Microsoft®

Microsoft Solutions for Security

Windows Server 2003 Security Guide

Microsoft®

Solutions for Security

Acknowledgements

The Microsoft Solutions for Security group (MSS) would like to acknowledge and thank the team that produced the *Windows Server 2003 Security Guide*. The following people were either directly responsible, or made a substantial contribution to the writing, development, and testing of this solution.

Authors
Kurt Dillard

José Maldonado

Brad Warrender

Content Contributors
William Dixon

Eric Fitzgerald

Stirling Goetz

Ian Hellen

Jesper Johansson

Kirk Soluk

Testers
Gaurav Singh Bora

Kenon Bliss

Paresh Gujar

Vince Humphreys

Ashish Java

Editors
Reid Bannecker

Wendy Cleary

John Cobb

Kelly McMahon

Jon Tobey

Program Manager
Chase Carpenter

Reviewers
Rich Benack

Rob Cooper

Duane Crider

Mike Greer

Robert Hensing

Chad Hilton

Andrew Mason

Joe Porter

Joel Scambray

Ben Smith

Jeff Williams

Contributors
Ignacio Avellaneda

Ganesh Balakrishnan

Shelly Bird

Derick Campbell

Sean Finnegan

Joanne Kennedy

Jeff Newfeld

Rob Oikawa

Vishnu Patankar

Keith Proctor

Bill Reid

Sandeep Sinha

Bomani Siwatu

Graham Whiteley

At the request of Microsoft, The Center for Internet Security (CIS) and the United States Department of Commerce National Institute of Standards and Technology (NIST) participated in the final review of these Microsoft documents and provided comments, which were incorporated into the published versions.

Microsoft would also like to thank the Siemens Workplace Architecture Team as well as National Broadband LLC for their invaluable input and participation in the Early Adopter Program for this guide.

Table of Contents

1

Introduction to the Windows Server 2003 Security Guide

Overview

Welcome to the *Microsoft Windows Server 2003 Security Guide*. This guide is designed to provide you with the best information available to assess and counter security risks specific to Microsoft® Windows Server™ 2003 in your environment. The chapters in this guide provide detailed guidance on enhancing security setting configurations and features wherever possible in Windows Server 2003 to address threats identified in your environment. If you are a consultant, designer, or systems engineer involved in a Windows Server 2003 environment, this guide has been designed with you in mind.

The guidance has been reviewed and approved by Microsoft engineering teams, consultants, support engineers, as well as customers and partners to make it:

- Proven—Based on field experience
- Authoritative—Offers the best advice available
- Accurate—Technically validated and tested
- Actionable—Provides the steps to success
- Relevant—Addresses real-world security concerns

Working with consultants and systems engineers who have implemented Windows Server 2003, Windows® XP, and Windows® 2000 in a variety of environments has helped establish the latest best practices to secure these servers and clients. This information is provided in detail in this guide.

The companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, provides a comprehensive look at all of the major security settings present in Windows Server 2003 and Windows XP. Chapters 2 through 11 of this guide include step-by-step security prescriptions, procedures, and recommendations to provide you with task lists to transform the security state of computers running Windows Server 2003 in your organization to a higher level of security. If you want more in-depth discussion of the concepts behind this material, refer to resources such as the *Microsoft Windows 2003 Server Resource Kit*, the *Microsoft Windows XP Resource Kit*, the *Microsoft Windows 2000 Security Resource Kit*, and Microsoft TechNet.

Executive Summary

Whatever your environment, you are strongly advised to take security seriously. Many organizations make the mistake of underestimating the value of their information technology (IT) environment, generally because they exclude substantial indirect costs. If an attack on the servers in your environment is severe enough, it could greatly damage the entire organization. For example, an attack in which your corporate Web site is brought down that causes a major loss of revenue or customer confidence might lead to the collapse of your corporation's profitability. When evaluating security costs, you should include the indirect costs associated with any attack, as well as the costs of lost IT functionality.

Vulnerability, risk, and exposure analysis with regard to security informs you of the tradeoffs between security and usability that all computer systems are subject to in a networked environment. This guide documents the major security countermeasures available in Windows Server 2003 and Windows XP, the vulnerabilities that they address, and the potential negative consequences of implementing each.

The guide then provides specific recommendations for hardening these systems in three common enterprise environments: one in which older operating systems such as Windows 98 must be supported; one consisting of only Windows 2000 and later operating systems; and one in which concern about security is so high that significant loss of functionality and manageability is considered an acceptable tradeoff to achieve the highest level of security. These environments are referred to respectively as the Legacy Client, Enterprise Client, and High Security throughout this guide. Every effort has been made to make this information well organized and easily accessible so that you can quickly find and determine which settings are suitable for the computers in your organization. Although this guide is targeted at the enterprise customer, much of it is appropriate for organizations of any size.

To get the most value out of the material, you will need to read the entire guide. You can also refer to the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159. The team that produced this guide hopes that you will find the material covered in it useful, informative, and interesting.

Who Should Read This Guide

This guide is primarily intended for consultants, security specialists, systems architects, and IT professionals who are responsible for the planning stages of application or infrastructure development, and the deployment of Windows Server 2003. These roles include the following common job descriptions:

- Architects and planners responsible for driving the architecture efforts for the clients in their organizations.
- IT security specialists focused purely on providing security across the platforms within their organizations.
- Business analysts and business decision–makers (BDMs) with critical business objectives and requirements that depend on client support.
- Consultants from both Microsoft Services and partners who need detailed resources of relevant and useful information for enterprise customers and partners.

Get Secure Stay Secure

In October 2001, Microsoft launched an initiative known as the Strategic Technology Protection Program (STPP). The aim of this program is to integrate Microsoft products, services, and support that focus on security. Microsoft views the process of maintaining a secure environment as two related phases. Get Secure and Stay Secure.

Get Secure

The first phase is called Get Secure. To help your organization achieve an appropriate level of security, the advice in this guide is designed to help you secure your current and future computer systems.

Stay Secure

The second phase is known as Stay Secure. It is one thing to create an environment that is initially secure. However, once your environment is up and running, it is entirely another to keep the environment secure over time, take preventative action against threats, and then respond to them effectively when they do occur.

Scope of this Guide

This guide is focused on how to create and maintain a secure environment for computers running Windows Server 2003 in your organization. The material explains the different stages of how to secure the three environments defined in the guide, and what each prescribed server setting addresses in terms of client dependencies. The three environments considered are labeled Legacy Client, Enterprise Client, and High Security.

- The Legacy Client settings are designed to work in a Microsoft Active Directory® domain with member servers and domain controllers running Windows Server 2003, and clients running Microsoft Windows® 98, Windows NT 4.0 and later.
- The Enterprise Client settings are designed to work in an Active Directory domain with member servers and domain controllers running Windows Server 2003, and clients running Windows 2000, Windows XP, and later.
- The High Security settings are also designed to work in an Active Directory domain with member servers and domain controllers running Windows Server 2003, and clients running Windows 2000, Windows XP, and later. However, the High Security settings are so restrictive that many applications may not function. For this reason, the servers may encounter some impact on performance, and managing the servers will be more challenging.

Hardening guidance is provided for a group of distinct server roles. The countermeasures described and the tools provided assume that each server will have a single role, if you need to combine roles for some of the servers in your environment then you can customize the security templates included with this guide so that the appropriate combination of services and security options are configured for the servers with multiple roles. The roles covered by this guide include:

- Domain controllers
- Infrastructure servers
- File servers
- Print servers
- Internet Information Services (IIS) servers
- Internet Authentication Services (IAS) servers
- Certificate Services servers
- Bastion hosts

The settings recommended in this guide were tested thoroughly in lab environments depicting those described above: Legacy Client, Enterprise Client, and High Security. These settings were proven to work in the lab, but it is important that your organization test these settings in your own lab that accurately represents your production environment. It is likely that you will need to make some changes to the security templates and the manual procedures documented within this guide so that all of your business applications continue to function as expected. The detailed information provided in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available for download at http://go.microsoft.com/fwlink/?LinkId=15159, gives you the information you need to assess each specific countermeasure and to decide which of them are appropriate for your organization's unique environment and business requirements.

Content Overview

The *Windows Server 2003 Security Guide* consists of 12 chapters. Each chapter builds on the end–to–end solution process required to implement and secure Windows Server 2003 in your environment. The first few chapters describe building the foundation for hardening the servers in your organization, while the remaining chapters document the procedures unique to each server role.

Chapter 1: Introduction to the Windows Server 2003 Security Guide

This chapter introduces the *Windows Server 2003 Security Guide*, and includes a brief overview of each chapter.

Chapter 2: Configuring the Domain Infrastructure

This chapter explains how the domain environment will be constructed as a baseline in order to provide guidance to secure a Windows Server 2003 infrastructure. The chapter first focuses on domain–level security settings and countermeasures. High level descriptions of the Microsoft Active Directory service design, the organizational unit (OU) design, and domain policy are included.

The Legacy Client, Enterprise Client, and High Security environments mentioned in Chapter 1 are then explained in terms of securing a domain environment. This provides a vision of the evolution your organization can make toward a more secure environment within a domain infrastructure that is appropriate for each of these environments.

Chapter 3: Creating a Member Server Baseline

This chapter explains security template settings and additional countermeasures for the server roles covered in the three environments defined in the guide. The chapter largely focuses on establishing a Member Server Baseline Policy (MSBP) for the server role hardening recommendations discussed later in the guide.

The recommendations in this chapter are chosen to safely allow corporations to deploy strongly recommended setting configurations for Windows Server 2003 systems which suit both existing and newly–built systems. The default security configurations within Windows Server 20003 have been researched and tested. The recommendations specified in this chapter were determined to provide greater security than the default operating system settings. In some cases to provide support for legacy clients, a less restrictive setting configuration is suggested than that present in the default installation of Windows Server 2003.

Chapter 4: Hardening Domain Controllers

The domain controller server role is one of the most important roles to secure in any Active Directory environment with computers running Windows Server 2003. Any loss or compromise of a domain controller could prove devastating to clients, servers, and applications that rely on domain controllers for authentication, Group Policy, and a central lightweight directory access protocol (LDAP) directory.

This chapter outlines the need to always store domain controllers in physically secure locations that are accessible only to qualified administrative staff. The hazards of storing domain controllers in unsecured locations, branch offices for example, are addressed and a significant portion of the chapter is devoted to explaining the security considerations behind the recommended Domain Controller Group Policy.

Chapter 5: Hardening Infrastructure Servers

In this chapter, the Infrastructure server role is defined as either a Dynamic Host Control Protocol (DHCP) server or a Windows Internet Name Service (WINS) server. Details are provided on the areas in which the infrastructure servers in your environment can benefit from security settings that are not applied by the Member Server Baseline Policy (MSBP).

Chapter 6: Hardening File Servers

This chapter focuses on the File server role and the difficulties related to hardening servers designated for it. The most essential services for these servers require the Windows network basic input/output system (NetBIOS)–related protocols. The Server Message Block (SMB) and Common Internet File System (CIFS) protocols are also used to provide rich information to unauthenticated users, and yet these are often recommended to be disabled in high–security Windows® environments. This chapter details any areas in which File servers can benefit from security settings not applied by the MSBP.

Chapter 7: Hardening Print Servers

Print servers are the focus of this chapter. Again, the most essential services for these servers require use of Windows NetBIOS–related protocols. The protocols for SMB and CIFS can also provide rich information to unauthenticated users for this server role, but these are also often recommended to be disabled in high–security Windows environments. This chapter details the areas in which Print server security settings can be strengthened in ways that are not applied by the MSBP.

Chapter 8: Hardening IIS Servers

This chapter outlines how comprehensive security for Web sites and applications depends on an entire IIS server (including each Web site and application running on the IIS server) to be protected from client computers in your environment. Web sites and applications also must be protected from other Web sites and applications running on the same IIS server. Practices to ensure this distinction is achieved between the IIS servers in your environment are described in detail in this chapter.

IIS is not installed on members of the Microsoft Windows Server System™ family by default. When IIS is initially installed, it is installed in a highly secure, "locked" mode. For example, IIS by default serves only static content. Features such as Active Server Pages (ASP), ASP.NET, Server–Side Includes, WebDAV publishing, and Microsoft FrontPage® Server Extensions must now be enabled by the administrator through the Web Service Extensions node in Internet Information Services Manger (IIS Manager).

Sections in this chapter provide the detail on a variety of security hardening settings that should be implemented to enhance the security of IIS servers in your environment. The importance of security monitoring, detection, and response is emphasized to ensure the servers stay secure.

Chapter 9: Hardening IAS Servers

Internet Authentication Servers (IAS) provide RADIUS services, a standards–based authentication protocol designed for verifying identity of clients accessing networks remotely. This chapter details any areas in which IAS Servers can benefit from security settings not applied by the MSBP.

Chapter 10: Hardening Certificate Services Servers

Certificate Services provide the cryptographic and certificate management services needed to build a public key infrastructure (PKI) in your server environment. This chapter details any areas in which Certificate Services servers will benefit from security settings not applied by the MSBP.

Chapter 11: Hardening Bastion Hosts

Bastion hosts servers are accessible to clients from the Internet. In this chapter, it is explained how these systems exposed to the public are susceptible to attack from a much larger number of users who can remain completely anonymous in many cases if they wish. Many organizations do not extend their domain–infrastructure to public portions of this network. For this reason, this chapter content focuses on hardening recommendations for stand–alone computers. Details are provided on any areas in which bastion hosts can benefit from security settings not applied by the MSBP, or the methods used to apply those settings in an Active Directory–based domain environment.

Chapter 12: Conclusion

The concluding chapter of this guide recaps the important points of the material discussed in the previous chapters.

Tools and Templates

A collection of security templates, scripts, and additional tools are included with this guide to make it easier for your organization to evaluate, test, and implement the countermeasures recommended in this guide. The security templates are text files that can be imported into domain–based group policies, or applied locally using the Security Configuration and Analysis snap–in. These procedures are detailed in Chapter 2, "Configuring the Domain Infrastructure." The scripts included with this guide implement IPSec packet filters using the NETSH command line tool and test scripts used in testing the recommended countermeasures. This guide also includes a Microsoft Excel workbook called Windows Server 2003 Security Guide Settings that documents the settings included in each of the security templates. These tools and templates are included in the self-extracting WinZip archive that contains this guide. When you extracted the files from this archive the following folder structure is created in the location you specified:

- \Windows Server 2003 Security Guide—contains the Portable Document Format (PDF) file document that you are currently reading, as well as the Test Guide, Delivery Guide, and Support Guide associated with this material.
- \Windows Server 2003 Security Guide\Tools and Templates—contains subdirectories for any items that may accompany this guide.
- \Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Security Templates—contains all security templates that are discussed in the guide.
- \Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Sample Scripts—contains all sample IPSec filter scripts and an Excel workbook containing all traffic maps discussed in the guide.
- \Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Checklists—contains checklists specific to each server role.
- \Windows Server 2003 Security Guide\Tools and Templates\Test Guide—contains tools related to the test guide.
- \Windows Server 2003 Security Guide\Tools and Templates\Delivery Guide—contains tools related to the delivery guide.

Skills and Readiness

The following knowledge and skills are prerequisite for administrators or architects charged with developing, deploying, and securing installations of Windows Server 2003 and Windows XP in an enterprise:

- MCSE 2000 certification with more than 2 years of security–related experience.
- In–depth knowledge of corporate domain and Active Directory environments.
- Use of management tools, including Microsoft Management Console (MMC), secedit, gpupdate, and gpresult.
- Experience administering Group Policy.
- Experience deploying applications and workstations in enterprise environments.

Requirements

The software requirements for utilizing the tools and templates documented in this guide are:

- Windows Server 2003 Standard Edition; Windows Server 2003 Enterprise Edition; or Windows Server 2003 Datacenter Edition.
- A Windows Server 2003–based Active Directory domain.
- Microsoft Excel 2000 or later.

Style Conventions

This guide uses the following style conventions and terminology.

Table 1.1: Style Conventions

Element	Meaning
Bold font	Characters that are typed exactly as shown, including commands and switches. User interface elements in text that is prescriptive are also bold.
Italic font	Placeholder for variables where specific values are supplied. For example, Filename.ext could refer to any valid file name for the first case in question.
Important	Alerts the reader to supplementary information that is essential to the completion of the task.
`Monospace font`	Code samples.
%SystemRoot%	The folder in which the Windows Server 2003 operating system is installed.
Note	Alerts the reader to supplementary information.
Screen Para	Messages that appear on screen and command line commands are styled in this font.

Summary

This chapter provided an overview of the primary factors involved in securing Windows Server 2003 which are considered in greater depth in the rest of the guide. Now that you have an understanding of how this guide is organized, you can decide whether to read it from beginning to end, or to select only those sections of most interest to you.

However, it is important to remember that effective, successful, security operations require making improvements in all of the areas covered in this guide, not just a few. For this reason, it is highly recommended to read the entire guide to take advantage of all the information that can be used to secure Windows Server 2003 in your organization that the guide has to offer.

More Information

The following information sources were the latest available on topics closely related to securing Windows Server 2003 at the time this guide and product were released to the pubic.

For more information on Security at Microsoft, see: http://www.microsoft.com/security.

For more detail on how MOF can assist in your enterprise, see: http://www.microsoft.com/business/services/mcsmof.asp.

For information on the Microsoft Strategic Technology Protection Program Web site, see: http://microsoft.com/security/mstpp.asp.

For information on the Microsoft Security Notification Service, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp.

2

Configuring the Domain Infrastructure

Overview

This chapter uses the construction of a domain environment to demonstrate how to secure an infrastructure for Microsoft® Windows Server™ 2003.

The chapter first focuses on security settings and countermeasures at the domain level. This includes a high level description of the Microsoft Active Directory® design, the organizational unit (OU) design, Group Policy design, and administrative group design.

This chapter also explains how to secure a Windows Server 2003 domain environment for the Legacy, Enterprise, and High Security environments outlined in Chapter 1, "Introduction to Securing Windows Server 2003." This information lays the groundwork and provides a vision for evolving from a Legacy environment toward a High Security environment within a domain infrastructure.

Windows Server 2003 ships with default setting values set to a secure state. To improve the usability of this material, this chapter only discusses those settings that have been modified from the default values. For information on all default settings, see the companion guide, "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*."

Active Directory Design

Detailed information on designing an Active Directory structure could fill an entire book by itself. Active Directory enables applications to find, use, and manage directory resources in a distributed computing environment. This section briefly discusses these concepts to establish a frame of reference for the rest of the chapter.

When creating an Active Directory architecture you must carefully consider the environment's security boundaries. Adequately planning an organization's security delegation and implementation schedule will result in a much more secure Active Directory design for the organization. Then, only major changes to the environment, such as an acquisition or organizational restructuring will require restructuring.

If your organization already has an Active Directory design, this chapter may provide insight into some of its benefits or potential issues from a security perspective.

Establishing Windows Server 2003 Directory Boundaries

There are several different types of boundaries within Active Directory. These boundaries define the forest, the domain, the site topology, and permission delegation.

These boundaries are automatically established during Active Directory installation, but you must ensure that permission boundaries incorporate organizational requirements and policies. Administrative permissions delegation can be quite flexible depending on an organization's requirements. For instance, to maintain a proper balance between security and administrative functionality, you can break the permission delegation boundaries down further into security boundaries and administrative boundaries.

Security Boundaries

Security boundaries help define the autonomy or isolation of different groups within an organization. It is difficult to balance the tradeoffs between ensuring adequate security—based on how the corporation's business boundaries are established—and the need to continue providing a solid level of base functionality.

To successfully achieve this balance, you must weigh the threats to your organization against the security implications of delegating administration permissions and other choices regarding your environment's network architecture.

Forest vs. Domain Security Boundaries

The forest is the true *security* boundary. This guide recommends creating separate forests to keep your environment secure from rogue administrators as opposed to creating separate domains to provide security and isolation from rogue administrators and other potential threats.

A domain is the *management* boundary of Active Directory. With an organization of well–meaning individuals, the domain boundary will provide autonomous management of services and data within each domain of the organization.

Unfortunately, when discussing security, this is not so simple to achieve. A domain, for example, will not completely isolate an attack from a rogue domain administrator. This level of separation can only be achieved at the forest level.

Because of this, your organization may need to consider dividing the administrative control of services and data within the current Active Directory design. Active Directory design requires fully understanding your organization's requirements for service autonomy and service isolation, as well as for data autonomy and data isolation.

Administrative Boundaries

Because of the potential need to segment services and data, you must define the different administration levels required. In addition to administrators who may perform unique services for your organization, the following types of administrators are recommended.

Service Administrators

Active Directory service administrators are responsible for the configuring and delivering the directory service. For example, service administrators maintain domain controller servers, control directory–wide configuration settings, and are responsible for ensuring service availability. The Active Directory administrators in your organization should be considered your service administrators.

In many cases, the Active Directory service configuration is determined by attribute values. These attribute values correspond to settings for their respective objects stored in the directory. Consequently, service administrators in Active Directory are also data administrators. Depending on your organizational needs, here are some other service administrator groups you may need to include in your Active Directory service design:

- A domain administration group that is primarily responsible for directory services.

  The forest administrator is responsible for choosing the group to administer each domain. Because of the high–level access granted to the administrator for each domain, these administrators should be highly trusted individuals. The group performing domain administration controls the domains through the Domain Admins group and other built–in groups.

- Groups of administrators who are responsible for Domain Name System (DNS) management.

  The DNS administrator group is responsible for completing the DNS design and managing the DNS infrastructure. The DNS administrator manages the DNS infrastructure through the DNS Admins group.

- Groups of administrators that are responsible for OU management.

  The OU administrator designates a group or individual as a manager for each OU. Each OU administrator is responsible for managing the data stored within the assigned Active Directory OU. These groups can control how administration is delegated, and how policy is applied to objects within their OUs. In addition, OU administrators can also create new subtrees and delegate administration of the OUs they are responsible for.

- Groups of administrators that are responsible for infrastructure server management.

  The group responsible for infrastructure server administration is responsible for managing the Microsoft Windows® Internet Name Service (WINS), Dynamic Host Configuration Protocol (DHCP), and potentially the DNS infrastructure. In some cases, the group handling domain management will manage the DNS infrastructure because Active Directory is integrated with DNS and is stored and managed on the domain controllers.

Data Administrators

Active Directory data administrators are responsible for managing data stored in Active Directory or on computers joined to Active Directory. These administrators have no control over the configuration or delivery of the directory service. Data administrators are members of a security group created by your organization. Sometimes the default security groups in Windows do not make sense for all situations in the organization. Therefore, organizations can develop their own security group naming standards and meanings to best fit their environment. Some of the data administrators' daily tasks include:

- Controlling a subset of objects in the directory. Through inheritable attribute–level access control, data administrators can be granted control of very specific sections of the directory, but have no control over the configuration of the service itself.
- Managing member computers in the directory and the data that is on those computers.

Note: In many cases, attribute values for objects stored in the directory determine the directory's service configuration.

To summarize, allowing the owners of Active Directory service and directory structures to join a forest or domain infrastructure requires that the organization must trust all service administrators in the forest and all domains. In addition, enterprise security programs must develop standard policies and procedures which provide proper background screening for the administrators. In the context of this security guide, to trust service administrators means to:

- Reasonably believe that service administrators will look out for the organization's best interests. Organizations should not elect to join a forest or domain if the owners of the forest or domain might have legitimate reasons to act maliciously against the organization.
- Reasonably believe that service administrators will follow best practices and restrict physical access to the domain controllers.
- Understand and accept the risks to the organization that include the possibility for:
    - **Rogue administrators** —Trusted administrators might become rogue administrators, and thus abuse the power they have with the system. If you have a rogue administrator within a forest, it would be easy for that administrator to look up the security identifier (SID) for another administrator from another domain. The rogue administrator could then use an application programming interface (API) tool, disk editor, or debugger to add the stolen SID to the SID History list of an account within his own domain. With the stolen SID added to the user's SID History, along with his own domain the rogue administrator would have administrative privileges in the stolen SID's domain.
    - **Coerced administrators** — A trusted administrator might be coerced or compelled to perform operations that breach the security of the system. A user or administrator may use social engineering techniques on legitimate administrators of a computer system in order to gain the usernames and passwords he needs to gain access to the system.

Some organizations might accept the risk of a security breach by a rogue or a coerced service administrator from another part of the organization. Such organizations might determine that the collaborative and cost–saving benefit of participating in a shared infrastructure outweighs this risk. However, other organizations might not accept the risk because the potential consequences of a security breach are too severe.

OU Structure to Facilitate Group Policy Management and Delegation

While this guide is not about Active Directory design, some design information is necessary to provide insight into the using Group Policy to securely administer your organization's domains, domain controllers, and specific server roles.

While OUs offer an easy way to group users and other security principals, they also provide an effective mechanism to segment administrative boundaries.

In addition, using OUs to provide different Group Policy objects (GPOs) based on server role is an integral piece of the overall security architecture for the organization.

Delegating Administration and Applying Group Policy

An OU is simply a container within a domain. You can delegate control over an OU to a group or individual by setting specific access control lists (ACLs) on each of these containers.

Often, you can use an OU to provide administrative capabilities similar to those in Microsoft Windows NT® 4.0 resource domains. You can also create an OU to contain a group of resource servers to be administered by other users. This gives this group of other users autonomous control over a particular OU, without isolating them from the remainder of the domain.

Administrators that delegate control over specific OUs are likely to be service administrators. At a lower level of authority, users that control the OUs are usually data administrators.

Administrative Groups

Creating administrative groups gives administrators a way to segment clusters of users, security groups, or servers into containers for autonomous administration.

For example, consider the infrastructure servers that reside in a domain. Infrastructure servers include all of the nondomain controllers that are running basic network services, including servers running WINS and DHCP services. All DNS servers are running on domain controllers, which are in the Domain Controllers OU. DNS servers in this example are not considered as Infrastructure servers.

Often, an operations group or an infrastructure administration group maintains these servers. Using an OU can easily provide administrative capabilities to these servers.

▶ **To create an OU for administration**

1. Create an OU called **Member Servers**.
2. Create an OU called **Infrastructure**.
3. Move all WINS and DHCP servers into the **Infrastructure** OU.
4. Create a global security group called **Infrastructure Admins** with the appropriate domain accounts added to it.
5. Run the **Delegation of Control Wizard** to give the Infrastructure Admins group the setting Full Control of the OU.

The following illustration provides a high level view of such an OU.

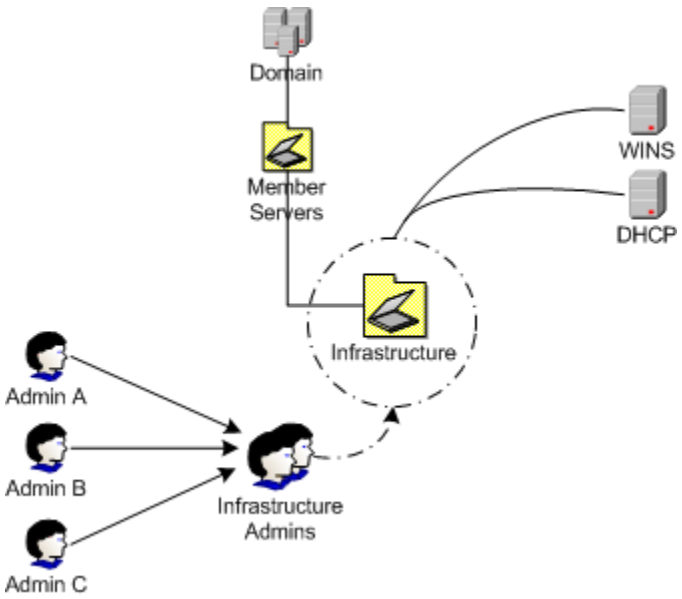

Figure 2.1
OU delegation of administration

This is only one of many ways of using OUs to provide administrative segmentation. For more complex organizations, see the "More Information" section at the end of this chapter.

After following this procedure, the Infrastructure Admin group should have full control over the Infrastructure OU, and all servers and objects within this OU. This prepares them for the next phase, securing the server roles with Group Policy.

Group Policy Application

Use Group Policy and delegate administration to apply specific settings, rights, and behavior to all servers within an OU. By using Group Policy rather than manual steps, it is simple to update a number of servers with any additional changes required in the future.

Group policies are accumulated and applied in the order shown in the illustration below.

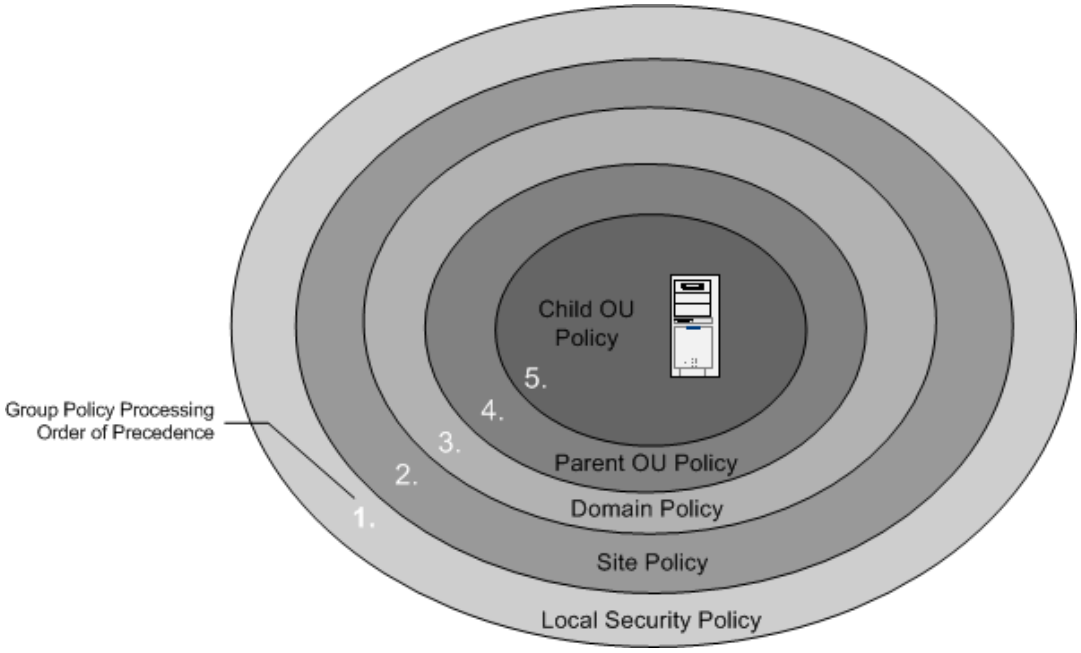

Figure 2.2
GPO application hierarchy

As seen above, policies are applied first from the local machine policy level of the computer. After that, any GPOs are applied at the site level, and then at the domain level. If the server is nested in several OUs, GPOs existing at the highest level OU are applied first. The process of applying GPOs continues down the OU hierarchy. The final GPO to be applied is at the child OU level containing the server object. The order of precedence for processing Group Policy extends from the highest OU (farthest from the user or computer account) to the lowest OU (that actually contains the user or computer account).

Keep the following in mind when applying Group Policy:

- You must set the GPO application order for group policy levels with multiple GPOs. If multiple policies specify the same option, the last one applied will take precedence.
- Configuring a Group Policy with the **No Override** option prevents other GPOs from overriding it.

Security Templates

Security templates are text based files. You can change these files using the Security Templates snap–in to the Microsoft Management Console (MMC) or by using a text editor such as Notepad. Some sections of the template files contain specific ACLs written in the Security Descriptor Definition Language (SDDL). You can find more information on editing security templates and SDDL on Microsoft MSDN®.

Template Management

By default, authenticated users have the right to read all settings contained in a Group Policy object. Therefore, it is very important to store security templates used for a production environment in a secure location that only administrators responsible for implementing Group Policy can access. The purpose is not to prevent the viewing of *.inf files, but rather to prevent unauthorized changes to the source security templates. To accommodate this, all computers running Windows Server 2003 store security templates in the %SystemRoot%\security\templates folder.

However, this folder is not replicated across multiple domain controllers. Therefore, you will need to designate one domain controller to hold the master copy of the security templates so that you do not encounter version control problems with the templates. This will ensure that you always are modifying the same copy of the templates.

Managing Group Policy and Importing Security Templates

The following procedure imports the security templates included with this guide into the OU structure suggested in this chapter. Before implementing the following procedure on a domain controller, the specific policy (.inf) files must be located on a Windows Server 2003 system in the environment.

Warning: The security templates in this guide are designed to increase security in your environment. It is quite possible that by installing the templates included with this guide, some functionality in the environment of your organization may be lost. This could include the failure of mission critical applications.

It is **essential** to thoroughly test these templates before deployed them in a production environment. Back up each domain controller and server in your environment before applying any new security settings. Ensure the system state is included in the backup to enable registry settings or Active Directory objects to be restored.

▶ **To import the Domain Policy security templates**

1. In **Active Directory Users and Computers**, right–click the **Domain**, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new GPO.
3. Type **Enterprise Client - Domain Policy**, and then press **Enter**.
4. Right–click **Enterprise Client - Domain Policy**, and then select **No Override**.
5. Select **Enterprise Client - Domain Policy**, and then click **Edit**.
6. In the Group Policy window, click **Computer Configuration\Windows Settings**. Right–click **Security Settings**, and then select **Import Policy**.
7. In the **Import Policy From** dialog box, navigate to **\Security Guide\Job Aids**, and then double–click **Enterprise Client - Domain.inf**.
8. Close the **Group Policy** that has been modified.
9. Close the **Domain Properties** window.

10. Force replication between the domain controllers so that all have the policy applied to them by doing the following:
    - Open a command prompt and use the **gpupdate.exe** command line tool to force the domain controller to refresh the domain policy with the command: `gpupdate /Force`.
11. Verify in the **Event Log** that the Group Policy downloaded successfully and that the server can communicate with the other domain controllers in the domain.

Warning: When you create the Enterprise Client–Domain Policy, ensure that the **No Override** option is enabled to enforce this policy throughout the domain. This is the only Group Policy in this guide in which the **No Override** option must be enabled. Do not enable this option in any of the other group policies specified in this guide. Also, do not modify the Windows Server 2003 Default Domain Policy, in case you need to return to its default settings.

To ensure that this new policy has precedence over the default policy, position it to have the highest priority among the GPO links.

You can modify the default policy directly to create a new security configuration, however, there is an advantage to creating a new Group Policy because if there are problems with it, the new one can be easily disabled, leaving the Default Domain Policy in place to resume control.

Gpupdate.exe is a command–line tool that when called from a batch file or automatic task scheduler, can be used to automatically apply templates and analyze system security. It can also be run dynamically from a command line.

Important: This policy should be imported into any additional domains in the organization. However, it is not uncommon to find environments where the root domain password policy is much stricter than any of the other domains. Care should also be taken to ensure that any other domains that will use this same policy have the same business requirements. Because the password policy can only be set at the domain level, there may be business or legal requirements that segment some users into a separate domain simply to enforce the use of a stricter password policy on that group.

In the three environments defined in this guide, the same policy for their root and child domains was used, along with the associated security template for each one. For example, Legacy Client–Domain.inf, Enterprise Client–Domain.inf, and High Security–Domain.inf files were used for each respective level. Procedures similar to those above should be used to apply any of the subsequent templates for the baseline policy and the incremental policies.

Successful GPO Application Events

Aside from manually checking all of the settings to ensure that they have been appropriately applied to the servers in your organization, an event should also appear in the Event Log to inform the administrator that the domain policy has downloaded successfully to each of the servers. The following event information should appear in the Application Log with its own unique Event ID number:

> Type: Information
>
> Source ID: SceCli
>
> Event ID: 1704
>
> Description: Security policy in the Group policy objects has been applied successfully.
>
> For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

If this message does not appear within a few minutes after applying the domain policy, rerun the Gpupdate.exe command–line tool to apply the domain policy, and then restart the server to force the domain policy download.

By default, the security settings are refreshed every 90 minutes on a workstation or server and every 5 minutes on a domain controller. You will see this event if any changes have occurred during these intervals. In addition, the settings are also refreshed every 16 hours, regardless of new changes or not.

Time Configuration

You should ensure that system time is accurate and that all servers in your organization are using the same time source. The Windows Server 2003 W32Time service provides time synchronization for Windows Server 2003 and Microsoft Windows XP–based computers running in an Active Directory domain.

The W32Time service synchronizes the client clocks of Windows Server 2003–based computers with the domain controllers in a domain. This is necessary for the Kerberos version 5 authentication protocol to work properly, as well as NTLMv2. To function correctly, a number of Windows Server™ family components rely on accurate and synchronized time. If the clocks are not synchronized on the clients, the Kerberos v5 authentication protocol might falsely interpret logon requests as intrusion attempts and deny access to users.

Another important benefit time synchronization provides is event correlation on all of the clients in your enterprise. Synchronized clocks on the clients in your environment ensures that you can correctly analyze events that take place in uniform sequence on the clients for success or failure across the enterprise.

Kerberos is a network authentication protocol developed by Massachusetts Institute of Technology (MIT). The protocol authenticates the identity of users attempting to log on to a network and encrypts their communications through secret–key cryptography.

The W32Time service synchronizes clocks using the Network Time Protocol (NTP). In a Windows Server 2003 forest, time is synchronized in the following manner:

- The primary domain controller (PDC) emulator operations master in the forest root domain is the authoritative time source for the organization.
- All PDC operation masters in other domains in the forest follow the hierarchy of domains when selecting a PDC emulator to synchronize their time.
- All domain controllers in a domain synchronize their time with the PDC emulator operations master in their domain as their inbound time partner.
- All member servers and client desktop computers use the authenticating domain controller as their inbound time partner.

To ensure that the time is accurate, the PDC emulator in the forest root domain can be synchronized to an external NTP time server. However, doing so may result in a requirement to open ports on the firewall. NTP uses UDP port 123. Before doing this, weigh the benefits against the potential security risk of making these configuration changes.

▶To synchronize an internal time source with an external time source

1. Open a **Command Prompt**.
2. Type the following, where PeerList is a comma–separated list of DNS names or Internet protocol (IP) addresses for the desired time sources:

   w32tm /config /syncfromflags:manual /manualpeerlist:PeerList
3. To update type:

   w32tm /config /update.
4. Check the **Event Log**. If the computer cannot reach the servers, the procedure fails and an entry is written to the **Event Log**.

The most common use of this procedure is to synchronize the internal network's authoritative time source with a very precise external time source. However, this procedure can be run on any computer running Windows XP or a member of the Windows Server 2003 family.

In many cases, it may not be necessary to have all servers times synchronized with an external source, as long as they are synchronized with the same internal source.

If the computers on your network are running Windows 98 or Windows NT 4.0 operating systems, then synchronize the clocks on those machines using the following command in a logon script where <*timecomputer*> is a domain controller on the network:

net time \\<*timecomputer*> /set /yes

Running this command will synchronize the time clocks in these computers with the time clocks in the other computers throughout the domain.

Note: For accurate log analysis, network computers running operating systems other than Windows should also synchronize their clocks to the Windows Server 2003 PDC emulator.

Baseline Sever Role Organizational Units

The previous example for managing an organization's infrastructure servers can be extended to encompass other servers and services in a corporate infrastructure. The goal is to create a seamless Group Policy that covers all servers, while ensuring that the servers residing within Active Directory meet the security standards for your environment.

This type of Group Policy covering all servers in your environment forms a consistent baseline for standard settings across all of the servers in your enterprise. In addition, the OU structure and the application of Group Policies must provide a granular design to provide security settings for specific types of servers in an organization. For example, Internet Information Server (IIS), File, Print, Internet Authentication Server (IAS), and Certificate Services, illustrate a few of the server roles in an organization that may require unique group policies.

Member Server Baseline Policy

The first step in establishing server role OUs is to create a baseline policy. To do this, create a baseline security template and imported it into the Group Policy. The Enterprise Client–Member Server Baseline.inf files are included with this security guide to provide this functionality and guidance. The Enterprise Client is a reference to the different middle level of security based on the organization's compatibility requirements discussed in Chapter 1,"Introduction to the Windows Server 2003 Security Guide."

Link this GPO security template to the Member Servers OU. The Enterprise Client – Member Server Baseline.inf security template will apply the settings of the baseline Group Policy to any servers in the Member Servers OU, as well as any servers in child OUs. For simplicity, the remaining examples in this chapter use the Enterprise Client security level. The Member Server Baseline Policy is discussed in Chapter 3, "Creating a Member Server Baseline."

The baseline Group Policy should define the desired settings for all servers across an organization. Make the baseline Group Policy as restrictive as possible, and segment any servers that need to differ from this policy into separate server–specific OUs.

Server Role Types and Organizational Units

Continuing the example above, create a separate policy for the incremental changes to the infrastructure server policies. Put the necessary setting into a security template called Enterprise Client–Infrastructure Server.inf, to ensure that the infrastructure services function and are accessible over the network.

Link this GPO infrastructure template to the Infrastructure OU. Finally, use the Restricted Groups setting to add the following three groups to the Local Administrators group in the "Enterprise Client: Infrastructure Server Policy": Domain Administrators, Enterprise Administrators, and Infrastructure Administrators.

This process is shown in the illustration below.

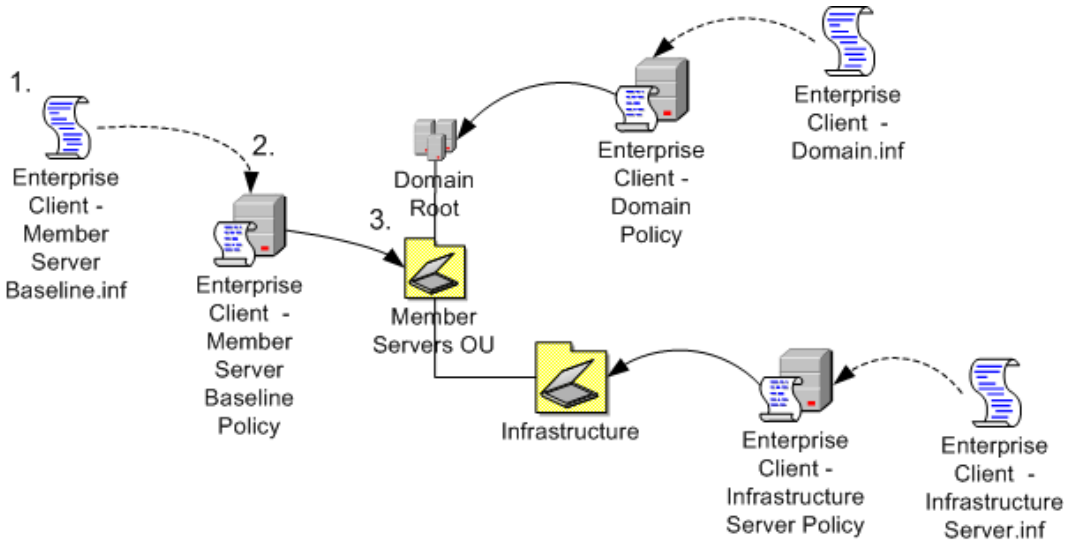

Figure 2.3
Configuring incremental group policies

As mentioned before, this is only one of many possible ways to create an OU structure for deploying GPOs. For more information on creating OUs for Group Policy implementation, see the Microsoft TechNet article, "How to Deploy Active Directory" at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/AD/windows2000/deploy/depovg/add.asp.

This security guide defines several server roles. The following table contains templates created to increase security for these roles when following the above process.

Table 2.1: Windows Server 2003 Roles

Server Role	Description	Security Template
Windows Server 2003 Domain Controllers	A group containing Active Directory domain controllers.	Enterprise Client – Domain Controller.inf
Windows Server 2003 Member servers	All servers that are members of the domain and reside in or below the member server OU.	Enterprise Client – Member Server Baseline.inf
Windows Server 2003 File servers	A group containing locked down file servers.	Enterprise Client – File Server.inf
Windows Server 2003 Print servers	A group containing locked down print servers.	Enterprise Client – Print Server.inf
Windows Server 2003 Infrastructure servers	A group containing locked down DNS, WINS, and DHCP servers.	Enterprise Client – Infrastructure Server.inf
Windows Server 2003 IAS servers	A group containing locked down IAS Servers.	Enterprise Client – IAS Server.inf
Windows Server 2003 Certificate Services servers	A group containing locked down Certificate Authority (CA) Servers.	Enterprise Client – CA Server.inf
Windows Server 2003 Bastion Hosts	A group containing Internet facing servers.	High Security– Bastion Host.inf
Windows Server 2003 IIS servers	A group containing locked down IIS Servers.	Enterprise Client – IIS Server.inf

All incremental template files are expected to be applied to OUs below the member servers OU. For this reason, each of these lower level OUs require that you apply both the Enterprise Client – Member Server Baseline.inf file and the specific incremental file to them to define the role each will fulfill in the organization.

The security requirements for each of these server roles are different. Appropriate security settings for each role are discussed in detail in later chapters.

Important: This guide assumes that computers running Windows Server 2003 will perform specifically defined roles. If the servers in your organization do not match these roles, or you have multipurpose servers, use the settings defined here as guidelines for creating your own security templates. However, bear in mind that the more functions each of your servers perform, the more vulnerable they are to attack.

The final OU design to support these defined server roles is shown in the illustration below.

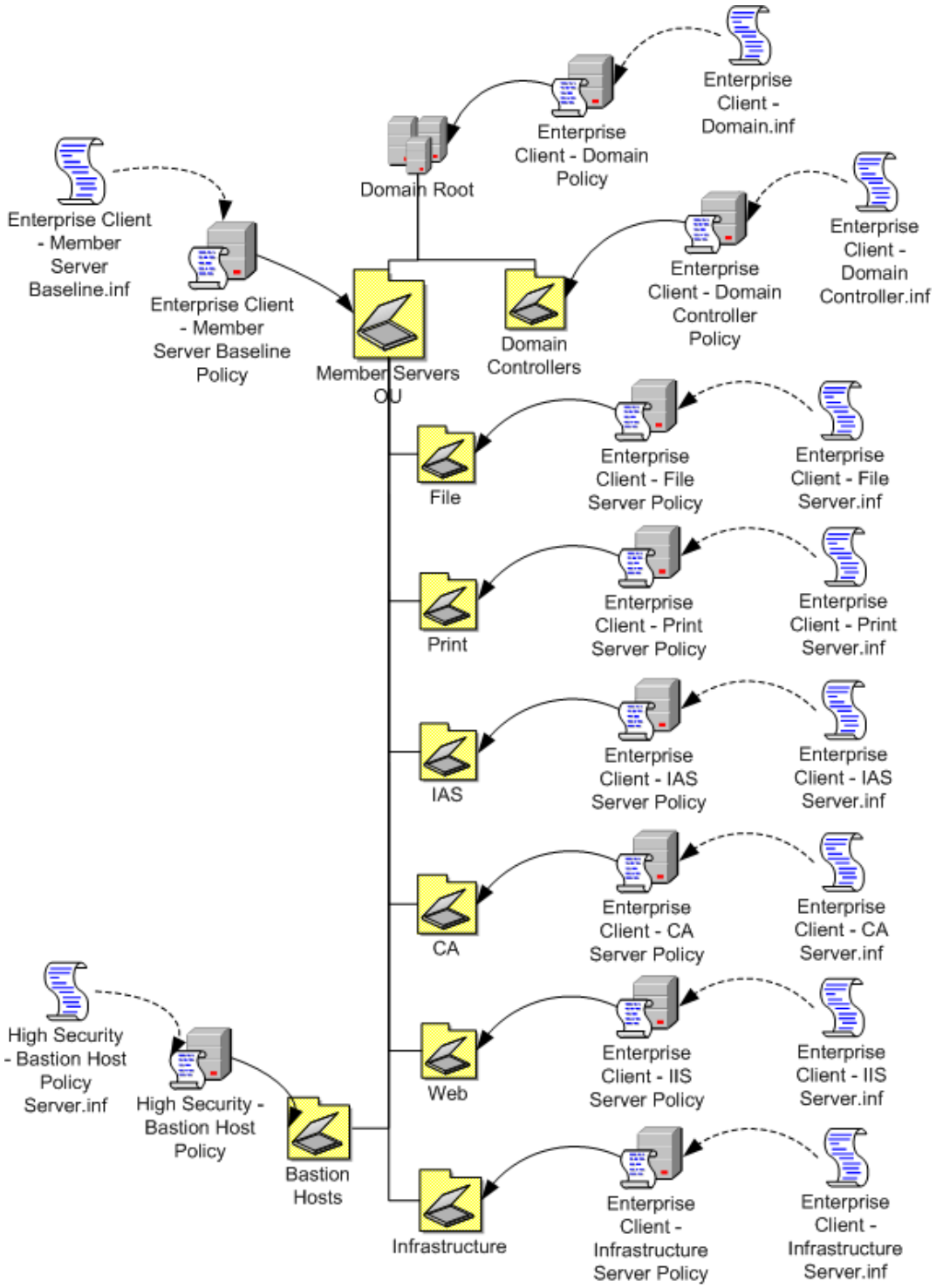

Figure 2.4
Example of OU design

OU, GPO, and Administrative Group Design

The recommended OUs and group policies discussed above create a baseline or new environment to restructure a company's existing OU structure for computers running Windows Server 2003. In addition, the administrators use their predefined administration boundaries to create their respective administrative groups. The correlation of these groups to the OUs they manage is shown in the following table.

Table 2.2: OUs and Administrative Groups

OU Name	Administrative Group
Domain Controllers	Domain Engineering
Member Servers	Domain Engineering
Infrastructure	Operations
File	Operations
Print	Operations
IAS	Domain Engineering
CA	Enterprise Admins
Web	Web Services

Each administrative group has been created within the environment as a Global Group within the child domain.

Domain Engineering has added each of these administrative groups to the appropriate restricted group by using the corresponding GPO. The administrative groups created above will only be members of the Local Administrators group for the computers located in the OUs that specifically contain computers related to their job functions.

Finally, the domain engineers set permissions on each GPO so that only administrators in the domain engineering group are able to edit them.

By default, the new OU structure inherits many security settings from its parent container. For each OU, clear the check box for **Allow inheritable permissions from parent to propagate to this object and all child objects**.

▶ **To clear the Allow Inheritable Permissions option**

1. Open **Active Directory Users and Computers**.
2. Select the **Advanced** view by clicking **View**, and then clicking **Advanced Features**.
3. Right−click the appropriate OU, and then click **Properties**.
4. Click the **Security** tab, and then click **Advanced**.
5. Clear the **Allow inheritable permissions from parent to propagate to this object and all child objects. Include these with entries specifically defined here** checkbox.

Remove any unnecessary groups previously added by administrators, and add the domain group that corresponds to each server role OU. Retain the **Full Control** setting for the Domain Administrators group.

You do not have to perform the tasks to establish these OUs in a particular order, but there are some obvious dependencies. For example, the domain groups must exist before you can delegate control of different OUs to them. The following list defines a suggested order for implementing these tasks:

1. Create the OU structure.
2. Move the computers to the appropriate OUs.
3. Create the administrative groups.
4. Add the appropriate domain accounts to the administrative groups.
5. Delegate administration for each OU to the appropriate domain groups.
6. Create the group policies in the OU where they will be applied.
7. Link each Group Policy to any additional OUs as necessary.
8. Import the appropriate security template to each GPO.
9. Set permissions on each GPO so that the appropriate domain groups have control over them.
10. Add the appropriate domain groups to Restricted Groups for each GPO.
11. Test and refine the group policies.

Domain Policy

You can apply Group Policy security settings at several different levels in an organization. The baseline environment discussed above used Group Policy to apply settings at the following three hierarchy levels in the domain infrastructure:

- **Domain Level** — To address common security requirements, such as account and password policies that must be enforced for all servers in the domain.
- **Baseline Level** — To address specific server security requirements that are common to all servers in the domain infrastructure.
- **Role Specific Level** — To address security requirements for specific server roles. For example, the security requirements for infrastructure servers differ from those for servers running Microsoft Internet Information Services (IIS).

The following sections of this chapter will only discuss the Domain Level policy in detail. Most of the domain security settings addressed are for user accounts and passwords. Keep in mind while reviewing these settings and recommendations that all settings apply to every user in the domain boundary.

Domain Policy Overview

Group Policy is extremely powerful because it allows an administrator to configure a standard network computer. By allowing administrators to make security changes simultaneously on all computers in the domain, or subsets of the domain, GPOs can provide a significant portion of a configuration management solution for any enterprise.

This section provides detailed documentation on the security settings you can use to enhance the security of Windows Server 2003. Tables are provided that describe the security objective of each setting and the configuration necessary to achieve each objective. The settings are divided into categories that correspond to their presentation in the Windows Server 2003 Security Configuration Editor (SCE) user interface.

The types of security changes you can simultaneously apply via Group Policy include:

- Modifying permissions on the file system.
- Modifying permissions on registry objects.
- Changing settings in the registry.
- Changing user rights assignments.
- Configuring system services.
- Configuring auditing and event logs.
- Setting account and password policies.

Account Policies

Account policies, which include Password Policy, Account Lockout Policy, and Kerberos Policy security settings, are only relevant in the Domain Policy for all three environments detailed in this guide. Password Policy provides a vehicle to set complexity and change schedules for highly secured environment passwords. Account Lockout Policy allows tracking of unsuccessful password logon attempts to initiate account lockouts if necessary. Kerberos policies are used for domain user accounts. They determine Kerberos–related settings, such as ticket lifetimes and enforcement.

Password Policy

Complex passwords that change regularly reduce the likelihood of a successful password attack. Password policy settings control the complexity and lifetime for passwords. This section discusses each specific password policy setting and how the settings relate to each of the three environments: Legacy Client, Enterprise Client, and High Security.

Creating strict requirements for password length and complexity does not necessarily translate into users and administrators using strong passwords. With password policies enabled, users of the system may meet the technical complexity requirements for a password defined by the system, but additional strong corporate security policy is needed to change password misuse habits. For example, **Breakfast!**, might meet all password complexity requirements. But this is not a very difficult password to crack.

By knowing the person who created their password, you might be able to guess his or her password based on their favorite food, car, or movie. One strategy of a corporation security program for educating users on choosing strong passwords is to create a poster describing poor passwords and display it in common areas, such as near the water fountain or copy machine. Your organization should set security guidelines for creating strong passwords which should include the following:

- Avoid using words from a dictionary, common or clever misspellings of words, and foreign words.
- Avoid using incrementing passwords with a digit.
- Avoid preceding or appending passwords with a number.
- Avoid using passwords that others can easily guess by looking at your desk (such as names of pets, sports teams, and family members).
- Avoid using words from popular culture.
- Avoid thinking of passwords as words per se—think secret codes.
- Enforce using passwords that require you to type with both hands on the keyboard.
- Enforce using uppercase and lowercase letters, numbers, and symbols in all passwords.
- Enforce using space characters and characters that can be produced only by pressing the Alt key.

The guidelines above should also be used for all service account passwords in your organization. The following sections include the Password Policy recommendations for the three security environments defined in this guide. These values are set at:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Enforce password history

Table 2.3: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
24 passwords remembered	24 passwords remembered	24 passwords remembered	24 passwords remembered

The **Enforce password history** setting determines the number of unique new passwords that have to be associated with a user account before it is possible to reuse an old password. The value must be set between 0 and 24 passwords. The default value for Windows Server 2003 is the maximum, 24 passwords. This policy setting enables administrators to enhance security by ensuring that old passwords are not continually reused. To maintain the effectiveness of the password history, also configure the **Minimum password age** to prevent passwords from being changed immediately. This combination makes it difficult for users to reuse passwords, either accidentally or on purpose.

Since there are common vulnerabilities associated with reusing passwords, and specifying a low number for this setting will allow users to continually recycle a small number of passwords repeatedly, this setting recommendation is consistent across all environments defined in this guide. Also, there are no known issues related to setting this value at the maximum number for environments containing legacy clients.

Maximum password age

Table 2.4: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
42 days	42 days	42 days	42 days

You can configure the **Maximum password age** setting so that passwords expire as often as necessary for your environment. The default values for this setting range from 1 to 999 days. This policy setting defines the period in which an attacker who has cracked a password may use it to access a computer on the network before the password expires. Changing passwords regularly is one way to prevent passwords from being compromised. The default value for this setting is 42 days.

Most passwords can be cracked given enough time and computing power; the more frequently the password changes, the less time an attacker has to crack a password before a new one is created to invalidate his efforts at cracking the old password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support. In order to balance the needs of security and usability in corporate environments, you can increase this setting in the Legacy Client and Enterprise Client. These recommended values increase password security by ensuring passwords are cycled periodically. In addition, the recommended values prevent users from having to change their password so often that they cannot remember what it is.

Minimum password age

Table 2.5: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
1 day	2 days	2 days	2 days

The **Minimum password age** setting determines the number of days that a password must be used before a user changes it. The range of values for this setting is between 0 and 999 days. Setting this to 0 allows you to change the password immediately. The default value for the setting is **1** day.

The **Minimum password age** setting must be less than the **Maximum password age** setting, unless the **Maximum password age** setting is set to **0**, indicating that passwords will never expire. In this case, the **Minimum password age** can be set to any value between 0 and 999.

Set the **Minimum password age** to be greater than 0 if you want **Enforce password history** to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite.

Change this setting from the default to **2** days because when the setting is used in conjunction with a similar low value in the **Enforce password history** setting, the restriction discourages users from recycling the same password again and again. If **Minimum password age** is left at 1 day, and the **Enforce password history** is set to 2 passwords, users would only have to wait 2 days before arriving at an old favorite password. This setting value ensures that users must wait a full two days to change passwords.

The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator–defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, **Enforce password history** is set to 1 by default. It also prevents users from circumventing the **Password history setting** restriction by rapidly setting 24 new passwords.

Minimum password length

Table 2.6: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
7 characters	8 characters	8 characters	12 characters

The **Minimum password length** setting ensures passwords have at least a specified number of characters. Long passwords—eight or more characters—are usually stronger than short ones. With this policy setting, users cannot use blank passwords, and they must create passwords that are a certain number of characters long.

The default value for this setting is **7** characters, but an eight-character password is recommended as it is long enough to provide some level of security, but still short enough for users to easily remember. This setting will provide a great deal of defense against the commonly used dictionary and brute force attacks.

A dictionary attack is a method of obtaining a password through trial and error in which an attacker uses all items in a word list. A brute force attack is a method of obtaining a password or other encrypted text by trying every possible value. The feasibility of a brute force password attack depends on the length of the password, the size of the potential character set, and the computational power available to the attacker.

This guide recommends setting the value for password length in the High Security environment to 12 characters.

Passwords are stored in the Security Accounts Manager (SAM) database or Active Directory after being passed through a one–way hash algorithm. This type of algorithm is not reversible. Therefore, the only way to tell if you have the right password is to run it through the same one–way hash algorithm and compare the results. Dictionary attacks run entire dictionaries through the encryption process, looking for matches. They are a simplistic, yet very effective, approach to finding out who has used common words like "password" or "guest" as their account passwords.

If a password is seven characters or less, the second half of the LM Hash resolves to a specific value that can inform a cracker that the password is shorter than eight characters. Requiring passwords with at least eight characters strengthens even the weaker LMHash because the longer passwords require crackers to decrypt two portions of each password instead of only one. Since you can attack both halves of the LM hash in parallel, the second half of the LM hash is only 1 character long; it will succumb to a brute-force attack in milliseconds, so it doesn't really buy you all that much unless it's an ALT character set.

Also, each additional character in a password increases its complexity exponentially. For instance: A seven–digit password would have $26^{7,}$ or 1 x $10^{7,}$ possible combinations. A seven character alphabetic password with case sensitivity has 52^7 combinations. A seven character case–sensitive alphanumeric password without punctuation has 62^7 combinations. At 1,000,000 attempts per second, it would only take 48 minutes to crack. An eight–character password has 26^8, or 2 x 10^{11}, possible combinations. On the surface, this might seem a mind-boggling number. However, at 1,000,000 attempts per second, a capability of many password-cracking utilities, it would take only 59 hours to try all possible passwords. Remember these times will greatly increase with passwords that use ALT characters and other special keyboard characters, for example ! or @.

For these reasons, using shorter passwords in place of longer ones is not recommended. However, requiring passwords that are too long may generate a high number of mistyped passwords, resulting in an increase in locked out accounts and help desk calls. Furthermore, requiring extremely long passwords can actually decrease the security of an organization because users may be more likely to write their passwords down in fear of forgetting them.

Password must meet complexity requirements

Table 2.7: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Password must meet complexity requirements policy** option checks all new passwords to ensure that they meet basic requirements for strong passwords.

Complexity requirements are enforced when passwords are created. The Windows Server 2003 policy rules cannot be directly modified. However, you can create a new version of passfilt.dll to apply a different set of rules. For the source code for passfilt.dll, see the Microsoft Knowledge Base article 151082: "HOW TO: Password Change Filtering & Notification in Windows NT."

A password of 20 or more characters can actually be set so that it is easier for a user to remember—and more secure—than an eight-character password. The following 27–character password: **I love cheap tacos for $.99**, for example. This type of password, really a pass-phrase, might be simpler for a user to remember than a shorter password such as **P@55w0rd**.

This recommended value, combined with a **Minimum password length** set to **8**, includes upper and lowercase letters and numbers in the keyspace, which increases it from 26 to 62 characters. An eight–character password then has 2.18×10^{14} possible combinations. At 1,000,000 attempts per second, it would take 6.9 years to cycle through all possible permutations. Using these settings in conjunction makes it very difficult to mount a brute force attack. For these reasons, this is the recommendation the three environments defined in this guide.

Store password using reversible encryption

Table 2.8: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The security setting for **Store password using reversible encryption** determines whether the operating system stores passwords using reversible encryption or not.

This policy supports applications using protocols requiring the user's password for authentication purposes. Passwords stored using reversible encryption can be retrieved more easily than passwords stored without this option, increasing vulnerability. For this reason, never enable this policy unless application requirements outweigh the need to protect password information.

Challenge-Handshake Authentication Protocol (CHAP) through remote access or IAS and Digest Authentication in IIS both require this policy.

How to Prevent Users from Changing a Password Except When Required

In addition to the password policies above, some organizations require centralized control over all users. This section describes how to prevent users from changing their passwords except when they are required to do so.

Centralized control of user passwords is a cornerstone of a well–crafted Windows Server 2003 security scheme. You can use Group Policy to set minimum and maximum password ages as discussed previously. But bear in mind that requiring frequent password changes can enable users to circumvent the password–history setting for your environment. Requirements for passwords that are too long may also lead to more calls to the help desk due to users forgetting passwords.

Users can change their passwords during the period between the minimum and maximum password age settings. However, the High Security environment design requires that users change their passwords only when the operating system prompts them to after the 42 days, as configured in the **Maximum password age** setting. To prevent users from changing their passwords (except when required), you can disable the **Change Password** option in the **Windows Security** dialog box that appears when you press CTRL+ALT+DELETE.

You can implement this configuration for an entire domain by using a Group Policy, or implement it for one or more specific users by editing the registry. For more detailed instructions on this configuration, see the Microsoft Knowledge Base article 324744, "How To: Prevent Users from Changing a Password Except When Required in Windows Server 2003," at http://support.microsoft.com/default.aspx?scid=324744.

Account Lockout Policy

The Account lockout policy is a Windows Server 2003 security feature that locks a user account after a number of failed logon attempts occur within a specified time period. The number of attempts allowed and the time period are based on the values configured for the security policy lockout settings. A user cannot log on to a locked account. Windows Server 2003 tracks logon attempts, and the server software can be configured to respond to this type of potential attack by disabling the account for a preset number of failed logins.

When configuring the Account lockout policy in Windows Server 2003, an administrator can set any value for the attempt and time period variables. However, if the value for **Reset account lockout counter after** setting is greater than the value for **Account lockout duration** setting, Windows Server 2003 automatically adjusts the value of the **Account lockout duration** to the same value as **Reset account lockout counter after** setting. In addition, if the value of **Account lockout duration** is lower than the value set for **Reset account lockout counter after**, Windows Server 2003 automatically adjusts the value of the **Reset account lockout counter after** to the same value of the **Account lockout duration** setting. Therefore, if the **Account lockout duration** is defined, the **Reset account lockout counter after** must be less than or equal to the **Account lockout duration**.

Windows Server 2003 does this to avoid conflicting setting values in the security policy. If an administrator configures the **Reset account lockout counter after** setting to a value that is greater than the value for the **Account lockout duration** setting, then enforcement of the **Account lockout duration** setting will expire first, thus making it possible for the user to log back on to the network. However, the **Reset account lockout counter** setting would continue to count down. Because of this, the account lockout threshold would remain at the maximum of three invalid attempts, and the user would not be able to log on.

To avoid this situation, Windows Server 2003 automatically resets the value for the **Reset account lockout counter after** setting to be equal to the value for the **Account lockout duration** setting.

These security policy settings help prevent attackers from guessing user passwords, and they decrease the likelihood of successful attacks on your network environment. The values in the following sections can be configured in the Domain Group Policy at the following location:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Account Lockout Duration

Table 2.9: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Not Defined	30 minutes	30 minutes	15 minutes

The **Account lockout duration** setting determines the length of time before an account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. Setting the value for the **Account lockout duration** setting to **0**, keeps the accounts locked out until an administrator unlocks them. The Windows Server 2003 default value for this setting is **Not Defined**.

While configuring the value for this setting to never automatically unlock may seem like a good idea, doing so may increase the number of calls the help desk in your organization receives to unlock accounts that were locked by mistake. Setting the value for this setting to 30 minutes for the Legacy and Enterprise Client environments and 15 minutes for High Security level decreases the amount of operation overhead during a denial of service (DoS) attack. In a DoS attack, the attacker maliciously performs a number of failed logon attempts on all users in the organization, locking out their accounts. This setting value also gives locked out users the chance to log on again in 30 minutes, a period of time they are more likely to accept without resorting to the help desk.

This guide recommends setting the value to 15 minutes in the High Security environment.

Account lockout threshold

Table 2.10: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
0 invalid login attempts	50 invalid login attempts	50 invalid login attempts	10 invalid login attempts

The **Account lockout threshold** setting determines the number of attempts that a user can make to log on to an account before it is locked.

Authorized users can lock themselves out of an account by incorrectly entering their password, or by changing their password on one computer while logged on to another computer. The computer with the incorrect password may continuously try to authenticate the user, and because the password it is using to authenticate is incorrect, the user account is eventually locked out. To avoid locking out authorized users, set the account lockout threshold to a high number.

Because vulnerabilities can exist both for when the value for this setting is configured and when and it is not, distinct countermeasures for each of these possibilities are defined. Your organization should weigh the choice between the two based on the identified threats and the risks you are trying to mitigate.

- To prevent account lock outs, set the value for **Account lockout threshold** setting to **0**. Setting the **Account Lockout Threshold** setting to **0** helps reduce help desk calls because users can not accidentally lock themselves out of their accounts and it will prevent a DoS attack aimed at intentionally locking out accounts in your organization. Because it will not prevent a brute force attack, choose this setting *only* if both of the following criteria are explicitly met:
  - The password policy forces all users to have complex passwords made up of eight or more characters.
  - A robust auditing mechanism is in place to alert administrators when a series of account lockouts are occurring in the environment. For example, the auditing solution should monitor for security event 539 which is, "Logon failure. The account was locked out at the time the logon attempt was made". This event means that the account was locked out at the time the logon attempt threshold was made. However, event 539 only shows an account lockout, not a failed password attempt. Therefore, your administrators should also monitor for a series of bad password attempts.
- If these criteria are not met, the second option is to configure the **Account lockout threshold** setting to a high enough value to provide users with the ability to accidentally mistype their password several times without locking themselves out of their accounts, while ensuring that a brute force password attack will still lock out the account. In this case, setting the invalid logon attempts to a high number such as 50 ensures adequate security and acceptable usability. This setting value will prevent accidental account lockouts and reduce help desk calls, but will not prevent a DoS attack as mentioned above.

This guide recommends setting the value to 10 invalid login attempts in the High Security environment.

Reset account lockout counter after

Table 2.11: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Not defined	30 minutes	30 minutes	15 minutes

The **Reset account lockout counter after** setting determines the length of time before the **Account lockout threshold** resets to **0** and the account is unlocked. If you define an **Account lockout threshold**, then this reset time must be less than or equal to the value for the **Account lockout duration** setting.

In coordination with the other values configured as part of this guide, leaving this setting at its default value, or configuring the value at an interval that is too long, could make your environment vulnerable to an account lockout DoS attack. Without a policy to reset the account lockout, administrators would have to manually unlock all accounts. Conversely, if there is a reasonable time value for this setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended setting value of 30 minutes defines a time period users are more likely to accept without resorting to the help desk. Leaving this setting at its default only opens you up to an account lockout DoS if you leave it at defaults but change the other ones in the way we recommend. Lowering the level decreases the amount of operation overhead during a denial of service (DoS) attack. In a DoS attack, the attacker maliciously performs a number of failed logon attempts on all users in the organization, locking out their accounts.

This guide recommends setting the value to 15 minutes in the High Security environment.

Kerberos Policy

Kerberos policies are used for domain user accounts. These policies determine Kerberos version 5 protocol–related settings, such as ticket lifetimes and enforcement. Kerberos policies do not exist in the local computer policy. Reducing the lifetime of Kerberos tickets decreases the risk of an attacker stealing passwords and then impersonating legitimate user accounts. However, maintaining these policies increases the authorization overhead. In most environments the default values for these policies should not be changed. The Kerberos settings are include in the Default Domain Policy and enforced there, therefore, this guide does not include them in the security templates that accompany this guide.

This guide does not provide any changes for the default Kerberos policy. For more detail on these settings, please refer to the companion guide, "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*."

Security Options

The account policy must be defined in the Default Domain Policy and is enforced by the domain controllers that make up the domain. A domain controller always obtains the account policy from the Default Domain Policy GPO, even if there is a different account policy applied to the OU that contains the domain controller.

There are two policies in Security Options that also behave like account policies and should be considered at the domain level. You can configure the Domain Group Policy values in the following table at the following location:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Microsoft network server: Disconnect clients when logon hours expire

Table 2.12: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Not Defined	Enabled	Enabled	Enabled

The **Microsoft network server: Disconnect clients when logon hours expire** 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 server message block (SMB) component. When this policy is enabled, it causes client sessions with the SMB service 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. When enabling this setting, you should also enable **Network security: Force logoff when logon hours expire**.

If your organization has configured logon hours for users, then it makes sense to enable this policy, otherwise, users who are assumed to be unable to access network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

If logon hours are not used in your organization, enabling this setting will have no impact. If logon hours are used, then existing user sessions will be forcibly terminated when their logon hours expire.

Network Access: Allow anonymous SID/NAME translation

Table 2.13: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Not Defined	Disabled	Disabled	Disabled

The **Network Access: Allow anonymous SID/NAME translation** setting determines if an anonymous user can request the SID for another user.

If this policy is enabled on a domain controller, a user who knows an administrator's SID attributes could contact a computer that also has this policy enabled and use the SID to obtain the administrator's name. That person could then use the account name to initiate a password guessing attack. Disabled is the default setting on *member* computers; therefore it will have no impact on them. However, the default setting for *domain controllers* is Enabled. Disabling this setting may cause legacy systems to be unable to communicate with Windows Server 2003 based domains such as:

- Windows NT 4.0–based Remote Access Service servers.
- When a Web application on IIS is configured to allow Basic authentication and at the same time has Anonymous access disabled, the built-in Guest user account cannot access the Web application. Also, if you rename the built-in Guest user account to another name, the new name cannot be used to access the Web application.
- Remote Access Service servers running on Windows 2000–based computers that are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Network Security: Force Logoff when Logon Hours expire

Table 2.14: Settings

Domain Member Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Network Security: Force Logoff when Logon Hours expire** setting determines whether to disconnect users who are connected to a local computer outside their user account's valid logon hours. This setting affects the SMB component.

Enabling this policy forcibly disconnects client sessions with the SMB server when the client's logon hours expire and the user will be unable to log on to the system until his or her next scheduled access time. Disabling this policy maintains an established client session after the client's logon hours expire. To affect domain accounts, this setting must be defined in the Default Domain Policy.

Summary

There are several design considerations to make when reviewing a forest, domain, and an Organizational Unit (OU) design to secure an environment.

It is important to research and document any specific autonomy and isolation requirements for the organization. Political autonomy, operational isolation, and legal or regulatory isolation are all valid reasons to consider complex forest designs.

Understanding how to control service administrators is important. Malicious service administrators can present a great risk to an organization. At a lower level, malicious domain administrators can access data in any domain in the forest.

While it may not be easy to change the forest or domain design in an organization, it may be necessary to remediate some security risks for the enterprise. Planning the OU deployment in the organization according to the needs of the service administrators *and* the data administrators is also important. This chapter went into detail on creating an OU model that will support using GPOs for the ongoing management of different server roles in the enterprise.

Finally, the chapter points out the importance of reviewing all domain–wide settings in the organization. Only one set of password, account lockout, and Kerberos version 5 authentication protocol policies can be configured for each domain. Other password and account lockout settings will only affect the local accounts on member servers. Plan to configure settings that will apply to all member servers of the domain, and ensure that these provide an adequate level of security across your organization.

More Information

The following information sources were the latest available on topics closely related to creating a domain infrastructure and Windows Server 2003 at the time this product was released to the pubic.

For more information on account and local policies for Windows 2000, Windows XP, and Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/sag_sceacctpols.asp.

For more information on security and privacy at Microsoft, see: http://www.microsoft.com/security.

For information on the Ten Immutable Laws of Security, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp.

For information on design considerations for delegating administration in Active Directory, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/plan/addeladm.asp.

For information on configuring a Time Server, see: Microsoft Knowledge Base article, "How to Configure an Authoritative Time Server in Windows 2000," at:

http://support.microsoft.com/default.aspx?scid=216734.

For information on Network access and allowing SID/NAME translation, see:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/623.asp.

For information on Network security and forcing logoff when logon hours expire, see:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/566.asp.

Guest Account Cannot be Used When Anonymous Access Is Disabled

http://support.microsoft.com/default.aspx?scid=kb;en-us;251171

3

Creating a Member Server Baseline

Overview

This chapter documents the configuration requirements for managing a baseline security template for all servers running Microsoft® Windows Server™ 2003. The chapter will also provide administrative guidance to set up and configure a secure Windows Server 2003 system in three enterprise environments. The configuration requirements in the chapter form the baseline for all of the other hardening procedures that apply to the specific server roles discussed in later chapters of this guide.

The setting recommendations in this chapter establish a solid foundation for business application servers in an enterprise environment. However, you must comprehensively test the coexistence of these security configurations with your organization's business applications before implementing them in production environments.

The setting recommendations in this chapter are suitable for the majority of enterprises and may be deployed on either existing or new systems running Windows Server 2003. The default security configurations within Windows Server 2003 have been researched, reviewed, and tested. For information about all default settings and a detailed explanation on each of the settings discussed in this chapter, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159. However, the majority of the following configuration recommendations are for security levels that are higher than the default settings.

The following baseline security settings for all Windows Server 2003 systems in enterprise environments discussed in this chapter relate to the three environments defined below. The environments are:

- **Legacy Client** — Provides adequate security that will not constrain a mixed–state environment. The Legacy Client level is specific to environments with legacy clients. This environment is the lowest lockdown level defined in this guide. In order to further secure environments, organizations may choose to migrate to the next lockdown level, the Enterprise Client level, or start at this level if they do not have legacy clients to secure. This business environment includes Microsoft Windows® 98, Microsoft Windows NT® version 4.0 Workstation, Window 2000 Professional, and Windows XP Professional workstations. This environment only contains Windows 2000 or later domain controllers. There are no Windows NT 4.0 domain controllers in this environment, but Windows NT member servers may exist.
- **Enterprise Client** — Provides solid security that is designed for a new system environment. This business environment includes clients running Windows 2000 Professional and Windows XP Professional. The majority of work required to move from the Legacy Environment to the Enterprise Environment involves upgrading legacy clients, such as Windows 98 and Windows NT 4.0 Workstation to Windows 2000 or Windows XP. All domain controllers in this environment are Windows 2000 Server or later. Member servers in this environment are Windows 2000 Server or later.
- **High Security** — Provides enhanced security standards from the previous Enterprise Client level. Moving from the Enterprise Environment to the High Security Environment requires conforming to stringent security policies for both clients and servers. This environment contains clients running Windows 2000 Professional, Windows XP Professional, and domain controllers running Windows 2000 Server or later. In the High Security environment, concern about security is so great that significant loss of functionality and manageability is considered to be an acceptable tradeoff in order to achieve the highest level of security. Member servers in this environment are Windows 2000 Server or later.

The following figure shows the three layers of security and the clients supported in each.

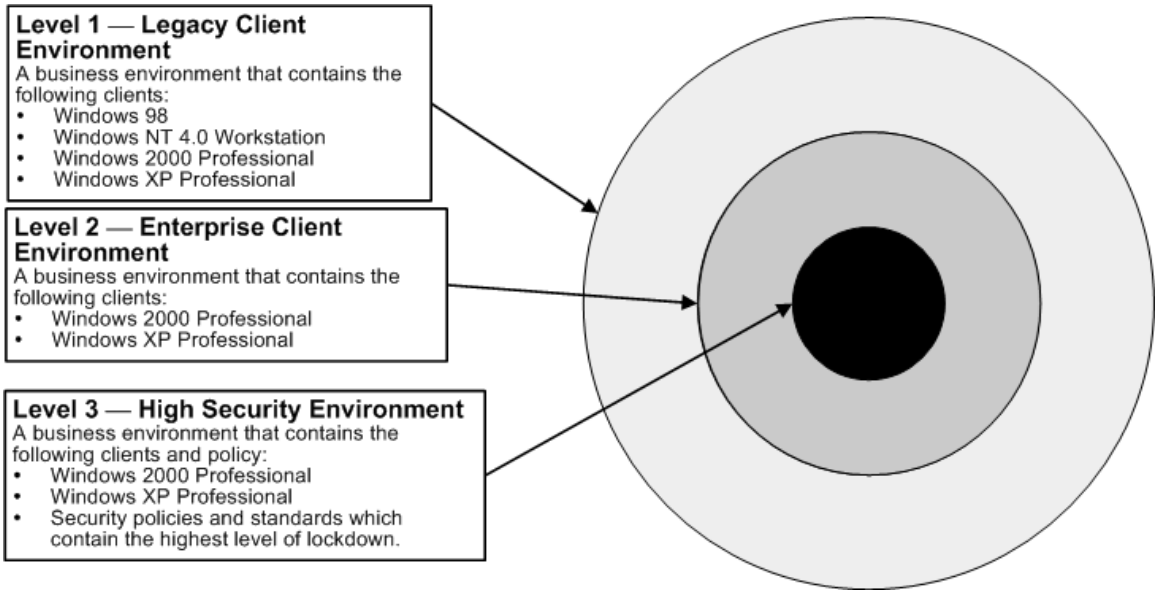

Figure 3.1
Existing and planned levels of lockdown

Organizations that want to provide a phased approach to securing their environments may choose to start at the Legacy Client environment level and then gradually move to the higher security levels as their applications and client computers are upgraded and tested with tightened security settings.

The following figure shows how the .inf file security templates are used as a foundation for the Enterprise Client–Member Server Baseline Policy (MSBP). The figure also shows one possible way of linking this policy in order to apply it to all servers in an organization.

Windows Server 2003 ships with default setting values that are set to a secure state. In many instances, this chapter prescribes settings other than default values, as well as enforces specific defaults for the three environments defined in this guide. For information about all default settings, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, available at http://go.microsoft.com/fwlink/?LinkId=15159.

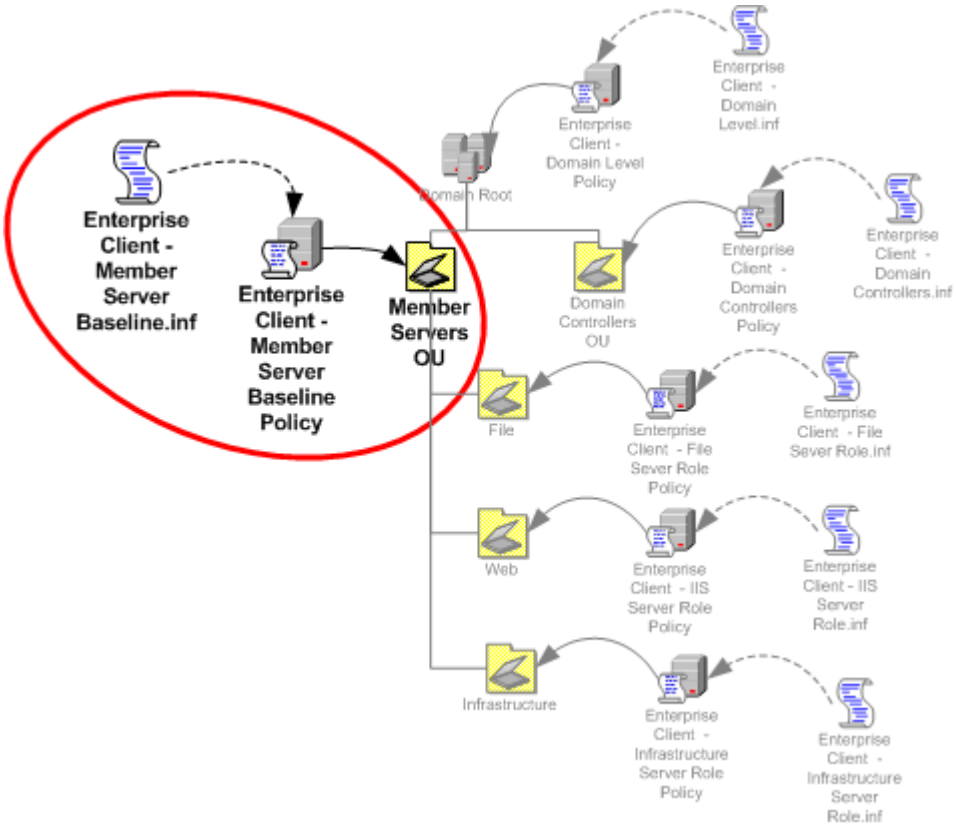

Figure 3.2
The security template Enterprise Client–Member Server Baseline.inf is imported into the MSBP, which is then linked to the Member Servers organizational unit (OU)

Hardening procedures for specific server roles are defined in the remaining chapters of this guide. The primary server roles in this guide include:

- Domain controllers, which include Domain Name System (DNS) services.
- Infrastructure server roles that include:
  - Windows Internet Name Service (WINS)
  - Dynamic Host Configuration Protocol (DHCP)
- File
- Print
- Internet Information Services (IIS)
- Microsoft Internet Authentication Server (IAS)
- Certificate Services servers (CA)
- Bastion Hosts

Many of the settings that appear in the Enterprise Client MSBP that follow also apply to these server roles in the three environments defined in this guide. The security templates are uniquely designed to address the security needs of each particular environment. The following table shows the relationship between the baseline security templates and the three environments. If there is a need to call out specifics in the Legacy Client, Enterprise Client, or High Security levels, the security template that relates to the recommended baseline policy contains the level identity to distinguish the correct template for it. For example, the Enterprise Client–Member Server Baseline.inf file is the recommended security template for the Enterprise Client environment.

Table 3.1: Baseline Security Templates for All Three Environments

Legacy Client	Enterprise Client	High Security
Legacy Client – Member Server Baseline.inf	Enterprise Client – Member Server Baseline.inf	High Security – Member Server Baseline.inf

The security settings common to all of the environments in the Member Server Baseline.inf security templates are described in the section below on the Windows Server 2003 Baseline Policy. These baseline security templates are also the starting point for the security templates for domain controllers defined in Chapter 4, "Hardening Domain Controllers."

The Enterprise Client–Domain Controllers Role.inf template provides the baseline for the Group Policy object (GPO) of the Domain Controllers Group Policy and is linked to the Domain Controllers organizational unit (OU) in all three environments. Step–by–step instructions for creating the OUs and Group Policies, and then importing the appropriate security template into each GPO, are provided in Chapter 2, "Configuring the Domain Infrastructure."

Note: Some hardening procedures cannot be automated using Group Policy; these are described in the Additional Member Server Hardening Procedures section of this chapter.

Windows Server 2003 Baseline Policy

The settings at the Member Server OU level define the common settings for all member servers in the domain. This is done by creating a GPO that is linked to the Member Server OU, known as a baseline policy. The GPO automates the process of configuring specific security settings on each server. The following settings are described as they appear in the user interface (UI) of the Security Configuration Editor (SCE) snap–in.

Audit Policy

Administrators should set up an audit policy. An audit policy determines the security events to report to the network administrators so that user or system activity in specified event categories is recorded. The administrator can monitor security–related activity, such as who accesses an object, if a user logs on to or off from a computer, or if changes are made to an auditing policy setting.

Before implementing audit policies, one must decide which event categories need to be audited for the corporate environment. The auditing settings that an administrator chooses for the event categories define the corporate auditing policy. By defining audit settings for specific event categories, administrators can create an audit policy that suits the security needs of an organization.

If no auditing is configured, it will be difficult or impossible to determine what took place during a security incident. However, if auditing is configured so that too many authorized activities generate events, the security event log will fill up with useless data. Therefore, the following recommendations help balance the decisions on what to monitor so that the data collected is relevant.

The table below includes the Audit Policy setting recommendations for the three environments defined in this guide. You may notice that the settings for most values are similar across the three environments.

The following values can be configured in the Domain Group Policy section of Windows Server 2003 at the following location:

> Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

For a summary of the prescribed settings in this section, see the Windows Server 2003 Security Guide Settings Microsoft Excel spreadsheet. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Audit account logon events

Table 3.2: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Success	Success Failure	Success Failure	Success Failure

The **Audit account logon events** setting determines whether to audit each instance of a user logging on to or off another computer that validates the account. Authenticating a domain user account on a domain controller generates an account logon event. The event is logged in the domain controller's security log. Authenticating a local user on a local computer generates a logon event. The event is logged in the local security log. There are no Account logoff events logged.

The following table includes some of the important security events that this setting logs in the Security Event Log.

Table 3.3: Account Logon Events

Event ID	Event Description
672	An authentication service (AS) ticket was successfully issued and validated.
673	A ticket granting service (TGS) ticket was granted. A TGS is a ticket issued by the Kerberos version 5 ticket – granting service TGS that allows a user to authenticate to a specific service in the domain.
674	A security principal renewed an AS ticket or TGS ticket.
675	Pre – authentication failed. This event is generated on a Key Distribution Center (KDC) when a user types in an incorrect password.
676	Authentication ticket request failed. This event is not generated in Windows XP Professional or in members of the Windows Server family.
677	A TGS ticket was not granted. This event is not generated in Windows XP Professional or in the members of the Windows Server family.
678	An account was successfully mapped to a domain account.
681	Logon failure. A domain account logon was attempted. This event is not generated in Windows XP Professional or in members of the Windows Server family.
682	A user has reconnected to a disconnected terminal server session.
683	A user disconnected a terminal server session without logging off.

The event IDs above can be useful when creating custom alerts to monitor any software suite, for example, Microsoft Operations Manager (MOM).

Audit account management

Table 3.4: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	Success Failure	Success Failure	Success Failure

The **Audit account management** setting determines whether to audit each account management event on a computer. Examples of account management events include:

- A user account or group is created, changed, or deleted.
- A user account is renamed, disabled, or enabled.
- A password is set or changed.

Organizations need to be able to determine who has created, modified, or deleted both domain and local accounts. Unauthorized changes could indicate mistaken changes made by an administrator who does not understand how to follow corporate policies or a deliberate attack.

For example, account management failure events often indicate that a lower–level administrator—or an attacker who has compromised a lower–level administrator's account—might be attempting to elevate his or her privilege. From the logs you can see which accounts an attacker has modified and created.

For this reason, the countermeasure for this setting is to configure it to include both the **Success** and **Failure** values for all three environments. The following table includes some of the important security events that this setting records in the Security Event Log.

Table 3.5: Account Management Events

Event ID	Event Description
624	A user account was created.
627	A user password was changed.
628	A user password was set.
630	A user account was deleted.
631	A global group was created.
632	A member was added to a global group.
633	A member was removed from a global group.
634	A global group was deleted.
635	A new local group was created.
636	A member was added to a local group.
637	A member was removed from a local group.
638	A local group was deleted.
639	A local group account was changed.
641	A global group account was changed.
642	A user account was changed.
643	A domain policy was modified.
644	A user account was automatically locked.
645	A computer account was created.
646	A computer account was changed.
647	A computer account was deleted.
648	A local security group with security disabled was created. **Note**: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks.
649	A local security group with security disabled was changed.
650	A member was added to a security – disabled local security group.
651	A member was removed from a security – disabled local security group.
652	A security – disabled local group was deleted.
653	A security – disabled global group was created.
654	A security – disabled global group was changed.
655	A member was added to a security – disabled global group.
656	A member was removed from a security – disabled global group.
657	A security – disabled global group was deleted.
658	A security – enabled universal group was created.
659	A security – enabled universal group was changed.
660	A member was added to a security – enabled universal group.
661	A member was removed from a security – enabled universal group.
662	A security – enabled universal group was deleted.
663	A security – disabled universal group was created.

(continued)

664	A security – disabled universal group was changed.
665	A member was added to a security – disabled universal group.
666	A member was removed from a security – disabled universal group.
667	A security – disabled universal group was deleted.
668	A group type was changed.
684	The security descriptor of administrative group members was set. **Note**: Every 60 minutes on a domain controller, a background thread searches all members of administrative groups (such as domain, enterprise, and schema administrators) and applies a fixed security descriptor on them. This event is logged.
685	Name of an account was changed.

The event IDs above can be useful when creating custom alerts to monitor any software suite, for example, MOM. Most operational management software can be customized with scripts in order to capture or flag events based on the event IDs above.

Audit directory service access

Table 3.6: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	Success Failure	Success Failure	Success Failure

The **Audit directory service access** setting determines whether to audit the event of a user accessing a Microsoft Active Directory® directory service object that has its own system access control list (SACL) specified. Setting **Audit directory service access** to **No Auditing** makes it difficult or impossible to determine what Active Directory objects may have been compromised during a security incident. There will be no audit record evidence available for analysis after a security incident if the values for this setting are not set to **Success** and **Failure**.

Configuring **Audit directory service access** to **Success** generates an audit entry each time that a user successfully accesses an Active Directory object with a specified SACL. Configuring this setting to **Failure** generates an audit entry each time that a user unsuccessfully attempts to access an Active Directory object with a specified SACL.

Table 3.7: Directory Service Access Events

Event ID	Event Description
566	A generic object operation took place.

Audit logon events

Table 3.8: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Success	Success Failure	Success Failure	Success Failure

The **Audit logon events** setting determines whether to audit each instance of a user logging on to or off of a computer. Records are generated from the **Account logon events** setting on domain controllers to monitor domain account activity and on local computers to monitor local account activity.

Configuring the **Audit logon events** setting to **No auditing** makes it difficult or impossible to determine which user has either logged on or attempted to log on to computers in the enterprise. Enabling the **Success** value for the **Auditing logon events** setting on a domain member will generate an event each time that someone logs on to the system regardless of where the accounts reside on the system. If the user logs on to a local account, and the **Audit account logon events** setting is **Enabled**, the user logon will generate two events.

There will be no audit record evidence available for analysis after a security incident takes place if the values for this setting are not configured to **Success** and **Failure** for all three security environments defined in this guide.

Table 3.9: Audit Logon Events

Event ID	Audit Logon Events
528	A user successfully logged on to a computer.
529	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
530	Logon failure. A logon attempt was made outside the allowed time.
531	Logon failure. A logon attempt was made using a disabled account.
532	Logon failure. A logon attempt was made using an expired account.
533	Logon failure. A logon attempt was made by a user who is not allowed to log on at the specified computer.
534	Logon failure. The user attempted to log on with a password type that is not allowed.
535	Logon failure. The password for the specified account has expired.
536	Logon failure. The Net Logon service is not active.
537	Logon failure. The logon attempt failed for other reasons. **Note**: In some cases, the reason for the logon failure may not be known.
538	The logoff process was completed for a user.
539	Logon failure. The account was locked out at the time the logon attempt was made.
540	A user successfully logged on to a network.
541	Main mode Internet Key Exchange (IKE) authentication was completed between the local computer and the listed peer identity (establishing a security association), or quick mode has established a data channel.
542	A data channel was terminated.
543	Main mode was terminated. **Note**: This might occur as a result of the time limit on the security association expiring (the default is eight hours), policy changes, or peer termination.
544	Main mode authentication failed because the peer did not provide a valid certificate or the signature was not validated.

(continued)

545	Main mode authentication failed because of a Kerberos failure or a password that is not valid.
546	IKE security association establishment failed because the peer sent a proposal that is not valid. A packet was received that contained data that is not valid.
547	A failure occurred during an IKE handshake.
548	Logon failure. The security identifier (SID) from a trusted domain does not match the account domain SID of the client.
549	Logon failure. All SIDs corresponding to untrusted namespaces were filtered out during an authentication across forests.
550	Notification message that could indicate a possible denial – of – service (DoS) attack.
551	A user initiated the logoff process.
552	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
682	A user has reconnected to a disconnected terminal server session.
683	A user disconnected a terminal server session without logging off. **Note**: This event is generated when a user is connected to a terminal server session over the network. It appears on the terminal server.

Audit object access

Table 3.10: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	Success Failure	Success Failure	Success Failure

By itself, this setting will not cause any events to be audited. The **Audit object access** setting determines whether to audit the event of a user accessing an object—for example, a file, folder, registry key, printer, and so forth—that has a specified SACL.

A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:

- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.
- A flag to indicate whether to audit failed access events, successful access events, or both.

Configuring this setting to **Success** generates an audit entry each time that a user successfully accesses an object with a specified SACL. Configuring this setting to **Failure** generates an audit entry each time that a user unsuccessfully attempts to access an object with a specified SACL.

Corporations should define only the actions they want enabled when configuring SACLs. For example, you might want to enable the **Write and Append Data auditing** setting on executable files to track the replacement or changes to those files, which computer viruses, worms, and Trojan horses will commonly cause. Similarly, you might want to track changes to or even the reading of sensitive documents.

Therefore, this guide recommends enabling both the **Success** and **Failure** auditing values for this setting in all three environments defined in this guide.

Table 3.11: Object Access Events

Event ID	Event Description
560	Access was granted to an already existing object.
562	A handle to an object was closed.
563	An attempt was made to open an object with the intent to delete it. **Note**: This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified in Createfile().
564	A protected object was deleted.
565	Access was granted to an already existing object type.
567	A permission associated with a handle was used. **Note**: A handle is created with certain granted permissions (Read, Write, and so on). When the handle is used, up to one audit is generated for each of the permissions that were used.
568	An attempt was made to create a hard link to a file that is being audited.
569	The resource manager in Authorization Manager attempted to create a client context.
570	A client attempted to access an object. **Note**: An event will be generated for every attempted operation on the object.
571	The client context was deleted by the Authorization Manager application.
572	The Administrator Manager initialized the application.
772	The Certificate Manager denied a pending certificate request.
773	Certificate Services received a resubmitted certificate request.
774	Certificate Services revoked a certificate.
775	Certificate Services received a request to publish the certificate revocation list (CRL).
776	Certificate Services published the CRL.
777	A certificate request extension was made.
778	One or more certificate request attributes changed.
779	Certificate Services received a request to shut down.
780	Certificate Services backup started.
781	Certificate Services backup completed.
782	Certificate Services restore started.
783	Certificate Services restore completed.
784	Certificate Services started.
785	Certificate Services stopped.
786	The security permissions for Certificate Services changed.
787	Certificate Services retrieved an archived key.
788	Certificate Services imported a certificate into its database.
789	The audit filter for Certificate Services changed.
790	Certificate Services received a certificate request.
791	Certificate Services approved a certificate request and issued a certificate.
792	Certificate Services denied a certificate request.
793	Certificate Services set the status of a certificate request to pending.
794	The certificate manager settings for Certificate Services changed.

(continued)

795	A configuration entry changed in Certificate Services.
796	A property of Certificate Services changed.
797	Certificate Services archived a key.
798	Certificate Services imported and archived a key.
799	Certificate Services published the certificate authority (CA) certificate to Active Directory.
800	One or more rows have been deleted from the certificate database.
801	Role separation enabled.

Audit policy change

Table 3.12: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	Success	Success	Success

The **Audit policy change** setting determines whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies. This includes making changes to the audit policy itself.

Configuring this setting to **Success** generates an audit entry for each successful change to user rights assignment policies, audit policies, or trust policies. Configuring this setting to **Failure** generates an audit entry for each failed change to user rights assignment policies, audit policies, or trust policies.

The recommended settings would let you see any account privileges that an attacker attempts to elevate—for example, by adding the **Debug programs** privilege or the **Back up files and directories** privilege. Policy change auditing also includes making changes to the audit policy itself as well as to trust relationships.

Note: This guide recommends configuring the value for this setting to **Success** only because including the setting value for **Failure** will not provide meaningful access information. Currently, setting this value to **Failure** does not capture meaningful events.

Table 3.13: Audit Policy Change Events

Event ID	Event Description
608	A user right was assigned.
609	A user right was removed.
610	A trust relationship with another domain was created.
611	A trust relationship with another domain was removed.
612	An audit policy was changed.
613	An Internet Protocol security (IPSec) policy agent started.
614	An IPSec policy agent was disabled.
615	An IPSec policy agent changed.
616	An IPSec policy agent encountered a potentially serious failure.
617	A Kerberos version 5 policy changed.
618	Encrypted Data Recovery policy changed.
620	A trust relationship with another domain was modified.
621	System access was granted to an account.
622	System access was removed from an account.
623	Auditing policy was set on a per−user basis
625	Auditing policy was refreshed on a per−user basis.
768	A collision was detected between a namespace element in one forest and a namespace element in another forest. **Note**: When a namespace element in one forest overlaps a namespace element in another forest, it can lead to ambiguity in resolving a name belonging to one of the namespace elements. This overlap is also called a collision. Not all parameters are valid for each entry type. For example, fields such as DNS name, NetBIOS name, and SID are not valid for an entry of type 'TopLevelName.'
769	Trusted forest information was added. **Note**: This event message is generated when forest trust information is updated and one or more entries are added. One event message is generated for each added, deleted, or modified entry. If multiple entries are added, deleted, or modified in a single update of the forest trust information, all the generated event messages are assigned a single unique identifier called an operation ID. This allows you to determine that the multiple generated event messages are the result of a single operation. Not all parameters are valid for each entry type. For example, parameters such as DNS name, NetBIOS name and SID are not valid for an entry of type "TopLevelName."
770	Trusted forest information was deleted. **Note**: See event description for event 769.
771	Trusted forest information was modified. **Note**: See event description for event 769.
805	The event log service read the security log configuration for a session.

Audit privilege use

Table 3.14: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	No Auditing	Failure	Success Failure

The **Audit privilege use** setting determines whether to audit each instance of a user exercising a user right. Configuring this value to **Success** generates an audit entry each time that a user right is exercised successfully. Configuring this value to **Failure** generates an audit entry each time that a user right is exercised unsuccessfully.

Audits are not generated when the following user rights are exercised, even if the **Audit privilege use** settings is configured to **Success** or **Failure**. This is because auditing these user rights generates many events in the security log, which may constrain the performance of your computers. To audit the following excluded rights, you must enable the **Audit: Audit the use of Backup and Restore privilege** security option in Group Policy:

- **Bypass traverse checking**
- **Debug programs**
- **Create a token object**
- **Replace process level token**
- **Generate security audits**
- **Back up files and directories**
- **Restore files and directories**

Enabling privilege auditing generates a very large number of event records. For this reason, each security environment defined in this guide has unique recommendations for these settings. Failed use of a user right is an indicator of a general network problem and often can be a sign of an attempted security breach. Corporations should set the **Audit privilege use** setting to **Enable** only if there is a specific business reason to do so.

Table 3.15: Privilege Use Events

Event ID	Event Description
576	Specified privileges were added to a user's access token. **Note**: This event is generated when the user logs on.
577	A user attempted to perform a privileged system service operation.
578	Privileges were used on an already open handle to a protected object.

Audit process tracking

Table 3.16: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	No Auditing	No Auditing	No Auditing

The **Audit process tracking** setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Configuring this setting to **Success** generates an audit entry each time the process being tracked succeeds. Configuring this setting to **Failure** generates an audit entry each time the process being tracked fails.

Enabling **Audit process tracking** will generate a large number of events, so typically it is set to **No Auditing**. However, these settings can provide a great benefit during an incident response from the detailed log of the processes started and the time when they were launched.

Table 3.17: Detailed Tracking Events

Event ID	Event Description
592	A new process was created.
593	A process exited.
594	A handle to an object was duplicated.
595	Indirect access to an object was obtained.
596	A data protection master key was backed up. **Note**: The master key is used by the CryptProtectData and CryptUnprotectData routines, and Encrypting File System (EFS). The master key is backed up each time a new one is created. (The default setting is 90 days.) The key is usually backed up by a domain controller.
597	A data protection master key was recovered from a recovery server.
598	Auditable data was protected.
599	Auditable data was unprotected.
600	A process was assigned a primary token.
601	A user attempted to install a service.
602	A scheduler job was created.

Audit system events

Table 3.18: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Auditing	Success	Success	Success

The **Audit system events** setting determines whether to audit when a user restarts or shuts down a computer or when an event occurs that affects either the system security or the security log. Configuring this setting to **Success** generates an audit entry when a system event is executed successfully. Configuring this setting to **Failure** generates an audit entry when a system event is attempted unsuccessfully.

The table below includes some of the most useful successful events for this category.

Table 3.19: System Event Messages for Audit System Events

Event ID	Event Description
512	Windows is starting up.
513	Windows is shutting down.
514	An authentication package was loaded by the Local Security Authority.
515	A trusted logon process has registered with the Local Security Authority.
516	Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.
517	The audit log was cleared.
518	A notification package was loaded by the Security Accounts Manager.
519	A process is using an invalid local procedure call (LPC) port in an attempt to impersonate a client and reply or read from or write to a client address space.
520	The system time was changed. **Note**: This audit normally appears twice.

User Rights Assignments

User Rights Assignments determine which users or groups have logon rights or privileges on the computers in your organization. Logon rights and privileges govern the rights that users have on the target system. They are used to grant the right to perform certain actions, such as logging on from the network or locally, as well as administrative tasks, such as generating new logon tokens.

Note: Throughout the following section, User Rights Assignments, "Not defined" means Administrators still have the privilege for every right not defined.

Local administrators can make changes, but any domain-based Group Policy settings will override them the next time that the Group Policies are refreshed or reapplied.

User rights assignment settings can be configured in Windows Server 2003 in the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

The default User Rights Assignments are different between the various types of servers in your enterprise. For example, Windows Server 2003 contains the following differences in User Rights Assignments with built–in groups between member servers and domain controllers. Similar built–in groups between member servers and domain controllers are not documented in the list below.

Member Servers

- **Power Users**
  Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications.
- **HelpServicesGroup**
  This is the group for the Help and Support Center. Support_388945a0 is a member of this group by default.
- **TelnetClients**
  Members of this group have access to Telnet Server on the system.

Domain Controllers

- **Server Operators**
  Members of this group can administer domain servers.
- **Terminal Server License Services**
  Members of this group have access to Terminal Server License Servers on the system.
- **Windows Authorization Access Group**
  Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on user objects.

The group **Guests** and the user accounts Guest and Support_388945a0 have unique SIDs between different domains. Therefore, this Group Policy for user right assignments may need to be modified on a system where only the specific target group exists. Alternatively, the policy templates can be edited individually to include the appropriate groups within the .inf files. For example, a domain controller Group Policy should be created on a domain controller in a testing environment.

Note: Because of the unique SIDs that exist between Guests, Support_388945a0, and Guest, some hardening settings cannot be automated using the security templates included with this guide; these are described in the Additional Member Server Hardening Procedures section later in this chapter.

This section provides details on the prescribed user rights assignments for the three environments defined in this guide for the MSBP. For a summary of the prescribed settings in this section, see the Windows Server 2003 Security Guide Settings Excel spreadsheet. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Access this computer from the network

Table 3.20: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators, Backup Operators, Everyone, Power Users, and Users	Not Defined	Not Defined	Administrators, Authenticated Users

The **Access this computer from the network** user right determines which users and groups are allowed to connect to the computer over the network. This user right is required by a number of network protocols including server message block (SMB) – based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP).and Component Object Model Plus (COM+).

Although in Windows Server 2003 permissions granted to the **Everyone** security group no longer grant access to anonymous users, guest groups and accounts can still be granted access through the **Everyone** security group. For this reason, this guide recommends removing the **Everyone** security group from the **Access this computer from the network** user right in the High Security environment to further guard from attacks targeting guest access to the domain.

Act as part of the operating system

Table 3.21: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Not Defined	Not Defined	Revoke all security groups and accounts

The **Act as part of the operating system** user right allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. Typically, only low – level authentication services require this privilege. There are no security groups defined by default; therefore, this user right is sufficient for the Legacy Client and Enterprise Client environments. However, in the High Security environment, configure this setting to **Revoke all security groups and accounts**.

Add workstations to domain

Table 3.22: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Not Defined	Not Defined	Administrators

The **Add workstations to domain** user right allows the user to add a computer to a specific domain. For the privilege to take effect, it must be assigned to the user as part of the Default Domain Controllers Policy for the domain. There are no security groups defined by default; therefore, this user right is sufficient for the Legacy Client and Enterprise Client environments. However, this setting is configured to grant only the **Administrators** group this user right in the High Security environment.

Adjust memory quotas for a process

Table 3.23: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators, NETWORK SERVICE, LOCAL SERVICE	Not Defined	Not Defined	Administrators, NETWORK SERVICE, LOCAL SERVICE

The **Adjust memory quotas for a process** user right allows a user to adjust the maximum memory that is available to a process. This privilege is useful for system tuning, but it can be abused. In the wrong hands, this user right can be used to launch a DoS attack. The default security groups for this user right are sufficient for the **Legacy Client** and **Enterprise Client** environments. However, this user right is configured to enforce **Administrators, NETWORK SERVICE, LOCAL SERVICE** value only in the **High Security** environment.

Allow log on locally

Table 3.24: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators, Backup Operators, Power Users, and Users	Administrators, Backup Operators, Power Users	Administrators, Backup Operators, Power Users	Administrators, Backup Operators, Power Users

The **Allow log on locally** user right determines which users can interactively log on to the specified computer. Logons initiated by pressing the CTRL+ALT+DEL key– combination on the keyboard require the user to have this logon right. Any account with this user right could be used to log on to the local console of the computer. Restricting this privilege to legitimate users who need to be able to log on to the system prevents unauthorized users from elevating their privileges or from introducing viruses into the computing environment.

Allow log on through Terminal Services

Table 3.25: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators and Remote Desktop Users	Administrators and Remote Desktop Users	Administrators and Remote Desktop Users	Administrators

The **Allow log on through Terminal Services** user right determines which users or groups have permission to log on as a Terminal Services client. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, in the High Security environment, only **Administrators** should have the ability to log on as a Terminal Services client.

Change the system time

Table 3.26: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators and Power Users	Not Defined	Not Define	Administrators

The **Change the system time** user right determines which users and groups can change the time and date on the internal clock of the computer. Users with this user right can affect the appearance of event logs because event logs will reflect the new time, not the actual time that the events occurred. Limit the **Change the system time** privilege to users with a legitimate need to be able to change the time, such as members of the IT department. Discrepancies between the time on the local computer and on the domain controllers may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or to get authorization for accessing domain resources after logging on.

Debug programs

Table 3.27: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Revoke all security groups and accounts	Revoke all security groups and accounts	Revoke all security groups and accounts

The **Debug programs** user right determines which users can attach a debugger to any process or to the kernel. This user right provides complete access to sensitive and critical operating system components. Program debugging should not take place in production environments except in extreme circumstances, such as troubleshooting a business–critical application that cannot be effectively assessed in the test environment.

Deny access to this computer from the network

Table 3.28: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
SUPPORT_388945a0	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONOYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts

Note: ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0; Guest; and all NON-operating system service accounts are not included in the .inf security template. These accounts and groups have unique SIDs for each domain in your organization. Therefore, they must be added manually. For further information, see the Manual Hardening Procedures at the end of this chapter.

The **Deny access to this computer from the network** user right determines which users are prevented from accessing a computer over the network. This user right will deny a number of network protocols including SMB – based protocols, NetBIOS, CIFS, HTTP. and COM+. This policy setting supersedes the **Access this computer from the network** user right when a user account is subject to both policies. Configuring this logon right for other groups could limit the abilities of users assigned to specific administrative roles in your environment. Verify that delegated tasks will not be negatively impacted.

Deny log on as a batch job

Table 3.29: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Guests; Support_388945a0; Guest	Guests; Support_388945a0; Guest	Guests; Support_388945a0; Guest

Note: ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0; Guest; and all NON-operating system service accounts are not included in the .inf security template. These accounts and groups have unique SIDs for each domain in your organization. Therefore, they must be added manually. For further information, see the Manual Hardening Procedures at the end of this chapter.

The **Deny log on as a batch job** user right determines which accounts are prevented from logging on to the system as a batch job. A batch job is not a batch file (bat)—but rather a batch–queue facility. Accounts used for scheduling jobs via the Task Scheduler need this right. This **Deny log on as a batch job** user right setting overrides the **Log on as a batch job** user right setting. Accounts with this logon right could be used to schedule jobs that could consume excessive system resources leading to a DoS condition. For this reason, not assigning the **Deny log on as a batch job** user right to the recommended accounts can be a security risk.

Deny log on through Terminal Services

Table 3.30: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Built-in Administrator; Guests; Support_388945a0; Guest ;all NON-operating system service accounts	Built-in Administrator; Guests; Support_388945a0; Guest ;;all NON-operating system service accounts	Built-in Administrator ; Guests; Support_388945a0; Guest ; all NON-operating system service accounts

Note: ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0; Guest; and all NON-operating system service accounts are not included in the .inf security template. These accounts and groups have unique SIDs for each domain in your organization. Therefore, they must be added manually. For further information, see the Manual Hardening Procedures at the end of this chapter.

The **Deny log on through Terminal Services** user right determines which users and groups are prohibited from logging on as a Terminal Services client. After joining the baseline member server to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end–user processing. Remember, the MSBP will not receive this Group Policy until the server is joined to the domain and restarted twice. Therefore, the use of the local Administrator accounts is prohibited.

Enable computer and user accounts to be trusted for delegation

Table 3.31: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not defined	Not Defined	Not Defined	Revoke all security groups and accounts

The **Enable computer and user accounts to be trusted for delegation** privilege allows the user to change the **Trusted for Delegation** setting on a user or computer object in Active Directory. The user or computer that is granted this privilege must also have write access to the account control flags on the object. Misuse of this privilege could lead to unauthorized users impersonating other users on the network.

Force shutdown from a remote system

Table 3.32: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not Defined	Not Defined	Administrators

The **Force shutdown from a remote system** user privilege allows a user to shut down a computer from a remote location on the network. Any user who can shut down a computer can cause a DoS condition; therefore, this privilege should be tightly restricted.

Generate security audits

Table 3.33: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
NETWORK SERVICE, LOCAL SERVICE	Not defined	Not defined	NETWORK SERVICE, LOCAL SERVICE

The **Generate security audits** user privilege allows a process to generate audit records in the security log. The security log can be used to trace unauthorized system access. Accounts that are able to write to the security log could be used by an attacker to fill that log with meaningless events. If the computer is configured to overwrite events as needed, the attacker could use this method to remove evidence of his or her unauthorized activities. If the computer is configured to shut down when it is unable to write to the security log, this method could be used to create a DoS condition.

Impersonate a client after authentication

Table 3.34: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
SERVICE, Administrators	Not defined	Not defined	Local Service; Network Service

Assigning the **Impersonate a client after authentication** privilege allows applications 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 service that he or she has created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to **Local Service, NETWORK SERVICE** in the High Security environment.

Increase scheduling priority

Table 3.35: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Increase scheduling priority** privilege allows a user to increase the base priority class of a process. Increasing relative priority within a priority class is not a privileged operation. This privilege is not required by administrative tools supplied with the operating system but might be required by software development tools. A user with this privilege can increase the scheduling priority of a process to **Real – Time**, leaving little processing time for all other processes, which could lead to a DoS condition. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** group in the High Security environment.

Load and unload device drivers

Table 3.36: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Load and unload device drivers** privilege determines which users can dynamically load and unload device drivers. This privilege is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer. Device drivers run as highly privileged code. A user granted the **Load and unload device drivers** privilege can unintentionally install malicious code masquerading as a device driver. It is assumed that administrators will exercise greater care and install only drivers with verified digital signatures. The default user groups for this right are sufficient for the **Legacy Client** and **Enterprise Client** environments. However, this right is configured to enforce the default **Administrators** group in the High Security environment.

Lock pages in memory

Table 3.37: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Not defined	Not defined	Administrators

The **Lock pages in memory** user right allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Enabling this user right can result in significant degradation of system performance. Users with this privilege can assign physical memory to several processes, leaving little or no random access memory (RAM) for other processes. This could lead to a DoS condition. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** in the High Security environment.

Log on as a batch job

Table 3.38: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
SUPPORT_388945a0 , LOCAL SERVICE	Not defined	Not defined	Revoke all security groups and accounts

The **Log on as a batch job** user right allows a user to log on by using a batch–queue facility such as the Task Scheduler service. This is a low – risk vulnerability so the default settings for this user right are sufficient for most organizations. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to **Revoke all security groups and accounts** in the High Security environment.

Manage auditing and security log

Table 3.39: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Manage auditing and security log** privilege allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. The right to manage the security event log is a powerful user privilege that should be closely guarded. Anyone with this user right can clear the security log, possibly erasing important evidence of unauthorized activity. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** in the High Security environment.

Modify firmware environment values

Table 3.40: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Modify firmware environment values** user right allows modification of system environment variables either by a process through an API, or by a user through **System Properties**. Anyone with this privilege could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** group in the High Security environment.

Perform volume maintenance tasks

Table 3.41: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Perform volume maintenance tasks** user right allows a non–administrative or remote user to manage volumes or disks. A user with this privilege could delete a volume, leading to the loss of data or a DoS condition. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** group in the High Security environment.

Profile single process

Table 3.42: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators and Power Users	Not Defined	Not Defined	Administrators

The **Profile single process** user right determines which users can use performance monitoring tools to monitor the performance of non–system processes. This is a moderate vulnerability; an attacker with this privilege could monitor a computer's performance to help identify critical processes that he or she might want to attack directly. The attacker may also be able to determine what processes are running on the system so that he or she could identify countermeasures to avoid—such as antivirus software, an intrusion–detection system, or other users logged onto a system. To better secure an environment, remove **Power Users** from this user right in the High Security environment.

Profile system performance

Table 3.43: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Profile system performance** user right allows a user to monitor the performance of system processes. Not restricting this user right presents a moderate vulnerability; an attacker with this privilege could monitor a computer's performance to help identify critical processes that he or she might want to attack directly. The attacker could also determine what processes are running on the system to identify countermeasures to avoid, such as antivirus software or an intrusion–detection system. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **Administrators** group in the High Security environment.

Remove computer from docking station

Table 3.44: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators, Power Users	Not defined	Not defined	Administrators

The **Remove computer from docking station** user right allows the user of a portable computer to undock the computer by clicking **Eject PC** on the **Start** menu. Anyone who has this user right can remove a portable computer that has been booted up from its docking station. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the **Administrators** group in the High Security environment.

Replace a process level token

Table 3.45: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
LOCAL SERVICE, NETWORK SERVICE	Not defined	Not defined	LOCAL SERVICE, NETWORK SERVICE

The **Replace a process level token** user right allows a parent process to replace the access token that is associated with a child process. The default security groups for this user right are sufficient for the Legacy Client and Enterprise Client environments. However, this user right is configured to enforce the default **LOCAL SERVICE** and **NETWORK SERVICE** groups in the High Security environment.

Restore files and directories

Table 3.46: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators and Backup Operators	Not Defined	Administrators	Administrators

The **Restore files and directories** user right determines which users can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories. It also determines which users can set any valid security principal as the owner of an object. In an Enterprise or High Security environment, only **Administrators** should have the right to restore files and directories. The job of restoring files is usually carried out by administrators or another specifically delegated security group, especially for highly sensitive servers and domain controllers.

Shut down the system

Table 3.47: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Backup Operators, Power Users, Administrators	Not Defined	Not Defined	Administrators

The **Shut down the system** user right determines which locally logged on users can shut down the operating system using the **Shut Down** command. Misuse of this user right can result in a DoS attack. The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Even though a system shutdown requires the ability to log on to the server, you should be very careful about the accounts and groups that you allow to shut down a domain controller. In the High Security environment, only **Administrators** should be granted the **Shut down the system** user right.

Synchronize directory service data

Table 3.48: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Not defined	Not defined	Revoke all security groups and accounts

The **Synchronize directory service data** user right allows a process to read all objects and properties in the directory, regardless of the protection on the objects and properties. This privilege is required in order to use LDAP directory synchronization (Dirsync) services. The default setting specifies no accounts; however, this user right is configured to **Revoke all security groups and accounts** in the High Security environment

Take ownership of files or other objects

Table 3.49: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Not defined	Not defined	Administrators

The **Take ownership of files or other objects** user right allows a user to take ownership of any securable object in the system, including Active Directory objects, NTFS file system (NTFS) files, and folders, printers, registry keys, services, processes, and threads. Ensure that only the local **Administrators** group has the **Take ownership of files or other objects** user right.

Security Options

The Security Options section of Group Policy is used to configure security settings for computers, such as digital signing of data, administrator and guest account names, floppy disk drive and CD–ROM drive access, driver installation behavior, and logon prompts.

The Security Options settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Not all security groups exist on all types of systems. Also, many security group SIDs are unique among the domains in your enterprise. Therefore, the Security Options portion of Group Policy may need to be manually modified on a system where the target group exists. This section provides details on the prescribed security options for the three environments defined in this guide for the MSBP. For a summary of the prescribed settings in this section, see the Windows Server 2003 Security Guide Settings Excel spreadsheet. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Accounts: Guest account status

Table 3.50: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Accounts: Guest account status** security option setting determines whether the Guest account is enabled or disabled. This account allows unauthenticated network users to gain access to the system by logging in as **Guest**. Therefore, this security option setting is configured to **Disabled** in all three environments.

Accounts: Limit local account use of blank passwords to console logon only

Table 3.51: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Accounts: Limit local account use of blank passwords to console logon only** security option setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. Enabling this setting prevents a local account with a nonblank password from logging on to a network from a remote client, and local accounts that are not password protected will only be able to log on physically via the keyboard of the computer. Therefore, enforce the default value for this countermeasure across all three environments.

Audit: Audit the access of global system objects

Table 3.52: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Audit: Audit the access of global system objects** security option setting audits the access of global system objects when it is in effect. If both the **Audit: Audit the access of global system objects** and the **Audit object access audit policy** settings are enabled, a large number of audit events will be generated. This setting is configured to the default in all three environments defined in this guide.

Note: Changes to the configuration of this security option setting will not take effect until you restart Windows Server 2003.

Audit: Audit the use of Backup and Restore privilege

Table 3.53: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Audit: Audit the use of Backup and Restore privilege** security option setting determines whether to audit the use of all user privileges, including **Backup and Restore**, when the **Audit privilege use** policy setting is in effect. Enabling this policy could generate a large number of security events, causing servers to respond slowly and forcing the security event log to record numerous events of little significance. Therefore, this setting is configured to the default across all three environments.

Note: Changes to the configuration of this security option setting will not take effect until you restart Windows Server 2003.

Audit: Shut down system immediately if unable to log security audits

Table 3.54: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Enabled

The **Audit: Shut down system immediately if unable to log security audits** security option setting determines whether the system shuts down immediately if it is unable to log security events. The administrative overhead required to enable this setting in the Legacy Client and Enterprise Client environments was determined to be too high; therefore, Group Policy configures the **Shut down system immediately if unable to log security audits** setting to **Disabled**. However, this setting is enabled in High Security environments because the burden of this additional administrative overhead is acceptable in order to prevent deleting events from the security event log unless an administrator specifically chooses to do so.

Devices: Allow undock without having to log on

Table 3.55: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Disabled	Disabled	Disabled

The **Devices: Allow undock without having to log on** security option setting determines whether a portable computer can be undocked without the user having to log on to the system. Enabling this setting eliminates a logon requirement and allows using an external hardware eject button to undock the computer. Disabling this setting means a user must be granted the **Remove computer from docking station** user right (not defined in this guidance) in order to undock the computer without logging on to the system.

Devices: Allowed to format and eject removable media

Table 3.56: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators	Administrators	Administrators	Administrators

The **Devices: Allowed to format and eject removable media** security option setting determines who can format and eject removable media. Only administrators should be able to eject removable media on servers. Therefore, the countermeasure for this setting is the default for all three of the environments defined in this guide.

Devices: Prevent users from installing printer drivers

Table 3.57: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

For a computer to print to a network printer, it must have the driver for that network printer installed. Enabling the **Devices: Prevent users from installing printer drivers** security option setting allows only those in the **Administrators** or **Power Users** groups, or those with **Server Operator** privileges to install a printer driver as part of adding a network printer. Disabling this setting allows any user to install a printer driver as part of adding a network printer. The countermeasure for this setting is the default for all three of the environments defined in this guide.

Devices: Restrict CD–ROM access to locally logged–on user only

Table 3.58: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Not Defined	Not Defined	Enabled

The **Devices: Restrict CD – ROM access to locally logged – on user only** security option setting determines whether a CD–ROM is accessible to both local and remote users simultaneously. Enabling this setting allows only the interactively logged–on user to access removable CD–ROM media. If this policy is enabled, and no one is logged on interactively, the CD–ROM is accessible over the network. In the Legacy Client and Enterprise Client environments, this value is set to **Not Defined**. In the High Security environment, the value is set to **Enabled**.

Devices: Restrict floppy access to locally logged–on user only

Table 3.59: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Not Defined	Not Defined	Enabled

The **Devices: Restrict floppy access to locally logged–on user only** security option setting determines whether removable floppy media are accessible to both local and remote users simultaneously. Enabling this setting allows only the interactively logged–on user to access removable floppy media. If this policy is enabled, and no one is logged on interactively, the floppy media is accessible over the network. In the **Legacy Client** and **Enterprise Client** environments, this value is set to **Disabled**. In the High Security environment, the value is set to **Enabled**.

Devices: Unsigned driver installation behavior

Table 3.60: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Warn but allow installation	Warn but allow installation	Warn but allow installation	Warn but allow installation

The **Devices: Unsigned driver installation behavior** security option setting determines what happens when an attempt is made to install a device driver (by means of Setup API) that has not been approved and signed by the Windows Hardware Quality Lab (WHQL). This option prevents the installation of unsigned drivers or warns the administrator that an unsigned driver is about to be installed. This can prevent installing drivers that have not been certified to run on Windows Server 2003. One potential problem with configuring this setting to the **Warn but allow installation** value is that unattended installation scripts will fail when installing unsigned drivers.

Domain controller: Allow server operators to schedule tasks

Table 3.61: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Disabled	Disabled	Disabled

The **Domain controller: Allow server operators to schedule tasks** security option setting determines whether Server Operators are allowed to submit jobs by means of the AT schedule facility. This setting is disabled in all three environments defined in this guide. The impact of disabling this setting should be small for most organizations. Users, including those in the **Server Operators** group, will still be able to create jobs via the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

Note: AT Service Account can be modified in order to select a different account rather than the LOCAL SYSTEM account. To change the account, open **System Tools**, click **Scheduled Tasks**, and then click **Accessories** folder. Then click **AT Service Account** on the **Advanced** menu.

Domain controller: LDAP server signing requirements

Table 3.62: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Not Defined	Not Defined	Require signing

The **Domain controller: LDAP server signing requirements** security option setting determines whether the LDAP server requires signing to negotiate with LDAP clients. Network traffic that is neither signed nor encrypted is susceptible to man–in–the–middle attacks in which an intruder captures packets between the server and the client and modifies them before forwarding them to the client. In the case of an LDAP server, this means that an attacker could cause a client to make decisions based on false records from the LDAP directory. If all domain controllers are running Windows 2000 or later, set this security option to **Require signing**. Otherwise, leave this setting as **Not Defined**. Since all computers in the High Security environment are running either Windows 2000 or Windows Server 2003, this setting is configured to **Require signing** for this environment.

Domain controller: Refuse machine account password changes

Table 3.63: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	Disabled	Disabled	Disabled

The **Domain controller: Refuse machine account password changes** security option setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. Enabling this setting on all domain controllers in a domain prevents computer account passwords on domain members from changing, leaving them susceptible to attack. Therefore, the value for this security option is set to **Disabled** in the three environments defined in this guide.

Domain member: Digitally encrypt or sign secure channel data (always)

Table 3.64: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Disabled	Disabled	Enabled

The **Domain member: Digitally encrypt or sign secure channel data (always)** security option setting determines whether all secure channel traffic initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, then it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data is signed and encrypted. This security option to **Disabled** in the Legacy Client and Enterprise Client environments and it is configured to **Enabled** in the High Security environment.

Note: In order to take advantage of this security option setting on member workstations and servers, all domain controllers that constitute the member's domain must be running Windows NT 4.0 with Service Pack 6a or later; this is not supported in Windows 98 Second Edition clients (unless they have the dsclient installed).

Domain member: Digitally encrypt secure channel data (when possible)

Table 3.65: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Domain member: Digitally encrypt secure channel data (when possible)** security option setting determines whether a domain member may attempt to negotiate encryption for all secure channel traffic that it initiates. Enabling this setting causes the domain member to request encryption of all secure channel traffic. Disabling this setting prevents the domain member from negotiating secure channel encryption. Therefore, this setting is configured to **Enabled** in all three environments defined in this guide.

Domain member: Digitally sign secure channel data (when possible)

Table 3.66: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Domain member: Digitally sign secure channel data (when possible)** security option setting determines whether a domain member may attempt to negotiate signing for all secure channel traffic that it initiates. Signing protects the traffic from being modified by anyone who captures the data en route. This setting is configured to **Enabled** in all three environments defined in this guide.

Domain member: Disable machine account password changes

Table 3.67: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Domain member: Disable machine account password changes security** option setting determines whether a domain member may periodically change its computer account password. Enabling this setting prevents the domain member from changing its computer account password. Disabling this setting allows the domain member to change its computer account password as specified by the **Domain Member: Maximum age for machine account password** setting, which by default is every 30days. Computers that are no longer able to automatically change their account passwords are in risk of an attacker determining the password for the system's domain account. Therefore, set this countermeasure to **Disabled** across the three environments defined in this guide.

Domain member: Maximum machine account password age

Table 3.68: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
30 days	30 days	30 days	30 days

The **Domain member: Maximum machine account password age** security option setting determines the maximum allowable age for a computer account password. This setting also applies to computers running Windows 2000, but it is not available through the Security Configuration Manager tools on these computers. By default, the domain members automatically change their domain passwords every 30 days. Increasing this interval significantly, or setting it to 0 so that the computers no longer change their passwords, gives an attacker more time to undertake a brute force password guessing attack against one of the computer accounts. Therefore, this setting is configured to the **30 days** in all three environments defined in this guide.

Domain member: Require strong (Windows 2000 or later) session key

Table 3.69: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Domain member: Require strong (Windows 2000 or later) session key** security option setting determines whether 128–bit key strength is required for encrypted secure channel data. Enabling this setting prevents establishing a secure channel without 128–bit encryption. Disabling this setting requires the domain member to negotiate key strength with the domain controller. Session keys used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Therefore, since the three security environments described in this guide contain Windows 2000 domain controllers or later, this setting is configured to **Enabled** in all three environments.

Note: You will be unable to join computers running Windows 2000 with this setting enabled to Windows NT 4.0 domains.

Interactive logon: Do not display last user name

Table 3.70: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Interactive logon: Do not display last user name** security option setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. Enabling this setting prevents displaying the last logged on user's name in the **Log On to Windows** dialog box. The **Interactive logon: Do not display last user name** setting is enabled in the baseline server policy in the three environments defined in this guide.

Interactive logon: Do not require CTRL+ALT+DEL

Table 3.71: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Interactive logon: Do not require CTRL+ALT+DEL** security option setting determines whether pressing CTRL+ALT+DEL is required before a user can log on. Disabling this setting requires all users to press CTRL+ALT+DEL before logging on to Windows (unless they are using a smart card for Windows logon). This setting is set to **Disabled** in all three environments defined in this guide to decrease the chance of an attacker being able to intercept user passwords via a Trojan horse program.

Interactive logon: Message text for users attempting to log on

Table 3.72: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. If unauthorized, terminate access now! Clicking on OK indicates your acceptance of the information in the background.	This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. If unauthorized, terminate access now! Clicking on OK indicates your acceptance of the information in the background.	This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted. If unauthorized, terminate access now! Clicking on OK indicates your acceptance of the information in the background.

The **Interactive logon: Message text for users attempting to log on** security option setting specifies a text message that is displayed to users when they log on. 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. The message text setting is recommended for all three environments.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives. In addition, both the **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings must both be enabled in order for either one to work properly.

Interactive logon: Message title for users attempting to log on

Table 3.73: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION

The **Interactive logon: Message title for users attempting to log on** security option setting allows a title to be specified in the title bar of the window that contains the Interactive logon users see when they log on to the system. The reasoning behind this setting is the same as that for the **Message text for user attempting to log on** setting. Organizations that do not utilize this setting are more legally vulnerable to trespassers who attack the network surface. Therefore, this setting is enabled in the three environments defined in this guide.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives. In addition, both the **Interactive logon: Message text for users attempting to log on and Interactive logon: Message title for users attempting to log on** settings must both be enabled in order for either one to work properly.

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Table 3.74: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
10	1	0	0

The **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** security option setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally so that in the event that a domain controller cannot be contacted on subsequent logons, a user can still log on. This setting determines the number of unique users for whom logon information is cached locally. Configuring this value to **0** disables logon caching, which is the recommended setting for all three environments.

Interactive logon: Prompt user to change password before expiration

Table 3.75: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
14 days	14 days	14 days	14 days

The **Interactive logon: Prompt user to change password before expiration** security option setting determines how many days in advance users are warned that their passwords are about to expire. The Account Policies section of this guide recommends configuring user passwords to expire periodically. If users are not notified when their passwords are about to expire, they may not realize it until the passwords have already expired. This could lead to confusion for users accessing the network locally, or make it impossible for users who are accessing your organization's network via dial–up or virtual private networking (VPN) connections. Therefore, this setting is configured to the default setting value **14 days** in the three environments defined in this guide.

Interactive logon: Require Domain Controller authentication to unlock workstation

Table 3.76: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

For domain accounts, the **Interactive logon: Require Domain Controller authentication to unlock workstation** security option setting determines whether a domain controller must be contacted to unlock a computer. This setting addresses a vulnerability similar to the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting. A user could disconnect the network cable of the server and unlock the server using an old password without authenticating to unlock the server. To prevent this, this setting is configured to **Enabled** in the three environments defined in this guide.

Important: This setting applies to computers running Windows 2000 or later, but it is not available through the Security Configuration Manager tools on computers running Windows 2000 —only Windows Server 2003.

Interactive logon: Smart card removal behavior

Table 3.77: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No Action	Not Defined	Lock Workstation	Lock Workstation

The **Interactive logon: Smart card removal behavior** security option setting determines what happens when the smart card for a logged–on user is removed from the smart card reader. Setting this option to **Lock Workstation** locks the workstation when the smart card is removed, allowing users to leave the area, take their smart cards with them, and automatically lock their workstations. Setting this option to **Force Logoff** automatically logs the user off when the smart card is removed.

Microsoft network client: Digitally sign communications (always)

Table 3.78: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Enabled	Enabled

The **Microsoft network client: Digitally sign communications (always)** security option setting determines whether packet signing is required by the SMB client component. Enabling this setting prevents the Microsoft network client from communicating with a Microsoft network server unless that server agrees to perform SMB packet signing. In mixed environments with legacy clients, set this option to **Disabled** as these clients will not be able to authenticate or gain access to domain controllers. However, you can use this setting in Windows 2000 or later environments. The Enterprise Client and High Security environments defined in this guide only contain systems running Windows 2000 or later, which support signing digital communications. Therefore, to increase communications security between systems in this environment, this setting is configured to **Enabled** in the Enterprise Client and High Security environments.

Microsoft network client: Digitally sign communications (if server agrees)

Table 3.79: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Microsoft network client: Digitally sign communications (if server agrees)** security option setting determines whether the SMB client will attempt to negotiate SMB packet signing. Implementing digital signing in Windows networks helps to prevent session hijacking. By enabling this setting, the Microsoft network client on member servers will request signing only if the servers with which it is communicating accept digitally signed communication. This setting is configured to **Enabled** in the three environments defined in this guide.

Microsoft network client: Send unencrypted password to third–party SMB servers

Table 3.80: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

If the **Microsoft network client: Send unencrypted password to third–party SMB servers** security option setting is enabled, the SMB redirector is allowed to send plaintext passwords to non–Microsoft SMB servers that do not support password encryption during authentication. This setting is configured to the default value **Disabled** in the three environments defined in this guide, unless application requirements supersede the need to maintain secret passwords.

Microsoft network server: Amount of idle time required before suspending session

Table 3.81: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
15 minutes	15 minutes	15 minutes	15 minutes

The **Microsoft network server: Amount of idle time required before suspending session** security option setting determines the amount of continuous idle time that must pass in an SMB session before the session is suspended due to inactivity. Administrators can use this policy to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. This setting is configured to **15 minutes** in the three environments defined in this guide.

Microsoft network server: Digitally sign communications (always)

Table 3.82: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Enabled	Enabled

The **Microsoft network server: Digitally sign communications (always)** security option setting determines whether packet signing is required by the SMB server component before further communication with an SMB client is permitted. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which closes session hijacking attacks and supports message authentication (thus preventing man-in-the-middle attacks). SMB signing provides this authentication by placing a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating systems will be unable to connect. Completely disabling all SMB signing leaves the computers vulnerable to session hijacking attacks.

Microsoft network server: Digitally sign communications (if client agrees)

Table 3.83: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Microsoft network server: Digitally sign communications (if client agrees)** security option setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which closes session hijacking attacks and supports message authentication (thus preventing man-in-the-middle attacks). SMB signing provides this authentication by placing a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating systems will be unable to connect. Completely disabling all SMB signing leaves the computers vulnerable to session hijacking attacks.

Microsoft network server: Disconnect clients when logon hours expire

Table 3.84: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Microsoft network server: Disconnect clients when logon hours expire** security option setting determines whether to disconnect users who are connected to a network computer outside of their user account's valid logon hours. This setting affects the SMB component. If your organization has configured logon hours for users, then it makes sense to enable this setting; otherwise, users should not be able to access network resources outside of their logon hours or they may be able to continue to use those resources with sessions established *during* allowed hours. Therefore, this setting is configured to **Enabled** in the three environments defined in this guide.

Network access: Do not allow anonymous enumeration of SAM accounts

Table 3.85: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Network access: Do not allow anonymous enumeration of SAM accounts** security option setting determines what additional permissions will be granted for anonymous connections to the computer. This setting is configured to **Enabled** in the three environments defined in this guide.

Network access: Do not allow anonymous enumeration of SAM accounts and shares

Table 3.86: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Network access: Do not allow anonymous enumeration of SAM accounts and shares** security option setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This setting is configured to **Enabled** in the three environments defined in this guide.

Network access: Do not allow storage of credentials or .NET Passports for network authentication

Table 3.87: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Network access: Do not allow storage of credentials or .NET Passports for network authentication** security option setting determines whether settings for **Stored User Names and Passwords** will save passwords, credentials, or Microsoft .NET Passports for later use after gaining domain authentication. This setting is configured to **Enabled** in the three security environments defined in this guide.

Note: When configuring this security setting, changes will not take effect until you restart Windows.

Network access: Let Everyone permissions apply to anonymous users

Table 3.88: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Network access: Let Everyone permissions apply to anonymous users** security option setting determines what additional permissions are granted for anonymous connections to the computer. Enabling this setting allows anonymous Windows users to perform certain activities, such as enumerating the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks. Therefore, this setting is configured to **Disabled** in the three environments defined in this guide.

Note: Domains with this setting will be unable to establish or maintain trusts with Windows NT 4.0 domains or domain controllers.

Network access: Named Pipes that can be accessed anonymously

Table 3.89: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not defined	None	None	None

The **Network access: Named Pipes that can be accessed anonymously** security option setting determines which communication sessions (named pipes) will have attributes and permissions that allow anonymous access. The value for the **Network access: Named Pipes that can be accessed anonymously** setting should be configured to **None** in Enterprise Client and High Security environments.

Important: If you need to enable this setting, ensure that you only add the named pipes that are needed to support the applications in your environment. As with all recommended settings in this guide, this setting should be carefully tested in your production environment.

Network access: Remotely accessible registry paths

Table 3.90: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
System\CurrentControlSet\Control\ProductOptions; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion

The **Network access: Remotely accessible registry paths** security option setting determines which registry paths can be accessed over the network. It is recommended to enforce the default setting in the baseline security templates for all three security environments defined in this guide.

Note: Even if this security option is set, you must also start the Remote Registry system service if authorized users are going to be able to access the registry over the network.

Network access: Remotely accessible registry paths and sub–paths

Table 3.91: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\TerminalServer	System\CurrentControlSet\Control\TerminalServer	System\CurrentControlSet\Control\TerminalServer	System\CurrentControlSet\Control\TerminalServer
System\CurrentControlSet\Control\TerminalServer\UserConfig	System\CurrentControlSet\Control\TerminalServer\UserConfig	System\CurrentControlSet\Control\TerminalServer\UserConfig	System\CurrentControlSet\Control\TerminalServer\UserConfig
System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration	System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration	System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration	System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog

The **Network access: Remotely accessible registry paths and sub–paths** security option setting determines which registry paths and sub–paths can be accessed over the network. It is recommended to enforce the default setting in the baseline security templates for all three security environments defined in this guide.

Network access: Restrict anonymous access to Named Pipes and Shares

Table 3.92: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Network access: Restrict anonymous access to Named Pipes and Shares** security option setting restricts anonymous access to shares and named pipes when it is enabled to the settings for:

- **Network access: Named pipes that can be accessed anonymously**
- **Network access: Shares that can be accessed anonymously**

This setting is configured to the default for the three environments defined in this guide.

Network access: Shares that can be accessed anonymously

Table 3. 93: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
COMCFG,DFS$	None	None	None

The **Network access: Shares that can be accessed anonymously** security option setting determines which network shares can be accessed by anonymous users. The default for this setting has little impact as all users have to be authenticated before they can access shared resources on the server. Therefore, ensure that this setting is configured to **None** in the three environments defined in this guide.

Note: Enabling this Group Policy setting is very dangerous; any shares that are listed can be accessed by any network user. This could lead to the exposure or corruption of sensitive corporate data.

Network access: Sharing and security model for local accounts

Table 3.94: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Classic – local users authenticate as themselves	Classic – local users authenticate as themselves	Classic – local users authenticate as themselves	Classic – local users authenticate as themselves

The **Network access: Sharing and security model for local accounts** security option setting determines how network logons using local accounts are authenticated. The **Classic** setting allows fine control over access to resources. Using the **Classic** setting allows you to grant different types of access to different users for the same resource. Using the **Guest only** setting allows you to treat all users equally. In this context, all users authenticate as **Guest only** to receive the same access level to a given resource. Therefore, the **Classic** default setting option is used for the three environments defined in this guide.

Network security: Do not store LAN Manager hash value on next password change

Table 3.95: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Enabled

The **Network security: Do not store LAN Manager hash value on next password change** security option setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT hash. For this reason, this setting is configured to **Enabled** in the security environments defined in this guide.

Note: Very old legacy operating systems and some third–party applications may fail when this setting is enabled. Also you will need to change the password on all accounts after enabling this setting.

Network security: LAN Manager authentication level

Table 3.96: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Send NTLM response only	Send NTLMv2 responses only	Send NTLMv2 response only\refuse LM	Send NTLMv2 response only\refuse LM & NTLM

The **Network security: LAN Manager authentication level** security option setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of security negotiated, and the level of authentication accepted by servers as follows. The following numbers in parentheses below are the actual settings for the **LMCompatibilityLevel** registry value. This setting should be configured to the highest level that your environment allows according to the following guidelines:

In a pure Windows NT 4.0 SP4 or later environment—including Windows 2000 and Windows XP Professional—configure this setting to **Send NTLMv2 response only\refuse LM & NTLM** on all clients, and then to **Send NTLMv2 response only\refuse LM & NTLM** on all servers once all clients are configured. The exception to this recommendation is Windows 2003 Routing and Remote Access servers, which will not function properly if this setting is set higher than **Send NTLMv2 response only\refuse LM**.

The Enterprise Client environment contains Routing and Remote Access servers. For this reason, the setting for this environment is configured to **Send NTLMv2 response only\refuse LM**. The High Security environment does not contain Routing and Remote Access servers, so the setting for this environment is configured to **Send NTLMv2 response only\refuse LM & NTLM**.

If you have Windows 9*x* clients, and you can install the DSClient on all such clients, configure this setting to **Send NTLMv2 response only\refuse LM & NTLM** on computers running Windows NT (Widows NT, Windows 2000, and Windows XP Professional) Otherwise, you must leave this setting configured at no higher than **Send NTLMv2 responses only** on computers not running Windows 9*x*.

If you find applications that break when this setting is enabled, roll it back one step at a time to discover what breaks. At a minimum, this setting should be set to **Send LM & NTLM – use NTLMv2 session security if negotiated** on all computers and can typically be set to **Send NTLMv2 responses only** on all computers in the environment.

Network security: LDAP client signing requirements

Table 3.97: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Negotiate signing	Negotiate signing	Negotiate signing	Negotiate signing

The **Network security: LDAP client signing requirements** security option setting determines the level of data signing that is requested on behalf of clients issuing LDAP BIND requests. Unsigned network traffic is susceptible to man–in–the–middle attacks. In the case of an LDAP server, this means that an attacker could cause a server to make decisions based on false queries from the LDAP client. Therefore, the value for this setting is configured to **Negotiate signing** in the three environments defined in this guide.

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

Table 3.98: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No minimum	No minimum	Enabled all settings	Enabled all settings

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** security option setting allows a client to require the negotiation of message confidentiality (encryption), message signing, 128–bit encryption, or NTLM version 2 (NTLMv2) session security. Configure this setting as high as possible while still allowing the applications on the network to function fully to ensure that network traffic from NTLM SSP based servers is protected from man–in–the–middle attacks and data exposure.

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Table 3.99: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
No minimum	No minimum	Enabled all settings	Enabled all settings

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** security option setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128–bit encryption, or NTLMv2 session security. Configure this setting as high as possible while still allowing the applications on the network to function fully to ensure that network traffic from NTLM SSP based clients is protected from man–in–the–middle attacks and data exposure.

Recovery console: Allow automatic administrative logon

Table 3.100: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Recovery console: Allow automatic administrative logon** security option setting determines whether the password for the **Administrator** account must be given before access to the system is granted. If this option is enabled, the Recovery Console does not require you to provide a password, and it automatically logs on to the system. The Recovery Console can be very useful when troubleshooting and repairing systems that cannot be restarted normally. However, enabling this setting can be detrimental because anyone can then walk up to the server, shut it down by disconnecting the power, restart it, select **Recover Console** from the **Restart** menu, and then assume full control of the server. Therefore, this setting is configured to the default for the three environments defined in this guide. To use the Recovery Console when this setting is disabled, the user will have to enter a user name and password to access the Recovery Console account.

Recovery console: Allow floppy copy and access to all drives and all folders

Table 3.101: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Enabled	Enabled	Disabled

Enabling the **Recovery console: Allow floppy copy and access to all drives and all folders** security option setting makes the Recovery Console **SET** command available, which allows you to set the following Recovery Console environment variables:

- **AllowWildCards**: Enables wildcard support for some commands (such as the DEL command)
- **AllowAllPaths**: Allows access to all files and folders on the computer
- **AllowRemovableMedia**: Allows files to be copied to removable media, such as a floppy disk
- **NoCopyPrompt**: Does not prompt when overwriting an existing file

For maximum security, this setting is configured to **Disabled** in the High Security environment.

Shutdown: Allow system to be shut down without having to log on

Table 3.102: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Shutdown: Allow system to be shut down without having to log on** security option setting determines whether a computer can be shut down without having to log on to the Windows operating system. Users who can access the console could shut the system down. An attacker or misguided user could connect to the server via Terminal Services and shut it down or restart it without having to identify him or herself. Therefore, this countermeasure should be set to the default across all three environments.

Shutdown: Clear virtual memory page file

Table 3.103: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Enabled

The **Shutdown: Clear virtual memory page file** security option setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this setting is enabled, it causes the system pagefile to be cleared each time that the system shuts down gracefully. If you enable this security setting, the hibernation file (hiberfil.sys) is also zeroed out when hibernation is disabled on a portable computer system. Shutting down and restarting the server will take longer and will be especially noticeable on servers with large paging files. For these reasons, this setting is configured to **Enabled** in the High Security environment but set to **Disabled** in the Legacy Client and Enterprise Client environments.

Note: An attacker who has physical access to the server could bypass this countermeasure by simply unplugging the server from its power source.

System cryptography: Force strong key protection for user keys stored on the computer

Table 3.104: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Not Defined	User is prompted when the key is first used	User is prompted when the key is first used	User must enter a password each time they use a key

The **System cryptography: Force strong key protection for user keys stored on the computer** security option setting determines whether users' private keys, such as their S-MIME keys, require a password to be used. If this policy is configured so that users must provide a password — distinct from their domain password — every time that they use a key, then even if an attacker takes control of their computer and determines what their logon password is, accessing locally stored user keys will be more difficult. For usability requirements in the Legacy Client and Enterprise Client environments, the value for this setting is configured to the **User is prompted when the key is first used** setting option. To further secure the environment, in the High Security environment this setting value is configured to **User must enter a password each time they use a key**.

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

Table 3.105: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** security option setting determines whether the Transport Layer Security/Secure Sockets Layer (TL/SS) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Enabling this policy ensures that computers in your environment will use the most powerful algorithms available for digital encryption, hashing, and signing. This will minimize the risk of an unauthorized user compromising digitally encrypted or signed data. For these reasons, this setting is configured to **Disabled** in the three environments defined in this guide.

System objects: Default owner for objects created by members of the Administrators group

Table 3.106: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Administrators group	Object creator	Object creator	Object creator

The **System objects: Default owner for objects created by members of the Administrators group** security option setting determines whether the Administrators group or an object creator is the default owner of any system objects that are created. When system objects are created, the ownership will reflect which account created the object rather than the more generic **Administrators** group.

System objects: Require case insensitivity for non – Windows subsystems

Table 3.107: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **System objects: Require case insensitivity for non – Windows subsystems** security option setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32® subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Since Windows is case insensitive (but the POSIX subsystem will support case sensitivity), not enforcing this setting makes it possible for a user of this subsystem to create a file with the same name as another file by using mixed case to label it. Doing this may block another user accessing these files with normal Win32 tools, because only one of the files will be available. To ensure consistency of file names, this setting is set to **Enabled** in the three environments defined in this guide.

System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

Table 3.108: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)** security option setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes. Ensuring that this setting is set to the default strengthens the DACL, allowing users who are not administrators to read shared objects but not to modify any that they did not create. Therefore, this setting is configured to the default **Enabled** in the three environments defined in this guide.

System settings: Optional subsystems

Table 3.109: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
POSIX	None	None	None

The **System settings: Optional subsystems** security option setting determines which subsystems are used to support applications in your environment. The default value for this setting in Windows Server 2003 is **POSIX**. In order to disable the POSIX subsystem, this setting is configured to **None** in the three environments defined in this guide.

Event Log

The event logs records events on the system. The security log records audit events. The event log container of Group Policy is used to define attributes related to the application, security, and system event logs, such as maximum log size, access rights for each log, and retention settings and methods. The settings for the application, security, and system event logs are configured in the MSBP and applied to all member servers in the domain.

The Event Log settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Event Log

This section provides details on the prescribed security options for the three environments defined in this guide for the MSBP. For a summary of the prescribed settings in this section, see the Windows Server 2003 Security Guide Settings Excel spreadsheet. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Maximum application log size

Table 3.110: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
16,384 KB	16,384 KB	16,384 KB	16,384 KB

The **Maximum application log size** security setting specifies the maximum size of the application event log, which has a maximum capacity of 4 gigabytes (GB), although this is not recommended because of the risk of memory fragmentation leading to slow performance and unreliable event logging. Requirements for the application log size vary depending on the function of the platform and the need for historical records of application related events. The default value of 16,384 kilobytes (KB), is enforced in all three environments.

Maximum security log size

Table 3.111: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
16,384 KB	81,920 KB	81,920 KB	81,920 KB

The **Maximum security log size** security setting specifies the maximum size of the security event log, which has a maximum capacity of 4 GB. Configuring the security log to at least 80 MB on domain controllers and stand–alone servers should adequately store enough information to conduct audits. Configuring this log for other systems to an adequate size is based on factors that include how frequently the log will be reviewed, available disk space, and so on.

Maximum system log size

Table 3.112: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
16,384 KB	16,384 KB	16,384 KB	16,384 KB

The **Maximum system log size** security setting specifies the maximum size of the application event log, which has a maximum capacity of 4 GB—although this is not recommended because of the risk of memory fragmentation leading to slow performance and unreliable event logging. Requirements for the application log size vary depending on the function of the platform and the need for historical records of application related events. The default value of 16,384 KB is enforced in all three environments.

Prevent local guests group from accessing application log

Table 3.113: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Prevent local guests group from accessing application log** security setting determines whether guests are prevented from accessing the application event log. By default in Windows Server 2003, guest access is prohibited on all systems. Therefore, this setting has no real effect on default systems. However, this is considered a defense–in–depth setting with no side effects.

Note: This setting does not appear in the Local Computer Policy object.

Prevent local guests group from accessing security log

Table 3.114: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Prevent local guests group from accessing security log** security setting determines whether guests are prevented from accessing the security event log. A user must possess the Manage auditing and security log user right that is not defined in this guidance to access the security log. Therefore, this setting has no real effect on default systems. However, this setting is considered a defense–in–depth setting with no side effects.

Note: This setting does not appear in the Local Computer Policy object.

Prevent local guests group from accessing system log

Table 3.115: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Enabled	Enabled	Enabled	Enabled

The **Prevent local guests group from accessing system log** security setting determines whether guests are prevented from accessing the system event log. By default in Windows Server 2003, guest access is prohibited on all systems. Therefore, this setting has no real effect on default systems. However, this is considered a defense–in–depth setting with no side effects.

Note: This setting does not appear in the Local Computer Policy object.

Retention method for application log

Table 3.116: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
As needed	As needed	As needed	As needed

The **Retention method for application log** security setting determines the "wrapping" method for the application log. It is imperative that the application log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this could result in a loss of historical data.

Retention method for security log

Table 3.117: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
As needed	As needed	As needed	As needed

The **Retention method for security log** security setting determines the "wrapping" method for the security log. It is imperative that the security log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this could result in a loss of historical data.

Retention method for system log

Table 3.118: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
As needed	As needed	As needed	As needed

The **Retention method for system log** security setting determines the "wrapping" method for the system log. It is imperative that the logs are archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this could result in a loss of historical data.

System Services

When Windows Server 2003 is first installed, default system services are created and are configured to run when the system starts. Many of these system services do not need to run in the three environments defined in this guide.

There are additional optional services available with Windows Server 2003, such as Certificate Services, that are not installed during the default installation of Windows Server 2003. The optional services can be added to an existing system by using **Add/Remove Programs** or the Windows Server 2003 Configure Your Server Wizard, or by creating a customized automated installation of Windows Server 2003.

Any service or application is a potential point of attack. Therefore, any unneeded services or executable files are disabled or removed in the target environment. The MSBP only enables the services required for a Windows Server 2003 member server to participate in a Windows Server 2003 domain to provide basic management services. Specific services required for each server role are also enabled. Specific group policies will be described in other chapters of this guide, which will detail the specific steps required to harden each server role.

Specific services required for each server role are enabled on a per server role basis—the specific Group Policies for these server roles as described in the chapters to follow this one. If additional server roles were needed in the environments detailed in this guide, it would have been necessary to enable additional services for them. For example, if Microsoft SQL Server™ was going to be used for storing customer data on the back end of a Web application, then SQL Server would need to be installed. A Group Policy that applies to that new server role in this case would also need to be created that sets the SQL Services service to **Automatic.**

Note: If additional services are enabled, they may in turn have dependencies that require further services. All of the services needed for a specific server role are added in the policy for the server role that it performs in your organization.

The system services settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\System Services\

This section provides details on the prescribed security options for the three environments defined in this guide for the MSBP. For a summary of the prescribed settings in this section, see the Windows Server 2003 Security Guide Settings Excel spreadsheet. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Alerter

Table 3.119: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Alerter	Disabled	Disabled	Disabled	Disabled

The **Alerter** system service notifies selected users and computers of administrative alerts. Use the Alerter service to send alert messages to specified users that are connected on your network. To ensure greater security in the three environments defined in this guide, disable this service. If the service is stopped, programs that use administrative alerts will not receive them.

Note: Disabling this service can break functionality in uninterruptible power supply (UPS) alert messages systems.

Application Layer Gateway Service

Table 3.120: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ALG	Manual	Disabled	Disabled	Disabled

The **Application Layer Gateway Service** system service is a subcomponent of the Internet Connection Sharing (ICS) / Internet Connection Firewall (ICF) service that provides support for independent software vendors (ISVs) to write protocol plug–ins that allow their proprietary network protocols to pass through the firewall and work behind ICS. To ensure greater security in the three environments defined in this guide and to prevent unauthorized computers from acting as Internet gateways, disable this system service.

Application Management

Table 3.121: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
AppMgmt	Manual	Disabled	Disabled	Disabled

The **Application Management** system service provides software installation services, such as Assign, Publish, and Remove. This service processes requests to enumerate, install, and remove programs deployed via a corporate network. When you click **Add/Remove Programs** on a computer joined to a domain, the program calls this service to retrieve the list of your deployed programs. Most corporations do not use this system service on servers; instead, they use automated software delivery applications to distribute software packages. For these reasons, disable this service on the baseline server policy.

ASP .NET State Service

Table 3.122: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
aspnet_state	Not installed	Disabled	Disabled	Disabled

The **ASP .NET State Service** system service provides support for out–of–process session states for ASP.NET. This service is set to **Disabled** in the baseline policy.

Automatic Updates

Table 3.123: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
wuauserv	Automatic	Automatic	Automatic	Automatic

The **Automatic Updates** system service enables the download and installation of critical Windows updates. To ensure greater control over the installation of software updates in the three environments defined in this guide, disable this service. Searching for, downloading, and installing applicable critical fixes will have to be done by going to the Windows Update Web site at http://v4.windowsupdate.microsoft.com/en/default.asp.

Background Intelligent Transfer Service

Table 3.124: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
BITS	Manual —Automatic if BITS jobs are pending	Manual	Manual	Manual

The **Background Intelligent Transfer Service** (BITS) system service is a background file–transfer mechanism and queue manager. BITS is used to transfer files asynchronously between a client and an HTTP server. Requests to the BITS service are submitted and the files are transferred using otherwise idle network bandwidth so that other network related activities, such as browsing, are not affected. This service is configured to **Manual** in the three environments defined in this guide.

Certificate Services

Table 3.125: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
CertSvc	Not installed	Disabled	Disabled	Disabled

The **Certificate Services** system service is part of the core operating system that enables a business to act as its own certification authority (CA) and issue and manage digital certificates. This is a service for a specific server role. Therefore, disable this setting in the baseline server policies for the three environments defined in this guide.

MS Software Shadow Copy Provider

Table 3.165: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SwPrv	Manual	Manual	Manual	Manual

The **MS Software Shadow Copy Provider** system service manages software for file shadow copies taken by the Volume Shadow Copy service. A shadow copy enables you to create a copy of a disk volume (or apparent copy) that represents a consistent read–only point in time, for that volume. This point in time then stays constant and allows an application, like Ntbackup, to copy data from the shadow copy to tape. If this service is disabled, software–based volume shadow copies cannot be managed.

Client Service for Netware

Table 3.126: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NWCWorkstation	Not installed	Disabled	Disabled	Disabled

The **Client Service for Netware** system service provides access to file and print resources on NetWare networks to users interactively logged on to servers on which the service is installed. With Client Service for Netware, you can access file and print resources on Netware Servers that are running Novell Directory Services (NDS) or bindery security (NetWare versions 3.x or 4.x) from your computer. To ensure greater security in the three environments defined in this guide, disable this service.

ClipBook

Table 3.127: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ClipSrv	Disabled	Disabled	Disabled	Disabled

The **ClipBook** system service enables the Clipbook Viewer to create and share “pages” of data that may be viewed by remote computers. This service depends on the Network Dynamic Data Exchange (NetDDE) service to create the actual file shares that other computers can connect to, while the Clipbook application and service allow you to create the pages of data to share.

To ensure greater security in the three environments defined in this guide, disable this service. Any services that explicitly depend on this service will fail to start. Clipbrd.exe can still be used to view the local Clipboard—where data is stored when a user selects text and then clicks **Copy** on the **Edit** menu, or presses CTRL+C.

Cluster Service

Table 3.128: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ClusSvc	Not installed	Disabled	Disabled	Disabled

The **Cluster Service** system service controls server cluster operations and manages the cluster database. A cluster is a collection of independent computers that is as easy to use as a single computer, but it can be very difficult to manage. Managers see it as a single system, and programmers and users see it as a single system. The **Cluster Service** spreads data and computation among the nodes of the cluster. When a node fails, other nodes provide the services and data formerly provided by the missing node. When a node is added or repaired, the **Cluster Service** software migrates some data and computation to that node. To ensure greater security in the three environments defined in this guide, disable this service.

COM+ Event System

Table 3.129: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
COMSysApp	Manual	Manual	Manual	Manual

The **COM+ Event System** service provides automatic distribution of events to subscribing COM components. The **COM+ Events** service extends the COM+ programming model to support late–bound events or method calls between the publisher or subscriber and the event system. Instead of repeatedly polling the server, the event system notifies you as information becomes available. To ensure usability and greater security in the three environments defined in this guide, this service is set to **Manual**.

COM+ System Application

Table 3.130: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
EventSystem	Manual	Disabled	Disabled	**Disabled**

The **COM+ System Application** system service manages the configuration and tracking of components based on COM+. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Computer Browser

Table 3.131: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Browser	Automatic	Automatic	Automatic	Automatic

The **Computer Browser** system service maintains an up–to–date list of computers on your network and supplies the list to programs that request it. The **Computer Browser** service is used by Windows–based computers that need to view network domains and resources. To ensure greater security in the three environments defined in this guide, set this service to **Automatic**.

Cryptographic Services

Table 3.132: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
CryptSvc	Automatic	Automatic	Automatic	Automatic

The **Cyrptographic Services** system service provides key management services for your computer. To ensure greater security in the three environments defined in this guide, this system service is set this service to **Automatic.** If this service is stopped, the management services mentioned above will not function properly.

DHCP Client

Table 3.133: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Dhcp	Automatic	Automatic	Automatic	Automatic

The **DHCP Client** system service manages network configuration by registering and updating IP addresses and updating Dynamic Domain Naming Service (DDNS) entries for your computer with DNS servers. You do not have to manually change the IP settings when a client, such as a roaming user, wanders throughout the network. The client is automatically given a new IP address regardless of the subnet it reconnects to—as long as a DHCP server is accessible from each of those subnets. To ensure greater security in the three environments defined in this guide, configure this setting to **Automatic**. If this service is stopped, your computer will not receive dynamic IP addresses and DNS updates. Also be aware that disabling the DHCP Client will prevent servers from registering in DNS through DDNS.

DHCP Server

Table 3.134: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
DHCPServer	Not installed	Disabled	Disabled	Disabled

The **DHCP Server** system service allocates IP addresses and enables advanced configuration of network settings such as DNS servers and WINS servers to DHCP clients automatically. The **DHCP Server** service is not needed on member servers in the three environments defined in this guide. However, this setting is required and is set to **Automatic** for the DHCP servers in all three environments.

Distributed File System

Table 3.135: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Dfs	Automatic	Disabled	Disabled	Disabled

The **Distributed File System** (DFS) service manages logical volumes distributed across a local or wide area network. DFS is a distributed service that integrates disparate file shares into a single logical namespace. DFS is not needed on member servers in the three environments defined in this guide. However, this setting is required and is set to **Automatic** for the domain controllers in all three environments.

Distributed Link Tracking Client

Table 3.136: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TrkWks	Automatic	Disabled	Disabled	Disabled

The **Distributed Link Tracking Client** system service maintains links between the NTFS files within your computer or across computers in your network domain. The Distributed Link Tracking (DLT) Client service ensures that shortcuts and Object Linking and Embedding (OLE) links continue to work after the target file is renamed or moved. To ensure greater security in the three environments defined in this guide, disable the **Distributed Link Tracking Client** service. If this service is stopped, the links on your computer will not be maintained or tracked.

Distributed Link Tracking Server

Table 3.137: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TrkSvr	Manual	Disabled	Disabled	Disabled

The **Distributed Link Tracking Server** system service stores information so that files moved between volumes can be tracked for each volume in the domain. When enabled, the **Distributed Link Tracking Server** service runs on domain controllers. Therefore, this service is only set to **Automatic** in the domain controller's policy.

Distributed Transaction Coordinator

Table 3.138: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MSDTC	Automatic	Disabled	Disabled	Disabled

The **Distributed Transaction Coordinator** system service is responsible for coordinating transactions that are distributed across multiple computer systems or resource managers, such as databases, message queues, file systems, or other transaction–protected resource managers. This service is configured to **Disabled** in the three environments defined in this guide.

DNS Client

Table 3.139: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Dnscache	Automatic	Automatic	Automatic	Automatic

The **DNS Client** system service resolves and caches DNS names for your computer. The DNS client service must be running on every computer that performs DNS name resolution. Resolving DNS names is essential for locating domain controllers in Active Directory domains. Running the DNS client service is also critical for locating devices identified using DNS name resolution. Therefore, this service setting is configured to **Automatic** in the three environments defined in this guide.

DNS Server

Table 3.140: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
DNS	Not installed	Disabled	Disabled	Disabled

The **DNS Server** system service enables DNS name resolution by answering queries and update requests for DNS names. The presence of a DNS server is crucial for locating devices identified using DNS names and domain controllers in Active Directory. These functions are not needed on the baseline server; they are only required on domain controllers. Therefore, this setting is disabled in the baseline policy for the three environments defined in this guide. This value for this system service is set to **Automatic** only on DNS servers in the three environments.

Error Reporting Service

Table 3.141: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ERSvc	Automatic	Disabled	Disabled	Disabled

The **Error Reporting Service** system service collects, stores, and reports unexpected application closures to Microsoft and authorizes error reporting for services and applications running in non–standard environments. This service provides Microsoft product groups with efficient and effective information to debug driver and application faults. If the Display Error Notification service is enabled, users will still get a message indicating that a problem occurred, but they will not have the option to report this information to Microsoft or a local network error reporting server. For these reasons, this service is disabled in the three environments defined in this guide.

Event Log

Table 3.142: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Eventlog	Automatic	Automatic	Automatic	Automatic

The **Event Log** system service enables event log messages issued by Windows–based programs and components to be viewed in Event Viewer. Event Log reports contain information that can be useful in diagnosing problems. If the **Event Log** is disabled, you will be unable to track events, which will significantly reduce the ability to successfully diagnose system problems. Therefore, this service sets the value of **Automatic** in the three environments defined in this guide.

Fax Service

Table 3.143: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Fax	Not installed	Disabled	Disabled	Disabled

The **Fax Service** system service, a Telephony API (TAPI)–compliant service, provides fax capabilities from your computer. The **Fax Service** allows users to send and receive faxes from their desktop applications by using either a local fax device or a shared network fax device. On a baseline server, this service is disabled, so your computer will not be able to send or receive faxes.

File Replication

Table 3.144: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NtFrs	Manual	Disabled	Disabled	Disabled

The **File Replication Service** (FRS) enables files to be automatically copied and maintained simultaneously on multiple servers. If the **File Replication Service** is disabled, file replication will not occur, and server data will not synchronize. In the case of a domain controller, stopping the FRS service might have a serious impact on the domain controller's ability to function. Therefore, the value for this service is set to **Disabled** in the baseline policy. However, this setting is set to **Automatic** in the domain controller baseline policy for the three environments defined in this guide.

File Server for Macintosh

Table 3.145: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MacFile	Not installed	Disabled	Disabled	Disabled

The **File Server for Macintosh** system service enables Macintosh users to store and access files on a local Windows server computer. This is not a requirement for a standard server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

FTP Publishing Service

Table 3.146: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MSFtpsvc	Not installed	Disabled	Disabled	Disabled

The **FTP Publishing Service** provides connectivity and administration through the IIS snap–in. The **FTP Publishing Service** is not a requirement for a standard server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Help and Support

Table 3.147: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
helpsvc	Automatic	Disabled	Disabled	Disabled

The **Help and Support** system service enables the Help and Support Center to run on your computer. The service supports the Help and Support Center application and enables communication between the client application and the help data. If this system service is disabled, the Help and Support Center will be unavailable. This service is configured to **Disabled** in the three environments defined in this guide.

HTTP SSL

Table 3.148: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
HTTPFilter	Manual	Disabled	Disabled	Disabled

The **HTTP SSL** system service enables IIS to perform SSL functions. HTTP SSL service enables secure electronic transactions; however, in order to reduce the attack surface, it is recommended to configure the service to **Disabled** in the baseline policy. This service should only be set to **Automatic** in the IIS server role policy.

Human Interface Device Access

Table 3.149: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
HidServ	Disabled	Disabled	Disabled	Disabled

The **Human Interface Device Access** system service enables generic input access to Human Interface Devices (HID), which activate and maintain the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices. These features are not needed in the baseline server environment. For this reason, set the value for this service to **Disabled.**

IAS Jet Database Access

Table 3.150: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
IASJet	Not installed	Disabled	Disabled	Disabled

The **IAS Jet Database Access** system service is only available on 64-bit versions of Windows Server 2003. The service uses the Remote Authentication Dial–in User Service (RADIUS) protocol to provide authentication, authorization, and accounting services. This service is configured to **Disabled.**

IIS Admin Service

Table 3.151: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
IISADMIN	Not installed	Disabled	Disabled	Disabled

The **IIS Admin Service** allows administration of IIS components such as FTP, Applications Pools, Web sites, Web service extensions, and both Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) virtual servers. If this service is disabled, you cannot run Web, FTP, NNTP, or SMTP sites. For this reason, set this service to **Automatic** in the IIS server policy. These features are not needed in the baseline server environment. Therefore, this service is configured to **Disabled**. However, this service is set to **Automatic** in the IIS role policy.

IMAPI CD–Burning COM Service

Table 3.152: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ImapiService	Disabled	Disabled	Disabled	Disabled

The **IMAPI CD – Burning COM Service** manages CD burning through the Image Mastering Applications Programming Interface (IMAPI) COM interface and performs CD–R writes when requested by the user through Windows Explorer, Windows Media™ Player, (WMP) or third–party applications that use this API. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.**

Indexing Service

Table 3.153: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
cisvc	Disabled	Disabled	Disabled	Disabled

The **Indexing Service** indexes contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. The **Indexing Service** also enables quick searching of documents on local and remote computers and a search index for content shared on the Web. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.**

Infrared Monitor

Table 3.154: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Irmon	Not installed	Disabled	Disabled	Disabled

The **Infrared Monitor** system service enables file and image sharing using infrared. This service is installed by default only if an infrared device is detected during operating system installation of Windows Server 2003. This service is not available on Windows Server 2003 Web, Enterprise, or Datacenter Server.

If this service is disabled, files and images cannot be shared using infrared. These features are not needed in the baseline server environment. Therefore, this service is configured to **Disabled.**

Internet Authentication Service

Table 3.155: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
IAS	Not installed	Disabled	Disabled	Disabled

The **Internet Authentication Service** (IAS) centrally manages network access authentication, authorization, auditing, and accounting. IAS is for virtual private network (VPN), dial−up, 802.1X wireless or Ethernet switch connection attempts sent by access servers that are compatible with the IETF RADIUS protocol. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.**

Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)

Table 3.156: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SharedAccess	Disabled	Disabled	Disabled	Disabled

The **Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)** system service provides network address translation (NAT), addressing and name resolution, and intrusion prevention services for all computers in your home or small−office network through a dial−up or broadband connection. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.**

Intersite Messaging

Table 3.157: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
IsmServ	Disabled (Started for a domain controller)	Disabled	Disabled	Disabled

The **Intersite Messaging** system service enables messages to be exchanged between computers running Windows Server sites. This service is used for mail–based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.** This service is, however, required on domain controllers. For this reason, the **Intersite Messaging** service is set to **Automatic** on the domain controllers in the three environments defined in this guide.

IP Version 6 Helper Service

Table 3.158: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
6to4	Not installed	Disabled	Disabled	Disabled

The **IP Version 6 Helper Service** system service offers IPv6 connectivity over an existing IPv4 network. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled.**

IPSEC Policy Agent (IPSec Service)

Table 3.159: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
PolicyAgent	Automatic	Automatic	Automatic	Automatic

The **IPSEC Policy Agent** service provides end-to-end security between clients and servers on TCP/IP networks. It also manages IP security (IPSec) policy, starts the Internet Key Exchange (IKE), and coordinates IPSec policy settings with the IP security driver. This service is enabled in the three environments defined in this guide.

Kerberos Key Distribution Center

Table 3.160: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Kdc	Disabled	Disabled	Disabled	Disabled

The **Kerberos Key Distribution Center** system service enables users to log on to the network by using the Kerberos v5 authentication protocol. For these reasons, set the value for this service to **Automatic** in the domain controllers' policy.

License Logging Service

Table 3.161: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
LicenseService	Disabled	Disabled	Disabled	Disabled

The **License Logging Service** monitors and records client access licensing for portions of the operating system. These include IIS, Terminal Server, and File/Print, as well as products that are not a part of the operating system, such as SQL Server and Microsoft Exchange Server. This service is configured to **Disabled** in the three environments defined in this guide.

Logical Disk Manager

Table 3.162: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
dmserver	Automatic	Manual	Manual	Manual

The **Logical Disk Manager** system service detects and monitors new hard disk drives and sends disk volume information to Logical Disk Manager Administrative Service for configuration. This service watches Plug and Play events for new drives that are detected and passes volume and disk information to the Logical Disk Manager Administrative Service to be configured. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

Logical Disk Manager Administrative Service

Table 3.163: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
dmadmin	Manual	Manual	Manual	Manual

The **Logical Disk Manager Administrative Service** performs administrative service for disk management requests and configures hard disk drives and volumes. The **Logical Disk Manager Administrative Service** is started only when you configure a drive or partition or a new drive is detected. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

Message Queuing

Table 3.164: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
msmq	Not installed	Disabled	Disabled	Disabled

The **Message Queuing** system service is a messaging infrastructure and development tool for creating distributed messaging applications for Windows. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Message Queuing Down Level Clients

Table 3.165: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
mqds	Not installed	Disabled	Disabled	Disabled

The **Message Queuing Down Level Clients** system service provides Active Directory access for Message Queuing clients (Windows 9*x*, Windows NT 4.0, and Windows 2000) on domain controllers. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Message Queuing Triggers

Table 3.166: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Mqtgsvc	Not installed	Disabled	Disabled	Disabled

The **Message Queuing Triggers** system service provides rule–based monitoring of messages arriving in a Message Queuing queue and, when the conditions of a rule are satisfied, invokes a COM component or a stand–alone executable program to process the message. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Messenger

Table 3.167: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Messenger	Disabled	Disabled	Disabled	Disabled

The **Messenger** system service transmits and sends Alerter service messages between clients and servers. This service is not related to Windows Messenger. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Microsoft POP3 Service

Table 3.168: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
POP3SVC	Not installed	Disabled	Disabled	Disabled

The **Microsoft POP3 Service** provides e–mail transfer and retrieval services. Administrators can use the POP3 service to store and manage e–mail accounts on the mail server. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

MSSQL$UDDI

Table 3.170: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MSSQL$UDDI	Not installed	Disabled	Disabled	Disabled

The **MSSQL$UDDI** system service—Universal Description Discovery and Integration (UDDI)—is an industry specification for publishing and locating information about Web services. The Windows Server 2003 family includes UDDI Services, a Web service that provides UDDI capabilities for use within an enterprise or across organizations. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

MSSQLServerADHelper

Table 3.171: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MSSQLServerADHelper	Not installed	Disabled	Disabled	Disabled

The **MSSQLServerADHelper** system service enables SQL Server and SQL Server Analysis Services to publish information in Active Directory when the services are not running under the LocalSystem account. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

.NET Framework Support Service

Table 3.172: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
CORRTSvc	Not installed	Disabled	Disabled	Disabled

The **.NET Framework Support Service** system service notifies a subscribing client when a specified process is initializing the Client Runtime Service. The **.NET Framework Support Service** provides a run−time environment called the Common Language Runtime, which manages the execution of code and provides services that make the development process easier. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Netlogon

Table 3.173: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Netlogon	Automatic	Automatic	Automatic	Automatic

The **Netlogon** system service maintains a secure channel between your computer and the domain controller for authenticating users and services. If this service is disabled, computers on the system network may not authenticate users and services, and the domain controller will not register DNS records. Specifically, disabling this service could deny NTLM authentication requests, and, in case of domain controllers, they will not be discoverable by client computers. For these reasons, set the value for this service to **Automatic**.

NetMeeting Remote Desktop Sharing

Table 3.174: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
mnmsrvc	Disabled	Disabled	Disabled	Disabled

The **NetMeeting Remote Desktop Sharing** system service enables an authorized user to access this computer remotely by using Microsoft NetMeeting® over a corporate intranet. The service must be explicitly enabled by NetMeeting and can be disabled in NetMeeting or shut down via a Windows tray icon. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Network Connections

Table 3.175: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Netman	Manual	Manual	Manual	Manual

The **Network Connections** service manages objects in the Network Connections folder, in which you can view both network and remote connections. This service will start automatically when the start up type is **Manual** and the Network Connections interface is invoked. This service is configured to **Manual** in the three environments defined in this guide.

Network DDE

Table 3.176: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NetDDE	Disabled	Disabled	Disabled	Disabled

The **Network DDE** system service provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Network DDE DSDM

Table 3.177: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NetDDEdsdm	Disabled	Disabled	Disabled	Disabled

The **Network DDE DSDM** system service manages DDE network shares. This service is used only by the Network DDE service to manage shared DDE conversations. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Network Location Awareness (NLA)

Table 3.178: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NLA	Manual	Manual	Manual	Manual

The **Network Location Awareness (NLA)** system service collects and stores network configuration information such as IP address and domain name changes, as well as location change information, and then notifies programs when this information changes. Disabling this service prevents it from locating networks, and any services that explicitly depend on it will fail to start. These features may be needed in the baseline server environment. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

Network News Transport Protocol (NNTP)

Table 3.179: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NntpSvc	Not installed	Disabled	Disabled	Disabled

The **Network News Transport Protocol (NNTP)** system service allows computers running Windows Server 2003 to act as a news server. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

NTLM Security Support Provider

Table 3.180: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NtLmSsp	Not installed	Automatic	Automatic	Automatic

The **NTLM Security Support Provider** system service provides security to RPC programs that use transports other than named pipes and enables users to log on to the network using the NTLM authentication protocol. The NTLM protocol authenticates clients that do not use Kerberos v5 authentication. If this service is disabled, users cannot log on to clients by using the NTLM authentication protocol or access network resources. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

Performance Logs and Alerts

Table 3.181: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SysmonLog	Manual	Manual	Manual	Manual

The **Performance Logs and Alerts** system service collects performance data from local or remote computers based on preconfigured schedule parameters; it then writes the data to a log or triggers an alert. These features are needed in the baseline server environment. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

Plug and Play

Table 3.182: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
PlugPlay	Automatic	Automatic	Automatic	Automatic

The **Plug and Play** system service enables a computer to recognize and adapt to hardware changes with little or no user input. If this service is stopped by using the MSCONFIG troubleshooting tool, the Device Manager interface will appear blank, and no hardware devices will be displayed. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

Portable Media Serial Number

Table 3.183: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WmdmPmSN	Manual	Disabled	Disabled	Disabled

The **Portable Media Serial Number** system service retrieves the serial number of any portable music player connected to your computer. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Print Server for Macintosh

Table 3.184: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MacPrint	Not installed	Disabled	Disabled	Disabled

The **Print Server for Macintosh** system service enables Macintosh clients to route printing to a print spooler located on a computer running Windows Server 2003 Enterprise Server. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Print Spooler

Table 3.185: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Spooler	Automatic	Disabled	Disabled	Disabled

The **Print Spooler** system service manages all local and network print queues and controls all print jobs. These features are not required in the baseline server environment. Therefore, this service is configured to. However, this service is set to **Automatic** for the Print server role. For more information on this server role, see Chapter 7, "Hardening Print Servers."

Protected Storage

Table 3.186: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ProtectedStorage	Automatic	Automatic	Automatic	Automatic

The **Protected Storage** system service protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. If this service is disabled, private keys will be inaccessible, certificate server will not operate, S/MIME and SSL will not work, and smart card logon will fail. For these reasons, set the value for this service to **Automatic**.

Remote Access Auto Connection Manager

Table 3.187: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RasAuto	Manual	Disabled	Disabled	Disabled

The **Remote Access Auto Connection Manager** system service detects unsuccessful attempts to connect to a remote network or computer and then provides alternative methods for connection. The **Remote Access Auto Connection Manager** service offers to establish a dial–up or virtual private network (VPN) connection to a remote network whenever a program fails in an attempt to reference a remote DNS or NetBIOS name or address. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Access Connection Manager

Table 3.188: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RasMan	Manual	Disabled	Disabled	Disabled

The **Remote Access Connection Manager** system service manages dial–up and VPN connections from your computer to the Internet or other remote networks. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Administration Service

Table 3.189: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SrvcSurg	Not installed	Manual	Manual	Manual

The **Remote Administration Service** system service is responsible for running the following Remote Administration tasks when the server restarts:

- Increments the server boot count
- Raises an alert if the date and time has not been set on the server
- Raises an alert if the event e-mail notification functionality has not been configured

This service is configured to **Manual** in the three environments defined in this guide.

Remote Desktop Help Session Manager

Table 3.190: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RDSessMgr	Manual	Disabled	Disabled	Disabled

The **Remote Desktop Help Session Manager** system service manages and controls the Remote Assistance feature in the Help and Support Center application (helpctr.exe). This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Installation

Table 3.191: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
BINLSVC	Not installed	Disabled	Disabled	Disabled

The **Remote Installation Services** (RIS) system service is a Windows deployment feature included in members of the Windows Server family. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Procedure Call (RPC)

Table 3.192: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RpcSs	Automatic	Automatic	Automatic	Automatic

The **Remote Procedure Call (RPC)** system service is a secure inter-process communication (IPC) mechanism that enables data exchange and invocation of functionality residing in a different process. Different processes can take place on the same computer, the local area network (LAN), or across the Internet. This service should not be disabled. Disabling the **Remote Procedure Call (RPC)** service will result in the operating system not loading numerous services that are dependent on it. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

Remote Procedure Call (RPC) Locator

Table 3.193: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RpcLocator	Manual (Automatic on a domain controller)	Disabled	Disabled	Disabled

The **Remote Procedure Call (RPC) Locator** system service enables RPC clients using the RpcNs* family of APIs to locate RPC servers and manages the RPC name service database. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled**. However, this system service is required for domain controllers and is set to **Automatic**.

Remote Registry Service

Table 3.194: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RemoteRegistry	Automatic	Automatic	Automatic	Automatic

The **Remote Registry Service** system service enables remote users to modify registry settings on your computer—provided remote users have the required permissions. The service is primarily used by remote administrators and performance counters. If **Remote Registry Service** is disabled, modifying the registry will only be allowed on the local computer, and any services that explicitly depend on this service will fail to start. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

Remote Server Manager

Table 3.195: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
AppMgr	Not installed	Disabled	Disabled	Disabled

The **Remote Server Manager** acts as a Windows Management Instrumentation (WMI) instance provider for Remote Administration Alert Objects and a WMI method provider for Remote Administration Tasks. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Server Monitor

Table 3.196: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Appmon	Not installed	Disabled	Disabled	Disabled

The **Remote Server Monitor** system service provides monitoring of critical system resources and manages optional watchdog timer hardware on remotely managed servers. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Storage Notification

Table 3.197: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Remote_Storage _User_Link	Not installed	Disabled	Disabled	Disabled

The **Remote Storage Notification** system service notifies you when you read or write to files that are only available from a secondary storage media. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Remote Storage Server

Table 3.198: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Remote_Storage _Server	Not installed	Disabled	Disabled	Disabled

The **Remote Storage Server** system service stores infrequently used files in secondary storage media. This service allows Remote Storage Notification to notify the user when an offline file has been accessed. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Removable Storage

Table 3.199: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NtmsSvc	Manual	Disabled	Disabled	Disabled

The **Removable Storage** system service manages and catalogs removable media and operates automated removable media devices. This service maintains a catalog of identifying information for removable media used by your computer, including tapes and CDs. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Important: This service is required for system backups using Ntbackup.exe—if you are using Ntbackup.exe, set this service to **Manual**.

Resultant Set of Policy Provider

Table 3.200: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RSoPProv	Manual	Disabled	Disabled	Disabled

The **Resultant Set of Policy Provider** system service enables you to connect to a Windows Server 2003 domain controller, access the WMI database for that computer, and simulate Resultant Set of Policy (RSoP) for Group Policy settings that would be applied to a user or computer located in Active Directory on a Windows 2000 or later domain. This is commonly referred to as planning mode. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Routing and Remote Access

Table 3.201: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
RemoteAccess	Disabled	Disabled	Disabled	Disabled

The **Routing and Remote Access** system service provides multi–protocol LAN–to–LAN, LAN–to–WAN, VPN, and NAT routing services. In addition, this service also provides dial–up and VPN remote access services. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

SAP Agent

Table 3.202: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
nwsapagent	Not installed	Disabled	Disabled	Disabled

The **SAP Agent** system service advertises network services on an IPX network by using the IPX Service Advertising Protocol (IPX SAP) protocol. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Secondary Logon

Table 3.203: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
seclogon	Automatic	Disabled	Disabled	Disabled

The **Secondary Logon** system service allows the user to create processes in the context of different security principals. Restricted users commonly use this service to log on as a user with elevated privileges for temporarily running administrative programs. This service enables users to start processes under alternate credentials. These features are not required in the baseline server environment. While this service is beneficial on client computers, it is not appropriate on most servers because users logging onto them interactively will be members of the IT team performing some sort of maintenance tasks that typically require administrative privileges. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Security Accounts Manager

Table 3.204: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SamSs	Automatic	Automatic	Automatic	Automatic

The **Security Accounts Manager** (SAM) system service is a protected subsystem that manages user and group account information. In Windows 2000 and the Windows Server 2003 family, the SAM in the local computer registry stores workstation security accounts and domain controller accounts are stored in Active Directory. This service should not be disabled.

Server

Table 3.205: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
lanmanserver	Automatic	Automatic	Automatic	Automatic

The **Server** system service provides RPC support, file, print, and named pipe sharing over the network. For these reasons, it is recommended to set the value for this service to **Automatic** in the three environments defined in this guide.

Shell Hardware Detection

Table 3.206: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
ShellHWDetection	Automatic	Disabled	Disabled	Disabled

The **Shell Hardware Detection** system service monitors and provides notification for AutoPlay hardware events. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Simple Mail Transport Protocol (SMTP)

Table 3.207: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SMTPSVC	Not installed	Disabled	Disabled	Disabled

The **Simple Mail Transport Protocol (SMTP)** system service transports electronic mail across the network. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Simple TCP/IP Services

Table 3.208: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SimpTcp	Not installed	Disabled	Disabled	Disabled

The **Simple TCP/IP Services** system service supports the following TCP/IP protocols:

- Echo (port 7, RFC 862)
- Discard (port 9, RFC 863)
- Character Generator (port 19, RFC 864)
- Daytime (port 13, RFC 867)
- Quote of the Day (port 17, RFC 865)

These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Single Instance Storage Groveler

Table 3.209: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Groveler	Not installed	Disabled	Disabled	Disabled

The **Single Instance Storage Groveler** (SIS) system service is an integral component of the Remote Installation Service (RIS) that reduces the overall storage required on the RIS volume. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Smart Card

Table 3.210: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SCardSvr	Manual	Disabled	Disabled	Disabled

The **Smart Card** system service manages and controls access to a smart card inserted into a smart card reader attached to your computer. If this service is disabled, computers in your environment will be unable to read smart cards. Also, any services that explicitly depend on it will fail to start. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Note: A form of authentication in which the principal wanting to be authenticated verifies its identity by demonstrating two factors of identification. Often this involves showing something that you know with something that you have, for example, inserting a smart card into a computer and entering the PIN for that card. A third factor commonly used for proving one's identity is by demonstrating something you are; an example of a two-factor authentication including this type would be requiring users to submit to a retina scanner followed by entering their passwords before granting them access to restricted resources. Using smart cards to implement multifactor authentication is a best practice and is employed for all administrator accounts. If your organization utilizes smart card authentication, this service needs to be set to **Manual**.

SNMP Service

Table 3.211: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SNMP	Not installed.	Disabled	Disabled	Disabled

The **SNMP Service** allows incoming SNMP requests to be serviced by the local computer. The **SNMP Service** includes agents that monitor activity in network devices and report to the network console workstation. There are no requirements or dependencies in the three environments for the **SNMP Server**. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

SNMP Trap Service

Table 3.212: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SNMPTRAP	Not installed	Disabled	Disabled	Disabled

The **SNMP Trap Service** receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on your computer. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Special Administration Console Helper

Table 3.213: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Sacsvr	Manual	Disabled	Disabled	Disabled

The **Special Administration Console Helper** system service (SAC) performs remote management tasks if any of the Windows Server 2003 family of operating systems stops functioning due to a Stop error message. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

SQLAgent$* (*UDDI or WebDB)

Table 3.214: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SQLAgent$WEBDB	Not installed	Disabled	Disabled	Disabled

SQLAgent$* (* UDDI or WebDB) is a job scheduler and monitoring service. It also moves information between computers running SQL Server and is used heavily for backups and replication. If the **SQLAgent$* (* UDDI or WebDB)** service is stopped, SQL replication will not occur. In addition, there will be a disruption of all scheduled jobs and alert/event monitoring and auto restart of the SQL Server service. If this service is disabled, any services that explicitly depend on this service will fail to start. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

System Event Notification

Table 3.215: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
SENS	Automatic	Automatic	Automatic	Automatic

The **System Event Notification** system service monitors and tracks system events such as Windows logon network and power events and then notifies COM+ Event System subscribers of these events. This service is configured to **Automatic** in the three environments defined in this guide.

Task Scheduler

Table 3.216: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Schedule	Automatic	Disabled	Disabled	Disabled

The **Task Scheduler** system service enables you to configure and schedule automated tasks on your computer. The Task Scheduler service monitors whatever criteria you choose and carries out the task when the criteria have been met. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Important: This service must be set to **Automatic** if you are using Ntbackup.exe for scheduled backups.

TCP/IP NetBIOS Helper Service

Table 3.217: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
LMHosts	Automatic	Automatic	Automatic	Automatic

The **TCP/IP NetBIOS Helper Service** system service provides support for NetBIOS over the TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network, thus enabling users to share files, print, and log on to the network. This service is configured to **Automatic** in the three environments defined in this guide.

TCP/IP Print Server

Table 3.218: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
LPDSVC	Not installed	Disabled	Disabled	Disabled

The **TCP/IP Print Server** system service enables TCP/IP–based printing using the Line Printer Daemon protocol. This feature is not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Telephony

Table 3.219: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TapiSrv	Manual	Disabled	Disabled	Disabled

The **Telephony** service provides API (TAPI) support for programs that control telephony devices, as well as IP-based voice connections on the local computer and through the LANs on servers also running the service. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Telnet

Table 3.220: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TIntSvr	Disabled	Disabled	Disabled	Disabled

The **Telnet** system service for Windows provides ASCII terminal sessions to Telnet clients. This service supports two types of authentication and four types of terminals: ANSI, VT–100, VT–52, and VTNT. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Terminal Services

Table 3.221: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TermService	Manual	Automatic	Automatic	Automatic

The **Terminal Services** system service provides a multi–session environment that allows client devices to access a virtual Windows desktop session and Windows–based programs running on the server. **Terminal Services** allows multiple users to be connected interactively to a computer and to display desktops and applications on remote computers. By default, the **Terminal Services** system service is installed in remote Administration mode. To install **Terminal Services** in Application Mode, use **Configure Your Server** or **Add/Remove Windows Components** to change the **Terminal Services** mode. Because this service is such a powerful tool for remote administration of servers, it is configured to **Automatic** in the three environments defined in this guide.

Note: To prevent remote use of computers in your environment, clear the **Allow Remote Assistance** and **Allow Remote Desktop** check boxes on the **Remote** tab of the **System properties** dialog box.

Terminal Services Licensing

Table 3.222: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
TermServLicensing	Not installed.	Disabled	Disabled	Disabled

The **Terminal Services Licensing** system service installs a licensed server and provides registered client licenses when connecting to a Terminal Server. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Terminal Services Session Directory

Table 3.223: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Tssdis	Disabled	Disabled	Disabled	Disabled

The **Terminal Services Session Directory** system service provides a multi−session environment that allows client devices to access a virtual Windows desktop session and Windows−based programs running on Windows Server 2003. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Themes

Table 3.224: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Themes	Disabled	Disabled	Disabled	Disabled

The **Themes** system service provides user experience theme management services. The **Themes** service provides rendering support for the new Windows XP Professional graphic user interface (GUI). This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Trivial FTP Daemon

Table 3.225: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
tftpd	Not installed	Disabled	Disabled	Disabled

The **Trivial FTP Daemon** (TFTP) system service does not require a user name or password and is an integral part of RIS. The **Trivial FTP Daemon** service implements support for the TFTP protocol defined by the following RFCs:

- RFC 1350 - TFTP
- RFC 2347 - Option extension
- RFC 2348 - Block size option
- RFC 2349 - Timeout interval and transfer size options

Client computers requesting RIS from this server will fail to install if this service is disabled. However, this feature is not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Uninterruptible Power Supply

Table 3.226: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
UPS	Manual	Disabled	Disabled	Disabled

The **Uninterruptible Power Supply** system service manages an uninterruptible power supply (UPS) connected to your computer by a serial port. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Upload Manager

Table 3.227: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Uploadmgr	Manual	Disabled	Disabled	Disabled

The **Upload Manager** system service manages the synchronous and asynchronous file transfers between clients and servers on the network. Driver data is anonymously uploaded from customer computers to Microsoft and then used to help users find the drivers required for their systems. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Virtual Disk Service

Table 3.228: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
VDS	Manual	Disabled	Disabled	Disabled

The **Virtual Disk Service** (VDS) system service provides a single interface for managing block storage virtualization whether done in operating system software, redundant array of independent disks (RAID) storage hardware subsystems, or other virtualization engines. These features are not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Volume Shadow Copy

Table 3.229: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
VSS	Manual	Manual	Manual	Manual

The **Volume Shadow Copy** system service manages and implements Volume Shadow copies used for backup and other purposes. This service is a core requirement for the baseline server policy. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

WebClient

Table 3.230: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WebClient	Disabled	Disabled	Disabled	Disabled

The **WebClient** system service allows Win32 applications to access documents on the Internet. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Web Element Manager

Table 3.231: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
elementmgr	Not installed	Disabled	Disabled	Disabled

The **Web Element Manager** system service is responsible for serving Web user interface elements for the Administration Web site at port 8098. This feature is not needed in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Windows Audio

Table 3.232: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
AudioSrv	Disabled	Disabled	Disabled	Disabled

The **Windows Audio** system service provides support for sound and related Windows Audio event functions. This feature is not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Windows Image Acquisition (WIA)

Table 3.233: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
StiSvc	Disabled	Disabled	Disabled	Disabled

The **Windows Image Acquisition (WIA)** system service provides image acquisition services for scanners and cameras. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Windows Installer

Table 3.234: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
MSIServer	Manual	Automatic	Automatic	Automatic

The **Windows Installer** system service manages the installation and removal of applications by applying a set of centrally–defined setup rules during the installation process. This service is required in the baseline server environment; therefore, it is configured to **Automatic** in the three environments defined in this guide.

Windows Internet Name Service (WINS)

Table 3.235: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WINS	Not installed	Disabled	Disabled	Disabled

The **Windows Internet Name Service (WINS)** system service enables NetBIOS name resolution. Presence of the WINS server(s) is crucial for locating the network resources identified by using NetBIOS names. WINS servers are required unless all domains have been upgraded to Active Directory and all computers on the network are running Windows Server 2003. These features are not required in the baseline server environment. Therefore, it is recommended to set the value for this service to **Disabled**. This service also is set to **Automatic** in the Infrastructure Server role policy.

Windows Management Instrumentation

Table 3.236: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
winmgmt	Automatic	Automatic	Automatic	Automatic

The **Windows Management Instrumentation** system service provides a common interface and object model to access management information about operating systems, devices, applications, and services. WMI is an infrastructure for building management applications and instrumentation shipped as part of the current generation of Microsoft operating systems. If this service is disabled, most Windows–based software will not function properly, and any services that explicitly depend on it will fail to start. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

Windows Management Instrumentation Driver Extensions

Table 3.237: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Wmi	Manual	Manual	Manual	Manual

The **Windows Management Instrumentation Driver Extensions** system service monitors all drivers and event trace providers that are configured to publish WMI or event trace information. This service is configured to **Manual** in the three environments defined in this guide.

Windows Media Services

Table 3.238: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WMServer	Not installed	Disabled	Disabled	Disabled

The **Windows Media Services** system service provides streaming media services over IP–based networks. This service replaces the four separate services that comprised Windows Media Services versions 4.0 and 4.1: Windows Media Monitor Service, Windows Media Program Service, Windows Media Station Service, and Windows Media Unicast Service. This service is not needed in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Windows System Resource Manager

Table 3.239: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WindowsSystemResourceManager	Not installed	Disabled	Disabled	Disabled

The **Windows System Resource Manager** (WSRM) system service is a tool to help customers deploy applications into consolidation scenarios. This feature is not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Windows Time

Table 3.240: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
W32Time	Automatic	Automatic	Automatic	Automatic

The **Windows Time** system service maintains date and time synchronization on all computers running on a Windows network. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or timestamp, can be assigned to network validation and resource access requests. It is a core requirement for reliable Kerberos authentication in Active Directory domains Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

WinHTTP Web Proxy Auto–Discovery Service

Table 3.241: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WinHttpAutoProxySvc	Manual	Disabled	Disabled	Disabled

The **WinHTTP Web Proxy Auto – Discovery Service** system service implements the Web Proxy Auto–Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol to enable an HTTP client to automatically discover a proxy configuration. This feature is not required in the baseline server environment. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Wireless Configuration

Table 3.242: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WZCSVC	Automatic on Standard, Enterprise, and Datacenter Server. Manual on Web Server	Disabled	Disabled	Disabled

The **Wireless Zero Configuration** system service enables automatic configuration for IEEE 802.11 wireless adapters for wireless communications. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

WMI Performance Adapter

Table 3.243: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WmiApSrv	Manual	Manual	Manual	Manual

The **WMI Performance Adapter** system service provides performance library information from WMI HiPerf providers. The service is a manual service and is not running by default. It runs on demand when a performance client (for example, Sysmon) uses Performance Data Helper (PDH) to query performance data. Once the client disconnects, the service stops. If this service is disabled, WMI performance counters will be unavailable. Therefore, this service is configured to **Manual** in the three environments defined in this guide.

Workstation

Table 3.244: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
lanmanworkstation	Automatic	Automatic	Automatic	Automatic

The **Workstation** system resource creates and maintains client network connections and communications. If this service is disabled, you cannot establish connections to remote servers and access files through named pipes. Therefore, this service is configured to **Automatic** in the three environments defined in this guide.

World Wide Web Publishing Service

Table 3.245: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
W3SVC	Not installed	Disabled	Disabled	Disabled

The **World Wide Web Publishing Service** system service provides Web connectivity and administration through the Internet Information Service snap–in. This service is not a requirement for the baseline server policy. Therefore, this service is configured to **Disabled** in the three environments defined in this guide.

Additional Registry Settings

Additional registry value entries were created for the baseline security template files that are not defined within the Administrative Template (.adm) file for the three security environments defined in this guide. The .adm file defines the system policies and restrictions for the desktop, shell, and security for Windows Server 2003.

These settings are embedded within the security templates, in the Security Options section, to automate the changes. If the policy is removed, these settings are not automatically removed with it and must be manually changed by using a registry editing tool such as Regedt32.exe. The same registry values are applied across all three environments.

This guide includes additional settings added to the Security Configuration Editor (SCE) by modifying the sceregvl.inf file, located in the %windir%\inf folder, and re–registering scecli.dll. The original security settings, as well as the additional ones, appear under Local Policies\Security in the snap–ins and tools listed previously in this chapter. You should update the sceregvl.inf file and re–register scecli.dll on any computers where you will be editing the security templates and Group Policies provided with this guide, as described in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

This section is only a summary of the additional registry settings that were covered in full in the companion guide. For information on the default settings and a detailed explanation of each of the settings discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Security Consideration for Network Attacks

Table 3.246: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
EnableICMPRedirect	DWORD	0	0	0
SynAttackProtect	DWORD	1	1	1
EnableDeadGWDetect	DWORD	0	0	0
EnablePMTUDiscovery	DWORD	0	0	0
KeepAliveTime	DWORD	300,000	300,000	300,000
DisableIPSourceRouting	DWORD	2	2	2
TcpMaxConnectResponseRetransmissions	DWORD	2	2	2
TcpMaxDataRetransmissions	DWORD	3	3	3
PerformRouterDiscovery	DWORD	0	0	0
TCPMaxPortsExhausted	DWORD	5	5	5

Denial of service (DoS) attacks are network attacks that are aimed at making a computer or a particular service on a computer unavailable to network users. DoS attacks can be difficult to defend against. To help prevent these attacks, you should keep your computer updated with the latest security fixes and harden the TCP/IP protocol stack on your computers running Windows Server 2003 that are exposed to potential attackers. The default TCP/IP stack configuration is tuned to handle standard intranet traffic. If you connect a computer directly to the Internet, Microsoft recommends that you harden the TCP/IP stack against DoS attacks.

The following registry value entries have been added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters** registry key.

AFD.SYS Settings

Table 3.247 Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
DynamicBacklogGrowthDelta	DWORD	10	10	10
EnableDynamicBacklog	DWORD	1	1	1
MinimumDynamicBacklog	DWORD	20	20	20
MaximumDynamicBacklog	DWORD	20000	20000	20000

Windows Sockets applications such as FTP servers and Web servers have their connection attempts handled by Afd.sys. Afd.sys has been modified to support large numbers of connections in the half−open state without denying access to legitimate clients. This is accomplished by allowing the administrator to configure a dynamic backlog. The version of Afd.sys included with Windows Server 2003 supports four registry parameters that can be used to control the dynamic backlog behavior.

The following registry value entries have been added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters** registry key:

Configure NetBIOS Name Release Security: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

Table 3.248 Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
NoNameReleaseOnDemand	DWORD	1	1	1

This entry appears as "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" in the SCE. NetBIOS over TCP/IP is a networking protocol that among other things provides a means of easily resolving NetBIOS names registered on Windows–based systems to the IP addresses configured on those systems. This value determines whether the computer releases its NetBIOS name when it receives a name–release request.

The following registry value entry was added to the template file to the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters** registry key.

Disable Auto Generation of 8.3 File Names: Enable the computer to stop generating 8.3 style filenames

Table 3.249: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
NtfsDisable8dot3NameCreation	DWORD	1	1	1

This entry appears as "MSS: Enable the computer to stop generating 8.3 style filenames" in the SCE. Windows Server 2003 supports 8.3 file name formats for backward compatibility with16–bit applications. The 8.3 file name convention is a naming format that allows file names up to eight characters long.

The following registry value entry has been added to the template file in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem** registry key:

Disable Autorun: Disable Autorun for all drives

Table 3.250: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
NoDriveTypeAutoRun	DWORD	0xFF	0xFF	0xFF

This entry appears as "MSS: Disable Autorun for all drives" in the SCE. Autorun begins reading from a drive on your computer as soon as media is inserted into it. As a result, the setup file of programs and the sound on audio media starts immediately.

The following registry value entry has been added to the template file in the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer** registry key.

Make Screensaver Password Protection Immediate: The time in seconds before the screen saver grace period expires (0 recommended)

Table 3.251: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
ScreenSaverGracePeriod	String	0	0	0

This entry appears as "MSS: The time in seconds before the screen saver grace period expires (0 recommended)" in the SCE. Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled.

The following registry value entries have been added to the template file the **HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon** registry key.

Security Log Near Capacity Warning: Percentage threshold for the security event log at which the system will generate a warning

Table 3.252: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
WarningLevel	DWORD	90	90	90

This entry appears as "MSS: Percentage threshold for the security event log at which the system will generate a warning" in the SCE. This option became available with SP3 for Windows 2000, a new feature for generating a security audit in the security event log when the security log reaches a user–defined threshold. For example, if this value is set to 90, then when the security log reaches 90 percent of capacity, it will show one event entry for eventID 523 with the following text: “The security event log is 90 percent full.”

Note: If log settings are configured for **Overwrite events as needed** or **Overwrite events older than x days**, this event will not be generated.

The following registry value entries have been added to the security template file the **HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security** registry key.

Enable Safe DLL Search Order: Enable Safe DLL search mode (recommended)

Table 3.253: Settings

Subkey Registry Value Entry	Format	Legacy Client	Enterprise Client	High Security
SafeDllSearchMode	DWORD	1	1	1

This entry appears as "MSS: Enable Safe DLL search mode (recommended)" in the SCE. The DLL search order can be configured to search for DLLs requested by running processes in one of two ways:

- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.

The registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. With a setting of 0, the system first searches the current working folder and then searches the folders that are specified in the system path.

The following registry value entries have been added to the template file the **HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager** registry key.

Additional Security Settings

Although most of the countermeasures used to harden the baseline servers in the three environments defined in this guide were applied through Group Policy, there are additional settings that are difficult or impossible to apply with Group Policy. For a detailed explanation of each of the countermeasures discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP,* available at: http://go.microsoft.com/fwlink/?LinkId=15159.

Manual Hardening Procedures

This section describes how some additional countermeasures were implemented manually, such as securing accounts, and how others were put in place by using shell scripts, such as the IPSec filters, to secure the MSBP for each of the security environments defined in this guide.

Manually Adding Unique Security Groups to User Rights Assignments

Most of the recommended security groups for User Rights Assignments have been configured within the security templates that accompany this guide. However, there are a few rights that cannot be included in the security templates, because the SIDs of the certain security groups are unique between different Windows 2003 domains. The problem is that the unique RID (Relative Identifier), which is part of the SID, is unique. These unique instances are described in the table below.

Warning: The table below contains values for Built-in Administrator. The Built-in Administrator is the built-in user account, not the security group "Administrators". If the security group Administrators is added to any of the deny access user rights below, your will need to log on locally in order to correct the mistake of adding the Administrators group to these rights.

In addition, the Built-in Administrator account may have a new name from renaming your Administrator account based on the recommendations from above. When adding this account, be sure that you are selecting the newly renamed administrator account.

Table 3.254 Manually Added User Rights Assignments

Setting Name in UI	Legacy Client	Enterprise Client	High Security
Deny access to this computer from the network	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on as a batch job	Support_388945a0 and Guest	Support_388945a0 and Guest	Support_388945a0 and Guest
Deny log on through Terminal Services	Built-in Administrator; Guests; Support_388945a0; Guest ; all NON-operating system service accounts	Built-in Administrator; Guests; Support_388945a0; Guest ; all NON-operating system service accounts	Built-in Administrator; Guests; Support_388945a0; Guest; all NON-operating system service accounts

Important: All NON-operating system service accounts are service accounts for specific applications in your enterprise.

This does *not* include LOCAL SYSTEM, LOCAL SERVICE, or the NETWORK SERVICE accounts that are built-in accounts for the operating system.

To manually add the above security groups to the Enterprise Client - Member Server Baseline Policy, follow the steps below.

▶ **To add security groups to the User Rights Assignments**

1. In Active Directory Users and Computers, right – click the **Member Servers** OU, and then select **Properties**.
2. On the **Group Policy** tab, select the **Enterprise Client Member Server Baseline Policy** to edit the linked GPO.
3. Select **Enterprise Client – Member Server Baseline Policy**, and then click **Edit**.
4. In the Group Policy window, click **Computer Configuration\Windows Settings\Security Setting\Local Policies\User Rights Assignment** to add the unique security groups from the table above for each right.
5. Close the Group Policy that has been modified.
6. Close the **Member Servers** OU Properties window.
7. Force replication between the domain controllers so that all have the policy applied to them by doing the following:
   a. Open a command prompt, and use the **gpupdate.exe** command line tool to force the server to refresh the policy with the command:

      gpupdate /Force.

   b. Reboot server for changes in the registry and services.
8. Verify in the Event Log that the Group Policy downloaded successfully and that the server can communicate with the other domain controllers in the domain.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This setting should not be changed. The built–in Administrator account is renamed and the description altered to help prevent attackers from compromising a remote server by using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the SID of the built–in Administrator account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

Complete the following steps to secure well known accounts on domains and servers:

1. Rename the Administrator and Guest accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built–in administrator account can be renamed via Group Policy. This setting was not implemented in the DCBP because you should choose a unique name for your environment. The **Accounts: Rename administrator account** can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings of a GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If the server is physically compromised, domain account passwords can be easily obtain by dumping LSA secrets.

NTFS

NTFS partitions support ACLs at the file and folder levels. This support is not available with the file allocation table (FAT), FAT32, or file systems. FAT32 is a version of the FAT file system that has been updated to permit significantly smaller default cluster sizes and to support hard disks up to two terabytes in size. FAT32 is included in Windows 95 OSR2, Windows 98, Microsoft Windows Me, Windows 2000, Windows XP Professional, and Windows Server 2003.

Format all partitions on every server using NTFS. Use the **convert utility** to carefully convert FAT partitions to NTFS, but keep in mind that the convert utility will set the ACLs for the converted drive to **Everyone: Full Control**.

For Windows 2003 Server–based systems, apply the following security templates locally to configure the default file system ACLs for workstations, servers, and domain controllers, respectively:

- %windir%\inf\defltsv.inf
- %windir%\inf\defltdc.inf

Note: The default domain controller security settings are applied during the promotion of a server to a domain controller.

All partitions on servers in all three environments defined in this guide are formatted with NTFS partitions in order to provide the means for file and directory security management via ACLs.

Terminal Services Settings

Table 3.255 Settings

Setting Name in UE	Legacy Client	Enterprise Client	High Security
Set client connection encryption level	High	High	High

The **Set client connection encryption level** setting determines the level of encryption for Terminal Services client connections in your environment. The **High Level** setting option that uses 128–bit encryption prevents an attacker from eavesdropping on Terminal Services sessions using a packet analyzer. Some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such clients, set the encryption level of the connection to send and receive data at the highest encryption level supported by the client.

The path to configure this setting in Group Policy is:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security.

There are three levels of encryption available, as the table below describes.

Table 3.256 Terminal Services Encryption Levels

Encryption Level	Description
High level	This level encrypts data sent from client to server and from server to client by using strong 128–bit encryption. Use this level when the terminal server is running in an environment containing 128–bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.
Client Compatible	This level encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this level when the terminal server is running in an environment containing mixed or legacy clients.
Low level	This level encrypts data sent from the client to the server using 56–bit encryption. **Important:** Data sent from the server to the client is not encrypted.

Error Reporting

Table 3.257: Settings

Setting Name in UE	Legacy Client	Enterprise Client	High Security
Report Errors	Disabled	Disabled	Disabled

Error reporting helps Microsoft track and address errors. You can configure error reporting to generate reports for operating system errors, Windows component errors, or program errors. Enabling **Report Errors** causes such errors to be reported to Microsoft via the Internet or to an internal corporate file share. This setting is only available on Windows XP Professional and Windows Server 2003.

This is the path for configuring this setting in the Group Policy editor:

Computer Configuration\Administrative Templates\System\Error Reporting

Error reports can potentially contain sensitive or even confidential corporate data. Microsoft's privacy policy regarding error reporting ensures that Microsoft Corporation will not use that data improperly. But the data is transmitted in clear-text HTTP, which could be intercepted on the Internet and viewed by third – parties. For these reasons, this guide recommends disabling **Report Errors**.

Summary

This chapter explained the server hardening procedures initially applied to all of the servers in all three of the security environments defined in this guide. Most of these procedures were accomplished by creating a unique security template for each security environment and then importing it into a GPO linked to the parent OU for the member server to achieve the targeted level of security.

However, some of these hardening procedures cannot be applied through Group Policy. In these cases, guidance is provided on how to configure these hardening procedures manually. Additional steps were taken for specific server roles to enable them to function within their roles in as secure a manner as possible.

Server role–specific steps include both additional hardening procedures, as well as procedures to reduce the security settings in the baseline security policy. These changes are discussed in detail in the following chapters of this guide.

More Information

The following information sources were the latest available on topics closely related to Windows Server 2003 at the time this product was released to the public.

For more information on Windows Server 2003 Security setting descriptions, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/615.asp

For more information on Security for Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SEtopnode.asp.

For more information on Auditing Policy for Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp.

For more information on Microsoft Operations Manger (MOM), see: http://www.microsoft.com/mom/.

For more information on User Rights Assignment for Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/URAtopnode.asp.

For more information on differences in default security settings for Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/windows_security_differences.asp.

For more information on securing Windows 2000 Terminal Services, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp.

For more information about hardening the Windows Server 2003 TCP/IP stack, see Microsoft Knowledge Base article Q324270, "Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003," at: http://support.microsoft.com/default.aspx?scid=324270

For more details on hardening the settings for Windows Sockets applications, see Knowledge Base article Q142641, "Internet Server Unavailable Because of Malicious SYN Attacks," at: http://support.microsoft.com/default.aspx?scid=142641.

For more information about the location of .adm files, see Knowledge Base article Q228460, "Location of ADM (Administrative Template) Files in Windows," at: http://support.microsoft.com/default.aspx?scid=228460.

For more information on customizing the Security Configuration Editor user interface, see Microsoft Knowledge Base article 214752, “How to Add Custom Registry Settings to Security Configuration Editor,” at: http://support.microsoft.com/default.aspx?scid=214752.

For more information on creating custom administrative template files in Windows, see Knowledge Base Article 323639, “How to: Create Custom Administrative Templates in Windows 2000,” at: http://support.microsoft.com/default.aspx?scid= 323639. Also review the “Implementing Registry-Based Group Policy” white paper at: http://www.microsoft.com/WINDOWS2000/techinfo/howitworks/management/rbppaper.asp.

For more information on ensuring that more secure LAN Manager Authentication Level settings work in networks with a mix of Windows 2000 and Windows NT 4.0 systems, see Knowledge Base article Q305379, "Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain," at: http://support.microsoft.com/default.aspx?scid=305379.

For more information on LAN Manager Compatibility levels, see http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/regentry/76052.asp.

For more information on NTLMv2 authentication, see Knowledge Base article Q239869, "How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT," at: http://support.microsoft.com/default.aspx?scid=239869.

For more information on the default settings for services in Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/sys_srv_default_settings.asp.

For more information on smart card deployment, see the Technet Smart Card Web site, at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/default.asp.

For more information on Auditing Policy for Windows Server 2003, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp.

For more information on how the "RestrictAnonymous" registry value may break the trust to a Windows 2000 domain; see: http://support.microsoft.com/default.aspx?scid=kb;en-us;296405.

For more information on disabling error reporting, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sysdm_advancd_exception_reporting.asp.

For more information on Windows Corporate Error Reporting, see: http://www.microsoft.com/office/ork/xp/appndx/appa19.htm.

4

Hardening Domain Controllers

Overview

The domain controller server role is one of the most important roles to secure in any environment with computers running Microsoft® Windows Server™ 2003 that use Microsoft Active Directory® directory service. Any loss or compromise of a domain controller in the environment could prove devastating to clients, servers, and applications that rely on domain controllers for authentication, Group Policy, and a central lightweight directory access protocol (LDAP) directory.

Due to their importance, domain controllers should always be stored in physically secure locations that are accessible only to qualified administrative staff. When domain controllers must be stored in unsecured locations, branch offices for example, several security settings can be adjusted to limit the potential damage from physical threats.

Domain Controller Baseline Policy

Unlike the other server role policies detailed later in this guide, the Group Policy for the Domain Controllers server role is a baseline policy, putting it in the same class as the Member Server Baseline Policy (MSBP) defined in Chapter 3, "Creating a Member Server Baseline." The Domain Controllers Baseline Policy (DCBP) is linked to the Domain Controllers organizational unit (OU) and takes precedence over the Default Domain Controllers Policy. The settings included in the DCBP will strengthen the overall security across the domain controllers in any given environment.

Most of the DCBP is a direct copy of the MSBP. Since the DCBP is based on the MSBP, Chapter 3, "Creating a Member Server Baseline," should be closely reviewed in order to fully understand the many settings that are also included in the DCBP. Only the DCBP settings that differ from those in the MSBP are documented in this chapter.

Domain controller templates are uniquely designed to address the security needs of the three environments defined in this guide. The following table shows the relationship between the domain controller .inf files included with this guide, and these environments. For example, the Enterprise Client – Domain Controller.inf file is the security template for the Enterprise Client environment.

Table 4.1: Domain Controller Baseline Security Templates

Legacy Client	Enterprise Client	High Security
Legacy Client – Domain Controller.inf	Enterprise Client – Domain Controller.inf	High Security – Domain Controller.inf

Note: Linking an incorrectly configured group policy object (GPO) to the Domain Controllers OU could severely hinder the proper operation of a domain. Exercise extreme care when importing these security templates, and verify all settings imported are correct before linking a GPO the Domain Controllers OU.

Audit Policy Settings

The Audit Policy settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." The baseline policy settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers.

User Rights Assignments

The DCBP specifies a number of user rights assignments for the domain controllers. In addition to the default settings, seven other user rights were modified to strengthen the security for the domain controllers in the three environments defined in this guide.

This section provides details on the prescribed user rights settings for the DCBP which differ from those in the MSBP. For a summary of the prescribed settings in this section, refer to the Windows Server 2003 Security Guide Settings Excel workbook included with this guide.

Access this computer from the network

Table 4.2: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Everyone, Pre-Windows 2000 Compatible Access.	Not Defined.	Not Defined	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS

The **Access this computer from the network** user right determines which users and groups are allowed to connect to the computer over the network. This user right is required by a number of network protocols including server message block (SMB)–based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP).and Component Object Model Plus (COM+).

Although permissions granted to the **Everyone** security group no longer grant access to anonymous users in Windows Server 2003, guest groups and accounts can still be granted access through the **Everyone** security group. For this reason, this guide recommends removing the **Everyone** security group from the **Access this computer from the network** user right in the High Security environment to further guard from attacks targeting guest access to the domain.

Add workstations to domain

Table 4.3: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Authenticated Users	Administrators	Administrators	Administrators

The **Add workstations to domain** user right allows the user to add a computer to a specific domain. For this right to take effect, it must be assigned to the user as part of the Default Domain Controllers Policy for the domain. A user who has been granted this right can add up to 10 workstations to the domain. Users who have been granted the **Create Computer Objects** permission for an OU or the Computers container in Active Directory can also join a computer to a domain. Users who have been granted this permission can add an unlimited number of computers to the domain regardless of whether they have been assigned the **Add workstations to a domain** user right or not.

By default, all users in the **Authenticated Users** group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.

In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. Some organizations want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage them.

Allowing users to add workstations to the domain can hamper this effort. It also provides avenues for users to perform activities that are more difficult to trace because they can create additional unauthorized domain computers.

For these reasons, the **Add workstations to domain** user right is granted only to the **Administrators** group in the three environments defined in this guide.

Allow log on locally

Table 4.4: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Account Operators, Backup Operators, Print Operators, and Server Operators	Administrators	Administrators	Administrators

The **Allow log on locally** user right allows a user to start an interactive session on the computer. Users who do not have this right are still able to start a remote interactive session on the computer if they have the **Allow logon through Terminal Services** right.

Limiting which accounts can be used to log on to domain controller consoles in an environment will help prevent unauthorized access to domain controller file systems and system services. A user who is able to log on to the console of a domain controller could maliciously exploit the system, and possibly compromise the security of an entire domain or forest.

By default, the **Account Operators**, **Backup Operators**, **Print Operators**, and **Server Operators** groups are granted the right to log on locally to domain controllers. Users in these groups should not need to log on to a domain controller to perform their management tasks. Users in these groups can normally perform their duties from other workstations. Only users in the **Administrators** group should perform maintenance tasks on domain controllers.

Granting this right only to the **Administrators** group limits physical and interactive access to domain controllers to only highly trusted users, therefore enhancing security. For this reason, the **Allow log on locally** user right is granted only to the **Administrators** group in the three environments defined in this guide.

Allow log on through Terminal Services

Table 4.5: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Not Defined	Administrators	Administrators	Administrators

The **Allow log on through Terminal Services** user right allows a user to log on to the computer by using a Remote Desktop connection.

Limiting which accounts can be used to log on to domain controller consoles via Terminal Services will help prevent unauthorized access to domain controller file systems and system services. A user who is able to log onto the console of a domain controller via Terminal Services can exploit that system, and possibly compromise the security of an entire domain or forest.

Granting this right only to the **Administrators** group limits interactive access to domain controllers only to highly trusted users, therefore enhancing security. For this reason, the **Allow log on locally** user right is granted only to the **Administrators** group in the three environments defined in this guide. Although logging on to a domain controller via Terminal Services requires administrative access by default, configuring this user right helps protect against inadvertent or malicious actions that might compromise this restriction.

As a further security measure, the DCBP denies the default **Administrator** account the right to log on to a domain controller via Terminal Services. This setting also prevents malicious users from attempting to remotely break into a domain controller using the default **Administrator** account. For more details on this setting, see Chapter 3, "Creating a Member Server Baseline."

Change the system time

Table 4.6: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Server Operators	Administrators	Administrators	Administrators

The **Change the system time** user right allows the user to adjust the time on the computer's internal clock. This right is not required to change the time zone or other display characteristics of the system time.

Synchronized system time is critical to the operation of Active Directory. Proper Active Directory replication and authentication ticket generation process used by the Kerberos version 5 authentication protocol both rely on time being synchronized across any environment.

A domain controller configured with a system time that is out of sync with the system time on other domain controllers in the environment could interfere with the operation of domain services. Allowing only administrators to modify system time minimizes the possibility of a domain controller being configured with an incorrect system time.

By default, the **Server Operators** group is granted the right to modify system time on domain controllers. Because of the possible repercussions that may result from members of this group incorrectly modifying system time on a domain controller, this user right is configured in the DCBP so that only the **Administrators** group can change the system time in any of the three environments defined in this guide.

For more information on the Microsoft Windows® Time Service, refer to Knowledge Base articles Q224799, "Basic Operation of the Windows Time Service," located at: http://support.microsoft.com/default.aspx?scid=224799 and Q216734, "How to Configure an Authoritative Time Server in Windows 2000," located at: http://support.microsoft.com/default.aspx?scid=216734.

Enable computer and user accounts to be trusted for delegation

Table 4.7: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators	Not Defined	Not Defined	Administrators

The **Enable computer and user accounts to be trusted for delegation** user right allows the user to change the Trusted for Delegation setting on a user or computer object in Active Directory. Delegation of authentication is a capability that is used by multi–tier client/server applications. It allows a front–end service to use the credentials of a client in authenticating to a back–end service. For this to be possible, both client and server must be running under accounts that are trusted for delegation.

Misuse of this right could lead to unauthorized users impersonating other users on the network. An attacker could exploit this right to gain access to network resources while appearing to be a different user, which could make determining what has happened after a security incident more difficult to decipher.

This guide recommends assigning the **Enable computer and user accounts to be trusted for delegation** right to the **Administrators** group on domain controllers.

Note: Although the Default Domain Controllers Policy assigns the Administrators group this right, the DCBP enforces this right in the High Security environment only because it was originally based on the MSBP. The MSBP assigns this right a NULL value.

Load and unload device drivers

Table 4.8: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Print Operators	Administrators	Administrators	Administrators

The **Load and unload device drivers** user right determines which users can load and unload device drivers. This user right is necessary for loading and unloading Plug and Play devices.

Maliciously loading or unloading a device driver on a domain controller can have an adverse impact on its operation. Limiting the accounts that are capable of loading and unloading device drivers to only the most trusted users minimizes the opportunity of device drivers being used to compromise domain controllers in your environment.

By default, the **Print Operators** group is granted this right. As mentioned earlier, it is not recommended to create printer shares on domain controllers. This removes the need for **Print Operators** to require the right to load and unload device drivers. Therefore, this user right is granted only to the **Administrators** group in the three environments defined in this guide.

Restore files and directories

Table 4.9: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Backup Operators, Server Operators	Administrators	Administrators	Administrators

The **Restore files and directories** user right 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.

Enabling a user account to restore files and directories to the file system of a domain controller gives the account owner the power to easily modify service executables. Malicious users can exploit the access this right provides to not only render a domain controller useless, but compromise the security of a domain or an entire forest.

By default, the **Server Operators** and **Backup Operators** groups are granted this right. Removing this user right from these groups and granting it only to the **Administrators** group reduces the likelihood of a domain controller being compromised by improper modifications to the file system. Therefore, this user right is granted only to the **Administrators** group in the three environments defined in this guide.

Shutdown the system

Table 4.10: Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Server Operators, Print Operators, Backup Operators	Administrators	Administrators	Administrators

The **Shutdown the system** user right allows a user to shut down the local computer.

Malicious users with the ability to shutdown domain controllers can easily initiate a denial of service (DoS) attack that could severely impact an entire domain or forest. Furthermore, this user right can be exploited to launch an elevation of privilege attack on a domain controller's system account when it is restarting services. A successful elevation of privilege attack on a domain controller compromises the security of a domain or an entire forest.

By default the **Administrators**, **Server Operators**, **Print Operators**, and **Backup Operators** groups are granted this right to shutdown domain controllers. In secure environments, none of these groups, except for **Administrators**, require this right to perform administrative tasks. For this reason, this user right is granted to the **Administrators** group only in the three environments defined in this guide.

Security Options

Most of the Security Options settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." Differences between the MSBP and the DCBP are described in the following section.

Network security: Do not store LAN Manager hash value on next password change

Table 4.11: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Enabled	Enabled

The **Network security: Do not store LAN Manager hash value on next password change** security option setting determines if the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT® hash. For this reason, this MSBP enables this setting in the three security environments defined in this guide.

The DCBP enables this setting on domain controllers in the Enterprise Client and High Security environments, and disables it on domain controllers in the Legacy Client environment. If this setting were enabled on domain controllers in the Legacy Client environment, Windows 98 clients would be unable to login after changing their passwords.

Note: Legacy operating systems and some third – party applications may fail when this setting is enabled. Furthermore, enabling this setting will require all accounts to change their password.

Event Log Settings

The Event Log settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." The baseline Group Policy settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers, including Directory Services Access.

System Services

The following system services must be enabled on all Windows Server 2003 domain controllers. The baseline policy settings in the DCBP ensure that all the required system services are configured uniformly across domain controllers.

This section provides details on the prescribed system services settings for the DCBP which differ from those in the MSBP. For a summary of the prescribed settings in this section, refer to the Windows Server 2003 Security Guide Settings Excel workbook included with this guide.

Note: If you run the DCDiag.exe utility from the Windows Server 2003 Support Tools, it will check for all services that can run on the domain controllers in your environment. The DCDiag.exe will report errors because some services are disabled in the Domain Controller Baseline Policy—including IISADMIN, SMTPSVC, and TrkSvr. This information does not indicate a problem with your configuration.

Distributed File System

Table 4.12: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Dfs	Automatic	Automatic	Automatic

The **Distributed File System (DFS)** service distributes and integrates disparate file shares into a single logical namespace. The service manages logical volumes distributed across a local or wide area network (WAN), and is required for the Active Directory System Volume (SYSVOL) share. SYSVOL replication relies on the proper operation of DFS.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

DNS Server

Table 4.13: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Dns	Automatic	Automatic	Automatic

The **DNS Server** service resolves Domain Name System (DNS) queries and update requests for DNS names. **DNS Server** is a crucial service for locating devices identified using DNS names and domain controllers in Active Directory.

The reliability and availability of Active Directory relies heavily on the proper operation of the **DNS Server** service. Without DNS, domain controllers cannot locate each other to replicate directory information, and clients cannot contact domain controllers for authentication.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

File Replication

Table 4.14: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	NtFrs	Automatic	Automatic	Automatic

The **File Replication** service allows files to be automatically copied and maintained simultaneously on multiple servers. File Replication Service (FRS) is the automatic file replication service in Windows 2000 and the Windows Server™ family. The service replicates the SYSVOL on all domain controllers, and can be configured to replicate files on other targets associated with the fault tolerant DFS. SYSVOL replication also relies on the proper operation of the **File Replication** service.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Intersite Messaging

Table 4.15: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	IsmServ	Automatic	Automatic	Automatic

The **Intersite Messaging** (ISM) service enables messages to be exchanged between computers running Windows Server sites. This service is used for mail–based replication between sites. Active Directory includes support replication between sites using Simple Mail Transfer Protocol (SMTP) over Internet Protocol (IP) transport. SMTP support is provided by the SMTP service, which is a component of Microsoft Internet Information Services (IIS).

The set of transports used for communication between sites must be extensible; therefore, each transport is defined in a separate add–in dynamic link library (DLL). These add–in DLLs are loaded into the ISM service, which runs on all domain controllers that may perform intersite communication. The ISM service directs send and receive message requests to the appropriate transport add–in DLLs, and then routes the messages to the ISM service on the destination computer. Active Directory replication relies on the **Intersite Messaging** service running properly.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Kerberos Key Distribution Center

Table 4.16: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Kdc	Automatic	Automatic	Automatic

The **Kerberos Key Distribution Center** (KDC) service enables users to log on to the network using the Kerberos v5 authentication protocol.

The KDC service is required for users to log on to the network. Disabling this service blocks users from logging on to the network.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Remote Procedure Call (RPC) Locator

Table 4.17: Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	RpcLocator	Automatic	Automatic	Automatic

The **Remote Procedure Call (RPC) Locator** service enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database.

Stopping or disabling this service may prevent RPC clients using RpcNs* APIs from locating servers or fail to start. Also, RPC clients that rely on RpcNs* APIs from the same computer may not find RPC servers supporting a given interface. Stopping or disabling this service on your domain controller may cause RPC clients using the RpcNs* APIs and the domain controller to experience service interruption while trying to locate clients.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Additional Security Settings

This section describes manual modifications that must be made to the DCBP, as well as additional settings and countermeasures that cannot be implemented via Group Policy.

Manually Adding Unique Security Groups to User Rights Assignments

Most User Rights Assignments applied via the DCBP have been properly specified in the security templates that accompany this guide. However, there are a few accounts and security groups that cannot be included in the templates because their security identifiers (SIDs) are specific to individual Windows 2003 domains. User rights assignments that must be configured manually are specified below.

Warning: The following table contains values for the built – in Administrator account. This account is not to be confused with the built – in Administrators security group. If the Administrators security group is added to any of the deny access user rights below you will need to log on locally in order to correct the mistake.

In addition, the built – in Administrator account may have been renamed based on some of the recommendations described in Chapter 3, "Creating a Member Server Baseline." When adding the Administrator account, ensure the renamed account is specified.

Table 4.18: Manually Added User Rights Assignments

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Deny access to this computer from the network	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts
Deny log on as a batch job	Support_388945a0 and Guest	Support_388945a0 and Guest	Support_388945a0 and Guest
Deny log on through Terminal Services	Built–in Administrator; all NON-operating system service accounts	Built–in Administrator; all NON-operating system service accounts	Built–in Administrator; all NON-operating system service accounts

Important: All non–operating system service accounts include service accounts used for specific applications across an enterprise. This does NOT include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts which are built – in accounts the operating system uses.

Directory Services

Domain controllers running Windows Server 2003 store directory data and manage user and domain interactions, including user logon processes, authentication, and directory searches.

Relocating Data – Active Directory Database and Log Files

Safeguarding the Active Directory database and log files is crucial to maintaining directory integrity and reliability.

Moving the ntds.dit, edb.log, and temp.edb files from their default location will help to conceal them from an attacker if a domain controller is compromised. Furthermore, moving the files off the system volume to a separate physical disk will also improve domain controller performance.

For these reasons, this guide recommends moving the Active Directory database and log files for the domain controllers in the three environments defined in this guide from their default location on the system volume to a non–system striped or striped/mirrored disk volume.

Resizing Active Directory Log Files

Ensuring an adequate amount of information is logged and maintained for domain controllers across an environment is crucial to effectively monitor and maintain the integrity, reliability, and availability of Active Directory.

Increasing the maximum size of the log files to support this effort will assist administrators in maintaining an adequate amount of information needed to perform meaningful audits in the event of hacker attacks.

For these reasons, this guide recommends increasing the maximum size of the Directory Service and File Replication Service log files from the 512 KB default to 16 MB on the domain controllers in the three environments defined in this guide.

Using Syskey

On domain controllers, password information is stored in directory services. It is not unusual for password–cracking software to target the Security Accounts Manager (SAM) database or directory services to access passwords for user accounts.

The System Key utility (Syskey) provides an extra line of defense against offline password–cracking software. Syskey uses strong encryption techniques to secure account password information that is stored in directory services.

Table 4.19: Syskey Modes

System Key Option	Security Level	Description
Mode 1: System Generated Password, Store Startup Key Locally	Secure	Uses a computer–generated random key as the system key and stores an encrypted version of the key on the local computer. This option provides strong encryption of password information in the registry, and enables the user to restart the computer without the need for an administrator to enter a password or insert a disk.
Mode 2: Administrator generated password, Password Startup	More secure	Uses a computer–generated random key as the system key and stores an encrypted version of the key on the local computer. The key is also protected by an administrator–chosen password. Users are prompted for the system key password when the computer is in the initial startup sequence. The system key password is not stored anywhere on the computer.
Mode 3: System Generated Password, Store Startup Key on Floppy Disk	Most secure	Uses a computer-generated random key and stores the key on a floppy disk. The floppy disk that contains the system key is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Syskey is enabled on all Windows Server 2003 servers in Mode 1 (obfuscated key). There are many reasons to recommend using Syskey in Mode 2 (console password) or Mode 3 (floppy storage of Syskey password) for any domain controller that is exposed to physical security threats.

From a security standpoint, this appears sensible at first, as the domain controller would be vulnerable to being restarted by an attacker with physical access to it. Syskey in Mode 1 allows an attacker to read and alter the contents of the directory.

However, the operational requirements for ensuring that domain controllers can be made available through restarts tend to make Syskey Mode 2 or Mode 3 difficult to support. To take advantage of the added protection provided by these Syskey modes, the proper operational processes must be implemented in your environment to meet specific availability requirements for the domain controllers.

The logistics of Syskey password or floppy disk management can be quite complex, especially in branch offices. For example, requiring one of your branch managers or local administrative staff to come to the office at 3 A.M. to enter the passwords, or insert a floppy to enable other users to access the system is expensive and makes it very challenging to achieve high availability service level agreements (SLAs).

Alternatively, allowing your centralized IT operations personnel to provide the Syskey password remotely requires additional hardware—some hardware vendors have add–on solutions available to remotely access server consoles.

Finally, the loss of the Syskey password or floppy disk leaves your domain controller in a state where it cannot be restarted. There is no method for you to recover a domain controller if the Syskey password or floppy disk is lost. If this happens, the domain controller must be rebuilt.

Nevertheless, with the proper operational procedures in place, Syskey can provide an increased level of security that can greatly protect the sensitive directory information found on domain controllers.

For these reasons, Syskey Mode 2 or Mode 3 is recommended for domain controllers in locations without strong physical storage security. This recommendation also applies to domain controllers in any of the three environments described in this guide.

▶ **To create or update a system key:**

1. Click **Start**, click **Run**, type **syskey**, and then click **OK**.
2. Click **Encryption Enabled**, and then click **Update**.
3. Click the desired option, and then click **OK**.

Active Directory Integrated DNS

Microsoft recommends using Active Directory integrated DNS in the three environments defined in this guide, in part because integrating the zones into Active Directory simplifies the process of securing the DNS infrastructure.

Protecting DNS Servers

Safeguarding DNS servers is essential to any environment with Active Directory. The following sections provide several recommendations and explanations for doing this.

When a DNS server is attacked, one possible goal of the attacker is to control the DNS information being returned in response to DNS client queries. In this way, clients can be inadvertently misdirected to unauthorized computers. IP spoofing and cache poisoning are examples of this type of attack.

In IP spoofing, a transmission is given the IP address of an authorized user to obtain access to a computer or network. Cache poisoning is an attack in which an unauthorized host transmits false information regarding another host into the cache of a DNS server. The attack results in redirecting clients to unauthorized computers.

Once clients start inadvertently communicating with unauthorized computers, those computers may attempt to gain access to information stored on the client computers.

Not all attacks focus on spoofing DNS servers. Some DoS attacks could alter DNS records in legitimate DNS servers to provide invalid addresses in response to client queries. By causing the server to respond with invalid addresses, clients and servers cannot locate the resources they need to function, such as domain controllers, Web servers, or file shares.

For these reasons, this guide recommends configuring the routers used in the three environments to drop spoofed IP packets to ensure that the IP addresses of the DNS servers cannot be spoofed by other computers.

Configuring Secure Dynamic Updates

The Windows Server 2003 DNS client service supports Dynamic DNS updates, which allow client systems to add DNS records directly into the database. Dynamic DNS servers can receive malicious or unauthorized updates from an attacker using a client that supports the DDNS protocol if the server is configured to accept unsecured updates.

At a minimum, an attacker can add bogus entries to the DNS database; at worst, the attacker can overwrite or delete legitimate entries in the DNS database. Such an attack may result in any of the following conditions:

- Directing clients to unauthorized domain controllers: When a client submits a DNS query looking for the address of a domain controller, a compromised DNS server can be instructed to return the address of an unauthorized server. Then, with the use of other non–DNS related attacks, the client might be tricked into passing on secure information to the bogus server.
- Responding to DNS queries with invalid addresses: This makes clients and servers unable to locate one another. If clients cannot locate servers, they cannot access the directory. When domain controllers cannot locate other domain controllers, directory replication stops, creating a DoS condition that could affect users throughout a forest.
- Creating a DoS condition in which a server's disk space may be exhausted by a huge zone file filled with dummy records, or large numbers of entries that slow down replication.

Using secure DDNS updates guarantees that registration requests are only processed if they are sent from valid clients in an Active Directory forest. This greatly limits the opportunity for an attacker to compromise the integrity of a DNS server.

For these reasons, this guide recommends configuring Active Directory DNS servers in the three environments defined in this guide to accept only Secure Dynamic Updates.

Limiting Zone Transfers to Authorized Systems

Because of the important role that zones play in DNS, they should be available from more than one DNS server on the network to provide adequate availability and fault tolerance when resolving name queries. Otherwise, name queries sent to just one server that does not respond in the zone can fail to resolve. For additional servers to host a zone, zone transfers are required to replicate and synchronize all copies of the zone used at each server configured to host the zone.

Furthermore, a DNS server that is not configured to limit who can request zone transfers is vulnerable to transferring the entire DNS zone to anyone who requests it. This can be easily accomplished using tools such as nslookup.exe. Such tools can expose the entire domain's DNS dataset, including such things as which hosts are serving as domain controllers, directory–integrated Web servers, or Microsoft SQL Server™ 2000 databases.

For these reasons, this guide recommends configuring Active Directory Integrated DNS servers in the three environments defined in this guide to allow zone transfers, but to limit which systems can make transfer requests.

Resizing the Event Log and DNS Service Log

Ensuring an adequate amount of information is logged and maintained for domain controllers across an environment is crucial to effectively monitor the DNS Service.

Increasing the maximum size of the DNS Service log file will assist administrators in maintaining an adequate amount of information to perform meaningful audits in the event of an attack.

For this reason, this guide recommends configuring the maximum size for the DNS Service log file on the domain controllers in the three environments defined in this guide to at least 16 MB, and ensure that the **Overwrite events as needed** option in the DNS Service is selected to maximize the amount of log entries preserved.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that can not be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

By default, the **Guest** account is disabled on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the SID of the built–in Administrator account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

Complete the following steps to secure well known accounts on domains and servers:

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built – in administrator account can be renamed via Group Policy. This setting was not configured in the DCBP because you should choose a unique name for your environment. The Accounts: Rename administrator account can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings of a GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Terminal Services Settings

Table 4.20: Settings

Default	Legacy Client	Enterprise Client	High Security
Set client connection encryption level	High	High	High

The **Set client connection encryption level** setting determines the level of encryption for Terminal Services client connections in your environment. The **High Level** setting option that uses 128–bit encryption prevents an attacker from eavesdropping on Terminal Services sessions using a packet analyzer. Some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such clients, set the encryption level of the connection to send and receive data at the highest encryption level supported by the client. For these reasons, this guide recommends configuring the **Set client connection encryption level** setting to **Enabled**, and the option for **High Level** encryption is selected in the DCBP in the three security environments defined in this guide.

This path for configuring this setting in the Group Policy Object Editor is:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security.

There are three levels of encryption available:

Table 4.21: Terminal Services Encryption Levels

Encryption Level	Description
High level	This level encrypts data sent from client to server and from server to client by using strong 128–bit encryption. Use this level when the terminal server is running in an environment containing 128–bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.
Client Compatible	This level encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this level when the terminal server is running in an environment containing mixed or legacy clients.
Low level	This level encrypts data sent from the client to the server using 56–bit encryption. **Important:** Data sent from the server to the client is not encrypted.

Error Reporting

Table 4.22: Settings

Default	Legacy Client	Enterprise Client	High Security
Report Errors	Disabled	Disabled	Disabled

The **Error Reporting** service helps Microsoft track and address errors. You can configure this service to generate reports for operating system errors, Windows component errors, or program errors. Enabling the **Report Errors** service causes such errors to be reported to Microsoft via the Internet or to an internal corporate file share.

This setting is only available on Microsoft Windows® XP Professional and Windows Server 2003. The path for configuring this setting in the Group Policy Object Editor is:

Computer Configuration\Administrative Templates\System\Error Reporting

Error reports can potentially contain sensitive or even confidential corporate data. The Microsoft privacy policy regarding error reporting ensures that Microsoft will not use such data improperly, but the data is transmitted in cleartext Hypertext Transfer Protocol (HTTP), which could be intercepted on the Internet and viewed by third – parties. For these reasons, this guide recommends configuring the **Error Reporting** setting to **Disabled** in the DCBP in all three security environments defined in this guide.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that can be created on domain controllers in the High Security environment defined in this guide.

The following table lists all of the IPSec filters that should be created on domain controllers in the High Security environment defined in this guide.

Table 4.23: Domain Controller IPSec Filter Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
CIFS/SMB Server	TCP	ANY	445	ANY	ME	ALLOW	YES
	UDP	ANY	445	ANY	ME	ALLOW	YES
RPC Server	TCP	ANY	135	ANY	ME	ALLOW	YES
	UDP	ANY	135	ANY	ME	ALLOW	YES
NetBIOS Server	TCP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	138	ANY	ME	ALLOW	YES
	TCP	ANY	139	ANY	ME	ALLOW	YES
Monitoring Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services Server	TCP	ANY	3389	ANY	ME	ALLOW	YES
Global Catalog Server	TCP	ANY	3268	ANY	ME	ALLOW	YES
	TCP	ANY	3269	ANY	ME	ALLOW	YES

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
DNS Server	TCP	ANY	53	ANY	ME	ALLOW	YES
	UDP	ANY	53	ANY	ME	ALLOW	YES
Kerberos Server	TCP	ANY	88	ANY	ME	ALLOW	YES
	UDP	ANY	88	ANY	ME	ALLOW	YES
LDAP Server	TCP	ANY	389	ANY	ME	ALLOW	YES
	UDP	ANY	389	ANY	ME	ALLOW	YES
	TCP	ANY	636	ANY	ME	ALLOW	YES
	UDP	ANY	636	ANY	ME	ALLOW	YES
NTP Server	TCP	ANY	123	ANY	ME	ALLOW	YES
	UDP	ANY	123	ANY	ME	ALLOW	YES
Static AD Replication Server	TCP	ANY	57952	ANY	ME	ALLOW	YES
DC Comms	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
DC Comms	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
ICMP	ICMP	ANY	ANY	ME	ANY	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role – specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. Opening additional ports will make the domain controllers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Recommendations from Knowledge Base article Q224196, "Restricting Active Directory Replication Traffic to a Specific Port," located at http://support.microsoft.com/default.aspx?scid=224196, need to be implemented on domain controllers. This ensures that domain replication occurs over a specific port. Once again, a random port over 50,000 should be used for this purpose. In the example above, the port 57952 was chosen. A different port should be used in your environment, but this change should be made on all domain controllers where this guidance will be implemented. After the steps from the Knowledge Base article are implemented, the servers must be restarted for the changes to take effect.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client — the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand – alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Note: Domain controllers are extremely dynamic, and implementing IPSec filters on them should be carefully evaluated, and then thoroughly tested in a lab environment. Because of the large amount of interaction between domain controllers, IPSec filters need to be added to allow all traffic between domain controllers that replicate information with each other. In complex environments with many domain controllers, this will require the creation of dozens of additional filters so the filters can effectively protect the domain controllers. This could make it very difficult to implement and manage IPSec policies. Nevertheless, environments with few domain controllers can efficiently leverage the advantages gained by implementing IPSec filters.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for a domain controller. The PacketFilters-DC.cmd file uses the NETSH command to create the appropriate filters. This .cmd file must be modified to include the IP addresses of the other domain controllers in the environment. The script contains place holders for two domain controllers to be added. Additional domain controllers can be added if desired. This list of IP addresses for the domain controllers must be kept up to date.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP. Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings required to secure domain controllers in each of the three environments defined in this guide. Most of the settings discussed were configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the Default Domain Controller Policy was linked to the Domain Controllers Organizational Unit (OU). The settings included in the Domain Controllers Baseline Policy (DCBP) will enhance overall security across the domain controllers in any given environment. Using two GPOs to secure domain controllers allows for the default environment to be preserved and simplifies troubleshooting.

Several of the server hardening settings cannot be applied through Group Policy. In these cases, details on configuring these settings manually have been provided.

Now that the domain controllers are secured, the following chapters of this guide will focus on securing several other specific server roles.

More Information

The following information sources were the latest available on topics closely related to securing domain controllers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For information about the Microsoft Systems Architecture: Enterprise Data Center prescriptive architecture guides, see:

http://www.microsoft.com/technet/itsolutions/edc/default.asp.

For information about enabling anonymous access to Active Directory, see Knowledge Base article 257988, "Description of Dcpromo Permissions Choices," see:

http://support.microsoft.com/default.aspx?scid=257988.

For information about Windows 2000 DNS, see the "Windows 2000 DNS White Paper" at: http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp.

For more information about Windows 2000 DNS, see Chapter 6 of the online version of "TCP/IP Core Networking Guide" at: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp.

For information about Windows 2003 DNS, see the "Changes to DNS in Windows Server 2003 at:

http://www.microsoft.com/windows2000/technologies/communications/dns/dns2003.asp

For more information on IPSec filtering, see "How To: Use IPSec IP Filter Lists in Windows 2000," at: http://support.microsoft.com/default.aspx?scid=313190.

For more information on restricting Active Directory, see "Restricting Active Directory Replication Traffic to a Specific Port," at:

http://support.microsoft.com/default.aspx?scid=224196.

For more information on restricting FRS replication traffic, see "How to Restrict FRS Replication Traffic to a Specific Static Port," at:

http://support.microsoft.com/default.aspx?scid=319553.

For more information on the Windows Time Service, see "Basic Operation of the Windows Time Service," at: http://support.microsoft.com/default.aspx?scid=224799.

For more information on configuring the Windows Time Service, see "How to Configure an Authoritative Time Server in Windows 2000," at:

http://support.microsoft.com/default.aspx?scid=216734.

For more information on IP spoofing, see the article in the SANS Info Sec Reading Room, at: http://www.sans.org/rr/threats/intro_spoofing.php.

5

Hardening Infrastructure Servers

Overview

This chapter explains the server hardening settings for securing infrastructure servers across the three environments defined in this guide. For the purposes of this guide, an infrastructure server refers to a server providing Dynamic Host Control Protocol (DHCP) services or Microsoft® Windows® Internet Name Service (WINS) functionality.

Most of the settings discussed are configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) containing the infrastructure servers to provide additional security based on the services these servers provide.

A few of the settings discussed cannot be applied using Group Policy. In these cases, details for configuring these settings manually are provided. Details for creating and applying Internet Protocol Security (IPSec) filters that control the type of network traffic that can communicate with both types of infrastructure server outlined in this chapter is also provided.

To improve the usability of this chapter, only those settings that have been modified from the MSBP are included here. For information on settings in the MSBP, see Chapter 3, “Creating a Member Server Baseline.” For information on all default settings, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*.

Audit Policy Settings

The Audit Policy settings for infrastructure servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all infrastructure servers.

User Rights Assignments

The User Rights Assignments for infrastructure servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all appropriate User Rights Assignments are uniformly configured across infrastructure servers.

Security Options

The Security Options settings for infrastructure servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant Security Options are uniformly configured across infrastructure servers.

Event Log Settings

The Event Log settings for infrastructure servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline."

System Services

This System Services settings section provides details on the prescribed system that should be either enabled or disabled on the infrastructure servers in your environment. These service settings are specified in the Infrastructure Server Incremental Policy. In order to minimize the possibility of a denial of service (DoS) attack, the GPO ensures these services are configured to start automatically. For a summary of the prescribed settings in this section, refer to the Windows Server 2003 Security Guide Settings Excel workbook included with this guide.

DHCP Server

Table 5.1: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
DHCP	Not installed	Automatic	Automatic	Automatic

The DHCP service allocates Internet Protocol (IP) addresses and enables advanced configuration of network settings such as DNS servers and WINS servers to DHCP clients automatically. DHCP uses a client/server model. The network administrator establishes one or more DHCP servers that maintain Transmission Control Protocol/Internet Protocol (TCP/IP) configuration information and provide it to clients.

The DHCP Server service must be running for a DHCP server to assign IP address configuration to its clients. Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. Group Policy will also prevent administrators from inadvertently disabling the service.

WINS

Table 5.2: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
WINS	Not installed	Automatic	Automatic	Automatic

WINS enables network basic input/output system (NetBIOS) name resolution. The presence of the WINS servers is crucial for locating the network resources identified using NetBIOS names. WINS servers are required unless all domains have been upgraded to Microsoft Active Directory®, all computers on the network are running Windows 2000 or later, and no applications rely on WINS resolution for proper operation.

The WINS Server service must be running for a WINS server to provide name resolution to its clients. Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. Group Policy will also prevent administrators from inadvertently disabling the service.

Additional Security Settings

The security settings applied through the MSBP provide a great deal of enhanced security for infrastructure servers. There are a few additional considerations that should be taken into account. These steps cannot be completed via Group Policy and should be performed manually on all infrastructure servers.

Configure DHCP Logging

The DHCP service only logs startup and shutdown events by default in the Event Viewer. A more detailed log can be enabled on the DHCP server by following these steps:

1. Right–click the DHCP server in the DHCP Administration Tool.
2. Select **Properties**.
3. On the **General** tab of the **Properties** dialog box, click **Enable DHCP Audit Logging**.

Upon completion of these steps, the DHCP server will create a log file in the following location:

```
%systemroot%\system32\dhcp\
```

DHCP clients are often difficult to locate in log entries because the only information that is stored in most event logs are computer names, not IP addresses. The DHCP audit logs can provide one more tool for locating the sources of internal attacks or inadvertent activities.

However, the information in these logs is not by any means foolproof, since both host names and media access control (MAC) addresses can be forged or spoofed. Spoofing is the practice of making a transmission appear to come from a user other than the user who performed the action. Nevertheless, the benefits of collecting this information by far exceed the costs incurred by enabling logging on a DHCP server. Having more than just an IP address and a machine name can be of great assistance in determining how a particular IP address was used on a network.

Server Operators and Authenticated Users by default have read–permissions to these log files. In order to best preserve the integrity of the information logged by a DHCP server, it is recommended that access to these logs be limited to server administrators. The Server Operators and Authenticated Users groups should be removed from the Access Control List (ACL) of the %systemroot%\system32\dhcp\ folder.

The DHCP audit logs could in theory fill the disk they are stored on. Nevertheless, the default configuration for the DHCP audit logging setting ensures that this logging will stop if there is less than 20 MB of free disk space available on the server. This default setting is adequate for servers in most environments, but you can modify this setting to ensure sufficient free disk space is available for other applications on a server. For information on how to modify this setting, refer to the "DhcpLogMinSpaceOnDisk" topic in the *Windows 2000 Server Resource Kit* at:
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/regentry/46692.asp.

The registry settings described in this article also apply to DHCP running on Windows Server 2003.

Protect Against DHCP Denial of Service Attacks

Because DHCP servers are critical resources that provide client access to the network, they could be prime targets for a DoS attack. If a DHCP server is attacked and is no longer able to service DHCP requests, DHCP clients will eventually be unable to acquire leases. Those clients will then lose their existing IP lease, and the ability to access network resources.

It would not be very difficult to write an attack tool script to request all available addresses on a DHCP server. This would exhaust the pool of available IP addresses for subsequent, legitimate requests from DHCP clients. It is also possible for a malicious user to configure all DHCP IP addresses on the network adapter of a computer they administer, thus causing the DHCP server to detect IP address conflicts for all addresses in its scope, and to refuse to allocate DHCP leases.

Furthermore, as with all other network services, a DoS attack—for example, CPU exhaustion or filling the request buffer of the DHCP listener—that exhausts the DHCP server's ability to respond to legitimate traffic, could make it impossible for clients to requests leases and renewals. By properly designing the DHCP services in an environment, this can be avoided.

Configuring DHCP servers in pairs, and following the best practice 80/20 Rule—that is, splitting DHCP server scopes between servers so that 80 percent of the addresses are distributed by one DHCP server and 20 percent by another—assists with mitigating the impact of these types of attacks by ensuring that clients can continue receiving IP address configuration in the event of a server failure. For more information on the 80/20 rule and the DHCP protocol, see the DHCP protocol topic in the Windows 2000 Server Resource Kit at: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/cnet/cncb_dhc_ogjw.asp.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is by default disabled on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in **Administrator** account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on infrastructure servers:**

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built–in **Administrator** account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that can be created on DHCP servers in the High Security environment defined in this guide.

Table 5.3: DHCP Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
OnePoint Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
DHCP Server	UDP	68	67	ANY	ME	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

The following table lists all of the IPSec filters that could be created on WINS servers in the High Security environment defined in this guide.

Table 5.4: WINS Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
one point Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
WINS Resolution Server	TCP	ANY	1512	ANY	ME	ALLOW	YES
	UDP	ANY	1512	ANY	ME	ALLOW	YES
WINS Replication Client	TCP	ANY	42	ME	WINS Replication Partner	ALLOW	YES
	UDP	ANY	42	ME	WINS Replication Partner	ALLOW	YES

(continued)

WINS Replication Server	TCP	ANY	42	WINS Replication Partner	ME	ALLOW	YES
	UDP	ANY	42	WINS Replication Partner	ME	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The tables above represent the base ports that should be opened for the server to perform its role – specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. Opening additional ports will make the infrastructure servers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Because of the large amount of interaction between a domain member and the domain controller, in particular RPC and authentication traffic, all communications are permitted between an infrastructure server and all domain controllers. Traffic could be further limited, but most environments would require the creation of dozens of additional filters in order for the filters to effectively protect the server. This would make it very difficult to implement and manage IPSec policies. Similar rules should be created for each of the domain controllers an infrastructure server will interact with. To increase the reliability and availability of infrastructure servers, this will often include adding rules for all domain controllers in the environment.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client — the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand – alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Included with this guide are .cmd files that simplify the creation of the IPSec filters prescribed for infrastructure servers. The PacketFilters-DHCP.cmd and PacketFilters-WINS.cmd files both use the NETSH command to create the appropriate filters. These .cmd files must be modified to include the IP addresses of domain controllers in your environment. The scripts contain placeholders for two domain controllers to be added. Additional domain controllers can be added to these scripts if desired. This list of IP addresses for the domain controllers must be kept up to date. Placeholders are included only for WINS replication partners. The appropriate WINS replication partners must also be specified in the PacketFilters-WINS.cmd file for WINS replication to take effect.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP. Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings for securing DHCP and WINS servers across the three environments defined in this guide. Most of the settings for these roles are applied through the MSBP. The primary goal of the incremental .inf files for the DHCP and WINS servers is to enable the necessary services for these roles to fully function while keeping them well secured.

While the MSBP provides a great level of security, a few other considerations for the infrastructure roles were discussed. Primarily these included enabling logging and optionally using IPSec filters to block unauthorized network traffic to these computers.

More Information

The following information sources were the latest available on topics closely related to infrastructure servers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For the latest on changes in Windows Server 2003 to DHCP logging, see: http://support.microsoft.com/default.aspx?scid=328891.

For more information on DHCP servers in an Active Directory domain, see "How To: Install and Configure a DHCP Server in an Active Directory Domain in Windows Server 2003," at: http://support.microsoft.com/default.aspx?scid=323360.

For more information on DHCP, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/tcpip/part2/tcpch04.asp

For more information on WINS, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/featfunc/nt5wins.asp.

For information on installing Wins in Windows Server 2003, see "How To: Install WINS in Windows Server 2003," at: http://support.microsoft.com/default.aspx?scid=323429.

6

Hardening File Servers

Overview

There are some challenges to further hardening file servers, since the most essential services they provide are the ones that require the Microsoft® Windows® Network Basic Input/Output System (NetBIOS) related protocols. The protocols for Server Message Block (SMB) and Common Internet File System (CIFS) can provide rich information to unauthenticated users. Therefore, it is often recommended to disable file servers from using these protocols in high security Windows environments. Nevertheless, disabling these protocols can make accessing file servers difficult for both administrators and the users in your environment.

The following sections of this chapter detail the areas in which file servers can benefit from security settings not applied by the Member Server Baseline Policy (MSBP). For more information about the MSBP, see Chapter 3, "Creating a Member Server Baseline."

Audit Policy Settings

The Audit Policy settings for file servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all file servers.

User Rights Assignments

The User Rights Assignments for file servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all appropriate User Rights Assignments are uniformly configured across file servers.

Security Options

The Security Options settings for file servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all relevant Security Option settings are uniformly configured across file servers.

Event Log Settings

The Event Log settings for file servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline."

System Services

Any service or application is a potential point of attack, and therefore any unneeded services or executable files should be disabled or removed. In the MSBP, optional services, as well as any unnecessary services, are disabled.

There are additional services that are often enabled on file servers running Microsoft Windows Server™ 2003 that are not essential. The use and security of these services is frequently the subject of debate. For this reason, recommendations for file servers in this guide may not be applicable to your environment. Adjust the File Server Group Policy recommendations as needed to meet the requirements of your organization.

Distributed File System

Table 6.1: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
DFS	Automatic	Disabled	Disabled	Disabled

The **Distributed File System** (DFS) service manages logical volumes distributed across a local area network (LAN) or wide area network (WAN) and is required for the Microsoft Active Directory® SYSVOL share. DFS is a distributed service that integrates disparate file shares into a single logical namespace.

This namespace is a logical representation of the network storage resources that are available to users on the network. Disabling the DFS service prevents users from accessing network data through a logical namespace, and requires them to know the names of all the servers and shares in the environment to access them.

The File Server Incremental Group Policy disables the DFS service to minimize the attack surface of the file servers in your environment. For this reason, the **Distributed File System** setting is configured to **Disabled** in all of the security environments defined in this guide.

Note: Organizations using DFS on file servers to simplify accessing distributed resources must modify the File Server Incremental Group Policy or create a new GPO to enable this service.

File Replication Service

Table 6.2: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
NTFRS	Manual	Disabled	Disabled	Disabled

The **File Replication Service** (FRS) enables files to be automatically copied and maintained simultaneously on multiple servers. FRS is the automatic file replication service in Windows® 2000 and the Windows Server™ 2003 family. The service replicates the system volume (Sysvol) on all domain controllers. In addition, this service can be configured to replicate files among alternate targets associated with the fault–tolerant DFS. If this service is disabled, file replication will not occur and server data will not be synchronized.

The File Server Incremental Group Policy disables the FRS to minimize the attack surface for to the file servers in your environment. For this reason, the **File Replication Service** setting is configured to **Disabled** in all of the security environments defined in this guide.

Note: Organizations using FRS on file servers to replicate data across multiple servers must modify the File Server Incremental Group Policy or create a new GPO to enable this service.

Additional Security Settings

The security settings applied through the MSBP provide a great deal of enhanced security for file servers. Nevertheless, there are a few additional considerations that should be taken into account. These steps cannot be completed via Group Policy and should be performed manually on all file servers.

Securing Well Known Accounts

Microsoft Windows Server™ 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is disabled by default on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in **Administrator** account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on file servers:**

1. Rename the **Administrator** and **Guest** accounts, and then change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built–in **Administrator** account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings in Group Policy.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that could be created on file servers in the High Security environment defined in this guide.

Table 6.3: File Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
CIFS Server	TCP	ANY	445	ANY	ME	ALLOW	YES
	UDP	ANY	445	ANY	ME	ALLOW	YES
NetBIOS Server	TCP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	138	ANY	ME	ALLOW	YES
	TCP	ANY	139	ANY	ME	ALLOW	YES
OnePoint Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role–specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. Opening additional ports will make the file servers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Because of the large amount of interaction between a domain member and the domain controller, in particular RPC and authentication traffic, all communications are permitted between a file server and all domain controllers. Traffic could be further limited, but most environments would require the creation of dozens of additional filters in order for the filters to effectively protect the server. This would make it very difficult to implement and manage IPSec policies. Similar rules should be created for each of the domain controllers a file server will interact with. To increase the reliability and availability of file servers, this will often include adding rules for all domain controllers in the environment.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client—the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand–alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for a file server. The **PacketFilters-File.cmd** file uses the NETSH command to create the appropriate filters. This .cmd file must be modified to include the IP addresses of domain controllers in an environment. The script contains place holders for two domain controllers to be added. Additional domain controllers can be added if desired. This list of IP addresses for the domain controllers must be kept up to date.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.* Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings for securing file servers across the three environments defined in this guide. Most of the settings discussed are configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the MSBP can be linked to the appropriate organizational units (OUs) containing the File servers to provide additional security based on the services these servers provide.

A few of the settings discussed cannot be applied using Group Policy. In these cases, details on configuring these settings manually have been provided. Details for creating and applying IPSec filters that can control the type of network traffic that can communicate with file servers have been included.

More Information

The following information sources were the latest available on topics closely related to file servers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For more information on file servers, see "Technical Overview of Windows Server 2003 File Services," at: http://www.microsoft.com/windowsserver2003/techinfo/overview/file.mspx.

For more information on DFS, see the white paper on "Distributed File System," at: http://www.microsoft.com/windows2000/techinfo/howitworks/fileandprint/dfsnew.asp.

For more information on FRS, see "File Replication Service," at: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/distrib/dsdh_frs_BNYR.asp.

For more information on IPSec filtering, see "How To: Use IPSec IP Filter Lists in Windows 2000," at: http://support.microsoft.com/default.aspx?scid=313190.

7

Hardening Print Servers

Overview

This chapter focuses on the challenges of further hardening print servers, since the most essential services they provide are the ones that require the Microsoft® Windows® Network Basic Input/Output System (NetBIOS) related protocols. The protocols for Server Message Block (SMB) and Common Internet File System (CIFS) can provide rich information to unauthenticated users, therefore it is often recommended to disable print servers from using these protocols in high–security Windows environments. Nevertheless, disabling these protocols can make accessing these servers difficult for both administrators and users in your environment.

The following sections in this chapter detail the areas in which print servers can benefit from security settings not applied by the Member Server Baseline Policy (MSBP). For more information about the MSBP, see Chapter 3, "Creating a Member Server Baseline."

Audit Policy Settings

The Audit Policy settings for print servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all print servers.

User Rights Assignments

The User Rights Assignments for print servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all appropriate User Rights Assignments are uniformly configured across print servers.

Security Options

Most Security Options settings for print servers in the three environments defined in this guide are configured via the MSBP. For more information about MSBP, see Chapter 3, "Creating a Member Server Baseline." Differences between the MSBP and the Incremental IIS Group Policy are described in the following section.

Microsoft network server: Digitally sign communications (always)

Table 7.1: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Disabled	Disabled

The **Microsoft network server: Digitally sign communications (always)** setting determines whether packet signing is required by the SMB server component. The SMB protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent man–in–the–middle attacks that modify SMB packets in transit, the SMB protocol supports SMB packet digital signing. This setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

Although this setting is disabled by default, the MSBP enables this setting for servers in the High Security environment defined in this guide. Not disabling this setting on print servers allows users to print, but not view the print queue. Users attempting to view the print queue will receive an access denied message. For these reasons, the **Microsoft network server: Digitally sign communications (always)** setting is configured to **Disabled** for print servers in all three environments defined in this guide.

Event Log Settings

The Event Log settings for print servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline."

System Services

Any service or application is a potential point of attack, and therefore any unneeded services or executable files should be disabled or removed. In the MSBP, these optional services, as well as any other unnecessary services, are disabled. The following section details services that must be enabled on print servers.

Print Spooler

Table 7.2: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
Print Spooler	Automatic	Automatic	Automatic	Automatic

The **Print Spooler** service manages all local and network print queues and controls all print jobs. The **Print Spooler** service is the center of the Windows printing subsystem and communicates with printer drivers and input/output (I/O) components.

Print servers rely on the proper operation of the **Print Spooler** service. This service must be configured to run in order for a print server to process print jobs for clients. Using Group Policy to secure and set the startup mode of the **Print Spooler** service grants access solely to server administrators, and prevents the service from being configured or operated by unauthorized or malicious users. Group Policy will also prevent administrators from inadvertently disabling the service. For these reasons, the **Print Spooler** setting is configured to **Automatic** in the three security environments defined in this guide.

Additional Security Settings

The security settings applied through the MSBP provide a great deal of enhanced security for print servers. Nevertheless, there are a few additional considerations that should be taken into account. These steps cannot be completed via Group Policy and should be performed manually on all print servers.

Securing Well Known Accounts

Microsoft Windows Server™ 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is disabled by default on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in **Administrator** account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on print servers:**

1. Rename the **Administrator** and **Guest** accounts, and then change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built–in **Administrator** account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings in Group Policy.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that can be created on print servers in the High Security environment defined in this guide.

Table 7.3: Print Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
CIFS Server	TCP	ANY	445	ANY	ME	ALLOW	YES
	UDP	ANY	445	ANY	ME	ALLOW	YES
NetBIOS Server	TCP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	138	ANY	ME	ALLOW	YES
	TCP	ANY	139	ANY	ME	ALLOW	YES
OnePoint Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role–specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. For example, port 515 would need to be opened on print servers hosting LPR printers. Opening additional ports will make the print servers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Because of the large amount of interaction between a domain member and the domain controller, in particular RPC and authentication traffic, all communications are permitted between a print server and all domain controllers. Traffic could be further limited, but most environments would require the creation of dozens of additional filters in order for the filters to effectively protect the server. This would make it very difficult to implement and manage IPSec policies. Similar rules should be created for each of the domain controllers a print server will interact with. To increase the reliability and availability of print servers, this will often include adding rules for all domain controllers in the environment.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client—the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand–alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for a print server. The **PacketFilters-Print.cmd** file uses the NETSH command to create the appropriate filters. This .cmd file must be modified to include the IP addresses of domain controllers in the environment. The script contains place holders for two domain controllers to be added. Additional domain controllers can be added if desired. This list of IP addresses for the domain controllers must be kept up to date.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.* Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings for securing print servers across the three client environments defined in this guide. Most of the settings discussed are configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the MSBP is linked to the appropriate organizational units (OUs) containing the print servers to provide additional security based on the services these servers provide.

A few of the settings discussed cannot be applied using Group Policy. In these cases, details on configuring these settings manually have been provided. Details on creating and applying IPSec filters that control the type of network traffic that can communicate with print servers also have been included.

More Information

The following information sources were the latest available on topics closely related to print servers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For an overview on print servers, see the "Technical Overview of Windows Server 2003 Print Services," at: http://www.microsoft.com/windowsserver2003/techinfo/overview/print.mspx.

For more information on print servers, see "What's New in File and Print Services," at: http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx.

For more information on IPSec filtering, see "How To: Use IPSec IP Filter Lists in Windows 2000," at: http://support.microsoft.com/default.aspx?scid=313190.

8

Hardening IIS Servers

Overview

This chapter focuses on the guidance and procedures required to harden the IIS servers in your environment. To provide comprehensive security for Web servers and applications within an organization's corporate intranet, each Microsoft® Internet Information Services (IIS) server, as well as each Web site and application running on these servers, should be protected from client computers that can connect to them. The Web sites and applications running on each of these IIS servers should also be protected from the Web sites and applications running on the other IIS servers within a corporate intranet.

In order to take a more proactive stance against malicious users and attackers, IIS is by default not installed on members of the Microsoft Windows® Server™ 2003 family. IIS initially installs in a highly secure, "locked" mode. For example, IIS will by default initially only serve static content. Features such as Active Server Pages (ASP), ASP.NET, Server Side Includes (SSI), Web Distributed Authoring and Versioning (WebDAV) publishing, and Microsoft FrontPage® Server Extensions will not work until an administrator enables them. These features and services can be enabled through the Web Service Extensions node in Internet Information Services Manger (IIS Manager).

IIS Manager is a graphical user interface (GUI) designed to facilitate administration of IIS. It includes resources for file and directory management, and configuration of application pools, as well as security, performance, and reliability features.

The following sections of this chapter detail a variety of security hardening settings that should be implemented to enhance the security of IIS servers hosting HTML content within a corporate intranet. However, to ensure the IIS servers stay secure, security monitoring, detection, and response procedures should also be implemented.

Audit Policy Settings

The Audit Policy settings for IIS servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all IIS servers.

User Rights Assignments

Most User Rights Assignments for IIS servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." Differences between the MSBP and the Incremental IIS Group Policy are described in the following section.

Deny access to this computer from the network

Table 8.1: Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
SUPPORT_388945a0	ANONOYMOUS LOGON; Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	ANONOYMOUS LOGON; Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	ANONOYMOUS LOGON; Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts

Note: ANONOYMOUS LOGON, Built – in Administrator, Support_388945a0, Guest, and all NON – operating system service accounts are not included in the security template. These accounts and groups have unique security identifiers (SIDs) for each domain in your organization. Therefore, they must be added manually.

The **Deny access to this computer from the network** setting determines which users are prevented from accessing a computer over the network. This setting will deny a number of network protocols, including server message block (SMB) – based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP), and Component Object Model Plus (COM+).This setting overrides the **Access this computer from the network** setting when a user account is subject to both policies. Configuring this user right for other groups could limit the ability of users to perform delegated administrative tasks in your environment.

In Chapter 3, "Creating a Member Server Baseline," this guide recommends including the **Guests** group in the list of users and groups assigned this right to provide the highest level of security possible. Nevertheless, the IUSR account used for anonymous access to IIS is by default a member of the **Guests** group. This guide recommends removing the **Guests** group from the Incremental IIS Group Policy to ensure anonymous access to IIS servers can be configured when necessary. For these reasons, the **Deny access to this computer from the network** setting is configured to include **ANONOYMOUS LOGON; Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts** for IIS servers in all three environments defined in this guide.

Security Options

The Security Options settings for IIS servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant Security Options are uniformly configured across IIS servers.

Event Log Settings

The Event Log settings for IIS servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure the appropriate Event Log settings are uniformly configured across IIS servers in an enterprise.

System Services

In order for IIS to add Web server functionality to Microsoft Windows Server™ 2003, the following three services must be enabled. The Incremental IIS Group Policy ensures these services are configured to start automatically.

Note: The MSBP disables several other IIS related services. FTP, SMTP, and NNTP are some of the services disabled by the MSBP. The incremental IIS Group Policy must be modified if any of these services are to be enabled on IIS servers in any of the three environments defined in this guide.

HTTP SSL

Table 8.2: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
HTTPFilter	Manual	Automatic	Automatic	Automatic

The **HTTP SSL** service enables IIS to perform Secure Sockets Layer (SSL) functions. SSL is an open standard for establishing a secure communications channel to prevent the interception of critical information, such as credit card numbers. Primarily, it enables secure electronic financial transactions on the World Wide Web, although it is designed to work on other Internet services as well.

If the HTTP SSL service is stopped, IIS will not perform SSL functions. Disabling this service causes any services that explicitly depend on it to fail. Using Group Policy to secure and set the startup mode of a service grants access solely to server administrators, thus preventing the service from being configured or operated by unauthorized or malicious users. The Group Policy will also prevent administrators from inadvertently disabling the service. For these reasons, the **HTTP SSL** setting is configured to **Automatic** for IIS servers in all three environments defined in this guide.

IIS Admin Service

Table 8.3: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
IISADMIN	Not installed	Automatic	Automatic	Automatic

The **IIS Admin Service** allows administration of IIS components such as File Transfer Protocol (FTP), Application Pools, Web sites, Web service extensions and both Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) virtual servers.

The **IIS Admin Service** must be running for an IIS server to provide Web, FTP, NNTP, and SMTP services. If this service is disabled, IIS cannot be configured, and requests for any Web services will not succeed. Using Group Policy to secure and set the startup mode of a service grants access solely to server administrators, thus preventing the service from being configured or operated by unauthorized or malicious users. The Group Policy will also prevent administrators from inadvertently disabling the service. For these reasons, the **IIS Admin Service** setting is configured to **Automatic** for IIS servers in the three environments defined in this guide.

World Wide Web Publishing Service

Table 8.4: Settings

Service Name	Member Server Default	Legacy Client	Enterprise Client	High Security
W3SVC	Not installed	Automatic	Automatic	Automatic

The **World Wide Web Publishing Service** provides Web connectivity and administration of Web sites through the IIS snap–in.

The **World Wide Web Publishing Service** must be running for an IIS server to provide Web connectivity and administration through the IIS Manager. Using Group Policy to secure and set the startup mode of a service grants access solely to server administrators, thus preventing the service from being configured or operated by unauthorized or malicious users. The Group Policy will also prevent administrators from inadvertently disabling the service. For these reasons, the **World Wide Web Publishing Service** setting is configured to **Automatic** for IIS servers in all three environments defined in this guide.

Additional Security Settings

After installing Windows Server 2003 and IIS, IIS by default transmits only static Web content. When Web sites and applications contain dynamic content, or require one or more additional IIS components, each additional IIS feature must be individually enabled. However, care should be taken during this process to ensure that the attack surface of each IIS server in your environment is minimized. If the Web sites in your organization are comprised of static content and do not require any other IIS components, then the default IIS configuration is sufficient to minimize the attack surface of the IIS servers in your environment.

The security settings applied through the MSBP provide a great deal of enhanced security for IIS servers. Nevertheless, there are a few additional considerations and procedures that should be taken into account. These steps cannot be completed via Group Policy and should be performed manually on all IIS servers.

Installing Only Necessary IIS Components

IIS 6.0 includes other components and services in addition to the **World Wide Web Publishing Service**, such as the services for FTP and SMTP. IIS components and services are installed and enabled using the Windows Components Wizard Application Server that can be launched by double–clicking **Add or Remove Programs** in the **Control Panel**. After installing IIS, all necessary IIS components and services required by Web sites and applications must be enabled.

▶ **To install Internet Information Services (IIS) 6.0:**

1. On the **Control Panel**, double–click **Add or Remove Programs**.
2. Click the **Add/Remove Windows Components** button to start the Windows Components Wizard.
3. In the **Components** list, click **Application Server**, and then **Details**.
4. In the **Application Server** dialog box, under **Subcomponents of Application Server**, click **Internet Information Services (IIS)**, and then **Details**.
5. In the Internet Information Services (IIS) dialog box, in the Subcomponents of Internet Information Services (IIS) list, do either of the following:
   - To add optional components, select the check box next to the component that you want to install.
   - To remove optional components, clear the check box next to the component that you want to remove.
6. Click **OK** until you return to the Windows Component Wizard.
7. Click **Next**, and then **Finish**.

Only essential IIS components and services required by Web sites and applications should be enabled. Enabling unnecessary components and services increases the attack surface of an IIS server.

The following illustrations and tables show the location and suggested settings for IIS components.

The subcomponents in the **Application Server** dialog box appear as follows:

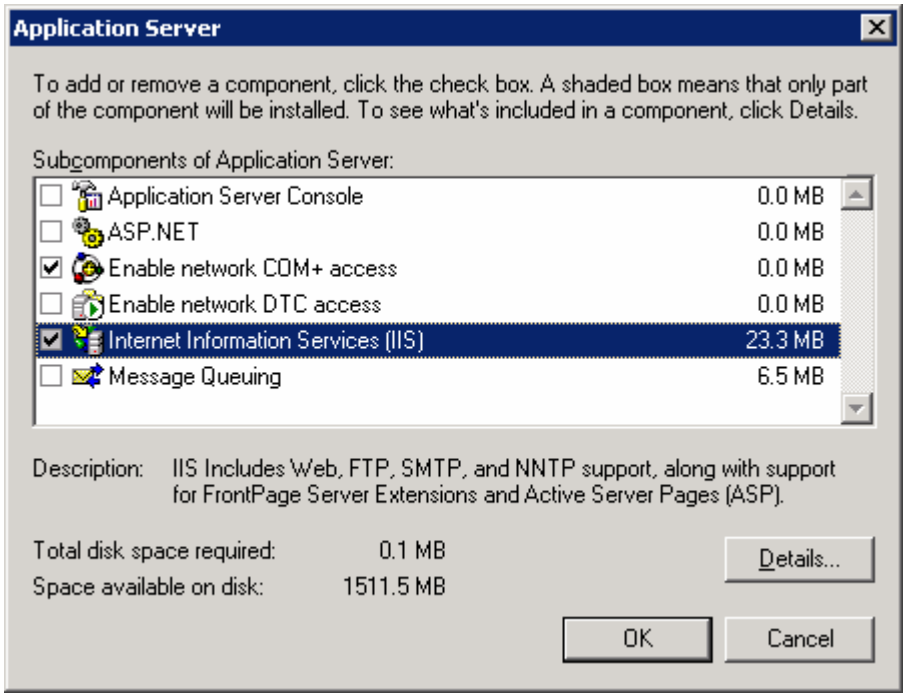

Figure 8.1
Application Server subcomponents

The following table briefly describes the Application Server subcomponents, and provides recommendations for when to enable them.

Table 8.5: Application Server Subcomponents

Component Name in UI	Setting	Setting Logic
Application Server Console	Disabled	Provides a Microsoft Management Console (MMC) snap – in that allows for all the Web Application Server components to be administered. This component is not required on a dedicated IIS server because IIS Server Manager can be used.
ASP.NET	Disabled	Provides support for ASP.NET applications. Enable this component when an IIS server runs ASP.NET applications.
Enable network COM+ access	Enabled	Allows an IIS server to host COM+ components for distributed applications. Required for FTP, BITS server extension, World Wide Web Service, and IIS Manager among others.
Enable network DTC access	Disabled	Allows an IIS server to host applications that participate in network transactions through Distributed Transaction Coordinator (DTC). Disable this component unless the applications running on the IIS server require it.
Internet Information Services (IIS)	Enabled	Provides basic Web and FTP services. This component is required for dedicated IIS servers.
Message Queuing	Disabled	Note: If this component is not enabled, then all subcomponents are disabled.

The subcomponents in the **Internet Information Services (IIS)** dialog box appear as follows:

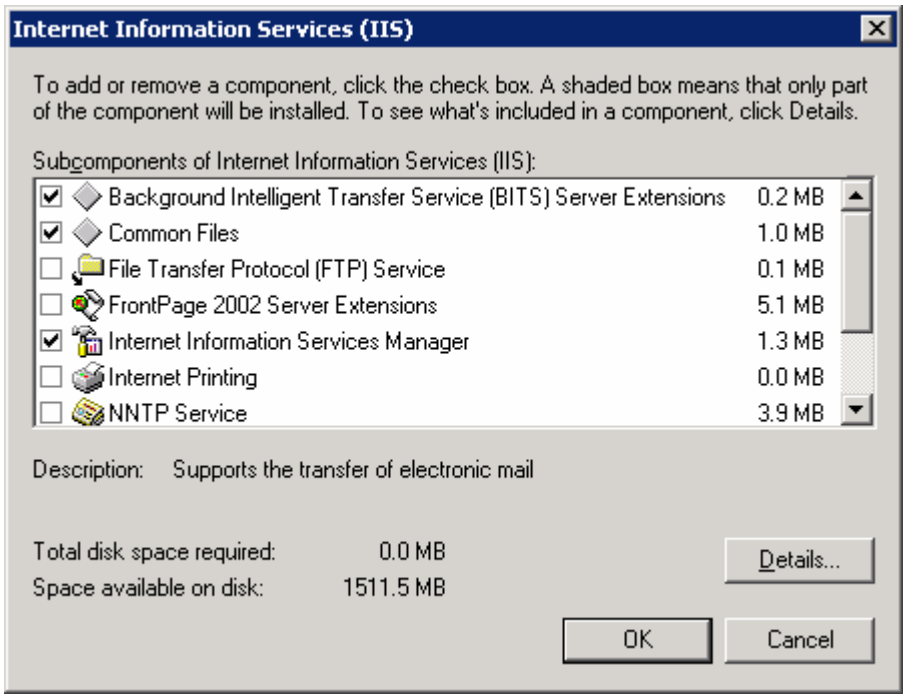

Figure 8.2
IIS subcomponents

The following table briefly describes the IIS subcomponents, and provides recommendations for when to enable them.

Table 8.6: IIS Subcomponents

Component Name in UI	Setting	Setting Logic
Background Intelligent Transfer Service (BITS) server extension	Enabled	BITS is a background file transfer mechanism used by Windows Update and Automatic Update. This component is required when Windows updates or Automatic updates are used to automatically apply service packs and hotfixes to an IIS server.
Common Files	Enabled	IIS requires these files and they must always be enabled on IIS servers.
File Transfer Protocol (FTP) Service	Disabled	Allows IIS servers to provide FTP services. This service is not required for dedicated IIS servers.
FrontPage 2002 Server Extensions	Disabled	Provides FrontPage support for administering and publishing Web sites. Disable on dedicated IIS servers when no Web sites use FrontPage extensions.
Internet Information Services Manager	Enabled	Administrative interface for IIS.
Internet Printing	Disabled	Provides Web – based printer management and allows printers to be shared over HTTP. This is

Component Name in UI	Setting	Setting Logic
		not required on dedicated IIS servers.
NNTP Service	Disabled	Distributes, queries, retrieves, and posts Usenet news articles on the Internet. This component is not required on dedicated IIS servers.
SMTP Service	Disabled	Supports the transfer of electronic mail. This component is not required on dedicated IIS servers.
World Wide Web Service	Enabled	Provides Web services, static, and dynamic content to clients. This component is required on dedicated IIS servers.

The subcomponents in the **Message Queuing** dialog box appear as follows:

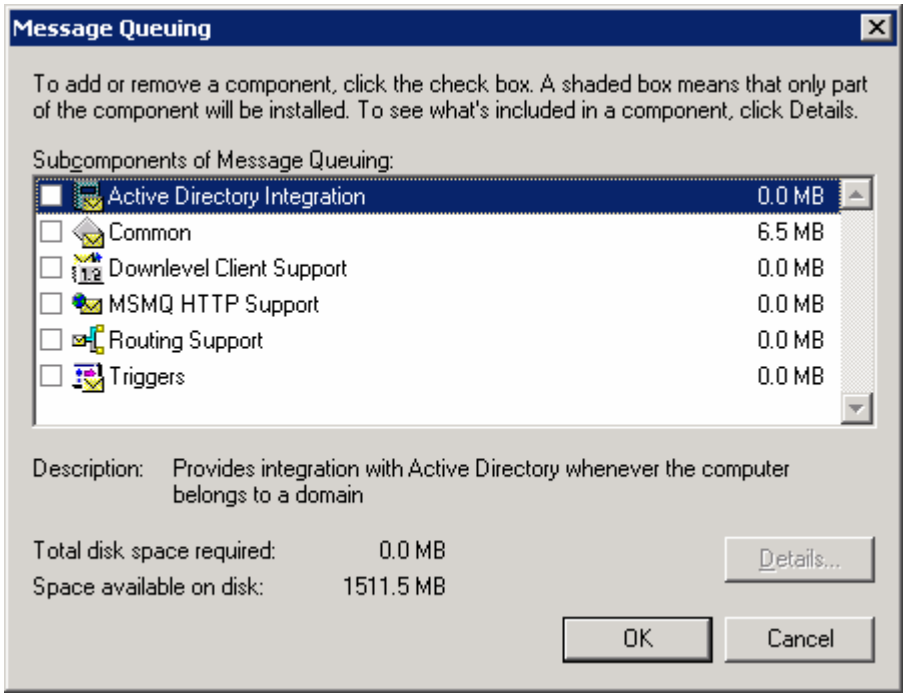

Figure 8.3
Message Queuing subcomponents

The following table briefly describes the Message Queuing subcomponents, and provides recommendations for when to enable them.

Table 8.7: Message Queuing Subcomponents

Component Name in UI	Installation Option	Setting Logic
Active Directory Integration	Disabled	Provides integration with Microsoft Active Directory® whenever an IIS server belongs to a domain. This component is required when Web sites and applications running on IIS servers use Microsoft Message Queuing (MSMQ).
Common	Disabled	Required by MSMQ. This component is required when Web sites and applications running on IIS servers use MSMQ.
Downlevel Client Support	Disabled	Provides access to Active Directory and site recognition for downstream clients. This component is required when an IIS server's Web sites and applications use MSMQ.
MSMQ HTTP Support	Disabled	Provides the sending and receiving of messages over the HTTP transport. This component is required when an IIS server's Web sites and applications use MSMQ.
Routing support	Disabled	Provides store – and – forward messaging as well as efficient routing services for MSMQ. This component is required when Web sites and applications running on IIS servers use MSMQ.

The subcomponents in the **Background Intelligent Transfer Service (BITS) Server Extensions** dialog box appear as follows:

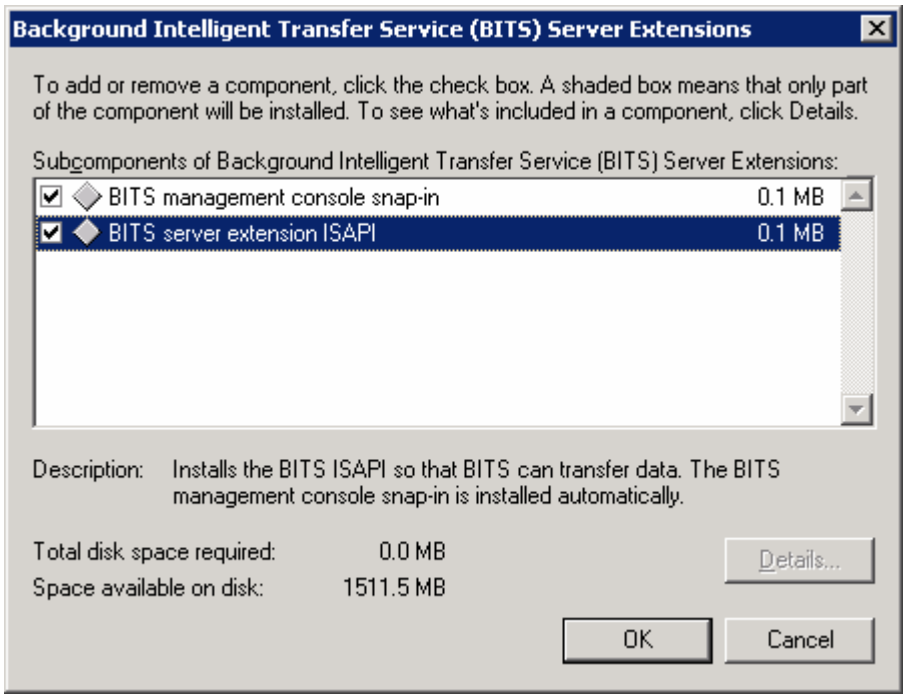

Figure 8.4
Background Intelligent Transfer Service (BITS) Server Extensions *subcomponents*

The following table briefly describes the Background Intelligent Transfer Service (BITS) Server Extensions subcomponents, and provides recommendations for when to enable them.

Table 8.8: Background Intelligent Transfer Service (BITS) Server Extensions subcomponents

Component Name in UI	Installation Option	Setting Logic
BITS management console snap – in	Enabled	Installs an MMC snap – in for administering BITS. Enable this component when the BITS server extension for Internet Server Application Programming Interface (ISAPI) is enabled.
BITS server extension ISAPI	Enabled	Installs the BITS ISAPI so that an IIS server can transfer data using BITS. This component is required when either Windows Update or Automatic Update is used to automatically apply service packs and hotfixes to IIS servers. Disable if Windows Update or Automatic Update are not being used.

The subcomponents in the **World Wide Web Service** dialog box appear as follows:

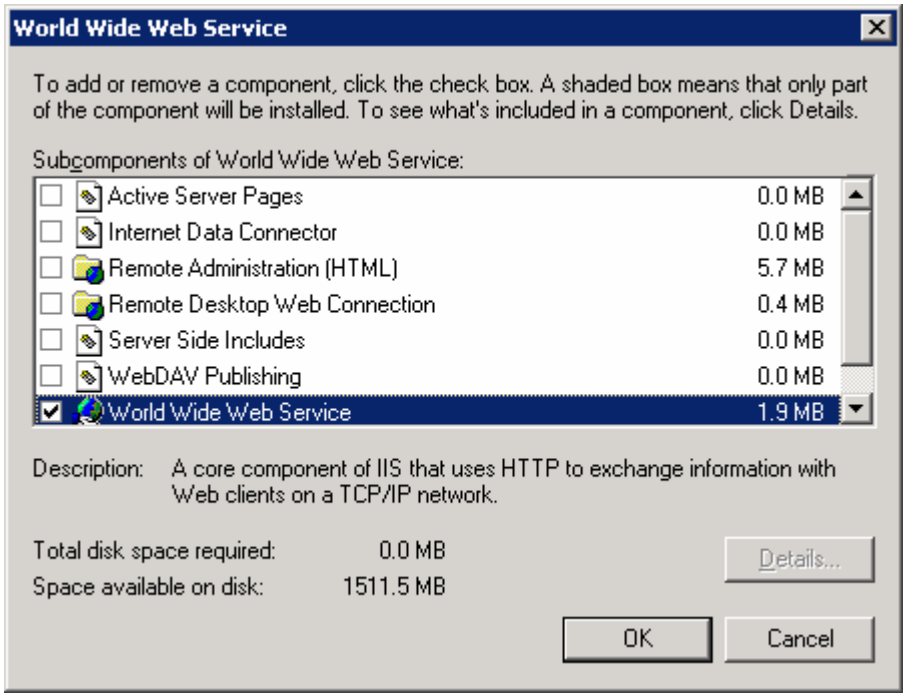

Figure 8.5
World Wide Web Service *subcomponents*

The following table briefly describes the World Wide Web Service subcomponents, and provides recommendations for when to enable them.

Table 8.9: World Wide Web Service subcomponents

Component Name in UI	Installation Option	Setting Logic
Active Server Pages	Disabled	Provides support for ASP. Disable this component when no Web sites or applications on IIS servers use ASP, or disable it using the Web service extensions. For more information, see the section on “Enabling Only Essential Web Service Extensions” in this chapter.
Internet Data Connector	Disabled	Provides support for dynamic content provided through files with .idc extensions. Disable this component when no Web sites or applications running on IIS servers include files with .idc extensions, or disable it using the Web service extensions. For more information, see the section on “Enabling Only Essential Web Service Extensions” in this chapter.

(continued)

Remote Administration (HTML)	Disabled	Provides an HTML interface for administering IIS. Use IIS Manager instead to provide easier administration and to reduce the attack surface of an IIS server. This feature is not required on dedicated IIS servers.
Remote Desktop Web Connection	Disabled	Includes Microsoft ActiveX® control and sample pages for hosting Terminal Services client connections. Use IIS Manager instead to provide easier administration and to reduce the attack surface of an IIS server. Not required on a dedicated IIS server.
Server – Side Includes	Disabled	Provides support for .shtm, .shtml, and .stm files. Disable this component when no Web sites or applications running on IIS server use include files with these extensions.
WebDAV	Disabled	WebDAV extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web. Disable this component on dedicated IIS servers or disable it using the Web service extensions. For more information, see the section on "Enabling Only Essential Web Service Extensions" in this chapter.
World Wide Web Service	Enabled	Provides Web services, static, and dynamic content to clients. This component is required on dedicated IIS servers.

Enabling Only Essential Web Service Extensions

Many Web sites and applications running on IIS servers have extended functionality that goes beyond static pages, including the ability to generate dynamic content. Any dynamic content served or extended through features provided by an IIS server is accomplished using Web service extensions.

Enhanced security features in IIS 6.0 allow individual Web service extensions to be enabled or disabled. After a new installation, IIS servers will transmit only static content. Dynamic content capabilities can be enabled through the Web Service Extensions node in IIS Manager. These extensions include ASP.NET, SSI, WebDAV, and FrontPage Server Extensions.

Enabling all Web service extensions ensures the highest possible compatibility with existing applications; however, this also creates a security risk because when all extensions are enabled, the attack surface of IIS increases by enabling functionality that may be unnecessary for the IIS servers in your environment.

In order to reduce the attack surface of IIS servers as much as possible, only necessary Web service extensions should be enabled on IIS servers in the three environments defined in this guide.

Enabling only the Web Service Extensions required by the Web sites and applications running on IIS servers in your environment enhances security by minimizing server functionality, and therefore reducing the attack surface of each IIS server.

The following table lists predefined Web Service Extensions, and provides details on when to enable each extension.

Table 8.10: Enabling Web Service Extensions

Web Service Extension	Enable Extension When
Active Server Pages	One or more Web sites and applications running on IIS servers contain ASP content.
ASP.NET v1.1.4322	One or more Web sites and applications running on IIS servers contain ASP.NET content.
FrontPage Server Extensions 2002	One or more Web sites running on IIS servers use FrontPage Extensions.
Internet Data Connector (IDC)	One or more Web sites and applications running on IIS servers use IDC to display database information (This content includes .idc and .idx files).
Server Side Includes (SSI)	One or more Web sites running on IIS servers use SSI directives to instruct IIS servers to insert reusable content (for example, a navigation bar, a page header or footer) into different Web pages.
Web Distributed Authoring and Versioning (WebDav)	WebDAV support is required on IIS servers for clients to transparently publish and manage web resources.

Placing Content on a Dedicated Disk Volume

IIS stores files for its default Web site in the <systemroot>\inetpub\wwwroot, where <systemroot> is the drive on which the Windows Server 2003 operating system is installed.

Place all files and folders that make up Web sites and applications on dedicated disk volumes on IIS servers in the three environments defined in this guide. Placing these files and folders on a dedicated disk volume—that does not contain the operating system—on an IIS server helps prevent directory traversal attacks. Directory traversal attacks involve an attacker sending requests for a file located outside the directory structure of an IIS server.

For example, cmd.exe exists in the <systemroot>\System32 folder. An attacker could make a request to the following location:

```
..\..\Windows\system\cmd.exe in an attempt to invoke the command prompt
```

If the Web site content is on a separate disk volume, a directory traversal attack of this type would not work for two reasons. First, permissions on cmd.exe have been reset as part of the base build of Windows Server 2003, restricting its access to a much more limited group of users. Second, after making this change, cmd.exe does not exist on the same disk volume as the Web root, and there are currently no known methods to access commands on a different drive using such an attack.

In addition to security concerns, placing Web site and application files and folders on a dedicated disk volume makes administration tasks, such as backup and restore, easier. Furthermore, placing this type of content on a separate, dedicated physical drive can help reduce disk contention on the system volume and improve overall disk–access performance.

Setting NTFS Permissions

Windows Server 2003 examines NTFS file system permissions to determine the types of access a user or a process has on a specific file or folder.

NTFS permissions should be assigned to grant or deny access to specific users for Web sites on IIS servers in the three environments defined in this guide.

NTFS permissions should be used in conjunction with Web permissions, not in place of Web permissions. NTFS permissions affect only the accounts that have been granted or denied access to the Web site and application content. Web site permissions affect all users who access the Web site or application. If Web permissions conflict with NTFS permissions for a directory or file, more restrictive settings are applied.

Access to anonymous accounts should be explicitly denied on Web sites and applications in which anonymous access is not desired. Anonymous access occurs when a user who has no authenticated credentials accesses system resources. Anonymous accounts include the built–in **Guest** account, the **Guests** group, and **IIS Anonymous** accounts. In addition, eliminate any write access permissions to any users except those that are IIS administrators.

The following table provides some recommendations on the NTFS permissions that should be applied to the different file types on an IIS server. The different file types can be grouped in separate folders to simplify the process of applying NTFS permissions.

Table 8.11: NTFS Permissions

File Type	Recommended NTFS Permissions
CGI files (.exe, .dll, .cmd, .pl)	Everyone (execute) Administrators (full control) System (full control)
Script files (.asp)	Everyone (execute) Administrators (full control) System (full control)
Include files (.inc, .shtm, .shtml)	Everyone (execute) Administrators (full control) System (full control)
Static content (.txt, .gif, .jpg, .htm, .html)	Everyone (read–only) Administrators (full control) System (full control)

Setting IIS Web Site Permissions

IIS examines Web site permissions to determine the types of action that can occur within a Web site, such as allowing script source access or directory browsing. Web site permissions should be assigned to further secure Web sites on IIS servers in the three environments defined in this guide.

Web site permissions can be used in conjunction with NTFS permissions. They can be configured for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access a Web site that runs on an IIS server. Web site permissions can be applied using the IIS Manager snap–in.

The following table lists the Web site permissions supported by IIS 6.0, and provides a brief description explaining when to assign any given permission to a Web site.

Table 8.12: IIS 6.0 Web Site Permissions

Web Site Permission:	Permission Granted:
Read	Users can view the content and properties of directories or files. This permission is selected by default.
Write	Users can change content and properties of directories or files.
Script Source Access	Users can access source files. If Read is enabled, then source can be read; if Write is enabled, then the script source code can be changed. Script Source Access includes the source code for scripts. If neither Read nor Write is enabled, this option is not available. **Important:** When Script Source Access is enabled, users may be able to view sensitive information, such as a user name and password. They may also be able to change source code that runs on an IIS server, and seriously affect the server's security and performance.
Directory browsing	Users can view file lists and collections.
Log visits	A log entry is created for each visit to the Web site.
Index this resource	Allows Indexing Service to index resources. This allows searches to be performed on resources.
Execute	The following options determine the level of script execution for users: ● **None**—Does not allow scripts executables to run on the server. ● **Scripts only**—Allows only scripts to run on the server. ● **Scripts and Executables**—Allows both scripts and executables to run on the server.

Configuring IIS Logging

This guide recommends enabling IIS logging on IIS servers in the three environments defined in this guide.

Separate logs can be created for each Web site or application. IIS logs information beyond the scope of the event logging or performance monitoring features provided by Microsoft Windows. The IIS logs can include information such as who has visited a site, what the visitor viewed, and when the information was last viewed. IIS logs can be used to assess content popularity, identify information bottlenecks, or as resources to assist in investigating attacks.

The IIS Manager snap–in can be used to configure the log file format, the log schedule, and the exact information to be logged. To limit the size of the logs, careful planning should go into the selection of the fields that will be logged.

When IIS logging is enabled, IIS uses the W3C Extended Log File Format to create daily activity logs which are stored in the directory specified for the Web site in IIS Manager. To improve server performance, logs should be stored on a non–system striped or striped/mirrored disk volume.

Furthermore, logs can be written to a remote share over a network using a full, Universal Naming Convention (UNC) path. Remote logging allows for administrators to set up centralized log file storage and backup. However, writing the log file over the network could negatively impact server performance.

IIS logging can be configured to use several other ASCII or Open Database Connectivity (ODBC) log file formats. ODBC logging enables IIS to store activity information in a SQL database. However, it should be noted that when ODBC logging is enabled, IIS disables the kernel–mode cache. For this reason, implementing ODBC logging can degrade overall server performance.

IIS servers that host hundreds of sites can improve logging performance by enabling centralized binary logging. Centralized binary logging enables all Web sites on an IIS server to write activity information to a single log file. This can greatly increase the manageability and scalability of the IIS logging process by reducing the number of logs that need to be individually stored and analyzed. For more information on centralized binary logging, see the Microsoft TechNet topic, "Centralized Binary Logging," located at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_binary.asp.

When IIS logs are stored on IIS servers by default only server administrators have permission to access them. If a log file directory or file owner is not in the **Local Administrators** group, HTTP.sys—the kernel–mode driver in IIS 6.0—publishes an error to the NT Event log. This error indicates that the owner of the directory or file is not in the **Local Administrators** group, and that logging has been suspended for that site until the owner is added to the **Local Administrators** group, or the existing directory or log file is deleted.

Manually Adding Unique Security Groups to User Rights Assignments

Most User Rights Assignments applied via the MSBP have the proper security groups specified in the security templates that accompany this guide. However, there are a few accounts and security groups that cannot be included in the templates because their security identifiers (SIDs) are specific to individual Windows 2003 domains. User rights assignments that must be configured manually are specified below.

Warning: The following table contains values for the built – in **Administrator** account. Be careful not to confuse **Administrator** account with the built – in **Administrators** security group. If the **Administrators** security group is added to any of the deny access user rights below, you will need to log on locally to correct the mistake.

In addition, the built – in **Administrator** account may have been renamed based in some of the recommendations described in Chapter 3, "Creating a Member Server Baseline." When adding the **Administrator** account, ensure the renamed account is specified.

Table 8.13: Manually Added User Rights Assignments

Member Server Default	Legacy Client	Enterprise Client	High Security
Deny access to this computer from the network	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts

---

Warning: All non – operating system service accounts include service accounts used for specific applications across an enterprise. This does NOT include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts which are built – in accounts the operating system uses.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is by default disabled on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in Administrator account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on IIS servers:**

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built – in administrator account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings in Group Policy.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that can be created on IIS servers in the High Security environment defined in this guide.

Table 8.14: IIS Server IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
one point Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services	TCP	ANY	3389	ANY	ME	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES
Domain Member	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
HTTP Server	TCP	ANY	80	ANY	ME	ALLOW	YES
HTTPS Server	TCP	ANY	443	ANY	ME	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role–specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. Opening additional ports will make the IIS servers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Because of the large amount of interaction between a domain member and the domain controller, in particular RPC and authentication traffic, all communications are permitted between an IIS server and all domain controllers. Traffic could be further limited, but most environments would require the creation of dozens of additional filters in order for the filters to effectively protect the server. This would make it very difficult to implement and manage IPSec policies. Similar rules should be created for each of the domain controllers an IIS server will interact with. To increase the reliability and availability of IIS servers, this will often include adding rules for all domain controllers in the environment.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client—the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand–alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for an IIS server. The **PacketFilters-IIS.cmd** file uses the NETSH command to create the appropriate filters. This .cmd file must be modified to include the IP addresses of domain controllers in the environment. The script contains place holders for two domain controllers to be added. Additional domain controllers can be added if desired. This list of IP addresses for the domain controllers must be kept up to date.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.* Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings to secure IIS servers in the three environments defined in this guide. Most of the settings discussed are configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the MSBP can be linked to the appropriate organizational units (OUs) containing IIS servers in order to provide additional security based on the services these servers provide.

A few of the settings discussed cannot be applied using Group Policy. In these cases, details on configuring these settings manually have been provided. Details also were provided for creating and applying IPSec filters that control the type of network traffic that can communicate with IIS servers.

More Information

The following information sources were the latest available on topics closely related to IIS servers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For information on enabling logging in IIS 5.0, see "HOW TO: Enable Logging in IIS 5.0," at: http://support.microsoft.com/default.aspx?scid=313437.

For more information on this topic, see "Enable Logging," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_enablelogging.asp.

For information on logging site activity, see "Logging Site Activity," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_aboutlogging.asp.

For information on extended logging, see "Customizing W3C Extended Logging," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_customw3c.asp.

For information on centralized binary logging, see "Centralized Binary Logging," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_binary.asp.

For information on remote logging, see "Remote Logging," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_remote.asp.

For information about generating, viewing, or understanding security logs (auditing), visit the Microsoft TechNet site on security at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/sec_security.asp.

For additional information about IIS 6.0, visit TechNet at: http://www.microsoft.com/technet/prodtechnol/windowsnetserver/proddocs/server/iiswelcome.asp.

For more information on IPSec filtering, see "How To: Use IPSec IP Filter Lists in Windows 2000," at: http://support.microsoft.com/default.aspx?scid=313190.

9

Hardening IAS Servers

Overview

This chapter provides hardening recommendations and resources for securing Internet Authentication Service (IAS) servers running Microsoft® Windows Server™ 2003. IAS is a Remote Authentication Dial–in User Service (RADIUS) server that enables centralized management of user authentication, authorization, and accounting. IAS can be used to authenticate users in databases on Windows Server 2003, Windows NT 4.0, or Windows 2000 domain controllers. In addition, IAS supports a variety of network access servers (NAS), including Routing and Remote Access (RRAS).

The RADIUS hiding mechanism uses the RADIUS shared secret, the Request Authenticator, and the MD5 hashing algorithm to encrypt the User–Password and other attributes, such as Tunnel–Password and MS–CHAP–MPPE–Keys. RFC 2865 notes the potential need for evaluating the threat environment and determining whether additional security should be used.

You can provide additional protection for hidden attributes by using Internet Protocol Security (IPSec) with Encapsulating Security Payload (ESP) and an encryption algorithm, such as Triple DES (3DES) to provide data confidentiality for the entire RADIUS message.

Windows Server 2003 ships with default setting values that are configured to a secure state. To improve the usability of this chapter, only those settings that have been modified from the Member Server Baseline Policy (MSBP) are included here. For more information on settings in the MSBP, see Chapter 3, “Creating a Member Server Baseline.” For information on all default settings, see the companion guide *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

Note: The setting prescriptions for the IAS server role were tested for the Enterprise Client environment only. For this reason, the IPSec filter and DoS attack information specified for the majority of the other server roles in this guide is not included here.

Audit Policy

Audit Policy settings for IAS servers in the three environments defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, “Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all IAS Servers.

User Rights Assignments

User Rights Assignments for IAS servers in the three environments defined in this guide are also configured via the MSBP. For more information on the MSBP, see Chapter 3, “Creating a Member Server Baseline." The MSBP settings ensure that appropriate access to IAS servers is uniformly configured across an enterprise.

Security Options

The Security Options settings for IAS servers in the three environments defined in this guide are also configured via the MSBP. For more information on the MSBP, see Chapter 3, “Creating a Member Server Baseline." The MSBP settings ensure that appropriate access to IAS servers is uniformly configured across an enterprise.

Event Log

The Event Log settings for IAS servers in the three environments defined in this guide are also configured via the MSBP. For more information on the MSBP, see Chapter 3, “Creating a Member Server Baseline."

System Services

Any service or application is a potential point of attack, and therefore any unneeded services or executable files should be disabled or removed. In the MSBP, these optional services, as well as all other unnecessary services, are disabled.

For this reason, recommendations on the IAS server role in this guide may not be applicable to your environment. Adjust these IAS Server Group Policy recommendations as needed to meet the requirements of your organization.

IAS Service

Table 9.1: Setting

Service Name	Member Server Default	Enterprise Client
IAS	Not installed	Automatic

The **IAS Service** setting implements the IETF standard for the RADIUS protocol, which enables the use of heterogeneous network access equipment. Disabling this setting causes authentication requests to failover to a backup IAS server, if one is available. If no backup IAS servers are available, users cannot connect to the network. Disabling this service also causes any services that explicitly depend on it to fail.

The IAS Service setting is required for the IAS server role. This service must be running for an IAS server to respond to client authentication requests. Using Group Policy to secure and set the startup mode of this service grants access solely to server administrators, and thus prevents the service from being configured or operated by unauthorized or malicious users. This Group Policy will also prevent administrators from inadvertently disabling the service.

Additional Security Settings

The security settings applied through the MSBP provide a great deal of enhanced security for IAS servers. Nevertheless, there are a few additional considerations that should be taken into account. These steps cannot be performed through Group Policy, and should be done manually on all file servers.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that cannot be deleted, but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is by default disabled on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in **Administrator** account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in **Administrator** account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on IAS servers:**

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built – in administrator account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings section of Group Policy.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Summary

This chapter explained the server hardening settings required to secure IAS servers in the Enterprise Client environment defined in this guide. These settings may also work in the other environments defined in this guide, but they have not been tested or validated. The settings discussed were configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the MSBP can be linked to the appropriate organizational units (OUs) containing the IAS servers in your organization to provide additional security, based on the services provided by these servers.

More Information

The following information sources were the latest available on topics closely related to Windows Server 2003 and the IAS server role detailed in this guide at the time this product was released to the pubic.

For more information on IAS, see "Understanding IAS on Windows Server 2003," at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_understanding.asp.

For more information on IAS and security, see the TechNet article, “Security information for IAS,” at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_security_issues.asp.

For information on IAS and Firewalls on Windows Server 2003, "IAS and firewalls," at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_firewall.asp.

For information on RADIUS, see "Remote Authentication Dial In User Service (RADIUS)," at: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2865.html.

10

Hardening Certificate Services Servers

Overview

This chapter will provide you with complete guidance on securing the operating system for Microsoft® Certificate Services servers in your environment. Although this chapter includes all of the information you need to complete this task, the guidance does not provide the details to create a secure Certificate Services infrastructure in your environment or to deploy a certificate authority. These topics are covered in depth in the Microsoft Windows Server™ 2003 product documentation, the *Windows Server 2003 Resource Kit*, and in white papers on the subject that are available on the Microsoft Web site. Additional information can be found in a companion guide: *Securing Wireless LANs – a Windows Server 2003 Certificate Services Solution* available at http://go.microsoft.com/fwlink/?LinkId=14843.

Windows Server 2003 ships with default setting values that are set to a secure state. To improve the usability of this chapter, only those settings that have been modified from the Member Server Baseline Policy (MSBP) are included here. For information on settings in the MSBP, see Chapter 3, “Creating a Member Server Baseline.” For information on all default settings, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*.

You must install Microsoft Internet Information Services (IIS) on some of the Certificate Services servers in your environment in order for them to distribute Certificate Authority (CA) certificates and Certificate Revocation Lists (CRLs). IIS is also used to host the Certificate Services server Web enrollment pages, which allow non–Microsoft Windows® clients to enroll certificates. Understanding the procedures for securely installing IIS, which are covered in Chapter 8, "Hardening IIS Servers," is prerequisite to acting on the information in this chapter.

In addition, if you install IIS on your CAs, the security configuration template developed for Chapter 8 must be applied to your Certificate Services servers before configuring the prescribed settings for this server role detailed in this chapter.

Note: In simplified environments, the issuing CA server can be used to host the Web server, the CA certificate, and the CRL download points. However, consider using a separate Web server in your own environment to improve the security of your CAs.

IIS is used to host the certificate server enrollment pages, as well as distribute CA certificates and CRL download points for non–Windows clients. Microsoft recommends not installing IIS on the root certification authority (CA) server. If possible you should also avoid running IIS on your Issuing and any Intermediate CAs in your environment. It is more secure to host the Web download points for CA certificates and CRLs on a different server than the CA server itself. There might be many certificate users (internal and external) who need to retrieve CRLs or CA chain information who should not necessarily be permitted access to the CA. This restriction is impossible to achieve if the download points are hosted on the CA itself.

Note: The setting prescriptions for the Certificate Services server role were tested for the Enterprise Client environment only. For this reason, the IPSec filter and denial of service (DoS) information specified for the majority of the other server roles in this guide is not included here.

Audit Policy Settings

Audit Policy settings for Certificate Services servers in the Enterprise Client environment defined in this guide are configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that all the relevant security audit information is logged on all Certificate Services servers.

User Rights Assignments

User rights assignments for Certificate Services servers in the Enterprise Client environment defined in this guide are also configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The MSBP settings ensure that appropriate access to Certificate Services servers is uniformly configured across an enterprise.

Security Options

The Security Options section of Group Policy is used to enable or disable security settings for computers, such as digital signing of data, Administrator and Guest account names, floppy disk drive and CD–ROM drive access, driver installation behavior, and logon prompts.

The Security Options settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

The following tables in this section include the Security Options settings for the Certificate Services server role for the Enterprise Client environment defined in this guide.

Devices: Restrict CD–ROM access to locally logged–on user only

Table 10.1: Settings

Member Sever Default	Enterprise Client
Disabled	Enabled

The **Devices: Restrict CD – ROM access to locally logged – on user only** setting determines whether a CD–ROM is accessible to both local and remote users simultaneously. Enabling this setting allows only interactively logged–on users to access removable CD–ROM media. However, when this setting is enabled and no one is logged on interactively, users can access the CD–ROM over the network.

Users connecting to a Certificate Services server over the network cannot utilize any CD–ROM disk drives on the server whenever anyone is logged onto the local console of the server. Enabling this setting on a system serving as a CD jukebox for network users is not recommended. However, enabling this setting will prevent attackers from running malicious programs from the CD–ROM drive on there servers. On a CA, the administrator may be using the CD–ROM drive to copy sensitive key material to or from the server—this setting prevents anyone but the locally logged–on administrator from accessing this data. For this reason, this setting is configured to **Enabled** in the **Enterprise Client** environment defined in this guide.

Devices: Restrict floppy access to locally logged–on user only

Table 10.2: Settings

Member Server Default	Enterprise Client
Disabled	Enabled

The **Devices: Restrict floppy access to locally logged – on user only** setting determines whether removable floppy media are accessible to both local and remote users simultaneously. Enabling this setting allows only interactively logged–on users to access removable floppy media. However, when this setting is enabled and no one is logged on interactively, users can access the floppy over the network.

Users connecting to a Certificate Services server over the network cannot utilize any floppy disk drives installed on the server whenever anyone is logged onto the local console of the server. However, enabling this setting will prevent attackers from running malicious programs from the floppy drive on these servers. On a CA, the administrator may be using the floppy disk drive to copy sensitive key material to or from the server—this setting prevents anyone but the locally logged–on administrator from accessing this data. For this reason, this setting is configured to **Enabled** in the **Enterprise Client** environment defined in this guide.

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

Table 10.3: Settings

Member Server Default	Enterprise Client
Disabled	Enabled

The **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting determines if the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, this means that the provider only supports the TLS protocol as a client and a server (if applicable).

The TLS/SSL Security Provider uses the following:

- The Triple Data Encryption Standard (DES) encryption algorithm for the TLS traffic encryption.
- The Rivest, Shamir, and Adelman (RSA) public key algorithm for the TLS key exchange and authentication. (RSA is a public-key encryption technology developed by RSA Data Security, Inc.)
- The SHA–1 hashing algorithm for the TLS hashing requirements.

For the Encrypting File System Service (EFS), the TLS/SSL Security Provider supports only the Triple DES encryption algorithm to encrypt file data supported by the Windows NTFS file system. By default, EFS uses the DESX algorithm to encrypt file data.

Enabling this setting ensures that computers fulfilling this server role in your environment will use the most powerful algorithms available for digital encryption, hashing, and signing. This minimizes the risk of an unauthorized user compromising digitally encrypted or signed data. For these reasons, this setting is configured to **Enabled** in the **Enterprise Client** environment defined in this guide.

Note: Clients with this setting enabled will be unable to communicate with servers that do not support these algorithms via digitally encrypted or signed protocols. Network clients that do not support these algorithms will not be able to use servers that require them for network communications. For example, many Apache-based Web servers are not configured to support TLS. If you enable this setting you will also need to configure Internet Explorer to use TLS by opening the **Internet Options** dialog box from the Internet Explorer **Tools** menu. Click the **Advanced** tab on the **Internet Options** dialog box, scroll down towards the bottom of the **Settings** list, and then click the **Use TLS 1.0** checkbox. It is also possible to configure this through group policy or by using the Internet Explorer Administrators Kit.

Event Log Settings

The Event Log settings for Certificate Services servers in the Enterprise Client environment defined in this guide are also configured via the MSBP. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline."

System Services

Any service or application is a potential point of attack and, therefore, any unneeded services or executable files should be disabled or removed. In the MSBP, these optional services, as well as all other unnecessary services, are disabled.

There are additional services that are often enabled on computers running Windows Server 2003 that function as Certificate Services servers, but these are not essential. The use and security of these services is frequently the subject of debate. For this reason, recommendations on this server role in this chapter may not be applicable to your environment. Adjust the Certificate Services server Group Policy recommendations as needed to meet the requirements of your organization.

The System Services settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\System Services\

The following table includes the incremental policy service settings for the Certificate Services server role for the Enterprise Client environment defined in this guide.

Certificate Services

Table 10.4: Settings

Service Name	Member Server Default	Enterprise Client
CertSvc	Not Defined	Automatic

Certificate Services are part of the core operating system of Windows Server 2003 that enables a business to act as its own CA. This service is required for Certificate Services servers to function properly. These services are used to issue and manage digital certificates for applications, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), SSL, EFS, IPSec, and smart card log on. Windows Server 2003 supports multiple levels of a CA hierarchy, as well as a cross-certified trust network, including offline and online CAs.

Disabling this service causes certificate requests to not be accepted, and CRLs and delta CRLs will also not be published. Stopping the service long enough will cause CRLs to expire and the validation process for existing certificates to fail. For these reasons, the setting for these services is configured to **Automatic** in the Enterprise Client environment defined in this guide.

Computer Browser

Table 10.5: Settings

Service Name	Member Server Default	Enterprise Client
Browser	Automatic	Disabled

The **Computer Browser** service maintains an up-to-date list of computers on your network, and supplies the list to programs that request it. Windows-based computers use the **Computer Browser** service to view network domains and resources.

Computers designated as browsers maintain browse lists containing all shared resources used on the network. Earlier versions of Windows applications, such as My Network Places, the NET VIEW command, and Windows NT® Explorer all require browsing capability. For example, opening My Network Places on a computer running Windows 95 displays a list of domains and computers, which the computer does after obtaining a copy of the browse list from a computer designated as a browser.

There are several different roles a computer might perform in a browsing environment. Under some conditions, such as failure or shut down of a computer designated for a specific browser role, browsers—or potential browsers—may change to a different operation role.

Disabling the **Computer Browser** service results in the browser list not being updated or maintained, and services that explicitly depend on this service will not start. However, CA servers do not require this service. For this reason, this setting for this service is configured to **Disabled** in the Enterprise Client environment defined in this guide.

Additional Registry Settings

Additional registry value entries were created for the Certificate Services server security template files that are not defined within the Administrative Template (.adm) files for the Enterprise Client environment defined in this guide. The .adm files define the system policies and restrictions for the desktop, shell, and security settings for Windows Server 2003.

These additional registry settings are configured within the security templates to automate these changes. If the policy for the corresponding environment is removed, the settings for it are not automatically removed and must be manually changed using a registry editing tool such as Regedt32.exe.

The registry settings can be configured in Windows Server 2003 at the following location within the Group Policy Object Editor:

MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

The following table includes the registry path to the keys and subkeys to audit any changes to the Certificate Services server role configuration defined for the Enterprise Client environment in this guide.

Table 10.6: Registry Audit SACLs

Auditing Path in UI	Enterprise Client
MACHINE\SYSTEM\CurrentControlSet\Services\ Certsvc\ Configuration (and all subkeys)	Failed; Everyone Full Control; <not inherited> Special
MACHINE\SYSTEM\CurrentControlSet\Services\ Certsvc\ Configuration (and all subkeys)	Success; Everyone; Special: Set Value, Create Subkey, Create Link, Delete, Change permissions, Take ownership; <not inherited> Special

Additional Security Settings

The following settings can be assigned through Group Policy. However, this guide is not including the following settings because the installation of the database and logs can differ from server to server. For example, your Certificate Servers server could have a C:\, D:\, and E:\ drive. Details on how to manually implement these settings are outlined in the following section.

File System ACLs

Files that cannot be protected by access control lists (ACLs) can be easily viewed, changed, or deleted by unauthorized users who are able to access them locally or over the network. ACLs help to protect them. Encryption provides much more protection and is a viable option for files that only need to be accessible to a single user.

The following table includes the file system ACLs for Windows Server 2003–based systems running Certificate Services servers in the Enterprise Client environment defined in this guide. In this environment, the Certificate Services servers have the certificate database directory installed on the D:\ drive to D:\CertSrv and the database logs stored in the default folder %SystemRoot%\system32\CertLog. It is also possible to move the logs from the system drive on a physically separate mirrored drive for example E:\ - in the folder E:\CertLog. Separating the database and logs onto different drives is not a security requirement, but it is recommended for added protection from disk failures and to improve performance by placing these items on separate physical disk devices. The Certificate Services default installation folders %SystemRoot%\system32\CertLog and %SystemRoot%\system32\CertSrv, have the correct ACLs by default. These are shown in the table below.

Table 10.7: File System ACLs

ACL Path in UI	Enterprise Client
%SystemRoot%\system32\CertLog (propagate to all subfolders)	Administrators (Full Control) SYSTEM (Full Control)
%SystemRoot%\system32\CertSrv (propagate to all subfolders)	Administrators (Full Control) SYSTEM (Full Control) Users (Read and Execute, List Folder Contents, and Read)
D:\CertLog	Administrators (Full Control) SYSTEM (Full Control)
D:\CertSrv	Administrators (Full Control) SYSTEM (Full Control) Users (Read and Execute, List Folder Contents, and Read)

Because of the security–sensitive nature of CAs, file auditing is enabled on the Certificate Services folders listed in the preceding table. The audit entries are configured as follows:

Table 10.8: Certificate Services file and registry auditing

File Path or Registry Path	Audit Type	Audit Setting
%SystemRoot%\system32\CertLog	Fail	Everyone (Full Control)
%SystemRoot%\system32\CertSrv	Success	Everyone (Modify)
D:\CertSrv	Success	Everyone (Modify)
D:\CertLog	Success	Everyone (Modify)

The effect of these settings is to audit any type of failure access (read or modify) from any user and also to audit any successful modification by any user.

Securing Well Known Accounts

Windows Server 2003 has a number of built–in user accounts that can not be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

By default, the **Guest** account is disabled on member servers and domain controllers. This setting should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in Administrator account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

Complete the following steps to secure well known accounts on servers:

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Note: The built–in administrator account can be renamed via Group Policy. This setting was not configured in any of the security templates provided with this guide because you should choose a unique name for your environment. The **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings of a GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Summary

This chapter explained the server hardening settings in Windows Server 2003 that are recommended to secure Certificate Services servers in the Enterprise Client environment defined in this guide. The settings discussed are configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the MSBP is linked to the appropriate organizational units (OUs) containing the Certificate Services servers to provide additional security based on the services these servers provide.

More Information

The following information sources were the latest available on topics closely related to Windows Server 2003 and the Certificate Services server role detailed in this guide at the time this product was released to the pubic.

For a good introduction to public key infrastructure (PKI) concepts and the features of Windows 2000 certificate services, see "An Introduction to the Windows 2000 Public–Key Infrastructure," at: http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.asp.

For more detailed information on PKI functionality in Windows Server 2003 and Windows XP, see "PKI Enhancements in Windows XP Professional and Windows Server 2003," at: http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp.

For more background on key PKI concepts, see the TechNet information on "Public Key Infrastructure," at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/SE_PKI.asp.

11

Hardening Bastion Hosts

Overview

This chapter focuses on hardening bastion hosts in your environment. A bastion host is a secure but publicly accessible computer. Bastion hosts are located on the public side of the perimeter network (also known as the DMZ, demilitarized zone, and screened subnet). Bastion hosts are unprotected by a firewall or filtering router, making them fully exposed to attack. Due to this exposure, a great deal of effort must be put into designing and configuring bastion hosts to minimize the chance of one being compromised.

Bastion hosts are commonly used as Web servers, Domain Name System (DNS) servers, File Transfer Protocol (FTP) servers, Simple Mail Transport Protocol (SMTP) servers, and Network News Transfer Protocol (NNTP) servers. Ideally, bastion hosts are dedicated to performing just one of these functions since the more roles each host has to play, the greater the likelihood a security hole will be overlooked. It is easier to secure a single service on a single bastion host. Organizations that can afford the costs associated with multiple bastion hosts can benefit greatly from this type of network architecture.

Secure bastion hosts are configured very differently from typical hosts. All unnecessary services, protocols, programs, and network interfaces are disabled or removed, and then each bastion host is normally configured to fulfill a specific role. Hardening bastion hosts in this fashion limits potential methods of attack.

The following sections of this chapter detail a variety of security hardening settings that will most effectively secure bastions hosts in any environment.

Bastion Host Local Policy

Unlike the other server role group policies detailed earlier in this guide, Group Policy cannot be applied to bastion hosts servers because they are configured as stand–alone hosts that do not belong to a Microsoft® Active Directory® domain. Due to their high level of exposure, only one level of guidance is prescribed for bastion host servers in the three environments defined in this guide. The security settings described below are based on the Member Server Baseline Policy (MSBP) for the High Security environment defined in Chapter 3, "Creating a Member Server Baseline." They are included in a security template that must be applied to the Bastion Host Local Policy (BHLP) of each bastion host.

Applying the Bastion Host Local Policy

The High Security – Bastion Host.inf file included with this guide can be used to configure the BHLP. It will enable the services required for an SMTP bastion host server to function properly. Applying the High Security – Bastion Host.inf enhances server security by greatly reducing the attack surface of a bastion host, but makes remote management of the bastion host impossible. The BHLP must be modified to enable any further functionality or to increase manageability of a bastion host.

In order to apply all of the security settings included in the security template, it is necessary to use the **Security Configuration and Analysis** snap–in instead of the **Local Computer Policy** snap–in. It is not possible to import the security template using the **Local Computer Policy** snap–in because the security settings for System Services cannot be applied using this snap–in.

The following steps detail the process for importing and applying the BHLP security template using the **Security Configuration and Analysis** snap–in.

Warning: Microsoft strongly recommends performing a full backup of a bastion host server before applying the High Security – Bastion Host.inf to them. Reverting a bastion host to its original configuration after applying the High Security – Bastion Host.inf security template is very difficult. Ensure the security template is configured to enable the bastion host functionality your environment requires.

▶ **To import the security template:**

1. Launch the **Security Configuration and Analysis** snap–in.
2. Right–click the **Security Configuration and Analysis** scope item.
3. Click **Open Database**.
4. Type a new database name, and then click **Open**.
5. Select the High Security–Bastion Host.inf security template, and then click **Open**.

All of the bastion host settings will be imported, which can then be reviewed and applied.

▶ **To apply the security settings:**

1. Right–click the **Security Configuration and Analysis** scope item.
2. Select **Configure Computer Now**.
3. In the **Configure Computer Now** dialog box, type the name of the log file you wish to view, and click **OK**.

Completing these steps will apply all pertinent security template settings to the local policy of the bastion host in your environment. You must restart the bastion host for all settings to take effect.

The following sections describe the security settings applied using the BHLP. Only settings that differ from those in the MSBP are documented in this chapter.

Audit Policy Settings

The BHLP Audit Policy settings for bastion hosts are the same as those specified in the High Security – Member Server Baseline.inf file. For more information on the MSBP, see Chapter 3, "Creating a Member Server Baseline." The BHLP settings ensure that all relevant security audit information is logged on all bastion host servers.

User Rights Assignments

The BHLP User Rights Assignments for bastion hosts are based on those specified in the High Security – Member Server Baseline.inf file in Chapter 3, "Creating a Member Server Baseline." Differences between the BHLP and the MSBP are described below.

Allow log on locally

Table 11.1: Setting

Member Server Default	Setting
Allow log on locally	Administrators

The **Allow log on locally** user right enables a user to start an interactive session on the computer. Limiting the accounts that can be used to log on to a bastion host server console will help prevent unauthorized access to a server's file system and system services. A user who can log onto the console of a server can exploit the system to compromise its security.

The **Account Operators**, **Backup Operators**, **Print Operators**, and **Power Users** groups are granted the right to log on locally by default. Granting this right only to the **Administrators** group limits administrative access to bastion host servers to only highly trusted users, and provides an increased level of security.

Deny access to this computer from the network

Table 11.2: Settings

Member Server Default	Setting
SUPPORT_388945a0	ANONOYMOUS LOGON; Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts

Note: ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0, Guest, and all NON-operating system service accounts are not included in the security template. These accounts and groups have unique security identifier (SIDs). Therefore, they must be added manually to the BHLP.

The **Deny access to this computer from the network** user right determines which users are prevented from accessing a computer over the network. This setting will deny a number of network protocols including server message block (SMB) – based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP).and Component Object Model Plus (COM+).This setting overrides the **Access this computer from the network** setting when a user account is subject to both policies. Configuring this user right for other groups could limit the ability of users to perform delegated administrative tasks in your environment.

In Chapter 3, "Creating a Member Server Baseline," this guide recommends including the **Guests** group in the list of users and groups assigned this right to provide the highest level of security possible. Nevertheless, the IUSR account used for anonymous access to IIS is by default a member of the **Guests** group. For these reasons, the **Deny access to this computer from the network** setting is configured to include **ANONOYMOUS LOGON; Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts** for bastion hosts in the High Security environment defined in this guide.

Security Options

The BHLP Security Options settings for bastion hosts are the same as those specified in the High Security – Member Server Baseline.inf file in Chapter 3, "Creating a Member Server Baseline." These BHLP settings ensure that all relevant Security Options are uniformly configured across bastion host servers.

Event Log Settings

The BHLP Event Log settings for bastion hosts are the same as those specified in the High Security – Member Server Baseline.inf file in Chapter 3, "Creating a Member Server Baseline." These BHLP settings ensure that all relevant Event Log settings are uniformly configured across bastion host servers.

System Services

Bastion host servers are inherently exposed to outside attacks. For this reason, the attack surface of each bastion host must be minimized. In order to properly harden a bastion host server, all services not required by the operating system, as well as those not essential to the proper operation of the bastion host's role should be disabled. The High Security – Bastion Host.inf security template included with this guide configures the BHLP to enable the services an SMTP bastion host server requires to properly function. The BHLP enables the Internet Information Services Manager service, the HTTP SSL service, and the SMTP service. However, the BHLP must be modified to enable any other functionality.

A large number of disabled services could generate numerous Event Log warnings that can be ignored. In some cases, enabling some of these services will reduce Event Log warnings and error messages, and increase the manageability of bastion hosts. However, this will also increase the attack surface of each bastion host.

The following sections discuss services that should be disabled on bastion host servers to reduce their attack surface while maintaining their functionality. Only services not already disabled in the High Security – Member Server Baseline.inf file are included in these sections.

Automatic Updates

Table 11.3: Setting

Service Name	Setting
Wuauserv	Disabled

The **Automatic Updates** service enables bastion hosts to download and install critical Microsoft Windows® updates. This service automatically provides bastion hosts with the latest updates, drivers, and enhancements. You no longer have to manually search for critical updates and information; the operating system delivers them directly to the bastion hosts. The operating system recognizes when you are online and uses your Internet connection to search for applicable updates from the Windows Update service. Depending on your configuration settings, the service will notify you before a download, an installation, or it will automatically install updates for you.

Stopping or disabling the **Automatic Updates** service will prevent critical updates from downloading to the computer automatically. In this case, you will have to go directly to the Windows Update Web site at http://www.windowsupdate.microsoft.com to search for, download, and install any applicable critical fixes.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode for this service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Automatic Updates** setting is configured to **Disabled** in the BHLP.

Background Intelligent Transfer Service

Table 11.4: Setting

Service Name	Setting
BITS	Disabled

The **Background Intelligent Transfer Service** (BITS) is a background file transfer mechanism and queue manager. BITS transfers files asynchronously between a client and an HTTP server. BITS accepts requests to transfer files using otherwise idle network bandwidth so that other network–related activities, such as browsing, are not affected.

Stopping this service causes features such as Automatic Update to not automatically download programs and other information until the service is running again. This means that the computer will not receive automatic updates from Software Update Services (SUS) if this service has been configured via Group Policy. Disabling this service causes any services that explicitly depend on it to not transfer files, unless a fail–safe mechanism is in place to transfer files directly through other methods such as Internet Explorer.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of this service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, this service is disabled in the BHLP.

Computer Browser

Table 11.5: Setting

Service Name	Setting
Browser	Disabled

The **Computer Browser** service maintains an up–to–date list of computers on your network and supplies the list to programs that request it. The **Computer Browser** service is used by Windows–based computers that need to view network domains and resources. Computers designated as browsers maintain browse lists, which contain all shared resources used on the network. Earlier versions of Windows applications, such as My Network Places, the NET VIEW command, and Microsoft Windows NT® Explorer, all require browsing capability. For example, opening My Network Places on a computer running Windows 95 displays a list of domains and computers, which the computer does by obtaining a copy of the browse list from a computer designated as a browser.

Disabling the **Computer Browser** service will cause the browser list to not be updated or maintained. Disabling this service also causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Computer Browser** setting is configured to **Disabled** in the BHLP.

DHCP Client

Table 11.6: Setting

Service Name	Setting
Dhcp	Disabled

The **DHCP Client** service manages network configuration by registering and updating Internet Protocol (IP) addresses and DNS names for your computer. This service prevents you from having to manually change the IP settings when a client, such as when a roaming user wanders throughout the network. The client is automatically given a new IP address regardless of the subnet it reconnects to—as long as a Dynamic Host Configuration Protocol (DHCP) server is accessible from each of those subnets. There is no need to manually configure settings for DNS or Windows Internet Name Service (WINS). The DHCP server enforces these service settings to the client, as long as the DHCP server has been configured to issue such information. To enable this option on the client, simply select the **Obtain DNS Server Address Automatically** option button. Enabling this option will not cause duplicate IP address conflicts.

Stopping the **DHCP Client** service will cause your computer to not receive dynamic IP addresses and automatic Dynamic DNS updates will not be registered on the DNS server. Disabling this service also causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of this service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **DHCP Client** setting is configured to **Disabled** in the BHLP.

Network Location Awareness (NLA)

Table 11.7: Setting

Service Name	Setting
lanmanserver	Disabled

The **Network Location Awareness (NLA)** service collects and stores network configuration information such as IP address and domain name changes, as well as location change information and then notifies applications when this information changes.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Network Location Awareness (NLA)** setting is configured to **Disabled** in the BHLP.

NTLM Security Support Provider

Table 11.8: Setting

Service Name	Setting
NtLmSsp	Disabled

The **NTLM Security Support Provider** service provides security to remote procedure call (RPC) programs that use transports other than named pipes, and enables users to log on to the network using the NTLM authentication protocol. The NTLM protocol authenticates clients that do not use Kerberos version 5 authentication.

Stopping or disabling the **NTLM Security Support Provider** service will prevent you from logging on to clients using the NTLM authentication protocol, or accessing network resources. Microsoft Operations Manager (MOM) and Telnet rely on this service.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **NTLM Security Support Provider** setting is configured to **Disabled** in the BHLP.

Performance Logs and Alerts

Table 11.9: Setting

Service Name	Setting
SysmonLog	Disabled

The **Performance Logs and Alerts** service collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. The **Performance Logs and Alerts** service starts and stops each named performance data collection based on information contained in the named log collection setting. This service only runs if at least one collection is scheduled.

Stopping for disabling the **Performance Logs and Alerts** service causes performance information to not be collected, currently running data collections will terminate, and future scheduled collections will not occur.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Performance Logs and Alerts** setting is configured to **Disabled** in the BHLP.

Remote Administration Service

Table 11.10: Setting

Service Name	Setting
SrvcSurg	Disabled

The **Remote Administration Service** runs the following Remote Administration tasks when the server restarts:

- Increments the server restart count.
- Generates a self−signed certificate.
- Raises an alert if the date and time has not been set on the server.
- Raises an alert if the Alert E−mail functionality has not been configured.

Stopping **Remote Administration Service** may cause some features of the Remote Server Administration Tools to not function properly, such as Web interface for remote administration. Disabling this service causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Remote Administration Service** setting is configured to **Disabled** in the BHLP.

Remote Registry Service

Table 11.11: Setting

Service Name	Setting
RemoteRegistry	Disabled

The **Remote Registry Service** enables remote users to modify registry settings on the domain controller, provided the remote users have the required permissions. Only users in the **Administrators** and **Backup Operators** groups by default can access the registry remotely. This service is required for the Microsoft Baseline Security Analyzer (MBSA) utility. MBSA is a tool that allows you to verify which patches are installed on each of the servers in your organization.

Stopping the **Remote Registry Service** allows you to modify the registry only on the local computer. Disabling this service causes any services that explicitly depend on it to fail, but will not affect registry operations on your local computer. Other computers or devices will also no longer connect to your local computer's registry.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, **Remote Registry Service** setting is configured to **Disabled** in the BHLP.

Server

Table 11.12: Setting

Service Name	Setting
lanmanserver	Disabled

The **Server** service provides RPC support, file, print, and named pipe sharing over the network. This service allows local resource sharing, such as disks and printers, so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC. Named pipe communication is memory reserved for the output of one process to be used as input for another process. The input–accepting process does not need to be local to the computer.

Stopping the **Server** service prevents you from sharing files and printers on the computer with others on the network and it will also not satisfy RPC requests. Disabling this service also causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Server** setting is configured to **Disabled** in the BHLP.

TCP/IP NetBIOS Helper Service

Table 11.13: Setting

Service Name	Setting
LMHosts	Disabled

The **TCP/IP NetBIOS Helper Service** provides support for the network basic input/output system (NetBIOS) over TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network; thus, enabling users to share files, print, and log on to the network. The Transmission Control Protocol/Internet Protocol (TCP/IP) NetBIOS Helper service provides support for the NetBT service by performing DNS name resolution.

Stopping the **TCP/IP NetBIOS Helper Service** may prevent NetBT, Redirector (RDR), Server (SRV), Netlogon and Messenger service clients from sharing files, printers, and users from logging on to computers. For example, domain–based Group Policy will no longer function. Disabling this service causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **TCP/IP NetBIOS Helper Service** setting is configured to **Disabled** in the BHLP.

Terminal Services

Table 11.14: Setting

Service Name	Setting
TermService	Disabled

Terminal Services provides a multi−session environment that allows client devices to access a virtual Windows desktop session and Windows−based programs running on the server. **Terminal Services** allows users to remotely administer a server.

Stopping or disabling **Terminal Services** prevents a computer from being remotely administered making the computer difficult to manage and update.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **Terminal Services** setting is configured to **Disabled** in the BHLP.

Windows Installer

Table 11.15: Setting

Service Name	Setting
MSIServer	Disabled

The **Windows Installer** service manages the installation and removal of applications by applying a set of centrally defined setup rules during the installation process. These setup rules define the installation and configuration of the installed application. In addition, this service is used to modify, repair, or remove an existing application. The technology for this service consists of the **Windows Installer** service for the Windows operating systems and the (.msi) package file format used to hold information regarding the application setup and installations.

Windows Installer is not only an installation program; it is also an extensible software management system. The service manages the installation, addition, and deletion of software components, monitors file resiliency, and maintains basic file disaster recovery using rollbacks. In addition, **Windows Installer** supports installing and running software from multiple sources, and can be customized by developers who want to install custom applications.

Setting **Windows Installer** to manual causes applications that use the installer to start this service.

Stopping this service causes the installation, removal, repair, and modification of applications that rely on it to fail. Also, a number of applications that make use of this service while running may not execute. Disabling this service causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, The **Windows Installer** setting is configured to **Disabled** in the BHLP.

Windows Management Instrumentation Driver Extensions

Table 11.16: Setting

Service Name	Setting
lanmanserver	Disabled

The **Windows Management Instrumentation Driver Extensions** service monitors all drivers and event trace providers that are configured to publish WMI or event trace information.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, The **Windows Management Instrumentation Driver Extensions** setting is configured to **Disabled** in the BHLP.

WMI Performance Adapter

Table 11.17: Setting

Service Name	Setting
lanmanserver	Disabled

The **WMI Performance Adapter** service provides performance library information from WMI HiPerf providers. Applications and services that need to provide performance counters today can do so in two ways; by writing a WMI High Performance provider, or by writing a performance library.

The **WMI Performance Adapter** service transforms performance counters supplied by WMI High Performance providers into counters that can be consumed by the Performance Data Helper (PDH) through the Reverse Adapter Performance Library. In this way, PDH clients, for example Sysmon, can consume performance counters surfaced by any WMI High Performance providers on the computer.

If the **WMI Performance Adapter** service is stopped, WMI performance counters are unavailable. Disabling this service causes any services that explicitly depend on it to fail.

This service is not essential to the proper operation of a bastion host. Using a local policy to secure and set the startup mode of a service grants access only to server administrators, which prevents unauthorized or malicious users from configuring or operating the service. Furthermore, disabling this service effectively reduces the attack surface of a bastion host server. For these reasons, the **WMI Performance Adapter** setting is configured to **Disabled** in the BHLP.

Additional Security Settings

The security settings applied through the BHLP provide a great deal of enhanced security for bastion host servers. Nevertheless, there are a few additional considerations and procedures that should be taken into account. These steps cannot be performed through local policy, and should be completed manually on all bastion host servers.

Manually Adding Unique Security Groups to User Rights Assignments

Most User Rights Assignments applied via the MSBP have the proper security groups specified in the security templates that accompany this guide. However, there are a few accounts and security groups that cannot be included in the templates because their security identifiers (SIDs) are specific to individual Windows 2003 domains. User rights assignments that must be configured manually are specified below.

Warning: The following table contains values for the built – in **Administrator** account. This account is not to be confused with the built – in **Administrators** security group. If the **Administrators** security group is added to any of the deny access user rights below you will need to log on locally in order to correct the mistake.

In addition, the built – in **Administrator** account may have been renamed based on some of the recommendations described in Chapter 3, "Creating a Member Server Baseline." When adding the **Administrator** account, ensure the renamed account is specified.

Table 11.18: Manually Added User Rights Assignments

Member Server Default	Legacy Client	Enterprise Client	High Security
Deny access to this computer from the network	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts	Built–in Administrator; Support_388945a0; Guest; all NON–Operating System service accounts

Important: All non – operating system service accounts include service accounts used for specific applications across an enterprise. This does NOT include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts which are built – in accounts the operating system uses.

Removing Unnecessary Network Protocols and Bindings

Servers accessible directly over the Internet, particularly bastion host servers, should have all unnecessary protocols disabled to counter the threat of user enumeration. User enumeration is a type of information gathering exploit in which an attacker attempts to obtain system–specific information to plan further attacks.

The server message block (SMB) protocol will return rich information about a computer even to unauthenticated users using "null" sessions. The information that can be retrieved includes shares, user information (including groups and user rights), registry keys, and more.

Disabling SMB and NetBIOS over TCP/IP secures a bastion host by greatly reducing the server's attack surface. Although, servers operating under this configuration are more difficult to manage and cannot access folders shared on the network, these measures effectively protect the server from being easily compromised. Therefore, this guide recommends disabling SMB and NetBIOS over TCP/IP for the network connections on bastion host servers accessible from the Internet.

▶To disable SMB:

1. On the **Control Panel**, double-click **Network Connections**.
2. Right–click an Internet facing connection, and then click **Properties**.
3. On the **Properties** dialog box, select **Client for Microsoft Networks**, and then click **Uninstall**.
4. Follow the uninstall steps.
5. Select **File and Printer Sharing for Microsoft Networks**, and then click **Uninstall**.
6. Follow the uninstall steps.

▶ To disable NetBIOS over TCP/IP:

1. On the **Control Panel**, double–click **System**, click the **Hardware** tab, and then the **Device Manager** button.
2. On the **View** menu, click **Show hidden devices**.
4. Expand **Non–Plug and Play Drivers**.
5. Right–click **NetBIOS over Tcpip**, and then click **Disable**.

This procedure results in disabling the SMB direct host listener on TCP/445 and UDP 445.

Note: This procedure disables the nbt.sys driver. The **WINS** tab of the **Advanced TCP/IP Settings** dialog box contains a **Disable NetBIOS over TCP/IP** option. Selecting this option only disables the **NetBIOS Session Service** (which listens on TCP port 139). It *does not* disable SMB completely. To do so, use the steps above.

Securing Well Known Accounts

Microsoft Windows Server™ 2003 has a number of built–in user accounts that cannot be deleted but can be renamed. Two of the most well known built–in accounts in Windows 2003 are **Guest** and **Administrator**.

The **Guest** account is disabled by default on servers and should not be changed. The built–in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built–in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the security identifier (SID) of the built–in **Administrator** account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built–in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

▶ **To secure well known accounts on bastion host servers:**

1. Rename the **Administrator** and **Guest** accounts, and then change their passwords to a long and complex value on every server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all servers, an attacker who gains access to one server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

Error Reporting

Table 11.19: Settings

Default	Legacy Client	Enterprise Client	High Security
Report Errors	Disabled	Disabled	Disabled

The **Error Reporting** service helps Microsoft track and address errors. You can configure this service to generate reports for operating system errors, Windows component errors, or program errors. Enabling the **Report Errors** service causes such errors to be reported to Microsoft via the Internet or to an internal corporate file share.

This setting is only available on Microsoft Windows® XP Professional and Windows Server 2003. The path for configuring this setting in the Group Policy Object Editor is:

Computer Configuration\Administrative Templates\System\Error Reporting

Error reports can potentially contain sensitive or even confidential corporate data. The Microsoft privacy policy regarding error reporting ensures that Microsoft will not use such data improperly, but the data is transmitted in cleartext Hypertext Transfer Protocol (HTTP), which could be intercepted on the Internet and viewed by third – parties. For these reasons, this guide recommends configuring the **Error Reporting** setting in the BHLP to **Disabled** in all three security environments defined in this guide.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that should be created on an SMTP bastion host in the High Security environment defined in this guide.

Table 11.20: SMTP Bastion Host IPSec Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
SMTP Server	TCP	ANY	25	ANY	ME	ALLOW	YES
DNS Client	TCP	ANY	53	ME	DNS Server	ALLOW	YES
DNS Client	UDP	ANY	53	ME	DNS Server	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role–specific functions. These ports are sufficient if the server has a static IP address.

Warning: These IPSec filters are extremely restrictive and will significantly reduce the manageability of these servers. You will need to open additional ports to enable monitoring, patch management, and software update capabilities.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for a bastion host. The **PacketFilters-SMTPBastionHost.cmd** file uses the NETSH command to create the appropriate filters.

This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.* Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

Bastion host servers are highly exposed to outside attacks. They must be secured as much as possible to maximize their availability, and to minimize the impact of a bastion host server being compromised. The most secure bastion host servers limit access to only highly trusted accounts, and enable the fewest services possible to fully perform their functions.

This chapter has explained the prescribed server–hardening settings and procedures used to secure bastion host servers. Many of the settings can be applied through local Group Policy. Steps for configuring and applying manual settings have been provided.

Details on creating and applying IPSec filters that control the type of network traffic that can communicate with a bastion host server were also provided. These filters can be modified to block specific types of network traffic based on the customized role bastion host servers perform in your environment.

More Information

The following information sources were the latest available on topics closely related to bastion host servers in an environment with computers running Windows Server 2003 at the time this product was released to the pubic.

For more information on bastion hosts, see "Building a Bastion Host Using HP-UX 11" by Kevin Steves, at: http://people.hp.se/stevesk/bastion11.html.

For more information on building private networks, see "Firewalls and Virtual Private Networks" by Elizabeth D. Zwicky, Simon Cooper, and Brent D. Chapman at: http://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf.

For further information on firewalls and security, see "Internet Firewalls and Security – A Technology Overview" by Chuck Semeria at: http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html#Bastion%20Host.

For information on the defense–in–depth model, see the "U.S. Military with Rod Powers,"at: http://usmilitary.about.com/careers/usmilitary/library/glossary/d/bldef01834.htm.

For information on safeguards against intruders, see the "Intruder Detection Checklist" by Jay Beale at: http://www.cert.org/tech_tips/intruder_detection_checklist.html.

For information on hardening bastion hosts, see the SANS Info Sec Reading Room article on "Hardening Bastion Hosts," at: http://www.sans.org/rr/securitybasics/hard_bastion.php.

For further information on bastion hosts, see "How Bastion Hosts Work," at: http://thor.info.uaic.ro/~busaco/teach/docs/intranets/ch16.htm.

For information on turning off the Internet Connection Firewall in Windows Server 2003, see the Knowledge Base article, "How To: Turn On the Internet Connection Firewall Feature in Windows Server 2003,' at: http://support.microsoft.com/default.aspx?scid=317530.

For information on troubleshooting the Security Configuration and Analysis Tool, see the Knowledge Base article, "Problems After You Import Multiple Templates Into the Security Configuration and Analysis Tool," at: http://support.microsoft.com/default.aspx?scid=279125.

For information on the site security, see the "Site Security Handbook," at: http://www.theinternetbook.net/rfc/rfc2196.html.

12

Conclusion

Congratulations. Now that you have finished this guide, you should have a much more clear understanding of how to assess risks that may impact the security of computers running Microsoft® Windows Server™ 2003 in your organization. You have gained an understanding of how to plan and design security into your infrastructure where possible. This guide included prescriptive guidance that may be applied to any organization.

The guide includes material collected from consultants and systems engineers working in the field who have implemented Windows Server 2003, Windows XP, and Windows 2000 solutions in a variety of corporate settings to provide you with the current set of best practices to perform this complex task.

Regardless of your organization's environment, security should be taken seriously. However, many organizations still place little emphasis on security, mistakenly viewing it as something that restricts the agility and flexibility of their enterprise. When well – designed security becomes a core business requirement, and planning accounts for it at the start of every information technology (IT) project, a properly implemented security strategy can help to improve the availability and performance of your computer systems. On the other hand, when security is added to a project as an afterthought, it can have a negative effect on usability, stability, and management flexibility — all important reasons why every organization should make security a top priority.

This guide explained how to effectively mitigate security risks in three distinct environments with computers running Windows Server 2003. It documented methods for planning and designing security into your organization's network infrastructure, and provided detailed guidance on how to correct specific vulnerabilities that are commonly found on computers running Windows Server 2003.

The reasoning behind these choices was explained in terms of the tradeoffs that were often involved in deciding whether to implement each of the countermeasures for all three environments detailed in this guide. Details were provided on how specific countermeasures may impact the functionality, manageability, performance, and reliability of the computers so that you can make informed choices on which countermeasures to implement in your own environment.

Finally, it is important to understand that the task of securing the servers on your network is not a one time project, but rather an ongoing process that organizations must include in their budgets and schedules. Implementing all of the countermeasures discussed in this guide will improve the security in the majority of organizations operating Windows Server 2003.

However, when the next serious vulnerability is discovered, these environments may again be quite susceptible to attack. For these reasons, it is critical to monitor a variety of resources to stay current on security issues related to the operating systems, applications, and devices present in your environment.

Every member of the team that produced this guide hopes that you found the material covered in it useful, informative, and easy to understand.

More Information

The following information sources were the latest available on topics closely related to Windows Server 2003 at the time this product and guide were released to the pubic.

For more information on security at Microsoft, see: http://www.microsoft.com/security.

For more detail on how MOF can assist in your enterprise, see: http://www.microsoft.com/business/services/mcsmof.asp.

For information on the Microsoft Strategic Technology Protection Program, see: http://microsoft.com/security/mstpp.asp.

For information on the Microsoft Security Notification Service, see: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp.