SOLUTIONACCELERATORS

Act faster. Go further.

Windows Server® 2003 Security Guide

Security Compliance Management Toolkit

Version 3.1

Published: April 2003 | Updated: April 2010

For the latest information, please see

microsoft.com/ssa

Microsoft

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

Overview

Welcome to the *Windows Server 2003 Security Guide*. This guide is designed to provide you with the best information available to assess and counter security risks in your organization that are specific to Windows Server® 2003 Service Pack 2 (SP2). The chapters in this guide provide detailed guidance about how to enhance security setting configurations and features in Windows Server 2003 SP2 or later wherever possible to address threats that you have identified in your environment. This guide was created for systems engineers, consultants and network administrators who work in a Windows Server 2003 SP2 environment.

In order to create, test, and deploy the security settings for either the EC environment or the SSLF environment, you must first run the Windows® Installer (.msi) file for the Security Compliance Management (SCM) tool that accompanies the download for this toolkit. You can then use this tool to automatically create all the Group Policy Objects (GPOs) for the security settings that this guide recommends. For instructions on how to use this tool to accomplish these tasks, see the information available in the Help Topics for the tool. You can also use the Microsoft Excel® workbook Windows Server 2003 Security Baseline Settings to compare and evaluate the Group Policy settings.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved this prescriptive guidance 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.

The guide was developed and tested with computers running Windows Server 2003 SP2 joined to a domain that uses Active Directory®. As the operating system continues to evolve through future releases, you can expect updated versions of this guidance to include more security enhancements. Solution Accelerators are also available to assist you with the deployment and operation of Windows Server 2008. For more information about all available Solution Accelerators, visit Solution Accelerators on TechNet.

Executive Summary

Whatever your environment, you are strongly advised to be serious about security issues. Many organizations underestimate the value of their information technology (IT) environment, often because they exclude substantial indirect costs. If an attack on the servers in your environment is severe enough, it could significantly damage the entire organization. For example, an attack in which your organization's Web site is brought down could cause a major loss of revenue or customer confidence. When you evaluate security costs, it is important to include indirect costs associated with any attack in addition to 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 computers are subject to in a networked environment. This guide documents the major security countermeasures that are available in Windows Server 2003 SP2 or later, the vulnerabilities that they address, and the potential negative consequences (if any) of each countermeasure's implementation.

The guide then provides specific recommendations about how to harden computers that run Windows Server 2003 SP2 or later in two distinct enterprise environments. The Enterprise Client (EC) environment is one in which Windows 2000 is the earliest version of the Windows operating system in use. The second environment is one in which concern about security is so great that significant loss of client functionality and manageability is considered an acceptable tradeoff to achieve the highest level of security. This second is known as the Specialized Security – Limited Functionality (SSLF) environment. 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 enterprise customers, much of it is appropriate for organizations of any size.

In order to create, test, and deploy the security settings for any of the environments described in this guide, you must run the .msi file for the SCM tool that accompanies the download for this toolkit. You can then use this tool to automatically create all the GPOs for the security settings that this guide recommends. For instructions on how to use this tool to accomplish these tasks, see the information available in the Help Topics for the tool. To get the most value out of the material, Microsoft recommends reading the entire guide. For further information about security topics and settings related to Windows Server 2003 SP2, see the companion guide, *Threats and Countermeasures*.

After deploying the appropriate security settings across your enterprise you can verify that the settings are in effect on each computer using the *Security Compliance Management Toolkit*. The toolkit includes Configuration Packs that match the recommendations in this guide for the EC and SSLF environments. The toolkit can be used with the Desired Configuration Management (DCM) feature in Configuration Manager 2007® (SP1) to efficiently monitor compliance. In addition, you can quickly and easily run reports to demonstrate how your organization is meeting important compliance regulations. For further information about the toolkit see the Security Compliance Management Toolkit on TechNet.

Who Should Read This Guide

The *Windows Server 2003 Security Guide* is primarily for IT professionals, security specialists, network architects, computer engineers, and other IT consultants who plan application or infrastructure development and deployments of Windows Server 2003 SP2 for servers in an enterprise environment. The guide is not intended for home users. This guide is for individuals whose jobs may include one for more of the following roles:

- **Security specialist**. Users in this role focus on how to provide security across computing platforms within an organization. Security specialists require a reliable reference guide that addresses the security needs of every level of the organization and also offers proven methods to implement security countermeasures. Security specialists identify security features and settings, and then provide recommendations on how their customers can most effectively use them in high risk environments.
- **IT operations, help desk, and deployment staff**. Users in IT operations focus on integrating security and controlling change in the deployment process, whereas deployment staff focuses on administering security updates quickly. Both troubleshoot security issues related to installing and configuring applications to improve software usability and manageability. They monitor these issues to measure security improvements and limit impact on critical business applications.

- **Network architect and planner**. Users in this role drive the network architecture efforts for computers in their organizations.
- **Consultant**. Users in this role are aware of security scenarios that span all business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.

Scope of This Guide

This guide focuses on how to create and maintain a secure environment for computers that run Windows Server 2003 SP2 in your organization. The guidance explains the different stages of how to secure the two environments that are defined in the guide, and what each prescribed server setting addresses in terms of client dependencies. The two environments are described as follows:

- The Enterprise Client (EC) environment consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003 SP2 and client computers that run Windows 2000 and Windows XP Professional SP3.
- The Specialized Security – Limited Functionality (SSLF) environment also consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003 SP2 and clients that run Windows 2000 and Windows XP SP3. However, the Specialized Security – Limited Functionality settings are so restrictive that many applications may not function. For this reason, the servers' performance may be affected, and it will be more of a challenge to manage the servers.
- Also, client computers that are not secured by the SSLF policies could experience communication problems with client computers and servers that are secured by the SSLF policies. See the *Windows XP Security Guide* for information about how to secure client computers with SSLF-compatible settings.

Guidance about ways to harden computers in these environments is provided for a group of distinct server roles. The countermeasures that are described and the tools that are provided assume that each server will have a single role. If you need to combine roles for some of the servers in your environment, you can customize the GPO backup files that are included in the download that accompanies this guide to create the appropriate combination of services and security options. The roles that are described in this guide include:

- Domain controllers.
- Infrastructure servers that provide Dynamic Host Configuration Protocol (DHCP) services or Domain Name System (DNS) services.
- File services.
- Print services.
- Internet Information Services (IIS).
- Internet Authentication Services (IAS).
- Certificate Services.
- Bastion hosts.

The recommended settings in this guide were tested thoroughly in lab environments that simulated the previously described Enterprise Client and Specialized Security – Limited Functionality environments. 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 GPO backup files s and the manual procedures that are documented within this guide so that all of your business applications continue to function as expected. The detailed information that is provided in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, provides the information that you need to assess each specific countermeasure and to decide which of them are appropriate for your organization's unique environment and business requirements.

After downloading the *Windows Server 2003 Security Guide* Solution Accelerator from the Microsoft Download Center, use the Windows Installer (.msi) file to install these resources on your computer in a location of your choice. Then run the .msi file for the SCM tool that accompanies the download for this toolkit to create, test, and deploy the security settings for the *Windows Server 2008 Security Guide*.

Chapter Summaries

The *Windows Server 2003 Security Guide* consists of 11 chapters. Each chapter builds on the end-to-end solution process that is required to implement and secure Windows Server 2003 SP2 in your environment. The first few chapters describe how to build a foundation that will allow you to harden the servers in your organization, and the rest of the chapters document the procedures that are unique to each server role.

Overview

The Overview introduces the *Windows Server 2003 Security Guide* and includes a brief overview of each chapter. It describes the Enterprise Client and Specialized Security – Limited Functionality environments and the computers that run in them.

Chapter 1: Windows Server 2003 Hardening Mechanisms

This chapter provides an overview of the main mechanisms that are used to harden Windows Server 2003 SP2 in this guide—the Security Configuration Wizard (SCW) and Active Directory Group Policy. It explains how SCW provides an interactive framework to create, manage, and test security policies for Windows servers that serve in different roles. It also evaluates the capabilities of SCW within the context of the environments that are described in the Overview.

The next part of this chapter provides high-level descriptions of Active Directory design, organizational unit (OU) design, Group Policy Objects (GPOs), administrative group design, and domain policy. These topics are discussed in the context of the environments that are described in the Overview to provide a vision of an ideal secure end-state environment.

This chapter concludes with a detailed examination of how this guide combines the best features of SCW and traditional GPO-based approaches to harden Windows Server 2003 SP2.

Chapter 2: Implementing the Domain Policy

This chapter explains Group Policy settings and additional countermeasures for the domain-level policies in the environments that are described in the Overview. The chapter does not focus on any specific server role, but on the specific policies and settings that are useful for top-level domain policies.

Chapter 3: Implementing the Security Baseline

This chapter explains Group Policy settings and additional countermeasures for the different server roles in the environments that are described in the Overview. The chapter focuses on how to establish a Member Server Baseline Policy (MSBP) for the server roles that are discussed later in the guide.

The recommendations in this chapter are designed to allow organizations to safely deploy setting configurations for both existing and new deployments of Windows Server 2003 SP2. The default security configurations within Windows Server 2003 SP1 were researched and tested, and the recommendations in this chapter were determined to provide greater security than the default operating system settings.

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 that run Windows Server 2003 SP2. Any loss or compromise of a domain controller could seriously affect client computers, servers, and applications that rely on domain controllers for authentication, Group Policy, and a central lightweight directory access protocol (LDAP) directory.

This chapter describes the need to always store domain controllers in physically secure locations that are accessible only to qualified administrative staff. The hazards of domain controllers in unsecured locations such as branch offices are addressed, and a significant portion of the chapter is devoted to an explanation of the security considerations that are the basis for the recommended Domain Controller Group Policy.

Active Directory domain controllers require a stable, properly configured DNS service. By default, Windows Server 2003 SP2 integrates DNS zones into Active Directory, which allows domain controllers to run the DNS service and answer DNS requests for clients in the Active Directory domain. This chapter assumes that the domain controller will also provide DNS service and provides the appropriate guidance.

Chapter 5: Hardening Infrastructure Servers

In this chapter, the infrastructure server role is defined as either a DHCP server or a WINS server. Details are provided about how the Windows Server 2003 SP2 infrastructure servers in your environment can benefit from security settings that are not applied by the Member Server Baseline Policy (MSBP). This chapter does not include configuration information for the DNS service, which is included in the domain controller role.

Chapter 6: Hardening File Services

This chapter focuses on the File server role and the difficult aspects of how to harden such servers. The most essential services for file servers require use of Windows NetBIOS-related protocols and the SMB and CIFS protocols. The Server Message Block (SMB) and Common Internet File System (CIFS) protocols are typically used to provide access for authenticated users, but when improperly secured they can also disclose rich information to unauthenticated users or attackers. Because of this threat, these protocols are often disabled in high-security environments. This chapter describes how file servers that run Windows Server 2003 SP2 can benefit from security settings that are not applied by the MSBP.

Chapter 7: Hardening Print Services

This chapter focuses on print servers. Like file servers, the most essential services for print servers require use of Windows NetBIOS-related protocols and the SMB and CIFS protocols. As stated earlier, these protocols are often disabled in high-security environments. This chapter describes how Windows Server 2003 SP2 print server security settings can be strengthened in ways that are not applied by the MSBP.

Chapter 8: Hardening Web Services

This chapter describes how comprehensive security for Web sites and applications requires an entire IIS server (including each Web site and application that runs on the IIS server) to be protected from client computers in its environment. Web sites and applications also must be protected from other Web sites and applications that run on the same IIS server. Practices to ensure that these measures are achieved by the IIS servers that run Windows Server 2003 SP2 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 in a highly secure "locked" mode. For example, the default settings only allow IIS to serve static content. Features such as Active Server Pages (ASP), ASP.NET, Server-Side Includes, WebDAV publishing, and Microsoft FrontPage® Server Extensions must be enabled by the administrator through the Web Service Extensions node in Internet Information Services Manager (IIS Manager).

Sections in this chapter provide details about a variety of settings you can use to harden the IIS servers in your environment. The need to monitor, detect, and respond to security issues is emphasized to ensure that the servers stay secure. This chapter focuses on IIS Web protocols and applications, such as HTTP, and does not include guidance on the other protocols that IIS can provide, such as SMTP, FTP, and NNTP.

Chapter 9: Hardening Internet Authentication Services

Internet Authentication Services (IAS) provides Remote Authentication Dial-In User Services (RADIUS), a standards-based authentication protocol that is designed to verify the identity of clients who access networks remotely. This chapter describes ways in which IAS servers that run Windows Server 2003 SP2 can benefit from security settings that are not applied by the MSBP.

Chapter 10: Hardening Certificate Services

Certificate Services provide the cryptographic and certificate management services that are needed to build a public key infrastructure (PKI) in your server environment. This chapter describes ways in which Certificate Services servers that run Windows Server 2003 SP2 will benefit from security settings that are not applied by the MSBP.

Chapter 11: Hardening Bastion Hosts

Bastion host servers are accessible to client computers from the Internet. In this chapter, it is explained how these publicly exposed computers are susceptible to attack from a large number of users who can remain completely anonymous if they wish. Many organizations do not extend their domain infrastructure to the Internet. For this reason, this chapter content focuses on how to harden stand-alone computers. Details are provided about ways in which bastion hosts that run Windows Server 2003 SP2 can benefit from the security recommendations in this guide for computers that are not members of an Active Directory–based domain.

Skills and Readiness

IT professionals who develop, deploy, and secure installations of Windows Server 2003 SP2 and Windows XP SP3 in an enterprise environment require the following knowledge and skills:

- MCSE 2000 or MCSE 2003 certification with more than two years of security-related experience.
- In-depth knowledge of organizational domain and Active Directory environments.
- Use of management tools, including the Microsoft Management Console (MMC), Secedit, Gpupdate, and Gpresult.
- Experience in the administration of Group Policy.
- Experience in the deployment of applications and workstation computers in enterprise environments.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this guide on Microsoft.com:

- Microsoft Operations Framework.
- Microsoft Security Bulletin Search.
- Trustworthy Computing.

Feedback

Please direct questions and comments about this guide to secwish@microsoft.com.

Acknowledgments

The Solution Accelerators – Security and Compliance (SA–SC) team 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.

Development Team

Authors and Experts

Brad Warrender – *Microsoft*

Haikun Zhang – *Minesage Co Ltd*

Hui Zeng – *Minesage Co Ltd*

José Maldonado – *Microsoft*

Kurt Dillard – *kurtdillard.com*

Michael Tan – *Microsoft*

Mike Danseglio – *Microsoft*

ZhiQiang Yuan – *Minesage Co Ltd*

Content Contributors

Devin Ganger – *3Sharp – LLC*

Eric Fitzgerald – *Microsoft*

Ian Hellen – *Microsoft*

Jesper Johansson – *Microsoft*

Kirk Soluk – *Microsoft*

Liam Colvin – *3Sharp – LLC*

Steve Ryan – *Content Master*

Stirling Goetz – *Microsoft*

Tony Dowler – *3Sharp – LLC*

William Dixon – *V6 Security Inc.*

Product Managers

Shruti Kala – *Microsoft*

Bill Reid – *Microsoft*

Tony Bailey – *Microsoft*

Program Managers

Alison Woolford – *Content Master*

Bomani Siwatu – *Microsoft*

Vlad Pigin – *Microsoft*

Editors

John Cobb – *Wadeware LLC*

Jon Tobey – *Wadeware LLC*

Kelly McMahon – *Content Master*

Lynne Perry – *Content Master*

Reid Bannecker – *Volt Information Sciences*

Steve Wacker – *Wadeware LLC*

Wendy Cleary – *S&T Onsite*

Release Managers

Flicka Crandell – *Microsoft*

Karina Larson – *Microsoft*

Karl Seng – *Siemens Agency Services*

Test Manager

Sumit Parikh – *Microsoft*

Testers

Ankit Agarwal – *Infosys Technologies Ltd*

Ashish Java – *Infosys Technologies Ltd*

Dhanashri Dorle – *Infosys Technologies Ltd*

Gaurav Singh Bora – *Infosys Technologies Ltd*

Kenon Bliss – *Volt Information Sciences*

Mehul Mediwala – *Infosys Technologies Ltd*

Paresh Gujar – *Infosys Technologies Ltd*

Raxit Gajjar – *Infosys Technologies Ltd*

Rob Pike – *Microsoft*

Varun Rastogi – *Infosys Technologies Ltd*

Vince Humphreys – *Volt Information Sciences*

Contributors and Reviewers

Jose Luis Auricchio, Avi Ben-Menahem, Rich Benack, Shelly Bird, Susan Bradley, Steve Clark, Rob Cooper, Duane Crider, Karel Dekyvere, Eric Fitzgerald, Mike Greer, Robert Hensing, Chad Hilton, Andrew Mason, Don McGowan, James Noyce, Joe Porter, Joel Scambray, Debra Littlejohn Shinder, Tom Shinder, Steve Smegner, Ben Smith, Allen Stewart, Didier Vandenbroeck, Ryan Vatne, Jeff Williams, Shain Wray, , Ignacio Avellaneda, Ganesh Balakrishnan, Shelly Bird, Nathan Buggia, Derick Campbell, Chase Carpenter, Jeff Cohen, John Dwyer, Sean Finnegan, Karl Grunwald, Joanne Kennedy, David Mowers, Jeff Newfeld, Rob Oikawa, Vishnu Patankar, Peter Meister, Keith Proctor, Sandeep Sinha, Graham Whiteley, Rob Wickham, Lori Woehler, Jay Zhang, Roger Abell, *Arizona State University,* Christine Duell, *Valente Solutions*, Jim Whitney, *Configuresoft,* Karina Larson, *Volt Information Sciences*, Chrissy Lewis, *Siemens Business Services*, Stacy Tsurusaki, *Volt Information Sciences*, and David Visintainer, *Volt Information Sciences*

Note The United States Department of Commerce National Institute of Standards and Technology (NIST) participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

Note At the request of Microsoft, the National Security Agency Information Assurance Directorate participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

Chapter 1: Windows Server 2003 Hardening Mechanisms

This chapter introduces the mechanisms that you can use to implement security settings on Windows Server® 2003. Service Pack 2 (SP2) for Windows Server 2003 provides the Security Configuration Wizard (SCW), which is a role-based tool that you can use to make your servers more secure. When used in conjunction with Group Policy objects (GPOs), SCW allows greater control, flexibility, and consistency in the hardening process.

This chapter focuses on the following topics:

- How to use the SCW to create, test, and deploy role-based hardening policies.
- How the Active Directory® directory service facilitates consistent enterprise hardening through the use of GPOs.
- How the Active Directory domain design, the organizational unit (OU) design, Group Policy design, and administrative group design affect security deployments.
- How to use both the SCW and Group Policy to create a manageable, role-based approach to harden servers running Windows Server 2003 SP2.

This information provides a foundation and a vision that you can use to evolve to a Specialized Security – Limited Functionality (SSLF) environment within a domain infrastructure.

Hardening with the Security Configuration Wizard

The purpose of SCW is to provide a flexible, step-by-step process to reduce the attack surface on servers that run Windows Server 2003 SP2. The SCW is actually a collection of tools that is combined with an XML rules database. Its purpose is to help administrators quickly and accurately determine the minimum functionality that is required for the roles that specific servers must fulfill.

With the SCW, administrators can author, test, troubleshoot, and deploy security policies that disable all nonessential functionality. It also provides the ability to roll back security policies. The SCW provides native support for security policy management on single servers as well as groups of servers that share related functionality.

The SCW is a comprehensive tool that can help you accomplish the following tasks:

- Determine which services must be active, which services need to run when required, and which services can be disabled.
- Manage network port filtering in combination with Windows Firewall.
- Control which IIS Web extensions are allowed for Web servers.
- Reduce protocol exposure to the server message block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Lightweight Directory Access Protocol (LDAP).

- Create useful Audit policies that capture the events of interest.

Detailed instructions about how to install, use, and troubleshoot the SCW are available in a downloadable version of the Security Configuration Wizard Documentation.

Note: You can only use the SCW with Windows Server 2003 SP2. You cannot use it to create policies for Windows 2000 Server, Windows XP Professional SP3, or Windows Small Business Server 2003. To harden significant numbers of computers that run these operating systems, you will need to take advantage of the Group Policy–based hardening mechanisms described later in this chapter.

Creating and Testing Policies

You can use the SCW to rapidly create and test security policies for multiple servers or groups of servers from a single computer. This capability allows you to manage policies throughout the enterprise from a single location. These policies provide consistent, supported hardening measures that are appropriate for the functions that each server provides within the organization. If you use the SCW to create and test policies, you should deploy the SCW to all targeted servers. Although you create the policy on a management station, the SCW will attempt to communicate with the target servers to inspect their configuration and fine-tune the resulting policy.

The SCW is integrated with the IPsec and Windows Firewall subsystems and will modify those settings accordingly. Unless prevented, the SCW will configure the Windows Firewall to permit inbound network traffic to important ports that are required by the operating system as well as listening applications. If additional port filters are required, the SCW can create them. As a result, policies that are created by the SCW address the need for custom scripts to set or modify IPsec filters to block unwanted traffic. This capability simplifies the management of network hardening. The configuration of network filters for services that make use of RPC or dynamic ports can also be simplified.

The SCW also provides the capability to significantly customize the policies that you create. This flexibility helps you create a configuration that permits necessary functionality but also helps to reduce security risks. In addition to the baseline behaviors and settings, you can override the SCW in the following areas:

- Services
- Network ports
- Windows Firewall-approved applications
- Registry settings
- IIS settings
- Inclusion of pre-existing Security Templates (.inf files)

The SCW advises the administrator about some of the most important registry settings. To reduce the complexity of the tool, the designers chose to only include those settings that have the greatest impacts on security. However, this guide discusses many more registry settings. To overcome the limitations of the SCW, you can combine Security Templates with the results of the SCW to create a more complete configuration.

When you use the SCW to create a new policy, it uses the current configuration of a server as an initial configuration. Therefore, you should target a server of the same type as the servers on which you intend to deploy the policy so that you can accurately describe the configuration of the server's roles. When you use the SCW graphical user interface (GUI) to create a new policy, it creates an XML file and saves it in the **%systemdir%\security\msscw\Policies** folder by default. After you create your policies, you can use either the SCW GUI or the Scwcmd command-line tool to apply the policies to your test servers.

When you test the policies, you may need to remove a policy that you deployed. You can use either the GUI or the command-line tool to roll back the last policy you applied to a server or group of servers. The SCW saves the previous configuration settings in XML files.

For organizations that have limited resources to design and test security configurations, the SCW may be sufficient. Those organizations that lack such resources should not even attempt to harden servers, because such efforts often result in unexpected problems and lost productivity. If your organization does not have the expertise and time available to deal with these types of issues, then you should focus on other important security activities such as application and operating system upgrades to current versions and update management.

Deploying Policies

There are three different options you can use to deploy your policies:

- Apply the policy with the SCW GUI.
- Apply the policy with the Scwcmd command-line tool.
- Convert the SCW policy to a GPO and link it to a domain or OU.

Each option has its own advantages and drawbacks, which are described in the following subsections.

Apply the Policy with the SCW GUI

The main advantage of the SCW GUI option is simplicity. The GUI permits administrators to easily select a predefined policy and apply it to a single computer.

The disadvantage of the SCW GUI option is that it only permits application of policies to a single computer at a time. This option does not scale for large environments, and this guide does not use this method.

Apply the Policy with the Scwcmd Command-line Tool

One way to apply native SCW policies to multiple computers without Active Directory is to use the Scwcmd tool. You can also combine the use of Scwcmd with scripting technologies to provide a degree of automated policy deployment, perhaps as part of an existing process that is used to build and deploy servers.

The main disadvantage of the Scwcmd option is that it is not automatic. You have to specify the policy and target server, either manually or through some scripting solution, which means there are multiple chances to push the wrong policy to the wrong computer. If you have servers in a group with slightly different configurations, you will need to craft a separate policy for each of those computers and apply them separately. Because of these limitations, this guide does not use this method.

Convert the SCW Policy to a GPO and Link it to a Domain or OU

The third option for SCW policy deployment is to use the Scwcmd tool to convert the XML-based policy into a GPO. Although at first this conversion might seem to be an unnecessary step, its advantages include the following:

- Policies are replicated, deployed, and applied with familiar Active Directory–based mechanisms.

- Because they are native GPOs, policies can be used with OUs, policy inheritance, and incremental policies to fine-tune the hardening of servers that are configured similarly but not exactly the same as other servers. With Group Policy, you put these servers in a child OU and apply an incremental policy, whereas with SCW you would need to create a new policy for each unique configuration.
- Policies are automatically applied to all servers that are placed in the corresponding OUs. Native SCW policies must be either manually applied or used in conjunction with some custom scripting solution.

Hardening Servers with Active Directory Group Policy

Active Directory enables applications to find, use, and manage directory resources in a distributed computing environment. Although detailed information about how to design an Active Directory infrastructure could fill an entire book, this section briefly discusses these concepts to establish a context for the rest of the guide. This design information is necessary to provide insight into the use of Group Policy to securely administer your organization's domains, domain controllers, and specific server roles. If your organization already has an Active Directory design, this chapter may provide insight into some of its security benefits or potential issues.

This guide does not offer any specific guidance about how to secure the Active Directory database. For such guidance, see the "Best Practice Guide for Securing Active Directory Installations."

When you create an Active Directory infrastructure, you must carefully consider the environment's security boundaries. If you adequately plan an organization's security delegation and implementation schedule, the result will be a more secure Active Directory design for the organization. You should only need to restructure the design for major changes to the environment, such as an acquisition or reorganization.

Active 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, and they are automatically established when you install Active Directory. However, you must ensure that permission boundaries incorporate organizational requirements and policies. Administrative permissions delegation can be quite flexible to accommodate different organizations' requirements. For example, to maintain a proper balance between security and administrative functionality, you can divide the permission delegation boundaries between 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 adequate security (based on how the organization’s business boundaries are established) and the need to maintain a consistent level of base functionality. To successfully achieve this balance, you must weigh the threats to your organization against the security implications of delegated administration permissions and other choices that involve your environment's network architecture.

The forest is the true security boundary of your network environment. This guide recommends that you create separate forests to keep your environment secure from potential compromise by administrators of other domains. This approach also helps ensure that the compromise of one forest does not automatically lead to the compromise of the entire enterprise.

A domain is a management boundary of Active Directory, not a security boundary. With an organization of well-intentioned individuals, a domain boundary will provide autonomous management of services and data within each domain of the organization. Unfortunately, with regard to security, isolation 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.

Within the domain, the organizational unit (OU) provides another level of management boundary. OUs provide a flexible way to group related resources and delegate management access to the appropriate personnel without providing them the ability to manage the entire domain. Like domains, OUs are not a true security boundary. Although you can assign permissions to an OU, all OUs in the same domain authenticate resources against the domain and forest resources. Still, a well-designed OU hierarchy will aid the development, deployment, and management of effective security measures.

Your organization may need to consider divided administrative control of services and data within the current Active Directory design. Effective Active Directory design requires that you completely understand your organization's requirements for service autonomy and isolation as well as for data autonomy and isolation.

Administrative Boundaries

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

Service Administrators

Active Directory service administrators are responsible for the configuration and delivery of the directory service. For example, service administrators maintain domain controller servers, control directory-wide configuration settings, and ensure service availability. You should consider the Active Directory administrators in your organization to be your service administrators.

The Active Directory service configuration is often determined by attribute values. These attribute values correspond to settings for their respective objects, which are stored in the directory. Consequently, service administrators in Active Directory are also data administrators. Your organizational needs may require you to consider other service administrator groups for your Active Directory service design. Some examples include:

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

  The forest administrator chooses the group to administer each domain. Because of the high-level access that is granted to the administrator for each domain, these administrators should be highly trusted individuals. The domain administrators control the domains through the **Domain Administrators** group and other built-in groups.

- Groups of administrators who manage DNS.

  The DNS administrator group completes the DNS design and manages the DNS infrastructure. The DNS administrator manages the DNS infrastructure through the **DNS Administrators** group.

- Groups of administrators who manage OUs.

  The OU administrator designates a group or individual as a manager for each OU. Each OU administrator manages the data that is 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. OU administrators can also create new subtrees and delegate administration of the OUs for which they are responsible.

- Groups of administrators who manage infrastructure servers.

  The group that is responsible for infrastructure server administration manages WINS, DHCP, and potentially the DNS infrastructure. In some cases, the group that handles 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 manage data that is stored in Active Directory or on computers that are 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 that is 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:

- Control 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 no control over the configuration of the service itself.
- Manage member computers in the directory and the data that is on those computers.

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

To summarize, before the owners of Active Directory service and directory structures are allowed to join a forest or domain infrastructure, the organization must trust all service administrators in the forest and all domains. Also, enterprise security programs must develop standard policies and procedures that perform appropriate background checks for the administrators. In the context of this security guide, to trust service administrators means to:

- Reasonably believe that service administrators will primarily concern themselves with the organization's best interests. Organizations should not elect to join a forest or domain if the owners of that 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 abuse the privileges they have on the network. A rogue administrator within a forest could easily 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 their own domain. With the stolen SID added to the user's SID History, the rogue administrator would have administrative privileges in the stolen SID's domain as well as their own domain.
  - **Coerced administrators**. A trusted administrator might be coerced or compelled to perform operations that breach the security of a computer or the network. A user or administrator may use social engineering techniques or threats of physical or other harm on legitimate administrators of a computer to obtain the information that is needed to gain access to the computer.

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.

Active Directory and Group Policy

Although OUs offer an easy way to group computers, users, groups, and other security principals, they also provide an effective way to segment administrative boundaries. Additionally, OUs provide a crucial structure for the deployment of Group Policy objects (GPOs) because they can segment resources by security need and allow you to provide different security to different OUs. The use of OUs to manage and assign security policies based on server role is an integral piece of the overall security architecture for the organization.

Delegating Administration and Applying Group Policy

OUs are containers within the directory structure of a domain. These containers can hold any security principal in the domain, although they are usually used to hold objects of one specific type. To grant or revoke OU access permissions to a group or individual user, you can set specific access control lists (ACLs) on the OU and the permissions will be inherited by all of the objects within the OU.

You can use an OU to provide role-based administrative capabilities. For example, one group of administrators could be responsible for the user and group OUs while another group could manage the OUs that contain the servers. You can also create an OU to contain a group of resource servers to be administered by other users through a process called delegation of control. This approach provides the delegated group with autonomous control over a particular OU but does not isolate 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

Administrators can create administrative groups 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 run basic network services, including servers that provide WINS and DHCP services. Oftentimes an operations group or an infrastructure administration group maintains these servers. You can use an OU to easily provide administrative capabilities to these servers.

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

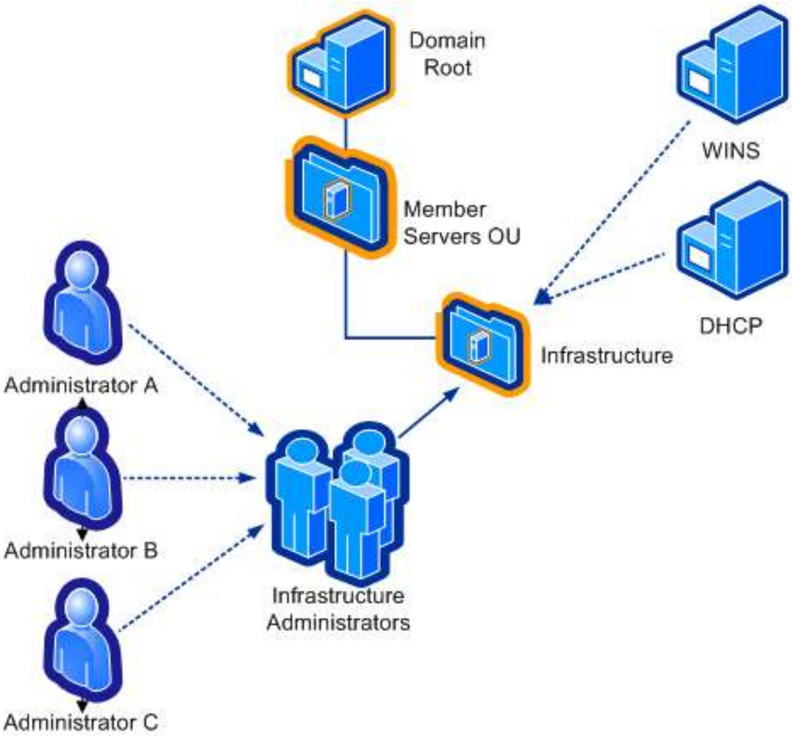


Figure 1.1 OU delegation of administration

When the **Infrastructure Administrators** group is delegated control of the Infrastructure OU, the members of this group gain full control of the Infrastructure OU and all servers and objects within the OU. This capability allows members of the group to secure the server roles with Group Policy.

This approach is only one way that you can use OUs to provide administrative segmentation. For more complex organizations, see the "More Information" section at the end of this chapter.

Note: Because Active Directory depends so heavily on DNS, it is common practice to run the DNS service on domain controllers. Domain controllers are placed in the built-in Domain Controllers OU by default. The examples in this guide follow this practice, so the infrastructure server role does not include the DNS service.

Time Configuration

Many security services, especially authentication, rely on an accurate computer clock to perform their jobs. You should ensure computer time is accurate and that all servers in your organization use the same time source. The Windows Server 2003 W32Time service provides time synchronization for Windows Server 2003 SP2 and Microsoft Windows XP SP3–based computers that run in an Active Directory domain.

The W32Time service synchronizes the clocks of Windows Server 2003 SP2–based computers with the domain controllers in a domain. This synchronization is necessary for the Kerberos authentication protocol and other authentication protocols to work properly. 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 authentication protocol might deny access to users.

Another important benefit that time synchronization provides is event correlation on all of the clients in your enterprise. Synchronized clocks on the clients in your environment ensure that you can correctly analyze events that take place in uniform sequence on those clients throughout the organization.

The W32Time service uses the Network Time Protocol (NTP) to synchronize clocks on computers that run Windows Server 2003 SP2. In a Windows Server 2003 SP2 forest, time is synchronized by default 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 they select a PDC emulator with which 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 authoritative time source, such as a reliable NTP source or a highly accurate clock on your network. Note that NTP synchronization uses UDP port 123 traffic. Before you synchronize with an external server, you should weigh the benefits of opening this port against the potential security risk.

Also, if you synchronize with an external server that you do not control, you risk configuring your servers with the incorrect time. The external server could be compromised or spoofed by an attacker to maliciously manipulate the clocks on your computers. As explained earlier, the Kerberos authentication protocol requires synchronized computer clocks. If they are not synchronized, a denial of service may occur.

Successful GPO Application Events

Although an administrator can manually check 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 was successfully downloaded to each of the servers.

An event similar to the following should display 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.

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 type of event if any changes occurred during these intervals. Also, the settings are refreshed every 16 hours, regardless of whether any changes were made. You can also manually force Group Policy settings to update using the procedure that is described later in this chapter.

Server Role OUs

The previous example showed a way to manage an organization's infrastructure servers. This method can be extended to encompass other servers and services in an organization. The goals are to create a seamless Group Policy for all servers and to ensure that the servers that reside within Active Directory meet the security standards for your environment.

This type of Group Policy forms a consistent baseline of standard settings for all of the servers in your organization. Also, the OU structure and the application of Group Policy must provide a detailed 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 are a few of the server roles in an organization that may require unique Group Policy.

Important: For simplicity, the examples in this chapter assume the use of the Enterprise Client environment. If you use one of the other two environments, substitute the appropriate file names. The differences between the two environments and their functionality are discussed in the Overview.

Member Server Baseline Policy

The first step in the establishment of server role OUs is to create a baseline policy. To create such a policy, you can use the SCW on a standard member server to create a Member Servers Baseline.xml file. As part of the XML creation, use the SCW to include one of the supplied Member Server Baseline Security Templates (EC-Member Server Baseline.inf or SSLF-Member Server Baseline.inf).

After you generate the SCW policy, it is converted into a GPO and linked with the Member Servers OU. This new baseline GPO 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. The Member Server Baseline Policy is discussed in Chapter 3, "Implementing the Security Baseline."

You should define the desired settings for most of the servers in your organization in the baseline Group Policy. Although there may be some servers that should not receive the baseline policy, these should not be many. If you create your own baseline Group Policy, make it as restrictive as possible and segment any servers that need to differ from this policy into separate server-specific OUs.

Server Role Types and OUs

Each identified server role requires an additional SCW policy, Security Template, and OU in addition to the baseline OU. This approach permits the creation of separate policies for the incremental changes that are required by each role.

In a previous example, the infrastructure servers were placed into the Infrastructure OU, which is a child of the Member Servers OU. The next step is to apply the appropriate configuration to these servers. Two Security Templates are provided with this solution, one for each security environment: EC-Infrastructure Server.inf and SSLF-Infrastructure Server.inf. When used together with the SCW, these Security Templates will help you create a security policy that contains the specific adjustments that are required by DHCP and WINS. The resultant policy is then converted into a new GPO and linked to the Infrastructure OU.

This GPO uses the **Restricted Groups** setting to add the following three groups to the **Local Administrators** group of all servers in the Infrastructure OU:

- **Domain Administrators**
- **Enterprise Administrators**
- **Infrastructure Administrators**

As mentioned earlier in this chapter, this approach is only one of many ways to create an OU structure that you can use to deploy GPOs. For more information about how to create

OUs for Group Policy implementation, see "Designing the Active Directory Structure" in the *Windows 2000 Server Resource Kit*.

The following table lists the Windows Server 2003 SP2 server roles and corresponding GPO backup files that are defined in this guide. The GPO backup file names are prefixed with the <*Env*> variable, which would be replaced by EC (for Enterprise Client) or SSLF (for Specialized Security – Limited Functionality) as appropriate.

Table 1.1 Windows Server 2003 SP2 Server Roles

Server role	Description	Security Template file name
Member server	All servers that are members of the domain and reside in or below the Member Servers OU.	<*Env*>-Member Server Baseline Policy
Domain controller	All Active Directory domain controllers. These servers are also DNS servers.	<*Env*>-Domain Controller Policy
Infrastructure server	All locked down WINS and DHCP servers.	<*Env*>-Infrastructure Servers Policy
File server	All locked down file servers.	<*Env*>-File Servers Policy
Print server	All locked down print servers.	<*Env*>-Print Servers Policy
Web server	All locked down IIS web servers.	<*Env*>-Web Servers Policy
IAS server	All locked down IAS servers.	<*Env*>-IAS Servers Policy
Certificate Services server	All locked down Certification Authority (CA) servers.	<*Env*>-CA Servers Policy

All GPOs are applied to the corresponding child OUs. Each of these child OUs require you to apply the specific configuration to define the role that each computer 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. Note that not all roles have GPOs that correspond to all environments. For example, the Certificate Authority role is always considered to be present in the EC environment.

Important: This guide assumes that computers running Windows Server 2003 SP2 perform specifically defined roles. If the servers in your organization do not match these roles, or if you use multipurpose servers, use the settings defined here as guidelines for your own Security Templates. However, remember that the more functions that each of your servers perform, the more vulnerable they are to attack.

Security Design

The security design this chapter recommends forms the starting point for the scenarios in this guide, as well as the mitigation suggestions for the scenarios. The remaining sections in this chapter provide design details about the core security structure:

- **OU Design for Security Policies**
- **GPO Design for Security Policies**

Microsoft strongly recommends that you perform your own testing in a lab environment before deploying new security policies to production computers. The settings recommended in this guide and stored as security baselines in the SCM tool have been thoroughly tested. However, your organization's network has unique business applications that may be impacted by some of these settings. Therefore, it is extremely important to thoroughly test the settings before implementing them on any production computers.

OU Design for Security Policies

The Microsoft security guides for Windows, Office, and Internet Explorer use organizational units (OUs). An *OU* is a container within a domain that uses AD DS. An OU may contain users, groups, computers, and other OUs. If an OU contains other OUs, it is a parent OU. An OU within a parent OU is a child OU.

You can link a GPO to an OU, which will then apply the GPO's settings to the users and computers that are contained in that OU and its child OUs. And to facilitate administration, you can delegate administrative authority to each OU.

OUs provide an effective way to segment administrative boundaries for users and computers. Microsoft recommends that organizations assign users and computers to separate OUs, because some settings only apply to users and other settings only apply to computers.

You can delegate control over a group or an individual OU by using the Delegation Wizard in the Microsoft® Management Console (MMC) Active Directory Users and Computers snap-in tool. See the "More Information" section at the end of this chapter for links to documentation about how to delegate authority.

One of the primary goals of an OU design for any environment is to provide a foundation for a seamless Group Policy implementation that applies to all client computers in AD DS. This ensures that the client computers meet the security standards of your organization. The OU design must also provide an adequate structure to accommodate security settings for specific types of users in an organization. For example, developers may require access to their computers that average users do not. Also, laptop users may have different security requirements than desktop users.

The following figure illustrates a simple OU structure that is sufficient for the Group Policy discussion in this chapter. This OU structure may differ from the requirements of your organization's environment.

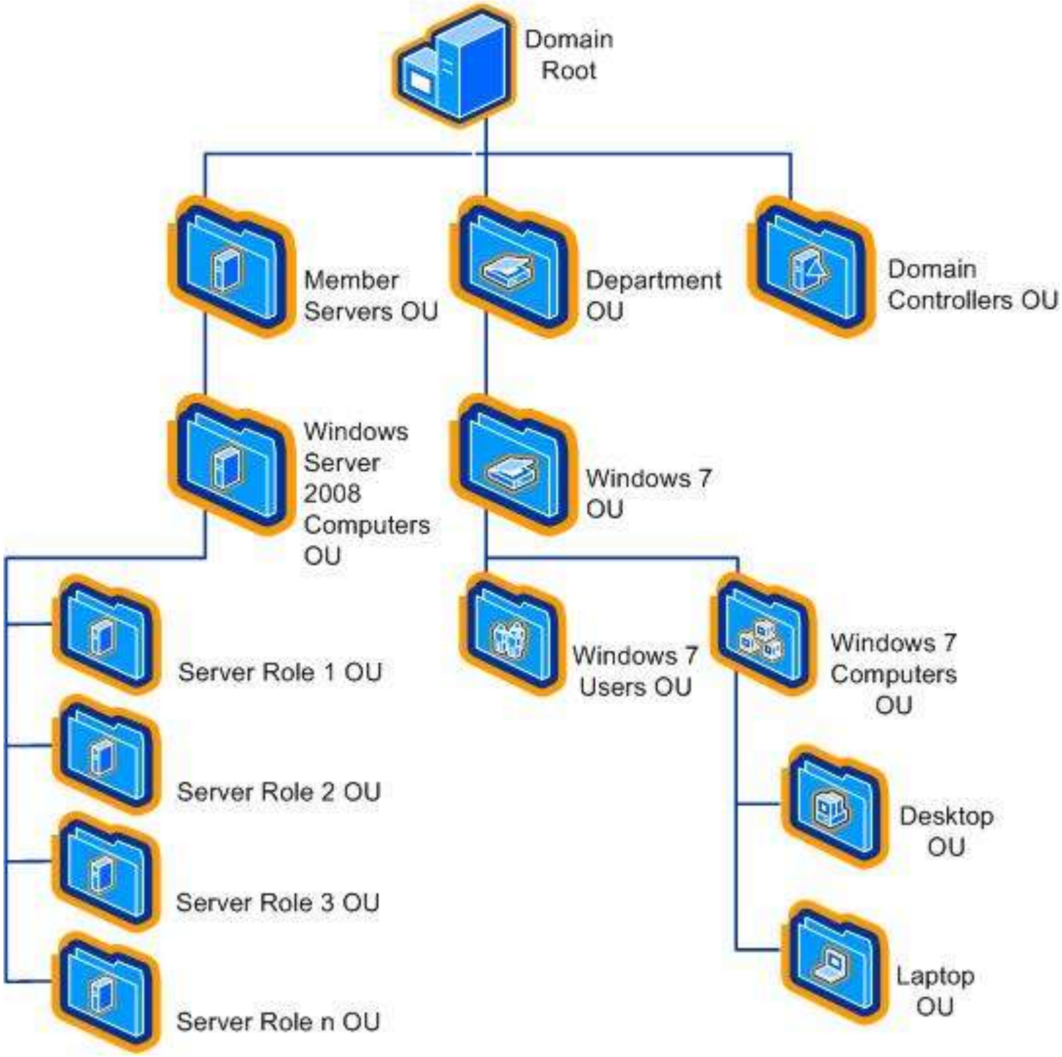


Figure 1.1 Example OU structure for computers running Windows 7 and Windows Server 2008

Domain Root

You should apply some security settings throughout the domain to control how the domain, as a whole, is configured. These settings are contained in GPOs that apply to the domain. Computers and Users are not managed in this container.

Domain Controllers OU

Domain controllers hold some of the most sensitive data in your organization — data that controls the security configuration itself. You apply GPOs at this level in the OU structure to configure and protect the domain controllers.

Member Servers OU

This OU contains child OUs as described below. You should include settings that apply to all servers, but not to workstations, in the GPOs that you apply to this OU.

Server Role OUs

Microsoft recommends creating an OU for each server role that your organization uses. Each OU should contain only one type of server computer. You can then configure GPO settings and apply them to OUs that are specific to each role.

You can also choose to combine certain roles on the same server, if your organization requires it. For example, you may choose to combine the File and Print server roles. In this case, you can create an OU for these combined server roles called "File and Print Server," and then link the two role-specific GPO policies to that OU.

Important Combining server roles on the same computer requires careful planning and testing to ensure that you do not negatively affect the overall security of the server roles that you combine.

Department OU

Security requirements often vary within an organization. For this reason, it may make sense to create one or more department OUs in your environment. This OU enables you to apply security settings from GPOs to computers and users in their respective department OUs.

Windows 7 Users OU

This OU contains the user accounts for the EC environment. The settings that you apply to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide.

Windows 7 Computers OU

This OU contains child OUs for each type of client computer running Windows 7 in the EC environment. This guide focuses on security guidance for desktop and laptop computers. For this reason, the engineers for this guide created the following computer OUs:

- **Desktop OU**. This OU contains desktop computers that constantly remain connected to the network. The settings applied to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook.
- **Laptop OU**. This OU contains laptop computers for mobile users that are not always connected to the network. The Windows 7 Security Baseline Settings Excel workbook also provides details about the settings that apply to this OU.

GPO Design for Security Policies

A *GPO* is a collection of Group Policy settings that are essentially the files created by the Group Policy snap-in. The settings are stored at the domain level and affect users and computers contained in sites, domains, and OUs.

You can use GPOs to ensure that specific policy settings, user rights, and computer behavior apply to all client computers or users in an OU. Using Group Policy instead of a manual configuration process makes it simple to manage and update changes for many computers and users. Manual configuration, which is inefficient because it requires a technician to visit each client computer, is also potentially ineffective. This is primarily because if the policy settings in domain-based GPOs are different than those applied locally, the domain-based GPO policy settings will overwrite the locally applied policy settings.

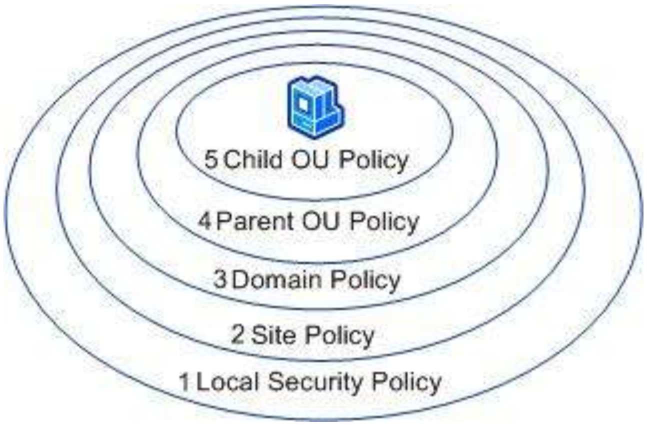


Figure 1.2 GPO order of precedence

The previous figure shows the order of precedence in which GPOs are applied to a computer that is a member of the Child OU, from the lowest priority (1) to the highest priority (5). Group Policy is applied first from the local security policy of each workstation. After the local security policy is applied, GPOs are next applied at the site level, and then at the domain level.

For computers running Windows Server 2008, Windows Server 2003 SP2 or later, and Windows Vista SP1 or Windows XP Professional SP3 or later that are nested in several OU layers, GPOs are applied in order from the parent OU level in the hierarchy to the lowest child OU level. The final GPO is applied from the OU that contains the computer account. This order of GPO processing for Group Policy—local security policy, site, domain, parent OU, and child OU—is significant because settings in GPOs that are applied later in the process will overwrite settings applied earlier. Different values for the same setting configured in different GPOs are never combined. User GPOs are applied in the same manner.

The following considerations apply when you design Group Policy:

- An administrator must set the order in which you link multiple GPOs to an OU, or Group Policy will be applied by default in the order it was linked to the OU, the order of precedence for the GPOs linked to the currently selected OU is shown in the **Link Order** list in the GPMC. If the same setting is configured in multiple policies, the policy that is highest on the policy list for the container will take precedence.
- You may configure a GPO with the **Enforced** option. However, if you select this option, other GPOs cannot override the settings that are configured in this GPO.
- Group Policy settings apply to users and computers, and are based on where the user or computer object is located in AD DS. In some cases, user objects may need policy applied to them based on the location of the computer object, not the location of the user object. The Group Policy loopback feature gives the administrator the ability to apply user Group Policy settings based on which computer the user is logged on to. The "Loopback Processing of Group Policy" article provides more information about this option.
- You may configure an Active Directory site, domain, or OU with the **Block policy inheritance** option. This option blocks GPO settings from GPOs that are higher in the Active Directory hierarchy unless they have the **Enforced** option selected. In other words, the **Enforced** option has precedence over the **Block policy inheritance** option.

Note Administrators should only use the **Enforced** option and the **Block policy inheritance** option with utmost care because enabling these options can make troubleshooting GPOs difficult and cumbersome.

Recommended GPOs

To implement the OU design described above requires a minimum of the following GPOs:

- A policy for the domain.
- A policy to provide the baseline security settings for all domain controllers.
- A policy to provide the baseline security settings for all member servers.
- A policy for each server role in your organization.
- A policy for the Windows 7 Users OU.
- A policy for the Desktop OU.
- A policy for the Laptop OU.

The following figure expands on the preliminary OU structure to show the linkage between these GPOs and the OU design.

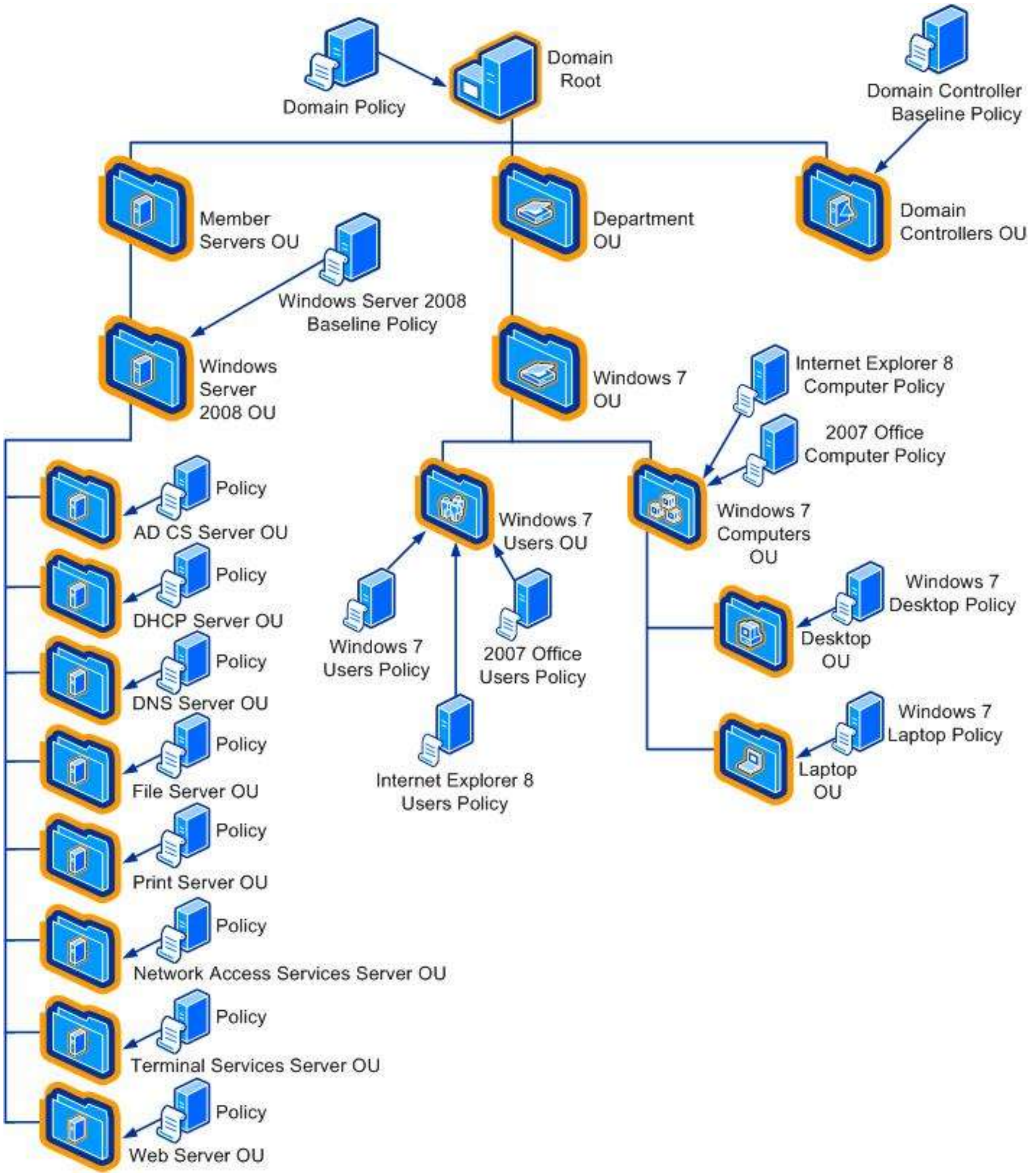


Figure 1.3 Example OU structure and GPO links for computers running Windows 7 and Windows Server 2008

While the guide you are reading only covers a single product from Microsoft, the previous figure illustrates an environment that combines recommendations from the following security guides available in the Security Compliance Management Toolkit Series:

- *Windows Server 2008 Security Guide*
- *Windows 7 Security Guide*
- *2007 Microsoft Office Security Guide*
- *Internet Explorer 8.0 Security Guide*

Presumably you network is running multiple versions of the Windows operating system and perhaps 2007 Office or Internet Explorer 2008. The combined example in the previous figure presents a notional AD DS design for OUs and Group Policy objects (GPOs). You will need to design your own OU hierarchy and Group Policy to fit the versions of Windows deployed in your environment, as well as settings for Microsoft Office or Internet Explorer as needed.

In the example in the previous figure, laptop computers are members of the Laptop OU. The first policy that is applied is the local security policy on the laptop computers. Because there is only one site in this example, no GPO is applied at the site level, which leaves the Domain GPO as the next policy that is applied. Finally, the Laptop GPO is applied.

Also in this figure, a File server is a member of the File Server OU. The first policy that is applied to the server is the local security policy. However, in general, little if any configuration of the servers is done by local policy. Security policies and settings should always be enforced by Group Policy.

Because there is only one File server in this example, no GPOs are applied at this level, which leaves the Domain GPO as the next policy that is applied to the servers. The Windows Server 2008 EC Baseline Policy is then applied to the Member Servers OU. Finally, any specific polices for the Web servers in the environment are applied to the Web Server OU.

As a precedence example, consider a scenario in which the policy setting for **Allow logon through Terminal Services** is set to apply to the following OUs and user groups:

- Member Servers OU – **Administrators** group
- Web Server OU – **Remote Desktop Users** and **Administrators** groups

In this example, logon through Terminal Services has been restricted to the **Administrators** group for servers in the Member Servers OU. However, a user whose account is in the **Remote Desktop Users** group can log on to a File server through Terminal Services because the File Servers OU is a child of the Member Servers OU and the child policy takes precedence.

If you enable the **Enforced** policy option in the GPO for the Member Servers OU, only users with accounts in the **Administrators** group can log on to the File server computer through Terminal Services. This is because the **Enforced** option prevents the child OU policy from overwriting the policy applied earlier in the process.

Using a GPO Created with the Security Compliance Manager Tool

The specific setting recommendations presented in this guide are available as pre-built baselines in the SCM tool. You can use these baselines created by Microsoft "as is", however most organizations will require some customization. When a baseline reflects your organization’s requirements, use the SCM tool to generate a GPO backup file. For more information about using the SCM tool, review the information available in the Help Topics for the tool. You can then use the Group Policy Management Consol (GPMC) to import the settings from the backed-up GPOs into your AD DS domain.

To import policy settings from a backed-up GPO into a GPO

1. In the GPMC console tree, expand **Group Policy Objects** in the forest and domain containing the GPO into which you want to import policy settings.
2. Right-click the GPO into which you want to import policy settings, and then click **Import Settings**.
3. When the **Import Settings Wizard** opens, follow the instructions in the wizard that opens, and then click **Finish**.
4. After the import operation completes, a summary will state whether the import succeeded. Click **OK**.

Using migration tables

Because some data in a GPO is domain-specific and might not be valid when copied directly to another domain, the GPMC provides migration tables. A migration table is a simple table that specifies a mapping between a source value and a destination value.

A migration table converts, during the copy or import operation, the references in a GPO to new references that will work in the target domain. You can use migration tables to update security principals and UNC paths to new values as part of the import or copy operation. Migration tables are stored with the file name extension .migtable, and are actually XML files. You do not need to know XML to create or edit migration tables; the GPMC provides the MTE for manipulating migration tables.

A migration table consists of one or more mapping entries. Each mapping entry consists of a source type, source reference, and destination reference. If you specify a migration table when performing an import or copy operation, each reference to the source entry is replaced with the destination entry when the policy settings are written into the destination GPO. Before you use a migration table, ensure that the destination references specified in the migration table already exist.

The following items can contain security principals and can be modified by using a migration table:

- Security policy settings of the following types:
  - User rights assignments.
  - Restricted groups.
  - System services.
  - File system.
  - Registry.
- Advanced folder redirection policy settings.
- The GPO Discretionary Access Control List (DACL), if it is preserved during a copy operation.
- The DACL on software installation objects, which is only preserved if the option to copy the GPO DACL is specified.

Also, the following items can contain UNC paths, which might need to be updated to new values as part of the import or copy operation, because servers in the original domain might not be accessible from the domain to which the GPO is being migrated:

- Folder redirection Group Policy settings.
- Software installation Group Policy settings.
- References to scripts, such as for logon and startup scripts, that are stored outside the source GPO. The script itself is not copied as part of the GPO copy or import operation, unless the script is stored inside the source GPO.

For more information about using the GPMC to import settings see the Group Policy Planning and Deployment Guide.

OU, GPO, and Group Design

The recommended OUs and policies that were discussed in the previous section create a baseline or new environment to restructure an organization's existing OU structure for computers that run Windows Server 2003 SP2. Administrators use their predefined administration boundaries to create their respective administrative groups. An example of the correlation of these groups to the OUs they manage is shown in the following table.

Table 1.2 OUs and Administrative Groups

OU name	Administrative group
Domain Controllers	Domain Engineering
Member Servers	Domain Engineering
Infrastructure	Infrastructure Administrators
File	Infrastructure Administrators
Print	Infrastructure Administrators
IAS	Domain Engineering
Web	Web Services
CA	Enterprise Administrators

Each administrative group was created as a global group within the domain by the **Domain Engineering** members, who are responsible for Active Directory infrastructure and security. They used the corresponding GPO to add each of these administrative groups to the appropriate restricted group. The administrative groups that are listed in the table will only be members of the **Local Administrators** group for the computers that are located in the OUs that specifically contain computers for their job functions.

Finally, the **Domain Engineering** members set permissions on each GPO so that only administrators in their group are able to edit them. Note that the creation and configuration of these groups is a part of your overall Active Directory design and implementation process. It is not part of this guide.

Process Overview

This guide combines the strengths of the SCW-based and Group Policy-based approaches. This hybrid approach allows you to create and test security configurations more easily, but still provides the flexibility and scalability that is required in large Windows networks.

The process that is used to create, test, and deploy the policies is as follows:

5. Create the Active Directory environment, including groups and OUs. You should create the appropriate administrative groups and delegate OU permissions to the corresponding groups.
6. Configure time synchronization on the domain controller that hosts the PDC Emulator FSMO.
7. Configure the domain policies.
8. Create the baseline policies with SCW.
9. Test the baseline policies with SCW.
10. Convert the baseline policies to GPOs and link them to the appropriate GPOs.
11. Create the role policies with SCW and the included Security Templates.
12. Test the role policies with SCW.
13. Convert the role policies to GPOs and link them to the appropriate GPOs.

The following sections describe these steps in greater detail.

Note: For simplicity, the examples in this section assume the use of the Enterprise Client (EC) environment. If you use one of the other two environments, substitute the appropriate file names. The differences between the two environments and their functionality are discussed in the Overview.

Create the Active Directory Environment

Before you can begin the hardening process, you must have an appropriate Active Directory domain and OU structure in place. The following procedure lists the steps to create the OUs and groups that are used in this guide and then configure them for appropriate administrative access.

1. Open the MMC Active Directory Users Computers snap-in (Dsa.msc).
2. In the root of the domain object, create an OU called **Member Servers**.
3. Navigate to this new OU, and then create a child OU within it called **Infrastructure**.
4. Move all WINS and DHCP servers into the **Infrastructure** OU.
5. Create a global security group called **Infrastructure Administrators**, and then add the appropriate domain accounts to it.
6. Run the Delegation of Control Wizard to provide the **Infrastructure Administrators** group with Full Control of the OU.
7. Repeat steps 3 through 6 for the file server, print server, Web server, IAS server, and Certificate Services server roles. Use the information in Table 1.2 for the appropriate OU and group names.

Configure Time Synchronization

The following procedure ensures that the domain controllers and member servers are synchronized with an external time source. This synchronization helps to ensure that Kerberos authentication works properly and allows you to keep your Active Directory domain synchronized with any external computers that you may have.

1. On the domain controller with the PDC Emulator FSMO, open a command prompt and then execute the following command, where <*PeerList*> is a comma-separated list of DNS names or IP addresses for the desired time sources:

   ```
   w32tm /config /syncfromflags:manual /manualpeerlist:<PeerList>
   ```

2. To update the configuration, execute the following command:

   ```
   w32tm /config /update
   ```

3. Check the event log. If the computer cannot reach the servers, the procedure will fail and an entry will be 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, you can run this procedure on any computer that runs Windows XP SP3 or Windows Server 2003 SP2.

It is not usually necessary to synchronize all server time clocks with an external source if they are synchronized with the same internal source. By default, member computers always synchronize their clocks with domain controllers.

Note: For accurate log analysis, you should also synchronize the clocks of network computers that run operating systems other than Windows to the Windows Server 2003 PDC emulator or to the same time source for that server.

Introducing the Local Policy Tool

When you install the SCM tool, another utility called the Local Policy Tool (LPT) becomes available. This tool is designed to assist you with two optional tasks:

- Applying a security baseline to the local Group Policy of a computer.
- Exporting the local Group Policy of a computer to a group policy backup file.
- Updating the user interface of the Group Policy management tools.

You may want to apply the settings to the local Group Policy for stand-alone computers. You should update the user interface on the computers you will use to manage Group Policy so that you can view and manage the additional security settings discussed in this guide. The following sections discuss how to use the LPT to accomplish these tasks.

Modifying Local Group Policy

You can use the LPT to modify the local Group Policy of a computer by applying the security settings included in the GPOs described earlier. The LPT will apply the security setting values recommended in this guide to modify the local policy. The tool does this by importing the settings from a GPO backup into the local Group Policy. Use the SCM tool to generate the GPO backup for the desired baseline.

To apply a GPO backup file to the local Group Policy

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.

   Note If prompted for logon credentials, type your user name and password, and then press ENTER.

4. At the command prompt, type **cscript LocalGPO.wsf /Path:<path>** and then press ENTER where <path> is the path to the GPO backup.

5. Completing this procedure modifies the local security policy settings using the values included in the GPO backup. You can use GPEdit.msc to review the configuration of the local Group Policy on your computer.

To restore local Group Policy to the default settings

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.

   Note If prompted for logon credentials, type your user name and password, and then press ENTER.

4. At the command prompt, type **cscript LocalGPO.wsf /Restore**, and then press ENTER.

Completing this procedure restores all local policy settings to their default values.

Exporting Local Group Policy to a GPO Backup

You can use LPT to export a computer’s local Group Policy to a GPO backup file, which you can than apply to the local Group Policy of other computers or import into Active Directory.

To export local Group Policy to a GPO backup file

5. Log on as an administrator.
6. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
7. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.

   Note If prompted for logon credentials, type your user name and password, and then press ENTER.
8. At the command prompt, type **cscript LocalGPO.wsf /Path:<path> /Export** and then press ENTER where <path> is the path to the GPO backup.
9. Completing this procedure exports all local security policy settings to a GPO backup.

Updating the Security Configuration Editor User Interface

The solution presented in this guidance uses GPO settings that do not display in the standard user interface (UI) for the GPMC or the Security Configuration Editor (SCE) tool. These settings, which are all prefixed with **MSS:**, were developed by the Microsoft Solutions for Security group for previous security guidance.

For this reason, you need to extend these tools so that you can view the security settings and edit them as required. To accomplish this, the LPT automatically updates your computer while it creates the GPOs. Use the following procedure to update the SCE on the computers where you plan to manage the GPOs created with the SCM tool.

To modify the SCE to display MSS settings

1. Ensure that you have met the following prerequisites:
   - The computer is joined to the domain using Active Directory where you created the GPOs.
   - The **SCM** tool is installed.
2. Log on as an administrator.
3. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
4. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.

   Note If prompted for logon credentials, type your user name and password, and then press ENTER.
5. At the command prompt, type **cscript LocalGPO.wsf /ConfigSCE** and then press ENTER.

   Note This script only modifies SCE to display MSS settings. This script does not create GPOs or OUs.

The following procedure removes the additional MSS security settings, and then resets the SCE tool to the default settings.

To reset the SCE tool to the default settings

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.

   Note If prompted for logon credentials, type your user name and password, and then press ENTER.
4. At the command prompt, type **cscript LocalGPO.wsf /ResetSCE** and then press ENTER.

Note Completing this procedure reverts the SCE on your computer to the default settings. Any settings added to the default SCE will be removed. This will only affect the ability to view the settings with the SCE. Configured Group Policy settings remain in place.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- *Best Practice Guide for Securing Active Directory Installations*.
- Design Considerations for Delegation of Administration in Active Directory.
- "How to configure an authoritative time server in Windows 2000": Microsoft Knowledge Base article 216734.
- "Service overview and network port requirements for the Windows Server system": Microsoft Knowledge Base article 832017.
- Ten Immutable Laws of Security.
- Trustworthy Computing.

Chapter 2: Implementing the Domain Policy

This chapter uses the construction of a domain environment to demonstrate ways to address security within a Windows Server® 2003 Service Pack 2 (SP2) infrastructure.

This chapter focuses on the following topics:

- Security settings and countermeasures at the domain level.
- How to secure a Windows Server 2003 SP2 domain for the Enterprise Client (EC) and Specialized Security – Limited Functionality (SSLF) environments that are defined in the Overview to this guide.

This information provides a foundation and a vision for how to evolve from an existing environment to an SSLF environment within a domain infrastructure.

Windows Server 2003 SP2 or later ships with default values that are set to a known, highly 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 about all default settings, see the companion guide, *Threats and Countermeasures*.

You can now harden the default operating system using only Group Policy objects (GPOs). Previous guidance from Microsoft required importing Security Template .inf files and extensive manual modification of the Administrative Templates portion of several GPOs. Working with these files and templates is no longer necessary. You can also use the Microsoft Excel® workbook Windows Server 2003 Security Baseline Settings to reference all of the recommended Group Policy settings.

To deploy this guidance, you need to:

- Create an organizational unit (OU) structure for your environment.
- Run the SCM tool for this guide.

  Important You must run the .msi file for the SCM tool that accompanies the download for this toolkit to create, test, and deploy the security settings for the *Windows Server 2003 Security Guide*. This tool automatically creates all the GPOs for the security settings this guide recommends. The tool also includes the LPT that you can use to apply security settings to stand-alone servers, as discussed in the previous chapter.

- Use the Group Policy Management Console (GPMC) to link and manage the GPOs.

Caution It is essential to thoroughly test your OU and GPO designs before deploying them in a production environment.

Domain Policy

You can apply Group Policy security settings at several different levels in an organization. The baseline environment discussed in Chapter 1, "Windows Server 2003 Hardening Mechanisms," uses Group Policy to apply settings at the following three hierarchy levels in the domain infrastructure:

- **Domain Level**. Settings at this level address common security requirements, such as account and password policies that must be enforced for all servers in the domain.

- **Baseline Level**. Settings at this level address specific server security requirements that are common to all servers in the domain infrastructure.
- **Role-Specific Level**. Settings at this level address security requirements for specific server roles. For example, the security requirements for infrastructure servers differ from those for servers that run Microsoft Internet Information Services (IIS).

The following sections of this chapter only discuss the Domain Level policy in detail. Most of the domain security settings that are addressed are for user accounts and passwords. When you review these settings and recommendations, remember 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 create a standard network computer configuration. Group Policy objects (GPOs) can provide a significant portion of a configuration management solution for any organization, because they allow administrators to make security changes simultaneously on all computers in the domain or subsets of the domain.

The following sections provide detailed information about the security settings that you can use to enhance the security of Windows Server 2003 SP2 or later. Tables are provided that summarize the settings, and detailed descriptions of how to achieve the security objectives for each setting are also provided. The settings are divided into categories that correspond to their presentation in the Windows Server 2003 Security Configuration Editor (SCE) user interface.

You can simultaneously apply the following types of security changes through Group Policy:

- Modify permissions on the file system.
- Modify permissions on registry objects.
- Change settings in the registry.
- Change user right assignments.
- Configure system services.
- Configure audit and event logs.
- Set account and password policies.

This guide recommends that you create a new Group Policy at the domain root to apply the domain-wide policies that are discussed in this chapter. This approach will make it easier for you to test or troubleshoot the new Group Policy, because if you need to roll back changes you can simply disable it. However, some applications that are designed to work with Active Directory make changes to the built-in Default Domain Policy. These applications are not going to be aware of the new Group Policy you implemented if you follow the recommendations in this guide. For this reason, before you deploy new enterprise applications, be sure to test them thoroughly. If you encounter problems, check to see whether the application has modified account policies, created new user accounts, modified user rights, or made other changes to the Default Domain Policy or local computer 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 both of the environments that are defined in this guide. Password policy provides a way to set complexity and change schedules for high security environments. Account lockout policy allows tracking of unsuccessful password logon attempts to initiate account lockouts if necessary. Kerberos policies are used for domain user accounts, and determine settings that relate to the Kerberos authentication protocol, such as ticket lifetimes and enforcement.

Password Policy

Complex passwords that are changed on a regular basis 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 they relate to each of the environments that are defined in this guide: Enterprise Client and Specialized Security – Limited Functionality.

Strict requirements for password length and complexity do not necessarily mean that users and administrators will use strong passwords. Although password policy may require users to comply with technical complexity requirements, additional strong security policy is needed to ensure that users create passwords that are hard to compromise. For example, Breakfast! might meet all password complexity requirements, but it is not a very difficult password to crack.

If you know certain facts about the person who creates a password, you might be able to guess their password if it is based on their favorite food, car, or movie. One strategy of organizational security programs that seek to educate users about strong passwords is to create a poster that describes poor passwords and display it in common areas, such as near a water fountain or copy machine. Your organization should set strong password creation guidelines that include the following:

- Avoid the use of words from a dictionary in any language, including common or clever misspellings of words.
- Do not create a new password that simply increments a digit in your current password.
- Avoid the use of passwords that begin or end with a numeral because they can be guessed easier than passwords that have a numeral in the middle.
- Avoid the use of passwords that others can easily guess by looking at your desk (such as names of pets, sports teams, and family members).
- Avoid the use of words from popular culture.
- Enforce the use of passwords that require you to type with both hands on the keyboard.
- Enforce the use of uppercase and lowercase letters, numbers, and symbols in all passwords.
- Enforce the use of space characters and characters that can be produced only by pressing the ALT key.

You should also use these guidelines for all service account passwords in your organization.

How to Prevent Users from Changing a Password Except When Required

Although the password policy settings that are described in the previous section provide a range of options, some organizations require centralized control over all users. This section describes how to prevent password changes by users except when changes are required.

Centralized control of user passwords is a cornerstone of a well-crafted Windows Server 2003 SP2 security scheme. You can use Group Policy to set minimum and maximum password ages as discussed earlier, but remember that frequent password change requirements 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 from users who forget their passwords.

Users can change their passwords during the period between the minimum and maximum password age settings. However, the Specialized Security – Limited Functionality environment design requires that users change their passwords only when the operating system prompts them to do so after the **Maximum password age** setting of 90 days. To prevent password changes (except when required), you can disable the **Change Password** option in the **Windows Security** dialog box that appears when you press CTRL+ALT+DELETE. Note that security-conscious users may want to change their passwords more often and will have to contact an administrator to do so, which will increase support costs.

You can implement this configuration for an entire domain through Group Policy, or you can edit the registry to implement it for one or more specific users. For more detailed instructions about this configuration, see "How To Prevent Users from Changing a Password Except When Required in Windows Server 2003": Microsoft Knowledge Base article 324744.

Account Lockout Policy

Account lockout policy is a Windows Server 2003 SP2 security feature that locks a user account after a number of failed logon attempts occur within a specified time period. The number of attempts that are allowed and the time period are based on the values that are configured for the policy. Windows Server 2003 SP2 tracks logon attempts, and the server software can be configured to disable accounts after a preset number of failed logins as a response to potential attacks.

These policy settings help protect user passwords from attackers who guess passwords, and they decrease the likelihood of successful attacks on your network. However, you will likely incur higher support costs if you enable account lockout policy, because users who forget or mistype their passwords repeatedly will need assistance. Before you enable the following settings, ensure that your organization is prepared for this additional overhead. For many organizations, an improved and less-costly solution is to automatically monitor the Security event logs for domain controllers and generate administrative alerts when apparent attempts to guess passwords for user accounts occur. See Chapter 2, "Domain Level Policies," of the companion guide, *Threats and Countermeasures*, for additional discussion of these settings and how they interact.

Kerberos Policies

Kerberos policies are used for domain user accounts. These policies determine settings that relate to the Kerberos version 5 authentication protocol, such as ticket lifetimes and enforcement. Kerberos policies do not exist in the local computer policy. If you reduce the lifetime of Kerberos tickets, the risk of an attacker who attempts to steal passwords to impersonate legitimate user accounts is decreased. However, the need to maintain these policies increases the authorization overhead.

In most environments, the default values for these policies should not be changed. Because the Kerberos settings are included in the default domain policy and enforced there, this guide does not include them in the Security Templates that accompany this guide. This guide recommends to not change any of the default Kerberos policies. For more information about these policy settings, refer to the companion guide, *Threats and Countermeasures*.

System Services

System services can be configured to one of three startup types: automatic, disabled, and manual. While the meanings of the first two should be obvious, the third startup type does cause confusion sometimes. When a service is configured to manual startup, it launches when a specific event occurs. For example, the Disk Management service launches when the Disk Management snap-in opens. In other cases a service may launch another when specific conditions are met. The key thing to remember when modifying the configuration of a system service is that changing the default startup type from manual or automatic to any other value will probably cause the service, and consequently some Windows features, to behave differently or fail.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- Network access: Allow anonymous SID/name translation for information about the ability of anonymous users to request security identifier attributes for other users.
- "The Mole #32: Technical Answers from Inside Microsoft - Moving Users, Sharing Printers, Two PDCs, Logoff, BackTalk" for information about network security and how to force logoff when logon hours expire.

Chapter 3: Implementing the Security Baseline

This chapter documents the configuration requirements to manage a baseline security template for all servers that run Windows Server® 2003 Service Pack 2 (SP2). The chapter also provides administrative guidance for the setup and configuration of a secure Windows Server 2003 SP2 or later configuration in two distinct environments. The configuration requirements in this chapter form the baseline for all of the procedures that are described in later chapters of this guide. These chapters describe how to harden specific server roles.

The setting recommendations in this chapter will help establish security at the foundation of 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 you implement them in production environments.

The recommendations in this chapter are suitable for most organizations and may be deployed on either existing or new computers that run Windows Server 2003 SP2. The default security configurations within Windows Server 2003 SP2 were researched, reviewed, and tested by the team that created this guide. For information about all default settings and a detailed explanation of each of the settings that are discussed in this chapter, see the companion guide, *Threats and Countermeasures*. Generally, most of the following configuration recommendations provide greater security than the default settings.

The security settings that are discussed in this chapter relate to the following environments:

- **Enterprise Client (EC)**. This environment provides solid security and is designed for more recent versions of the Windows operating system. The EC environment includes client computers that run Windows 2000 Professional and Windows XP Professional SP3. Most of the work that is required to migrate from an older environment to the EC environment involves upgrades of legacy clients such as Windows 98 and Windows NT 4.0 Workstation to Windows 2000 or Windows XP Professional SP3. All domain controllers and member servers in this environment run Windows 2000 Server or Windows Server 2003 SP2.
- **Specialized Security – Limited Functionality (SSLF)**. This environment provides much stronger security than the EC environment. Migration from the EC environment to the Specialized Security – Limited Functionality (SSLF) environment requires compliance with stringent security policies for both client computers and servers. This environment includes client computers that run Windows 2000 Professional and Windows XP Professional SP3, and domain controllers that run Windows 2000 Server or Windows Server 2003 SP2. In the SSLF environment, security concerns are so great that significant loss of client functionality and manageability is considered an acceptable tradeoff if the highest levels of security can be achieved. Member servers in this environment run Windows 2000 Server or Windows Server 2003 SP2.

You will notice that in many cases the SSLF environment will explicitly set the default value. You should assume that this configuration will affect compatibility, because it may cause applications that attempt to adjust some settings locally to fail. For example, some applications need to adjust user right assignments to grant their service account additional privileges. Because Group Policies take precedence over local machine policy, these operations will fail. You should thoroughly test all applications before you deploy any of the recommended settings to your production computers—especially SSLF settings.

Organizations that want to secure their environments by means of a phased approach may choose to start at the Enterprise Client environment level and then gradually migrate to more secure environments as they upgrade and test their applications and client computers 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 to link this policy and apply it to all servers in an organization.

Windows Server 2003 SP2 ships with default setting values that are configured to create a secure environment. In many instances, this chapter prescribes settings that are different than the default values. The chapter also enforces specific defaults for both of the environments. For information about all default settings, see the companion guide, *Threats and Countermeasures*.

Audit Policy

Administrators should create an Audit policy that defines which security events get reported, and that records user or computer activity in specified event categories. Administrators 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 Audit policy setting.

Before you implement an Audit policy, you must decide which event categories to audit for the environment. The audit settings that an administrator chooses for the event categories define the organization's Audit policy. When audit settings for specific event categories are defined, administrators can create an Audit policy that suits the security needs of the organization.

If no Audit policy exists, it will be difficult or impossible to determine what took place during a security incident. However, if audit settings are configured so that many authorized activities generate events, the Security log will fill up with useless data. The following recommendations and setting descriptions are provided to help you determine what to monitor so that the collected data is relevant.

Oftentimes, failure logs are much more informative than success logs because failures typically indicate errors. For example, successful logon to a computer by a user would typically be considered normal. However, if someone unsuccessfully tries to log on to a computer multiple times, it may indicate an attempt to break into the computer with someone else's account credentials. The event logs record events on the computer. In Microsoft Windows operating systems, there are separate event logs for applications, security events, and system events. The Security log records audit events. The event log container of Group Policy is used to define attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods.

Before an Audit policy implementation, organizations should determine how they will collect, organize, and analyze the data. Large volumes of audit data have little value if there is no plan to exploit it. Also, performance may be affected when computer networks are audited. The impact for a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server. Therefore, you should test whether performance will be affected before you deploy new audit settings in your production environment. For more information that can help you to analyze audit data, see "Security Monitoring and Attack Detection Planning Guide" and the “Events and Errors Message Center” online.

User Right Assignments

User right assignments provide users and groups with logon rights or privileges on the computers in your organization. An example of a logon right is the right to log on to a computer interactively. An example of a privilege is the right to shut down the computer. Both types are assigned by administrators to individual users or groups as part of the security settings for the computer.

Note: Throughout this section, "Not defined" applies only to users; Administrators still have the user right. Local administrators can make changes, but any domain-based Group Policy settings override them the next time that the Group Policies are refreshed or reapplied.

You can configure the user right assignment settings in Windows Server 2003 SP2 at the following location within the Group Policy Object Editor:

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

The default user right assignments are different for the various types of servers in your organization. For example, Windows Server 2003 SP2 assigns different rights to built-in groups on member servers and domain controllers. Similarities between built-in groups on different server types are not documented in the following list.

- **Member Servers**
  - **Power Users**. Possess most administrative powers with some restrictions. Power Users can run legacy applications in addition to applications that are certified for Windows Server 2003 SP2 or Windows XP Professional SP3.
  - **HelpServicesGroup**. 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 the Telnet server on the network.
- **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 network.
  - **Windows Authorization Access Group**. Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on user objects.

The **Guests** group 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 computer on which 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 could be created on a domain controller in a test environment.

Note: Because of the unique SIDs that exist between members of the **Guests** group, Support_388945a0, and Guest, some settings that are used to harden servers cannot be automated by means of the security templates that are included with this guide. These settings are described in the "Additional Security Settings" section later in this chapter.

Security Options

The policy settings in the Security Options section of Group Policy are used to enable or disable capabilities and features such as floppy disk drive access, CD-ROM drive access, and logon prompts. These policy settings are also used to configure various other settings, such as those for the digital signing of data, administrator and guest account names, and how driver installation works.

You can configure the security options settings in Windows Server 2003 SP2 at the following location within the Group Policy Object Editor:

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

Not all of the settings that are included in this section exist on all types of computers. Therefore, the settings that comprise the Security Options portion of Group Policy that are defined in this section may need to be manually modified on computers in which these settings are present to make them fully operable.

Potential Issues with SMB Signing Policies

When SMB signing policies are enabled and a Server Message Block (SMB) version 1 client establishes a non-guest session or a non-anonymous session with a server, the client enables security signatures for the server. Later sessions then inherit the security signature sequence that is already established.

To improve security, Windows Server 2008 and Windows Vista SP1 prevent server authenticated connections from being maliciously downgraded to a guest session or to an anonymous session. However, this improved security does not work as intended when the domain controller is running Windows Server 2003 and the client computers are running Windows Vista SP1 or Windows Server 2008. Specifically, this applies if the policies in the following locations are enabled on a domain controller that is running Windows Server 2003 in a domain:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

The following policies are enabled on a member computer that is running Windows Vista SP1 or Windows Server 2008 in the same domain:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (If server agrees)

To download a hotfix to resolve this issue, and learn more about this topic, see "Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled": Microsoft Knowledge Base article 950876.

Event Log

The event log records events on the computer, and the Security log records audit events. The event log container of Group Policy is used to define attributes of 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.

Restricted Groups

The Restricted Groups capability allows you to manage group membership through policy mechanisms and prevent either deliberate or inadvertent exploitation of groups that have powerful user rights. You should first review the needs of your organization to determine the groups that you want to restrict.

The **Backup Operators** and **Power Users** groups are restricted in both of the environments that are defined in this guide. Although members of the **Backup Operators** and **Power Users** groups have less access than members in the **Administrators** group, they still have powerful capabilities.

Note: If your organization uses any of these groups, then carefully control their membership and do not implement the guidance for the Restricted Groups setting. If your organization adds users to the Power Users group, you may want to implement the optional file system permissions that are described in the following "Securing the File System" section.

You can configure the Restricted Groups setting in Windows Server 2003 SP2 at the following location within the Group Policy Object Editor:

> **Computer Configuration\Windows Settings\Security Settings\Restricted Groups**

Administrators may configure restricted groups by adding the desired group directly to the MSBP. When a group is restricted, you can define its members and any other groups to which it belongs. If you do not specify these group members, the group remains totally restricted.

Securing the File System

The NTFS file system has been improved with each new version of Microsoft Windows, and the default permissions for NTFS are adequate for most organizations. The settings that are discussed in this section are provided for optional use by organizations that do not use restricted groups but still wish to have an additional level of hardening on their servers.

You can configure the file system security settings at the following location in the Group Policy Object Editor:

> **Computer Configuration\Windows Settings\Security Settings\File System**

Note: You should thoroughly test any changes to the default file system security settings in a lab environment before you deploy them in a large organization. There have been cases in which file permissions have been altered to a point that required the affected computers to be completely rebuilt.

The default file permissions in Windows Server 2003 SP2 are sufficient for most situations. However, if you do not plan to block membership of the **Power Users** group with the Restricted Groups feature or if you plan to enable the **Network access: Let Everyone permissions apply to anonymous users** setting, you may want to apply the optional permissions that are described in the paragraph that follows. They are very specific, and they apply additional restrictions to certain executable tools that a malicious user with elevated privileges may use to further compromise the computer or network.

Note how these changes do not affect multiple folders or the root of the system volume. It can be very risky to change permissions in that manner, and doing so can often cause computer instability. For computers running 32-bit Windows Server 2003, all of the following files are located in the **%SystemRoot%\System32\** folder, for computers running 64-bit editions, most are located in **%SystemRoot%\SysWow64\**. However, regedit.exe is in **%SystemRoot%**. They are all given the following permissions: **Administrators: Full Control, System: Full Control**.

- regedit.exe
- arp.exe
- at.exe
- attrib.exe
- cacls.exe
- debug.exe
- edlin.exe
- eventcreate.exe
- eventtriggers.exe
- ftp.exe
- nbtstat.exe
- net.exe
- net1.exe
- netsh.exe
- netstat.exe
- nslookup.exe
- ntbackup.exe
- rcp.exe
- reg.exe
- regedt32.exe
- regini.exe
- rexec.exe
- route.exe
- rsh.exe
- sc.exe
- secedit.exe
- subst.exe
- systeminfo.exe
- telnet.exe
- tftp.exe
- tlntsvr.exe

A brief explanation of the purpose and behavior of both **%systemroot%\System32** and **%systemroot%\SysWow64** on the 64-bit editions of Windows is merited. The SysWow64 folder contains 32-bit versions of the system binary files, The System32 folder contains 64-bit versions of these files. When a 64-bit program executes, it normally accesses the 64-bit binaries located in System32. When a 32-bit program executes, the operating system maps System32 to SysWow64 so that the program can seamlessly access the 32-bit binaries. This big of obfuscation helps to resolve compatibility issues, even if the folder names seem confusing.

Additional Security Settings

Although most of the countermeasures that are used to harden the baseline servers 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*.

Manual Hardening Procedures

This section describes how some additional countermeasures (such as securing accounts) were implemented manually for each of the security environments that are defined in this guide.

Manually Adding Unique Security Groups to User Right Assignments

Most of the recommended security groups for user right assignments were 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 specific security groups are unique between different Windows Server 2003 domains. The problem is that the RID (Relative Identifier), which is part of the SID, is unique. These rights are referenced in the following table.

Warning: The following table contains values for Built-in Administrator. The Built-in Administrator is the built-in user account, *not* the security group **Administrators**. If the **Administrators** security group is added to any of the following deny access user rights, you will need to log on locally to correct the mistake. Also, the Built-in Administrator account may have a new name if you followed the recommendation to rename it earlier in this guide. When you add this account to any deny access user rights, make sure that you select the newly renamed administrator account.

Table 3.1 Manually Added User Right Assignments

Setting name in UI	Enterprise Client	Specialized Security – Limited Functionality
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
Deny log on as a batch job	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

Important: All NON-operating system service accounts are service accounts for specific applications in your enterprise. These accounts do not include LOCAL SYSTEM, LOCAL SERVICE, or the NETWORK SERVICE accounts that are built-in accounts for the operating system.

To manually add the listed security groups to the Enterprise Client - Member Server Baseline Policy, complete the following steps.

To add security groups to the User Right 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 previous table for each right.
5. Close the Group Policy that you 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, type **gpupdate /Force** and press ENTER to force the server to refresh the policy.
   b. Reboot the server.
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 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of a remote server by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the SID (security identifier) of the built-in Administrator account to determine its true name and then break in to the server. 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. However, your operations groups can easily monitor attempted attacks against the Administrator account if you rename it with a unique name.

Complete the following steps to secure well-known accounts on domains and servers:

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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.

- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: The built-in Administrator account can be renamed through Group Policy. This setting was not implemented in the baseline policy because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename administrator accounts in both of the environments that are defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

NTFS

NTFS partitions support ACLs at the file and folder levels. This support is not available with the file allocation table (FAT) or FAT32 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 SP3, and Windows Server 2003 SP2.

Format all partitions on every server with NTFS. Use the convert utility to carefully convert FAT partitions to NTFS, but remember that the convert utility will set the ACLs for the converted drive to **Everyone: Full Control**.

For computers that run Windows Server 2003 SP2, apply the following two security templates locally to configure the default file system ACLs for member 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 both of the environments that are defined in this guide are formatted with NTFS partitions to provide the means for file and directory security management through ACLs.

Enable Manual Memory Dumps

Windows Server 2003 SP2 includes a feature that you can use to halt the computer and generate a Memory.dmp file. You must explicitly enable this feature, and it may not be appropriate for all servers in your organization. If you determine that it would be valuable to capture memory dumps on some servers, you can follow the instructions that are provided in "Windows feature lets you generate a memory dump file by using the keyboard": Microsoft Knowledge Base article 244139.

Important: When memory is copied to disk as described in the referenced article, sensitive information may be included in the Memory.dmp file. Ideally, all servers are protected from unauthorized physical access. If you generate a memory dump file on a server that is at risk for physical compromise, be sure to delete the dump file after troubleshooting is concluded.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- Auditing Policy for information about audit policy for Windows Server 2003.
- "Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain": Microsoft Knowledge Base article 305379, for more information about ensuring that more secure LAN Manager authentication level settings work in networks with Windows 2000 and Windows NT 4.0 computers.
- Default settings for services in Windows Server 2003.
- Differences in default security settings for more information about default security settings for Windows Server 2003.
- Get Smart! Boost Your Network's IQ With Smart Cards.
- "How to add custom registry settings to the Security Configuration Editor": Microsoft Knowledge Base article 214752.
- "How to create custom Administrative Templates in Windows 2000": Microsoft Knowledge Base article 323639.
- "How to enable NTLM 2 authentication": Microsoft Knowledge Base article 239869.
- "How to harden the TCP/IP stack against denial of service attacks in Windows Server 2003": Microsoft Knowledge Base article 324270.
- "Internet Server Unavailable Because of Malicious SYN Attacks": Microsoft Knowledge Base article 142641, to harden Windows Socket application settings.
- "Location of ADM (Administrative Template) Files in Windows": Microsoft Knowledge Base article 228460.
- System Center Operations Manager.
- Securing Windows 2000 Terminal Services.
- Security Guidance for Windows Server 2003.
- Security Setting Descriptions for Windows Server 2003.
- "Service overview and network port requirements for the Windows Server system": Microsoft Knowledge Base article 832017.
- "The "RestrictAnonymous" Registry Value May Break the Trust to a Windows 2000 Domain": Microsoft Knowledge Base article 296405.
- User rights for information about user rights in Windows Server 2003.
- "Using Administrative Template Files with Registry-Based Group Policy" white paper.

Chapter 4: Hardening Domain Controllers

Addressing security in the Domain Controller server role is one of the most important aspects of any environment with computers that run Windows Server® 2003 Service Pack 2 (SP2) or later and the Active Directory® directory service. Any loss or compromise of a domain controller in such an environment could seriously affect client computers, servers, and applications that rely on domain controllers for authentication, Group Policy, and a centralized lightweight directory access protocol (LDAP) directory.

Because of 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, such as branch offices, several security settings can be adjusted to limit the potential damage from physical threats.

Restricted Groups

As described in the previous chapter, the **Restricted Groups** setting allows you to manage the membership of groups in Windows Server 2003 SP2 or later through Active Directory Group Policy. First, review the needs of your organization to determine the groups you want to restrict. For domain controllers, the **Server Operators** and **Backup Operators** groups are restricted in both of the environments defined in this guide. Although members of the **Server Operators** and **Backup Operator** groups have less access than members in the **Administrators** group, they still have powerful capabilities.

Note: If your organization uses any of these groups, then carefully control their membership and do not implement the guidance for the **Restricted Groups** setting. If your organization adds users to the Server Users group, you may want to implement the optional file system permissions that are described in the "Securing the File System" section in the previous chapter.

Table 4.1 Restricted Groups Recommendations

Local group	Enterprise Client	Specialized Security – Limited Functionality
Backup Operators	No members	No members
Server Operators	No members	No members

The **Restricted Groups** setting can be configured in Windows Server 2003 SP2 at the following location in the Group Policy Object Editor:

> **Computer Configuration\Windows Settings\Security Settings\Restricted Groups**

To configure restricted groups for a GPO, administrators can add the desired group directly to the **Restricted Groups** node of the GPO namespace.

When a group is restricted, you can define its members and any other groups to which it belongs. If you do not specify these group members, the group is left totally restricted. Groups can only be restricted with Security Templates.

To view or modify the Restricted Groups setting

1. Open the Security Templates Management Console.

   Note: The Security Templates Management Console is not added to the Administrative Tools menu by default. To add it, start the Microsoft Management Console (mmc.exe) and add the Security Templates Add-in.

2. Double-click the configuration file directory, and then the configuration file.
3. Double-click the **Restricted Groups** item.
4. Right-click **Restricted Groups**.
5. Select **Add Group**.
6. Click the **Browse** button, then **Locations**, select the locations you want to browse, and then click **OK**.

   Note: Typically, this action will cause a local computer to display at the top of the list.

7. Type the group name in the **Enter the object names to select** text box, and then click the **Check Names** button.

   – or –

   Click the **Advanced** button, and then the **Find Now** button to list all available groups.

8. Select the groups you want to restrict, and then click **OK**.
9. Click **OK** on the **Add Groups** dialog box to close it.

In this guidance, all members—users and groups—of the **Server Operators** and **Backup Operators** groups were removed to totally restrict them in both environments. Also, for the SSLF environment, all members were removed for the **Remote Desktop Users** group. Microsoft recommends to restrict any built-in group that you do not plan to use in your organization.

Note: The configuration of Restricted Groups that is described in this section is very simple. Current versions of Windows XP and Windows Server 2003 support more complex designs. For more information, see "Updates to Restricted Groups ("Member of") Behavior of User-Defined Local Groups": Microsoft Knowledge Base article 810076.

Additional Security Settings

This section describes modifications that must be made to the DCBP manually, and other settings and countermeasures that cannot be implemented through Group Policy.

Manually Adding Unique Security Groups to User Right Assignments

Most user right assignments that are applied through the DCBP are 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 Server 2003 domains. User right assignments that must be configured manually are specified in the following table.

Warning: The following table contains values for the built-in Administrator account. Do not confuse this account with the built-in **Administrators** security group. If you add the **Administrators** security group to any of the deny access user rights in the following table, you will need to log on locally to correct the mistake. Also, if you renamed the built-in Administrator account in accordance with the recommendations in Chapter 3, "Implementing the Security

Baseline," ensure to select the newly renamed administrator account when you add the account to any deny access user right.

Table 4.2 Manually Added User Right Assignments

Setting	Enterprise Client	Specialized Security – Limited Functionality
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
Deny log on as a batch job	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

Important: "All non-operating system service accounts" include service accounts used for specific applications across an enterprise, but does *not* include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts (the built-in accounts that the operating system uses).

Directory Services

Domain controllers that run Windows Server 2003 SP2 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

To maintain directory integrity and reliability, it is essential to safeguard the Active Directory database and its log files. You can move the Ntds.dit, Edb.log, and Temp.edb files from their default location, which will help to conceal them from an attacker if a domain controller is compromised. If you move the files off the system volume to a separate physical disk, you will gain the added benefit of improved domain controller performance.

For these reasons, this guide recommends to move the Active Directory database and log files for the domain controllers to a striped or striped/mirrored disk volume that does not contain the operating system. These files should be moved for both of the environments defined in this guide.

Resizing Active Directory Log Files

An adequate amount of information must be logged to effectively monitor and maintain the integrity, reliability, and availability of Active Directory. Information is needed from all domain controllers in the environment.

You can increase the maximum size of the log files to support this effort. More log information will allow administrators to perform meaningful audits if hacker attacks occur.

This guide recommends to increase 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 two environments defined in this guide.

Using Syskey

On domain controllers, password information is stored in Active Directory. 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 the SAM on the domain controller.

Table 4.3 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 computer 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 SP2 servers in Mode 1 (obfuscated key). From a security standpoint, this configuration appears sensible at first. However, Syskey in Mode 1 allows an attacker to read and alter the contents of the directory, which would render the domain controller easily vulnerable to an attacker with physical access.

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. However, the operational need to restart domain controllers tends 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, it can be very expensive to require one of your branch managers or local administrative staff to come to the office at 3 A.M. to enter passwords or insert a floppy to enable user access. Such expensive requirements can make the achievement of high availability service level agreements (SLAs) a significant challenge.

Alternatively, if you decide to allow your centralized IT operations personnel to provide the Syskey password remotely, additional hardware is required. Some hardware vendors have add-on solutions that allow you to remotely access server consoles.

Finally, the loss of the Syskey password or floppy disk would leave 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.

With the proper operational procedures in place, Syskey can provide an increased level of security to protect sensitive directory information 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 configuration applies to domain controllers in both of the environments that are 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 to use Active Directory-integrated DNS in the two environments defined in this guide. Part of the reason for this recommendation is because Active Directory zone integration makes it simpler to secure the DNS infrastructure in an environment that uses Active Directory-integrated DNS than in an environment that does not use Active Directory-integrated DNS.

Protecting DNS Servers

It is essential to safeguard DNS servers in any Active Directory environment. The following sections provide several recommendations and explanations about how to safeguard DNS servers.

When a DNS server is attacked, one possible goal of the attacker is to control the DNS information that is returned in response to DNS client queries. If an attacker controls this information, clients may be unknowingly redirected 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 about another host into the cache of a DNS server. The attack causes clients to be redirected to unauthorized computers. If client computers are allowed to communicate with unauthorized computers, the unauthorized computers may attempt to gain access to information 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. If a DNS server responds 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, the routers used in the environments that are defined in this guide are configured to drop spoofed IP packets, which helps ensure that the IP addresses of the DNS servers are not spoofed by other computers.

Configuring Secure Dynamic Updates

The **DNS client** service in Windows Server 2003 SP2 supports dynamic DNS updates, which allow client computers to add DNS records directly into the database. If a dynamic DNS server is configured to accept unsecured updates, an attacker could transmit malicious or unauthorized updates from a client computer that supports the DNS dynamic update protocol.

At a minimum, an attacker can add false entries to the DNS database. At worst, an attacker can overwrite or delete legitimate entries in the DNS database. Such an attacker could accomplish any of the following:

- **Direct clients to unauthorized domain controllers**. When a client submits a DNS query to find 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 and convinced to transmit secure information to the unauthorized server.
- **Respond to DNS queries with invalid addresses**. Clients and servers would be 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, which creates a DoS condition that could affect users throughout a forest.
- **Create a DoS condition**. A server’s disk space could be exhausted by a huge zone file that is filled with dummy records or large numbers of entries that slow down replication.

Use of secure dynamic DNS updates guarantees that registration requests are only processed if they are sent from valid clients in an Active Directory forest. This method severely limits the ability of an attacker to compromise the integrity of a DNS server. For these reasons, the Active Directory DNS servers in the environments defined in this guide are configured to accept only secure dynamic updates.

Limiting Zone Transfers to Authorized Systems

Because of the importance of zones in DNS, they should be available from more than one DNS server on the network to provide adequate availability and fault tolerance for name resolution queries. When additional servers host a zone, zone transfers are required to replicate and synchronize all copies of the zone for each server that is configured to host the zone.

Also, a DNS server that does not limit who can request zone transfers is vulnerable to transfer of the entire DNS zone to anyone who requests it. This transfer can be easily accomplished with tools such as Nslookup.exe. Such tools can expose the entire domain's DNS dataset, including such things as which hosts serve as domain controllers, directory-integrated Web servers, or Microsoft SQL Server® databases.

For these reasons, Active Directory-integrated DNS servers in the environments that are defined in this guide are configured to allow zone transfers, but to limit which computers can make transfer requests.

Resizing the Event Log and DNS Service Log

An adequate amount of information must be logged to effectively monitor and maintain the DNS service. Information is needed from all domain controllers in the environment.

You can increase the maximum size of the DNS service log file, which will allow administrators to perform meaningful audits in the event of an attack.

This guide recommends to increase the maximum size of the DNS service log file to at least 16 MB on the domain controllers in the environments defined in this guide. Also, 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 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in administrator account to determine its true name and then break in to the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

Complete the following steps to secure well-known accounts on domains and servers:

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: The built-in administrator account can be renamed through Group Policy. This policy setting was not implemented in any of the Security Templates provided with this guide because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename administrator accounts in both of the environments defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

Avoid Combining the Domain Controller Role with Server Roles

Although it is possible to install other role services on computers with the domain controller role, Microsoft recommends to avoid doing this whenever possible. There are several ways in which undesirable situations may arise if you combine these roles. For example, users with accounts in Active Directory Directory Services (AD DS) may have too much access to data associated with another role or conversely, users accessing network services provided by another role may have inappropriate access to information stored in Active Directory. Installing certain roles with the domain controller role can be particularly risky, such as the Routing and Remote Access Services or Certificate Services.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- Changes to DNS in Windows Server 2003 in Microsoft PowerPoint®.
- "Description of Dcpromo Permissions Choices": Microsoft Knowledge Base article 257988 for information about how to enable anonymous access to Active Directory.
- "How to restrict FRS replication traffic to a specific static port": Microsoft Knowledge Base article 319553.
- Introduction to IP Spoofing in PDF from GIAC Certified Professionals.
- "Restricting Active Directory replication traffic to a specific port": Microsoft Knowledge Base article 224196.
- *Windows 2000 Server Resource Kit: Supplement 1* for information about Windows 2000 DNS in the "TCP/IP Core Networking Guide" section of the kit.
- Windows Time Service Technical Reference.

Chapter 5: Hardening Infrastructure Servers

This chapter explains the policy settings you can use to harden infrastructure servers that run Windows Server® 2003 Service Pack 2 (SP2) or later in the environments that are defined in this guide. For the purposes of this guide, an infrastructure server is one that provides DHCP services or Microsoft WINS functionality.

Most of the settings in this chapter are configured and applied through Group Policy. A Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) that contain the infrastructure servers to provide additional security for the servers. This chapter only discusses those policy settings that vary from the MSBP.

Where possible, these policy settings are gathered in an incremental Group Policy object that will be applied to the Infrastructure Servers OU. Some of the settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these settings manually is provided.

Additional Security Settings

The security settings that the MSBP applies significantly enhance the security of infrastructure servers. This section discusses some additional settings for consideration. You cannot configure the settings in this section through Group Policy; you need to configure them manually on all infrastructure servers.

Configure DHCP Logging

By default, the DHCP service only logs startup and shutdown events in the event log. Complete the following steps to enable a more detailed log on the DHCP server:

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**.

When you complete these steps, the DHCP server creates a log file in the following location:

%systemroot%\system32\dhcp\

DHCP client information is often difficult to locate in log files because the only information that is stored in most logs are computer names, not IP addresses. The DHCP audit logs provide an additional tool to help locate the sources of internal attacks or inadvertent activities.

However, the information in these logs is not foolproof, because both host names and media access control (MAC) addresses can be forged or spoofed. (*Spoofing* makes a transmission appear to come from a user other than the user who performed the action.)

However, the benefits that this information provides outweigh any costs that are incurred when logging is enabled on a DHCP server. It can be very helpful to have more than just an IP address and a computer name when you need to determine how a particular IP address was used on a network.

By default, the **Server Operators** and **Authenticated Users** groups have read permissions to the DHCP log files. To best preserve the integrity of the information logged by a DHCP server, Microsoft recommends to limit access to these logs 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.

In theory, the DHCP audit logs could fill the disk on which they are stored. However, the default configuration for the **DHCP Audit Logging** setting ensures that logging will stop if there is less than 20 MB of free disk space available on the server. This default configuration is adequate for servers in most environments, but you can modify it to ensure sufficient free disk space is available for other applications on a server. For information about how to modify this configuration, refer to the DhcpLogMinSpaceOnDisk page in the Windows Client Tech Center.

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 unable to service DHCP requests, DHCP clients will eventually be unable to acquire leases. Those clients will then lose their existing IP leases and the ability to access network resources.

It would not be very difficult to write an attack tool script that requests all available addresses on a DHCP server. Such a script 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, which would cause the DHCP server to detect IP address conflicts for all addresses in its scope and to refuse to allocate DHCP leases.

Also, 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 request leases and renewals. This type of problem can be avoided by proper design of DHCP services.

You can configure DHCP servers in pairs and follow the best practice 80/20 rule—split DHCP server scopes between servers so that 80 percent of the addresses are distributed by one DHCP server and 20 percent by another—to help mitigate the impact of these types of attacks. These configuration suggestions help ensure that clients can continue to receive IP address configuration despite server failure. For more information about the 80/20 rule and the DHCP protocol, see the topic "Dynamic Host Configuration Protocol" in the *Windows 2000 Server Resource Kit: Supplement 1*.

Note: The 80/20 Rule described in the *Windows 2000 Server Resource Kit* also applies to DHCP services in Windows Server 2003 SP2.

Securing Well-Known Accounts

Windows Server 2003 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well-known accounts on infrastructure servers

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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 other servers with the same account name and password.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: The built-in Administrator account can be renamed through Group Policy. This policy setting was not implemented in any of the security templates that are provided with this guide because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename administrator accounts in both of the environments that are defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- DhcpLogMinSpaceOnDisk page in the Windows Client Tech Center.
- "Dynamic Host Configuration Protocol" topic in the *Windows 2000 Server Resource Kit: Supplement 1*.
- *Services and Service Accounts Security Planning Guide*.

Chapter 6: Hardening File Services

It can be a challenge to harden file server computers that run Windows Server® 2003 Service Pack 2 (SP2), because the most essential services that these servers provide are the ones that require the Server Message Block (SMB) and Common Internet File System (CIFS) protocols. These protocols can provide rich information to unauthenticated users, and they are often disabled in high security Windows environments. However, it will be difficult for both users and administrators to access file servers if these protocols are disabled.

Most of the policy settings in this chapter are configured and applied through Group Policy. A Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) that contain the file servers to provide the required security settings for this server role. This chapter only discusses those policy settings that vary from the MSBP.

Where possible, these policy settings are gathered in an incremental Group Policy object that will be applied to the File Servers OU. Some of the policy settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these policy settings manually is provided.

Additional Security Settings

Although the security settings that the MSBP applies significantly enhance the security of file servers, this section discusses some additional considerations. However, the settings in this section cannot be implemented through Group Policy and must therefore be performed manually on all file servers.

Securing Well-Known Accounts

Windows Server 2003 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well-known accounts on file servers

- Rename the Administrator and Guest accounts, and then change their passwords to long and complex values on every domain and server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: You can rename the built-in Administrator account through Group Policy. This setting was not implemented in any of the Security Templates that are provided with this guide because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename administrator accounts in both of the environments that are defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- Distributed File System Technology Center.
- Technical Overview of Windows Server 2003 File Services.
- *Services and Service Accounts Security Planning Guide*.

Chapter 7: Hardening Print Services

This chapter focuses on how to harden print servers that run Windows Server® 2003 Service Pack 2 (SP2) or later, which can be a challenge. The essential services that these servers provide are ones that require the Server Message Block (SMB) and Common Internet File System (CIFS) protocols, both of which can provide rich information to unauthenticated users. These protocols are often disabled on print servers in high-security Windows environments. However, it will be difficult for both administrators and users to access print servers if these protocols are disabled in your environment.

Most of the settings in this chapter are configured and applied through Group Policy. A Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) that contain the print servers to provide the required security settings for this server role. This chapter only discusses those policy settings that vary from the MSBP.

Where possible, these settings are gathered in an incremental Group Policy template that will be applied to the Print Servers OU. Some of the settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these settings manually is provided.

Additional Security Settings

Although the security settings applied through the MSBP significantly enhance the security of print servers, there are a few additional settings that you should consider. The settings in this section cannot be applied through Group Policy and must therefore be performed manually on all print servers.

Securing Well-Known Accounts

Windows Server 2003 SP2 or later 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well known accounts on print servers

- Rename the Administrator and Guest accounts, and then change their passwords to long and complex values on every domain and server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: You can rename the built-in Administrator account through Group Policy. This setting was not implemented in any of the security templates that are provided with this guide because every organization should choose a unique name for this account. However, the **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in both of the environments that are defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- *Services and Service Accounts Security Planning Guide*.
- Technical Overview of Windows Server 2003 Print Services.
- What's New in File and Print Services.

Chapter 8: Hardening Web Services

This chapter provides guidance that will help you harden the Web servers in your environment that run Windows Server® 2003 Service Pack 2 (SP2) or later. To provide comprehensive security for Web servers and applications within your organization's intranet, Microsoft recommends that you protect each Microsoft Internet Information Services (IIS) server as well as each Web site and application that run on these servers from client computers that can connect to them. You should also protect these Web sites and applications from the Web sites and applications that run on the other IIS servers within your organization’s intranet.

To help protect against malicious users and attackers, the default configuration for members of the Windows Server 2003 family does not install IIS. When it is installed, IIS is configured in a highly secure, "locked" mode. For example, in its default state IIS will only serve static content. Because they could be exploited by potential intruders, 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 Manager (IIS Manager). IIS Manager has a graphical user interface (GUI) that is designed to facilitate administration of IIS. It includes resources for file management, directory management, and configuration of application pools, as well as security, performance, and reliability features.

Microsoft recommends to consider implementing the settings described in the following sections of this chapter to enhance the security of IIS Web servers that host HTML content within your organization’s intranet. To help secure your servers, you should also implement security monitoring, detection, and response procedures to watch for new threats.

Most of the settings in this chapter are configured and applied through Group Policy. An incremental GPO that complements the MSBP is linked to the appropriate OUs and provides additional security for the Web servers. To improve the usability of this chapter, only those policy settings that vary from the MSBP are discussed.

Where possible, these settings are gathered in an incremental Group Policy template that will be applied to the Web Servers OU. Some of the settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these settings manually is provided.

Anonymous Access and the SSLF Settings

Four of the user rights that are explicitly defined in the SSLF scenario in the MSBP are designed to break anonymous access to IIS Web sites. However, if you need to allow anonymous access in an SSLF environment you will need to make some important changes to the OU structure and GPOs that are described in Chapters 1, 2, and 3 of this guide. You will need to create a new OU that is not part of the hierarchy below the Member Servers OU. This OU could be linked directly to the domain root, or it could be a child OU of some other OU hierarchy. However, you should not assign user rights in a GPO that will affect the IIS servers that will be placed in this new OU. You can move the IIS servers to the new OU, create a new GPO, apply the MSBP settings to it, and then reconfigure user right assignments so that they can be controlled by local policy rather than the domain–based GPO. In other words, Microsoft recommends to configure the following user right settings to **Not defined** in this new GPO:

- Access this computer from the network
- Allow log on locally
- Bypass traverse checking
- Log on as a batch job

The IIS features that you enable determine whether you need to also reconfigure other user right assignment settings to **Not defined**.

Additional Security Settings

When IIS is installed on a computer that runs Windows Server 2003 SP2 or later, its default setting only allows transmission of 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, you should be careful to minimize the attack surface of each IIS server in your environment. 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.

The security settings that are applied through the MSBP provide a great deal of enhanced security for IIS servers. However, there are a few additional settings that you should consider. The settings in the following sections cannot be implemented through Group Policy and must therefore 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 that are required to provide FTP, NNTP, and SMTP support. IIS components and services are installed and enabled with the Windows Components Wizard Application Server that can be launched through Add or Remove Programs in Control Panel. After you install IIS, you will need to enable all IIS components and services that are required by your Web sites and applications.

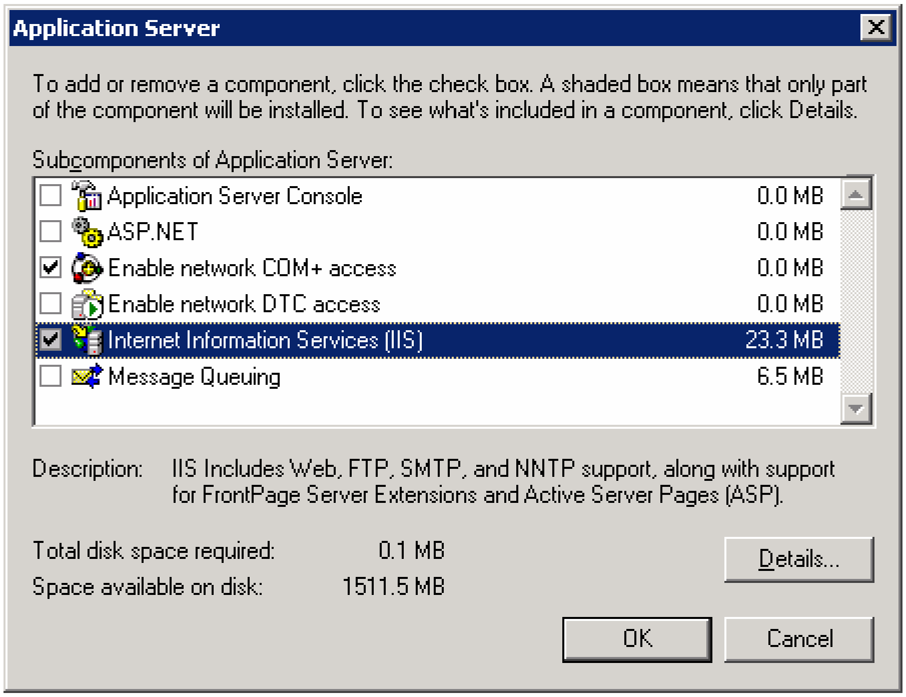
To install Internet Information Services (IIS) 6.0

1. In 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**.

You should only enable essential IIS components and services that are required by Web sites and applications. If you enable unnecessary components and services, the attack surface of an IIS server increases. The following illustrations and tables show the location and suggested settings for IIS components.

The subcomponents in the **Application Server** dialog box are shown in the following figure.



Application Server

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☐	Application Server Console	0.0 MB
☐	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
☐	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	23.3 MB
☐	Message Queuing	6.5 MB

Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 0.1 MB

Space available on disk: 1511.5 MB

Figure 8.1 Application Server dialog box with list of subcomponents

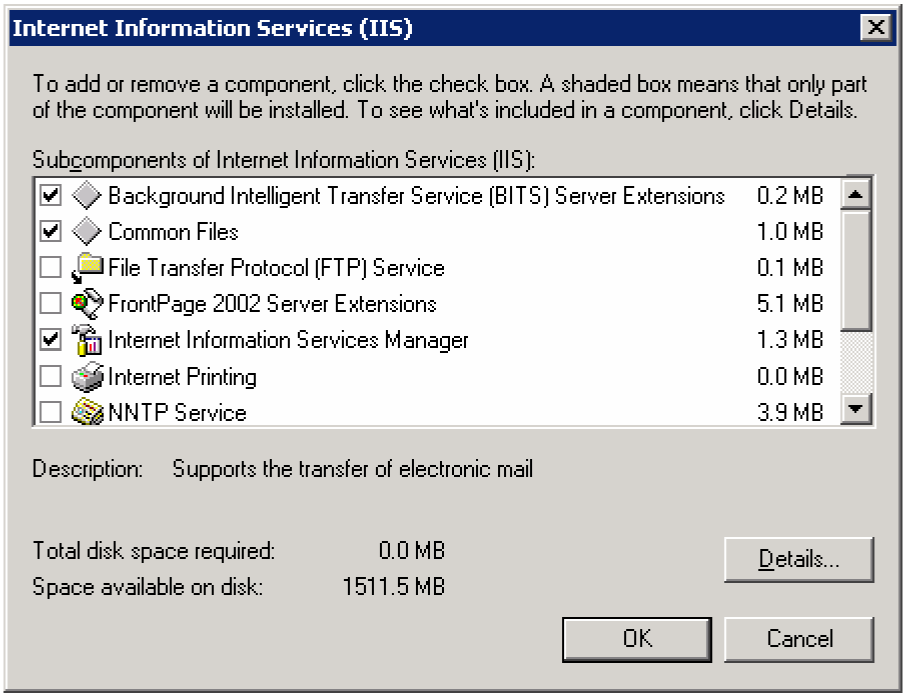
The following table briefly describes the Application Server subcomponents and provides recommendations for when to enable them.

Table 8.1 Recommended Application Server Subcomponents Settings

Component name in UI	Setting	Setting logic
Application Server Console	Disabled	Provides a Microsoft Management Console (MMC) snap-in that you can use to administer all the Web Application Server components. This component is not required on a dedicated IIS server because IIS Server Manager can be used.

Component name in UI	Setting	Setting logic
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 that run 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. **Note**: If this component is not enabled, then all subcomponents are disabled.
Message Queuing	Disabled	Microsoft Message Queuing (MSMQ) Provides a message routing, storage, and forwarding middleware layer for enterprise Web applications.

The subcomponents in the **Internet Information Services (IIS)** dialog box are shown in the following figure.



Internet Information Services (IIS)

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Internet Information Services (IIS):

☑	Background Intelligent Transfer Service (BITS) Server Extensions	0.2 MB
☑	Common Files	1.0 MB
□	File Transfer Protocol (FTP) Service	0.1 MB
□	FrontPage 2002 Server Extensions	5.1 MB
☑	Internet Information Services Manager	1.3 MB
□	Internet Printing	0.0 MB
□	NNTP Service	3.9 MB

Description: Supports the transfer of electronic mail

Total disk space required: 0.0 MB

Space available on disk: 1511.5 MB

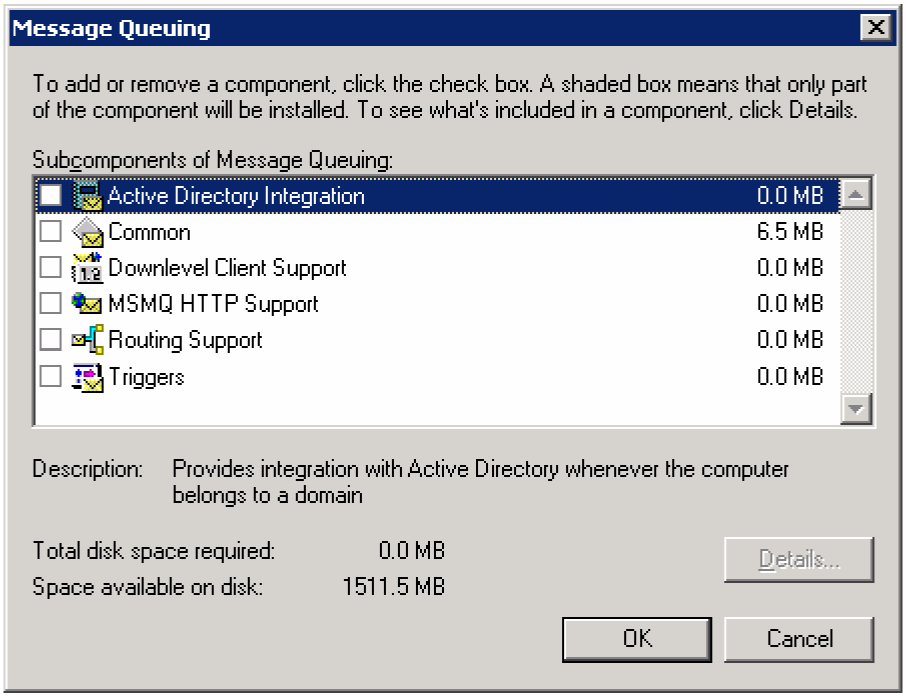
Figure 8.2 IIS dialog box with list of subcomponents

The following table briefly describes the IIS subcomponents and provides recommendations for when to enable them.

Table 8.2 Recommended IIS Subcomponents Settings

Component name in UI	Setting	Setting logic
Background Intelligent Transfer Service (BITS) server extension	Disabled	The BITS server extension allows BITS on the clients to upload files to this server in the background. If you have an application on the clients that uses BITS to upload files to this server, then enable and configure the BITS server extension; otherwise, leave it disabled. Note that Windows Update, Microsoft Update, SUS, WSUS, and Automatic Updates do not require this component to run. They require the BITS client component, which is not part of IIS.
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 to administer and publish 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 component is 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 are shown in the following figure.



Message Queuing

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Message Queuing:

□	Active Directory Integration	0.0 MB
□	Common	6.5 MB
□	Downlevel Client Support	0.0 MB
□	MSMQ HTTP Support	0.0 MB
□	Routing Support	0.0 MB
□	Triggers	0.0 MB

Description: Provides integration with Active Directory whenever the computer belongs to a domain

Total disk space required: 0.0 MB

Space available on disk: 1511.5 MB

Figure 8.3 Message Queuing dialog box with list of subcomponents

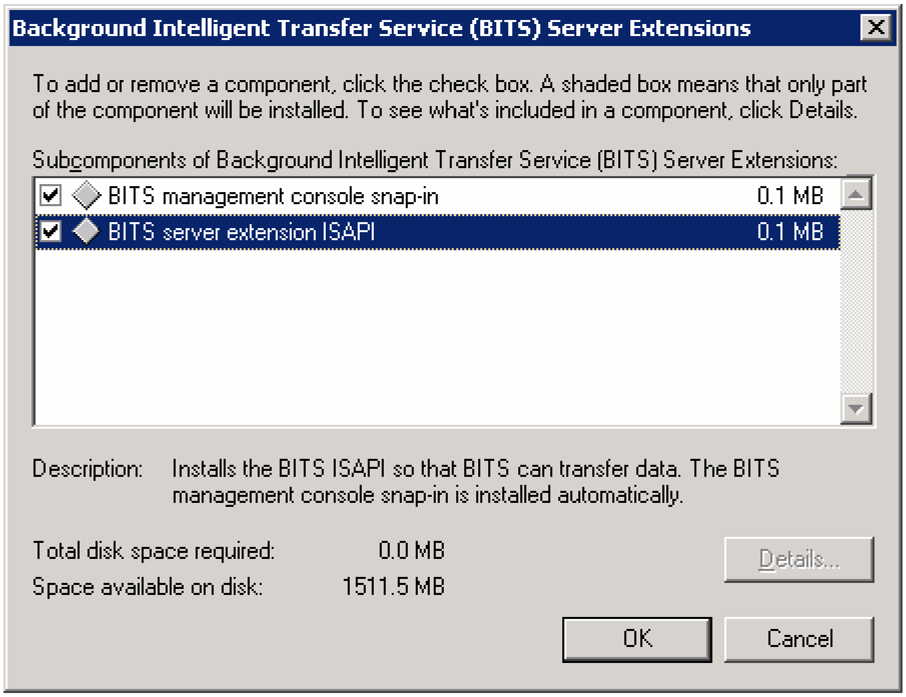
The following table briefly describes the Message Queuing subcomponents and provides recommendations for when to enable them.

Table 8.3 Recommended Message Queuing Subcomponents Settings

Component name in UI	Setting	Setting logic
Active Directory Integration	Disabled	Provides integration with the Active Directory® directory service whenever an IIS server belongs to a domain. This component is required when Web sites and applications that run on IIS servers use Microsoft Message Queuing (MSMQ).
Common	Disabled	This component is required when Web sites and applications that run 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 ability to send and receive messages over the HTTP transport. This component is required when an IIS server's Web sites and applications use MSMQ.

Component name in UI	Setting	Setting logic
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 that run on IIS servers use MSMQ.
Triggers	Disabled	Associates the arrival of incoming messages at a queue with functionality in a COM component or a stand-alone executable program.

The subcomponents in the **Background Intelligent Transfer Service (BITS) Server Extensions** dialog box are shown in the following figure.



Background Intelligent Transfer Service (BITS) Server Extensions

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Background Intelligent Transfer Service (BITS) Server Extensions:

☑	BITS management console snap-in	0.1 MB
☑	BITS server extension ISAPI	0.1 MB

Description: Installs the BITS ISAPI so that BITS can transfer data. The BITS management console snap-in is installed automatically.

Total disk space required: 0.0 MB

Space available on disk: 1511.5 MB

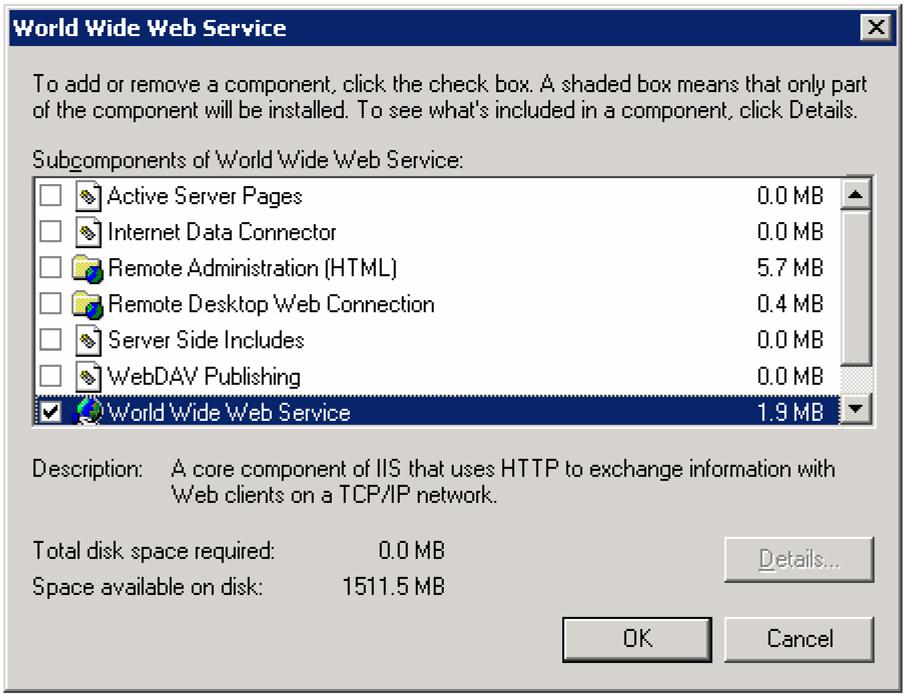
Figure 8.4 BITS Server Extensions with list of subcomponents

The following table briefly describes the BITS Server Extensions subcomponents and provides recommendations for when to enable them.

Table 8.4 Recommended BITS Server Extensions Subcomponents Settings

Component name in UI	Setting	Setting logic
BITS management console snap-in	Disabled	Installs an MMC snap-in to administer BITS. Enable this component when the BITS server extension for Internet Server Application Programming Interface (ISAPI) is enabled.
BITS server extension ISAPI	Disabled	Installs the BITS ISAPI so that an IIS server can transfer data using BITS. BITS Server Extensions allow BITS on the clients to upload files to this server in the background. If you have an application on the clients that uses BITS to upload files to this server, then enable and configure the BITS server extension; otherwise leave it disabled. Note that Windows Update, Microsoft Update, SUS, WSUS, and Automatic Updates do not require this component to run. They require the BITS client component, which is not part of IIS.

The subcomponents in the **World Wide Web Service** dialog box are shown in the following figure.



World Wide Web Service

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of World Wide Web Service:

☐	Active Server Pages	0.0 MB
☐	Internet Data Connector	0.0 MB
☐	Remote Administration (HTML)	5.7 MB
☐	Remote Desktop Web Connection	0.4 MB
☐	Server Side Includes	0.0 MB
☐	WebDAV Publishing	0.0 MB
☑	World Wide Web Service	1.9 MB

Description: A core component of IIS that uses HTTP to exchange information with Web clients on a TCP/IP network.

Total disk space required: 0.0 MB

Space available on disk: 1511.5 MB

Figure 8.5 World Wide Web Service dialog box with list of subcomponents

The following table briefly describes the World Wide Web Service subcomponents and provides recommendations for when to enable them.

Table 8.5 Recommended World Wide Web Service Subcomponent Settings

Component name in UI	Setting	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 by using the Web service extensions. For more information, see the following “Enabling Only Essential Web Service Extensions” section in this chapter.
Internet Data Connector	Disabled	Provides support for dynamic content that is provided through files with .idc extensions. Disable this component when no Web sites or applications that run on IIS servers include files with .idc extensions, or disable it by using the Web service extensions. For more information, see the following “Enabling Only Essential Web Service Extensions” section in this chapter.
Remote Administration (HTML)	Disabled	Provides an HTML interface to administer 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 to host 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 that run 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 by using the Web service extensions. For more information, see the following “Enabling Only Essential Web Service Extensions” section 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 that run on IIS servers have extended functionality that goes beyond static pages, including the ability to generate dynamic content. Any dynamic content that is served or extended through features that are provided by an IIS server is accomplished through Web service extensions.

Enhanced security features in IIS 6.0 allow individual Web service extensions to be enabled or disabled. As stated earlier, IIS servers will transmit only static content after a new installation. 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.

One way to ensure the highest possible compatibility with existing applications is to enable all Web service extensions, but this method also creates a security risk because it increases the attack surface of IIS. Microsoft recommends to only enable those Web service extensions that are required by the Web sites and applications that run on IIS servers in your environment. This approach will minimize server functionality and reduce the attack surface of each IIS server.

To reduce the attack surface of IIS servers as much as possible, only necessary Web service extensions are enabled on IIS servers in the environments that are defined in this guide.

The following table lists predefined Web service extensions, and provides details on when to enable each extension.

Table 8.6 Enabling Web Service Extensions

Web service extension	Enable extension when
Active Server Pages	One or more Web sites and applications that run on IIS servers contain ASP content.
ASP.NET v1.1.4322	One or more Web sites and applications that run on IIS servers contain ASP.NET content.
All Unknown CGI Extensions	One or more Web sites and applications that run on IIS servers contain unknown CGI extension content.
All Unknown ISAPI Extensions	One or more Web sites and applications that run on IIS servers contain unknown ISAPI extension content.
FrontPage Server Extensions 2002	One or more Web sites that run on IIS servers use FrontPage Extensions.
Internet Data Connector (IDC)	One or more Web sites and applications that run 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 that run 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** folder (where <*systemroot*> is the drive on which the Windows Server 2003 SP2 operating system is installed).

In the environments that are defined in this guide, all files and folders that make up Web sites and applications are placed on dedicated disk volumes that are separate from the operating system. This approach helps prevent directory traversal attacks in which an attacker sends requests for a file that is located outside the directory structure of an IIS server.

For example, the Cmd.exe file 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 the Cmd.exe file have been reset as part of the base build of Windows Server 2003 SP2 that restricts access to a much more limited group of users. Second, the Cmd.exe file would 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 with this type of attack.

In addition to the security-related benefits, administration tasks such as backup and restore are easier when Web site and application files and folders are placed on a dedicated disk volume. Also, use of a separate, dedicated physical drive can help reduce disk contention on the system volume and improve overall disk access performance.

Setting NTFS Permissions

Computers that run Windows Server 2003 SP2 examine NTFS file system permissions to determine the types of access a user or a process has on a specific file or folder. You should assign NTFS permissions to allow or deny access to specific users for Web sites on IIS servers in the environments that are defined in this guide.

NTFS permissions affect only the accounts that have been allowed or denied access to the Web site and application content. You should use NTFS permissions in conjunction with Web permissions, not instead of Web permissions. 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, the more restrictive settings are applied.

You should explicitly deny access to anonymous accounts on Web sites and applications for which anonymous access is not desired. Anonymous access occurs when a user who has no authenticated credentials accesses network resources. Anonymous accounts include the built-in Guest account, the **Guests** group, and IIS Anonymous accounts. Also, eliminate any write-access permissions to all users except those who are IIS administrators.

The following table provides some recommendations about the NTFS permissions that Microsoft recommends to apply to different file types on an IIS server. The different file types can be grouped in separate folders to simplify the application of NTFS permissions.

Table 8.7 Recommended NTFS Permission Settings

File type	Recommended NTFS permission
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 script source access or directory browsing. You should assign Web site permissions to provide additional security for Web sites on IIS servers in the environments that are defined in this guide.

You can use Web site permissions in conjunction with NTFS permissions, and configure them 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 with the MMC IIS Manager snap-in.

The following table lists the Web site permissions that are supported by IIS 6.0, and provides brief explanations of when to assign any given permission to a Web site.

Table 8.8 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 the 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.

Web site permission	Permission granted
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 the **Indexing Service** to index resources, which 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

Microsoft recommends to enable IIS logging on IIS servers in the environments that are defined in this guide. You can create separate logs for each Web site or application. IIS logs more information than the event logs and performance monitoring features that are provided by the Windows operating system. 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 help investigate attacks.

You can use the MMC IIS Manager snap-in to configure the log file format, the log schedule, and the exact information to be logged. To limit the size of the logs, Microsoft recommends to use a careful planning process to determine which fields to log.

When IIS logging is enabled, IIS uses the W3C Extended Log File Format to create daily activity logs in the directory that is specified for the Web site in IIS Manager. To improve server performance, you should store logs on a nonsystem striped or striped/mirrored disk volume.

Logs can also be written to a remote share over a network by using a full, Universal Naming Convention (UNC) path. Remote logging allows administrators to set up centralized log file storage and backup. However, server performance could be negatively affected when log files are written over the network.

IIS logging can be configured to use several other ASCII or Open Database Connectivity (ODBC) log file formats. ODBC logs can store activity information in a SQL database. However, note that when ODBC logging is enabled, IIS disables the kernel-mode cache, which can degrade overall server performance.

IIS servers that host hundreds of sites can enable centralized binary logging to improve logging performance. Centralized binary logging enables all Web sites on an IIS server to write activity information to a single log file. This method can greatly increase the manageability and scalability of the IIS logging process because it reduces the number of logs that need to be individually stored and analyzed. For more information about centralized binary logging, see IIS Centralized Binary Logging (IIS6.0).

When IIS logs are stored on IIS servers, only server administrators have permission to access them by default. If a log file directory or file owner is not in the **Local Administrators** group, the HTTP.sys file (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 Right Assignments

Most user right assignments that are applied through 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 right assignments that must be configured manually are specified in the following table.

Warning: The following table contains values for the built-in Administrator account. Do not confuse the Administrator account with the built-in **Administrators** security group. If you add the **Administrators** security group to the deny access user right in the following table, you will need to log on locally to correct the mistake. Also, you may have renamed the built-in Administrator account in accordance with the recommendation in Chapter 3, "Implementing the Security Baseline." When you add the Administrator account to any user right, ensure that the renamed account is specified.

Table 8.9 Manually Added User Right Assignments

Member server default	Enterprise Client	Specialized Security – Limited Functionality
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

Important: "All non-operating system service accounts" include service accounts used for specific applications across an enterprise, but does *not* include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts (the built-in accounts that the operating system uses).

Securing Well-Known Accounts

Windows Server 2003 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well known accounts on IIS servers

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes you make in a secure location.

Note: You can rename the built-in administrator account through Group Policy. This setting was not implemented in any of the Security Templates that are provided with this guide because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename administrator accounts in the environments that are defined in this guide. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see the *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- Centralized Binary Logging in IIS 6.0 (IIS 6.0).
- Customizing W3C Extended Logging (IIS 6.0).
- Enable Logging (IIS 6.0).
- "How to enable logging in Internet Information Services (IIS)": Microsoft Knowledge Base article 313437.
- Internet Information Services for information about IIS 6.0.
- Logging Site Activity (IIS 6.0).
- Remote Logging (IIS 6.0).

Chapter 9: Hardening Internet Authentication Services

This chapter provides recommendations and resources to help you harden Internet Authentication Services (IAS) servers in your environment that run Windows Server® 2003 Service Pack 2 (SP2) or later. IAS is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy that enables centralized management of user authentication, authorization, and accounting. You can use IAS to authenticate users in databases on Windows Server 2003 SP2, Windows NT® 4.0, or Windows 2000 domain controllers. IAS also 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 to evaluate the threat environment and to determine whether additional security should be used.

The settings in this chapter are configured and applied through Group Policy. A Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) that contain the IAS servers to provide the required security setting changes for this server role. This chapter only discusses those policy settings that vary from the MSBP.

Where possible, these settings are gathered in an incremental Group Policy template that will be applied to the IAS Servers OU. Some of the settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these settings manually is provided.

The name of the infrastructure server Security Template for the EC environment is EC-Infrastructure Server.inf. This template provides the settings for the incremental IAS Server template, which in turn is used to create a new GPO that is linked to the IAS Servers OU. Step-by-step instructions are provided in Chapter 1, "Windows Server 2003 Hardening Mechanisms" to help you create the OUs and Group Policies and then import the appropriate Security Template into each GPO.

For information about settings in the MSBP, see Chapter 3, "Implementing the Security Baseline." For information about all default setting configurations, see the companion guide, *Threats and Countermeasures*.

Note: The setting prescriptions for the IAS server role were tested for the Enterprise Client environment only. For this reason, the DoS attack information specified for the majority of the other server roles in this guide is not included here.

Additional Security Settings

Although the security settings that are applied through the MSBP significantly enhance the security of IAS servers, this section discusses some additional considerations. However, the settings in this section cannot be applied through Group Policy, and must therefore be performed manually on all IAS servers.

Securing Well-Known Accounts

Windows Server 2003 SP2 or later 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter the description for it to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well-known accounts on IAS servers

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Note: The built-in Administrator account can be renamed through Group Policy. This policy setting was not implemented in any of the Security Templates provided with this guide because every environment should choose a unique name for this account. However, the **Accounts: Rename administrator account** setting can be configured to rename administrator accounts in the EC environment. This policy setting is a part of the Security Options settings section of a GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- IAS and firewalls.
- Internet Authentication Service.
- RADIUS Accounting.
- *Services and Service Accounts Security Planning Guide*.

- *Threats and Countermeasures*.
- Understanding IAS.

Chapter 10: Hardening Certificate Services

This chapter provides guidance to help you harden servers that run Windows Server® 2003 Service Pack 2 (SP2) or later and Microsoft Certificate Services in your environment. Although this chapter includes all of the information you need to secure these types of servers, it does not provide any details about how to create a secure Certificate Services infrastructure in your environment or how to deploy a certification authority (CA). These topics are discussed in detail in the Windows Server 2003 SP2 product documentation. They are also discussed in the *Windows Server 2003 Resource Kit* and in white papers that are available on the Microsoft Web site. Additional information can be found in a companion guide: *Securing Wireless LANs with Certificate Services*.

The settings in this chapter are configured and applied through Group Policy. A Group Policy object (GPO) that complements the Member Server Baseline Policy (MSBP) can be linked to the appropriate organizational units (OUs) that contain the CA servers to provide the required security setting changes for this server role. This chapter only discusses those policy settings that vary from the MSBP.

Where possible, these settings are gathered in an incremental Group Policy template that will be applied to the CA Servers OU. Some of the settings in this chapter cannot be applied through Group Policy. Detailed information about how to configure these settings manually is provided.

The name of the CA Server security template for the EC environment is EC-CA Server.inf. This is the incremental CA Server template, which is used to create a new GPO that is linked to the CA Servers OU in the appropriate environment. Step-by-step instructions are provided in Chapter 1, "Windows Server 2003 Hardening Mechanisms" to help you create the OUs and Group Policies and then import the appropriate security template into each GPO.

For information about settings in the MSBP, see Chapter 3, "Implementing the Security Baseline." For information on all default settings, see the companion guide, *Threats and Countermeasures*.

Note: The policy setting recommendations for the Certificate Services server role were tested for the Enterprise Client environment only. For this reason, the denial of service (DoS) information that was specified for most of the other server roles in this guide is not included in this chapter.

You might install Microsoft Internet Information Services (IIS) on some of the Certificate Services servers in your environment so that these servers can distribute 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. Before you act on the information in this chapter, make sure you understand how to securely install IIS, which is described in Chapter 8 "Hardening Web Services" in this guide. If you install IIS on your CAs, the Security Template developed for Chapter 8 must be applied to your Certificate Services servers before you configure the prescribed settings that are described in this chapter.

Note: In simplified environments, you can use the issuing CA server to host the Web server, the CA certificate, and the CRL download points. However, Microsoft recommends to 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 and to distribute CA certificates and CRL download points for non–Windows clients. Microsoft recommends to not install IIS on the root CA server. If possible, do not run IIS on your issuing CA 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. Many certificate users (internal and external) who need to retrieve CRLs or CA chain information should not necessarily be permitted access to the CA. However, you cannot isolate users from the CA if you host the download points on it.

Additional Security Settings

You can assign the following suggested access control lists (ACLs) through Group Policy. However, these ACLs are not included in the Security Templates provided with this guide because the path for the database and logs differ from server to server. For example, your Certificate Servers server could have a C:\, D:\, and E:\ drive. Details about how to manually implement these policy settings are provided in the following section.

File System ACLs

Files that are not protected by access control lists (ACLs) can be easily viewed, changed, or deleted by unauthorized users who can access them locally or over the network. Although ACLs can help protect files, 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 SP2–based Certificate Services servers in the Enterprise Client environment. In this environment, the Certificate Services servers use **D:\CertSrv** as the certificate database directory and the database logs are stored in the default folder **%SystemRoot%\system32\CertLog**. It is also possible to move the logs from the system drive to a physically separate mirrored drive, such as **E:\CertLog**. Security considerations do not require separation of the database and logs onto different physical disk drives, but this configuration is recommended for added protection from disk failures and to improve performance. The Certificate Services default installation folders **%SystemRoot%\system32\CertLog** and **%SystemRoot%\system32\CertSrv** have the correct ACLs by default, which are included in the following table.

Table 10.1 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)

ACL path in UI	Enterprise Client
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 that are listed in the preceding table. The audit entries are configured as shown in the following table:

Table 10.2 Certificate Services File and Registry Audit Configuration

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)

These policy settings audit any type of failure access (read or modify) from any user and also audit any successful modification by any user.

Securing Well-Known Accounts

Windows Server 2003 SP2 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 Server 2003 SP2 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this well-known account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well-known accounts on CA servers

- Rename the Administrator and Guest accounts, and change their passwords to long and complex values on every domain and server.
- 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.

- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record these changes in a secure location.

Note: You can rename the built-in Administrator account through Group Policy. This policy setting was not implemented in any of the Security Templates that are provided with this guide because every organization should choose a unique name for this account. However, you can configure the **Accounts: Rename administrator account** setting to rename the Administrator account in the EC environment. This policy 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 it is unavoidable. If the server is physically compromised, domain account passwords could be easily obtained by dumping LSA secrets. For more information about how to secure service accounts, see *Services and Service Accounts Security Planning Guide*.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter on Microsoft.com:

- An Introduction to the Windows 2000 Public Key Infrastructure for information about PKI concepts and the features of Windows 2000 certificate services.
- PKI Enhancements in Windows XP Professional and Windows Server 2003.
- Public Key Infrastructure.
- *Securing Wireless LANs with Certificate Services*.
- *Services and Service Accounts Security Planning Guide*
- *Threats and Countermeasures*.

Chapter 11: Hardening Bastion Hosts

This chapter focuses on how to harden bastion hosts that run Windows Server® 2003 Service Pack 2 (SP2) or later in your environment. Bastion hosts are secure but publicly accessible computers that are located on the public-facing side of an organization’s perimeter network (also known as DMZ, demilitarized zone, and screened subnet). Bastion hosts are unprotected by a firewall or filtering router, which makes them fully exposed to attack. To minimize the possibility of compromise, bastion hosts need to be carefully designed and configured.

Bastion hosts are commonly used as Web servers, DNS servers, File Transfer Protocol (FTP) servers, Simple Mail Transfer Protocol (SMTP) servers, and Network News Transfer Protocol (NNTP) servers. Ideally, bastion hosts are dedicated to just one of these functions, because the more functions that a server provides the greater the likelihood that a security hole will be overlooked. It is easier to secure a single service on a single bastion host than it is to secure multiple services. Organizations that can afford multiple bastion hosts can greatly benefit 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 configured to fulfill a specific role. If you use this method to harden bastion hosts you can limit potential methods of attack.

The following sections of this chapter describe various security settings that you can use to help secure bastion hosts in any environment. The steps included in the chapter are designed to help you create an SMTP bastion host. You will need to modify the configuration files that are included with the guide to add any additional functionality.

Additional Security Settings

The security settings that the BHLP applies significantly enhance the security of bastion host servers. However, there are a few additional settings to consider. These settings cannot be applied through local policy, and must therefore be completed manually on all bastion host servers.

Manually Adding Unique Security Groups to User Right Assignments

Most user right assignments applied through 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 Server 2003 domains. The user right assignment setting in the following table must be configured manually.

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 the specified “Deny access” user right you will need to log on locally in order to correct the mistake. Also, the built-in Administrator account may have been renamed, as recommended in Chapter 3, "Implementing the Security Baseline." When you add the Administrator account to a user right, ensure that you specify the renamed account.

Table 11.1 Manually Added User Right Assignment

Setting	Enterprise Client	Specialized Security – Limited Functionality
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

Important: "All non-operating system service accounts" include service accounts used for specific applications across an enterprise, but does *not* include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts (the built-in accounts that the operating system uses).

Securing Well-Known Accounts

Windows Server 2003 SP2 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 Server 2003 SP2 are Guest and Administrator. By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. However, many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, Microsoft recommends to rename the built-in Administrator account and alter its description to help prevent compromise of remote servers by attackers who try to use this account.

The value of this configuration change has diminished over the past few years since the release of attack tools that specify the security identifier (SID) of the built-in Administrator account to determine its true name and then break into the server. 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. However, your operations groups can easily monitor attempted attacks against this Administrator account if you rename it with a unique name.

To secure well known accounts on bastion host servers

- Rename the Administrator and Guest accounts, and then change their passwords to long and complex values on every server.
- 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.
- Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
- Record any changes that you make in a secure location.

Error Reporting

Table 11.2 Recommended Error Reporting Setting

Setting	Enterprise Client	Specialized Security – Limited Functionality
Turn off Windows Error Reporting	Enabled	Enabled

This 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. It is only available in Windows XP Professional SP3 and Windows Server 2003 SP2.

The **Error Reporting** service can report such errors to Microsoft through the Internet or to an internal file share. Although error reports can potentially contain sensitive or even confidential data, the Microsoft privacy policy with regard to error reporting ensures that Microsoft will not use such data improperly. However, the data is transmitted in plaintext HTTP, which could be intercepted on the Internet and viewed by third parties.

The **Turn off Windows Error Reporting** setting controls whether the **Error Reporting** service transmits any data.

You can configure this policy setting in Windows Server 2003 SP2 at the following location within the Group Policy Object Editor:

> **Computer Configuration\Administrative Templates\System\Internet Communications Management\Internet Communications settings**

Configure the **Turn off Windows Error Reporting** setting to **Enabled** in the BHLP for both of the environments that are defined in this guide.

More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this chapter:

- Chapter 9, "Firewalls and Virtual Private Networks" in a .pdf file by Elizabeth D. Zwicky, Simon Cooper, and Brent D. Chapman.
- "Hardening Bastion Hosts" white paper from the SANS Institute.
- Intruder Detection Checklist.
- "Problems After You Import Multiple Templates Into the Security Configuration and Analysis Tool": Microsoft Knowledge Base article 279125.
- *RFC 2196 Site Security Handbook*.
- U.S. Military defense in depth page.