Microsoft Solutions for Security and Compliance

Windows Server 2003 Security Guide

April 26, 2006

Microsoft

Contents

Feedback

The Microsoft Solutions for Security and Compliance team would appreciate your thoughts about this and other security solutions.

Have an opinion? Let us know on the secguide's WebLog at http://blogs.technet.com/secguide.

Or e-mail your feedback to the following address: secwish@microsoft.com.

We look forward to hearing from you.

Chapter 1: Introduction to the Windows Server 2003 Security Guide

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 Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1). The chapters in this guide provide detailed guidance about how to enhance security setting configurations and features in Windows Server 2003 with SP1 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 with SP1 environment.

This guide was reviewed and approved by Microsoft engineering teams, consultants, support engineers, as well as customers and partners. Microsoft worked with consultants and systems engineers who have implemented Windows Server 2003, Windows® XP, and Windows 2000 in a variety of environments to help establish the latest best practices to secure these servers and clients. This best practice information is described in detail in this guide.

The companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP (available at http://go.microsoft.com/fwlink/?LinkId=15159), provides a comprehensive overview of all of the major security settings that are present in Windows Server 2003 with SP1 and Windows XP with SP2. Chapters 2 through 12 of this guide include step-by-step security prescriptions, procedures, and recommendations to provide you with task lists that will help you achieve an elevated level of security for those computers that run Windows Server 2003 with SP1 in your organization. If you want more in-depth discussion of the concepts behind this material, refer to resources such as the *Microsoft Windows Server 2003 Resource Kit*, the *Microsoft Windows XP Resource Kit*, the *Microsoft Windows 2000 Security Resource Kit*, and Microsoft TechNet.

Executive Summary

Whatever your environment, you are strongly advised to 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, which could affect your organization's profitability. When you evaluate security costs, you should include the indirect costs that are 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 with SP1, 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 with SP1 in three distinct enterprise environments. The Legacy Client (LC) environment must support older operating systems such as Windows 98. The Enterprise Client (EC) environment is one in which Windows 2000 is the earliest version of the Windows operating system in use. The third 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 third environment 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 the enterprise customer, much of it is appropriate for organizations of any size.

To get the most value out of the material, you will need to read the entire guide. You can also refer to the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, at http://go.microsoft.com/fwlink/?LinkId=15159.

The team that produced this guide hopes that you will find the material covered in it useful, informative, and interesting.

Who Should Read This Guide

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

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

Scope of this Guide

This guide focuses on how to create and maintain a secure environment for computers that run Windows Server 2003 with SP1 in your organization. The guidance explains the different stages of how to secure the three environments that are defined in the guide, and what each prescribed server setting addresses in terms of client dependencies. The three environments are described as follows:

- The Legacy Client (LC) environment consists of an Active Directory® directory service domain with member servers and domain controllers that run Windows Server 2003 and some client computers that run Microsoft Windows 98 and Windows NT® 4.0. Computers that run Windows 98 must have the Active Directory Client Extension (DSCLient) installed. More information is available in the Microsoft Knowledge Base article "How to install the Active Directory client extension" at http://support.microsoft.com/kb/288358.

- The Enterprise Client (EC) environment consists of an Active Directory domain with member servers and domain controllers that run Windows Server 2003 with SP1 and client computers that run Windows 2000 and Windows XP.
- 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 with SP1 and clients that run Windows 2000 and Windows XP. 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 three 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 security templates 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
- File servers
- Print servers
- Internet Information Services (IIS) servers
- Internet Authentication Services (IAS) servers
- Certificate Services servers
- Bastion hosts

The recommended settings in this guide were tested thoroughly in lab environments that simulated the previously described Legacy Client, 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 security templates 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.

Chapter Summaries

The *Windows Server 2003 Security Guide* consists of 13 chapters. Each chapter builds on the end-to-end solution process that is required to implement and secure Windows Server 2003 with SP1 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.

Chapter 1: Introduction to the Windows Server 2003 Security Guide

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

Chapter 2: Windows Server 2003 Hardening Mechanisms

This chapter provides an overview of the main mechanisms that are used to harden Windows Server 2003 SP1 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 three environments that are described in Chapter 1.

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 three environments that are described in Chapter 1 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 with SP1.

Chapter 3: The Domain Policy

This chapter explains security template settings and additional countermeasures for the domain-level policies in the three environments that are described in Chapter 1. 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 4: The Member Server Baseline Policy

This chapter explains security template settings and additional countermeasures for the different server roles in the three environments that are described in Chapter 1. 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 with SP1. 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. Occasionally, a less restrictive setting is suggested than the one that is present in the default installation of Windows Server 2003 with SP1 to provide support for Legacy Client environments.

Chapter 5: The Domain Controller Baseline Policy

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 with SP1. 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 with SP1 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 6: The Infrastructure Server Role

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 with SP1 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 7: The File Server Role

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 with SP1 can benefit from security settings that are not applied by the MSBP.

Chapter 8: The Print Server Role

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 with SP1 print server security settings can be strengthened in ways that are not applied by the MSBP.

Chapter 9: The Web Server Role

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 with SP1 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 10: The IAS Server Role

Internet Authentication Servers (IAS) provide 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 with SP1 can benefit from security settings that are not applied by the MSBP.

Chapter 11: The Certificate Services Server Role

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 with SP1 will benefit from security settings that are not applied by the MSBP.

Chapter 12: The Bastion Hosts Role

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 with SP1 can benefit from the security recommendations in this guide for computers that are not members of an Active Directory–based domain.

Chapter 13: Conclusion

The concluding chapter of this guide reviews the important points of the material that was presented in the previous chapters.

Appendix A: Security Tools and Formats

Although this guide focuses on how to use SCW to create policies which are then converted to security templates and Group Policy objects, there are a variety of other tools and file formats that can be used to augment or replace this methodology. This appendix provides a short list of these tools and formats.

Appendix B: Key Settings to Consider

This guide discusses many security countermeasures and security settings, but it is important to understand a small number of them are particularly important. This appendix discusses the settings that will have the biggest impact on security of computers that run Windows Server 2003 with SP1.

Appendix C: Security Template Setting Summary

This appendix introduces the Microsoft Excel® workbook "Windows Server 2003 Security Guide Settings," which is included with the tools and templates in the downloadable version of this guide at http://go.microsoft.com/fwlink/?LinkId=14846. This spreadsheet provides a comprehensive master reference in a compact, usable form of all of the recommended settings for the three environments that are defined in this guide.

Appendix D: Testing the Windows Server 2003 Security Guide

This guide provides a significant amount of information about how to harden servers that run Windows Server 2003 with SP1, but the reader is constantly cautioned to test and validate all settings before they implement any settings in a production environment.

This appendix provides guidance about how to create a suitable test lab environment that can be used to help ensure successful implementation of the recommended settings in a production environment. It helps users to perform necessary validation and minimizes the amount of resources that are needed to do so.

Tools and Templates

A collection of security templates, scripts, and additional tools are included with the downloadable version of this guide to help your organization to evaluate, test, and implement the recommended countermeasures. The security templates are text files that can be imported into domain–based Group Policies or applied locally with the Microsoft Management Console (MMC) Security Configuration and Analysis snap-in. These procedures are detailed in Chapter 2, "Windows Server 2003 Hardening Mechanisms." The scripts that are included with this guide include scripts to create and link Group Policy objects as well as test scripts that are used to test the recommended countermeasures. Also included is the Excel workbook that summarizes the security template settings (referenced in the earlier "Appendix C" section).

The files that accompany this guide are collectively referred to as tools and templates. These files are included in a .msi file within the self-extracting WinZip archive that contains this guide, which is available on the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=14846. When you execute the .msi file, the following folder structure will be created in the location you specify:

- **\Windows Server 2003 Security Guide Tools and Templates\Security Templates**. This folder contains all security templates that are discussed in the guide.
- **\Windows Server 2003 Security Guide Tools and Templates\Test Tools**. This folder contains various files and tools that relate to "Appendix D: Testing the Windows Server 2003 Security Guide."

Skills and Readiness

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

- MCSE 2000 or 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.

Software Requirements

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

- Windows Server 2003 Standard Edition with SP1, Windows Server 2003 Enterprise Edition with SP1, or Windows Server 2003 Datacenter Edition with SP1.
- A Windows Server 2003–based Active Directory domain.
- Microsoft Excel 2000 or later.

Style Conventions

This guide uses the following style conventions and terminology.

Table 1.1 Style Conventions

Element	Meaning
Bold font	Signifies characters typed exactly as shown, including commands, switches, and file names. User interface elements also appear in bold.
Italic font	Titles of books and other substantial publications appear in italic.

Element	Meaning
<*Italic*>	Placeholders set in italic and angle brackets <*file name*> represent variables.
`Monospace font`	Defines code and script samples.
Note	Alerts the reader to supplementary information.
Important	Alerts the reader to essential supplementary information.

Summary

This chapter provided an overview of the primary factors that are involved to secure computers that run Windows Server 2003 with SP1, which are considered and discussed in greater detail in the rest of the guide. Now that you understand how this guide is organized, you can decide whether to read it from beginning to end or select only those sections that interest you.

However, it is important to remember that effective and successful security operations require improvements in all of the areas that are discussed in this guide, not just a few. For this reason, Microsoft recommends that you read the entire guide to take full advantage of all the information it contains to secure computers that run Windows Server 2003 with SP1 in your organization.

More Information

The following links provide additional information about topics that relate to security and Windows Server 2003 with SP1.

- For more information about security at Microsoft, see the Trustworthy Computing page at www.microsoft.com/mscorp/twc/default.mspx.
- For more details about how MOF can assist in your enterprise, see the Microsoft Operations Framework page at www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspx.
- For information about Microsoft security notifications, see the Microsoft Security Bulletin Search page at www.microsoft.com/technet/security/current.aspx.

Chapter 2: Windows Server 2003 Hardening Mechanisms

Overview

This chapter introduces the mechanisms that can be used to implement security settings on Microsoft® Windows Server™ 2003. Service Pack 1 (SP1) of Windows Server 2003 provides the Security Configuration Wizard (SCW), a new role-based tool 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 SCW is used 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 SCW and Group Policy to create a manageable, role-based approach to harden servers that run Windows Server 2003 with SP1.

This information provides a foundation and a vision that you can use to evolve from a Legacy Client (LC) environment 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 with SP1. 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 SCW, administrators can author, test, troubleshoot, and deploy security policies that disable all non-essential functionality. It also provides the ability to roll back security policies. SCW provides native support for security policy management on single servers as well as groups of servers that share related functionality.

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 SCW are available in a downloadable version of the Security Configuration Wizard Documentation at www.microsoft.com/downloads/details.aspx?FamilyID=903fd496-9eb9-4a45-aa00-3f2f20fd6171&displaylang=en.

Note: SCW can only be used with Windows Server 2003 with SP1. It cannot be used to create policies for Windows 2000 Server, Windows XP, 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 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 SCW to create and test policies, you should deploy SCW to all targeted servers. Although you create the policy on a management station, SCW will attempt to communicate with the target servers to inspect their configuration and fine-tune the resulting policy.

SCW is integrated with the IPsec and Windows Firewall subsystems and will modify those settings accordingly. Unless prevented, 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, SCW can create them. As a result, policies that are created by 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.

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 SCW in the following areas:

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

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 SCW, you can combine security templates with the results of SCW to create a more complete configuration.

When you use 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. SCW saves the previous configuration settings in XML files.

For organizations that have limited resources to design and test security configurations, 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 Group Policy object 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 Group Policy Object

The third option for SCW policy deployment is to use the Scwcmd tool to convert the XML-based policy into a Group Policy object (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" at www.microsoft.com/downloads/details.aspx?FamilyID=4e734065-3f18-488a-be1e-f03390ec5f91&.

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 non-domain 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.

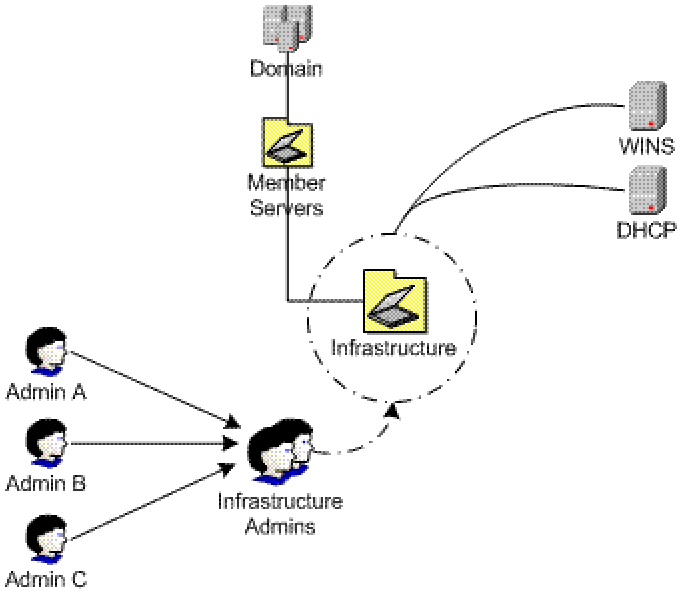

Figure 2.1 OU delegation of administration

When the **Infrastructure Admin** group is delegated control of the Infrastructure OU, the members of this group will have 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 OUs can be used 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.

Group Policy Application

Use Group Policy and delegate administration to apply specific settings, rights, and behavior to all servers within an OU. When you use Group Policy instead of manual steps, it is simple to update multiple servers with any additional changes that might be required.

Group Policies are accumulated and applied in the order that is shown in the following illustration.

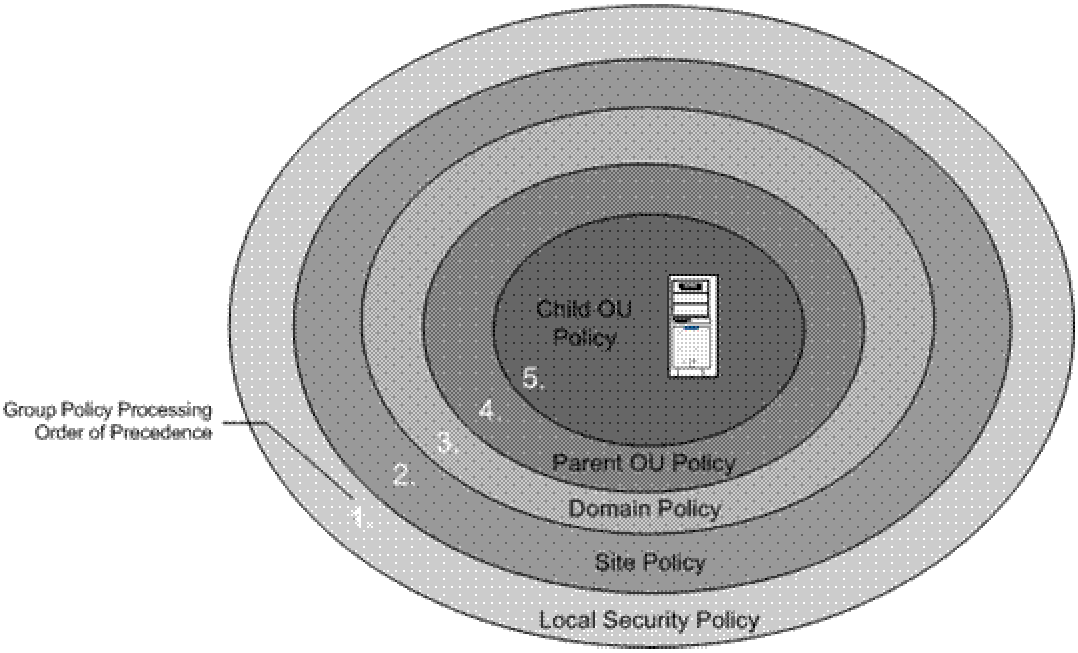

Figure 2.2 GPO application hierarchy

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

Remember the following basic considerations when you apply Group Policy:

- You must set the GPO application order for Group Policy levels with multiple GPOs. If multiple policies specify the same option, the last one that is applied will take precedence.
- You must configure a Group Policy with the **No Override** option if you do not want other GPOs to override it. If you use the Group Policy Management Console (GPMC) to manage your GPOs, the name of this option is **Enforced**.

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 and Microsoft Windows XP–based computers that run in an Active Directory domain.

The W32Time service synchronizes the clocks of Windows Server 2003–based computers with the domain controllers in a domain. This synchronization is necessary for the Kerberos 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. In a Windows Server 2003 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.

Security Template Management

Security templates are text–based files that you can use to apply a security configuration to a computer. You can modify security templates with the Microsoft Management Console (MMC) Security Templates snap-in or with a text editor such as Notepad. Some sections of the template files contain specific ACLs that are written in the Security Descriptor Definition Language (SDDL). You can find more information about how to edit security templates and SDDL on the "Security Descriptor Definition Language" page on Microsoft MSDN® at http://msdn.microsoft.com/library/en-us/secauthz/security/security_descriptor_definition_language.asp.

By default, authenticated users have the right to read all settings in a Group Policy object. Therefore, it is very important to store security templates for a production environment in a secure location that only administrators who implement Group Policy can access. The purpose is not to prevent *.inf files from being viewed, but rather to prevent unauthorized changes to the source security templates.

All computers that run Windows Server 2003 store security templates in their local **%SystemRoot%\security\templates** folder. This folder is not replicated across multiple domain controllers, so you will need to designate one location to hold the master copy of the security templates to prevent version control problems with the templates. After the centrally-located template is modified, it can be redeployed to the appropriate computers. This approach will ensure that you always modify the same copy of the templates.

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.

Sever Role Organizational Units

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 Policies 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 Policies.

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 three environments and their functionality are discussed in Chapter 1, "Introduction to the Windows Server 2003 Security Guide."

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 SCW on a standard member server to create a Member Servers Baseline.xml file. As part of the XML creation, use SCW to include one of the supplied Member Server Baseline security templates (LC-Member Server Baseline.inf, 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 4, "The Member Server Baseline Policy."

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 Organizational Units

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. Three security templates are provided with this solution, one for each security environment: LC-Infrastructure Server.inf, EC-Infrastructure Server.inf, and SSLF-Infrastructure Server.inf. When used together with 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" and related topics at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/deploy/dgbd_ads_heqs.asp?frame=true.

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

Table 2.1 Windows Server 2003 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.inf
Domain controller	All Active Directory domain controllers. These servers are also DNS servers.	<*Env*>-Domain Controller.inf
Infrastructure server	All locked down WINS and DHCP servers.	<*Env*>-Infrastructure Server.inf
File server	All locked down file servers.	<*Env*>-File Server.inf

Server role	Description	Security template file name
Print server	All locked down print servers.	<*Env*>-Print Server.inf
Web server	All locked down IIS web servers.	<*Env*>-Web Server.inf
IAS server	All locked down IAS servers.	<*Env*>-IAS Server.inf
Certificate Services server	All locked down Certification Authority (CA) servers.	<*Env*>-CA Server.inf
Bastion host	All Internet-facing servers.	<*Env*>-Bastion Host.inf

All template files except those for the bastion host servers are applied to the corresponding child OUs. Each of these child OUs require that you 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 templates that correspond to all environments. For example, the bastion host role is always considered to be in the SSLF environment.

Important: This guide assumes that computers that run Windows Server 2003 will perform specifically defined roles. If the servers in your organization do not match these roles, or if you have multipurpose servers, use the settings that are 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.

An example of the final OU design to support these defined server roles in the EC environment is shown in the following illustration.

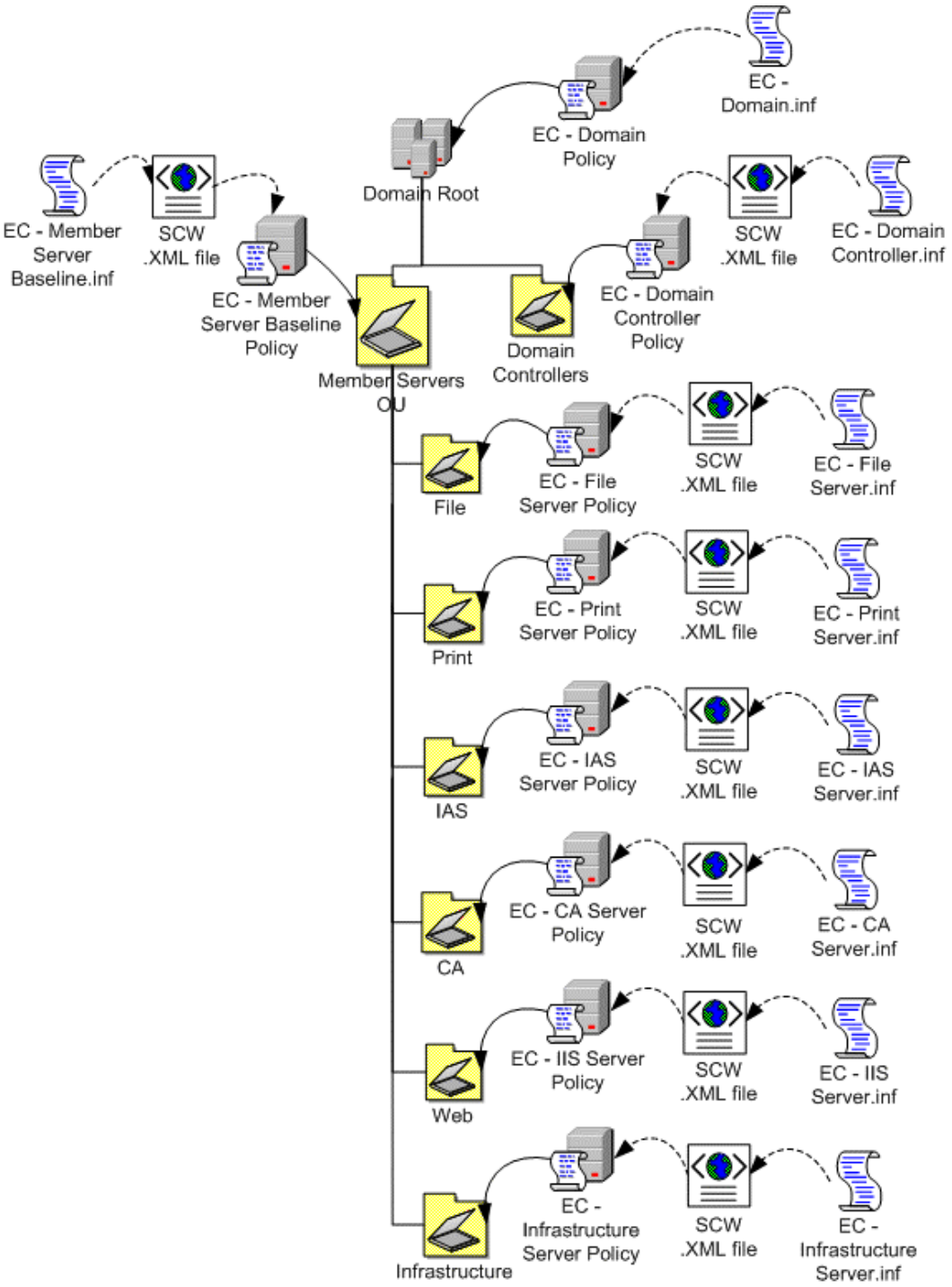

Figure 2.3 OU design example

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. 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 2.2 OUs and Administrative Groups

OU name	Administrative group
Domain Controllers	Domain Engineering
Member Servers	Domain Engineering
Infrastructure	Infrastructure Admins
File	Infrastructure Admins
Print	Infrastructure Admins
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 that are related to 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:

1. Create the Active Directory environment, including groups and OUs. You should create the appropriate administrative groups and delegate OU permissions to the corresponding groups.
2. Configure time synchronization on the domain controller that hosts the PDC Emulator FSMO.
3. Configure the domain policies.
4. Create the baseline policies with SCW.

5. Test the baseline policies with SCW.
6. Convert the baseline policies to GPOs and link them to the appropriate GPOs.
7. Create the role policies with SCW and the included security templates.
8. Test the role policies with SCW.
9. 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 three environments and their functionality are discussed in Chapter 1, "Introduction to the Windows Server 2003 Security Guide."

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 that you will use to create the OUs and groups that are used in this guide and configure them for the 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 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 Admins** and add the appropriate domain accounts to it.
6. Run the Delegation of Control Wizard to provide the **Infrastructure Admins** 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 2.2 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 will help ensure that Kerberos authentication works properly and allow 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 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, this procedure can be run on any computer that runs Windows XP or member of the Windows Server 2003 family. It is not usually necessary to synchronize all servers' 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.

Configure the Domain Policy

The following procedure imports the security templates that are provided with this guide for the domain-level policy. This policy is provided as a security template, because SCW does not address domain-level policies. Before you implement the following procedure, the specific policy (.inf) file must be located on your computer.

Warning: The security templates in this guide are designed to increase security in your environment. It is quite possible that their installation could cause some functionality in your environment to be lost, and mission critical applications could fail. It is **essential** that you thoroughly test these settings before you deploy them in a production environment. Back up each domain controller and server in your environment before you apply any new security settings. Ensure the system state is included in the backup, which will enable registry settings and Active Directory objects to be restored if necessary.

To import the Domain Policy security templates

1. In Active Directory Users and Computers, right-click the domain, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new GPO.
3. Type **EC-Domain Policy**, and then press ENTER.
4. Right-click **EC-Domain Policy**, and then select **No Override**.
5. Select **EC-Domain Policy**, and then click **Edit**.
6. In the Group Policy Object Editor window, click **Computer Configuration\Windows Settings**. Right-click **Security Settings**, and then select **Import Policy**.
7. In the **Import Policy From** dialog box, navigate to **"\Tools and Templates\Security Guide\Security Templates"** and then double-click **EC-Domain.inf**.
8. Close the Group Policy that has been modified.
9. Close the **Domain Properties** window.
10. If you do not want to wait for scheduled Group Policy application, you can initiate the process manually. Open a command prompt, type **gpupdate /Force** and press ENTER.
11. Verify in the event log that the Group Policy downloaded successfully and that the server can communicate with the other domain controllers in the domain.

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

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

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

To clear the Allow Inheritable Permissions option

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

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

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

Create the Baseline Policies Manually Using SCW

The next step is to use SCW to create the member server baseline policy.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use hardware that is similar to the hardware that you will use in your deployment, which will help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the member server baseline policy (MSBP) creation steps, note that you remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the Member Server Baseline Policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain.
4. Install only the mandatory applications that should be on every server in your environment. Examples include your software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch SCW, select **Create new policy**, and point it to the reference computer.
6. Remove the File server role from the listed of detected roles.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that required by your baseline, such as backup agents or antivirus software, are detected.

10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Review the network settings and ensure that the appropriate ports and applications have been detected and will be configured as exceptions for the Windows Firewall.
12. Skip the "Registry Settings" section.
13. Skip the "Audit Policy" section.
14. Include the appropriate security template (for example, EC-Member Server Baseline.inf).
15. Save the policy with an appropriate name (for example, Member Server Baseline.xml).

To create the Domain Controller policy

You must use a computer that is configured as a domain controller to create the Domain Controller policy. You can use either an existing domain controller or create a reference computer and use the Dcpromo tool to make the computer a domain controller. However, most organizations do not want to add a domain controller to their production environment because it may violate their security policy. If you use an existing domain controller, make sure that you do not apply any setting to it with SCW or modify its configuration.

1. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
2. Install only the mandatory applications that should be on every server in your environment. Examples include your software and management agents, tape backup agents, and antivirus or antispyware utilities.
3. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
4. Ensure that the detected roles are appropriate for your environment.
5. Ensure that the detected client features are appropriate for your environment.
6. Ensure that the detected administrative options are appropriate for your environment.
7. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
8. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network, because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
9. Review the network settings and ensure that the appropriate ports and applications have been detected and will be configured as exceptions for the Windows Firewall.
10. Skip the "Registry Settings" section.
11. Skip the "Audit Policy" section.
12. Include the appropriate security template (for example, EC-Domain Controller.inf).
13. Save the policy with an appropriate name (for example, Domain Controller.xml).

Test the Baseline Policies Using SCW

After you create and save the baseline policies, Microsoft strongly recommends that you deploy them to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policies. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push policies to a single server at a time, or use Scwcmd to push them to a group of servers. The native deployment method offers the advantage of the ability to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the testing process.

The policies are tested to ensure that their application to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more detailed information about how to test SCW policies, see "Deployment Guide for the Security Configuration Wizard" at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the downloadable version of the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert the Baseline Policies to GPOs

After you thoroughly test the baseline policies, complete the following steps to convert them into GPOs and link them to the appropriate OUs:

1. At a command prompt, type the following:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform
   /p:"C:\Windows\Security\msscw\Policies\Infrastructure.xml"
   /g:"Infrastructure Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Create the Role Policies Using SCW

The next step is to use SCW to create the role policies for each server role.

The steps to create the role-specific policies are similar to the steps you followed when you created the MSBP. You should once again use a reference computer to help ensure that there are no legacy settings or software from previous configurations.

To create the role policies

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the new server to the domain.
4. Install the mandatory applications that should be on every server in your environment. Examples include your software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Configure the appropriate roles for the computer. For example, if your target servers will run DHCP and WINS, install those components. They do not need to be configured exactly the same as the deployed servers, but the roles must be installed.
6. Launch SCW.
7. Select **Create new policy** and point it to the reference computer.
8. Ensure that the detected roles are appropriate for your environment.
9. Ensure that the detected client features are appropriate for your environment.
10. Ensure that the detected administrative options are appropriate for your environment.
11. Ensure that any additional services required by your baseline, such as backup agents or antivirus software, are detected.
12. Decide how to handle unspecified services in your environment. For stronger security (and reduced functionality) you may wish to configure this policy setting to **Disable**, which will disable any new service that was not explicitly allowed through SCW. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
13. Confirm all service changes that are listed.
14. Review the network settings and ensure that SCW detected the appropriate ports and applications to configure as exceptions for the Windows Firewall.
15. Skip the "Registry Settings" section.
16. Skip the "Audit Policy" section.
17. If the server is configured with the Web server role, complete the steps in the “Internet Information Services” section to ensure that SCW is configured to support the necessary IIS features.
18. Click **Include Security Templates** to add the appropriate security template.
19. Save the policy with an appropriate name.

Test the Role Policies Using SCW

As with the baseline policies, there are two different ways to test the policies. You can use the native SCW deployment facilities, or you can deploy the policies through GPOs.

Again, Microsoft strongly recommends that you deploy your role policies in a test environment before you use them in production. This approach will help minimize downtime and failures in your production environment. After you thoroughly test the new configuration, you can convert the policies into GPOs as shown in the following procedure and apply them to the appropriate OU.

Convert the Role Policies to GPOs

After you thoroughly test the role policies, complete the following steps to convert them into GPOs and link them to the appropriate OUs:

1. At a command prompt, type the following:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform
   /p:"C:\Windows\Security\msscw\Policies\Infrastructure.xml"
   /g:"Infrastructure Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU, and make sure to move it above the Default Domain Controllers Policy so that it receives the highest priority.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click Windows Firewall.

Summary

Security administrators need to understand the strengths and weaknesses of SCW compared to conventional Group Policy-based hardening methods so that they can choose the right methodology for their environment. SCW and Group Policy can be used together to gain the ability to rapidly and consistently prototype policies that SCW provides together with the scalable deployment and management capabilities of Group Policy.

Several design considerations are involved when forest, domain, and OU designs are reviewed to secure an environment.

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

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

Although it may not be easy to change the forest or domain design in an organization, it may be necessary to remediate some security risks. It is also important to plan the OU deployment in the organization to accommodate the needs of both service administrators and data administrators. This chapter provided detailed information about how to create an OU model that will support the use of GPOs for the ongoing management of different server roles in the organization.

More Information

The following links provide additional information about topics that relate to hardening servers that run Windows Server 2003 with SP1.

- For more information about security and privacy at Microsoft, see the Trustworthy Computing: Security page at www.microsoft.com/mscorp/twc/default.mspx.
- For sound security guidelines, see "Ten Immutable Laws of Security" at www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx.
- For guidance about how to secure the Active Directory database, see "Best Practice Guide for Securing Active Directory Installations" at www.microsoft.com/downloads/details.aspx?FamilyID=4e734065-3f18-488a-be1e-f03390ec5f91&.
- For information about Active Directory design considerations, see "Design Considerations for Delegation of Administration in Active Directory" at www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/addeladm.mspx.
- For information about how to configure a time server, see the Microsoft Knowledge Base article "How to configure an authoritative time server in Windows 2000" at http://support.microsoft.com/?kbid=216734.
- For information about network ports that are used by Microsoft applications, see the Microsoft Knowledge Base article "Service overview and network port requirements for the Windows Server system" at http://support.microsoft.com/kb/832017.

Chapter 3: The Domain Policy

Overview

This chapter uses the construction of a domain environment to demonstrate ways to address security within a Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) infrastructure.

This chapter focuses on the following topics:

- Security settings and countermeasures at the domain level.
- How to secure a Windows Server 2003 domain for the Legacy Client (LC), Enterprise Client (EC), and Specialized Security – Limited Functionality (SSLF) environments that are defined in Chapter 1, "Introduction to the Windows Server 2003 Security Guide."

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

Windows Server 2003 with SP1 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: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Domain Policy

You can apply Group Policy security settings at several different levels in an organization. The baseline environment that is discussed in Chapter 2, "Windows Server 2003 Hardening Mechanisms" used 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 will 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 with SP1. 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 rights 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. 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 all three 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 three environments that are defined in this guide: Legacy Client, 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.

Password Policy Settings

The following table includes the password policy setting recommendations for all three environments that are defined in this guide. You can configure the password policy settings in the following location in the Group Policy Object Editor:

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

Additional information for each setting is provided in the subsections that follow the table.

Table 3.1 Password Policy Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Enforce password history	24 passwords remembered	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	42 days	42 days
Minimum password age	1 day	1 day	1 day
Minimum password length	8 characters	8 characters	12 characters
Password must meet complexity requirements	Enabled	Enabled	Enabled
Store password using reversible encryption	Disabled	Disabled	Disabled

Enforce password history

This policy setting determines the number of unique new passwords that must be associated with a user account before it is possible to reuse an old password. The value can be set between 0 and 24 passwords.

The default value for the **Enforce password history** setting in Windows Server 2003 with SP1 is the maximum, 24 passwords. Microsoft recommends this value for all three environments because it helps ensure that old passwords are not continually reused, because common vulnerabilities are associated with password reuse, and because a low number for this setting will allow users to continually recycle a small number of passwords repeatedly. Also, there are no known issues with this recommendation for environments that include legacy clients.

To enhance the effectiveness of this policy setting, you may also configure the **Minimum password age** setting so that passwords cannot be changed immediately. This combination makes it difficult for users to reuse passwords, either accidentally or on purpose.

Maximum password age

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

Regular password changes can help prevent passwords from being compromised. Most passwords can be cracked if an attacker has enough time and computing power. The more frequently the password changes, the less time an attacker has to crack it. However, the lower this value is set, the greater the potential for an increase in calls to help desk support.

Microsoft recommends that the **Maximum password age** setting be left at the default value of 42 days for all three environments that are defined in this guide. This configuration ensures that passwords are changed periodically but does not require users

to change their password so often that they cannot remember what it is. To balance the needs of security and usability, you can increase the value for this policy setting in the Legacy Client and Enterprise Client environments.

Minimum password age

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

The **Minimum password age** setting must be less than the **Maximum password age** setting, unless the **Maximum password age** setting is configured to **0** (which means that passwords would never expire). Configure the **Minimum password age** to be greater than 0 if you want the **Enforce password history** setting to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they can reuse an old favorite.

Microsoft recommends that you enforce the **Minimum password age** default value of 1 day for all three environments that are defined in this guide. When this setting is used in conjunction with a similar low value in the **Enforce password history** setting, users can recycle the same passwords again and again. For example, if **Minimum password age** is configured to 1 day and **Enforce password history** is configured to 2 passwords, users would only have to wait 2 days before being able to reuse an old favorite password. However, if **Minimum password age** is configured to 1 day and **Enforce password history** to 24, users would need to change their password every day for at least 24 days before they could reuse a password—which is unlikely.

Minimum password length

This policy setting ensures that passwords have at least a specified number of characters. Long passwords—eight or more characters—are usually stronger than short ones. When the **Minimum password length** setting is used, users cannot use blank passwords and they must create passwords with a specific number of characters. The default value for this setting is seven characters.

This guide recommends that you configure the **Minimum password length** setting to eight characters for the Legacy Client and Enterprise Client environments. This configuration is long enough to provide some level of security but still short enough for users to easily remember. Also, this configuration provides a reasonably strong defense against the commonly used dictionary and brute force attacks.

(Dictionary attacks use word lists to obtain a password through trial and error. Brute force attacks try every possible password or encrypted text value. The likelihood of a successful brute force attack depends on the length of the password, the size of the potential character set, and the computational power that is available to the attacker.)

This guide recommends that you configure the **Minimum password length** setting to 12 characters for the Specialized Security – Limited Functionality environment.

Each additional character in a password increases its complexity exponentially. For example, a seven-character password would have 26^7, or 1×10^7, possible combinations. A seven-character case-sensitive alphabetic password has 52^7 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 62^7 combinations. At 1,000,000 attempts per second, it would take approximately 40 days to crack. An eight-character password has 26^8, or 2×10^{11}, possible combinations. Although this might seem to be an overwhelmingly large number, at 1,000,000 attempts per second (a capability of many password-cracking utilities) it would take only 59 hours to try

all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters, such as ! or @.

Passwords are stored in the Security Accounts Manager (SAM) database or Active Directory after they are passed through a one-way (non-reversible) hash algorithm. Therefore, the only known way to tell if you have the right password is to run it through the same one-way hash algorithm and compare the results. Dictionary attacks run entire dictionaries through the encryption process, looking for matches. They are a simplistic yet very effective approach to determine who uses common words like "password" or "guest" as their account passwords.

Older versions of Windows used a specific type of hashing algorithm known as the LAN Manager Hash (LMHash). This algorithm breaks up the password into blocks of seven or fewer characters and then calculates a separate hash value for each block. Although Windows 2000 Server, Windows XP, and Windows Server 2003 all use a newer hashing algorithm, they may still calculate and store the LMHash for backward compatibility.

When the LMHash values are present, they present a shortcut for password crackers. If a password is seven characters or less, the second half of the LMHash resolves to a specific value that can inform a cracker that the password is shorter than eight characters. Passwords of at least eight characters strengthen even the weaker LMHash, because the longer passwords require crackers to decrypt two portions of each password instead of only one. It is possible to attack both halves of an LMHash in parallel, and the second half of the LMHash is only 1 character long; it will succumb to a brute-force attack in milliseconds. Therefore it is not really beneficial unless it is part of the ALT character set.

For these reasons, the use of shorter passwords in place of longer ones is not recommended. However, minimum length requirements that are too long may cause more mistyped passwords, which can cause an increase in locked out accounts and help desk calls. Also, extremely long password requirements can actually decrease the security of an organization because users may be more likely to write their passwords down so that they do not forget them.

Password must meet complexity requirements

This policy setting checks all new passwords when they are created to ensure that they meet complexity requirements. The Windows Server 2003 policy rules cannot be directly modified. However, you can create a new version of the Passfilt.dll file to apply a different set of rules. For more information about creating a custom Passfilt.dll file, see the MSDN® article "Sample Password Filter" at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmgmt/security/sample_password_filter.asp.

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

When combined with a **Minimum password length** of 8, this setting makes it very difficult to mount a brute force attack. If you include upper and lower case letters and numbers in the keyspace, the number of available characters increases from 26 to 62 characters. An eight-character password then has 2.18×10^{14} possible combinations. At 1,000,000 attempts per second, it would take 6.9 years to cycle through all possible permutations.

For these reasons, Microsoft recommends that the **Password must meet complexity requirements** setting be configured to **Enabled** for all three environments that are defined in this guide.

Store password using reversible encryption

This policy setting determines whether the operating system uses reversible encryption to store passwords. It supports applications that use protocols that require user passwords for authentication purposes.

Passwords that are stored with an encryption method that can be reversed can be retrieved more easily than passwords that are stored with non-reversible encryption. If this setting is enabled, vulnerability is increased.

For this reason, Microsoft recommends that you configure the **Store password using reversible encryption** setting to **Disabled** unless application requirements outweigh the need to protect password information. Also, environments that deploy the Challenge-Handshake Authentication Protocol (CHAP) through remote access or IAS and environments that use digest authentication for Internet Information Services (IIS) require this policy setting to be enabled.

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 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 42 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 the Microsoft Knowledge Base article "How To Prevent Users from Changing a Password Except When Required in Windows Server 2003" at http://support.microsoft.com/?kbid=324744.

Account Lockout Policy

Account lockout policy is a Windows Server 2003 with SP1 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 with SP1 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: Security Settings in Windows Server 2003 and Windows XP at http://go.microsoft.com/fwlink/?LinkId=15159, for additional discussion of these settings and how they interact.

Account Lockout Policy Settings

The following table summarizes the recommended account lockout policy settings. You can use the Group Policy Object Editor to configure these settings in the Domain Group Policy at the following location:

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

Additional information for each setting is provided in the subsections that follow the table.

Table 3.2 Account Lockout Policy Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Account lockout duration	30 minutes	30 minutes	15 minutes
Account lockout threshold	50 invalid login attempts	50 invalid login attempts	10 invalid login attempts
Reset account lockout counter after	30 minutes	30 minutes	15 minutes

Account lockout duration

This policy setting determines the length of time before an account is unlocked and a user can try to log on again. It specifies the number of minutes a locked out account will remain unavailable. If you set the **Account lockout duration** value to 0, accounts will remain locked out until an administrator unlocks them. The Windows Server 2003 with SP1 default value for this policy setting is **Not Defined**.

Although it may seem like a good idea to configure the **Account lockout duration** setting to never automatically unlock, such a configuration may increase the number of calls the help desk receives to unlock accounts that were locked by mistake.

This guide recommends that you configure the **Account lockout duration** setting to **30 minutes** for Legacy Client and Enterprise Client environments and to **15 minutes** for

Specialized Security - Limited Functionality environments. This configuration decreases the amount of operation overhead during a denial of service (DoS) attack. In a DoS attack, an attacker maliciously performs a number of failed logon attempts on all users in the organization, which locks out their accounts. The recommended settings give locked out users the chance to log on again in a reasonable amount of time without the need for assistance from the help desk. However, information about this setting value needs to be communicated to users.

Account lockout threshold

This policy setting determines the number of attempts that a user can make to log on to an account before it is locked.

Authorized users can lock themselves out of their accounts in different ways. They can incorrectly enter their password or they can change their password on one computer while logged on to another computer. The computer with the incorrect password may continuously try to authenticate the user, and because the password it uses to authenticate is incorrect, the user account will eventually be locked out. To avoid lockout of authorized users, configure the **Account lockout threshold** setting to a high number.

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

- To prevent account lockouts, set the value for **Account lockout threshold** setting to 0. This configuration helps reduce help desk calls because users cannot accidentally lock themselves out of their accounts. Also, DoS attacks that try to intentionally lock out accounts in your organization will not succeed. Because it will not prevent a brute force attack, choose this setting only if both of the following criteria are explicitly met:
  - The password policy requires all users to have complex passwords that consist of eight or more characters.
  - A robust audit mechanism is in place that can alert administrators when a series of account logon failures occur in the environment. For example, the audit mechanism should monitor for security event 539, which is "Logon failure. The account was locked out at the time the logon attempt was made." This event means that the account was locked out at the time the logon attempt threshold was reached. However, event 539 only shows an account lockout, not a failed password attempt. Therefore, your administrators should also monitor for a series of bad password attempts.
- If these criteria are not met, the second option is to configure the **Account lockout threshold** setting to a high enough value that will provide users with the ability to accidentally mistype their password several times and not lock themselves out of their accounts. However, the value should help ensure that a brute force password attack will still lock out the account.

This guide recommends that you configure the **Account lockout threshold** setting value to **50** for the Legacy Client and Enterprise Client environments, which should provide adequate security and acceptable usability. This value will prevent accidental account lockouts and reduce help desk calls, but will not prevent a DoS attack as described earlier. However, this guide recommends that you configure this policy setting value to **10** for Specialized Security - Limited Functionality environments.

Reset account lockout counter after

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

The **Reset account lockout counter after** setting works in coordination with other settings. If you leave this policy setting at its default value or configure it to an interval that is too long, you could make your environment vulnerable to an account lockout DoS attack. Without a policy setting to reset the account lockout, administrators would have to manually unlock all accounts. Conversely, if there is a reasonable time value for this setting, users would be locked out for a set period until all of the accounts are unlocked automatically.

This guide recommends that you configure the **Reset account lockout counter after** setting to 30 minutes for the Legacy Client and Enterprise Client environments. This configuration defines a reasonable time period that users are more likely to accept without the need for assistance from the help desk. However, this guide recommends that you configure this policy setting to 15 minutes for Specialized Security – Limited Functionality environments.

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 that no changes be made to the default Kerberos policies. For more information about these policy settings, refer to the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Security Options

The three different types of account policies that are discussed earlier in this chapter are defined at the domain level and are enforced by all of the domain controllers in the domain. A domain controller always obtains the account policy from the Default Domain Policy GPO, even if there is a different account policy applied to the OU that contains the domain controller.

There are three security options settings that are similar to account policies. You should apply these settings at the level of the entire domain and not within individual OUs. You can configure these settings in the Group Policy Object Editor at the following location:

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

Security Options Settings

The following table summarizes the recommended security options settings. Additional information for each setting is provided in the subsections that follow the table.

Table 3.3 Security Options Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled	Enabled
Network Access: Allow anonymous SID/NAME translation	Disabled	Disabled	Disabled
Network Security: Force Logoff when Logon Hours expire	Enabled	Enabled	Enabled

Microsoft network server: Disconnect clients when logon hours expire

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This policy setting affects the server message block (SMB) component. When it is enabled, client sessions with the SMB service are forcibly disconnected when the client's logon hours expire. If it is disabled, an established client session is allowed to be maintained after the client's logon hours have expired. If you enable this policy setting, you should also enable the **Network security: Force logoff when logon hours expire** setting.

If your organization has configured logon hours for users, then it makes sense to enable the **Microsoft network server: Disconnect client when logon hours expire** setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

This guide recommends that you configure the **Microsoft network server: Disconnect client when logon hours expire setting** to **Enabled** for the three environments that are defined in the guide. If logon hours are not used, this policy setting will have no impact.

Network Access: Allow anonymous SID/NAME translation

This policy setting determines if an anonymous user can request the SID for another user.

If the **Network Access: Allow anonymous SID/NAME translation** setting is enabled on a domain controller, a user who knows an administrator's standard well-known SID attributes could contact a computer that also has this policy enabled and use the SID to obtain the administrator's name. That person could then use the account name to initiate a password guessing attack.

Because the default configuration for the **Network Access: Allow anonymous SID/NAME translation** setting is **Disabled** on member computers, they will not be affected by this policy setting. However, the default configuration for domain controllers is **Enabled**. If you disable this policy setting, computers that run older operating systems

may not be able to communicate with domains that are based on Windows Server 2003 with SP1. Examples of such computers include:

- Windows NT® 4.0–based Remote Access Service servers.
- Microsoft SQL Servers™ that run on Windows NT 3.x–based or Windows NT 4.0–based computers.
- Remote Access Service servers that run on Windows 2000–based computers that are located in Windows NT 3.x domains or Windows NT 4.0 domains.

This guide recommends that you configure the **Network Access: Allow anonymous SID/NAME translation** setting to **Disabled** for the three environments that are defined in the guide.

Network Security: Force Logoff when Logon Hours expire

This policy setting determines whether to disconnect users who are connected to a local computer outside their user account's valid logon hours. This setting affects the SMB component.

If you enable the **Network Security: Force Logoff when Logon Hours expire** setting, client sessions with the SMB server will be forcibly disconnected when the user's logon hours expire. The user will be unable to log on to the computer until their next scheduled access time. If you disable this policy setting, users will be able to maintain an established client session after their logon hours expire. To affect domain accounts, this setting must be defined in the Default Domain Policy.

This guide recommends that you configure the **Network Security: Force Logoff when Logon Hours expire** setting to **Enabled** for the three environments that are defined in the guide.

Summary

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

More Information

The following links provide additional information about topics that relate to domain policy for servers that run Windows Server 2003 with SP1.

- For information about the ability of anonymous users to request security identifier attributes for other users, see the Network access: Allow anonymous SID/name translation page at http://technet2.microsoft.com/WindowsServer/en/Library/299803be-0e85-4c60-b0b5-1b64486559b31033.mspx.
- For information about network security and how to force logoff when logon hours expire, see "The Mole #32: Technical Answers from Inside Microsoft - Moving Users, Sharing Printers, Two PDCs, Logoff, BackTalk" at www.microsoft.com/technet/archive/community/columns/inside/techan32.mspx.
- Also, see the Microsoft Knowledge Base article "Guest Account Cannot be Used When Anonymous Access Is Disabled" at http://support.microsoft.com/?kbid=251171.

Chapter 4: The Member Server Baseline Policy

Overview

This chapter documents the configuration requirements to manage a baseline security template for all servers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1). The chapter also provides administrative guidance for the setup and configuration of a secure Windows Server 2003 with SP1 configuration in three 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 with SP1. The default security configurations within Windows Server 2003 with SP1 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: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159. 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 three environments:

- **Legacy Client (LC)**. This environment includes computers that run Windows NT® 4.0 and Microsoft Windows® 98, which are sometimes referred to as *legacy* operating systems. Although this environment provides adequate security, it is the least secure of the three environments that are defined in this guide. To provide stronger security, organizations may choose to migrate to the more secure Enterprise Client environment. In addition to the referenced legacy operating systems, the LC environment includes Windows 2000 Professional and Windows XP Professional workstations. This environment only contains Windows 2000 or Windows Server 2003 domain controllers. There are no Windows NT 4.0 domain controllers in this environment, but Windows NT member servers may exist.
- **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. Most of the work that is required to migrate from the LC 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. All domain

controllers and member servers in this environment run Windows 2000 Server or Windows Server 2003.

- **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, and domain controllers that run Windows 2000 Server or Windows Server 2003. 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.

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 rights 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.

The following figure shows the three security environments and the clients that are supported in each.

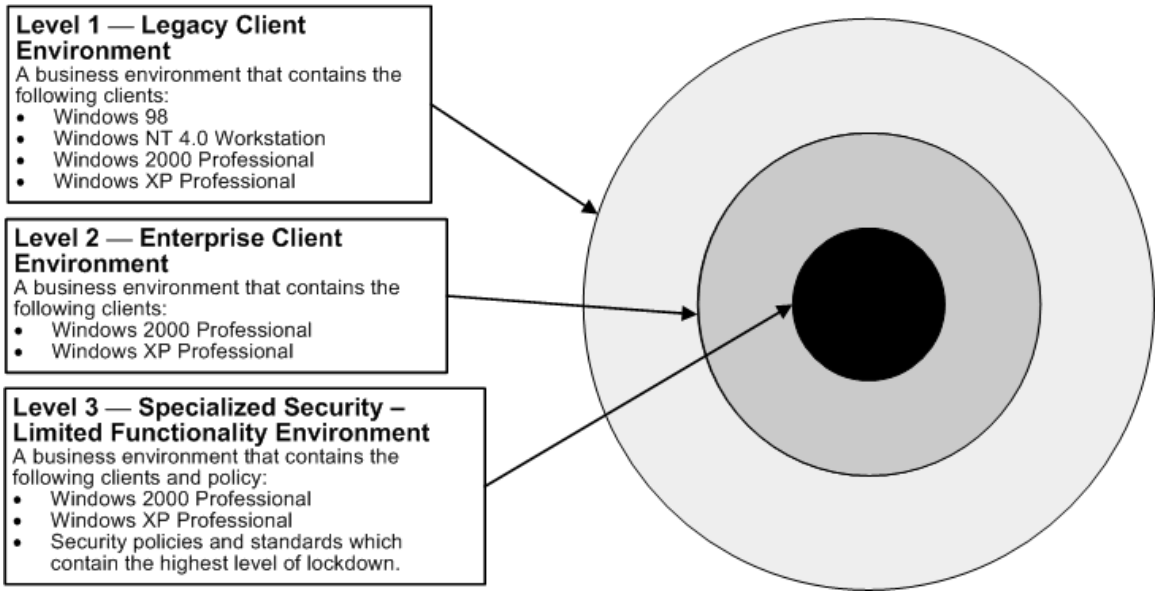

Figure 4.1 Existing and planned security environments

Organizations that want to secure their environments by means of a phased approach may choose to start at the Legacy 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 with SP1 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 all three

environments. For information about all default settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP at http://go.microsoft.com/fwlink/?LinkId=15159.

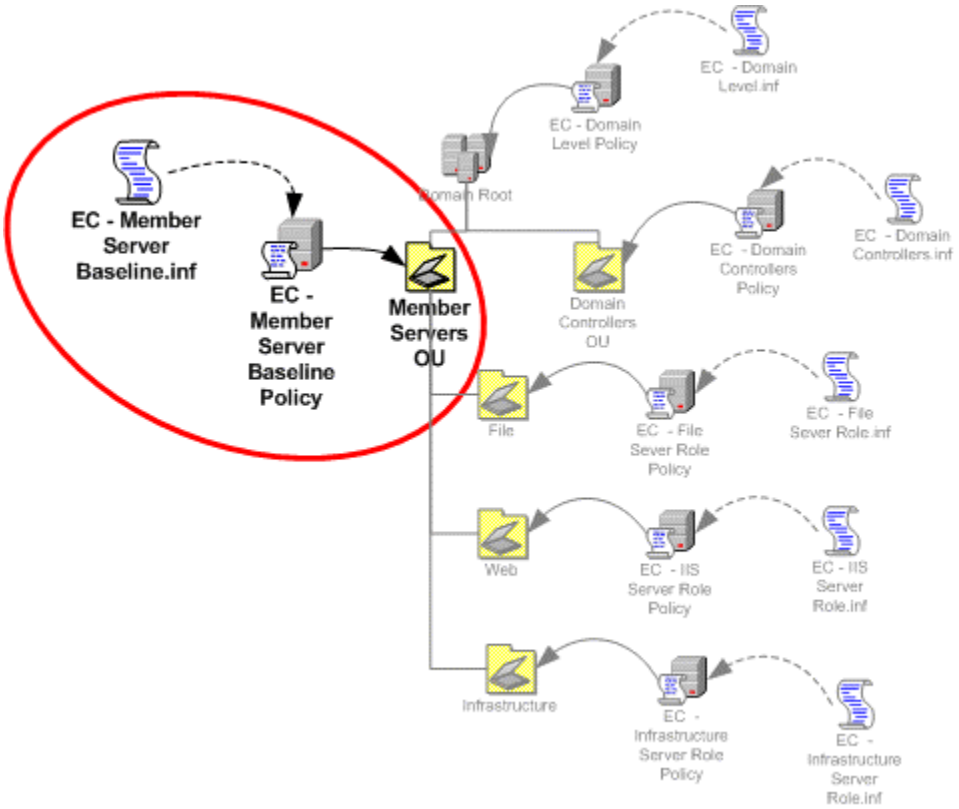

Figure 4.2 The EC-Member Server Baseline.inf security template is imported into the MSBP, which is then linked to the Member Servers organizational unit (OU)

Procedures to harden specific server roles are defined in the remaining chapters of this guide. The primary server roles that are discussed in this guide include:

- Domain controllers that include DNS services
- Infrastructure servers that include WINS and DHCP services
- File servers
- Print servers
- Web servers that run Internet Information Services (IIS)
- Microsoft Internet Authentication Server (IAS) servers
- Certificate Services (CA) servers
- Bastion hosts

Many of the following settings that appear in the Enterprise Client MSBP also apply to these server roles in the three environments that are defined in this guide. The security templates are uniquely designed to address the security needs of each particular environment. The following table shows the names of the baseline security templates for the three environments.

Table 4.1 Baseline Security Templates for All Three Environments

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-Member Server Baseline.inf	EC-Member Server Baseline.inf	SSLF-Member Server Baseline.inf

The security settings that are common to all three environments and therefore all **Member Server Baseline** security templates are described throughout the rest of this chapter.

The baseline security templates are also the basis for the domain controller security templates that are defined in Chapter 5, "The Domain Controller Baseline Policy." The **Domain Controllers Role** security templates include baseline settings for the Domain Controllers Group Policy GPO, which is linked to the Domain Controllers OU in all three environments. Step-by-step instructions for how to create the OUs and Group Policies and then import the appropriate security template into each GPO are provided in Chapter 2, "Windows Server 2003 Hardening Mechanisms."

Note: Some procedures that are used to harden servers cannot be automated by means of Group Policy. These procedures are described in the "Additional Security Settings" section of this chapter.

Windows Server 2003 Baseline Policy

Settings at the Member Server OU level define the common settings for all member server roles that are discussed in this guide. To apply these settings, you can create a GPO that is linked to the Member Server OU, which is known as a baseline policy. The GPO automates the configuration of specific security settings on each server. You will have to move the server accounts to the appropriate child OUs of the Member Server OU based on each server's role.

The following settings are described as they appear in the user interface (UI) of the Microsoft Management Console (MMC) Security Configuration Editor (SCE) snap-in.

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.

The following table includes the Audit policy setting recommendations for all three environments that are defined in this guide. You may notice that the settings for most values are similar for all three environments. Additional information about each setting is provided in the subsections that follow the table.

You can configure the Audit policy setting values in Windows Server 2003 with SP1 at the following location within the Group Policy Object Editor:

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

For a summary of the prescribed settings in this section, see the Microsoft Excel® workbook "Windows Server 2003 Security Guide Settings," which is included with the downloadable version of this guide. For more information about the default settings and a detailed explanation of each of the settings that are discussed in this section, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Table 4.2 Audit Policy Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Audit account logon events	Success	Success	Success Failure
Audit account management	Success	Success	Success Failure
Audit logon events	Success	Success	Success Failure
Audit object access	No Auditing	No Auditing	Failure
Audit policy change	Success	Success	Success
Audit privilege use	No Auditing	No Auditing	Failure
Audit process tracking	No Auditing	No Auditing	No Auditing
Audit system events	Success	Success	Success

Audit account logon events

This policy setting determines whether to audit each instance of a user who logs on to or off from another computer that validates the account. Authentication of a domain user account on a domain controller generates an account logon event that is logged in the domain controller's Security log. Authentication of a local user on a local computer generates a logon event that is logged in the local Security log. No account logoff events are logged.

The **Audit account logon events** setting is configured to log **Success** values for the LC and EC baseline policies, and to log both **Success** and **Failure** events for the SSLF baseline policy.

The following table includes the important security events that this policy setting logs in the Security log. These event IDs can be useful when you want to create custom alerts to monitor any software suite, such as Microsoft Operations Manager (MOM).

Table 4.3 Account Logon Events

Event ID	Event description
672	An authentication service (AS) ticket was successfully issued and validated. In Windows Server 2003 with SP1, the type of this event will be Success Audit for successful requests or Failure Audit for failed requests.
673	A ticket granting service (TGS) ticket was granted. A TGS is a ticket that is issued by the Kerberos version 5 TGS that allows a user to authenticate to a specific service in the domain. Windows Server 2003 with SP1 will log successes and failures for this event type.
674	A security principal renewed an AS ticket or a TGS ticket.
675	Pre-authentication failed. This event is generated on a Key Distribution Center (KDC) when a user enters an incorrect password.
676	Authentication ticket request failed. This event is not generated by Windows Server 2003 with SP1. Other Windows versions use this event to indicate an authentication failure that was not due to incorrect credentials.
677	A TGS ticket was not granted. This event is not generated by Windows Server 2003 with SP1, which uses a failure audit event with ID 672 for this case.
678	An account was successfully mapped to a domain account.
681	Logon failure. A domain account logon was attempted. This event is only generated by domain controllers.
682	A user has reconnected to a disconnected Terminal Server session.
683	A user disconnected a Terminal Server session but did not log off.

Audit account management

This policy setting determines whether to audit each account management event on a computer. Examples of account management events include:

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

Organizations need to be able to determine who creates, modifies, or deletes both domain and local accounts. Unauthorized changes could indicate mistaken changes made by an administrator who does not understand how to follow organizational policies, but could also indicate a deliberate attack.

For example, account management failure events often indicate attempts by a lower-level administrator—or an attacker who has compromised a lower-level administrator's account—to elevate their privileges. The logs can help you determine which accounts an attacker has modified and created.

The **Audit account management** setting is configured to log **Success** values for the LC and EC baseline policies, and to log both **Success** and **Failure** values for the SSLF baseline policy.

The following table includes the important security events that this policy setting records in the Security log. These event IDs can be useful when you want to create custom alerts to monitor any software suite, such as MOM. Most operational management software can be customized with scripts to capture or flag events that are based on these event IDs.

Table 4.4 Account Management Events

Event ID	Event description
624	A user account was created.
627	A user password was changed.
628	A user password was set.
630	A user account was deleted.
631	A global group was created.
632	A member was added to a global group.
633	A member was removed from a global group.
634	A global group was deleted.
635	A new local group was created.
636	A member was added to a local group.
637	A member was removed from a local group.
638	A local group was deleted.
639	A local group account was changed.
641	A global group account was changed.
642	A user account was changed.
643	A domain policy was modified.
644	A user account was automatically locked.

Event ID	Event description
645	A computer account was created.
646	A computer account was changed.
647	A computer account was deleted.
648	A local security group with security disabled was created. **Note**: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks.
649	A local security group with security disabled was changed.
650	A member was added to a security-disabled local security group.
651	A member was removed from a security-disabled local security group.
652	A security-disabled local group was deleted.
653	A security-disabled global group was created.
654	A security-disabled global group was changed.
655	A member was added to a security-disabled global group.
656	A member was removed from a security-disabled global group.
657	A security-disabled global group was deleted.
658	A security-enabled universal group was created.
659	A security-enabled universal group was changed.
660	A member was added to a security-enabled universal group.
661	A member was removed from a security-enabled universal group.
662	A security-enabled universal group was deleted.
663	A security-disabled universal group was created.
664	A security-disabled universal group was changed.
665	A member was added to a security-disabled universal group.
666	A member was removed from a security-disabled universal group.
667	A security-disabled universal group was deleted.
668	A group type was changed.
684	The security descriptor of administrative group members was set. **Note**: Every 60 minutes on a domain controller, a background thread searches all members of administrative groups (such as domain, enterprise, and schema administrators) and applies a fixed security descriptor on them. This event is logged.
685	Name of an account was changed.

Audit logon events

This policy setting determines whether to audit each instance of user logon and logoff from a computer. The **Audit logon events** setting generates records on domain controllers to monitor domain account activity and on local computers to monitor local account activity.

If you configure the **Audit logon events** setting to **No auditing**, it is difficult or impossible to determine which users have either logged on or attempted to log on to computers in the organization. If you enable the **Success** value for the **Audit logon events** setting on a domain member, an event will be generated each time that someone logs on to the network, regardless of where the accounts reside on the network. If the user logs on to a local account and the **Audit account logon events** setting is **Enabled**, the user logon will generate two events.

Even if you do not modify the default values for this policy setting, no audit record evidence will be available for analysis after a security incident takes place. The **Audit logon events** setting is configured to log **Success** values in the LC and EC baseline policies and to log both **Success** and **Failure** values for the SSLF policy.

The following table includes the important security events that this policy setting records in the Security log.

Table 4.5 Audit Logon Events

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

Event ID	Event description
545	Main mode authentication failed because of a Kerberos authentication protocol failure or a password that is not valid.
546	IKE security association establishment failed because the peer sent a proposal that is not valid. A packet was received that contained data that is not valid.
547	A failure occurred during an IKE handshake.
548	Logon failure. The security identifier (SID) from a trusted domain does not match the account domain SID of the client.
549	Logon failure. All SIDs corresponding to untrusted namespaces were filtered out during an authentication across forests.
550	Notification message that could indicate a possible denial-of-service (DoS) attack.
551	A user initiated the logoff process.
552	A user successfully logged on to a computer with explicit credentials while already logged on as a different user.
682	A user has reconnected to a disconnected terminal server session.
683	A user disconnected a terminal server session but did not log off. **Note**: This event is generated when a user is connected to a terminal server session over the network. It appears on the terminal server.

Audit object access

By itself, this policy setting will not cause any events to be audited. The **Audit object access** setting determines whether to audit the event when a user accesses an object—for example, a file, folder, registry key, or printer—that has a specified system access control list (SACL).

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

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

If you configure the **Audit object access** setting to log **Success** values, an audit entry will be generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to log **Failure** values, an audit entry will be generated each time that a user unsuccessfully attempts to access an object with a specified SACL.

Organizations should define only the actions they want enabled when SACLs are configured. For example, you might want to enable the **Write and Append Data** audit setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.

The **Audit object access** setting is configured to the default value of **No auditing** in the baseline policy for the LC and EC environments. However, this policy setting is configured to log **Failure** values in the baseline policy for the SSLF environment.

The following table includes the important security events that this policy setting records in the Security log.

Table 4.6 Object Access Events

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

Event ID	Event description
785	Certificate Services stopped.
786	The security permissions for Certificate Services changed.
787	Certificate Services retrieved an archived key.
788	Certificate Services imported a certificate into its database.
789	The audit filter for Certificate Services changed.
790	Certificate Services received a certificate request.
791	Certificate Services approved a certificate request and issued a certificate.
792	Certificate Services denied a certificate request.
793	Certificate Services set the status of a certificate request to pending.
794	The certificate manager settings for Certificate Services changed.
795	A configuration entry changed in Certificate Services.
796	A property of Certificate Services changed.
797	Certificate Services archived a key.
798	Certificate Services imported and archived a key.
799	Certificate Services published the certification authority (CA) certificate to Active Directory.
800	One or more rows have been deleted from the certificate database.
801	Role separation enabled.

Audit policy change

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

If you configure the **Audit policy change** setting to log **Success** values, an audit entry will be generated for each successful change to user rights assignment policies, trust policies, or Audit policies. If you configure this policy setting to log **Failure** values, an audit entry will be generated for each failed change to user rights assignment policies, trust policies, or Audit policies.

The recommended settings would allow you to you see any account privileges that an attacker attempts to elevate—for example, if they tried to add the **Debug programs** privilege or the **Back up files and directories** privilege.

The **Audit policy change** setting is configured to log **Success** values in the baseline policy for all three environments that are defined in this guide. Currently, the **Failure** setting value does not capture meaningful events.

The following table includes the important security events that this policy setting records in the Security log.

Table 4.7 Audit Policy Change Events

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

Audit privilege use

This policy setting determines whether to audit each exercise of a user right. If you configure the **Audit privilege use** setting to log **Success** values, an audit entry will be generated each time that a user right is exercised successfully. If you configure this policy setting to log **Failure** values, an audit entry will be generated each time that a user right is exercised unsuccessfully.

Audits are not generated when the following user rights are exercised, even if you configure the **Audit privilege use** setting, because these user rights generate many events in the Security log. Performance of your computers would likely be affected if these user rights were audited:

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

Note: If you wish to audit these user rights, you must enable the **Audit: Audit the use of Backup and Restore privilege** security option in Group Policy.

The **Audit privilege use** setting is left at the default value of **No auditing** in the baseline policy for the LC and EC environments. However, this policy setting is configured to log **Failure** values in the baseline policy for the SSLF environment. Failed use of a user right is an indicator of a general network problem, and can often indicate an attempted security breach. Organizations should configure the **Audit privilege use** setting to **Enable** only if there is a specific business reason to do so.

The following table includes the important security events that this setting records in the Security log.

Table 4.8 Privilege Use Events

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

Audit process tracking

This policy setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. If you configure this policy setting to log **Success** values, an audit entry is generated each time that the process that is being tracked succeeds. If you configure this policy setting to log **Failure** values, an audit entry is generated each time that the process that is being tracked fails.

The **Audit process tracking** setting will generate a large number of events, so it is typically configured to **No auditing**, as it is in the baseline policy for all three

environments that are defined in this guide. However, this policy setting can be very helpful during an incident response because it provides a detailed log of the processes that are started and the time when each one was launched.

The following table includes the important security events that this setting records in the Security log.

Table 4.9 Process Tracking Events

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

Audit system events

This policy setting determines whether to audit when a user restarts or shuts down a computer or when an event occurs that affects either the computer's security or the Security log. If you configure this policy setting to log **Success** values, an audit entry is generated when a system event is executed successfully. If you configure this policy setting to log **Failure** events, an audit entry is generated when a system event is attempted unsuccessfully.

The following table includes the most useful successful events for this setting.

Table 4.10 System Event Messages for Audit System Events

Event ID	Event description
512	Windows is starting up.
513	Windows is shutting down.
514	An authentication package was loaded by the Local Security Authority.
515	A trusted logon process has registered with the Local Security Authority.
516	Internal resources that were allocated to queue of security event messages have been exhausted, and the loss of some security event messages has occurred.

Event ID	Event description
517	The audit log was cleared.
518	A notification package was loaded by the Security Accounts Manager.
519	A process is using an invalid local procedure call (LPC) port in an attempt to impersonate a client and reply or read from or write to a client address space.
520	The system time was changed. **Note**: This audit typically appears twice.

User Rights Assignments

User rights 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 will override them the next time that the Group Policies are refreshed or reapplied.

You can configure the user rights assignment settings in Windows Server 2003 with SP1 at the following location within the Group Policy Object Editor:

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

The default user rights assignments are different for the various types of servers in your organization. For example, Windows Server 2003 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 with SP1 or Windows XP.
  - **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 rights 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.

This section provides details about the prescribed MSBP user rights assignment settings for all three environments that are defined in this guide. For a summary of the prescribed settings in this section, see the Microsoft Excel workbook "Windows Server 2003 Security Guide Settings," which is included with the downloadable version of this guide. For information about the default settings and a detailed explanation of each of the settings that are discussed in this section, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*.

The following table includes the user rights assignments setting recommendations for all three environments that are defined in this guide. Additional information about each setting is provided in the subsections that follow the table.

Table 4.11 User Rights Assignments Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Access this computer from the network	Not defined	Not defined	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
Act as part of the operating system	Not defined	Not defined	No one
Adjust memory quotas for a process	Not defined	Not defined	Administrators, NETWORK SERVICE, LOCAL SERVICE
Allow log on locally	Administrators, Backup Operators, Power Users	Administrators, Backup Operators, Power Users	Administrators
Allow log on through Terminal Services	Administrators and Remote Desktop Users	Administrators and Remote Desktop Users	Administrators
Back up files and directories	Not defined	Not defined	Administrators
Bypass traverse checking	Not defined	Not defined	Authenticated Users
Change the system time	Not defined	Not defined	Administrators, LOCAL SERVICE
Create a pagefile	Not defined	Not defined	Administrators
Create a token object	Not defined	Not defined	No one
Create global objects	Not defined	Not defined	Administrators, SERVICE

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Create permanent shared objects	Not defined	Not defined	No one
Debug programs	Not defined	Administrators	No one
Deny access to this computer from the network	ANONOYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts	ANONOYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts	ANONOYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts
Deny logon as a batch job	Guests; Support_388945a0	Guests; Support_388945a0	Guests; Support_388945a0;
Deny logon as a service	Not defined	Not defined	No one
Deny logon locally	Not defined	Not defined	Guests; Support_388945a0;
Deny logon through Terminal Services	Guests	Guests	Guests
Enable computer and user accounts to be trusted for delegation	Not defined	Not defined	Administrators
Force shutdown from a remote system	Not defined	Not defined	Administrators
Generate security audits	Not defined	Not defined	NETWORK SERVICE, LOCAL SERVICE
Impersonate a client after authentication	Not defined	Not defined	Administrators, SERVICE
Increase scheduling priority	Not defined	Not defined	Administrators
Load and unload device drivers	Not defined	Not defined	Administrators
Lock pages in memory	Not defined	Not defined	No one
Log on as a batch job	Not defined	Not defined	Not defined
Log on as a service	Not defined	Not defined	NETWORK SERVICE
Manage auditing and security log	Not defined	Not defined	Administrators
Modify firmware environment values	Not defined	Not defined	Administrators
Perform volume maintenance tasks	Not defined	Not defined	Administrators

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Profile single process	Not defined	Not defined	Administrators
Profile system performance	Not defined	Not defined	Administrators
Remove computer from docking station	Not defined	Not defined	Administrators
Replace a process level token	Not defined	Not defined	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Not defined	Not defined	Administrators
Shut down the system	Not defined	Not defined	Administrators
Synchronize directory service data	Not defined	Not defined	No one
Take ownership of files or other objects	Not defined	Not defined	Administrators

Access this computer from the network

This policy setting determines which users and groups are allowed to connect to the computer over the network. It is required by a number of network protocols, including server message block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), HTTP, and Component Object Model Plus (COM+).

The **Access this computer from the network** setting is configured to **Not defined** for the LC and EC environments. However, although permissions that are assigned to the **Everyone** security group in Windows Server 2003 with SP1 no longer provide access to anonymous users, guest groups and accounts can still be assigned access through the **Everyone** security group. For this reason, the **Everyone** security group is denied the **Access this computer from the network** user right in the SSLF environment, which helps guard against attacks that target guest access to the domain. Only the **Administrators**, **Authenticated Users**, and **ENTERPRISE DOMAIN CONTROLLERS** groups are assigned this user right in the SSLF environment.

Act as part of the operating system

This policy setting determines whether a process can assume the identity of any user and thereby gain access to the resources that the user is authorized to access. Typically, only low-level authentication services require this user right.

The **Act as part of the operating system** user right is configured to **Not defined** for the LC and EC environments. However, for the SSLF environment this policy setting is configured to a null value or blank, which denies this user right to all security groups and accounts.

Adjust memory quotas for a process

This policy setting determines whether users can adjust the maximum amount of memory that is available to a process. It is useful for computer tuning purposes, but it can be abused. An attacker could exploit this user right to launch a DoS attack.

The **Adjust memory quotas for a process** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to the **Administrators** group, NETWORK SERVICE, and LOCAL SERVICE for the SSLF environment.

Allow log on locally

This policy setting determines which users can log on interactively to the specified computer. Logons that are initiated with the CTRL+ALT+DEL key combination on the keyboard require the user to have this user right. Any account with this user right could be used to log on to the computer's local console.

The **Allow log on locally** user right is restricted to the **Administrators**, **Backup Operators**, and **Power Users** groups for the LC and EC environments, which helps prevent logon by unauthorized users who may want to elevate their privileges or introduce viruses into the environment. This user right is assigned to only the **Administrators** group for the SSLF environment.

Allow log on through Terminal Services

This policy setting determines which users or groups have permission to log on as a Terminal Services client.

For the LC and EC environments, the **Allow log on through Terminal Services** user right is restricted to the **Administrators** and **Remote Desktop Users** groups. For the SSLF environment, only members of the **Administrators** group are assigned this user right.

Back up files and directories

This policy setting determines whether users can circumvent file and directory permissions to back up the computer. It is used only when an application attempts access through the NTFS backup application programming interface (API) with a backup utility such as NTBACKUP.EXE. Otherwise, normal file and directory permissions apply.

The **Back up files and directories** setting is configured to **Not defined** for the LC and EC environments. This user right is assigned to only the **Administrators** group for the SSLF environment.

Bypass traverse checking

This policy setting determines whether users can pass through folders without being checked for the special "Traverse Folder" access permission when they navigate an object path in the NTFS file system or in the registry. The user right does not allow the user to list the contents of a folder; it only allows the user to traverse its directories.

The **Bypass traverse checking** setting is configured to **Not defined** for the LC and EC environments. This user right is assigned to only the **Authenticated Users** group for the SSLF environment.

Change the system time

This policy setting determines which users can change the time and date on the internal clock of the computer. Users who are assigned this user right can affect the appearance of event logs, which are time stamped by the computer's internal clock. If the computer's time is changed, the logs will not reflect the actual time that events occurred.

The **Change the system time** setting is configured to **Not defined** for the LC and EC environments. This user right is assigned to only the **Administrators** group and the **Local Service** account for the SSLF environment.

Note: Discrepancies between the time on the local computer and on the domain controllers may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or to obtain authorization to access domain resources after they log on.

Create a pagefile

This policy setting determines whether users can create and change the size of pagefiles. To perform this task, the user specifies a page file size for a particular drive in the **Performance Options** box that is located on the **Advanced** tab of the **System Properties** dialog box.

The **Create a pagefile** setting is configured to **Not defined** for the LC and EC environments, This user right is assigned to only the **Administrators** group for the SSLF environment.

Create a token object

This policy setting determines whether a process can create a token, which the process can then use to gain access to any local resources when it uses NtCreateToken() or other token-creation APIs.

The **Create a token object** setting is configured to **Not defined** for the LC and EC environments. However, for the SSLF environment this policy setting is configured to a null value or blank, which means no security group or account will have this user right.

Create global objects

This policy setting allows users to create global objects that are available to all sessions. Users can still create objects that are specific to their own session without being assigned this user right.

The **Create global objects** setting is configured to **Not defined** for the LC and EC environments. For the SSLF environment, this user right is only assigned to the **SERVICE** and **Administrators** groups.

Create permanent shared objects

This policy setting determines whether users can create directory objects in the object manager, which means that they can create shared folders, printers, and other objects. It is useful to kernel-mode components that extend the object namespace, and such components have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right to users.

The **Create permanent shared objects** setting is configured to **Not defined** for the LC and EC environments. However, for the SSLF environment this policy setting is

configured to a null value or blank, which means no security group or account will have this user right.

Debug programs

This policy setting determines which users can attach a debugger to any process or to the kernel. It provides complete access to sensitive and critical operating system components. Programs should not be debugged in production environments except in extreme circumstances, such as when there is a need to troubleshoot a business-critical application that cannot be effectively assessed in the test environment.

The **Debug programs** setting is configured to **Not defined** for the LC environment. For the EC environment, this user right is assigned only to the **Administrators** group. However, for the SSLF environment this policy setting is configured to a null value or blank, which means no security group or account will have this user right.

Note: On Windows Server 2003 with SP1, removal of the **Debug programs** user right may result in an inability to use the Windows Update service. However, patches can still be manually downloaded and installed or applied through other means. Removal of this user right may also interfere with the Cluster Service. For more information, see the Microsoft Knowledge Base article "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/?kbid=891597.

Deny access to this computer from the network

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

This policy setting determines which users will not be able to access a computer over the network. It denies a number of network protocols, including SMB-based protocols, NetBIOS, CIFS, HTTP, and COM+. This policy setting supersedes the **Access this computer from the network** user right when a user account is subject to both settings.

For all three environments that are defined in this guide, the **Deny access to this computer from the network** user right is assigned to the **Guests** group, ANONOYMOUS LOGON, Support_388945a0, and all service accounts that are not part of the operating system.

Configuration of this policy setting for other groups could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

Deny log on as a batch job

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

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right.

The **Deny log on as a batch job** user right overrides the **Log on as a batch job** user right, which could be used to allow accounts to schedule jobs that consume excessive

system resources. Such an occurrence could cause a DoS condition. For this reason, the **Deny log on as a batch job** user right is assigned to the **Guests** group and the Support_388945a0 user account in the baseline policy for all three environments that are defined in this guide. Failure to assign this user right to the recommended accounts can be a security risk.

Deny logon as a service

This policy setting determines whether services can be launched in the context of the specified account.

The **Deny logon as a service** setting is configured to **Not defined** for the LC and EC environments. However, for the SSLF environment this policy setting is configured to a null value or blank, which means no security group or account will have this user right.

Deny logon locally

This policy setting determines whether users can log on directly at the computer's keyboard.

The **Deny logon locally** setting is configured to **Not defined** for the EC and LC environments. However, this user right is assigned only to the **Guests** group and the Support_388945a0 user account for the SSLF environment. Failure to assign this user right to the recommended accounts can be a security risk.

Deny log on through Terminal Services

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

This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing.

For all three environments that are defined in this guide, the **Guests** group is assigned the **Deny log on through Terminal Services** user right so that they cannot log on through Terminal Services.

Enable computer and user accounts to be trusted for delegation

This policy setting determines whether users can change the **Trusted for Delegation** setting on a user or computer object in Active Directory. Users or computers that are assigned this user right must also have write access to the account control flags on the object. Misuse of this user right could cause unauthorized impersonation of other users on the network.

The **Enable computer and user accounts to be trusted for delegation** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to the **Administrators** group for the SSLF environment.

Force shutdown from a remote system

This policy setting determines whether users can shut down computers from remote locations on the network. Any user who can shut down a computer could cause a DoS condition. Therefore, this user right should be tightly restricted.

The **Force shutdown from a remote system** setting is configured to **Not defined** for the LC and EC environments. This user right is assigned only to the **Administrators** group for the SSLF environment.

Generate security audits

This policy setting determines whether a process can generate audit records in the Security log. Because the Security log can be used to trace unauthorized access, accounts that can write to the Security log could be used by an attacker to fill that log with meaningless events. If you configure the computer to overwrite events as needed, an attacker could use this capability to remove evidence of their unauthorized activities. If you configure the computer to shut down when it is unable to write to the Security log, an attacker could use this capability to create a DoS condition.

The **Generate security audits** setting is configured to **Not defined** for the LC and EC environments. This user right is assigned only to the NETWORK SERVICE and LOCAL SERVICE accounts for the SSLF environment.

Impersonate a client after authentication

This policy setting determines whether applications that run on behalf of an authenticated user can impersonate clients. If this user right is required for this type of impersonation, unauthorized users will not be able to convince a client to connect—for example, by remote procedure call (RPC) or named pipes—to a service that they created to impersonate that client. The unauthorized user could use this capability to elevate their permissions to administrative or system levels.

The **Impersonate a client after authentication** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to the **Administrators** group and SERVICE for the SSLF environment.

Increase scheduling priority

This policy setting determines whether users can increase the base priority class of a process. Increasing relative priority within a priority class is not a privileged operation. This user right is not required by administrative tools that are supplied with the operating system, but it might be required by software development tools. A user who is assigned this user right can increase the scheduling priority of a process to Real-Time and leave little processing time for all other processes, which could cause a DoS condition.

The **Increase scheduling priority** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to the **Administrators** group for the SSLF environment.

Load and unload device drivers

This policy setting determines which users can dynamically load and unload device drivers. This user right is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer. Device drivers run as highly privileged code. A user who is assigned the **Load and unload device drivers** user right can install

malicious code that masquerades as a device driver (unintentionally or otherwise). (Administrators should exercise greater care and install only drivers with verified digital signatures.)

The **Load and unload device drivers** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to only the **Administrators** group for the SSLF environment.

Lock pages in memory

This policy setting determines whether a process can keep data in physical memory, which prevents the computer from paging the data to virtual memory on disk. Such an occurrence could significantly degrade performance. Users who are assigned this user right can assign physical memory to several processes and leave little or no random access memory (RAM) for other processes, which could lead to a DoS condition.

The **Lock pages in memory** setting is configured to **Not defined** for the LC and EC environments. However, for the SSLF environment this policy setting is configured to a null value or blank, which means no security group or account will have this user right.

Log on as a service

This policy setting determines whether a security principal can log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have built-in rights to log on as a service. Any service that runs under a separate user account must be assigned this user right.

The **Log on as a service** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to the Network Service account for the SSLF environment.

Manage auditing and security log

This policy setting determines whether users can specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. This user right is powerful and should be closely guarded. Anyone with this user right can clear the Security log and possibly erase important evidence of unauthorized activity.

The **Manage auditing and security log** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to **Administrators** in the SSLF environment.

Important: Microsoft Exchange Server 2003 modifies this user right in the Default Domain Controller Policy during the installation process. For details, see Exchange Server 2003 Deployment online at www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3ADPerm/110e37bf-a68c-47bb-b4d5-1cfd539d9cba.mspx. If this user right is restricted to the Administrator's group, Exchange will frequently record error messages to the Application event log. If you use Exchange Server 2003 you will need to adjust the value of this setting for the domain controllers. As with all of the settings that are recommended in this guide, you may need to make some adjustments to allow your organization's applications to function normally.

Modify firmware environment values

This policy setting determines whether the computer's environment variables can be modified, either by a process through an API or by a user through **System Properties**. Anyone who is assigned this user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

The **Modify firmware environment values** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to only the **Administrators** group for the SSLF environment.

Perform volume maintenance tasks

This policy setting determines whether a non-administrative or remote user can manage volumes or disks. A user who is assigned this user right could delete a volume and cause the loss of data or a DoS condition.

The **Perform volume maintenance tasks** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned only to the **Administrators** group for the SSLF environment.

Profile single process

This policy setting determines which users can use performance monitoring tools to monitor the performance of non-system processes. This user right presents a moderate vulnerability, in that an attacker with this capability could monitor a computer's performance to help identify critical processes that they might want to attack directly. An attacker could also determine what processes run on the computer so that they could identify countermeasures to avoid, such as antivirus software, an intrusion detection system, or other users logged onto a computer.

The **Profile single process** setting is configured to **Not defined** for the LC and EC environments. For greater security, ensure that the **Power Users** group is not assigned this user right in the SSLF environment; only members of the **Administrators** group should have this capability in such an environment.

Profile system performance

This policy setting is similar to the previous setting. It determines whether users can monitor the performance of system processes. This user right presents a moderate vulnerability, in that an attacker with this privilege could monitor a computer's performance to help identify critical processes that they might want to attack directly. An attacker could also determine what processes run on the computer to identify countermeasures to avoid, such as antivirus software or an intrusion detection system.

The **Profile system performance** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to only the **Administrators** group for the SSLF environment.

Remove computer from docking station

This policy setting determines whether users of portable computers can click **Eject PC** on the **Start** menu to undock the computers. Anyone who is assigned this user right can remove a portable computer from its docking station.

The **Remove computer from docking station** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to only the **Administrators** group for the SSLF environment.

Replace a process level token

This policy setting determines whether a parent process can replace the access token that is associated with a child process.

The **Replace a process level token** setting is configured to **Not defined** for the LC and EC environments. However, this user right is assigned to only the LOCAL SERVICE and NETWORK SERVICE accounts for the SSLF environment.

Restore files and directories

This policy setting determines which users can bypass file, directory, registry, and other persistent objects permissions when they restore backed up files and directories. It also determines which users can set any valid security principal as the owner of an object.

The **Restore files and directories** setting is configured to **Not defined** for the LC and EC environments. However, only the **Administrators** group is assigned this user right for the SSLF environment. File restoration tasks are usually performed by administrators or members of another specifically delegated security group, especially for highly sensitive servers and domain controllers.

Shut down the system

This policy setting determines which locally logged on users can shut down the operating system with the **Shut Down** command. Because misuse of this capability could cause a DoS condition, the ability to shut down domain controllers should be limited to a very small number of trusted administrators. Even though a system shutdown requires the ability to log on to the server, you should be very careful about the accounts and groups that you allow to shut down a domain controller.

The **Shut down the system** setting is configured to **Not defined** for the LC and EC environments. However, only the **Administrators** group is assigned this user right for the SSLF environment.

Synchronize directory service data

This policy setting determines whether a process can read all objects and properties in the directory, regardless of the protection on the objects and properties. This user right is required to use LDAP directory synchronization (Dirsync) services.

The default configuration of the **Synchronize directory service data** setting is **Not defined**, which is sufficient for the LC and EC environments. However, for the SSLF environment this policy setting is configured to a null value or blank, which means no security group or account will have this user right.

Take ownership of files or other objects

This policy setting determines whether users can take ownership of any securable object in the network, including Active Directory objects, NTFS file system (NTFS) files, and folders, printers, registry keys, services, processes, and threads.

The **Take ownership of files or other objects** setting is configured to **Not defined** for the LC and EC environments. However, you should assign this user right only to the local **Administrators** group for the SSLF environment.

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 with SP1 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 [0]exist on all types of computers. Therefore, the settings that comprise the Security Options portion of Group Policy that are defined in this section [0]may need to be manually modified on computers in which these settings are present to make them fully operable.

The following sections provide information about the prescribed MSBP security options settings for all three environments that are defined in this guide. For a summary of the prescribed settings, see the Microsoft Excel workbook "Windows Server 2003 Security Guide Settings," which is included with the downloadable version of this guide. For information about the default configuration and a detailed explanation of each of the settings, see the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*.

The tables in each of the following sections summarize the recommended settings for the different types of security option settings. Detailed information about the settings is provided in the subsections that follow each table.

Accounts Settings

Table 4.12 Security Options: Accounts Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Administrator account status	Not defined	Not defined	Enabled
Guest account status	Disabled	Disabled	Disabled
Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled

Accounts: Administrator account status

This policy setting enables or disables the Administrator account during normal operation. When you start a computer in safe mode, the Administrator account is always enabled, regardless of this setting.

The **Accounts: Administrator account status** setting is configured to **Not defined** for the LC and EC environments and to **Enabled** for the SSLF environment.

Accounts: Guest account status

This policy setting determines whether the Guest account is enabled or disabled. This account allows unauthenticated network users to log on as Guest and gain access to the computer.

The **Accounts: Guest account status** setting is configured to **Disabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If this policy setting is enabled, local accounts with nonblank passwords will not be able to log on to the network from a remote client, and local accounts that are not password protected will only be able to log on while physically located at the keyboard of the computer.

The **Accounts: Limit local account use of blank passwords to console logon only** setting is configured to the default value of **Enabled** in the baseline policy for all three of the environments that are defined in this guide.

Audit Settings

Table 4.13 Security Options: Audit Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Audit the access of global system objects	Disabled	Disabled	Disabled
Audit the use of Backup and Restore privilege	Disabled	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Disabled	Enabled

Audit: Audit the access of global system objects

This policy setting audits the access of global system objects when it is in effect. If both the **Audit: Audit the access of global system objects** and the **Audit object access audit policy** settings are enabled, a large number of audit events will be generated.

The **Audit: Audit the access of global system objects** setting is configured to the default value of **Disabled** in the baseline policy for all three environments that are defined in this guide.

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

Audit: Audit the use of Backup and Restore privilege

This policy setting determines whether to audit the use of all user privileges, including Backup and Restore, when the **Audit privilege use** policy setting is in effect. If you enable this policy setting, a large number of security events could be generated, which would cause servers to respond slowly and the Security log to record numerous events of little significance.

Therefore, the **Audit: Audit the use of Backup and Restore privilege** setting is configured to the default value of **Disabled** in the baseline policy for all three environments that are defined in this guide.

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

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

This policy setting determines whether the computer shuts down immediately if it is unable to log security events.

The amount of administrative overhead that was required to enable the **Audit: Shut down system immediately if unable to log security audits** setting in the LC and EC environments was determined to be too great. Therefore, this policy setting is configured to **Disabled** in the baseline policy for those environments. However, this policy setting is configured to **Enabled** in the baseline policy for the SSLF environment because the additional administrative overhead was deemed acceptable to prevent the deletion of events from the Security log unless an administrator specifically chooses to do so.

Devices Settings

Table 4.14 Security Options: Devices Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Allow undock without having to log on	Disabled	Disabled	Disabled
Allowed to format and eject removable media	Administrators	Administrators	Administrators
Prevent users from installing printer drivers	Enabled	Enabled	Enabled
Restrict CD-ROM access to locally logged-on user only	Not defined	Not defined	Disabled
Restrict floppy access to locally logged-on user only	Not defined	Not defined	Disabled
Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation	Warn but allow installation

Devices: Allow undock without having to log on

This policy setting determines whether a portable computer can be undocked without the user having to log on to the computer. You can enable this policy setting to eliminate a logon requirement and allow use of an external hardware eject button to undock the computer. If you disable this policy setting, a user who is not logged on must be assigned the **Remove computer from docking station** user right.

The **Devices: Allow undock without having to log on** setting is configured to **Disabled** in the baseline policy for all three environments that are defined in this guide.

Devices: Allowed to format and eject removable media

This policy setting determines who can format and eject removable media. Only administrators should be able to eject removable media on servers.

Therefore, the recommended value for the **Devices: Allowed to format and eject removable media** setting is the default value of **Administrators** in the baseline policy for all three environments that are defined in this guide.

Devices: Prevent users from installing printer drivers

For a computer to print to a network printer, it must have the driver for that network printer installed. If you enable the **Devices: Prevent users from installing printer drivers** setting, only those in the **Administrators** or **Power Users** groups or those with Server Operator privileges are allowed to install a printer driver to add a network printer. If you disable this policy setting, any user can install a printer driver.

The **Devices: Prevent users from installing printer drivers** setting is configured to the default value of **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether a CD-ROM is accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable CD-ROM media. When this policy setting is enabled and no one is logged on interactively, the CD-ROM is accessible over the network.

The **Devices: Restrict CD-ROM access to locally logged-on user only** setting is configured to **Not defined** in the baseline policy for the LC and EC environments. In the baseline policy for the SSLF environment, this policy setting is configured to **Disabled**.

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

This policy setting determines whether removable floppy media are accessible to both local and remote users simultaneously. If you enable this policy setting, only the interactively logged-on user is allowed to access removable floppy media. If this policy setting is enabled and no one is logged on interactively, the floppy media is accessible over the network.

The **Devices: Restrict floppy access to locally logged-on user only** setting is configured to **Not defined** in the baseline policy for the LC and EC environments. In the baseline policy for the SSLF environment, this policy setting is configured to **Disabled**.

Devices: Unsigned driver installation behavior

This policy setting determines what happens when an attempt is made to install a device driver (by means of Setup API) that has not been approved and signed by the Windows Hardware Quality Lab (WHQL). Depending on how you configure it, this policy setting will prevent the installation of unsigned drivers or warn the administrator that an unsigned driver is about to be installed.

The **Devices: Unsigned driver installation behavior** setting can be used to prevent the installation of drivers that have not been certified to run on Windows Server 2003 with SP1. However, this policy setting is configured to **Warn but allow installation** in the baseline policy for all three environments that are defined in this guide. One potential problem with this configuration is that unattended installation scripts will fail when they attempt to install unsigned drivers.

Domain Member Settings

Table 4.15 Security Options: Domain Member Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Digitally encrypt or sign secure channel data (always)	Disabled	Enabled	Enabled
Digitally encrypt secure channel data (when possible)	Enabled	Enabled	Enabled
Digitally sign secure channel data (when possible)	Enabled	Enabled	Enabled
Disable machine account password changes	Disabled	Disabled	Disabled
Maximum machine account password age	30 days	30 days	30 days
Require strong (Windows 2000, Windows XP, or Windows Server 2003) session key	Enabled	Enabled	Enabled

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

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. If a computer is set to always encrypt or sign secure channel data, then it cannot establish a secure channel with a domain controller that cannot sign or encrypt all secure channel traffic.

The **Domain member: Digitally encrypt or sign secure channel data (always)** setting is configured to **Disabled** in the baseline policy for the LC environment and to **Enabled** for the EC and SSLF environments.

Note: To take advantage of this setting on member workstations and servers, all domain controllers that constitute the member's domain must run Windows NT 4.0 with Service Pack 6a or la more recent version of Windows. Also, this policy setting is not supported in Windows 98 Second Edition clients unless they have the Dsclient installed.

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

This policy setting determines whether a domain member may attempt to negotiate encryption for all secure channel traffic that it initiates. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will not be allowed to negotiate secure channel encryption.

Therefore, the **Domain member: Digitally encrypt secure channel data (when possible)** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether a domain member may attempt to negotiate a signature for all secure channel traffic that it initiates. Requirement of a signature protects the traffic from modification by anyone who might capture the data.

The **Domain member: Digitally sign secure channel data (when possible)** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

Domain member: Disable machine account password changes

This policy setting determines whether a domain member may periodically change its computer account password. If you enable this policy setting, the domain member will not be able to change its computer account password. If you disable this policy setting, the domain member will be able to change its computer account password as specified by the **Domain Member: Maximum machine account password age** setting, which is every 30 days by default.

Computers that are no longer able to automatically change their account passwords are at risk of attack by someone who has determined the password for the computer's domain account. Therefore, the **Domain member: Disable machine account password changes** setting is configured to **Disabled** in the baseline policy for all three environments that are defined in this guide.

Domain member: Maximum machine account password age

This policy setting determines the maximum allowable age for a computer account password. It also applies to computers that run Windows 2000, but is not available through the Security Configuration Manager tools on these computers. By default, the domain members automatically change their domain passwords every 30 days. If this interval is increased significantly, or if it is set to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack and guess the password of one or more computer accounts.

Therefore, the **Domain member: Maximum machine account password age** setting is configured to **30 days** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether 128-bit key strength is required for encrypted secure channel data. If you enable this policy setting, a secure channel will not be able to be established without 128-bit encryption. If you disable this policy setting, the domain member is required to negotiate key strength with the domain controller. Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems.

Therefore, because the three security environments described in this guide contain Windows 2000 domain controllers or later, the **Domain member: Require strong**

(Windows 2000 or later) session key setting is configured to **Enabled** in the baseline policy for all three environments.

Note: If you enable this policy setting you will not be able to join computers that run Windows 2000 to Windows NT 4.0 domains.

Interactive Logon Settings

Table 4.16 Security Options: Interactive Logon Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Display user information when the session is locked	Not defined	Not defined	User display name, domain and user names
Do not display last user name	Enabled	Enabled	Enabled
Do not require CTRL+ALT+DEL	Disabled	Disabled	Disabled
Message text for users attempting to log on	(Consult with the relevant people in your organization.)	(Consult with the relevant people in your organization.)	(Consult with the relevant people in your organization.)
Message title for users attempting to log on	(Consult with the relevant people in your organization.)	(Consult with the relevant people in your organization.)	(Consult with the relevant people in your organization.)
Number of previous logons to cache (in case domain controller is not available)	1	0	0
Prompt user to change password before expiration	14 days	14 days	14 days
Require Domain Controller authentication to unlock workstation	Enabled	Enabled	Enabled
Require smart card	Not defined	Not defined	Disabled
Smart card removal behavior	Not defined	Lock Workstation	Lock Workstation

Interactive logon: Display user information when the session is locked

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will display in each computer's respective Windows logon screen. If you enable this policy setting, intruders will not be able to collect account names visually from the screens of desktop or laptop computers in your organization.

The **Interactive logon: Display user information when the session is locked** setting is configured to **Not defined** for the LC and EC environments. It is configured to **User display name, domain and user names** in the baseline server policy for the SSLF environment.

Interactive logon: Do not display last user name

This policy setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. If you enable this policy setting, the last logged on user's name will not display in the **Log On to Windows** dialog box.

The **Interactive logon: Do not display last user name** setting is configured to **Enabled** in the baseline server policy for all three environments that are defined in this guide.

Interactive logon: Do not require CTRL+ALT+DEL

This policy setting determines whether a user must press CTRL+ALT+DEL before they can log on. If you disable this policy setting, all users will be required to press CTRL+ALT+DEL before they log on to Windows (unless they use a smart card for Windows logon).

The **Interactive logon: Do not require CTRL+ALT+DEL** setting is configured to **Disabled** in the baseline policy for all three environments that are defined in this guide to decrease the chance of an attacker being able to intercept user passwords by means of a Trojan horse program.

Interactive logon: Message text for users attempting to log on

This policy setting specifies a text message that displays to users when they log on. Typically, this text is used for legal reasons—for example, to warn users about the ramifications of unauthorized access, misuse of company information, or that their actions may be audited.

The **Interactive logon: Message text for users attempting to log on** security option setting is recommended. You should consult with the relevant people in your organization to determine what this text should say.

Note: Both the **Interactive logon: Message text for users attempting to log on** and the **Interactive logon: Message title for users attempting to log on** settings must be enabled for either one to work properly.

Interactive logon: Message title for users attempting to log on

This policy setting allows a title to be specified in the title bar of the interactive logon dialog box that displays when users log on to the computer. The reason for this policy setting is the same as that for the **Message text for user attempting to log on** setting.

Therefore, the **Interactive logon: Message title for users attempting to log on** setting is recommended. You should consult with the relevant people in your organization to determine what this text should say

Note: Both the **Interactive logon: Message text for users attempting to log on** and **Interactive logon: Message title for users attempting to log on** settings must be enabled for either one to work properly.

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

This policy setting determines whether a user can log on to a Windows domain with cached account information. Logon information for domain accounts can be cached locally so that if a domain controller cannot be contacted on subsequent logons, a user can still log on. This capability may allow users to log on after their account has been disabled or deleted, because the workstation does not contact the domain controller. This policy setting determines the number of unique users for whom logon information is cached locally. If you configure this setting to 0, the logon cache is disabled.

The **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting is configured to **0** in the baseline policy for the EC and SSLF environments. In the LC environment, the setting is configured to **1** to allow access for legitimate clients when they are unable to contact the domain controller.

Interactive logon: Prompt user to change password before expiration

This policy setting determines how many days in advance users are warned that their passwords are about to expire. The “Account Policies” section in Chapter 3 recommends that user passwords be configured to expire periodically. If users are not notified when their passwords are about to expire, they may not realize it until the passwords have already expired, which could cause confusion for local users who find it difficult to change their passwords. Unexpected expirations also make it impossible for remote users to log on through dial-up or virtual private networking (VPN) connections.

Therefore, the **Interactive logon: Prompt user to change password before expiration** setting is configured to the default setting of 14 days in the baseline policy for all three environments that are defined in this guide.

Interactive logon: Require Domain Controller authentication to unlock workstation

For domain accounts, this policy setting determines whether a domain controller must be contacted to unlock a computer. This policy setting addresses a potential vulnerability that is similar to one for the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting. A user could disconnect the network cable of the server, unlock the server with an old password, and unlock the server without authentication.

To prevent such an occurrence, the **Interactive logon: Require Domain Controller authentication to unlock workstation** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

Important: This policy setting applies to computers that run Windows 2000, Windows XP, and Windows Server 2003, but it is not available through the Security Configuration Manager tools on computers that run Windows 2000.

Interactive logon: Require smart card

This policy setting requires users to log on to a computer with a smart card. Security is enhanced when users are required to use long, complex passwords for authentication, especially if they are required to change their passwords regularly. This approach reduces the chance that an attacker will be able to guess a user’s password by means of a brute force attack. However, it is difficult to make users choose strong passwords, and even strong passwords are still vulnerable to brute-force attacks.

The use of smart cards instead of passwords for authentication dramatically increases security, because current technology makes it almost impossible for an attacker to impersonate another user. Smart cards that require personal identification numbers (PINs) provide two-factor authentication: the user must possess the smart card and know its PIN. An attacker who captures the authentication traffic between the user's computer and the domain controller will find it extremely difficult to decrypt the traffic. Even if they can decrypt the traffic, the next time the user logs onto the network a new session key will be generated to encrypt traffic between the user and the domain controller.

Microsoft encourages organizations to migrate to smart cards or other strong authentication technologies. However, you should only enable the **Interactive logon: Require smart card** setting if smart cards are already deployed. For this reason, this policy setting is configured to **Not defined** in the baseline policy for the LC and EC environments. This policy setting is configured to **Disabled** in the baseline policy for the SSLF environment.

Interactive logon: Smart card removal behavior

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. If you configure this setting to **Lock Workstation**, the workstation is locked when the smart card is removed, which allows users to leave the area and take their smart cards with them. If you configure this setting to **Force Logoff**, the user is automatically logged off when the smart card is removed.

The **Interactive logon: Smart card removal behavior** setting is configured to **Not defined** in the baseline policy for the LC environment and to **Lock Workstation** for the EC and SSLF environments.

Microsoft Network Client Settings

Table 4.17 Security Options: Microsoft Network Client Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Digitally sign communications (always)	Disabled	Enabled	Enabled
Digitally sign communications (if server agrees)	Enabled	Enabled	Enabled
Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled

Microsoft network client: Digitally sign communications (always)

This policy setting determines whether packet signing is required by the SMB client component. If you enable this setting, Microsoft network clients will not be able to communicate with a Microsoft network server unless that server agrees to perform SMB packet signing. In mixed environments with legacy clients you should set this option to **Disabled**, because these clients will not be able to authenticate or gain access to domain controllers. However, you can use this setting in environments that run Windows 2000, Windows XP, and Windows Server 2003. The EC and SSLF environments that are defined in this guide only contain computers that run these operating systems, all of which support digital signatures.

Therefore, to increase communications security between computers in this environment, the **Microsoft network client: Digitally sign communications (always)** setting is configured to **Enabled** in the baseline policy for the EC and SSLF environments.

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

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signatures. The implementation of digital signatures in Windows networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network clients on member servers will request signatures only if the servers with which they communicate accept digitally signed communication.

The **Microsoft network client: Digitally sign communications (if server agrees)** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

If you enable this policy setting, the SMB redirector is allowed to send plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication.

The **Microsoft network client: Send unencrypted password to third-party SMB servers** setting is configured to the default value of **Disabled** in the baseline policy for the three environments that are defined in this guide, unless application requirements supersede the need to maintain secret passwords.

Microsoft Network Server Settings

Table 4.18 Security Options: Microsoft Network Server Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Amount of idle time required before suspending session	15 minutes	15 minutes	15 minutes
Digitally sign communications (always)	Disabled	Enabled	Enabled
Digitally sign communications (if client agrees)	Enabled	Enabled	Enabled
Disconnect clients when logon hours expire	Enabled	Enabled	Enabled

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

This policy setting determines the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

The **Microsoft network server: Amount of idle time required before suspending session** setting is configured to **15 minutes** in the baseline policy for all three environments that are defined in this guide.

Microsoft network server: Digitally sign communications (always)

This policy setting determines whether packet signing is required by the SMB server component before further communication with an SMB client is permitted. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which prevents attempts to hijack sessions and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication because it places a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating systems will be unable to connect. If all SMB signing is completely disabled, computers are vulnerable to attacks that attempt to hijack their communications sessions.

The **Microsoft network server: Digitally sign communications (always)** setting is configured to **Disabled** in the baseline policy for the LC and environment and to **Enabled** for the EC and SSLF environments.

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

This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which blocks attempts to hijack sessions and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication because it places a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating systems will be unable to connect. If all SMB signing is completely disabled, computers are vulnerable to attacks that attempt to hijack their communications sessions.

The **Microsoft network server: Digitally sign communications (if client agrees)** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

Microsoft network server: Disconnect clients when logon hours expire

This policy setting determines whether to disconnect users who are connected to a network computer outside of their user account's valid logon hours. This policy setting affects the SMB component. If your organization has configured logon hours for users, then it makes sense to enable this policy setting. Otherwise, users should not be able to access network resources outside of their logon hours or they may be able to continue to use those resources with sessions that were established during allowed hours.

The **Microsoft network server: Disconnect clients when logon hours expire** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

Network Access Settings

Table 4.19 Security Options: Network Access Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Allow anonymous SID/NAME translation	Not defined	Not defined	Disabled
Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled	Enabled
Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Enabled	Enabled
Do not allow storage of credentials or .NET Passports for network authentication	Enabled	Enabled	Enabled
Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled
Named Pipes that can be accessed anonymously	Not defined	Not defined	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, netlogon, lsarpc, samr, browser
Remotely accessible registry paths	System\ CurrentControlSet\ Control\ Product Options; System\ CurrentControlSet\ Control\ Server Applications; Software\Microsoft\ Windows NT\ CurrentVersion	System\ CurrentControlSet\ Control\ Product Options; System\ CurrentControlSet\ Control\ Server Applications; Software\Microsoft\ Windows NT\ Current Version	System\ CurrentControlSet\ Control\ Product Options; System\ CurrentControlSet\ Control\ Server Applications; Software\Microsoft\ Windows NT\Current Version

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Remotely accessible registry paths and sub-paths	(see the following subsection for setting information)	(see the following subsection for setting information)	(see the following subsection for setting information)
Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled	Enabled
Shares that can be accessed anonymously	Not defined	Not defined	None
Sharing and security model for local accounts	Classic—local users authenticate as themselves	Classic—local users authenticate as themselves	Classic—local users authenticate as themselves

Network access: Allow anonymous SID/name translation

This policy setting determines whether an anonymous user can request SID attributes for another user. If this policy setting is enabled, a user with local access could use the well-known Administrators SID to obtain the real name of the built-in Administrator account, even if the account has been renamed. That person could then use the account to initiate a password guessing attack.

The **Network access: Allow anonymous SID/Name translation** setting is configured to **Not defined** in the baseline policy for the LC and EC environments. This policy setting is configured to **Disabled** in the baseline policy for the SSLF environment.

Network access: Do not allow anonymous enumeration of SAM accounts

This policy setting determines what additional permissions will be granted for anonymous connections to the computer. Windows allows anonymous users to perform certain activities, such as enumerate the names of domain accounts. This capability is convenient, for example, when an administrator wants to grant access to users in a trusted domain that does not maintain a reciprocal trust. However, even if this setting is enabled, anonymous users will still have access to any resources that have permissions that explicitly include the special built-in group **ANONYMOUS LOGON.**

The **Network access: Do not allow anonymous enumeration of SAM accounts** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether anonymous enumeration of SAM accounts and shares is allowed.

The **Network access: Do not allow anonymous enumeration of SAM accounts and shares** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines whether settings for **Stored User Names and Passwords** will save passwords, credentials, or Microsoft .NET Passports for later use after domain authentication is achieved.

The **Network access: Do not allow storage of credentials or .NET Passports for network authentication** setting is configured to **Enabled** in the baseline policy for all three security environments that are defined in this guide.

Note: Changes that are made to the configuration of this policy setting will not take effect until you restart Windows.

Network access: Let Everyone permissions apply to anonymous users

This policy setting determines what additional permissions are granted for anonymous connections to the computer. If you enable this policy setting, anonymous Windows users will be able to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks.

Therefore, the **Network access: Let Everyone permissions apply to anonymous users** setting is configured to **Disabled** in the baseline policy for all three environments that are defined in this guide.

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

Network access: Named Pipes that can be accessed anonymously

This policy setting determines which communication sessions (named pipes) will have attributes and permissions that allow anonymous access.

You should enforce the default values for the **Network access: Named Pipes that can be accessed anonymously** setting in the SSLF environment. The default values consist of the following named pipes:

- COMNAP – SNA session access
- COMNODE – SNA session access
- SQL\QUERY – SQL instance access
- SPOOLSS – Spooler service
- LLSRPC – License Logging service
- Netlogon – Net Logon service
- Lsarpc – LSA access

- Samr – SAM access
- browser – Computer Browser service

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

Network access: Remotely accessible registry paths

This policy setting determines which registry paths can be accessed over the network.

The **Network access: Remotely accessible registry paths** setting is configured to its default value in the baseline security templates for all three security environments that are defined in this guide.

Note: Even if you configure this policy setting, you must also start the Remote Registry system service if authorized users need to be able to access the registry over the network.

Network access: Remotely accessible registry paths and sub-paths

This policy setting determines which registry paths and sub-paths can be accessed over the network.

The default values for the **Network access: Remotely accessible registry paths and sub-paths** setting are enforced in the baseline security templates for all three security environments that are defined in this guide. The default values consist of the following paths and sub-paths:

- System\CurrentControlSet\Control\Print\Printers
- System\CurrentControlSet\Services\Eventlog
- Software\Microsoft\OLAP Server
- Software\Microsoft\Windows NT\CurrentVersion\Print
- Software\Microsoft\Windows NT\CurrentVersion\Windows
- System\CurrentControlSet\Control\ContentIndex
- System\CurrentControlSet\Control\Terminal Server
- System\CurrentControlSet\Control\Terminal Server\UserConfig
- System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
- Software\Microsoft\Windows NT\CurrentVersion\Perflib
- System\CurrentControlSet\Services\SysmonLog

Network access: Restrict anonymous access to Named Pipes and Shares

This policy setting can be used to restrict anonymous access to shares and named pipes in the following settings:

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

The **Network access: Restrict anonymous access to Named Pipes and Shares** setting is configured to the default setting of **Enabled** in the baseline policy for all three environments that are defined in this guide.

Network access: Shares that can be accessed anonymously

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this setting has little impact, because all users must be authenticated before they can access shared resources on the server.

The **Network access: Shares that can be accessed anonymously** setting is configured to **Not defined** for the LC and EC environments and to **None** for the SSLF environment.

Note: This policy setting can be very dangerous, because any shares that are listed can be accessed by any network user. Sensitive data could be exposed or corrupted if this policy setting is enabled.

Network access: Sharing and security model for local accounts

This policy setting determines how network logons that use local accounts are authenticated. The **Classic** configuration allows fine control over access to resources, and allows you to provide different types of access to different users for the same resource. The **Guest only** setting allows you to treat all users equally. In this context, all users authenticate as **Guest only** to receive the same access level to a given resource.

The **Network access: Sharing and security model for local accounts** setting is configured to the default configuration of **Classic** in the baseline policy for all three environments that are defined in this guide.

Network Security Settings

Table 4.20 Security Options: Network Security Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled
LAN Manager authentication level	Send NTLMv2 responses only	Send NTLMv2 response only\refuse LM	Send NTLMv2 response only\refuse LM & NTLM
LDAP client signing requirements	Negotiate signing	Negotiate signing	Negotiate signing

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum	Enabled all settings	Enabled all settings
Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum	Enabled all settings	Enabled all settings

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

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Windows NT hash.

For this reason, the **Network security: Do not store LAN Manager hash value on next password change** setting is configured to **Enabled** in the baseline policy for all three security environments that are defined in this guide.

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

Network security: LAN Manager authentication level

This policy setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol that is used by client computers, the level of security that is negotiated, and the level of authentication that is accepted by servers as follows. The numbers in the following table are the actual settings for the **LMCompatibilityLevel** registry value.

Table 4.21 LMCompatibilityLevel Registry Value Settings

Value	Protocol
0	Clients use LAN Manager and NTLM authentication and never use NTLMv2 session security.
1	Clients use LAN Manager and NTLM authentication and NTLMv2 session security if the server supports it.
2	Clients use only NTLM authentication and NTLMv2 session security if the server supports it.
3	Clients use only NTLMv2 authentication and NTLMv2 session security if the server supports it.
4	Clients use only NTLM authentication and NTLMv2 session security if the server supports it. The domain controller refuses LAN Manager authentication.
5	Clients use only NTLMv2 authentication and NTLMv2 session security if the server supports it. The domain controller refuses LAN Manager and NTLM authentication and accepts only NTLMv2.

You should configure this policy setting to the highest level that your environment allows according to the following guidelines:

In an environment that includes only Windows NT 4.0 SP4, Windows 2000, and Windows XP Professional, configure this policy setting to **Send NTLMv2 response only\refuse LM & NTLM** on all clients, and then to **Send NTLMv2 response only\refuse LM & NTLM** on all servers after all clients are configured. The exception to this recommendation is Windows Server 2003 Routing and Remote Access servers, which will not function properly if this policy setting is configured higher than **Send NTLMv2 response only\refuse LM**.

The EC environment may need to support Routing and Remote Access servers, therefore the **Network security: LAN Manager authentication level** setting for this environment is configured to **Send NTLMv2 response only\refuse LM** in the baseline policy. Routing and Remote Access servers are not supported in the SSLF environment, so the policy setting for this environment is configured to **Send NTLMv2 response only\refuse LM & NTLM**.

If you have Windows 9x clients on which you can install the DSClient, configure this policy setting to **Send NTLMv2 response only\refuse LM & NTLM** on computers that run Windows NT (Windows NT, Windows 2000, and Windows XP Professional). Otherwise, you must leave this policy setting configured to no higher than **Send NTLMv2 responses only** in the baseline policy for computers that do not run Windows 9x, which is how the setting is configured for the LC environment.

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

Network security: LDAP client signing requirements

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. Unsigned network traffic is susceptible to man-in-the-middle attacks. For an LDAP server, an attacker could cause a server to make decisions that are based on false queries from the LDAP client.

Therefore, the **Network security: LDAP client signing requirements** setting is configured to **Negotiate signing** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting allows a client to require the negotiation of message confidentiality (encryption), message signing, 128-bit encryption, or NTLM version 2 (NTLMv2) session security. Configure this policy setting to as high a security level as possible, but remember that you still need to allow the applications on the network to function. Proper configuration of this policy setting will help ensure that network traffic from NTLM SSP–based servers is protected from man-in-the-middle attacks and data exposure.

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** setting is configured to **No minimum** in the baseline policy for the LC environment. All settings are enabled for the EC and SSLF environments.

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

This policy setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. Configure this policy setting to as high a security level as possible, but remember that you still need to allow the applications on the network to function. Like the previous policy setting, proper configuration of this policy setting will help ensure that network traffic from NTLM SSP–based clients is protected from man-in-the-middle attacks and data exposure.

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** security option setting is configured to **No minimum** in the baseline policy for the LC environment. All settings are enabled for the EC and SSLF environments.

Recovery Console Settings

Table 4.22 Security Options: Recovery Console Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Allow automatic administrative logon	Disabled	Disabled	Disabled
Allow floppy copy and access to all drives and all folders	Enabled	Enabled	Disabled

Recovery console: Allow automatic administrative logon

This policy setting determines whether the password for the Administrator account must be entered before computer access is granted. If you enable this policy setting, the Recovery Console does not require you to provide a password, and it automatically logs on to the computer. The Recovery Console can be very useful when you need to work with computers that have startup problems. However, it can be detrimental to enable this setting because anyone can then walk up to the server, disconnect its power to shut it down, restart it, select **Recover Console** from the **Restart** menu, and then assume full control of the server.

Therefore, the **Recovery console: Allow automatic administrative logon** setting is configured to the default setting of **Disabled** in the baseline policy for all three environments that are defined in this guide. To use the Recovery Console when this setting is disabled, the user will have to enter a user name and password to access the Recovery Console account.

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

You can enable this policy setting to make the Recovery Console **SET** command available, which allows you to set the following Recovery Console environment variables:

- **AllowWildCards**. Enables wildcard support for some commands (such as the DEL command).
- **AllowAllPaths**. Allows access to all files and folders on the computer.

- **AllowRemovableMedia**. Allows files to be copied to removable media, such as a floppy disk.
- **NoCopyPrompt**. Does not prompt when overwriting an existing file.

For maximum security, the **Recovery console: Allow floppy copy and access to all drives and all folders** setting is configured to **Disabled** in the baseline policy for the SSLF environment. However, this policy setting is configured to **Enabled** for the LC and EC environments.

Shutdown Settings

Table 4.23 Security Options: Shutdown Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Allow system to be shut down without having to log on	Disabled	Disabled	Disabled
Clear virtual memory page file	Disabled	Disabled	Disabled

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

This policy setting determines whether a computer can be shut down by a user who is not required to log on to the Windows operating system. Users who can access the console could shut down the computer. An attacker or misguided user could connect to the server through Terminal Services and shut it down or restart it without having to identify themselves.

Therefore, the **Shutdown: Allow system to be shut down without having to log on** setting is configured to the default setting of **Disabled** in the baseline policy for all three environments that are defined in this guide.

Shutdown: Clear virtual memory page file

This policy setting determines whether the virtual memory pagefile is cleared when the computer is shut down. When this policy setting is enabled, it causes the system pagefile to be cleared each time that the computer shuts down gracefully. If you enable this policy setting, the hibernation file (Hiberfil.sys) is also zeroed out when hibernation is disabled on a portable computer. Server shutdowns and restarts will take longer and will be especially noticeable on servers with large pagefiles.

For these reasons, the **Shutdown: Clear virtual memory page file** setting is configured to **Disabled** in all three environments that are defined in this guide.

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

System Cryptography Settings

Table 4.24 Security Options: System Cryptography Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Force strong key protection for user keys stored on the computer	User is prompted when the key is first used	User is prompted when the key is first used	User must enter a password each time they use a key
Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	Disabled	Enabled

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

This policy setting determines whether users' private keys (such as their S-MIME keys) require a password to be used. If you configure this policy setting so that users must provide a password—distinct from their domain password—every time that they use a key, then it will be more difficult for an attacker to access locally stored keys, even an attacker who discovers logon passwords.

For usability requirements in the LC and EC environments, the **System cryptography: Force strong key protection for user keys stored on the computer** setting is configured to **User is prompted when the key is first used** in the baseline policy. To provide additional security, this policy setting is configured to **User must enter a password each time they use a key** for the SSLF environment.

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

This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. Although this policy setting increases security, most public Web sites that are secured with TLS or SSL do not support these algorithms. Many client computers are also not configured to support these algorithms.

For these reasons, the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting is configured to **Disabled** in the baseline policy for the LC and EC environments. This policy setting is configured to **Enabled** for the SSLF environment.

System Objects Settings

Table 4.25 Security Options: System Objects Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Default owner for objects created by members of the Administrators group	Object creator	Object creator	Object creator
Require case insensitivity for non-Windows subsystems	Enabled	Enabled	Enabled
Strengthen default permissions of internal system objects (for example, Symbolic Links)	Enabled	Enabled	Enabled

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

This policy setting determines whether the **Administrators** group or an object creator is the default owner of any system objects that are created. When system objects are created, the ownership will reflect which account created the object rather than the more generic **Administrators** group.

The **System objects: Default owner for objects created by members of the Administrators group** setting is configured to **Object creator** in the baseline policy for all three environments that are defined in this guide.

System objects: Require case insensitivity for non-Windows subsystems

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32® subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive and the POSIX subsystem supports case sensitivity, failure to enforce this setting makes it possible for a POSIX user to create a file with the same name as another file if they use mixed case letters to label it. Such an occurrence may block another user's access to these files with typical Win32 tools, because only one of the files will be available.

To ensure consistency of file names, the **System objects: Require case insensitivity for non-Windows subsystems** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

This policy setting determines the strength of the default discretionary access control list (DACL) for objects, and helps secure objects that can be located and shared among processes. To strengthen the DACL you can use the default value of **Enabled**, which it allows users who are not administrators to read shared objects but not to modify any that they did not create.

The **System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)** setting is configured to the default value of **Enabled** in the baseline policy for all three environments that are defined in this guide.

System Settings

Table 4.26 Security Options: System Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
System settings: Optional subsystems	None	None	None
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not defined	Disabled	Enabled

System settings: Optional subsystems

This policy setting determines which subsystems are used to support applications in your environment. The default value for this policy setting in Windows Server 2003 is **POSIX**.

To disable the POSIX subsystem, the **System settings: Optional subsystems** setting is configured to **None** in the baseline policy for all three environments that are defined in this guide.

System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. It enables or disables certificate rules (a type of software restriction policies rule). With software restriction policies, you can create a certificate rule that will allow or disallow the execution of Authenticode®-signed software, based on the digital certificate that is associated with the software. For certificate rules to take effect in software restriction policies, you must enable this policy setting.

The **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies** setting is configured to **Enabled** in the SSLF environment. However, it is configured to **Disabled** in the EC environment and to **Not defined** in the LC environment because of the potential performance impact.

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.

You can configure the event log settings in Windows Server 2003 with SP1 at the following location within the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Event Log

This section provides details about the prescribed MSBP event log settings for all three environments that are defined in this guide. For a summary of the prescribed settings in this section, see the Microsoft Excel workbook "Windows Server 2003 Security Guide Settings," which is available in the downloadable version of this guide. For information about the default configuration and a detailed explanation of each of the settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

The following table summarizes the event log setting recommendations for the three environments that are defined in this guide. Additional information about each setting is provided in the subsections that follow the table.

Table 4.27 Event Log Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Maximum application log size	16,384 KB	16,384 KB	16,384 KB
Maximum security log size	81,920 KB	81,920 KB	81,920 KB
Maximum system log size	16,384 KB	16,384 KB	16,384 KB
Prevent local guests group from accessing application log	Enabled	Enabled	Enabled
Prevent local guests group from accessing security log	Enabled	Enabled	Enabled
Prevent local guests group from accessing system log	Enabled	Enabled	Enabled
Retention method for application log	As needed	As needed	As needed
Retention method for security log	As needed	As needed	As needed
Retention method for system log	As needed	As needed	As needed

Maximum application log size

This policy setting specifies the maximum size of the Application event log, which has a maximum capacity of 4 GB. However, this size is not recommended because of the risk of memory fragmentation, which causes slow performance and unreliable event logging. Requirements for the Application log size vary, and depend on the function of the platform and the need for historical records of application-related events.

The **Maximum application log size** setting is configured to the default value of **16,384 KB** in the baseline policy for all three environments that are defined in this guide.

Maximum security log size

This policy setting specifies the maximum size of the Security event log, which has a maximum capacity of 4 GB. You should configure the Security log to at least 80 MB on domain controllers and stand-alone servers, which should adequately store enough information to conduct audits. How you configure this policy setting for other computers depends on factors that include how frequently the log will be reviewed, available disk space, and so on.

The **Maximum security log size** security setting is configured to **81,920 KB** in the baseline policy for all three environments that are defined in this guide.

Maximum system log size

This policy setting specifies the maximum size of the System event log, which has a maximum capacity of 4 GB. However, this size is not recommended because of the risk of memory fragmentation, which causes slow performance and unreliable event logging. Requirements for the System log size vary, and depend on the function of the platform and the need for historical records.

The **Maximum system log size** setting is configured to the default value of **16,384 KB** in the baseline policy for all three environments that are defined in this guide.

Prevent local guests group from accessing application log

This policy setting determines whether guests are denied access to the Application event log. By default in Windows Server 2003 with SP1, guest access is prohibited on all computers. Therefore, this policy setting has no real effect on computers with default configurations.

However, because this configuration is considered a defense-in-depth measure with no side effects, the **Prevent local guests group from accessing application log** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

Prevent local guests group from accessing security log

This policy setting determines whether guests are denied access to the Security event log. A user must be assigned the **Manage auditing and security log** user right (not defined in this guidance) to access the Security log. Therefore, this policy setting has no real effect on computers with default configurations.

However, because this configuration is considered a defense-in-depth measure with no side effects, the **Prevent local guests group from accessing security log** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

Prevent local guests group from accessing system log

This policy setting determines whether guests are denied access to the System event log. By default in Windows Server 2003 with SP1, guest access is prohibited on all computers. Therefore, this policy setting has no real effect on computers with default configurations.

However, because this configuration is considered a defense-in-depth setting measure with no side effects, the **Prevent local guests group from accessing system log** setting is configured to **Enabled** in the baseline policy for all three environments that are defined in this guide.

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

Retention method for application log

This policy setting determines the "wrapping" method for the Application log. It is imperative that the Application log be archived regularly if historical events are needed for either forensics or troubleshooting purposes. If events are overwritten as needed, the log will always store the most recent events—although this configuration could result in a loss of historical data.

The **Retention method for application log** setting is configured to **As needed** in the baseline policy for all three environments that are defined in this guide.

Retention method for security log

This policy setting determines the "wrapping" method for the Security log. It is imperative that the Security log be archived regularly if historical events are needed for either forensics or troubleshooting purposes. If events are overwritten as needed, the log will always store the most recent events—although this configuration could result in a loss of historical data.

The **Retention method for security log** setting is configured to **As needed** in the baseline policy for all three environments that are defined in this guide.

Retention method for system log

This policy setting determines the "wrapping" method for the System log. It is imperative that the logs be archived regularly if historical events are needed for either forensics or troubleshooting purposes. If events are overwritten as needed, the log will always store the most recent events—although this configuration could result in a loss of historical data.

The **Retention method for system log** setting is configured to **As needed** in the baseline policy for all three environments that are defined in this guide.

Additional Registry Entries

Additional registry entries (also called *registry values*) were created for the baseline security template files that are not defined within the default Administrative Template (.adm) file for the three security environments that are defined in this guide. The .adm files define the policies and restrictions for the desktop, shell, and security for Windows Server 2003.

These registry entries are embedded within the security templates (in the "Security Options" section) to automate the changes. If the policy is removed, these registry entries are not automatically removed with it; they must be manually changed with a registry editing tool such as Regedt32.exe. The same registry entries are applied across all three environments.

This guide includes additional registry entries that are added to the Security Configuration Editor (SCE). To add these registry entries, you need to modify the Sceregvl.inf file

(located in the **%windir%\inf** folder) and re-register the Scecli.dll file. The original security entries, as well as the additional ones, appear under **Local Policies\Security** in the snap-ins and tools that are listed earlier in this chapter. You will need to update the Sceregvl.inf file and re-register the Scecli.dll file for any computers on which you will edit the security templates and Group Policies that are provided with this guide. Details about how to update these files are provided in the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

This section is only a summary of the additional registry entries that are described in detail in the companion guide. For information about the default settings and a detailed explanation of each of the settings that are discussed in this section, see *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*.

Security Consideration for Network Attacks

Denial of service (DoS) attacks are network attacks that attempt to make a computer or a particular service on a computer unavailable to network users. DoS attacks can be difficult to defend against.

To help prevent these attacks, you should keep your computer updated with the latest security fixes and harden the TCP/IP protocol stack on computers that run Windows Server 2003 with SP1 and are exposed to potential attackers. The default TCP/IP stack configuration is tuned to handle standard intranet traffic. If you connect a computer directly to the Internet, Microsoft recommends that you harden the TCP/IP stack against DoS attacks.

You can add the registry values in the following table to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

subkey.

Table 4.28 TCP/IP Registry Entry Recommendations

Registry entry	Format	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
EnableICMPRedirect	DWORD	0	0	0
SynAttackProtect	DWORD	1	1	1
EnableDeadGWDetect	DWORD	0	0	0
KeepAliveTime	DWORD	300,000	300,000	300,000
DisableIPSourceRouting	DWORD	2	2	2
TcpMaxConnectResponseRetransmissions	DWORD	2	2	2
TcpMaxDataRetransmissions	DWORD	3	3	3
PerformRouterDiscovery	DWORD	0	0	0

Other Registry Entries

Other recommended registry entries that are not specific to TCP/IP are listed in the following table. Additional information about each entry is provided in the subsections that follow the table.

Table 4.29 Other Registry Entry Recommendations

Registry entry	Format	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	DWORD	1	1	1
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)	DWORD	0	0	1
MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)	DWORD	0xFF	0xFF	0xFF
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	String	0	0	0
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	DWORD	90	90	90
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	DWORD	1	1	1
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	DWORD	1	1	0
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	DWORD	0	0	0
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)	DWORD	1	1	0

Registry entry	Format	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)	DWORD	1	1	1
MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)	DWORD	3	3	3

Configure NetBIOS Name Release Security: Allow the computer to ignore NetBIOS name release requests except from WINS servers

This entry appears as **MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers** in the SCE.

NetBIOS over TCP/IP is a network protocol that (among other things) provides a way to easily resolve NetBIOS names that are registered on Windows-based computers to the IP addresses that are configured on those computers. This value determines whether the computer releases its NetBIOS name when it receives a name-release request.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters

subkey.

Disable Auto Generation of 8.3 File Names: Enable the computer to stop generating 8.3 style filenames

This entry appears as **MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)** in the SCE.

Windows Server 2003 with SP1 supports 8.3 file name formats for backward compatibility with16-bit applications. The 8.3 file name convention is a format that only allows file names of eight characters or less.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem

subkey.

Disable Autorun: Disable Autorun for all drives

This entry appears as **MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)** in the SCE.

Autorun begins to read from a drive on your computer as soon as media is inserted into it. As a result, things like the setup file (for programs) or the sound (for audio content) start immediately.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

subkey.

Make Screensaver Password Protection Immediate: The time in seconds before the screen saver grace period expires (0 recommended)

This entry appears as **MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)** in the SCE.

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

subkey.

Security Log Near Capacity Warning: Percentage threshold for the security event log at which the system will generate a warning

This entry appears as **MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning** in the SCE.

This option became available with SP3 for Windows 2000. It generates a security audit in the Security log when its size reaches a user-defined threshold. For example, if you configure the value for this registry entry to 90 and the Security log reaches 90 percent of capacity, the log will show one entry with an eventID of 523 that reads as follows: “The security event log is 90 percent full.”

Note: If you configure log settings to **Overwrite events as needed** or **Overwrite events older than x days**, this event will not be generated.

You can add this registry value to the security template file in the

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security

subkey.

Enable Safe DLL Search Order: Enable Safe DLL search mode (recommended)

This entry appears as **MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)** in the SCE.

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways:

- Search folders that are specified in the system path first, and then search the current working folder.
- Search the current working folder first, and then search the folders that are specified in the system path.

The registry value is configured to 1, which causes the computer to first search the folders that are specified in the system path and then the current working folder. If you configure this entry to 0, the computer first searches the current working folder and then the folders that are specified in the system path.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Session Manager

subkey.

Automatic Reboot: Allow Windows to automatically restart after a system crash

This entry appears as **MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)** in the SCE.

This entry, when enabled, permits a server to automatically reboot after a fatal crash. It is enabled by default, which is undesirable on highly secure servers.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl

subkey.

Automatic Logon: Enable Automatic Logon

This entry appears as **MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)** in the SCE. By default, this entry is not enabled and should never be used on a server in practically any conceivable circumstance.

For more information, see the Microsoft Knowledge Base article "How to turn on automatic logon in Windows XP" at http://support.microsoft.com/default.aspx?kbid=315231.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon

subkey.

Administrative Shares: Enable Administrative Shares

This entry appears as **MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)** in the SCE. By default, when Windows networking is active on a server, Windows will create hidden administrative shares—which is undesirable on highly secure servers.

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters

subkey.

Disable Saved Passwords: Prevent the dial-up password from being saved

This entry appears as **MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)** in the SCE. By default, Windows will offer the option to save passwords for dial-up and VPN connections, which is not desirable on a server.

You can add this registry value to the template file in the

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\
Parameters**

subkey.

Enable IPSec to protect Kerberos RSVP Traffic: Enable NoDefaultExempt for IPSec Filtering

This entry appears as **MSS: (NoDefaultExempt) Enable NoDefaultExempt for IPSec Filtering (recommended)** in the SCE. The default exemptions to IPsec policy filters are documented in the Microsoft Windows Server 2003 online help. These filters make it possible for Internet Key Exchange (IKE) and the Kerberos authentication protocol to function. The filters also make it possible for the network Quality of Service (QoS) to be signaled (RSVP) when the data traffic is secured by IPsec, and for traffic that IPsec might not secure (such as multicast and broadcast traffic).

You can add this registry value to the template file in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IPSEC

subkey.

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 all three 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 with SP1 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 with SP1 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. All of the following files are located in the **%SystemRoot%\System32** folder, and 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
- regsvr32.exe
- rexec.exe
- route.exe
- rsh.exe
- sc.exe
- secedit.exe
- subst.exe
- systeminfo.exe
- telnet.exe
- tftp.exe
- tlntsvr.exe

For your convenience, these optional permissions are already configured in the security template called **Optional-File-Permissions.inf**, which is included with the downloadable version of this guide.

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: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

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 Rights Assignments

Most of the recommended security groups for user rights 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 4.30 Manually Added User Rights Assignments

Setting Name in UI	Legacy Client	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	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on as a batch job	Support_388945a0 and Guest	Support_388945a0 and Guest	Support_388945a0 and Guest

Setting Name in UI	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Deny log on through Terminal Services	Built-in Administrator; Guests; Support_388945a0; Guest ; all NON-operating system service accounts	Built-in Administrator; Guests; Support_388945a0; Guest ; all NON-operating system service accounts	Built-in Administrator; Guests; Support_388945a0; Guest; all NON-operating system service accounts

Important: All NON-operating system service accounts are service accounts for specific applications in your enterprise. 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 Rights Assignments

In Active Directory Users and Computers, right-click the Member Servers OU, and then select **Properties**.

1. On the Group Policy tab, select the Enterprise Client Member Server Baseline Policy to edit the linked GPO.
2. Select Enterprise Client – Member Server Baseline Policy, and then click Edit.
3. 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.
4. Close the Group Policy that you modified.
5. Close the Member Servers OU Properties window.
6. 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.
7. 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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, the built-in Administrator account is renamed and the description altered 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 all three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

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, and Windows Server 2003.

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 2003 Server with SP1, 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 all three environments that are defined in this guide are formatted with NTFS partitions to provide the means for file and directory security management through ACLs.

Terminal Services Settings

The **Set client connection encryption level** setting determines the level of encryption for Terminal Services client connections in your environment. The **High Level** setting option that uses 128-bit encryption prevents an attacker from eavesdropping on Terminal Services sessions with a packet analyzer. Some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such clients, set the encryption level of the connection to send and receive data at the highest encryption level that is supported by the client.

You can configure this setting in Group Policy at the following location:

Computer Configuration\Administrative Templates\Windows Components\ Terminal Services\Encryption and Security

Table 4.31 Client Connection Encryption Level Setting Recommendation

Setting name in UI	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Set client connection encryption level	High	High	High

The three available levels of encryption are described in the following table:

Table 4.32 Terminal Services Encryption Levels

Encryption level	Description
High level	Encrypts data that is sent from client to server and from server to client with strong 128-bit encryption. Use this level when the terminal server runs in an environment that contains 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.
Client Compatible	Encrypts data that is sent between the client and the server at the maximum key strength that is supported by the client. Use this level when the terminal server runs in an environment that contains mixed or legacy clients.
Low level	Encrypts data that is sent from the client to the server with 56-bit encryption. **Important**: Data sent from the server to the client is not encrypted.

Error Reporting

Table 4.33 Recommended Error Reporting Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Turn off Windows Error Reporting	Enabled	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 and Windows Server 2003.

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 can control whether the Error Reporting service transmits any data.

You can configure this policy setting in Windows Server 2003 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 DCBP for all three environments that are defined in this guide.

Enable Manual Memory Dumps

Windows Server 2003 with SP1 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 allows a Memory.dmp file to be generated with the keyboard at http://support.microsoft.com/default.aspx?kbid=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.

Creating the Baseline Policy Using SCW

To deploy the necessary security settings, you first need to create a member server baseline policy (MSBP). To do so, you must use SCW (the Security Configuration Wizard tool) and the security templates that are included with the downloadable version of this guide.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the MSBP creation steps you will probably remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the Member Server Baseline Policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain.
4. Install and configure only the mandatory applications that will be on every server in your environment. Examples include your software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Remove the File server role from the listed of detected roles.
7. Ensure that the detected server roles are appropriate for your environment.
8. Ensure that the detected client features are appropriate for your environment.
9. Ensure that the detected administrative options are appropriate for your environment.
10. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
11. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
12. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
13. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
15. Include the appropriate security template (for example, EC-Member Server Baseline.inf).
16. Save the policy with an appropriate name (for example, Member Server Baseline.xml).

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method offers the advantage of the ability to easily roll back deployed policies from within SCW.

This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\Member
   Server Baseline.xml" /g:"Member Server Baseline Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained the server hardening procedures that were initially applied to all of the servers that run Windows Server 2003 with SP1 in all three security environments that are defined in this guide. Most of these procedures created a unique security template for each security environment and imported it into a GPO that is linked to the parent OU for the member server to achieve the targeted level of security.

However, some of these hardening procedures cannot be applied through Group Policy. Guidance was provided about how to configure these settings manually. Additional steps were taken for specific server roles to enable them to function within their roles as securely as possible.

Server role-specific steps include both additional hardening procedures and procedures to reduce the security settings in the baseline security policy. These changes are discussed in detail in the following chapters of this guide.

More Information

The following links provide additional information about topics that relate to hardening servers that run Windows Server 2003 with SP1.

- For more information about Windows Server 2003 security settings, see the Security Setting Descriptions page at http://technet2.microsoft.com/WindowsServer/en/Library/dd980ca3-f686-4ffc-a617-50c6240f55821033.mspx.
- For more information about security for Windows Server 2003, see the Windows Server 2003 Security Center at www.microsoft.com/technet/security/prodtech/windowsserver2003.mspx.
- For more information about audit policy for Windows Server 2003, see the Auditing Policy page at http://technet2.microsoft.com/WindowsServer/en/Library/6847e72b-9c47-42ab-b3e3-691addac9f331033.mspx.
- For more information about Microsoft Operations Manger (MOM), see the Microsoft Operations Manager page at www.microsoft.com/mom/.
- For more information about user rights in Windows Server 2003, see the User rights page at http://technet2.microsoft.com/WindowsServer/en/Library/589980fb-1a83-490e-a745-357750ced3d91033.mspx.
- For more information about default security settings for Windows Server 2003, see the Differences in default security settings page at http://technet2.microsoft.com/WindowsServer/en/Library/1494bf2c-b596-4785-93bb-bc86f8e548d51033.mspx.
- For more information about how to secure Windows 2000 Terminal Services, see "Securing Windows 2000 Terminal Services" at www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.mspx.
- For more information about how to secure the Windows Server 2003 TCP/IP stack, see the Microsoft Knowledge Base article "How To Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003" at http://support.microsoft.com/?kbid=324270.
- For more details about how to harden the settings for Windows Sockets applications, see the Microsoft Knowledge Base article "Internet Server Unavailable Because of Malicious SYN Attacks" at http://support.microsoft.com/?kbid=142641.
- For more information about the location of .adm files, see the Microsoft Knowledge Base article "Location of ADM (Administrative Template) Files in Windows" at http://support.microsoft.com/?kbid=228460.
- For more information about how to customize the Security Configuration Editor user interface, see the Microsoft Knowledge Base article "How to Add Custom Registry Settings to Security Configuration Editor" at http://support.microsoft.com/?kbid=214752.
- For more information about how to create custom administrative template files in Windows, see the Microsoft Knowledge Base article "HOW TO: Create Custom Administrative Templates in Windows 2000" at http://support.microsoft.com/?kbid=323639. Also review the white paper "Using Administrative Template Files with Registry-Based Group Policy" at www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx.

- For more information about ensuring that more secure LAN Manager authentication level settings work in networks with a mix of Windows 2000 and Windows NT 4.0 computers, see the Microsoft Knowledge Base article "Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain" at http://support.microsoft.com/?kbid=305379.
- For more information about NTLMv2 authentication, see the Microsoft Knowledge Base article "How to enable NTLM 2 authentication" at http://support.microsoft.com/?kbid=239869.
- For more information about the default settings for services in Windows Server 2003, see the Default settings for services page at http://technet2.microsoft.com/WindowsServer/en/Library/2b1dc6cf-2e34-4681-9aa6-8d0ffba2d3e31033.mspx.
- For more information about smart card deployment, see "Get Smart! Boost Your Network's IQ With Smart Cards" at www.microsoft.com/technet/technetmag/issues/2005/01/SmartCards/default.aspx.
- For more information about the "Restrict Anonymous" registry value and Windows 2000, see the Microsoft Knowledge Base article "The "RestrictAnonymous" Registry Value May Break the Trust to a Windows 2000 Domain" at http://support.microsoft.com/?kbid=296405.
- For more information about error reporting, see the Corporate Error Reporting page at www.microsoft.com/resources/satech/cer/.
- For information about network ports used by Microsoft applications, see the Microsoft Knowledge Base article "Service overview and network port requirements for the Windows Server system" at http://support.microsoft.com/kb/832017.

Chapter 5: The Domain Controller Baseline Policy

Overview

Addressing security in the Domain Controller server role is one of the most important aspects of any environment with computers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) 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.

Domain Controller Baseline Policy

Unlike the other server role policies that are detailed later in this guide, the Group Policy for the Domain Controllers server role is a baseline policy like the Member Server Baseline Policy (MSBP) defined in Chapter 4, "The Member Server Baseline Policy." The Domain Controller Baseline Policy (DCBP) is linked to the Domain Controllers organizational unit (OU) and takes precedence over the Default Domain Controllers Policy. The policy settings that are included in the DCBP will strengthen the overall security of all domain controllers in any environment.

Most of the DCBP is copied from the MSBP. Therefore, you should carefully review Chapter 4, "The Member Server Baseline Policy" to fully understand the many policy settings that are also included in the DCBP. Only the DCBP settings that differ from those in the MSBP are documented in this chapter.

Domain controller templates are uniquely designed to address the security needs of the three environments that are defined in this guide. The following table shows the domain controller .inf files that are included with this guide for the Legacy Client (LC), Enterprise Client (EC), and Specialized Security – Limited Functionality (SSLF) environments. For example, the EC-Domain Controller.inf file is the security template for the Enterprise Client environment.

Table 5.1 Domain Controller Baseline Security Templates

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-Domain Controller.inf	EC-Domain Controller.inf	SSLF-Domain Controller.inf

Note: Domain operations could be severely impaired if an incorrectly configured Group Policy object (GPO) is linked to the Domain Controllers OU. Use extreme care when you import these security templates, and verify that all imported policy settings are correct before you link a GPO to the Domain Controllers OU.

Audit Policy Settings

The Audit policy settings for domain controllers are almost the same as those specified in the MSBP. For more information, see Chapter 4, "The Member Server Baseline Policy." The policy settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers.

Table 5.2 Recommended Audit Policy Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Audit directory service access	No auditing	No auditing	Failure

Audit directory service access

This policy setting determines whether to audit user access to an Active Directory object that has its own specified system access control list (SACL). If you define the **Audit directory service access** setting, you can specify whether to audit successes, failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an Active Directory object that has a specified SACL. Failure audits generate an audit entry when a user unsuccessfully attempts to access an Active Directory object that has a specified SACL.

If you enable the **Audit directory service access** setting in the DCBP and configure SACLs on directory objects, a large volume of entries can be generated in the Security logs on domain controllers. You should only enable this setting if you actually intend to use the information that is created.

The **Audit directory service access** setting is configured to **No auditing** in the LC and EC environments. It is configured to log **Failure** events in the SSLF environment.

The following table includes the important security events that the **Audit directory service access** setting records in the Security log.

Table 5.3 Directory Service Access Events

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

User Rights Assignment Settings

The DCBP specifies a number of user rights assignments for the domain controllers. In addition to the default configuration, several user rights settings were modified to strengthen the security for the domain controllers in the three environments that are defined in this guide.

This section provides details about the prescribed user rights settings for the DCBP that differ from those in the MSBP. For a summary of the prescribed settings in this section, refer to the Microsoft Excel® workbook "Windows Server 2003 Security Guide Settings" that is included with the downloadable version of this guide.

The following table summarizes the recommended user rights assignment settings for the DCBP. Additional information for each setting is provided in the sections that follow the table.

Table 5.4 Recommended User Rights Assignments Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Access this computer from the network	Not defined	Not defined	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
Add workstations to domain	Not defined	Not defined	Administrators
Allow log on locally	Administrators, Server Operators, Backup Operators	Administrators, Server Operators, Backup Operators	Administrators
Allow log on through Terminal Services	Administrators	Administrators	Administrators
Change the system time	Administrators, LOCAL SERVICE	Administrators, LOCAL SERVICE	Administrators, LOCAL SERVICE
Enable computer and user accounts to be trusted for delegation	Not Defined	Not Defined	Administrators
Load and unload device drivers	Administrators	Administrators	Administrators
Restore files and directories	Administrators	Administrators	Administrators
Shutdown the system	Administrators	Administrators	Administrators

Access this computer from the network

This policy setting determines which users and groups are allowed to connect to the domain controller over the network. It is required by a number of network operations, including Active Directory replication between domain controllers, authentication requests

to domain controllers from users and from computers, and for access to shared folders and printers.

Although permissions that are assigned to the **Everyone** security group no longer provide access to anonymous users in Windows Server 2003 with SP1, guest groups and accounts can still be provided with access through the **Everyone** security group.

For this reason, the **Everyone** security group is removed from the **Access this computer from the network** user right in the DCBP for the SSLF environment. Removal of this group provides an extra safeguard against attacks that target guest access to the domain. This policy setting is configured to **Not defined** for the LC and EC environments.

Add workstations to domain

This policy setting specifies which users can add computer workstations to a specific domain. For this policy setting to take effect, it must be assigned to the user as part of the Default Domain Controller Policy for the domain. A user who has been assigned this right can add up to 10 workstations to the domain. Users who have been assigned the **Create Computer Objects** permission for an OU or the Computers container in Active Directory can add an unlimited number of computers to the domain, regardless of whether they have been assigned the **Add workstations to a domain** user right.

By default, all users in the **Authenticated Users** group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.

In Windows–based networks, the term *security principal* is defined as a user, group, or computer that is automatically assigned a security identifier to control access to resources. In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. However, some organizations may want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage the computers. If users are allowed to add computers to the domain, tracking and management efforts would be hampered. Also, users could perform activities that are more difficult to trace because of their ability to create additional unauthorized domain computers.

For these reasons, the **Add workstations to domain** user right is assigned only to the **Administrators** group in the DCBP for the SSLF environment. This policy setting is configured to **Not defined** for the LC and EC environments.

Allow log on locally

This policy setting specifies which users can start interactive sessions on the domain controller. Users who do not have this right are still able to start a remote interactive session on the domain controller if they have been assigned the **Allow logon through Terminal Services** user right.

You should restrict the number of accounts that can log on to domain controller consoles to help prevent unauthorized access to domain controller file systems and system services. A user who is able to log on to the console of a domain controller could maliciously exploit the computer and possibly compromise the security of an entire domain or forest.

By default, the **Account Operators**, **Backup Operators**, **Print Operators**, and **Server Operators** groups are assigned the **Allow log on locally** user right on domain controllers. Users in these groups should not need to log on to a domain controller to perform their management tasks, and they should be able to perform their duties from

other workstations. Only users in the **Administrators** group should perform maintenance tasks on domain controllers.

If you assign the **Allow log on locally** user right only to the **Administrators** group, physical and interactive domain controller access is limited to only highly trusted users, which enhances security. For this reason, the **Allow log on locally** user right is assigned only to the **Administrators** group in the DCBP for the SSLF environment. This policy setting is configured to include the **Server Operators** and **Backup Operators** groups for the LC and EC environments.

Allow log on through Terminal Services

This policy setting specifies which users can log on to the domain controller through a Remote Desktop connection.

You should restrict the number of accounts that can log on to domain controller consoles through Terminal Services to help prevent unauthorized access to domain controller file systems and system services. A user who is able to log on to the console of a domain controller through Terminal Services can exploit that computer and possibly compromise the security of an entire domain or forest.

If you assign the **Allow log on through Terminal Services** user right only to the **Administrators** group, interactive domain controller access is limited to only highly trusted users, which enhances security. For this reason, the **Allow log on through Terminal Services** user right is assigned only to the **Administrators** group in the DCBP for all three environments that are defined in this guide. Although logon to a domain controller through Terminal Services requires administrative access by default, configuration of this policy setting helps protect against inadvertent or malicious actions that might compromise the network.

As an additional security measure, the DCBP denies the default Administrator account the **Allow log on through Terminal Services** user right. This configuration prevents attempts by malicious users to remotely break into a domain controller with the default Administrator account. For more details about this policy setting, see Chapter 4, "The Member Server Baseline Policy."

Change the system time

This policy setting specifies which users can adjust the time on a computer's internal clock. However, it is not needed to change the time zone or other display characteristics of the system time.

Synchronized system time is critical to the operation of Active Directory. Proper Active Directory replication and authentication ticket generation processes that are used by the Kerberos authentication protocol rely on time being synchronized across any environment.

A domain controller clock that is not synchronized with the system time on other domain controllers in the environment could interfere with the operation of domain services. If only administrators are allowed to modify system time, the possibility of incorrect system time on a domain controller is minimized.

By default, the **Server Operators** group has the ability to modify system time on domain controllers. Because of the problems that could be caused by incorrect modification of a domain controller's clock by members of this group, the **Change the system time** user right is assigned in the DCBP to only the **Administrators** group and the **Local Service** account for all three environments that are defined in this guide.

For more information on the Microsoft Windows® Time Service, see the Windows Time Service Technical Reference at http://technet2.microsoft.com/WindowsServer/en/Library/a0fcd250-e5f7-41b3-b0e8-240f8236e2101033.mspx.

Enable computer and user accounts to be trusted for delegation

This policy setting specifies which users can change the **Trusted for Delegation** setting on a user or computer object in Active Directory. Delegation of authentication is a capability that is used by multi-tier client/server applications. It allows a front-end service, such as an application, to use the credentials of a client in authenticating to a back-end service, such as a database. For such authentication to be possible, both client and server must run under accounts that are trusted for delegation.

Misuse of this user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this user right to gain access to network resources as if they were a different user, which could make it difficult to determine what has happened after a security incident.

The **Enable computer and user accounts to be trusted for delegation** user right is assigned only to the **Administrators** group on domain controllers for the SSLF environment. This policy setting is configured to **Not defined** for the LC and EC environments.

Note: Although the Default Domain Controllers Policy assigns the **Administrators** group this user right, the DCBP enforces this right in the SSLF environment only because it was originally based on the MSBP. The MSBP assigns this right a null value.

Load and unload device drivers

This policy setting specifies which users can load and unload device drivers, and is necessary to load and unload Plug and Play devices.

Careless device driver management on domain controllers provides opportunities for bugs or malicious code to adversely impact the operation of the domain controllers. If the accounts that can load and unload device drivers are restricted in the DCBP to only the most trusted users, you minimize the potential for device drivers to be used to compromise domain controllers.

By default, the **Load and unload device drivers** user right is assigned to the **Print Operators** group. As mentioned earlier, creation of printer shares is not recommended on domain controllers, which removes the need for **Print Operators** to have the ability to load and unload device drivers. Therefore, the **Load and unload device drivers** user right is assigned only to the **Administrators** group in the DCBP for all three environments that are defined in this guide.

Restore files and directories

This policy setting specifies which users can circumvent file and directory permissions during the restore process. Any valid security principal could be set as the owner of an object.

An account that has the ability to restore files and directories to the file system of a domain controller can easily modify executable files. Malicious users could exploit this capability to not only render a domain controller useless, but also to compromise the security of a domain or an entire forest.

By default, the **Restore files and directories** user right is assigned to the **Server Operators** and **Backup Operators** groups. If you remove this user right from these groups and assign it only to the **Administrators** group, the likelihood of domain controller compromise by improper modifications to the file system is reduced. Therefore, the **Restore files and directories** user right is assigned only to the **Administrators** group in the DCBP for all three environments that are defined in this guide.

Shutdown the system

This policy setting specifies which users can shut down the local computer.

Malicious users with the ability to shut down domain controllers can easily initiate a denial of service (DoS) attack that could severely affect an entire domain or forest. An attacker could exploit this user right to launch an elevation of privilege attack on a domain controller's account when it restarts services. A successful elevation of privilege attack on a domain controller compromises the security of a domain or an entire forest.

By default, the **Shutdown the system** user right is assigned to the **Administrators**, **Server Operators**, **Print Operators**, and **Backup Operators** groups. In secure environments, none of these groups except **Administrators** require this right to perform administrative tasks. For this reason, the **Shutdown the system** user right is assigned only to the **Administrators** group in the DCBP for all three environments that are defined in this guide.

Security Options

Most of the security option settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 4, "The Member Server Baseline Policy." Differences between the MSBP and the DCBP policy settings are described in the following sections.

Domain Controller Settings

Table 5.5 Security Options: Domain Controller Setting Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Allow server operators to schedule tasks	Disabled	Disabled	Disabled
LDAP server signing requirements	Not defined	Not defined	Require signing
Refuse machine account password changes	Disabled	Disabled	Disabled

Domain controller: Allow server operators to schedule tasks

This policy setting determines whether members of the **Server Operators** group are allowed to submit jobs by means of the AT schedule facility.

The **Domain controller: Allow server operators to schedule tasks** setting is configured to **Disabled** in the DCBP for all three environments that are defined in this

guide. The impact of this policy setting configuration should be small for most organizations. Users, including those in the **Server Operators** group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

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

Domain controller: LDAP server signing requirements

This policy setting determines whether the LDAP server requires a signature before it will negotiate with LDAP clients. Network traffic that is neither signed nor encrypted is susceptible to man-in-the-middle attacks in which an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. For an LDAP server, an attacker could cause a client to make decisions that are based on false records from the LDAP directory.

If all domain controllers run Windows 2000 or Windows Server 2003, configure the **Domain controller: LDAP server signing requirements** setting to **Require signing**. Otherwise, leave this policy setting configured as **Not defined**, which is the DCBP configuration for the LC and EC environments. This policy setting is configured to **Require signing** in the DCBP for the SSLF environment because all computers in this environment run either Windows 2000 or Windows Server 2003.

Domain controller: Refuse machine account password changes

This policy setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. If you enable this policy setting on all domain controllers in a domain, computer account passwords on domain members will not be able to be changed and they will be more susceptible to attack.

Therefore, the **Domain controller: Refuse machine account password changes** setting is configured to **Disabled** in the DCBP for all three environments that are defined in this guide.

Network Security Settings

Table 5.6 Security Options: Network Security Settings Recommendations

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled

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

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Windows NT® hash.

For this reason, the DCBP enables the **Network security: Do not store LAN Manager hash value on next password change** setting in all three environments that are defined in this guide.

Note: Older operating systems and some third-party applications may fail if you enable this policy setting. For example, Windows 95 and Windows 98 will fail if they do not have the Active Directory Client Extension installed. Also, all accounts will be required to change their password if you enable this policy setting.

Event Log Settings

The event log settings for domain controllers are the same as those that are specified in the MSBP. For more information, see Chapter 4, "The Member Server Baseline Policy." The baseline settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers, including Directory Services Access.

Restricted Groups

As described in the previous chapter, the **Restricted Groups** setting allows you to manage the membership of groups in Windows Server 2003 with SP1 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 all three environments that are 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 5.7 Restricted Groups Recommendations

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

The **Restricted Groups** setting can be configured in Windows Server 2003 with SP1 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 that you restrict any built-in group you do not plan to use in your organization.

Note: The configuration of Restricted Groups that is described in this section is very simple. Versions of Windows XP with SP1 and SP2 as well as Windows Server 2003 support more complex designs. For more information, see the Microsoft Knowledge Base article "Updates to Restricted Groups ("Member of") Behavior of User-Defined Local Groups" at http://support.microsoft.com/default.aspx?kbid=810076.

Additional Security Settings

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

Manually Adding Unique Security Groups to User Rights Assignments

Most user rights 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 rights assignments that must be configured manually are specified in the following table.

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 you add the **Administrators** security group to any of the following deny access user rights, 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 4, "The Member Server Baseline Policy," ensure that you select the newly renamed administrator account when you add the account to any deny access user rights.

Table 5.8 Manually Added User Rights Assignments

Setting	Legacy Client	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	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on as a batch job	Support_388945a0 and Guest	Support_388945a0 and Guest	Support_388945a0 and Guest
Deny log on through Terminal Services	Built-in Administrator; all NON-operating system service accounts	Built-in Administrator; all NON-operating system service accounts	Built-in Administrator; all NON-operating system service accounts

Important: "All non-operating system service accounts" includes service accounts that are 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 with SP1 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 that you 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 that you 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 all three environments that are 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 that you 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 three environments that are 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 5.9 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 with SP1 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 all three 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 the use of Active Directory-integrated DNS in the three environments that are 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 that are used in the three 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 with SP1 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 three environments that are 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 three 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 that you increase the maximum size of the DNS service log file to at least 16 MB on the domain controllers in the three environments that are 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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 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 all three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

Terminal Services Settings

Table 5.10 Recommended Terminal Services Settings

Default	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Set client connection encryption level	High	High	High

The **Set client connection encryption level** setting determines the level of encryption for Terminal Services client connections in your environment. The **High Level** option that uses 128-bit encryption prevents an attacker from eavesdropping on Terminal Services sessions with a packet analyzer. Some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such clients, set the encryption level of the connection to send and receive data at the highest encryption level that is supported by the client.

The **Set client connection encryption level** setting is configured to **Enabled** and **High Level** encryption is selected in the DCBP for the three security environments that are defined in this guide.

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

> **Computer Configuration\Administrative Templates\Windows Components\ Terminal Services\Encryption and Security**

The three available levels of encryption are described in the following table:

Table 5.11 Terminal Services Encryption Levels

Encryption level	Description
High level	Encrypts data that is sent from client to server and from server to client with strong 128-bit encryption. Use this level when the Terminal Server runs in an environment that contains 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.
Client Compatible	Encrypts data that is sent between the client and the server at the maximum key strength that is supported by the client. Use this level when the Terminal Server runs in an environment that contains mixed or legacy clients.
Low level	Encrypts data that is sent from the client to the server with 56-bit encryption. **Important**: Data sent from the server to the client is not encrypted.

Error Reporting

Table 5.12 Recommended Error Reporting Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Turn off Windows Error Reporting	Enabled	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 and Windows Server 2003.

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 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 DCBP for all three environments that are defined in this guide.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a domain controller baseline policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These policy settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that are configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should install the operating system on hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

To create the Domain Controller Baseline Policy

You must use a computer that is configured as a domain controller to create the Domain Controller Baseline Policy. You can use either an existing domain controller or create a reference computer and use the Dcpromo tool to make the computer a domain controller. However, most organizations do not want to add a domain controller to their production environment because it may violate their security policy. If you use an existing domain

controller, make sure that you do not apply any setting to it with SCW or modify its configuration.

1. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
2. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
3. Ensure that the detected server roles are appropriate for your environment. Do not remove the File server role, because it is required for the proper operation of domain controllers.
4. Ensure that the detected client features are appropriate for your environment.
5. Ensure that the detected administrative options are appropriate for your environment.

   Note: If your environment contains domain controllers in multiple sites, ensure that **Mail-based Active Directory replication** is selected.
6. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
7. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
8. Ensure that the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.

   Note: Ensure that **Ports for System RPC Applications** is selected.
9. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
10. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
11. Include the appropriate security template (for example, EC-Domain Controller.inf).
12. Save the policy with an appropriate name (for example, Domain Controller.xml**)**.

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method offers the advantage of the ability to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you

should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   `scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>`

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\Domain
   Controller.xml" /g:"Domain Controller Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the Domain Controllers OU, and make sure to move it above the Default Domain Controllers Policy so that it receives the highest priority.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

Remember that the newly created GPO can take some time to replicate to all domain controllers, especially in environments with domain controllers in multiple sites. After you verify that the GPO has replicated successfully, you should perform a final test to ensure that the GPO applies the desired policy settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained how to harden domain controller servers that run Windows Server 2003 with SP1 in each of the three environments that are defined in this guide. Most of the policy settings that were discussed were configured and applied through Group Policy. The Domain Controller Baseline Policy (DCBP) that complements the Default Domain Controller Policy was linked to the Domain Controllers OU.

The DCBP settings will enhance overall security for domain controllers in any environment. The use of two GPOs to secure domain controllers allows the default environment to be preserved and simplifies troubleshooting.

Several of the settings that were discussed cannot be applied through Group Policy. For these settings, manual configuration details were provided.

After the domain controllers are configured for security, other server roles can be made more secure. The following chapters of this guide focus on how to secure several other specific server roles.

More Information

The following links provide additional information about topics that relate to hardening domain controllers that run Windows Server 2003 with SP1.

- For information about the Microsoft Systems Architecture: Enterprise Data Center prescriptive architecture guides, see the MSA EDC Prescriptive Architecture Guide page at www.microsoft.com/resources/documentation/msa/edc/all/solution/en-us/pak/pag/default.mspx.
- For information about how to enable anonymous access to Active Directory, see the Microsoft Knowledge Base article "Description of Dcpromo Permissions Choices" at http://support.microsoft.com/?kbid=257988.
- For information about Windows 2000 DNS, see the "Windows 2000 DNS White Paper" at www.microsoft.com/technet/prodtechnol/windows2000serv/plan/w2kdns2.mspx.
- For more information about Windows 2000 DNS, see Chapter 6 of the online version of "TCP/IP Core Networking Guide" in the Windows 2000 Server Resource Kit at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/2000/server/reskit/en-us/w2rkbook/CoreNetwork.asp.
- For more information about the changes to DNS in Windows Server 2003, see the "Changes to DNS in Windows Server 2003 Microsoft PowerPoint presentation" at http://download.microsoft.com/download/e/1/a/e1aba157-4983-480e-aae5-347b4a38ea52/ChangestoDNS.ppt.
- For more information about restricting Active Directory, see the Microsoft Knowledge Base article "Restricting Active Directory replication traffic to a specific port" at http://support.microsoft.com/?kbid=224196.
- For more information about restricting FRS replication traffic, see the Microsoft Knowledge Base article "How to restrict FRS replication traffic to a specific static port" at http://support.microsoft.com/?kbid=319553.
- For more information about the Windows Time Service, see the Windows Time Service Technical Reference at http://technet2.microsoft.com/WindowsServer/en/Library/a0fcd250-e5f7-41b3-b0e8-240f8236e2101033.mspx.
- For more information about IP spoofing, see the PDF version of the article "Introduction to IP Spoofing" at www.giac.org/practical/gsec/Victor_Velasco_GSEC.pdf.

Chapter 6: The Infrastructure Server Role

Overview

This chapter explains the policy settings you can use to harden infrastructure servers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) in the three 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.

The following table shows the names of the infrastructure server security templates for the three environments that are defined in this guide. These templates provide the policy settings for the incremental Infrastructure Server template, which in turn is used to create a new GPO that is linked to the Infrastructure Servers OU in the appropriate environment. Step-by-step instructions are provided in Chapter 2, "Windows Server 2003 Hardening Mechanisms" to help you create the OUs and Group Policies and then import the appropriate security template into each GPO.

Table 6.1 Infrastructure Server Security Templates and Policies

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-Infrastructure Server.inf	EC-Infrastructure Server.inf	SSLF-Infrastructure Server.inf

For information about policy settings in the MSBP, see Chapter 4, “The Member Server Baseline Policy.” For information on all default policy settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Audit Policy Settings

The Audit policy settings for infrastructure servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings turn on logging for the relevant security audit information on infrastructure servers.

User Rights Assignment Settings

The user rights assignments for infrastructure servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings configure user rights assignments uniformly on all infrastructure servers.

Security Options

The security options settings for infrastructure servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings configure relevant security options settings uniformly on all infrastructure servers.

Event Log Settings

The event log settings for infrastructure servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy."

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, it is recommended that access to these logs be limited to server administrators. The **Server Operators** and **Authenticated Users** groups should be removed from the Access Control List (ACL) of the **%systemroot%\system32\dhcp** folder.

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 Server 2003 Tech Center at http://technet2.microsoft.com/WindowsServer/en/Library/f7802dce-3ff9-406a-b3e6-c0c6b3ed49411033.mspx.

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 Dynamic Host Configuration Protocol page in the Windows 2000 Server Resource Kit at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cncb_dhc_klom.asp.

Note: The 80/20 Rule described in the Windows 2000 Server Resource Kit also applies to DHCP services in Windows Server 2003 with SP1.

Securing Well-Known Accounts

Windows Server 2003 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 all three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These policy settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should install the operating system on hardware that is

similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the server policy creation steps you will probably remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the infrastructure server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.
4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment—for example, the DHCP server and WINS server roles.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. Include the appropriate security template (for example, EC-Infrastructure Server.inf).
15. Save the policy with an appropriate name (for example, Infrastructure Server.xml).

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method allows you to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform
   /p:"C:\Windows\Security\msscw\Policies\Infrastructure.xml"
   /g:"Infrastructure Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired policy settings. To complete this procedure, confirm that the appropriate policy settings were made and that functionality is not affected.

Summary

This chapter explained the policy settings that can be used for DHCP and WINS servers that run Windows Server 2003 with SP1 in the three environments that are defined in this guide. Most of the settings for these roles are applied through the MSBP. The primary goal of creating an Infrastructure Policy object for the DHCP and WINS servers is to

enable the necessary services for these roles to fully function and keep them well secured.

Although the MSBP provides a great level of security, this chapter also discussed other considerations for the infrastructure server roles. Primarily, these considerations included the generation of log files.

More Information

The following links provide additional information about topics that relate to hardening infrastructure servers that run Windows Server 2003 with SP1.

- For information about how DHCP logging has changed in Windows Server 2003, see the Microsoft Knowledge Base article "Changes in Windows Server 2003 DHCP Logging" at http://support.microsoft.com/?kbid=328891.
- For more information about DHCP, see the Dynamic Host Configuration Protocol page at www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cncb_dhc_klom.asp.
- For more information about WINS, see the "Windows 2000 Server Windows Internet Naming Service (WINS) Overview" at www.microsoft.com/technet/archive/windows2000serv/evaluate/featfunc/nt5wins.mspx.
- For information about installing WINS in Windows Server 2003, see the "Install and Manage WINS Servers" page at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a29d0a59-8bdd-4a82-a980-b53bd72fcb0e.mspx.

Chapter 7: The File Server Role

Overview

It can be a challenge to harden file server computers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1), 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.

The following table shows the names of the file server security templates for the three environments that are defined in this guide. These templates provide the settings for the incremental File Server template, which in turn is used to create a new GPO that is linked to the File Servers OU in the appropriate environment. Step-by-step instructions are provided in Chapter 2, "Windows Server 2003 Hardening Mechanisms" to help you create the OUs and Group Policies and then import the appropriate security template into each GPO.

Table 7.1 File Server Security Templates

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-File Server.inf	EC-File Server.inf	SSLF-File Server.inf

For information about policy settings in the MSBP, see Chapter 4, “The Member Server Baseline Policy.” For information on all default policy settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Audit Policy Settings

The Audit policy settings for file servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see

Chapter 4, "The Member Server Baseline Policy." The MSBP settings activate security audit information logging on all file servers.

User Rights Assignments

The user rights assignment settings for file servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings uniformly configure all appropriate user rights assignments on all file servers.

Security Options

The security options settings for file servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings uniformly configure all relevant security option settings on all file servers.

Event Log Settings

The event log settings for file servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy."

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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 all three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should install the operating system on hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

To create the file server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.
4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.

5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment—for example, the File server role.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. Include the appropriate security template (for example, EC-File Server.inf).
15. Save the policy with an appropriate name (for example, File Server.xml**)**.

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use the SCW GUI to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method allows you to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more information about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\File Server.xml" /g:"File Server Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained the policy settings that can be used to configure file servers that run Windows Server 2003 with SP1 in the three environments that are defined in this guide. Most of the policy settings are applied through a Group Policy object (GPO) that was designed to complement the MSBP. GPOs can be linked to the appropriate organizational units (OUs) that contain the file servers to provide additional security.

Some policy settings cannot be applied through Group Policy. For these policy settings, manual configuration details were provided.

More Information

The following links provide additional information about topics that relate to hardening file servers that run Windows Server 2003 with SP1.

- For more information about file servers, see "Technical Overview of Windows Server 2003 File Services" at www.microsoft.com/windowsserver2003/techinfo/overview/file.mspx.
- For more information about DFS and FRS, see the Distributed File System Technology Center at www.microsoft.com/windowsserver2003/technologies/storage/dfs/default.mspx.

Chapter 8: The Print Server Role

Overview

This chapter focuses on how to harden print servers that run Microsoft® Windows Server™ 2003 with SP1, 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.

The following table shows the names of the print server security templates for the three environments that are defined in this guide. These templates provide the policy settings for the incremental Print Server template, which in turn is used to create a new GPO that is linked to the Print Servers OU in the appropriate environment. Step-by-step instructions are provided in Chapter 2, "Windows Server 2003 Hardening Mechanisms" to help you create the OUs and Group Policies and then import the appropriate security template into each GPO.

Table 8.1 Print Server Security Templates for All Three Environments

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-Print Server.inf	EC-Print Server.inf	SSLF-Print Server.inf

For information about settings in the MSBP, see Chapter 4, “The Member Server Baseline Policy.” For information on all default settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

Note: Print servers that are secured with the SSLF-Print Server.inf security template can only be accessed reliably by client computers that are secured with compatible settings. See the *Windows XP Security Guide* for information about how to secure client computers with SSLF-compatible settings.

Audit Policy Settings

The Audit policy settings for print servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings activate logging for security audit information on all print servers.

User Rights Assignments

The user rights assignment settings for print servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings uniformly configure user rights assignments on all print servers.

Security Options

Most security option settings for print servers in the three environments that are defined in this guide are configured through the MSBP. For more information about MSBP, see Chapter 4, "The Member Server Baseline Policy." Differences between the MSBP and the Print Server Group Policy are described in the following section.

Microsoft network server: Digitally sign communications (always)

Table 8.2 Recommended Settings for Digitally Signing Communications (Always)

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Microsoft network server: Digitally sign communications (always)	Disabled	Disabled	Disabled

This policy setting determines whether packet signing is required by the SMB server component. The SMB protocol provides the basis for Microsoft file and print sharing and many other network operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports SMB packet digital signing. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

Although the **Microsoft network server: Digitally sign communications (always)** setting is disabled by default, the MSBP enables this setting for servers in the SSLF environment, which allows users to print but not view the print queue. Users who attempt to view the print queue will see an access denied message.

The **Microsoft network server: Digitally sign communications (always)** setting is configured to **Disabled** for print servers in all three environments that are defined in this guide.

Event Log Settings

The event log settings for print servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy."

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

Microsoft Windows Server 2003 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 all three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

To create the print server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.
4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment, for example the Print server role.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.

14. Include the appropriate security template (for example, EC-Print Server.inf).
15. Save the policy with an appropriate name (for example, Print Server.xml**)**.

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method offers the advantage of the ability to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   `scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>`

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\Print
   Server.xml" /g:"Print Server Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained the policy settings that can be used for print servers that run Windows Server 2003 with SP1 for the three environments that are defined in this guide. Most of the policy settings are applied through a Group Policy object (GPO) that was designed to complement the MSBP. GPOs can be linked to the appropriate organizational units (OUs) that contain the print servers to provide additional security.

Some policy settings that were discussed cannot be applied through Group Policy. For these policy settings, manual configuration details were provided.

More Information

The following links provide additional information about topics that relate to hardening print servers that run Windows Server 2003 with SP1.

- For an overview of print servers, see the "Technical Overview of Windows Server 2003 Print Services," which is available for download at www.microsoft.com/windowsserver2003/techinfo/overview/print.mspx.
- For more information about print servers, see "What's New in File and Print Services" at www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx.

Chapter 9: The Web Server Role

Overview

This chapter provides guidance that will help you harden the Web servers in your environment that run Microsoft® Windows Server™ 2003 with SP1. 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.

You should consider implementation of the settings that are 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.

The following table shows the names of the Web server security templates for the three environments that are defined in this guide. These Web server security templates provide the policy settings for the incremental Web Server template. You can use this template to create a new GPO that is linked to the Web Servers OU in the appropriate environment. Chapter 2, "Windows Server 2003 Hardening Mechanisms," provides step-by-step instructions to help you create the OUs and Group Policies and then import the appropriate security template into each GPO.

Table 9.1 IIS Server Security Templates

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
LC-Web Server.inf	EC-Web Server.inf	SSLF-Web Server.inf

For information about all default setting configurations, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

This guide illustrates how to secure IIS with minimal features installed and enabled. If you plan to use additional features in IIS you may need to need to adjust some of the security settings. If you install additional services such as SMTP, FTP, or NNTP, you will need to adjust the provided templates and policies.

The online article "IIS and Built-in Accounts (IIS 6.0)" at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/3648346f-e4f5-474b-86c7-5a86e85fa1ff.mspx explains the accounts that different features of IIS use and the privileges that are required by each. To implement more secure settings on Web servers that host complex applications, you may find it useful to review the complete IIS 6.0 Documentation at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/848968f3-baa0-46f9-b1e6-ef81dd09b015.mspx.

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 2, 3, and 4 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 rights assignments so that they can be controlled by local policy rather than the domain–based GPO. In other words, you should configure the following user rights 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 need to enable will determine whether you will need to also reconfigure other user rights assignment settings to **Not defined**.

Audit Policy Settings

The Audit policy settings for IIS servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that all the relevant security audit information is logged on all IIS servers.

User Rights Assignments

The user rights assignment settings for IIS servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that all the relevant security audit information is logged on all IIS servers.

Security Options

The security option settings for IIS servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that all the relevant security options are uniformly configured on all IIS servers.

Event Log Settings

The event log settings for IIS servers in the three environments that are defined in this guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that the appropriate event log settings are uniformly configured on all IIS servers in an organization.

Additional Security Settings

When IIS is installed on a computer that runs Windows Server 2003 with SP1, 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:

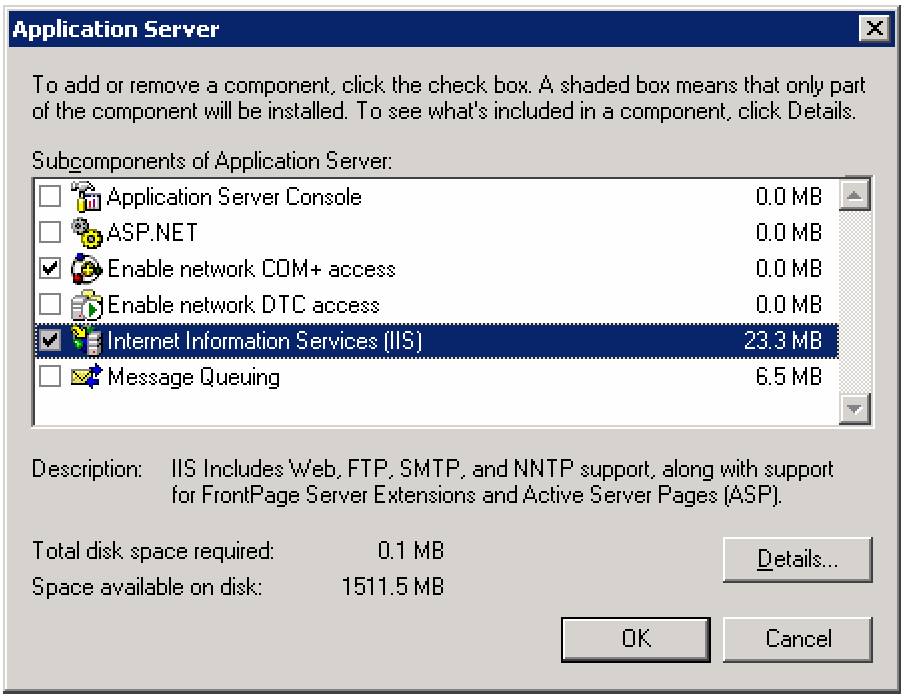

Figure 9.1 Application Server dialog box with list of subcomponents

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

Table 9.2 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.
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:

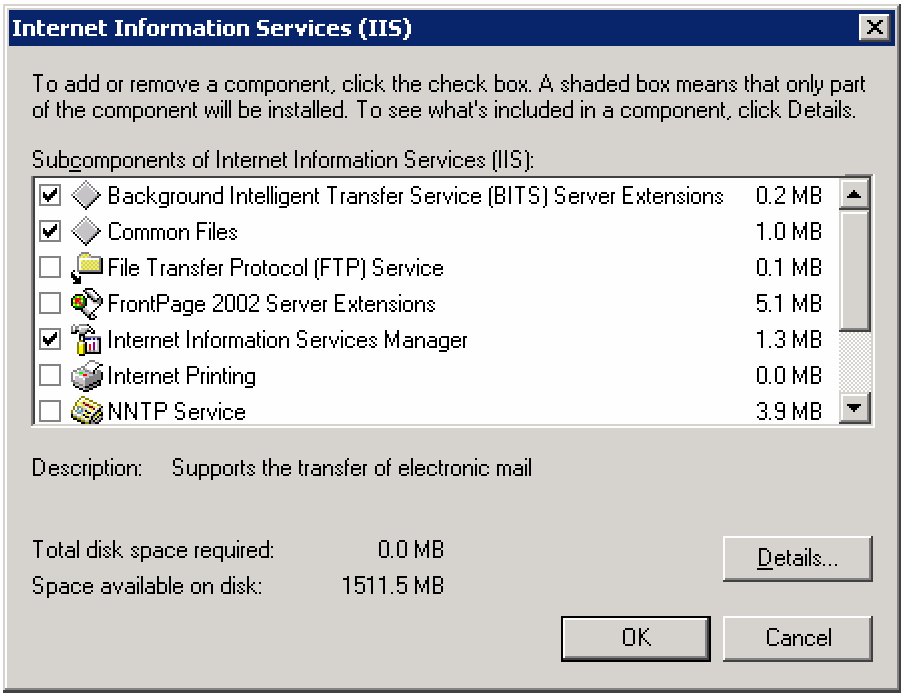

Figure 9.2 IIS dialog box with list of subcomponents

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

Table 9.3 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.

Component name in UI	Setting	Setting logic
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:

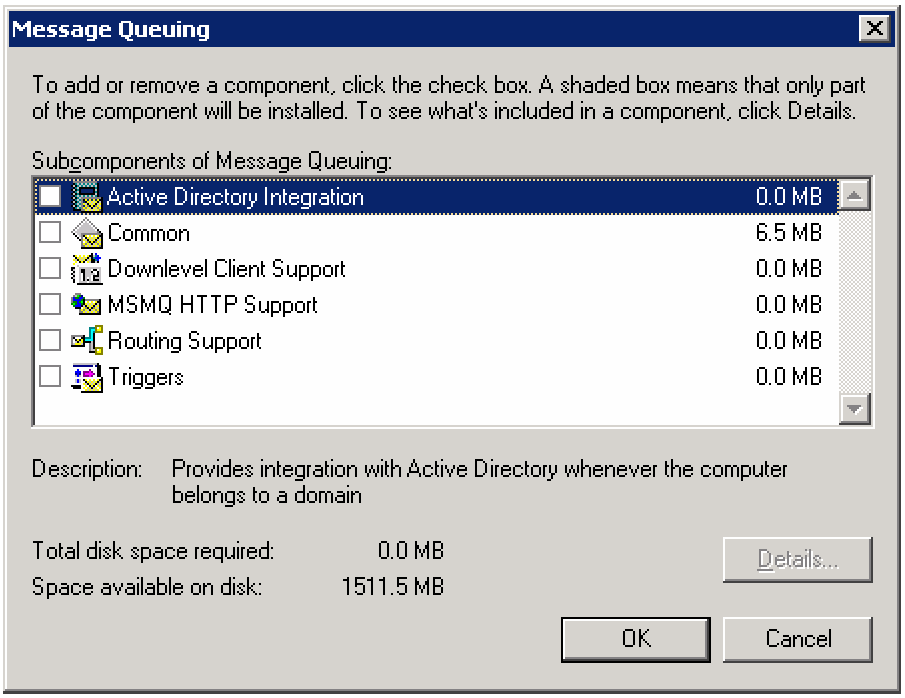

Figure 9.3 Message Queuing dialog box with list of subcomponents

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

Table 9.4 Recommended Message Queuing Subcomponents Settings

Component name in UI	Installation option	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.
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:

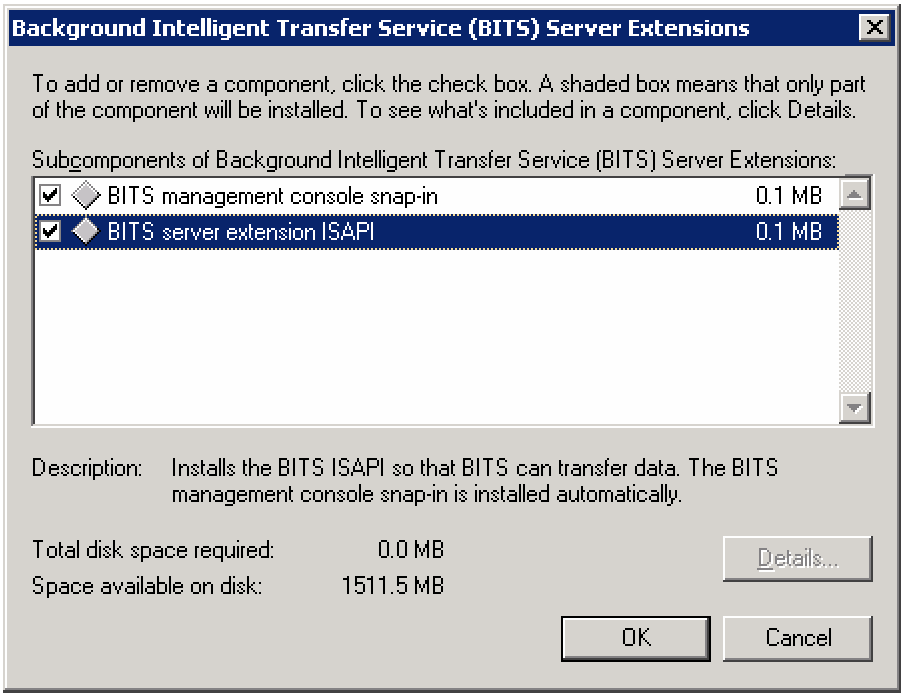

Figure 9.4 BITS Server Extensions with list of subcomponents

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

Table 9.5 Recommended BITS Server Extensions Subcomponents Settings

Component name in UI	Installation option	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:

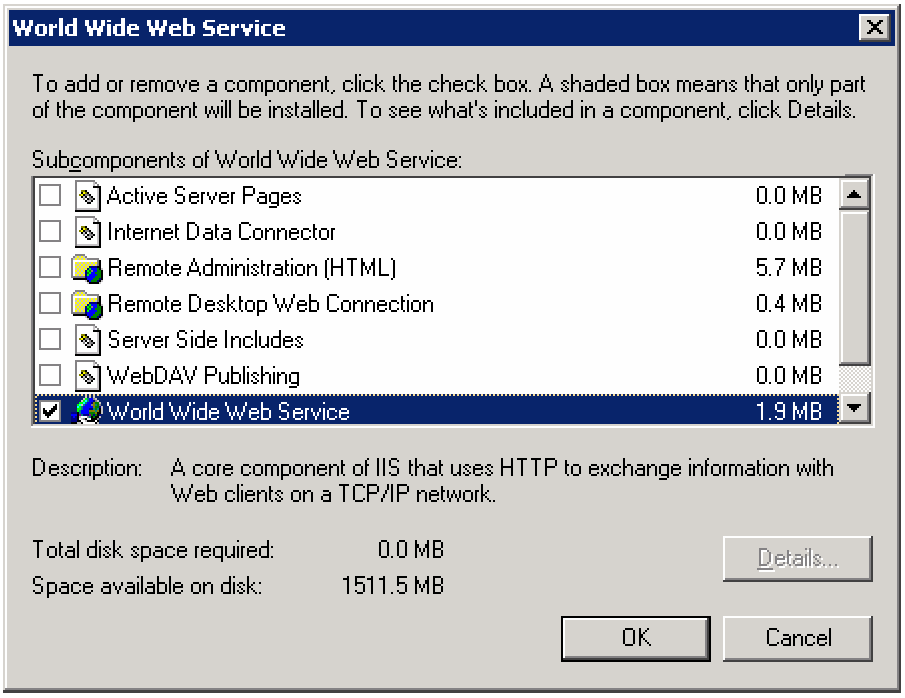

Figure 9.5 World Wide Web Service dialog box with list of subcomponents

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

Table 9.6 Recommended World Wide Web Service Subcomponent Settings

Component name in UI	Installation option	Setting logic
Active Server Pages	Disabled	Provides support for ASP. Disable this component when no Web sites or applications on IIS servers use ASP, or disable it 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.

Component name in UI	Installation option	Setting logic
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. You should 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 three 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 9.7 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 operating system is installed).

In the three 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 with SP1 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 with SP1 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 three 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 should be applied to the different file types on an IIS server. The different file types can be grouped in separate folders to simplify the application of NTFS permissions.

Table 9.8 Recommended NTFS Permissions Settings

File type	Recommended NTFS permissions
CGI files (.exe, .dll, .cmd, .pl)	Everyone (execute) Administrators (full control) System (full control)
Script files (.asp)	Everyone (execute) Administrators (full control) System (full control)
Include files (.inc, .shtm, .shtml)	Everyone (execute) Administrators (full control) System (full control)
Static content (.txt, .gif, .jpg, .htm, .html)	Everyone (read-only) Administrators (full control) System (full control)

Setting IIS Web Site Permissions

IIS examines Web site permissions to determine the types of action that can occur within a Web site, such as script source access or directory browsing. You should assign Web

site permissions to provide additional security for Web sites on IIS servers in the three environments that are defined in this guide.

Web site permissions can be used in conjunction with NTFS permissions, and can be configured for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access a Web site that runs on an IIS server. Web site permissions can be applied 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 9.9 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.
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 that IIS logging be enabled on IIS servers in the three environments that are defined in this guide.

Separate logs can be created 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.

The MMC IIS Manager snap-in can be used to configure the log file format, the log schedule, and the exact information to be logged. To limit the size of the logs, you should 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 non-system 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 the IIS Centralized Binary Logging (IIS6.0) page at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/13a4c0b5-686b-4766-8729-a3402da835f1.mspx.

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 Rights Assignments

Most user rights 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 rights 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 any of the listed deny access user rights, 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 4, "The Member Server Baseline Policy." When you add the Administrator account to any user rights, ensure that the renamed account is specified.

Table 9.10 Manually Added User Rights Assignments

Member server default	Legacy Client	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	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts

Important: "All non-operating system service accounts" includes service accounts that are 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 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 three 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 at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use on hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

To create the IIS server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.
4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment—for example the Application server and Web server roles.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.

12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. Include the appropriate security template (for example, EC-IIS Server.inf).
15. Save the policy with an appropriate name (for example, IIS Server.xml).

Note: The MSBP disables several other IIS-related services, including FTP, SMTP, and NNTP. The Web Server policy must be modified if any of these services are to be enabled on IIS servers in any of the three environments that are defined in this guide.

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method allows you to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   `scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>`

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\IIS
   Server.xml" /g:"IIS Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained the policy settings that can be used to harden IIS servers that run Windows Server 2003 with SP1 in the three environments that are defined in this guide. Most of the settings are applied through a Group Policy object (GPO) that was designed to complement the MSBP. GPOs can be linked to the appropriate organizational units (OUs) that contain the IIS servers to provide additional security.

Some of the settings that were discussed cannot be applied through Group Policy. For these settings, manual configuration details were provided.

More Information

The following links provide additional information about topics that relate to hardening IIS–based Web servers that run Windows Server 2003 with SP1.

- For information about how to enable logging in IIS, see the Microsoft Knowledge Base article "How to enable logging in Internet Information Services (IIS)" at http://support.microsoft.com/?kbid=313437.
- Additional information about logging is available on the Enable Logging (IIS 6.0) page at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/d29207e8-5274-4f4b-9a00-9433b73252d6.mspx.
- For information about how to log site activity, see the Logging Site Activity (IIS 6.0) page at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/ab7e4070-e185-4110-b2b1-1bcac4b168e0.mspx.
- For information about extended logging, see the Customizing W3C Extended Logging (IIS 6.0) page at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/96af216b-e2c0-428e-9880-95cbd85d90a1.mspx.
- For information about centralized binary logging, see the Centralized Binary Logging in IIS 6.0 (IIS 6.0) page on Microsoft.com at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/b9cdc076-403d-463e-9a36-5a14811d34c7.mspx.
- For information about remote logging, see the Remote Logging (IIS 6.0) page at www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/a6347ae3-39d1-4434-97c9-5756e5862c61.mspx.
- For additional information about IIS 6.0, see the Internet Information Services page at www.microsoft.com/WindowsServer2003/iis/default.mspx.

Chapter 10: The IAS Server Role

Overview

This chapter provides recommendations and resources that will help you harden Internet Authentication Service (IAS) servers in your environment that run Microsoft Windows Server 2003 with SP1. 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. IAS can be used to authenticate users in databases on Windows Server 2003, 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 2, "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 4, “The Member Server Baseline Policy.” For information on all default setting configurations, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

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.

Audit Policy

Audit policy settings for IAS servers in the EC environment are configured through the MSBP. For more information about the MSBP, see Chapter 4, “The Member Server

Baseline Policy." The MSBP settings ensure that all the relevant security audit information is logged on all IAS servers in an organization.

User Rights Assignments

User rights assignments for IAS servers in the EC environment are also configured through the MSBP. For more information about the MSBP, see Chapter 4, “The Member Server Baseline Policy." The MSBP settings ensure that appropriate access to IAS servers is uniformly configured throughout an organization.

Security Options

The security options settings for IAS servers in the EC environment are also configured through the MSBP. For more information about the MSBP, see Chapter 4, “The Member Server Baseline Policy." The MSBP settings ensure that appropriate access to IAS servers is uniformly configured across an enterprise.

Event Log

The event log settings for IAS servers in the EC environment are also configured through the MSBP. For more information about the MSBP, see Chapter 4, “The Member Server Baseline Policy."

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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, the built-in Administrator account should be renamed and the description altered 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 that are 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 The Services and Service Accounts Security Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, the installation should be on hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the server policy creation steps you will probably remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the IAS server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.

4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment, for example the **IAS server (RADIUS)** role.
7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. Include the appropriate security template (for example, EC-IAS Server.inf).
15. Save the policy with an appropriate name (for example, IAS Server.xml).

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method allows you to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more information about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   `scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>`

   and then press ENTER. For example:

   ```
   scwcmd transform /p:"C:\Windows\Security\msscw\Policies\IAS
   Server.xml" /g:"IAS Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click Windows Firewall.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings wee made and that functionality is not affected.

Summary

This chapter explained the settings that can be used to harden IAS servers that run Windows Server 2003 with SP1 in the Enterprise Client environment that is defined in this guide. These settings may also work in the other environments defined in this guide, but they have not been tested or validated. The settings were configured and applied through a Group Policy object (GPO) that was designed to complement the MSBP. GPOs can be linked to the appropriate organizational units (OUs) that contain the IAS servers in your organization to provide additional security.

More Information

The following links provide additional information about topics that relate to hardening IAS servers that run Windows Server 2003 with SP1.

- For more information about IAS, see the Understanding IAS page at http://technet2.microsoft.com/WindowsServer/en/Library/ab4eeeb2-b0aa-4b4a-a959-3902b2b3f1af1033.mspx.
- For more information about IAS and security, see the Internet Authentication Service page at http://technet2.microsoft.com/WindowsServer/en/Library/d98eb914-258c-4f0b-ad04-dc4db9e4ee631033.mspx.
- For information about IAS, firewalls, and Windows Server 2003, see the IAS and firewalls page at www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/518e70a9-9e7a-422b-a13f-f3193d4fd215.mspx.
- For more information about RADIUS, see the RFC memo "RADIUS Accounting" at www.ietf.org/rfc/rfc2866.txt.

Chapter 11: The Certificate Services Server Role

Overview

This chapter provides guidance that will help you harden servers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) 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 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, which is available at http://go.microsoft.com/fwlink/?LinkId=14843.

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 2, "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 4, “The Member Server Baseline Policy.” For information on all default settings, see the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, which is available at http://go.microsoft.com/fwlink/?LinkId=15159.

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 9, "The Web Server Role" in this

guide. If you install IIS on your CAs, the security configuration template that was developed for Chapter 9 must be applied to your Certificate Services servers before you configure the prescribed settings that are described in this chapter.

Note: In simplified environments, the issuing CA server can be used to host the Web server, the CA certificate, and the CRL download points. However, you should 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 that you not install IIS on the root CA server. If possible, you should 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.

Audit Policy Settings

Audit policy settings for Certificate Services servers in the Enterprise Client environment guide are configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that all the relevant security audit information is logged on all Certificate Services servers.

User Rights Assignments

User rights assignment settings for Certificate Services servers in the Enterprise Client environment are also configured through the MSBP. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The MSBP settings ensure that appropriate access to Certificate Services servers is uniformly configured across an enterprise.

Security Options

The Security Options section of Group Policy is used to enable or disable security settings for computers, such as digital signing of data, Administrator and Guest account names, floppy disk drive and CD-ROM drive access, driver installation behavior, and logon prompts.

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

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

The following table includes the recommended security options setting for the Certificate Services server role in the Enterprise Client environment. Detailed information about the setting is provided in the text that follows the table.

Table 11.1 Recommended Security Options Settings

Setting	Enterprise Client
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

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

This policy setting determines whether the Transport Layer Security/Secure Sockets Layer (TLS/SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, support for this cipher suite means that the provider only supports the TLS protocol as a client and a server (if applicable).

The TLS/SSL Security Provider uses the following algorithms:

- The Triple Data Encryption Standard (3DES) encryption algorithm for the TLS traffic encryption.
- The Rivest, Shamir, and Adelman (RSA) public key algorithm for the TLS key exchange and authentication. (RSA is a public-key encryption technology that was developed by RSA Data Security, Inc.)
- The SHA-1 hashing algorithm for the TLS hashing requirements.

For the Encrypting File System Service (EFS), the TLS/SSL Security Provider supports only the Triple DES encryption algorithm to encrypt file data that is stored in the Windows NTFS file system. By default, in Windows 2000 and Windows XP with no service packs, EFS uses the DESX algorithm to encrypt file data, however in Windows XP SP1 and later, and Windows Server 2003, the default algorithm is Advanced Encryption Standard (AES) using a 256-bit key.

If you enable this policy setting, computers that fulfill this server role in your environment will use the most powerful algorithms that are available for digital encryption, hashing, and signing. Use of these algorithms minimizes risk because they limit the ability of an unauthorized user to compromise digitally encrypted or signed data.

For these reasons, the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting is configured to **Enabled** for the Enterprise Client environment.

Note: Client computers that have this policy setting enabled will be unable to communicate through digitally encrypted or signed protocols with servers that do not support these algorithms. Network client computers that do not support these algorithms will not be able to use servers that require the algorithms for network communications. For example, many Apache–based Web servers are not configured to support TLS. If you enable this setting you must also configure Internet Explorer to use TLS. To do so, open the **Internet Options** dialog box from the Internet Explorer **Tools** menu, click the **Advanced** tab on the **Internet Options** dialog box, scroll towards the bottom of the **Settings** list, and then click the **Use TLS 1.0** checkbox. It is also possible to configure this functionality through Group Policy or with the Internet Explorer Administrators Kit.

Event Log Settings

The event log settings for Certificate Services servers in the Enterprise Client environment are configured through the MSBP. For more information on the MSBP, see Chapter 4, "The Member Server Baseline Policy."

Additional Registry Entries

Additional registry entries were created for the EC-CA Server.inf template file. These entries are not defined within the Administrative Template (.adm) files for the Enterprise

Client environment as defined in this guide. The .adm files define the system policies and restrictions for the desktop, shell, and security settings for Windows Server 2003 with SP1.

The additional registry entries are configured within the security template to automate their implementation. If the Incremental Certificate Services Group Policy for this environment is removed, its settings are not automatically removed and must be manually changed with a registry editing tool such as Regedt32.exe.

You can configure the registry entries in Windows Server 2003 at the following location within the Group Policy Object Editor:

MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

Additional Security Settings

The following ACLs are suggested and can be assigned through Group Policy. However, these ACLs are not included in the security templates that are provided with this guide because the path for the database and logs will 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–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 shown in the following table.

Table 11.2 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 11.3 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 will 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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, the built-in Administrator account should be renamed and the description altered 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 The Services and Service Accounts Security Planning Guide at http://go.microsoft.com/fwlink/?LinkId=41311.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the server policy creation steps you will probably remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the Certificate Services server policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Join the computer to the domain, which will apply all security settings from parent OUs.
4. Install and configure only the mandatory applications that will be on every server that shares this role. Examples include role-specific services, software and management agents, tape backup agents, and antivirus or antispyware utilities.
5. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
6. Ensure that the detected server roles are appropriate for your environment—for example the Certificate Services role.

7. Ensure that the detected client features are appropriate for your environment.
8. Ensure that the detected administrative options are appropriate for your environment.
9. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.
10. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
11. Ensure the **Skip this section** checkbox is unchecked in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall.
12. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
14. Include the appropriate security template (for example, EC-CA Server.inf).
15. Save the policy with an appropriate name (for example, Certificate Services.xml).

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Two options are available to test the policy. You can use the native SCW deployment facilities, or deploy the policies through a GPO.

When you start to author your policies, you should consider using the native SCW deployment facilities. You can use SCW to push a policy to a single server at a time, or use Scwcmd to push the policy to a group of servers. The native deployment method allows you to easily roll back deployed policies from within SCW. This capability can be very useful when you make multiple changes to your policies during the test process.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Convert and Deploy the Policy

After you thoroughly test the policy, complete the following steps to convert it into a GPO and deploy it:

1. At the command prompt, type the following command:

   ```
   scwcmd transform /p:<PathToPolicy.xml> /g:<GPODisplayName>
   ```

   and then press ENTER. For example:

   ```
   scwcmd transform
   /p:"C:\Windows\Security\msscw\Policies\Certificate
   Services.xml" /g:"Certificate Services Policy"
   ```

   Note: The information to be entered at the command prompt shows on more than one line here because of display limitations. This information should all be entered on one line.

2. Use the Group Policy Management Console to link the newly created GPO to the appropriate OU.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that the GPO applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

This chapter explained the policy settings that can be used to harden Certificate Services servers that run Windows Server 2003 with SP1 in the Enterprise Client environment as defined in this guide. The settings are configured and applied through a Group Policy object (GPO) that complements the MSBP. GPOs can be linked to the appropriate organizational units (OUs) that contain the Certificate Services servers to provide additional security.

More Information

The following links provide additional information about topics that relate to hardening servers that run Windows Server 2003 with SP1 and Certificate Services.

- For a good introduction to public key infrastructure (PKI) concepts and the features of Windows 2000 certificate services, see "An Introduction to the Windows 2000 Public Key Infrastructure" at www.microsoft.com/technet/archive/windows2000serv/evaluate/featfunc/pkiintro.mspx.
- For more detailed information about PKI functionality in Windows Server 2003 and Windows XP, see "PKI Enhancements in Windows XP Professional and Windows Server 2003" at www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx.
- For more background information about key PKI concepts, see the Public Key Infrastructure page at http://technet2.microsoft.com/WindowsServer/en/Library/32aacfe8-83af-4676-a45c-75483545a9781033.mspx.

Chapter 12: The Bastion Host Role

Overview

This chapter focuses on how to harden bastion hosts that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) 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 will help secure bastion hosts in any environment. The steps that are included in this chapter will 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.

Bastion Host Local Policy

The server roles that are described earlier in this guide used Group Policy to configure servers. Group Policy cannot be applied to bastion host servers because they are configured as stand-alone hosts that do not belong to an Active Directory® directory service domain. Because they are exposed and not protected by other devices, only one level of guidance is prescribed for bastion host servers in the three environments that are defined in this guide. The security settings that are described in this chapter are based on the Member Server Baseline Policy (MSBP) for the SSLF environment that is defined in Chapter 4, "The Member Server Baseline Policy." The settings are included in a security template that must be applied to the Bastion Host Local Policy (BHLP) of each bastion host.

Table 12.1 Bastion Host Server Security Templates

Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
SSLF-Bastion Host.inf	SSLF-Bastion Host.inf	SSLF-Bastion Host.inf

Audit Policy Settings

The BHLP Audit policy settings for bastion hosts are included in the SSLF-Bastion Host.inf file. These settings are the same as those specified in the SSLF-Member Server Baseline.inf file. For more information about the MSBP, see Chapter 4, "The Member Server Baseline Policy." The BHLP settings ensure that all relevant security audit information is logged on all bastion host servers.

User Rights Assignments

The SSLF-Bastion Host.inf file includes the BHLP user rights assignments for bastion hosts. These policy settings are based on those that are specified in the SSLF-Member Server Baseline.inf file in Chapter 4, "The Member Server Baseline Policy." The information in the following table summarizes the differences between the BHLP and the MSBP. Detailed information is provided in the text that follows the table.

Table 12.2 Recommended User Rights Assignments Setting

User Rights assignment	Setting
Deny access to this computer from the network	ANONOYMOUS LOGON; Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts

Deny access to this computer from the network

Note: ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0, Guest, and all NON-operating system service accounts are not included in the security template. These accounts and groups have unique security identifier (SIDs). Therefore, you need to add them manually to the BHLP.

This policy setting determines which users cannot access a computer over the network. It denies a number of network protocols, including server message block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), HTTP, and Component Object Model Plus (COM+). This policy setting overrides the **Access this computer from the network** setting when a user account is subject to both policies. If you configure this user right for other groups, you could limit the ability of users to perform delegated administrative tasks in your environment.

In Chapter 4, "The Member Server Baseline Policy," this guide recommends that you include the **Guests** group in the list of users and groups that are assigned this user right to provide the highest possible level of security possible. However, the IUSR account that is used for anonymous access to IIS is a member of the **Guests** group by default.

The **Deny access to this computer from the network** setting is configured to include ANONOYMOUS LOGON, Built-in Administrator, Support_388945a0, Guest, and all NON-Operating System service accounts for bastion hosts in the SSLF environment that is defined in this guide.

Security Options

The BHLP security options settings for bastion hosts are the same as those specified in the SSLF-Member Server Baseline.inf file in Chapter 4, "The Member Server Baseline

Policy." These BHLP settings ensure that all relevant security options are uniformly configured on all bastion host servers.

Event Log Settings

The BHLP event log settings for bastion hosts are the same as those specified in the SSLF-Member Server Baseline.inf file in Chapter 4, "The Member Server Baseline Policy." These BHLP settings ensure that all relevant event log settings are uniformly configured on all bastion host servers.

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 that should be considered. 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 Rights Assignments

Most user rights 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 Server 2003 domains. The user rights 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 4, "The Member Server Baseline Policy." When you add the Administrator account to a user right, ensure that you specify the renamed account.

Table 12.3 Manually Added User Rights Assignments

Setting	Legacy Client	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	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts

Important: "All non-operating system service accounts" includes service accounts that are 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 with SP1 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 are Guest and Administrator.

By default, the Guest account is disabled on member servers and domain controllers. This configuration should not be changed. Many variations of malicious code use the built-in Administrator account in an initial attempt to compromise a server. Therefore, you should 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 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 12.4 Recommended Error Reporting Settings

Setting	Legacy Client	Enterprise Client	Specialized Security – Limited Functionality
Turn off Windows Error Reporting	Enabled	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 and Windows Server 2003.

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 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 all three environments that are defined in this guide.

Creating the Policy Using SCW

To deploy the necessary security settings, you must use both the Security Configuration Wizard (SCW) and the security templates that are included with the downloadable version of this guide to create a server policy.

When you create your own policy, be sure to skip the "Registry Settings" and “Audit Policy” sections. These settings are provided by the security templates for your chosen environment. This approach is necessary to ensure that the policy elements that are provided by the templates take precedence over those that would be configured by SCW.

You should use a new installation of the operating system to begin your configuration work, which helps ensure that there are no legacy settings or software from previous configurations. If possible, you should use hardware that is similar to the hardware that is used in your deployment to help ensure as much compatibility as possible. The new installation is called a *reference computer*.

During the server policy creation steps you will probably remove the File server role from the list of detected roles. This role is commonly configured on servers that do not require it and could be considered a security risk. To enable the File server role for servers that require it, you can apply a second policy later in this process.

To create the bastion host policy

1. Create a new installation of Windows Server 2003 with SP1 on a new reference computer.
2. Install the Security Configuration Wizard component on the computer through Control Panel, Add/Remove Programs, Add/Remove Windows Components.
3. Install and configure only the mandatory applications that will be on every bastion host. Examples include antivirus or antispyware utilities.
4. Launch the SCW GUI, select **Create new policy**, and point it to the reference computer.
5. Ensure that the detected server roles are appropriate for the bastion host (for example, Web server). Remove all other server roles.
6. Ensure that the detected client features are appropriate for your environment. Remove all unnecessary client features. For example, you should remove the **Microsoft networking client** and the **DHCP client** features to reduce the server’s attack surface.
7. For maximum protection, remove all administrative options except for Windows Firewall. Additional options will increase the manageability of the bastion host, but will also increase its attack surface. Carefully weigh the benefits of any options that are not crucial to the proper operation of the bastion host against the potential security risks they might pose.
8. Ensure that any additional services that are required by your baseline, such as backup agents or antivirus software, are detected.

9. Decide how to handle unspecified services in your environment. For extra security, you may wish to configure this policy setting to **Disable**. You should test this configuration before you deploy it to your production network because it may cause problems if your production servers run additional services that are not duplicated on your reference computer.
10. Ensure the **Skip this section** checkbox is unselected in the "Network Security" section, and then click **Next**. The appropriate ports and applications identified earlier are configured as exceptions for Windows Firewall. Uncheck all ports except those that are required for the bastion host function.
11. In the "Registry Settings" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
12. In the "Audit Policy" section, click the **Skip this section** checkbox and then click **Next**. These policy settings are imported from the supplied INF file.
13. Include the appropriate security template (for example, SSLF-Bastion Host.inf).
14. Save the policy with an appropriate name (for example, Bastion Host.xml).

Test the Policy Using SCW

After you create and save the policy, Microsoft strongly recommends that you deploy it to your test environment. Ideally, your test servers will have the same hardware and software configuration as your production servers. This approach will allow you to find and fix potential problems, such as the presence of unexpected services that are required by specific hardware devices.

Because computers in the bastion host role are not connected to a domain, you must apply the settings with SCW. You cannot use Group Policy without a domain.

The policy is tested to ensure that the application of this policy to the target servers will not adversely affect their critical functions. After you apply the configuration changes, you should begin to verify the core functionality of the computer. For example, if the server is configured as a certification authority (CA), ensure that clients can request and obtain certificates, download a certificate revocation list, and so on.

When you are confident in your policy configurations, you can use Scwcmd as shown in the following procedure to convert the policies to GPOs.

For more details about how to test SCW policies, see the Deployment Guide for the Security Configuration Wizard at http://technet2.microsoft.com/WindowsServer/en/Library/5254f8cd-143e-4559-a299-9c723b3669461033.mspx and the Security Configuration Wizard Documentation at http://go.microsoft.com/fwlink/?linkid=43450.

Implement the Policy

After you thoroughly test the policy, complete the following steps to implement it:

1. Launch the SCW GUI.
2. Select **Apply an existing security policy**.
3. Select the XML file that you created earlier. For example, Bastion Host.xml.
4. Complete the SCW wizard to apply the settings.

Note that if the SCW security policy file contains Windows Firewall settings, Windows Firewall must be active on the local computer for this procedure to complete successfully. To verify that Windows Firewall is active, open Control Panel and then double-click **Windows Firewall**.

You should now perform a final test to ensure that SCW applies the desired settings. To complete this procedure, confirm that the appropriate settings were made and that functionality is not affected.

Summary

Because bastion host servers that run Windows Server 2003 with SP1 are not protected by other devices such as firewalls, they are exposed to outside attacks. They must be secured as much as possible to maximize their availability and to minimize the possibility of compromise. The most secure bastion host servers limit access only to highly trusted accounts, and enable only those services that are necessary to fully perform their functions.

This chapter explained settings and procedures that can be used to harden bastion host servers and make them more secure. Many of the settings can be applied through local Group Policy. Guidance about how to configure and apply manual settings was also provided.

More Information

The following links provide additional information about topics that relate to hardening bastion host servers that run Windows Server 2003 with SP1.

- For more information about building private networks, open the .pdf file "Firewalls and Virtual Private Networks" by Elizabeth D. Zwicky, Simon Cooper, and Brent D. Chapman at www.wiley.com/legacy/compbooks/press/0471348201_09.pdf.
- For more information about firewalls and security, see "Internet Firewalls and Security – A Technology Overview" by Chuck Semeria at www.itmweb.com/essay534.htm.
- For information about the defense-in-depth model, see the U.S. Military About defense in depth page at http://usmilitary.about.com/od/glossarytermsd/g/did.htm.
- For information about safeguards against intruders, see the "Intruder Detection Checklist" by Jay Beale at www.cert.org/tech_tips/intruder_detection_checklist.html.
- For more information about how to harden bastion hosts, see the SANS Info Sec Reading Room article "Hardening Bastion Hosts" at www.sans.org/rr/whitepapers/basics/420.php.
- For additional information about bastion hosts, see "How Bastion Hosts Work" at http://thor.info.uaic.ro/~busaco/teach/docs/intranets/ch16.htm.
- For information about how to troubleshoot the Security Configuration and Analysis Tool, see the Microsoft Knowledge Base article "Problems After You Import Multiple Templates Into the Security Configuration and Analysis Tool" at http://support.microsoft.com/?kbid=279125.
- For information about site security, see the "Site Security Handbook" at www.faqs.org/rfcs/rfc2196.html.

Chapter 13: Conclusion

Congratulations. Now that you have finished this guide, you should have a clear understanding of how to assess risks that may affect the security of those computers that run Microsoft® Windows Server™ 2003 with SP1 in your organization. You have gained an understanding of how to plan and design security into your network infrastructure wherever possible.

This guide included prescriptive guidance that may be applied to any organization. Some of this guidance includes material that was collected from consultants and systems engineers who have implemented Windows Server 2003, Windows XP, and Windows 2000 solutions in a variety of settings. This material has helped establish a set of best practices for how to make Windows Server 2003 as secure as possible.

Regardless of your organization's environment, security-related matters should be treated seriously. However, many organizations still do not sufficiently address security issues because they mistakenly view security as something that restricts their agility and flexibility. When well-designed security becomes a core business requirement and is planned for at the start of every information technology (IT) project, a properly implemented security strategy can help to improve the availability and performance of your computer systems. However, security that is added to a project as an afterthought can negatively affect usability, stability, and management flexibility. Every organization should include security among its highest priorities.

This guide explained how to effectively mitigate security risks for computers that run Windows Server 2003 with SP1 in three distinct environments. It documented methods for how to plan and design security into your organization's network infrastructure, and provided detailed guidance about how to correct specific vulnerabilities that are commonly found on computers that run Windows Server 2003 with SP1.

The reasons for certain choices were explained in terms of the tradeoffs that must be considered when an organization needs to decide whether to implement each of the countermeasures. Details were provided about how specific countermeasures may affect the functionality, manageability, performance, and reliability of the computers so that you can make informed choices about which countermeasures to implement in your own environment.

Finally, it is important to understand that the task of securing the servers in a network is not a one time project, but rather an ongoing process that organizations must include in their budgets and schedules.

Most organizations that use the Windows Server 2003 operating system would improve their security if they implemented all of the countermeasures that are discussed in this guide. However, when the next serious vulnerability is discovered, these environments may again be quite susceptible to attack. For these reasons, it is essential that you monitor a variety of resources to stay current on security issues related to the operating systems, applications, and devices that are present in your environment.

Every member of the team that produced this guide hopes that you found the material covered in it useful, informative, and easy to understand.

More Information

The following links provide additional information about topics that relate to hardening servers that run Windows Server 2003 with SP1.

- For more information about security at Microsoft, see the Trustworthy Computing: Security page at www.microsoft.com/mscorp/twc/default.mspx.
- For more detail about how MOF can assist in your enterprise, see the Microsoft Operations Framework page at www.microsoft.com/technet/itsolutions/cits/mo/mof/default.mspx.

Appendix A: Security Tools and Formats

It can be a challenge to create, test, deploy, and manage a complete set of policy and templates for your organization. This appendix provides an overview of the available Microsoft tools and the formats that security policies may come in.

Security Tools

The following tools are available either with the Windows Server™ 2003 operating system or as free downloads from the Microsoft Web site.

Security Configuration Wizard

The Security Configuration Wizard (SCW) was introduced in Windows Server 2003 SP1. Unlike Group Policy, it is not integrated with the Active Directory® directory service, so it cannot be used to configure the domain-level policies. However, it does provide a consistent role-based hardening methodology that uses wizards, which makes it easy to create secure policies.

With SCW, you can quickly and easily create prototype policies for multiple server roles that are based on the latest guidance and best practices from Microsoft. SCW will automatically manage service settings, registry settings, Windows Firewall exceptions, and more. It includes the ability to remotely profile target computers, deploy policies, and roll back policies. The command-line tool Scwcmd allows SCW and Group Policy to be used together to deploy policies to groups of computers or convert policies to GPOs.

Security Configuration Editor

The Security Configuration Editor (SCE) tools are used to define security policy templates that can be applied to individual computers or to groups of computers through Active Directory Group Policy. The SCE first appeared as an add-on for Windows NT® 4.0 and has become an integral part of Group Policy.

The SCE is no longer a separate component and is used in the following Microsoft Management Console (MMC) snap-ins and administrative utilities:

- MMC Security Configuration and Analysis snap-in
- MMC Security Templates snap-in
- Group Policy Editor snap-in (used for the Security Settings portion of the Computer Configuration tree)
- Local Security Settings tool
- Domain Controller Security Policy tool
- Domain Security Policy tool

Because all of these tools use the SCE, Windows administrators enjoy a consistent, powerful interface to create and edit policies whether they are intended for a stand-alone computer or will be deployed as a GPO.

You can find more information about SCE from Windows Help.

Active Directory Users and Computers

The MMC Active Directory Users and Computers snap-in provides the primary GUI to create and manage organizational units (OUs) within the domain. You can link GPOs and OUs, control policy order and inheritance, and launch the Group Policy Object Editor as a separate process to edit GPOs. However, the snap-in does not offer a consistent, integrated way to inventory, author, and manage your Group Policies.

You can find more information about the MMC Active Directory Users and Computers snap-in from Windows Help.

Group Policy Management Console

The Group Policy Management Console (GPMC) was produced by Microsoft in response to feedback from customers who needed a better way to control Group Policy in a large environment. The GPMC must be run on Windows XP with SP1 or Windows Server 2003 and consists of an MMC snap-in and a set of scriptable interfaces that can be used to manage Group Policy. It can manage both Windows 2000 Server and Windows Server 2003 domains.

The GPMC provides:

- A user interface that focuses on Group Policy use and management.
- The ability to quickly back up, restore, import, export, copy, and paste GPOs.
- Simplified management of Group Policy-related security.
- Report capabilities for GPO and Resultant Set of Policy (RSoP) data.
- Scriptable GPO operations.

The Group Policy Management Console with Service Pack 1 is available as a free download for all Windows Server 2003 customers at www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&DisplayLang=en.

Security File Formats

Security policies can be created and stored in a variety of formats. The following sections detail the common file formats that are used by Windows Server 2003:

SCW Policy (.xml)

SCW introduces a new file format that is based on XML. Native SCW policies are saved with an extension of .xml. These XML policy files have no official schema, but can be identified by the <SecurityPolicy Version="1.0"> element.

The SCW policy file is actually a complete manifest of several different types of settings:

- System services startup mode
- Windows Firewall exceptions

- Selected computer roles
- Selected computer tasks
- Registry settings
- Policy settings
- Audit policies

Also, SCW policies can be linked to one or more policy templates to provide additional functionality that is not native to SCW, such as system service or registry access control lists (ACLs).

Policy Template (.inf)

Policy templates are text files that follow a standard format for Windows data files: one or more sections that are set off by special square bracket-enclosed keywords, which are followed by one or more attribute/value pairs.

Policy templates can contain one or more sections that define the following types of data:

- Password policies
- Lockout policies
- Kerberos authentication protocol policies
- Audit policies
- Event log settings
- Registry values
- Service startup modes
- Service permissions
- User rights
- Group membership restrictions
- Registry permissions
- File system permissions

Policy templates are supported by almost all of the tools that are listed earlier in this appendix, and the same template format can be used for both local computer policies and Active Directory Group Policies. Before they can be used, the templates must be imported by the appropriate tool.

Group Policy Objects

GPOs are policy data that is stored both in Active Directory and as a collection of files within special directories on domain controllers. These policy files represent computer policies and user policies and are not usually manipulated directly. You can use a tool such as the GPMC to modify the settings or export the GPO into a policy template.

You can export or back up a GPO from within GPMC to save all the information that is stored inside the GPO to the file system. GPO backups that are created in this way keep the following information:

- The GPO's globally unique identifier (GUID) and domain
- GPO settings
- The discretionary access control list (DACL) on the GPO

- The WMI filter link, if there is one (but not the filter itself)
- Links to IP Security policies, if any
- XML report of the GPO settings, which can be viewed as HTML from within GPMC
- Date and time stamp of when the backup was taken
- User-supplied description of the backup

However, this backup does not save any of the data that is external to the GPO. In particular, this file will not contain link information for sites, domains, or OUs and it will not contain the actual WMI filters or IP security policies.

Appendix B: Key Settings to Consider

Although this guide discussed many security countermeasures and security settings, it is important to understand that some of them are especially important. This appendix highlights those settings; you may wish to refer to the relevant chapter for an explanation of what the setting does and why it is important.

Which settings to include in this list could be the subject of an extensive debate. In fact, this topic was discussed at great length by a group of security experts within Microsoft. You may feel that some settings are missing, or that some of the listed settings do not need to be on the list. Because each organization has a distinct environment with unique business requirements, different opinions about security issues should be expected. Still, this list might help you prioritize tasks that relate to hardening computers that run Microsoft® Windows®.

Important countermeasures that are not security settings include:

- Keep computers up-to-date on service packs and hotfixes with automated tools for testing and deployment.
- Install and configure distributed firewall software or organizational IPsec policies.
- Deploy and maintain antivirus software.
- Deploy and maintain antispyware software on computers that are used to browse Web sites.
- Use a non-administrative account for day-to-day tasks. You should only use an account with administrator privileges to perform tasks that require elevated privileges.

Key security settings that are available in Microsoft Windows include:

- Password policy, which is discussed in Chapter 3, "The Domain Policy."
    - Enforce Password History
    - Maximum Password Age
    - Minimum Password Length
    - Passwords must meet complexity requirements
    - Store Password Using reversible encryption for all users in the domain
- User rights, which are discussed in Chapter 4, "The Member Server Baseline Policy."
    - Access this computer from the network
    - Act as part of the operating system
    - Allow logon locally
    - Allow Log on through Terminal Services

- Security options, which are discussed in Chapter 4, "The Member Server Baseline Policy."
  - Accounts: Limit local account use of blank passwords to console logon only
  - Domain Member: Digitally encrypt or sign Secure channel Data (always)
  - Domain Member: Digitally encrypt Secure channel Data (when possible)
  - Domain Member: Digitally sign Secure channel Data (when possible)
  - Domain member: require strong (Windows 2000 or later) session key
  - Network access: Allow anonymous SID/Name translation
  - Network Access: Do not allow anonymous enumeration of SAM accounts
  - Network access: do not allow enumeration of SAM accounts and shares
  - Network Access: Let Everyone permissions apply to anonymous users
  - Network Access: Remotely Accessible Registry Paths
  - Network Access: Restrict Anonymous access to named pipes and shares
  - Network Access: Shares that can be accessed anonymously
  - Network Access: Sharing and Security Model for Local Accounts
  - Network Security: Do not store LAN manager hash value on next password change
  - Network Security: LAN Manager Authentication Level
- Additional registry settings, which are discussed in Chapter 4, "The Member Server Baseline Policy."
  - Safe DLL Search Mode.

Appendix C: Security Template Setting Summary

The Microsoft® Excel® workbook "Windows Server 2003 Security Guide Settings.xls" (included with this guide) documents the policy and service settings for all of the roles and environments that are included in this guide. This workbook contains ten worksheets, one for each role in the guide:

- The **Domain** worksheet contains the Group Policy settings that configure the domain-level policy objects as described in Chapter 3, "The Domain Policy."
- The **Member Server Baseline** worksheet contains the Group Policy and SCW service settings that configure the MSBP as described in Chapter 4, "The Member Server Baseline Policy."
- The **Domain Controller** worksheet contains the Group Policy and SCW service settings that configure the DCBP as described in Chapter 5, "The Domain Controller Baseline Policy."
- The **Infrastructure Server** worksheet contains the Group Policy and SCW service settings that configure the infrastructure server policies as described in Chapter 6, "The Infrastructure Server Role."
- The **File Server** worksheet contains the Group Policy and SCW service settings that configure the file server policies as described in Chapter 7, "The File Server Role."
- The **Print Server** worksheet contains the Group Policy and SCW service settings that configure the print server policies as described in Chapter 8, "The Print Server Role."
- The **Web Server** worksheet contains the Group Policy and SCW service settings that configure the IIS Web server policies as described in Chapter 9, "The Web Server Role."
- The **IAS Server** worksheet contains the Group Policy and SCW service settings that configure the IAS server policies as described in Chapter 10, "The IAS Server Role."
- The **CA Server** worksheet contains the Group Policy and SCW service settings that configure the Certificate Services server policies as described in Chapter 11, "The Certificate Services Server Role."
- The **Bastion Host** worksheet contains the Group Policy and SCW service settings that configure the bastion host policies as described in Chapter 12, "The Bastion Host Role."

Each worksheet contains the following columns:

- The H column, **Policy Setting Name in User Interface**, is the name of the setting as it appears in the Windows Server 2003 Group Policy Editor snap-in.
- The J column, **Legacy Client**, is the recommended value for that setting in the LC environment.
- The K column, **Enterprise Client**, is the recommended value for that setting in the EC environment.
- The L column, **SSLF**, is the recommended value for that setting in the SSLF environment.

To make the spreadsheet easy to read, additional columns were used to illustrate the hierarchy of objects within the Group Policy Editor. Columns A through G are used to represent one level each of the hierarchy. For example, **Computer Configuration** appears in column A, and **Security Settings** appears in column C. Column I was also inserted to help with readability.

Appendix D: Testing the Windows Server 2003 Security Guide

Overview

The *Windows Server 2003 Security Guide* is designed to provide proven and repeatable configuration guidance to secure computers that run Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) in a variety of environments.

The *Windows Server 2003 Security Guide* was tested in a lab environment to ensure that the guidance works as expected. The documentation was checked for consistency and all recommended procedures were tested by the *Windows Server 2003 Security Guide* test team. Tests were performed to verify functionality, but also to help reduce the amount of resources that are needed by those who use the guidance to build and test their own implementations.

Scope

The *Windows Server 2003 Security Guide* was tested in a lab that simulated three different security environments—Legacy Client (LC), Enterprise Client (EC), and Specialized Security – Limited Functionality (SSLF). These environments are described in Chapter 1, "Introduction to the Windows Server 2003 Security Guide." Tests were conducted based on the criteria that are described in the following "Test Objectives" section.

A vulnerability assessment of the test lab environment that was used to secure the *Windows Server 2003 Security Guide* solution was out of scope for the test team.

Test Objectives

The *Windows Server 2003 Security Guide* test team was guided by the following test objectives:

- Validate the recommended changes in security settings for the three security levels that are defined in the guide. Reasons for these changes include:
    - Changes caused by the release of SP1 for Windows Server 2003.
    - Use of the new Security Configuration Wizard (SCW) tool that became available in SP1 and new features such as Windows Firewall.
    - Internal and external feedback that was received about the previous version of the guide.
- Ensure that the security settings and configuration changes that are recommended in the guide meet the requirements of the LC, EC, and SSLF environments.
- Ensure that hardened domain member servers are able to successfully perform their role tasks.

- Ensure that communication between the client computers and the domain controllers is not negatively affected.
- Verify that all prescriptive guidance is clear, complete, and technically correct.

Finally, the guidance should be repeatable and reliably usable by a Microsoft Certified Systems Engineer (MSCE) with two years of experience.

Test Environment

The test lab networks that were developed to test this guide were similar to those that were used in the previous version of the guide. Three separate but similar networks were developed, one for each of the defined environments.

Each test network consisted of a Windows Server 2003 with SP1 Active Directory® directory service forest, computers for infrastructure server roles that provided domain controller, DNS, WINS and DHCP services, and other computers for application server roles that provided file, print, and Web services. The EC network also included computers for the Certificate Services and IAS server roles, and the Bastion Host (BH) server role was included in the SSLF network. Also, the EC and SSLF networks included Microsoft Operations Manager (MOM) 2005 and Systems Management Server (SMS) 2003 to manage and monitor the domain member servers and client computers. These networks also included Microsoft Exchange Server 2003 for e-mail service.

The client computers in the different networks used Windows XP Professional with SP2 and Windows 2000 Professional with SP4. The LC network also included client computers that ran the Windows 98 SR2 and Windows NT® 4.0 workstation with SP6a operating systems.

The following diagram shows the test lab network that was developed for the EC environment.

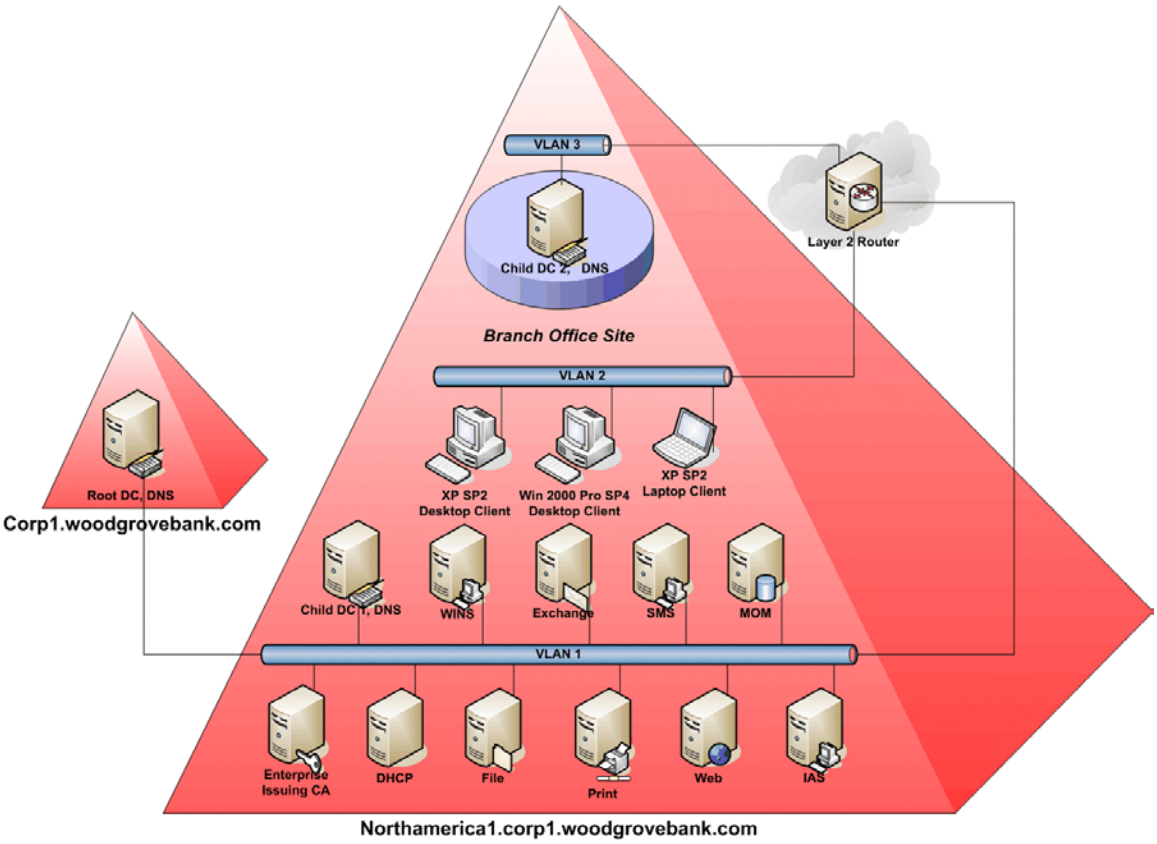

Figure D.1 Logical diagram of the test lab network for the EC environment

To verify replication scenarios between hardened domain controllers, the Active Directory forest consisted of two sites. One site was the main office site with an empty root domain and a child domain that consisted of the previously mentioned server and client computers. The second site consisted merely of a single second domain controller of the child domain.

The following diagram shows the test lab network that was developed for the SSLF environment.

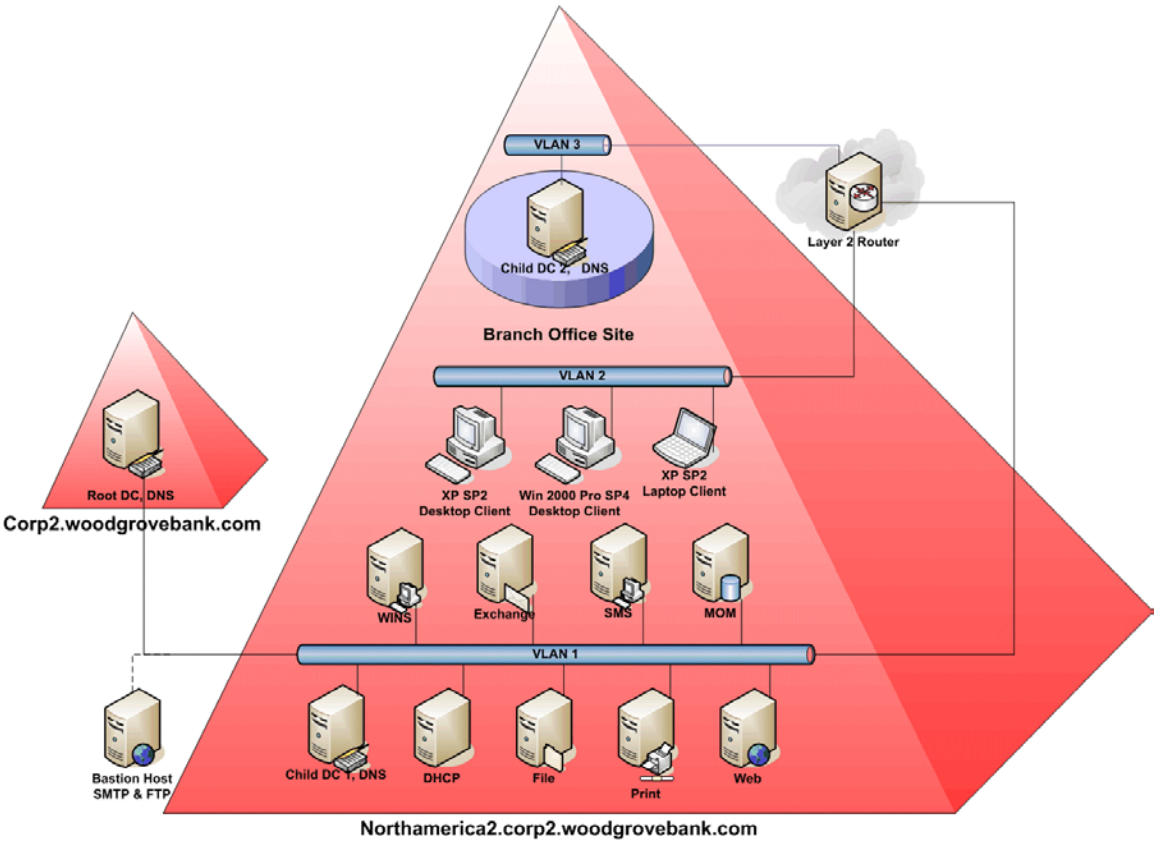

Figure D.2 Logical diagram of the test lab network for SSLF environment

Testing Methodology

This section describes the procedures that were followed to test the *Windows Server 2003 Security Guide*.

The test team established a lab that incorporated the three networks that are described in the previous section. A quick proof of concept (POC) test pass and then two more robust test cycles were executed. During each pass the team strove to stabilize the solution.

A test cycle was defined as a sequence of the following phases:

1. Security Configuration Build phase
   - Manual configuration phase
   - Group Policy configuration phase
2. Test Execution phase

The details of each phase are provided in the following "Phases in a Test Pass" section. The "Test Preparation Phase" section describes the steps that were performed to ensure that the lab environment was free of any issues that could cause a misinterpretation of the actual test results after the three environments were hardened through the first two incremental build phases. It is also referred to as the “baseline” state.

Phases in a Test Pass

The test pass phases are described in the following subsections. Any critical issues that were found during the build phase were identified as bugs and resolved in that phase before the test team moved to the test execution phase. This method ensured that correct security configuration was implemented in the network and validated the accuracy of the test results that were obtained.

Test Preparation Phase

This phase set up the baseline configuration to which the solution is applied during the Security Configuration Build phase. The following steps were performed for each of the three environments—LC, EC, and SSLF:

To complete the test preparation phase

1. Network the computers as illustrated in the network diagram and install the appropriate versions of the Windows operating system on all server and client computers.
2. Create and configure the domain, domain controllers, and the two sites.
3. Join and configure each member server and the management servers. Also, join the client computers to the domain.
4. Execute basic verification tests for each server role to confirm proper network and application configuration.
5. Check the event log of each member server in the network to ensure that there are no application or system level errors.
6. Ensure client computer accessibility to the services that are provided by the domain controller and member servers (DNS, DHCP, CA, file, print, Web and e-mail). Check the event logs on the client computers to ensure that there are no errors.
7. Ensure that all required applications, services, and agents are installed on each domain member. For example, verify that the MOM agent is installed on all the servers that will be managed by the MOM server.
8. After the previous steps are completed, create an image backup of each computer. These backup images are used to "roll back" the network to the baseline configuration before a new test pass is started.

Security Configuration Build Phase

The objective of this phase was to follow the procedures in the guide to configure the domain, domain controllers, and member servers to a more secure level than the baseline configuration.

Manual Configuration Phase

This phase is often the first security build phase. The manual hardening recommendations that were provided in each chapter were implemented during this phase.

Note: Some of these steps may be applicable for your network and some may not. Review each procedure carefully to understand its impact on your network.

To perform the manual configuration phase

1. Use the Microsoft Management Console (MMC) Computer Management snap-in to perform the prescribed policy setting changes (such as the local administrator account and password) on each member computer. Complete the following steps to secure the domain accounts:
    a. Ensure that the built-in local Administrator account has a complex password, has been renamed, and has had its default account description removed.
    b. Rename the Guest accounts on the host and disable them.
    c. Incorporate any additional recommendations from the guide about how to secure the domain accounts.
2. Add any unique security groups or accounts to the user rights settings as described in the chapters.
3. Perform all other applicable manual hardening procedures as prescribed in each chapter. For example, enable Manual Memory Dumps and Error reporting configuration.

Group Policy Configuration Phase

The purpose of this phase is to create and apply the Group Policy objects (GPOs) at the domain and organizational unit (OU) levels. GPOs are applied to the different OUs based on the recommendations in Chapter 2, "Windows Server 2003 Hardening Mechanisms."

Service Pack 1 for Windows Server 2003 introduced some new tools and features that caused the Group Policy implementation design to change from its previous version.

SCW is an attack-surface reduction tool that is used to create the required set of security policies for each of the server roles that are discussed in this guide. The availability of SCW caused the following two significant changes for the Group Policy Configuration Phase:

- IPsec filters that were provided with the previous version of this guide were replaced with Windows Firewall port configurations that were created with SCW.
- Security templates that are included with the guide are to be used in conjunction with SCW to create XML security template files. These templates are then converted to corresponding GPOs using the Scwcmd command-line tool.

The following steps were repeated for each of the three security environments:

To create Group Policy objects

1. Ensure that all required applications, services, and agents were installed on each domain member in the baseline network. For example, ensure that the MOM agent was installed on all the domain member servers that will be managed by MOM.
2. Use the MMC Active Directory Users and Computers snap-in to create the described OU structure.
3. Create the Domain Policy GPO with the .inf security template. This step does not require the use of SCW.
4. Use the SCW tool to create XML–based security templates for each server role that is described in the guide. Prescriptive steps are described in Chapter 2, "Windows Server 2003 Hardening Mechanisms" and each individual server role chapter. When you perform this step, include the appropriate .inf security template for the server role. The template files are included with the downloadable version of this guide.

5. Use the Scwcmd command-line tool to convert the XML security templates that were created in the previous step to GPOs.
6. Repeat step 4 on the Bastion Host server to create the Bastion Host XML security template and then use SCW again to convert and apply it to the Local GPO.

After the GPOs are successfully created, compare the settings with the guidance in the chapters to identify any incorrect configurations.

At this stage, all the domain member servers reside in the Computers OU. These servers are then moved to their respective OUs under the Member Server OU.

The next task (detailed in the following procedure) is to apply each of these GPOs to the respective OUs. The Group Policy Management Console (GPMC) tool was used to link the GPO with the OU. The Domain Controller Policy GPO was linked last.

The following steps were performed to complete the rest of the Security Configuration Build phase:

To apply Group Policy objects

1. Link the Domain Policy GPO to the domain object.

   Note: If default GPO links are already present or if there are multiple GPOs, you might need to elevate the GPO links in the priority list.
2. Use the Group Policy Management Console tool to link the Member Server Baseline Policy GPO to the Member Servers OU. (You can also perform this step with the MMC Active Directory Users and Computers snap-in.)
3. Link each individual server role GPO to the appropriate server role OU.
4. Link the Domain Controller Policy GPO to the Domain Controller OU.
5. To ensure application of the latest Group Policy settings, execute **`gpudpate /force`** at a command prompt on all domain controllers. Then restart all the domain controllers one at a time, starting with the primary domain controller. Allow sufficient time for Active Directory to replicate the changes between the sites.

   Important: It is very important to restart the domain controllers after you apply the Domain Controllers Policy GPO. If you do not perform this step you may see replication errors in the Directory Service folder or Userenv errors in the Application folder of Event Viewer.
6. Repeat step 5 on all of the domain member servers.
7. Check Event Viewer for any errors. Review the error logs to troubleshoot and resolve any failures.
8. On the Bastion Host server, use the SCW tool to apply the Bastion Host XML security template on the Local GPO of the server.

Verifying Group Policy Download on the Member Server Computers

The previous procedures created GPOs and applied them to OUs to configure the computers in those OUs. Complete the following steps to confirm the successful download of Group Policy from domain controllers to member server computers. (It is assumed that the member server computers were restarted after the GPO was linked to the OU.)

To verify Group Policy download on a member server computer

1. Log on to the member server computer.
2. Click **Start**, **Run**, type **rsop.msc**, and press ENTER.

3. In the **Resultant Set of Policy** console, expand **Console Root** and browse to **Computer Configuration**.
4. Right-click **Computer Configuration** and click **Properties**.

   The list of GPOs will display in the **Computer Configuration Properties** panel. The GPO that was applied to the OU should be available in the list, and there should be no errors associated with it.

Test Execution Phase

This phase executes the test cases that were developed by the test team. The test execution phase seeks to identify the following:

- Any potential application, security, or system failure events that are caused by processes that were used to harden the domain, domain controllers, member servers, or Bastion Host server.
- Lost availability of a service or functionality that is caused by changes to the security configuration of the servers in the network.
- Technical inaccuracies between what is documented in the chapters and the physical implementation in the test lab.

The test team executed the set of test cases that are included in **Windows Server 2003 Security Guide Tools and Templates\Test Tools** folder. (The tools and templates are included with the downloadable version of this guide.) These tests were executed on each of the three separate networks except for those that tested components that were only available in one network—such as Certificate Services, which was only available in the EC environment. In addition to these test cases, manual testing was performed at various time—for example, to periodically check Event Viewer logs or to verify any specific issues that were discovered in the previous version of the guide. All issues that were found were logged in a database and triaged with members of the development team until they were resolved.

More detailed information about the different types of tests that were performed is provided in the next section.

Types of Tests

The test team performed the following types of tests during the test phases to ensure that the secured domain, domain controllers, and member servers did not experience any significant loss of functionality. You may want to refer to the Excel workbooks in the **\Windows Server 2003 Security Guide Tools and Templates\Test Tools** folder that is included in the download for this guide, which contain the complete list of test cases that were executed for domain–based as well as stand-alone servers that run Windows Server 2003 with SP1. Details such as test scenarios, execution steps, and expected results are also provided.

These tests were executed multiple times. More importantly, they were executed before and after the security settings that are described in this guide were implemented. This approach helped the test team to identify potential errors and any variations in functionality for the listed server roles.

Client Side Tests

These test cases were executed on the client computers in the network. The main purpose of these tests was to ensure that domain services (such as authentication, access rights, name resolution, and so on) and application based services (such as File,

Print, and Web) are available to the client computers after the network servers are hardened. For the LC environment, these tests ensured that those client computers that run Windows NT 4.0 SP6a and Windows 98 were able to authenticate with the Windows Server 2003 Active Directory domain.

Documentation Build Tests

These tests validate that the statements, procedures, and functions that are documented in the implementation guidance are accurate, unambiguous, and complete. No separate test cases are listed for these tests.

Script Tests

Some of the client test scenarios were scripted in VBScript. These test cases are primarily concerned with proper functionality of Windows XP client computers that use network–based services, such as domain logon, password change, and print server access. The VBScript files for these test cases are available in the **\Windows Server 2003 Security Guide Tools and Templates\Test Tools** folder that is included in the downloadable version of this guide.

Server Side Tests

These test cases were developed to verify functionality and the effect of the build procedures on Windows Server 2003 with SP1 servers that were secured with the recommendations in this guide. All the server roles that are described in this guide were tested. The additional server roles that were included in the test network, such as Exchange, MOM, and SMS, were also tested.

Pass and Fail Criteria

Before tests were performed, the following criteria were defined to ensure defect prevention and bug resolution:

- All test cases must pass with expected results as described in the individual test case spreadsheets.
- A test case is considered to have passed if the actual result matched the expected result that is documented for the case. If the actual result does not match the expected result, it was treated as a failed test case, a bug was created, and a severity score was assigned.
- If a test case failed, it was not assumed that the solution guidance was necessarily defective. For example, misinterpretation of product documentation, incomplete documentation, or inaccurate documentation could cause failures. Each failure was analyzed to discover its cause based on actual results and the results that were described in project documentation. Failures were also escalated to the appropriate owners of the respective Microsoft products.

Release Criteria

The primary release criterion for the *Windows Server 2003 Security Guide* was related to the severity of bugs that were still open. However, other issues that were not being tracked through bugs were also discussed. The criteria for release are:

- No bugs are open with severity levels 1 and 2.
- All open bugs are triaged by the leadership team, and their impacts are fully understood.

- Solution guides are free of comments and revision marks.
- The solution successfully passes all test cases in the test lab environment.
- Solution contents have no conflicting statements.

Bug Classification

The bug severity scale is described in the following table. The scale is from 1 to 4, with 1 as the highest severity and 4 as the lowest severity.

Table D.1 Bug Severity Classification

Severity	Most common types	Conditions required
1	– Bug blocked build or further testing. – Bug caused unexpected user accessibility. – Steps defined in the documentation were not clear. – Results or behavior of a function or process contradicts expected results (as documented in functional specification). – Major mismatch between the security template files and the functional specification.	– Solution did not work. – User could not begin to use significant parts of the computer or network. – User had access privileges that should not be allowed. – User access was blocked to certain server(s) that should be allowed. – Expected results were not achieved. – Testing cannot proceed without being addressed.
2	– Steps defined in the guide are not clear. – Documented functionality is missing (in this case, test was blocked). – Documentation is missing or inadequate. – Inconsistency between security template files and content in the guide, but security template file is in sync with functional specification.	– User had no simple workaround to amend the situation. – User could not easily figure out a workaround. – Primary business requirements could not be met by the computer or network.
3	– Documented format issue. – Minor documentation errors and inaccuracies. – Text misspellings.	– User has a simple workaround to mend situation. – User can easily figure out workaround. – Bug does not cause a bad user experience. – Primary business requirements are still functional.
4	– Suggestions. – Future enhancements.	– Clearly not related to this version.

Summary

This appendix enables an organization that uses the *Windows Server 2003 Security Guide* to understand the procedures and steps that were used to test the implementation of the solution in a test lab environment. The actual experience of the *Windows Server 2003 Security Guide* test team is captured in this appendix, which includes descriptions of the test environment, types of tests, the release criteria, and bug classification details.

All of the test cases that were executed by the test team passed with the expected results. The test team confirmed that the requisite functionality was available after the recommendations from the *Windows Server 2003 Security Guide* for the defined environments were applied.

Acknowledgments

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

Authors

Mike Danseglio

Kurt Dillard

José Maldonado

Brad Warrender

Content Contributors

Liam Colvin, *3Sharp, LLC*

William Dixon, *V6 Security Inc.*

Tony Dowler, *3Sharp, LLC*

Eric Fitzgerald

Devin Ganger, *3Sharp, LLC*

Stirling Goetz

Ian Hellen

Jesper Johansson

Steve Ryan, *Content Master*

Kirk Soluk

Program Managers

Bomani Siwatu

Alison Woolford, *Content Master*

Editors

Reid Bannecker

Wendy Cleary, *S&T Onsite*

John Cobb, *Volt Information Sciences*

Kelly McMahon, *Content Master*

Lynne Perry, *Content Master*

Jon Tobey

Steve Wacker, Wadeware LLC

Release Managers

Flicka Crandell

Karl Seng, *Siemens Agency Services*

Testers

Kenon Bliss, *Volt Information Sciences*

Gaurav Singh Bora, *Infosys Technologies*

Paresh Gujar, *Infosys Technologies*

Vince Humphreys, *Volt Information Sciences*

Ashish Java, *Infosys Technologies*

Mehul Mediwala, *Infosys Technologies*

Rob Pike

Varun Rastogi, *Infosys Technologies*

Reviewers

Roger Abell, *Arizona State University*

Jose Luis Auricchio

Avi Ben-Menahem

Rich Benack

Shelly Bird

Susan Bradley

Steve Clark

Rob Cooper

Duane Crider

Karel Dekyvere

Christine Duell

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
Jim Whitney, *Configuresoft*
Shain Wray

Other Contributors

Ignacio Avellaneda
Ganesh Balakrishnan
Tony Bailey
Shelly Bird
Nathan Buggia
Derick Campbell
Chase Carpenter
Jeff Cohen
John Dwyer
Sean Finnegan
Karl Grunwald
Joanne Kennedy
Karina Larson, *Volt Information Sciences*
Chrissy Lewis, *Siemens Business Services*
David Mowers
Jeff Newfeld
Rob Oikawa
Vishnu Patankar
Peter Meister
Keith Proctor
Bill Reid
Sandeep Sinha
Stacy Tsurusaki, *Volt Information Sciences*
David Visintainer, *Volt Information Sciences*
Graham Whiteley
Rob Wickham
Lori Woehler
Jay Zhang

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