits a user or group from connecting to the computer from the network. This policy setting supersedes the **Access this computer from the network** policy setting if a user account is subject to both policies.	**Default:** SUPPORT_388945a0 **Required:** Do not remove the defaults. Organizations may add accounts if necessary.	**Default:** (Not Defined) **Required:** Organizations may add accounts if necessary. However, if they change the default, the Guest and SUPPORT_388945 a0 accounts must be included in the change.	**Default:** SUPPORT_388945a0 **Required:** Do not remove the defaults. Organizations may add accounts if necessary.	

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Deny log on as a batch file (SeDenyBatchLogonRight)	Prohibits a user or group from logging on through a batch-queue facility. This policy setting supersedes the **Log on as a batch job** policy setting if a user account is subject to both policies.	**Default:** None **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** None **Recommended:** No Change	
Deny log on as a service (SeDenyServiceLogonRight)	Prohibits a user or group from logging on as a service. This policy setting supersedes the **Log on as service** policy setting if a user account is subject to both policies.	**Default:** None **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** None **Recommended:** No Change	
Deny log on locally (SeDenyInteractiveLogonRight)	Prohibits a user or group from logging on locally at the keyboard.	**Default:** SUPPORT_388945a0 **Required:** Do not remove the defaults. Organizations may add accounts if necessary.	**Default:** (Not Defined) **Required:** Organizations may add accounts if necessary. However, if they change the default, the Guest and SUPPORT_388945	**Default:** SUPPORT_388945a0 **Required:** Do not remove the defaults. Organizations may add accounts if necessary.	

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
			a0 accounts must be included in the change.		
Deny log on through Terminal Services	This security setting determines which users and groups are prohibited from logging on as a Terminal Services client.	**Default:** None **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** None	**Default:** None **Recommended:** No Change	Terminal Services is not included in the Evaluated Configuration.
Privileges					
Act as part of the operating system (SeTcbPrivilege)	This privilege allows a process to impersonate any user without authentication. The process can therefore gain access to the same local resources as that user. 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	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required:** None	**Default:** None **Required:** No Change	Default settings support the following TOE Security Functional Requirements: FPT_SEP.2, SFP Domain Separation. Misuse of this privilege can violate FAU_GEN.1, Audit Generation, FAU_GEN.2, User Identity Association, and FIA_USB.1_EX, User Subject Binding. Implements the following TOE Security functions: Para 6.1.6.5, Domain Separation.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	provide any and all accesses. Additionally, the anonymous token does not provide a primary identity for tracking events in the audit log. The LocalSystem account uses this privilege by default.				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.2, FAU_GEN.1, FAU_GEN.2, and FIA_USB.1_EX.
Add workstations to 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 Server 2003, the behavior of this privilege is duplicated by the Create Computer Objects permission for	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required:** None	**Default:** Authenticated Users **Required:** Domain Admins	**Supports the following TOE Security Functional Requirement:** FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.5.2, Security Management Functions, describing the domain management function that allows an authorized administrator to add and remove computers to and

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	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.				from a domain. Para 6.1.5.1, Roles. Can be used to grant authorized users the privilege to add and remove computers 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. Enable the Domain Security Policy and do not add users. This will set the policy to ensure accounts are not added to this policy setting across the domain.
Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)	Determines which accounts can use a process with Write Property access to another process to increase the processor quota assigned to the other process.	**Default:** Administrators *IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE	**Default:** Not Defined	**Default:** Administrators LOCAL SERVICE NETWORK SERVICE	This privilege is useful for system tuning, but it can be misused, for example, in a denial-of-service attack. Could be used to support the following TOE Security Functional **Requirement:** FMT_SMR.1 Security Roles.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
		Required: No Change	**Required:** Administrators LOCAL SERVICE NETWORK SERVICE	**Required:** No Change	However, there is not an ST requirement that specifically mandates that this ability be restricted to the administrator. Can support the following TOE Security functions: Para 6.1.5.1, 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. Because managing the processor quota affects performance and availability. However, the ST does not claim to address Denial of Service. * The IWAM_ComputerName account is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0. **Changes:**

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					Set the Domain Policy to Administrators, LOCAL SERVICE, and NETWORK SERVICE for this privilege to enforce trusted administration. IIS servers may need their own OU Security Policy when a Domain Security Policy is set for this privilege.
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 application interface. Otherwise normal file and directory permissions apply. Assigning this user right is similar to granting the following permissions to a user or group on all files and folders on the system: Traverse Folder / Execute File	**Default:** Administrators Backup Operators **Required:** No Change	**Default:** (Not Defined) **Required:** Administrators Backup Operators	**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 restrictions. Implements the following TOE Security functions: Para 6.1.5.1, Roles. Can be used to grant authorized users the privilege to conduct backups. **Changes:** Do not assign this privilege

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	List Folder / Read Data Read Attributes Read Extended Attributes Read Permissions				to any account, other than the defaults, in order to ensure that only authorized administrators are granted this right through membership in the Administrators, Backup Operators, or Server Operators groups. Set the Domain Policy to Administrators and Backup Operators for this privilege to enforce trusted administration. Exception: The Windows Server 2003 Certificate Server Evaluated Configuration is allowed to assign this right to a Certification Authority (CA) Backup Operator administrative role by assignment in the Backup Operator's group. See the Windows Server 2003 Certificate Server Security Configuration Guide for details.
Bypass traverse checking (SeChangeNotifyPrivilege)	Allows the user to pass through folders to which the user otherwise has no access while navigating an	**Default:** Administrators	**Default:** (Not Defined)	**Default:** Administrators	The Windows Operating Systems, as well as many applications, have been designed with the

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	object path in any Microsoft Windows file system or in the registry. This privilege does not allow the user to list the contents of a folder; it only allows the user to traverse its directories.	Backup Operators Everyone Power Users Users **Recommended:** No Change	**Recommended:**: No Change	Authenticated Users Everyone Pre-Windows 2000 compatible access **Recommended:** Administrators Authenticated Users Everyone	expectation that anyone who can legitimately access the computer will have this user right. Therefore, removing the Everyone group may lead to operating system instability or application failure. It is recommended that the defaults not be modified. **Changes:** The Pre-Windows 2000 Compatible Access group is used for backward compatibility for computers that are running Microsoft Windows NT 4.0 and earlier. Windows NT 4.0 and earlier systems are not included in the Evaluated Configuration. Therefore, the Pre-Windows 2000 Compatible Access group may be removed from the Windows Server 2003 Domain Controller Security Policy's Bypass traverse checking user right setting.
Change the system time (SeSystemTimePrivilege)	Allows the user to set the time for the internal clock of the computer.	**Default:** Administrators	**Default:** (Not Defined)	**Default:** Administrators	Default settings support the following TOE Security Functional Requirements:

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
		Power Users **Required:** No Change	**Required:** No Change	LOCAL SERVICE Server Operators **Required:** No Change	FMT_SMR.1 Security Roles, and FMT_MTD.1.1(g) Management of TSF Time. Implements the following TOE Security functions: Para 6.1.5.1, Roles and para 6.1.6.6 Time Service. Can be used to grant authorized users the privilege to set the system time. Users that are assigned this user right can affect the appearance of event logs. If the system time is changed, events that are logged will reflect this new time, not the actual time that the events occurred.
Create a pagefile (SeCreatePagefilePrivilege)	Allows the user to create and change the size of a pagefile.	**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. Implements the following TOE Security functions: Para 6.1.5.1, Roles. Can be used to grant authorized users the privilege to change

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					pagefile settings. Change: Set the Domain Security Policy to Administrators for this privilege to enforce trusted administration and protect against unauthorized system modifications.
Create a token object (SeCreateTokenPrivilege)	This security setting determines which accounts can be used by processes to create a token that can then be used to get access to any local resources when the process uses an internal application programming interface (API) to create an access token. This user right is used internally by the operating system.	**Default:** None **Required:** No Change	**Default:** (Not Defined) **Required:** None	**Default:** None **Required:** No Change	Default settings support the following TOE Security Functional Requirements: FPT_SEP.2, Domain Separation. Implements the following TOE Security functions: Para 6.1.6.5, 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 Security Policy to None for this

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					privilege to enforce the default settings on the domain and ensure support of FPT_SEP.2. When a process requires this privilege, use the LocalSystem account (which already has this privilege), rather than creating a separate account and assigning this privilege to it.
Create Global Objects	This user right is required for a user account to create global objects during Terminal Services sessions. Users can still create session-specific objects without being assigned this user right.	**Default:** Administrators INTERACTIVE SERVICE **Recommended:** No Change	**Default:** Not Defined **Recommended:** No Change	**Default:** Not Defined **Recommended:** No Change	Terminal Services is not included in the Evaluated Configuration. **Changes:** Set all Security Policies to None to prevent use of this privilege.
Create permanent shared objects (SeCreatePermanentPrivilege)	This user right determines which accounts can be used by processes to create a directory object in the Windows 2000 Server, Windows 2000 Professional, Windows XP Professional, and Windows Server 2003 family object	**Default:** None **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** None **Recommended:** No Change	

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	manager. This user right is used internally by the operating system and is useful to kernel-mode components that extend the Windows 2000 Server, Windows 2000 Professional, Windows XP Professional, and Windows Server 2003 family object namespace. Because components that are running in kernel mode already have this user right assigned to them, it is not necessary to specifically assign it.				
Debug programs (SeDebugPrivilege)	Allows the user to attach a debugger to any process. This user right determines which users can attach a debugger to any process or to the kernel. Developers who are debugging their own applications do not need to be assigned this user right. Developers who are debugging new system components will need this	**Default:** Administrators **Required:** None	**Default:** (Not Defined) **Required:** None	**Default:** Administrators **Required:** None	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. This privilege is not auditable and should not be

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	user right to be able to do so. This user right provides complete access to sensitive and critical operating system components.				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:** (Not Defined) **Required:** 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 6.1.5.1, Roles. Can be used to grant authorized users the Trusted for Delegation settings on a user or computer in Active Directory. 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

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					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:** No Change	**Default:** (Not Defined) **Recommended:** Administrators	**Default:** Administrators Server Operators **Recommended:** No Change	**Changes:** Set the Domain Policy to Administrators to enforce the default settings across the domain.
Generate security audits (SeAuditPrivilege)	Allows a process to generate entries in the Security log. The Security log is used to trace unauthorized system access and other security relevant activities.	**Default:** LOCAL SERVICE NETWORK SERVICE **Required:** No Change	**Default:** (Not Defined) **Required:** LOCAL SERVICE	**Default:** LOCAL SERVICE NETWORK SERVICE **Required:** No Change	Supports the following TOE security requirement through the LocalSystem account: FAU_GEN.1.1, Audit Data Generation. Misuse of this user right can result in the generation of many auditing events, potentially hiding evidence

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
			NETWORK SERVICE		of an attack or causing a denial of service if the Audit: Shut down system immediately if unable to log security audits security policy setting is enabled. If granted to users, this privilege would allow non-TSF generated audit records in the audit log. Use of this privilege is not auditable. **Changes:** Set the Domain Policy to include the LOCAL SERVICE and NETWORK SERVICE accounts for this privilege to enforce the default settings across the domain.
Impersonate a client after authentication	Assigning this privilege to a user allows programs running on behalf of that user to impersonate a client. Requiring this user right for this kind of impersonation prevents an unauthorized user from convincing a client to connect (for example, by remote procedure call (RPC) or named pipes) to a	**Default:** Administrators * IIS_WPG SERVICE **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	* The IIS_WPG group is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	service that they have created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels.				
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:** (Not Defined) **Recommended:** 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 6.1.5.1, 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

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					issue. Because 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.
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 programs and giving them destructive access to resources.	**Default:** Administrators **Required:** No Change	**Default:** (Not Defined) **Required:** Administrators	**Default:** Administrators Print Operators **Required:** No Change	**Supports the following TOE Security Functional Requirement:** FMT_SMR.1 Security Roles. Implements the following TOE Security functions: Para 6.1.5.1, 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 privilege to support trusted

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					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:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** None **Recommended:** 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 in Audit Policy. A user who has this privilege can also view and clear the Security log from Event Viewer.	**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, FAU_SAR.1.1, Audit Review, FAU_SAR.2.1, Restricted Audit Review, FAU_SAR.3, Selectable Audit 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

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					Trail FMT_MTD.1.1(b), Management of Audited Events Implements the following TOE Security functions: Para 6.1.5.1, 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 privilege to support trusted administration. Exception: The Windows Server 2003 Certificate Server Evaluated Configuration is allowed to assign this right to a CA Auditor administrative role by assignment. See the Windows Server 2003 Certificate Server Security Configuration Guide for details.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Modify firmware environment values (SeSystemEnvironmentPrivilege)	This security setting determines who can modify firmware environment values. Firmware environment variables are settings stored in the nonvolatile RAM of non-x86-based computers. The effect of the setting depends on the processor. On x86-based computers, the only firmware environment value that can be modified by assigning this user right is the Last Known Good Configuration setting, which should only be modified by the system. On x64-based computers, boot information is stored in nonvolatile RAM. Users must be assigned this user right to run bootcfg.exe and to change the Default Operating System setting on Startup and Recovery in System Properties. On all computers, this user right is required to install or upgrade Windows.	**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. Implements the following TOE Security functions: Para 6.1.5.1, Roles. Can be used to grant authorized users the administrative capability to modify system environment variables. **Changes:** Set the Domain Security Policy to Administrators for this privilege to support trusted administration.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
Perform volume maintenance tasks	This security setting determines which users and groups can run maintenance tasks on a volume, such as remote defragmentation.	**Default:** Administrators **Required:** No Change	**Default:** (Not Defined) **Required:** Administrators	**Default:** (Not Defined) **Required:** No Change	Could be used to support the following TOE Security Functional **Requirement:** FMT_SMR.1 Security Roles. Could be used to support the following TOE Security functions: Para 6.1.5.1, Roles. Can be used to grant authorized users the administrative capability to perform volume maintenance. Users with this user right can explore disks and extend files in to memory that contain other data. When the extended files are opened, the user might be able to read and modify the acquired data. **Changes:** Set the Domain Security Policy to Administrators for this privilege to support trusted administration.
Profile a single process (SeProfileSingleProcessPrivilege)	This security setting determines which users can use performance	**Default:** Administrators	**Default:** (Not Defined)	**Default:** Administrators	Could be used to support the following TOE Security Functional **Requirement:**

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	monitoring tools to monitor the performance of non-system processes. LocalSystem has this privilege by default.	Power Users **Recommended:** No Change	**Recommended:** No Change	**Recommended:** No Change	FMT_SMR.1 Security Roles. Could be used to support the following TOE Security functions: Para 6.1.5.1, Roles. Can be used to grant authorized users the administrative capability to run performance diagnostics of non-system processes. However, the ST does not claim to address the ability provided by this privilege specifically.
Profile system performance (SeSystemProfilePrivilege)	This security setting determines which users can use performance monitoring tools to monitor the performance of system processes.	**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 Supports the following TOE Security functions: Para 6.1.5.1, Roles and Para 6.1.6.1, System Integrity. Can be used to grant authorized users the administrative capability to run performance diagnostics of system processes.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					Changes: Set the Domain Security Policy to Administrators for this privilege to support trusted administration.
Remove computer from docking station (SeUndockPrivilege)	This security setting determines whether a user can undock a portable computer from its docking station without logging on.	**Default:** Administrators Power Users Users **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** Administrators **Recommended:** No Change	
Replace a process-level token (SeAssignPrimaryTokenPrivilege)	This security setting determines which user accounts can call the `CreateProcessAsUser()` application programming interface (API) so that one service can start another. An example of a process that uses this user right is Task Scheduler.	**Default:** * IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE **Required:** No Change	**Default:** (Not Defined) **Required:** No Change	**Default:** LOCAL SERVICE NETWORK SERVICE **Required:** No Change	Assignment of this privilege violates the following TOE Security Functional **Requirement:** FDP_ACF.1(a), Discretionary Access Control Functions and FIA_USB.1_EX, User Subject Binding, and FAU_GEN.1, Audit Data Generation. This privilege is not auditable.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
					Changes: Change the 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. * The IWAM_ComputerName account is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0.
Restore files and directories (SeRestorePrivilege)	This security setting determines which users can bypass file, directory, registry, and other persistent object's permissions when restoring backed up files and directories, and determines which users can set any valid security principal as the owner of an object. Specifically, this user right is similar to granting the following permissions to the	**Default:** Administrators Backup Operators **Required:** No Change	**Default:** (Not Defined) **Required:** Administrators Backup Operators	**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 restrictions. Implements the following TOE Security functions:

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	user or group in question on all files and folders on the system: Traverse Folder / Execute File Write				Para 6.1.5.1, 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 through membership in the Administrators, Backup Operators, or Server Operators groups. Exception: The Windows Server 2003 Certificate Server Evaluated Configuration is allowed to assign this right to a CA Backup Operator administrative role by assignment in the Backup Operator's group. See the Windows Server 2003 Certificate Server Security Configuration Guide for details.
Shut down the system (SeShutdownPrivilege)	This security setting determines which users who are logged on locally to the computer can shut down the operating system	**Default:** Administrators Backup Operators	**Default:** (Not Defined)	**Default:** Administrators Backup Operators	

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	using the Shut Down command.	Power Users **Recommended:** No Change	**Recommended:** No Change	Print Operators Server Operators **Recommended:** 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 properties. By default, it is assigned to the LocalSystem account on domain controllers.	**Default:** None **Recommended:** No Change	**Default:** (Not Defined) **Recommended:** No Change	**Default:** None **Recommended:** No Change	
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,	**Default:** Administrators	**Default:** (Not Defined)	**Default:** Administrators	**Supports the following TOE Security Functional Requirement:** FMT_SMR.1 Security Roles.

User Rights/Privileges	Description	Stand-alone Windows Server 2003 (Local Security Policy)	Windows Server 2003 (Domain Security Policy)	Windows Server 2003 Domain Controller (Domain Controller Security Policy)	Applicable Security Target Requirements and/or Rationale for Change
	processes, and threads.	**Required:** No Change	**Required:** Administrators	**Required:** No Change	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 6.1.5.1, Roles. Can be used to grant authorized users the administrative capability of any securable object in the system. **Changes:** Set the Domain Security Policy to Administrators for this privilege to support trusted administration.

Appendix D User and Group Accounts

Table D.1 User and group accounts

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	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 or 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.
ASPNET	This account is used for running the ASP.NET worker process in IIS 5.0 isolation mode. It is used when doing ASP.NET development on the local computer. ASPNET has the following default user rights: Access this computer from a network (SeNetworkLogonRight) Log on as a batch job (SeBatchLogonRight)	✓			ASP.NET is not included in the Windows Server 2003 Evaluated Configuration. **Requirement:** This account should be disabled or deleted.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	Log on as a service (SeInteractiveLogonRight) Deny logon locally (SeDenyInteractiveLogonRight) Deny logon through Terminal Services (SeDenyRemoteInteractiveLogonRight)				
Guest	A built-in account used to log on to a computer running Windows when a user does not have an account on the computer, or domain, or in any of the domains trusted by the computer's domain. A user whose account is disabled, but not deleted, can also use the Guest account. The Guest account does not require a password. The Guest account is disabled by default, but can be enabled.	✓	✓		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.
HelpAssistant (installed with a Remote Assistance session)	The primary account used to establish a Remote Assistance session. This account is created automatically when a request is made for a Remote Assistance session and has limited access to the computer. The HelpAssistant account is managed by the Remote Desktop Help Session Manager service and is automatically	✓			Use of this account by more than one user violates FAU_GEN.2, User Identity Association. This account is disabled by default. **Requirement:** Terminal Services is not an objective of the

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	deleted if no Remote Assistance requests are pending.				TOE and accounts that support anonymous access are not to be allowed. Therefore, this account must remain disabled.
IUSR_ComputerName	This account is used for anonymous access to IIS. By default, when a user accesses a Web site that uses Anonymous authentication, that user is mapped to the IUSR_ComputerName account. IUSR_ComputerName has the following default user rights: Access this computer from a network (SeNetworkLogonRight) Bypass traverse checking (SeChangeNotifyPrivilege) Log on as a batch job (SeBatchLogonRight) Allow log on locally (SeInteractiveLogonRight)	✓			The IUSR_ComputerName account is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0.
IWAM__ComputerName	This account is for starting out-of-process applications in IIS 5.0 isolation mode. IWAM_ComputerName has the following default user rights: Access this computer from a network (SeNetworkLogonRight) Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)	✓			The IWAM_ComputerName account is installed with IIS 6.0 and is allowed only on a Windows Server 2003 running IIS 6.0.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	Bypass traverse checking (SeChangeNotifyPrivilege) Log on as a batch job (SeBatchLogonRight) Replace a process-level token (SeAssignPrimaryTokenPrivilege)				
krbtgt	Key distribution service center account. Windows Server 2003 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. **Note:** In Windows Server 2003, this account is not listed in the Active Directory Users and Computers interface.		✓		This account is disabled on domain controllers by default. Unlike other user accounts, the krbtgt account cannot be used to log on to the domain and in fact, cannot be enabled.
SUPPORT_388945a0	Account used to control access to signed scripts that are accessible from within Help and Support Services. Administrators can use this account to	✓	✓		Use of this account by more than one user violates FAU_GEN.2, User Identity Association.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	delegate the ability for an ordinary user, who does not have administrative access over a computer, to run signed scripts from links embedded within Help and Support Services.				This account is disabled by default. **Requirement:** The Help and Support Services functions are not an objective of the TOE and accounts that support anonymous access are not to be allowed. This account must remain disabled or can be deleted.
Global Groups	**When a domain is created, Windows Server 2003 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.**
DnsUpdateProxy (installed with DNS)	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).		✓	None	The TOE will support Fully Qualified Domain Name (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 Server 2003 computers configured 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		✓	Administrator	Supports assignment of administrative role with control within a specific domain. **Requirement:** Do not add non-administrative accounts (users) to this group.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	controller as its member.				
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 Server 2003 computers configured as domain controllers and initially only contains the Guest user account for the domain. Members of this group are only allowed to access the system from across the network and have very limited privileges by default.		✓	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.
Domain Users	This group is only available on Windows Server 2003 computers configured 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 Krbtgt SUPPORT_388945a0 (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 SUPPORT_388945a0 account, if desired. This may require changing the account's primary group or deleting the account from the computer. Do not add accounts that allow unauthenticated access to this group.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Enterprise Admins (only appears in the forest root domain)	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 (on root domain controller)	Supports assignment of administrative role with control over the entire network. **Requirement:** Do not add non-administrative accounts to this group.
Group Policy Creator Owners	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.
Schema Admins	Designated administrators of the Active Directory schema. Members of this group are authorized to make schema changes in Active Directory.		✓	Administrator	Supports assignment of administrative role designated to administer the Active Directory Schema. This group has significant power in the forest. **Requirement:** Do not add non-administrative accounts to this group.
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**

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
					Roles TOE Security Functional Requirement.
Account Operators	This group is only available on Windows Server 2003 computers configured as 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.
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.
Backup Operators	Members can back up and restore files on all domain controllers by using Windows Backup, regardless of the		✓	None	Misuse of this account can violate FDP_ACF.1(a), Discretionary Access Control. A member of the Backup Operators group can

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	permissions that protect those files. Backup Operators also can log on to the computer and shut it down.				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:** Do not add non-administrative accounts to this group.
Cert Publishers	Group account used for 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	**Requirement:** Do not add users to this group. Ensure that only authorized Certification Authority hosts are added to this group.
Certsvc_DCOM_Access	If a certification authority is installed on a domain controller, CERTSVC_DCOM_ACCESS is created as a domain local group and the Domain Users security group and the Domain Computers security group		✓	Domain Users Domain Computers	

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	from the certification authority's domain are added to it. This group is granted: Local and remote access permissions; Local and remote activation permissions; and Local or remote launch permissions. If the certification authority is installed on a domain controller, and the enterprise is made up of more than one domain, Certificate Services cannot automatically update the DCOM security settings for enrollees from outside the certification authority's domain. Therefore, these enrollees are denied enroll access to the certification authority. To resolve this issue, the user groups from the trusted domain must be manually added to the CERTSVC_DCOM_ACCESS security group.				
DnsAdmins (installed with DNS)	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.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
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	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.
HelpServicesGroup	Members of this group can use helper applications to diagnose system problems. This group, in conjunction with the SUPPORT_388945a0 and HelpAssistant accounts, can be used by members of Microsoft Help and Support Center to access the computer from the network and to log on locally.		✓	SUPPORT_388945a0	**Requirement:** Helper applications are not an objective of the TOE. Therefore, do not grant resource permissions or add user accounts to this group. Remove the SUPPORT_388945a0 account from this group.
Incoming Forest Trust Builders	A group whose members can create incoming, one-way forest trusts to the forest-root domain. For example, members of this group residing in forest A can create a one-way incoming forest trust from forest B. This one-way incoming forest trust allows users in forest A to access resources that are located in forest B. Members of this group are assigned the permission Create Inbound Forest Trust on the forest-root domain.		✓	None	Supports assignment of an administrative role with the ability to configure and modify network trust settings. **Requirement:** Do not add non-administrative accounts to this group.
Network Configuration Operators	Members of this group have limited administrative privileges that allow		✓	None	Supports assignment of an administrative role with the ability to configure and modify network

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	them to configure networking features, such as IP address assignment.				settings. **Requirement:** Do not add non-administrative accounts to this group.
Performance Log Users	Members of this group can manage performance counters, logs and alerts on domain controllers in the domain, locally and from remote clients without being a member of the Administrators group.		✓	NETWORK SERVICE	Supports assignment of an administrative role with the ability to configure and modify performance logs and alert settings. **Requirement:** Do not add non-administrative accounts to this group.
Performance Monitor users	Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients without being a member of the Administrators or Performance Log Users groups.		✓	None	Supports assignment of an administrative role with the ability to monitor performance counters. **Requirement:** Do not add non-administrative accounts to this group.
Pre-Windows 2000 Compatible Access	A backward compatibility group that allows read access on all users and groups in the domain.		✓	Authenticated Users	**Requirement:** Backward compatibility with pre-Windows 2000 systems is not an objective of the TOE. Therefore, remove Authenticated Users from this group and do not add other accounts 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		✓	None	Supports assignment of administrative role responsible for managing print services within a domain.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	group are 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.				Recommendation: This is an administrative function, therefore only add authorized administrators to this group.
Remote Desktop Users	Members of this group have the right to log on remotely.		✓	None	**Requirement:** Remote Desktop access is not an objective of the TOE. Therefore, do not grant resource permissions or add user accounts 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 Server 2003-based computers.		✓	None	Can be used in support of requirements identified in Para 6.1.5.3, TSF 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.
Remote Access Service (RAS) and Internet Authentication Service (IAS) Servers	Servers in this group can access remote access properties of users.		✓	None	RAS and IAS are not included in the Evaluated Configuration of Windows Server 2003.
Server Operators	This group is only available on Windows Server 2003 computers configured as domain controllers. Members of this group can perform server management tasks such as creating, changing, and deleting		✓	None	Supports assignment of administrative role responsible for server maintenance. **Requirement:** Do not add non-administrative accounts to this

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	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 services.				group.
TelnetClients	Members of this group have access to Telnet Server on the system. When the TelnetClients group exists, the Telnet service will allow only those users defined in the group to have access to the server.		✓	None	The Telnet service is not included in the Evaluated Configuration of Windows Server 2003.
Terminal Server License Servers	A Terminal Server License Server stores all client licenses that have been installed for a terminal server. A terminal server must be able to connect to an activated Terminal Server License Server before clients can be issued licenses. One Terminal Server License Server can serve many terminal servers concurrently. Terminal Server License Server should be installed on a computer that is not a terminal server.		✓	None	Terminal Server is not included in the Evaluated Configuration of Windows Server 2003.
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 Server 2003 adds all new local user		✓	Authenticated Users Domain Users INTERACTIVE (all new local users are	Supports assignment of user role supporting access to resources on the domain controller. **Requirement:** Do not add accounts with potential for unauthenticated access (such as Guest) to this

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	accounts to the Users group.			added by default)	group.
Windows Authorization Access Group	An alias. Members of this group have access to the computed **tokenGroupsGlobalAndUniversal** attribute on User objects.		✓	ENTERPRISE DOMAIN CONTROLLERS	Group account used by domain controllers. Recommendation: Maintain the default memberships and do not add accounts to this group.
Local Groups	**All stand-alone Windows Server 2003 and Domain member servers 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 computer running Windows Server 2003 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.
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 would normally not have access. Membership

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
					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.
Certsvc_DCOM_Access	If a certification authority is installed on a member server, CERTSVC_DCOM_ACCESS is created as a computer local group, and the Everyone security group is added to it. This group is granted: Local and remote access permissions; Local and remote activation permissions; and Local or remote launch permissions.	✓		Everyone	
DHCP Administrators (installed with the DHCP	Members of this group have administrative access to the Dynamic Host Configuration Protocol (DHCP)	✓		None	Supports assignment of administrative role with full administrative access rights to DHCP

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
Server service)	Server service. This group provides a way to assign limited administrative access to the DHCP server only, while not providing full access to the server. Members of this group can administer DHCP on a server using the DHCP console or the **Netsh** command, but are not able to perform other administrative actions on the server.				servers. **Requirement:** Do not add non-administrative accounts to this group.
DHCP Users (installed with the DHCP Server service)	Members of this group have read-only access to the DHCP Server service. This allows members to view information and properties stored at a specified DHCP server. This information is useful to support staff when they need to obtain DHCP status reports.	✓		None	Supports assignment of administrative role with read access rights to DHCP servers. **Requirement:** Do not add non-administrative accounts to this group.
Distributed COM Users	Members of this group are allowed to launch, activate and use Distributed Component Object Model (COM) objects on the local computer. Distributed COM Users is a new built-in group included with Windows Server 2003 Service Pack 1 to expedite the process of adding users to the DCOM computer restriction settings.	✓	✓	None	The default DCOM computer restriction settings are not altered in the Evaluated Configuration. Therefore, there is no need to use this group in the Evaluated Configuration.
Guests	The Guest group offers limited access to resources on the system. Members	✓		**Stand-alone:**	Guest/anonymous accounts can violate FAU_GEN.2, User Identity Association,

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	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.			Guest Domain Members: Guest Domain Guests	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.
HelpServicesGroup	Members of this group can use helper applications to diagnose system problems. This group, in conjunction with the SUPPORT_388945a0 and HelpAssistant accounts, can be used by members of Microsoft Help and Support Center to access the computer from the network and to log on locally.	✓		**Stand-alone:** SUPPORT_388945a0 **Domain member:** SUPPORT_388945a0	**Requirement:** Helper applications are not an objective of the TOE. Therefore, do not grant resource permissions or add user accounts to this group. Remove the SUPPORT_388945a0 account from this group.
IIS_WPG (installed with IIS 6.0)	This group account has the minimum permissions and user rights that are necessary to start and run a worker process on a Web server. Within the functioning of IIS 6.0 are worker processes that serve specific namespaces. For example, www.microsoft.com is a namespace served by one worker process, which can run under an identity added to the IIS_WPG group, such as MicrosoftAccount. This group is only available on Windows Server 2003 computers hosting an Internet Information Services (IIS) Web server.	✓		**Stand-alone:** IWAM_ComputerName LOCAL SERVICE NETWORK SERVICE SYSTEM **Domain member:** IWAM_ComputerName	**Requirement:** This is a group account for IIS services. Do not add users to this group.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	IIS_WPG has the following default user rights: Log on as a batch job (SeBatchLogonRight) Impersonate a client after authentication (SeImpersonatePrivilege)			LOCAL SERVICE NETWORK SERVICE SYSTEM	
Network Configuration Operators	Members of this group have limited administrative privileges that allow them to configure networking features, such as IP address assignment.	✓		None	Supports assignment of an administrative role with the ability to configure and modify network settings. **Requirement:** Do not add non-administrative accounts to this group.
Performance Log Users	Members of this group can manage performance counters, logs and alerts on domain controllers in the domain, locally and from remote clients without being a member of the Administrators group.	✓		NETWORK SERVICE	Supports assignment of an administrative role with the ability to configure and modify performance logs and alert settings. **Requirement:** Do not add non-administrative accounts to this group.
Performance Monitor users	Members of this group can monitor performance counters on domain controllers in the domain, locally and from remote clients without being a member of the Administrators or Performance Log Users groups.	✓		None	Supports assignment of an administrative role with the ability to monitor performance counters. **Requirement:** Do not add non-administrative accounts to this

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
					group.
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 granted privileges generally associated with an authorized administrator role. **Requirement:** Do not add non-administrative accounts 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 given the rights to create, change, and delete printer shares within the domain. Members can also log on to systems locally and shut	✓		None	Supports assignment of administrative role responsible for managing print services within a domain. Recommendation: This is an administrative function, therefore only add authorized administrators to this group.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	them down.				
Remote Desktop Users	Members of this group have the right to log on remotely.	✓		None	**Requirement:** Remote Desktop access is not an objective of the TOE. Therefore, do not grant resource permissions or add user accounts to this group.
Replicator	Members can configure file replication services. The directory Replicator Service is used to automatically copy files, such as user logon scripts, between Windows Server 2003-based computers.	✓		None	Can be used in support of requirements identified in Para 6.1.5.3, TSF Data Replication Consistency. Supports assignment of administrative role responsible for administering directory replication services within a computer. **Requirement:** Do not add non-administrative accounts to this group.
TelnetClients	Members of this group have access to the Telnet Server on the system. When the TelnetClients group exists, the Telnet service will allow only those users defined in the group to have access to the server.	✓		None	The Telnet service is not included in the Evaluated Configuration of Windows Server 2003.
TERMINAL SERVER USERs	This group contains any users who are currently logged on to the system using Terminal Services. Any program that a user can run with Windows NT 4.0 will run for a member of the TERMINAL SERVER USER group. The default permissions assigned to this group enable its members to run	✓			Terminal Server is not included in the Evaluated Configuration of Windows Server 2003.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	most programs developed prior to the release of Windows Server 2003.				
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 Server 2003 adds all new local user accounts to the Users group. When a computer running Windows Server 2003 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.
WINS Users (installed with WINS service)	Members of this group are permitted read-only access to Windows Internet Name Service (WINS). This allows members to view information and properties stored at a specified WINS server. This information is useful to support staff when they need to obtain WINS status reports.	✓			WINS is not included in the Evaluated Configuration of Windows Server 2003.
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				

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	are created by Windows Server 2003 systems automatically, but are not shown in the group administration GUIs.				
ANONYMOUS LOGON	Includes any user account that Windows Server 2003 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.	✓	✓	All users that have logged on through a batch queue facility.	Recommendation: Do not use this group. Do not grant resource permissions or user rights to this group.
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	✓	✓		Supports FDP_ACF.1(a), Discretionary Access Control Functions through assignment of object owner attributes.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	on Windows Server 2003 Server. 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.				
CREATOR GROUP	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's creator.	✓	✓	This account is replaced by the primary group of an object's creator and will allow the specified group access to all members of that group.	May violate FDP_ACF.1(a), Discretionary Access Control Functions. Improper use may allow all members of a group access to an object creator's resources. Recommendation: Use the CREATOR GROUP placeholder only in cases where all members of a group are to be allowed access to an object creator's resources. Otherwise, use the CREATOR OWNER placeholder instead to ensure that only the object creator is granted access.
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.
Digest Authentication	The Digest Authentication account is associated with a user token to define which package has been used to do the authentication as part of the token creation.		✓		

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
ENTERPRISE DOMAIN CONTROLLERS	A group that includes all domain controllers in a forest that uses an Active Directory Service.		✓		
Everyone	A group that includes all users, including Guests. In Windows 2003, the built-in Everyone group includes Authenticated Users and Guests, but no longer includes members of ANONYMOUS LOGON. Windows Server 2003 will attempt to authenticate a user who does not have a valid user account as Guest, unless Guest is disabled. The user automatically gets all rights and permissions assigned to the Everyone group.	✓	✓	Members of this group include all users accessing Windows Server 2003 locally, through the network, or through RAS. By default, Everyone includes Authenticated Users and Guests, but not anonymous logons.	Due to its inclusion of the Guest account, 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 on to Windows Server 2003 locally. Users who are connected across a network are not members of this group.	**Requirement:** Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.
LOCAL SERVICE	An account used to run services that are local to the computer, have no need for extensive local privileges, and do not need authenticated network access. A service running as LOCAL SERVICE has significantly less authority than a service running as SYSTEM, both locally and on the network. When services running as	✓	✓	This is a service account.	

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	LOCAL SERVICE access local resources, they do so as members of the local Users group. When they access network resources, they do so as Anonymous users. Use the LOCAL SERVICE user account if the worker process does not require access outside the server on which it is running. LOCAL SERVICE has the following default user rights: Replace a process-level token (SeAssignPrimaryTokenPrivilege) Adjust memory quotas for a process (SeIncreaseQuotaPrivilege) Generate security audits (SeAuditPrivilege) Bypass traverse checking (SeChangeNotifyPrivilege) Access this computer from a network (SeNetworkLogonRight) Log on as a batch job (SeBatchLogonRight)				
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	Recommendation: Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
				include those who are connected interactively.	where necessary.
NETWORK SERVICE	An account used to run services that have no need for extensive local privileges but do need authenticated network access. A service running as NETWORK SERVICE has the same network access as a service running as SYSTEM, but has significantly reduced local access. When services running as NETWORK SERVICE access local resources, they do so as members of the local Users group. When they access network resources, they do so using the SID assigned to the computer. NETWORK SERVICE has the following default user rights: Replace a process-level token (SeAssignPrimaryTokenPrivilege) Adjust memory quotas for a process (SeIncreaseQuotaPrivilege) Generate security audits (SeAuditPrivilege) Bypass traverse checking (SeChangeNotifyPrivilege) Access this computer from a network (SeNetworkLogonRight) Log on as a batch job (SeBatchLogonRight)	✓	✓	This is a service account.	

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
	Log on as a service (SeInteractiveLogonRight) Allow log on locally (SeInteractiveLogonRight)				
NTLM Authentication	The NTLM Authentication account is associated with a user token to define which package has been used to do the authentication as part of the token creation.		✓		
Other Organization	This account is present in tokens on all Windows XP, Windows Server 2003 and later systems that are coming across an Other Organization trust. It causes a check to ensure that a user from another forest or domain is allowed to authenticate to a particular service. This is part of the mechanism to support cross forest trust.		✓		
PROXY	This SID is not used in Windows Server 2003.		✓		
REMOTE INTERACTIVE LOGON	Account used to represent users accessing the computer by way of a Remote Desktop connection.	✓	✓	This group includes all users who log on to the computer by using a Remote Desktop connection.	**Requirement:** Remote Desktop access is not an objective of the TOE. Therefore, do not assign resource permissions or user rights to this account.

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
RESTRICTED	This SID is not used in Windows Server 2003.		✓		
SChannel Authentication	Secure Channel, also known as Schannel, is a security support provider (SSP) containing a set of security protocols that provide identity authentication and enhanced communication security through encryption. Schannel is primarily used for Internet applications that require enhanced security for Hypertext Transfer Protocol (HTTP) communications. The SChannel Authentication account is associated with a user token to define which package has been used to do the authentication as part of the token creation.		✓		
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.	✓	✓	All security principals logged on as a service.	**Requirement:** This is a service account. Instead of this account, use the more explicit NETWORK SERVICE or LOCAL SERVICE accounts in

Windows Server 2003 Built-In Users and Groups	Description	Stand-alone Server	Domain Controller	Default Members	Applicability to Security Target Requirements and/or Rationale for Changes
					order to better control service rights.
SYSTEM (LocalSystem)	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. If a worker process identity runs as the LocalSystem user account, that worker process has full access to the entire system.	✓	✓		This account is used by Windows Server 2003 to execute security services such as TSF protection functions that are beyond the control of authorized administrators. **Requirement:** Where specific service rights need to be granted, use the NETWORK SERVICE or LOCAL SERVICE accounts in order to avoid granting full SYSTEM rights to the service.
TERMINAL SERVER USER	A group that includes all users who log on to a Terminal Services server that is in Terminal Services application compatibility mode.	✓	✓		**Requirement:** Terminal service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.
This Organization	This account is present in tokens on all Windows XP, Windows Server 2003 and later systems as long as the authenticated entity is not coming across an Other Organization trust. It is added by the authentication server to the authentication data of a user, provided the Other Organization SID is not already present. An entity coming across an Other Organization trust will have an Other Organization SID in its token. This is part of the mechanism to support cross forest trust.		✓		

Appendix E Windows Server 2003 Security Configuration Checklist for the Evaluated Configuration

This appendix provides a checklist that can be used by authorized administrators as a guide in applying the security configuration settings defined in this document and may also be used to record the selected security configuration options.

Table E-1 can be used to record the oprating system and patch level of the configured computer.

Table E.2 provides a security configuration checklist for administrators to step through after setting up Windows Server 2003. The settings in the table apply to all Windows Server 2003 editions except where otherwise noted.

Table E.1 Operating system configuration checklist

Operating System Configuration		
Operating system type:	❑ Windows Server 2003 Standard Edition (32- & 64-bit)	
	❑ Windows Server 2003 Enterprise Edition (32- & 64-bit)	❑ Domain controller
	❑ Windows Server 2003 Datacenter Edition (32- & 64-bit)	❑ Domain controller
Service pack level:	Windows Server 2003 Service Pack 1 (Required) Service Pack 1 updates are already included in Windows Server 2003 x64 Edition operating systems	Required security updates (Microsoft Security Bulletin / Knowledge Base Article): ❑ MS06-049 / 921398 ❑ MS06-042 / 918899 ❑ MS06-041 / 920683 ❑ MS06-040 / 921883 ❑ Named Pipes Update / 922769 ❑ MS06-036 / 914388 ❑ MS06-035 / 917159 ❑ MS06-030 / 914385 ❑ MS06-015 / 908531 ❑ MS06-008 / 911927 ❑ MS06-001 / 912919 ❑ MS05-053 / 896424 ❑ MS05-051 / 902400 ❑ MS05-049 / 900725 ❑ IPSec Policy Agent / 907865 ❑ MS05-042 / 899587 ❑ MS05-027 / 896422 _____ _____ _____

Table E.2 Windows Server 2003 security configuration checklist

Completed and Verified	Task	Required	Recommended
Modifications During Setup			
❑	***Configure the file system type*** **Security Objective:** Allow configuration of evaluated security mechanisms and support conformance to Security Target requirements. **File System Type:** NTFS	✓	
Miscellaneous Post-Installation Modifications			
❑	***Prevent the automatic installation of device drivers*** **Security Objective:** Prevent the automatic installation of device drivers. **Computer Setting:** Move all information files (.inf files) that contain references to device drivers from the default %SystemRoot%\inf folder to an alternate folder location. Move the Drivers.cab and SP2.cab files from the default %SystemRoot%\Driver Cache folder to an alternate folder location.	✓	
❑	***Set permissions for WMI filters*** **Security Objective:** Remove permissions for the Everyone group. **Computer Setting:** On the WMI Control Properties, remove the security permissions for the group Everyone. Default permissions for Administrators, LOCAL SERVICE, and NETWORK SERVICE must remain.	✓	
❑	***Restrict launch and access permissions for Logical Disk Manager*** **Security Objective:** Remove permissions for the SELF account. **Computer Setting:** On the Logical Disk Manager Administrative Service Properties and the Logical Disk Manager Service Properties interfaces, remove the security permissions for the SELF account.	✓	

Completed and Verified	Task	Required	Recommended
❑	***Configure Distributed Transaction Coordinator (DTC) access*** **Security Objective:** Modify DTC Access. **Computer Setting:** Open the MSDTC Security Configuration interface from the MSDTC tab of the My Computer **Properties** interface and modify the setting to: ▪ allow Network DTC Access ▪ allow Remote clients ▪ allow remote administration ▪ allow inbound transaction manager communication ▪ allow outbound transaction manager communication ▪ require mutual authentication ▪ disable transaction internet protocol transactions ▪ disable XA transactions	✓	
❑	***Disable the creation of dump files*** **Security Objective:** Some system memory dumps may contain sensitive information, such as passwords that may be compromised if the dump file is accessed by an unauthorized user. To prevent the writing of sensitive information to dump files, the creation of dump files must be disabled. **Computer Setting:** Disable the Creation of Dump Files.	✓	
Post-Installation Account Policy Settings			
	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.)		✓

Completed and Verified	Task	Required	Recommended
❑	***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 of characters required for user passwords. **Computer Setting:** 8 characters.	✓	
❑	***Password must meet complexity requirements*** **Security Objective:** Requires the use of complex (strong) passwords. **Computer Setting:** ❑ Enabled ❑ Disabled (**Recommended:** Enabled.)		✓
❑	***Store passwords using reversible encryption*** **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 logon attempts allowed before locking the account. **Computer Setting:** _____ invalid logon 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 logon attempts.)	✓	

Completed and Verified	Task	Required	Recommended
❑	***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.)		✓
❑	***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)	✓	
Post-Installation Local Policy Settings			

Completed and Verified	Task	Required	Recommended
	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)		✓
❑	***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)		✓
❑	***Audit policy change*** **Security Objective:** Audit a change to user rights assignment policies, audit policies, or trust policies. **Computer Setting:** ❑ Success ❑ Failure (**Recommended:** Success, Failure)		✓

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></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, Failure)</td><td></td><td>✓</td></tr>
<tr><td></td><td colspan="3">User Rights Assignment</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:
<table>
<tr><td>Stand-alone / member server
Administrators
Authenticated Users
Backup Operators
Power Users
Users</td><td>IIS Server
Administrators
Authenticated Users
Backup Operators
IUSR_ComputerName
IWAM_ComputerName
Power Users
Users</td><td>Domain controller
Administrators
Authenticated Users
ENTERPRISE DOMAIN CONTROLLERS</td></tr>
</table>
(In Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>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: Do not assign this privilege to any account. The default setting does not assign this privilege to users and must be retained.

<table><tr><td>Stand-alone / member server

None</td><td>IIS Server

None</td><td>Domain controller

None</td></tr></table>(In Default Domain Security Policy set the policy with no accounts.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Add workstations to domain

Security Objective: Allows a user to add a computer to a specific domain.

Computer Setting: This setting is only effective on domain controllers, but must remain blank on all member servers. Remove the Authenticated Users account from domain controllers. The privilege can be assigned to Domain Admins on domain controllers, although this account already has the privilege by default.

<table><tr><td>Stand-alone / member server

None</td><td>IIS Server

None</td><td>Domain controller

Domain Admins</td></tr></table>(In Default Domain Security Policy set the policy with no accounts.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Adjust memory quotas for a process

Security Objective: Determines which accounts can use a process with Write Property access to another process to modify the processor quota assignment.

Computer Setting: Retain the defaults.

<table><tr><td>Stand-alone / member server

Administrators

LOCAL SERVICE

NETWORK SERVICE</td><td>IIS Server

Administrators

IWAM_ComputerName

LOCAL SERVICE

NETWORK SERVICE</td><td>Domain controller

Administrators

LOCAL SERVICE

NETWORK SERVICE</td></tr></table>(In Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Allow log on locally

Security Objective: Allows a user to log on locally at the computer’s keyboard.

Computer Setting:
<table><tr><td>Stand-alone / member server
Administrators
Backup Operators
Power Users
Users</td><td>IIS Server
Administrators
Backup Operators
IUSR_ComputerName
Power Users
Users</td><td>Domain controller
Account Operators
Administrators
Backup Operators
Print Operators
Server Operators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Allow log on through Terminal Services

Security Objective: Determines which users or groups are allowed to log on as a Terminal Services client.

Computer Setting: Do not assign this user right to any account. Terminal Services is not included in the Evaluated Configuration. In the Default Domain Security Policy, set the policy with no accounts.</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Back up files and directories

Security Objective: Allows the user to circumvent file and directory permissions to backup the system.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server
Administrators
Backup Operators</td><td>IIS Server
Administrators
Backup Operators</td><td>Domain controller
Administrators
Backup Operators
Server Operators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Bypass traverse checking

Security Objective: Allows the user to pass through folders to which the user otherwise has no access.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Change the system time

Security Objective: Allows the user to set the time for the internal clock of the computer.

Computer Setting: Retain the defaults.

<table><tr><td>Stand-alone / member server

Administrators

Power users</td><td>IIS Server

Administrators

Power users</td><td>Domain controller

Administrators

LOCAL SERVICE

Server Operators</td></tr></table>
(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Create a pagefile

Security Objective: Allows the user to create and change the size of a pagefile.

Computer Setting: Retain the defaults. Ensure all policies, including the Default Domain Security Policy, are set to Administrators only.</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Create a token object

Security Objective: Allows a process to create an access token.

Computer Setting: Do not assign this privilege to any account. The default setting does not assign this privilege to users and must be retained.

<table><tr><td>Stand-alone / member server

None</td><td>IIS Server

None</td><td>Domain controller

None</td></tr></table>
(In the Default Domain Security Policy set the policy with no accounts.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Create global objects

Security Objective: Allow a user to create Global objects during Terminal Services sessions. Terminal Services is not included in the Evaluated Configuration.

Computer Setting:

_____ _____ _____
_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Create permanent shared objects

Security Objective: Allow a process to create a directory object in the Windows Server 2003 and Windows XP object manager.

Computer Setting:

_____ _____ _____
_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Debug programs

Security Objective: Allows the user to attach a debugger to any process.

Computer Setting: Do not assign this privilege to any account. The default setting does not assign this privilege to users and must be retained.

<table><tr><td>Stand-alone / member server

None</td><td>IIS Server

None</td><td>Domain controller

None</td></tr></table>
(In the Default Domain Security Policy set the policy with no accounts.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>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: Retain the defaults. Organizations may add other accounts to this policy as needed.

<table><tr><td>Stand-alone / member server

SUPPORT_388945a0

_____

_____</td><td>IIS Server

SUPPORT_388945a0

_____

_____</td><td>Domain controller

SUPPORT_388945a0

_____

_____</td></tr></table>(In the Default Domain Security Policy set as indicated in the Windows XP Professional Security Configuration Guide, Version 3.0; Guest, SUPPORT_388945a0.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Deny logon as a batch job

Security Objective: Prohibits a user or group from logging on through a batch-queue facility.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Deny logon as a service

Security Objective: Prohibits a user or group from logging on as a service.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Deny logon locally

Security Objective: Prohibits a user or group from logging on locally at the keyboard.

Computer Setting: Retain the defaults. Organizations may add other accounts to this policy as needed.
<table><tr><td>Stand-alone / member server

SUPPORT_388945a0

_____

_____</td><td>IIS Server

SUPPORT_388945a0

_____

_____</td><td>Domain controller

SUPPORT_388945a0

_____

_____</td></tr></table>(In the Default Domain Security Policy set as indicated in the Windows XP Professional Security Configuration Guide, Version 3.0; Guest, SUPPORT_388945a0.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Deny logon through Terminal Services

Security Objective: Prohibits a user or group from logging on as a Terminal Services client.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>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:
<table><tr><td>Stand-alone / member server

None</td><td>IIS Server

None</td><td>Domain controller

Administrators</td></tr></table>(In the Default Domain Security Policy set the policy with no accounts.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>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:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Generate security audits

Security Objective: Allows a process to generate entries in the Security log.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

LOCAL SERVICE

NETWORK SERVICE</td><td>IIS Server

LOCAL SERVICE

NETWORK SERVICE</td><td>Domain controller

LOCAL SERVICE

NETWORK SERVICE</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Impersonate a client after authentication

Security Objective: Allows programs running on behalf of a user to impersonate a client.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators

SERVICE</td><td>IIS Server

Administrators

IIS_WPG

SERVICE</td><td>Domain controller

Not Defined</td></tr></table>(In the Default Domain Security Policy, do not change the default of Not Defined.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Increase scheduling priority

Security Objective: Allows a process that has Write Property access to another process to increase the execution priority of the other process.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Administrators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Load and unload device drivers
Security Objective: Allows a user to install and uninstall Plug and Play device drivers.
Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server
Administrators</td><td>IIS Server
Administrators</td><td>Domain controller
Administrators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>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:
_____ _____ _____
_____ _____ _____
(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Log on as a batch job
Security Objective: Allows a user to log on by using a batch-queue facility.
Computer Setting:
<table><tr><td>Stand-alone / member server
LOCAL SERVICE</td><td>IIS Server
IIS_WPG
IUSR_ComputerName
IWAM_ComputerName
LOCAL SERVICE</td><td>Domain controller
LOCAL SERVICE</td></tr></table>(Recommended: Remove the SUPPORT_388945a0 account. In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Log on as a service
Security Objective: Allows a security principal to log on as a service.
Computer Setting:
_____ _____ _____
_____ _____ _____
(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>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: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Administrators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>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: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Administrators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Perform volume maintenance tasks

Security Objective: Determines which accounts can run maintenance tasks on a volume.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Not Defined</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Profile single process

Security Objective: Allows a user to run performance monitoring tools to monitor the performance of non-system processes.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Profile system performance

Security Objective: Allows a user to run performance monitoring tools to monitor the performance of system processes.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Not Defined</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>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:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>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: Retain the defaults.
<table><tr><td>Stand-alone / member server

LOCAL SERVICE

NETWORK SERVICE</td><td>IIS Server

IWAM_ComputerName

LOCAL SERVICE

NETWORK SERVICE</td><td>Domain controller

LOCAL SERVICE

NETWORK SERVICE</td></tr></table>(In the Default Domain Security Policy, do not change the default of Not Defined.)</td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>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: Retain the defaults.

<table><tr><td>Stand-alone / member server

Administrators

Backup Operators</td><td>IIS Server

Administrators

Backup Operators</td><td>Domain controller

Administrators

Backup Operators

Server Operators</td></tr></table>
(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Shut down the system

Security Objective: Allows a user to shut down the local computer

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults.)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Synchronize directory service data

Security Objective: Allows a service to provide directory synchronization services.

Computer Setting:

_____ _____ _____

_____ _____ _____

(Recommended: Do not change the defaults.)</td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Take ownership of files or other objects

Security Objective: Allows the user to take ownership of any securable object in the system.

Computer Setting: Retain the defaults.
<table><tr><td>Stand-alone / member server

Administrators</td><td>IIS Server

Administrators</td><td>Domain controller

Administrators</td></tr></table>(In the Default Domain Security Policy set as indicated for stand-alone / member servers.)</td><td>✓</td><td></td></tr>
<tr><td></td><td colspan="3">Security Options</td></tr>
<tr><td>❑</td><td>Accounts: Administrator account status

Security Objective: Determines whether the Administrator account is enabled or disabled under normal operations.

Computer Setting: ❑ Enabled ❑ Disabled ❑ Not defined

(Recommended: Enabled)</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Accounts: Guest account status

Security Objective: Determines whether the Administrator account is enabled or disabled.

Computer Setting: Disabled</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Accounts: Limit local account use of blank passwords to console logon only

Security Objective: Determines whether remote interactive logons by network services such as Terminal Services, Telnet, and FTP are allowed for local accounts that have blank passwords.

Computer Setting: Enabled</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Accounts: Rename administrator account

Security Objective: Associates a different account name with the security identifier (SID) for the Administrator account.

Computer Setting: _____

(Recommended: Change and safeguard the recorded account name. Do not record it in this document.)</td><td></td><td>✓</td></tr>
</table>

Completed and Verified	Task	Required	Recommended
❑	***Accounts: Rename guest account*** **Security Objective:** Associates a different account name with the security identifier (SID) for the Guest account. **Computer Setting:** _____ (**Recommended:** Change and safeguard the recorded account name. Do not record it in this document.)		✓
❑	***Audit: Audit the access of global system objects*** **Security Objective:** Allows access of global system objects to be audited. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled, only when there is a strict audit management process in place.)		✓
❑	***Audit: Audit the use of Backup and Restore privilege*** **Security Objective:** Allow auditing of Backup and Restore user rights. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled, only when there is a strict audit management process in place.)		✓
❑	***Audit: 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 ❑ Not defined (**Recommended:** Enabled, only when there is a strict audit management process in place.)		✓
❑	***DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax*** **Security Objective:** DCOM access permissions control authorization to call a running COM server. **Computer Setting:** (**Recommended:** Do not change the default setting.)		✓
❑	***DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax*** **Security Objective:** DCOM launch permissions control authorization to start a COM server during COM activation if the server is not already running. **Computer Setting:** (**Recommended:** Do not change the default setting.)		✓

Completed and Verified	Task	Required	Recommended
❑	***Devices: Allow undock without having to log on*** **Security Objective:** Determines whether a user must log on to request that a portable computer be removed from a docking station. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Disabled for portable computers that cannot be mechanically undocked.)		✓
❑	***Devices: Allowed to format and eject removable media*** **Security Objective:** Determines who is allowed to format and eject removable NTFS media. **Computer Setting:** Accounts defined in the policy: _____ (**Recommended:** Administrators)		✓
❑	***Devices: Prevent users from installing print drivers*** **Security Objective:** Determines whether members of the Users group are prevented from installing print drivers. **Computer Setting:** Enabled	✓	
❑	***Devices: 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	✓	
❑	***Devices: 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	✓	
❑	***Devices: 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.)		✓

Completed and Verified	Task	Required	Recommended
❑	***Domain controller: Allow server operators to schedule tasks*** **Security Objective:** Determines if members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility (The AT schedule facility is not part of the Evaluated Configuration). This policy is only effective on domain controllers. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Domain controller: LDAP server signing requirements*** **Security Objective:** This security setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. This policy is only effective on domain controllers. **Computer Setting:** (**Recommended:** Set to Require signature on domain controllers through the Default Domain Controller Security Policy. Retain the default for all other servers.)		✓
❑	***Domain controller: Refuse machine account password changes*** **Security Objective:** Determines whether or not a domain controller will accept password change requests for computer accounts. This policy is only effective on domain controllers. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Domain member: Digitally encrypt or sign secure channel data (always***) **Security Objective:** Determines whether a secure channel can be established with a domain controller that is not capable of signing or encrypting all secure channel traffic. If this setting is Enabled, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data. If this setting is Disabled, a secure channel can be established, but the level of encryption and signing is negotiated. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled)		✓
❑	***Domain member: Digitally encrypt secure channel data (when possible)*** **Security Objective:** If this setting is enabled, it ensures that all secure channel traffic is encrypted if the partner domain controller is also capable of encrypting all secure channel traffic. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled)		✓

Completed and Verified	Task	Required	Recommended
❑	***Domain member: Digitally sign secure channel data (when possible)*** **Security Objective:** If this setting is enabled, it ensures that all secure channel traffic is signed if the partner domain controller is also capable of signing all secure channel traffic. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled)		✓
❑	***Domain member: Disable machine account password changes*** **Security Objective:** Determines whether a domain member periodically changes its computer account password. If this setting is enabled, the domain member does not attempt to change its computer account password. If this setting is disabled, the domain member attempts to change its computer account password as specified by the setting for **Domain Member: Maximum age for machine account password**, which by default is every 30 days. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Domain member: Maximum machine account password age*** **Security Objective:** Determines the maximum allowable age for a computer account password. By default, this policy is set to 30 days in Windows Server 2003, Not defined in the Default Domain Security Policy, and Not defined in the Default Domain Controller Security Policy. **Computer Setting:** _____ (**Recommended:** Do not change the default setting.)		✓
❑	***Domain member: Require strong (Windows 2000 or later) session key*** **Security Objective:** Determines whether a secure channel can be established with a domain controller that is not capable of encrypting secure channel traffic with a strong (128-bit) session key. If this setting is enabled, a secure channel is not established with any domain controller that cannot encrypt secure channel data with a strong key. **Computer Setting:** Enabled	✓	
❑	***Interactive logon: Display user information when the session is locked*** **Security Objective:** Determines whether a secure channel can be established with a domain controller that is not capable of encrypting secure channel traffic with a strong (128-bit) session key. If this setting is enabled, a secure channel is not established with any domain controller that cannot encrypt secure channel data with a strong key. **Computer Setting:** _____ (**Recommended:** Select **Do not display user information**.)		✓

Completed and Verified	Task	Required	Recommended
❑	***Interactive logon: Do not display last user name*** **Security Objective:** Enabling this option removes the name of the last user from the logon session. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled)		✓
❑	***Interactive logon: Do not require CTRL+ALT+DEL*** **Security Objective:** Determines whether pressing **CTRL+ALT+DEL** is required before a user can log on. **Computer Setting:** Disabled (A setting of Disabled actually requires the use of **CTRL+ALT+DEL**)	✓	
❑	***Interactive logon: 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:** _____ _____ _____ _____	✓	
❑	***Interactive logon: 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:** _____	✓	
❑	***Interactive logon: Number of previous logons to cache (in case domain controller is not available)*** **Security Objective:** Determines how many user account entries Windows XP Professional saves in the logon cache on the local computer. **Computer Setting:** 0 (The required setting is not recommended for mobile computers (laptops) that are used out of the organization's network environment since the user would not be able to log on unless the computer is directly connected to the network.)	✓	

Completed and Verified	Task	Required	Recommended
❑	***Interactive logon: Prompt user to change password before expiration*** **Security Objective:** Determines how far in advance Windows Server 2003 should warn users that their password is about to expire. **Computer Setting:** _____ (**Recommended:** Do not change the default setting.)		✓
❑	***Interactive logon: Require domain controller authentication to unlock workstation*** **Security Objective:** Logon information must be provided to unlock a locked computer. For domain accounts, this setting determines whether a domain controller must be contacted to unlock a computer. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Interactive logon: Require smart card*** **Security Objective:** Controls whether users have to use a smart card to log on to the computer. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Interactive logon: 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.)		✓
❑	***Microsoft network client: Digitally sign communications (always)*** **Security Objective:** Determines whether the computer will always digitally sign client communications. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Disabled)		✓
❑	***Microsoft network client: Digitally sign communications (if server agrees)*** **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	✓	

Completed and Verified	Task	Required	Recommended
❑	***Microsoft network client: 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. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Microsoft network server: Amount of idle time required before suspending 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. **Computer Setting:** _____ (**Recommended:** Do not change the default setting.)		✓
❑	***Microsoft network server: Digitally sign communications (always)*** **Security Objective:** If this policy is enabled, it requires the Windows Server 2003 Server Message Block (SMB) server to perform SMB packet signing. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting on member servers. Set to Disabled in the domain-level policies.)		✓
❑	***Microsoft network server: Digitally sign communications (if client agrees)*** **Security Objective:** If enabled, the SMB server will negotiate SMB packet signing with clients that request it. **Computer Setting:** Enabled	✓	
❑	***Microsoft network server: Disconnect clients when logon hours expire*** **Security Objective:** Determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. The allowed logon hour range for users is set at the domain controller. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting on member servers. Set to Enabled in the domain-level policies.)		✓
❑	***Network access: Allow anonymous SID/Name translation*** **Security Objective:** Determines if an anonymous user can request security identifier (SID) attributes for another user. **Computer Setting:** Disabled	✓	

Completed and Verified	Task	Required	Recommended
❑	***Network access: Do not allow anonymous enumeration of SAM accounts*** **Security Objective:** Controls the ability of anonymous users to enumerate the accounts contained within the Security Accounts Manager (SAM) database by determining which additional permissions will be granted for anonymous connections to the computer. This security policy setting has no impact on domain controllers. **Computer Setting:** Enabled	✓	
❑	***Network access: Do not allow storage of credentials or .NET Passports for network authentication*** **Security Objective:** Determines whether the Stored User Names and Passwords tool saves passwords or credentials for later use when it gains domain authentication. **Computer Setting:** Enabled	✓	
❑	***Network access: Let Everyone permissions apply to anonymous users*** **Security Objective:** Determines if anonymous users are to be allowed the same permissions as the built-in group Everyone. **Computer Setting:** Disabled	✓	
❑	***Network access: Named Pipes that can be accessed anonymously*** **Security Objective:** Determines which communication sessions (pipes) will have attributes and permissions that allow anonymous access. **Computer Setting for Domain and Local Security Policies:** SPOOLSS **Computer Setting for Domain Controller Security Policy:** SPOOLSS, LSARPC	✓	
❑	***Network access: Remotely accessible registry paths*** **Security Objective:** This security setting determines which registry paths are accessible after referencing the access control list (ACL) of the **WinReg** key to determine access permissions to those paths. **Computer Setting:** _____ _____ _____ _____ (**Recommended:** Remove all entries.)		✓

Completed and Verified	Task	Required	Recommended
❑	***Network access: Remotely accessible registry paths and subpaths*** **Security Objective:** This security setting determines which registry paths are accessible after referencing the access control list (ACL) of the **WinReg** key to determine access permissions to those paths. **Computer Setting:** _____ _____ _____ _____ (**Recommended:** Remove all entries.)		✓
❑	***Network access: Restrict anonymous access to named pipes and shares*** **Security Objective:** Enabling this security setting restricts anonymous access to shares and pipes to the settings for Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously. **Computer Setting:** Enabled	✓	
❑	***Network access: Shares that can be accessed anonymously*** **Security Objective:** This security setting determines which network shares can be accessed by anonymous users. **Computer Setting:** Remove all entries.	✓	
❑	***Network access: Sharing and security model for local accounts*** **Security Objective:** This security setting determines how network logons using local accounts are authenticated. **Computer Setting:** Classic-local users authenticate as themselves	✓	
❑	***Network security: Do not store LAN Manager hash value on next password change*** **Security Objective:** This security setting determines if, at the next password change, the LAN Manager (LM) hash value for the new password is stored. **Computer Setting:** Enabled	✓	
❑	***Network security: Force logoff when logon hours expire*** **Security Objective:** This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. **Computer Setting:** Enabled (To be effective it must be enforced by the Default Domain Security Policy in a Windows Server 2003 domain.)	✓	

Completed and Verified	Task	Required	Recommended
❑	***Network security: LAN Manager authentication level*** **Security Objective:** This security option is used to set the Windows Challenge/Response authentication level. **Computer Setting:** _____ (**Recommended:** Send NTLMv2 response only\refuse LM & NTLM)		✓
❑	***Network security: LDAP client signing requirements*** **Security Objective:** This security setting determines the level of data signing that is requested on behalf of clients issuing LDAP BIND requests. **Computer Setting:** _____ (**Recommended:** Require signing)		✓
❑	***Network security: Minimum session security for NTLM SSP based (including secure RPC) clients*** **Security Objective:** This security setting allows a client to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. **Computer Setting:** Select all of the options by checking the selection box for each of the options presented.	✓	
❑	***Network security: Minimum session security for NTLM SSP based (including secure RPC) servers*** **Security Objective:** This security setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. **Computer Setting:** Select all of the options by checking the selection box for each of the options presented.	✓	
❑	***Recovery console: Allow automatic administrative logon*** **Security Objective:** If this option is enabled, the Recovery Console does not require a password and will automatically log on to the system. **Computer Setting:** Disabled	✓	
❑	***Recovery Console: Allow floppy copy and access to all drives and folders*** **Security Objective:** Enabling this option enables the Recovery Console SET command. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** The Windows Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.)		✓

Completed and Verified	Task	Required	Recommended
❑	***Shutdown: Allow system to be shut down without having to log on*** **Security Objective:** Set a computer to allow shutdown without requiring a user to logon. **Computer Setting:** Disabled	✓	
❑	***Shutdown: Clear virtual memory pagefile*** **Security Objective:** Determines whether the virtual memory pagefile should be cleared when the system is shut down. **Computer Setting:** Enabled	✓	
❑	***System cryptography: Force strong key protection for user keys stored on the computer*** **Security Objective:** This security setting determines whether users can use private keys, such as their S-MIME key, without a password. **Computer Setting:** _____ (**Recommended:** User is prompted when the key is first used)		✓
❑	***System cryptography: Use FIPS-compliant algorithms for encryption, hashing and signing*** **Security Objective:** This security setting determines if the Transport Layer Security/Secure Sockets Layer (TL/SS) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. **Computer Setting:** Enabled	✓	
❑	***System Objects: Default owner for objects created by members of the Administrators group*** **Security Objective:** This security setting determines whether the Administrators group or an object creator is the default owner of any system objects created. **Computer Setting:** Object creator	✓	
❑	***System Objects: Require case insensitivity for non-Windows subsystems*** **Security Objective:** This security setting determines whether case insensitivity is enforced for all subsystems. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Enabled)		✓

Completed and Verified	Task	Required	Recommended
❑	***System Objects: Strengthen default permissions of internal 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	✓	
❑	***System Settings: Optional subsystems*** **Security Objective:** This security setting determines which subsystems support local applications. **Computer Setting:** Remove all entries.	✓	
❑	***System Settings: Use certificate rules on Windows executable program files for software restriction policies*** **Security Objective:** This security setting determines if digital certificates are processed when a user or process attempts to run software with an.exe file name extension. This security setting enables or disables certificate rules (a type of software restriction policies rule). **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
Post-Installation Event Log Settings			
	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 16,384 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 are manually reviewed, archived, and cleared. The default value on stand-alone and member servers is 16,384 kilobytes. The default value on domain controllers is 131,072 kilobytes.)		✓

Completed and Verified	Task	Required	Recommended
❑	***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 16,384 kilobytes is adequate.)		✓
❑	***Prevent local guests group from accessing the Application log*** **Security Objective:** If enabled, anonymous users are prevented from accessing to the application event log. This policy option is not available in stand-alone Windows Server 2003. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Prevent local guests group from accessing the Security log*** **Security Objective:** If enabled, anonymous users are prevented from accessing the security event log. This policy option is not available in stand-alone Windows Server 2003. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***Prevent local guests group from accessing the System log*** **Security Objective:** If enabled, anonymous users are prevented from accessing the system event log. This policy option is not available in stand-alone Windows Server 2003. **Computer Setting:** ❑ Enabled ❑ Disabled ❑ Not defined (**Recommended:** Do not change the default setting.)		✓
❑	***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 setting.)		✓
❑	***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 setting.)		✓

Completed and Verified	Task	Required	Recommended
❑	***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 setting.)		✓
❑	***Retention method for Application log*** **Security Objective:** Determines the "wrapping" method for the Application log. **Computer Setting:** _____ (**Recommended:** Do not change the default setting.)		✓
❑	***Retention method for Security log*** **Security Objective:** Determines the "wrapping" method for the Security log. **Computer Setting:** _____ (**Recommended:** Do not change the default setting for domain-level policies. Setting this policy to Do not overwrite events (clear log manually) is recommended at the local policy level for critical systems, but requires that a strict audit management process be in place for reviewing, archiving, and clearing the audit logs on a regular basis. Otherwise retain the default setting.)		✓
❑	***Retention method for System log*** **Security Objective:** Determines the "wrapping" method for the System log. **Computer Setting:** _____ ((**Recommended:** Do not change the default setting.)		✓
Post-installation System Services Settings			

Completed and Verified	Task	Required	Recommended
❑	***Evaluated Services*** **Security Objective: I**t is acceptable to have any of the services listed here enabled and running. All other services must be disabled. ❑ Alerter Service ❑ Application Experience Lookup Service ❑ Application Layer Gateway Service (ALG) ❑ Certificate Services ❑ COM+ Event System ❑ COM+ System Application ❑ Computer Browser ❑ Cryptographic Services ❑ DCOM Server Process Launcher ❑ DHCP Client ❑ DHCP Server ❑ Distributed File System (DFS) ❑ Distributed Transaction Coordinator ❑ DNS Client ❑ DNS Server ❑ Error Reporting Service ❑ Event Log ❑ File Replication Service ❑ Help and Support ❑ HTTP SSL ❑ Human Interface Device Service ❑ IIS Admin Service ❑ IMAPI CD-Burning COM Service ❑ Indexing Service ❑ Internet Authentication Service ❑ Intersite Messaging ❑ IP Version 6 Helper Service ❑ IPSEC Services ❑ Kerberos Key Distribution Center ❑ License Logging ❑ Logical Disk Manager ❑ Logical Disk Manager Administrative ❑ Network Connections ❑ Network Location Awareness (NLA) ❑ NTLM Security Support Provider ❑ Performance Logs and Alerts ❑ Plug and Play ❑ Print Spooler ❑ Protected Storage ❑ Remote Procedure Call (RPC) ❑ Remote Procedure Call (RPC) Locator ❑ Remote Registry Service ❑ Removable Storage ❑ Resultant Set of Policy Provider ❑ Secondary Logon ❑ Security Accounts Manager ❑ Server ❑ Single Instance Storage Groveler ❑ Smart Card ❑ System Event Notification ❑ Task Scheduler ❑ TCP/IP NetBIOS Helper Service ❑ Uninterruptible Power Supply ❑ Virtual Disk Service ❑ Volume Shadow Copy ❑ WebClient ❑ Windows Firewall (ICF) / Internet Connection Sharing (ICS) ❑ Windows Installer ❑ Windows Internet Name Service (WINS) ❑ Windows Management Instrumentation ❑ Windows Management Instrumentation Driver Extensions ❑ Windows Time ❑ WinHTTP Web Proxy Auto-Discovery Service	✓	

Completed and Verified	Task	Required	Recommended
Additional Registry Settings (Values are shown in decimal, unless otherwise noted)			
❑	***Disable DirectDraw Acceleration*** HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers — Format: REG_DWORD — Value: 0 Key: DCI — Value Name: Timeout	✓	
❑	***Disable unnecessary devices*** HKLM\SYSTEM\CurrentControlSet\Services — Format: REG_DWORD — Value: 4 Key: arp1394 — Value Name: Start Key: Atmarpc — Value Name: Start Key: audstub — Value Name: Start Key: cdac15ba — Value Name: Start Key: cdad10ba — Value Name: Star Key: crcdisk — Value Name: Start Key: IRENUM — Value Name: Start Key: mnmdd — Value Name: Start Key: mssmbios — Value Name: Start Key: ndproxy — Value Name: Start Key: nic1394 — Value Name: Start Key: NwlnkFlt — Value Name: Start Key: NwlnkFwd — Value Name: Start Key: Ohci1394 — Value Name: Start Key: parvdm — Value Name: Start Key: PDCOMP — Value Name: Start Key: PDFRAME — Value Name: Start Key: PDRELI — Value Name: Start Key: PDRFRAME — Value Name: Start Key: pptpminiport — Value Name: Start Key: ptilink — Value Name: Start Key: rasacd — Value Name: Start	✓	

Completed and Verified	Task				Required	Recommended
	Key: rasl2tp	Value Name: Start	REG_DWORD	4		
	Key: raspti	Value Name: Start	REG_DWORD	4		
	Key: RDPCDD	Value Name: Start	REG_DWORD	4		
	Key: rdpdr	Value Name: Start	REG_DWORD	4		
	Key: rdpwd	Value Name: Start	REG_DWORD	4		
	Key: sacdrv	Value Name: Start	REG_DWORD	4		
	Key: secdrv	Value Name: Start	REG_DWORD	4		
	Key: tdpipe	Value Name: Start	REG_DWORD	4		
	Key: tdtcp	Value Name: Start	REG_DWORD	4		
	Key: TermDD	Value Name: Start	REG_DWORD	4		
	Key: wanarp	Value Name: Start	REG_DWORD	4		
	Key: wdica	Value Name: Start	REG_DWORD	4		
	Key: wlbs	Value Name: Start	REG_DWORD	4		
❑	***Prevent interference of the session lock from application-generated input*** HKCU\Software\Policies\Microsoft\Windows\ Control Panel — Format: REG_SZ — Value: 1 Key: Desktop Value Name: BlockSendInputResets **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 screen saver is not properly configured this feature will essentially have no effect on the computer's overall security.				✓	
❑	***Generate an audit event when the audit log reaches a percentage full threshold*** HKLM\SYSTEM\CurrentControlSet\Services\ Eventlog — Format: REG_DWORD — Value: 90 Key: Security Value Name: WarningLevel (The value can be edited to conform to local requirements.)				✓	

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Generate administrative alert when the audit log is full
<table>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Services\ Alerter</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: Parameters
Value Name: AlertNames</td><td>REG_MULTI_SZ</td><td>(Enter the name(s) of accounts to receive alerts)</td></tr>
</table>
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.</td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Remove the default IPSec exemptions
<table>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Services</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: IPSEC Value Name: NoDefaultExempt</td><td>REG_DWORD</td><td>1</td></tr>
</table></td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Review access to raw TCP/IP sockets
<table>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Services\ Tcpip</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: Parameters
Value Name: AllowUserRawAccess</td><td>REG_DWORD</td><td>0</td></tr>
</table></td><td>✓</td><td></td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Disable remote assistance feature of Help and Support service
<table>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Control</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: Terminal Server
Value Name: fEnableSalem</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>Key: Terminal Server
Value Name: fAllowToGetHelp</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>Key: Terminal Server
Value Name: fAllowUnsolicited</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>Key: Terminal Server
Value Name: fAllowUnsolicitedFullControl</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>Key: Terminal Server
Value Name: RAUnsolicited</td><td>REG_DWORD</td><td>0</td></tr>
</table></td><td>✓</td><td></td></tr>
<tr><td>❑</td><td>Make screen saver password protection immediate
<table>
<tr><td>HKLM\Software\Microsoft\Windows NT\CurrentVersion</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: Winlogon
Value Name: ScreenSaverGracePeriod</td><td>REG_SZ</td><td>0</td></tr>
</table></td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Review time service authentication
<table>
<tr><td>HKLM\SYSTEM\CurrentControlSet\Services\ W32Time</td><td>Format</td><td>Value</td></tr>
<tr><td>Key: Parameters
Value Name: Type</td><td>REG_SZ</td><td>Nt5DS</td></tr>
</table></td><td></td><td>✓</td></tr>
</table>

<table>
<tr><th>Completed and Verified</th><th>Task</th><th>Required</th><th>Recommended</th></tr>
<tr><td>❑</td><td>Disable autorun
<table><tr><td>HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies</td><td>Format</td><td>Value</td></tr><tr><td>Key: Explorer

Value Name: NoDriveTypeAutoRun</td><td>REG_DWORD</td><td>255</td></tr></table></td><td></td><td>✓</td></tr>
<tr><td colspan="4">User and Group Accounts</td></tr>
<tr><td>❑</td><td>The management of user and group accounts varies by organization. Follow the requirements and recommendations provided in Tables 5.19 and 5.20 for modification and management of user and group accounts.</td><td></td><td></td></tr>
<tr><td colspan="4">Additional Recommendations</td></tr>
<tr><td>❑</td><td>Back up the Administrator’s encryption certificate

If applicable, back up the Administrator’s encryption certificate and store in a secured location.</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Enable automatic screen lock protection

Set a password-protected screen saver. A recommended timeout period is 15 minutes.</td><td></td><td>✓</td></tr>
<tr><td>❑</td><td>Update the Automated System Recovery (ASR) data

Update the system’s ASR data to reflect the changes made.</td><td></td><td>✓</td></tr>
</table>

Appendix F Windows Server 2003 Security Configuration Templates for the Evaluated Configuration

This Appendix contains the following Security Configuration Templates for the Evaluated Configuration or Windows Server 2003.

- Baseline Windows Server 2003 SP2 Security Configuration Template
- Baseline Windows Server 2003 SP2 Domain Security Policy Template
- Baseline Windows Server 2003 SP2 Domain Controller Security Policy Template
- High Security Windows Server 2003 SP2 Security Configuration Template
- High Security Windows Server 2003 SP2 Domain Security Policy Template
- High Security Windows Server 2003 SP2 Domain Controller Security Policy Template

For details on using these security configuration templates, see Chapter 8, Windows Server 2003 SP2 Common Criteria Security Configuration Templates.

Baseline Windows Server 2003 Security Configuration Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_Baseline_WS2K3_V3.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
;
; Revision History
; 1.0 - Original 12 May 2007




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

[Unicode]
Unicode=yes

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

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

;-------------------------------------------------------------------------
;Network security - Force logoff when logon hours expire.
;-------------------------------------------------------------------------
ForceLogoffWhenHourExpire = 1

;-------------------------------------------------------------------------
;Network access: Allow anonymous SID/Name translation (Disabled)
;-------------------------------------------------------------------------
LSAAnonymousNameLookup = 0
;-------------------------------------------------------------------------
;Accounts: Guest account status (Disabled)
;-------------------------------------------------------------------------
EnableGuestAccount = 0

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

;-------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-------------------------------------------------------------------------
[Privilege Rights]
seassignprimarytokenprivilege = *S-1-5-20,*S-1-5-19
seauditprivilege = *S-1-5-20,*S-1-5-19
sebackupprivilege = *S-1-5-32-551,*S-1-5-32-544
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
sedebugprivilege =
```

```
seenabledelegationprivilege =
seincreasequotaprivilege = *S-1-5-20,*S-1-5-19,*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
semachineaccountprivilege =
semanagevolumeprivilege = *S-1-5-32-544
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
seremoteinteractivelogonright =
serestoreprivilege = *S-1-5-32-551,*S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-547,*S-1-5-19,*S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
SeLoadDriverPrivilege = *S-1-5-32-544
SeImpersonatePrivilege = *S-1-5-6,*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\CurrentVersion\Policies\System\ShutdownWithoutLogon
=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional=7,
```

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,

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

;----------

;NOTICE: The warning banner 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=7,This is a message 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,"WARNING! This message is a temporary policy placeholder!"

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

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=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\RestrictAnonymousSAM=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0

```
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=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 acceleration.  Also direct frame-buffer access is not permitted
;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\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
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\RDPCDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpdr\Start=4,4
MACHINE\System\CurrentControlSet\Services\TermDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\Atmarpc\Start=4,4
MACHINE\System\CurrentControlSet\Services\IRENUM\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFwd\Start=4,4
```

MACHINE\System\CurrentControlSet\Services\NwlnkFlt\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\crcdisk\Start=4,4
MACHINE\System\CurrentControlSet\Services\wlbs\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDCOMP\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRELI\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\arp1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\nic1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ohci1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\secdrv\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdac15ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdad10ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdtcp\Start=4,4
MACHINE\System\CurrentControlSet\Services\wdica\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdpipe\Start=4,4
MACHINE\System\CurrentControlSet\Services\mssmbios\Start=4,4
MACHINE\System\CurrentControlSet\Services\sacdrv\Start=4,4

;----------
;Ensure that non-Adminstrative users do not have access to raw sockets. Default
;is no value present or 0.
;----------
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\AllowUserRawAccess=4,0

;----------
;Disable Remote Assistance feature of the Help and Support service.
;----------
MACHINE\System\CurrentControlSet\Control\Terminal Server\fEnableSalem=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowToGetHelp=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicited=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicitedFullControl=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\RAUnsolicited=4,0

;----------
;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 adequate 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

;----------
;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,Administrator

;----------
;Remove default IPSec exemptions.
;----------

MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt=4,1

;----------
;Disable remote management over RPC capability for DNS Servers.
;----------

MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4

;----------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;----------

[Service General Setting]

"TrkWks",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ClipSrv",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"NetDDEdsdm",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"SMTPSVC",4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TrkSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"Fax",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)"

"mnmsrvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"NetDDE",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWLORC;;;PU)"

"RasAuto",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(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)"

"TlntSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"TermService",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"UtilMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"xmlprov",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WmdmPmSN",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"RDSessMgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ShellHWDetection",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"sacsvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"Tssdis",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"uploadmgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AudioSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"stisvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"UMWdf",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WZCSVC",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AppMgmt",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWRC;;;PU)(A;;CCLCSWLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TapiSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLO;;;BU)"

"RasMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"

"RemoteAccess",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---

;Set audit at the %SystemRoot%\Tasks folder. This ensures that the creation and

;modification of Scheduled Tasks objects is audited when object audit is enabled

;in the Security Policy.

;---

[File Security]

"%SystemRoot%\Tasks",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)S:AR(AU;OICISAFA;DCLCDTSDWDWO;;;S-1-5-7)(AU;OICISAFA;DCLCDTSDWDWO;;;WD)"

[Profile Description]

Description=Evaluated Configuration minimum required security policy settings for Windows Server 2003.

Baseline Windows Server 2003 Domain Security Policy Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_Baseline_WS2K3_V3_Domain.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
; Revision History
; 1.0 - Original 12 May 2007



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

[Unicode]
Unicode=yes

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

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

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

;---------------------------------------------------------------------------
;Network security - Force logoff when logon hours expire.
;---------------------------------------------------------------------------
ForceLogoffWhenHourExpire = 1

;---------------------------------------------------------------------------
;Network access: Allow anonymous SID/Name translation (Disabled)
;---------------------------------------------------------------------------
LSAAnonymousNameLookup = 0

;---------------------------------------------------------------------------
;Accounts: Guest account status (Disabled)
;---------------------------------------------------------------------------
EnableGuestAccount = 0

;---------------------------------------------------------------------------
;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.
;---------------------------------------------------------------------------
[Privilege Rights]
```

```
seauditprivilege = *S-1-5-20,*S-1-5-19
sebackupprivilege = *S-1-5-32-551,*S-1-5-32-544
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
sedebugprivilege =
seenabledelegationprivilege =
seincreasequotaprivilege = *S-1-5-20,*S-1-5-19,*S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
semachineaccountprivilege =
semanagevolumeprivilege = *S-1-5-32-544
senetworklogonright = *S-1-5-32-545,*S-1-5-32-551,*S-1-5-11,*S-1-5-32-544,*S-1-5-32-547
seremoteinteractivelogonright =
serestoreprivilege = *S-1-5-32-551,*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
setcbprivilege =

;---------------------------------------------------------------------------
;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

;---

;NOTICE: The warning banner 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=7,This is a message 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," WARNING! This message is a temporary policy placeholder!"

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

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=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\RestrictAnonymousSAM=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS

MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional=7,

MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1

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

;==========

;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 acceleration. Also direct frame-buffer access is not permitted

;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\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

MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4

MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4

MACHINE\System\CurrentControlSet\Services\RDPCDD\Start=4,4

MACHINE\System\CurrentControlSet\Services\rdpdr\Start=4,4

MACHINE\System\CurrentControlSet\Services\TermDD\Start=4,4

```
MACHINE\System\CurrentControlSet\Services\Atmarpc\Start=4,4
MACHINE\System\CurrentControlSet\Services\IRENUM\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFlt\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\crcdisk\Start=4,4
MACHINE\System\CurrentControlSet\Services\wlbs\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDCOMP\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRELI\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\arp1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\nic1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ohci1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\secdrv\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdac15ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdad10ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdtcp\Start=4,4
MACHINE\System\CurrentControlSet\Services\wdica\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdpipe\Start=4,4
MACHINE\System\CurrentControlSet\Services\mssmbios\Start=4,4
MACHINE\System\CurrentControlSet\Services\sacdrv\Start=4,4

;-------------------------------------------------------------------------
;Ensure that non-Adminstrative users do not have access to raw sockets.  Default
;is no value present or 0.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\AllowUserRawAccess=4,0

;-------------------------------------------------------------------------
;Disable Remote Assistance feature of the Help and Support service.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Terminal Server\fEnableSalem=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowToGetHelp=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicited=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicitedFullControl=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\RAUnsolicited=4,0
```

```
;-----------------------------------------------------------------------------
;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 adequate 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

;-----------------------------------------------------------------------------
;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,Administrator

;-----------------------------------------------------------------------------
;Remove default IPSec exemptions.
;-----------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt=4,1

;-----------------------------------------------------------------------------
;Disable remote management over RPC capability for DNS Servers.
;-----------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4



;-----------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-----------------------------------------------------------------------------

[Service General Setting]
"TrkWks",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

"ClipSrv",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"NetDDEdsdm",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"SMTPSVC",4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TrkSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"Fax",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)"

"mnmsrvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"NetDDE",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWLORC;;;PU)"

"RasAuto",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(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)"

"TlntSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"TermService",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"UtilMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"xmlprov",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WmdmPmSN",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"RDSessMgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ShellHWDetection",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"sacsvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"Tssdis",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"uploadmgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AudioSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"stisvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"UMWdf",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WZCSVC",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AppMgmt",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWRC;;;PU)(A;;CCLCSWLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TapiSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLO;;;BU)"

"RasMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"

"RemoteAccess",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---

;Set audit at the %SystemRoot%\Tasks folder. This ensures that the creation and

;modification of Scheduled Tasks objects is audited when object audit is enabled

;in the Security Policy.

;---

[File Security]

"%SystemRoot%\Tasks",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)S:AR(AU;OICISAFA;DCLCDTSDWDWO;;;S-1-5-7)(AU;OICISAFA;DCLCDTSDWDWO;;;WD)"

[Profile Description]

Description=Evaluated Configuration minimum required security policy settings for Windows Server 2003 Domains.

Baseline Windows Server 2003 Domain Controller Security Policy Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_Baseline_WS2K3_V3_DC.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
; Revision History
; 1.0 - Original 12 May 2007


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

[Unicode]
Unicode=yes

;---------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;---------------------------------------------------------------------------
[Privilege Rights]
seauditprivilege = *S-1-5-19,*S-1-5-20
sebackupprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
```

```
sedebugprivilege =
seenabledelegationprivilege = *S-1-5-32-544
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-20
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
seloaddriverprivilege = *S-1-5-32-544,*S-1-5-32-550
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-544,*S-1-5-11,*S-1-5-9
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteinteractivelogonright =
seremoteshutdownprivilege = *S-1-5-32-544,*S-1-5-32-549
serestoreprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549
sesecurityprivilege = *S-1-5-32-544
seservicelogonright = *S-1-5-20
seshutdownprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-550,*S-1-5-32-549
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-32-549
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege = *S-1-5-32-544
SeCreatePermanentPrivilege =
SeAssignPrimaryTokenPrivilege = *S-1-5-19,*S-1-5-20

;---------------------------------------------------------------------------
;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]

;---

;Keep LSARPC Null Session Pipe on Domain Controllers

;---

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS,LSARPC

;---

;Disable remote management over RPC capability for DNS Servers.

;---

MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4

[Profile Description]

Description=Evaluated Configuration required security policy (delta) settings for Windows Server 2003 Domain Controllers.

High Security Windows Server 2003 Security Configuration Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_HiSec_WS2K3_V3.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
; Revision History
; 1.0 - Original 12 May 2007


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

[Unicode]
Unicode=yes


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
```

```
PasswordHistorySize = 24
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;Network Access: Allow anonymous SID/Name translation (Disabled)
;-------------------------------------------------------------------------------
LSAAnonymousNameLookup = 0

;-------------------------------------------------------------------------------
;Accounts: Administrator account status (Enabled)
;-------------------------------------------------------------------------------
EnableAdminAccount = 1

;-------------------------------------------------------------------------------
;Accounts: Guest account status (Disabled)
;-------------------------------------------------------------------------------
EnableGuestAccount = 0

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

;-------------------------------------------------------------------------------
;Network security - Force logoff when logon hours expire.
;-------------------------------------------------------------------------------
ForceLogoffWhenHourExpire = 1

;-------------------------------------------------------------------------------
;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"


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

;-------------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-------------------------------------------------------------------------------
[Privilege Rights]
seassignprimarytokenprivilege = *S-1-5-20,*S-1-5-19
seauditprivilege = *S-1-5-20,*S-1-5-19
sebackupprivilege = *S-1-5-32-551,*S-1-5-32-544
sebatchlogonright = *S-1-5-19
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
sedebugprivilege =
seenabledelegationprivilege =
seincreasequotaprivilege = *S-1-5-20,*S-1-5-19,*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
semachineaccountprivilege =
semanagevolumeprivilege = *S-1-5-32-544
```

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

seremoteinteractivelogonright =

serestoreprivilege = *S-1-5-32-551,*S-1-5-32-544

sesecurityprivilege = *S-1-5-32-544

sesystemenvironmentprivilege = *S-1-5-32-544

sesystemprofileprivilege = *S-1-5-32-544

sesystemtimeprivilege = *S-1-5-32-547,*S-1-5-19,*S-1-5-32-544

setakeownershipprivilege = *S-1-5-32-544

setcbprivilege =

seloaddriverprivilege = *S-1-5-32-544

SeImpersonatePrivilege = *S-1-5-6,*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\CurrentVersion\Policies\System\DontDisplayLockedUserId=4,3

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

MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine=7,

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine=7,

MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional=7,

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,

MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1

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

MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=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\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,0

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,0

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0

MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,2

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=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1

MACHINE\Software\Microsoft\Driver Signing\Policy=3,1

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

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1

;---

;NOTICE: The warning banner 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,"WARNING! This message is a temporary policy placeholder!"

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This is a message 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\UndockWithoutLogon=4,0

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"

;---

;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 acceleration.  Also direct frame-buffer access is not permitted
;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\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
```

MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\RDPCDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpdr\Start=4,4
MACHINE\System\CurrentControlSet\Services\TermDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\Atmarpc\Start=4,4
MACHINE\System\CurrentControlSet\Services\IRENUM\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFlt\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\crcdisk\Start=4,4
MACHINE\System\CurrentControlSet\Services\wlbs\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDCOMP\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRELI\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\arp1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\nic1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ohci1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\secdrv\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdac15ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdad10ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdtcp\Start=4,4
MACHINE\System\CurrentControlSet\Services\wdica\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdpipe\Start=4,4
MACHINE\System\CurrentControlSet\Services\mssmbios\Start=4,4
MACHINE\System\CurrentControlSet\Services\sacdrv\Start=4,4

;---
;Ensure that non-Adminstrative users do not have access to raw sockets. Default
;is no value present or 0.
;---
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\AllowUserRawAccess=4,0

;---
;Disable Remote Assistance feature of the Help and Support service.
;---

MACHINE\System\CurrentControlSet\Control\Terminal Server\fEnableSalem=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowToGetHelp=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicited=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicitedFullControl=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\RAUnsolicited=4,0

;---
;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 adequate 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

;---
;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,Administrator

;---
;Remove default IPSec exemptions.
;---
MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt=4,1

;---
;Disable remote management over RPC capability for DNS Servers.
;---
MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4

;===
=======
;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.
;=========================================================================
=======



;-------------------------------------------------------------------------
;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



;-------------------------------------------------------------------------
;Make sure Windows Server 2003 is using an authenticated time service.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type=1,Nt5DS

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

;-------------------------------------------------------------------------
;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 = 16384
```

RestrictGuestAccess = 1

[Application Log]

RestrictGuestAccess = 1

;---

;system Services - Disable Services not Included in Common Criteria Evaluated

;Configuration.

;---

[Service General Setting]

"TrkWks",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ClipSrv",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"NetDDEdsdm",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"SMTPSVC",4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TrkSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"Fax",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)"

"mnmsrvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"NetDDE",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWLORC;;;PU)"

"RasAuto",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(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)"

"TlntSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"TermService",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"UtilMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"xmlprov",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WmdmPmSN",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"RDSessMgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ShellHWDetection",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"sacsvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"Tssdis",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"uploadmgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AudioSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"stisvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"UMWdf",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WZCSVC",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AppMgmt",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWRC;;;PU)(A;;CCLCSWLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TapiSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLO;;;BU)"

"RasMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"

"RemoteAccess",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---

;Set audit at the %SystemRoot%\Tasks folder. This ensures that the creation and

;modification of Scheduled Tasks objects is audited when object audit is enabled

;in the Security Policy.

;---

[File Security]

"%SystemRoot%\Tasks",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)S:AR(AU;OICISAFA;DCLCDTSDWDWO;;;S-1-5-7)(AU;OICISAFA;DCLCDTSDWDWO;;;WD)"

[Profile Description]

Description=Evaluated Configuration high security policy settings for Windows Server 2003.

High Security Windows Server 2003 Domain Security Policy Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_HiSec_WS2K3_V3_Domain.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
; Revision History
; 1.0 - Original 12 May 2007



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

[Unicode]
Unicode=yes


[System Access]
;---------------------------------------------------------------------------
;Account Policies - Password Policy.
;---------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
```

```
PasswordComplexity = 1
PasswordHistorySize = 24
ClearTextPassword = 0

;---------------------------------------------------------------------------
;Network Access: Allow anonymous SID/Name translation (Disabled)
;---------------------------------------------------------------------------
LSAAnonymousNameLookup = 0

;---------------------------------------------------------------------------
;Accounts: Administrator account status (Enabled)
;---------------------------------------------------------------------------
EnableAdminAccount = 1

;---------------------------------------------------------------------------
;Accounts: Guest account status (Disabled)
;---------------------------------------------------------------------------
EnableGuestAccount = 0

;---------------------------------------------------------------------------
;Network security - Force logoff when logon hours expire.
;---------------------------------------------------------------------------
ForceLogoffWhenHourExpire = 1

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

;---------------------------------------------------------------------------
;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 - Kerberos Policy.
;-------------------------------------------------------------------------------
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1

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

;-------------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-------------------------------------------------------------------------------
[Privilege Rights]
seauditprivilege = *S-1-5-19,*S-1-5-20
sebackupprivilege = *S-1-5-32-544,*S-1-5-32-551
```

```
sebatchlogonright = *S-1-5-19
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
sedebugprivilege =
seenabledelegationprivilege =
seincreasequotaprivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-20
seloaddriverprivilege = *S-1-5-32-544
semachineaccountprivilege =
semanagevolumeprivilege = *S-1-5-32-544
senetworklogonright = *S-1-5-32-547,*S-1-5-32-544,*S-1-5-11,*S-1-5-32-551,*S-1-5-32-545
seremoteinteractivelogonright =
serestoreprivilege = *S-1-5-32-551,*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
setcbprivilege =
seremoteshutdownprivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *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\DisableDomainCreds=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
```

MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248

MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1

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

MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=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\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,0

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,0

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0

MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,2

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=4,1

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1

MACHINE\Software\Microsoft\Driver Signing\Policy=3,1

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

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1

;----------

;NOTICE: The warning banner 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," WARNING! This message is a temporary policy placeholder!"

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,This is a message 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\UndockWithoutLogon=4,0

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"

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS

MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional=7,

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine=7,

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine=7,

MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0

MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1

MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection=4,1

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

;----------

;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 acceleration.  Also direct frame-buffer access is not permitted
;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\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
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\RDPCDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpdr\Start=4,4
MACHINE\System\CurrentControlSet\Services\TermDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\Atmarpc\Start=4,4
MACHINE\System\CurrentControlSet\Services\IRENUM\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFlt\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\crcdisk\Start=4,4
MACHINE\System\CurrentControlSet\Services\wlbs\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDCOMP\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRELI\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\arp1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\nic1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ohci1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\secdrv\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdac15ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdad10ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdtcp\Start=4,4
MACHINE\System\CurrentControlSet\Services\wdica\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdpipe\Start=4,4
MACHINE\System\CurrentControlSet\Services\mssmbios\Start=4,4
MACHINE\System\CurrentControlSet\Services\sacdrv\Start=4,4

;----------

;Ensure that non-Adminstrative users do not have access to raw sockets. Default

```
;is no value present or 0.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\AllowUserRawAccess=4,0

;-------------------------------------------------------------------------
;Disable Remote Assistance feature of the Help and Support service.
;-------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Terminal Server\fEnableSalem=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowToGetHelp=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicited=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicitedFullControl=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\RAUnsolicited=4,0

;-------------------------------------------------------------------------
;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 adequate 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

;-------------------------------------------------------------------------
;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,Administrator

;-------------------------------------------------------------------------
;Remove default IPSec exemptions.
;-------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt=4,1

;-------------------------------------------------------------------------
;Disable remote management over RPC capability for DNS Servers.
;-------------------------------------------------------------------------
```

MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4

;===
=======

;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.

;===
=======

;---

;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

;---

;Make sure Windows Server 2003 is using an authenticated time service.

;---

MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type=1,Nt5DS

;---

;Disable autorun. Disables autorun capabilities on all drives.

;---

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=
4,255

;---

;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 = 16384

RestrictGuestAccess = 1

[Application Log]

RestrictGuestAccess = 1

;---

;system Services - Disable Services not Included in Common Criteria Evaluated

;Configuration.

;---

[Service General Setting]

"TrkWks",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ClipSrv",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"NetDDEdsdm",4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;OICI;CCLCSWRPLO;;;IU)(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"SMTPSVC",4,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TrkSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"Fax",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)"

"mnmsrvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"NetDDE",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWLORC;;;PU)"

"RasAuto",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(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)"

"TlntSvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"TermService",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"UtilMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

"xmlprov",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WmdmPmSN",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"RDSessMgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"ShellHWDetection",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"sacsvr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"Tssdis",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"uploadmgr",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AudioSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"stisvc",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"UMWdf",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"WZCSVC",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"AppMgmt",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCLCSWRPLO;;;IU)(A;;CCLCSWRC;;;PU)(A;;CCLCSWLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

"TapiSrv",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLO;;;BU)"

"RasMan",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"

"RemoteAccess",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;---

;Set audit at the %SystemRoot%\Tasks folder. This ensures that the creation and

;modification of Scheduled Tasks objects is audited when object audit is enabled

;in the Security Policy.

;---

[File Security]

"%SystemRoot%\Tasks",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)S:AR(AU;OICISAFA;DCLCDTSDWDWO;;;S-1-5-7)(AU;OICISAFA;DCLCDTSDWDWO;;;WD)"

[Profile Description]

Description=Evaluated Configuration high security policy settings for Windows Server 2003 Domains.

High Security Windows Server 2003 Domain Controller Security Policy Template

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: CC_HiSec_WS2K3_V3_DC.inf
; Template Version: 1.0
;
;Windows Server 2003 Evaluated Configuration, Version 3.0. This Security
;Configuration Template provides settings to support the Evaluated Configuration
;of Windows Server 2003 under the Common Criteria (CC) for Information Technology
;Security Evaluation.
;
;
; Revision History
; 1.0 - Original 12 May 2007

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

[Unicode]
Unicode=yes

;--------------------------------------------------------------------------------
;Local Policies - Audit Policy.
;--------------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
```

AuditAccountManage = 3

AuditProcessTracking = 3

AuditDSAccess = 3

AuditAccountLogon = 3

;---

;Local Policies - User Rights Assignment.

;---

[Privilege Rights]

seassignprimarytokenprivilege = *S-1-5-20,*S-1-5-19

seauditprivilege = *S-1-5-20,*S-1-5-19

sebackupprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549

sebatchlogonright = *S-1-5-19

sechangenotifyprivilege = *S-1-5-32-544,*S-1-5-11,*S-1-1-0

secreatepagefileprivilege = *S-1-5-32-544

secreatetokenprivilege =

sedebugprivilege =

seenabledelegationprivilege = *S-1-5-32-544

seincreasebaseprivilege = *S-1-5-32-544

seincreasequotaprivilege = *S-1-5-20,*S-1-5-19,*S-1-5-32-544

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

seloaddriverprivilege = *S-1-5-32-544,*S-1-5-32-550

selockmemoryprivilege =

semachineaccountprivilege =

senetworklogonright = *S-1-5-9,*S-1-5-11,*S-1-5-32-544

seprofilesingleprocessprivilege = *S-1-5-32-544

seremoteinteractivelogonright =

serestoreprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549

sesecurityprivilege = *S-1-5-32-544

seservicelogonright = *S-1-5-20

seshutdownprivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-550,*S-1-5-32-549

sesyncagentprivilege =

sesystemenvironmentprivilege = *S-1-5-32-544

sesystemprofileprivilege = *S-1-5-32-544

sesystemtimeprivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-32-549

setakeownershipprivilege = *S-1-5-32-544

```
setcbprivilege =
seundockprivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-544,*S-1-5-32-549
SeCreatePermanentPrivilege =

;---------------------------------------------------------------------------
;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 = 16384
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1



;---------------------------------------------------------------------------
;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]

;---

;LDAP BIND command request settings

;---

MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,2

;---

;Keep LSARPC Null Session Pipe on Domain Controllers

;---

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS,LSARPC

;---

;Disable remote management over RPC capability for DNS Servers.

;---

MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\RpcProtocol=4,4

[Profile Description]

Description=Evaluated Configuration high security policy (delta) settings for Windows Server 2003 Domain Controllers.

Appendix G Device Drivers

This Appendix includes provides a list of drivers that are allowed in the Evaluated Configuration of Windows Server 2003 and Windows XP Professional.

acpi.sys
adp94xx.sys
adpu160m.sys
afd.sys
agp440.sys
amdk8.sys
atapi.sys
ati2mpad.sys
ati2mtag.sys
b57xp32.sys
b57xp64.sys
beep.sys
bridge.sys
cdfs.sys
cdrom.sys
classpnp.sys
cmdide.sys
cpqcissm.sys
dfs.sys
disk.sys
dmboot.sys
dmio.sys
dmload.sys
e1000645.sys
e1000325.sys
e100b325.sys
e100b645.sys
e1g5132e.sys
fastfat.sys
fdc.sys
fips.sys
flpydisk.sys
fltmgr.sys
fs_rec.sys
ftdisk.sys
hidclass.sys
hidparse.sys
hidusb.sys
http.sys
i2omgmt.sys
i2omp.sys
i8042prt.sys
imapi.sys
intelide.sys
intelppm.sys
ip6fw.sys
ipfltdrv.sys
ipinip.sys
ipnat.sys
ipsec.sys
isapnp.sys
kbdclass.sys
kbdhid.sys
ksecdd.sys
loop.sys
mouclass.sys
mouhid.sys
mountmgr.sys
mraid35x.sys
mrxdav.sys
mrxsmb.sys
msfs.sys
msgpc.sys
mup.sys
ndis.sys
ndisuio.sys
netbt.sys
nfrd960.sys
npfs.sys
ntfs.sys
null.sys
p3.sys
parport.sys
partmgr.sys
pci.sys
pciide.sys
pciidex.sys
portcls.sys
processr.sys
psched.sys
rdbss.sys
redbook.sys
rndismp.sys
scsiport.sys
serenum.sys
serial.sys
sfloppy.sys
smb.sys
smclib.sys
sr.sys
srv.sys
storport.sys
swenum.sys
sym_u3.sys
symmpi.sys
tape.sys
tcpip.sys
tcpip6.sys
tdi.sys
udfs.sys
update.sys
usb8023.sys
usbccgp.sys
usbccid.sys
usbd.sys
usbehci.sys
usbhub.sys
usbohci.sys
usbport.sys
usbstor.sys
usbuhci.sys

vga.sys
vgapnp.sys
videoprt.sys
volsnap.sys
watchdog.sys
win32k.sys
wmiacpi.sys
wmilib.sys
ws2ifsl.sys