

Microsoft[®]

Security Operations for Microsoft Exchange 2000 Server



patterns & practices
proven practices for predictable results

ISBN: 0-7356-1834-8

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2002 Microsoft Corporation. All rights reserved.

Version 1.0

Microsoft, Active Directory, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Chapter 1

Introduction	1
Microsoft Operations Framework (MOF)	1
Get Secure and Stay Secure	2
Get Secure	3
Stay Secure	3
Scope of This Guide	3
Chapter Outlines	5
Chapter 2 – Securing Your Exchange Environment	5
Chapter 3 – Securing Exchange 2000 Servers Based on Role	5
Chapter 4 – Securing Exchange Communications	5
Who Should Read This Guide	5
Summary	5
More Information	6

Chapter 2

Securing Your Exchange Environment	7
General Exchange Security Considerations	7
Exchange Service Dependencies	8
Installing Exchange	9
Exchange 2000 Patch Management	10
Securing the Client Environment	11
Protecting Against Address Spoofing	11
Anti-Virus Measures	12
Protecting Against Unsolicited Mail (Spam)	12
Protecting Against Denial-of-Service Attack	14
Using Permissions and Administrative Groups to Control Access to Exchange 2000	14
Centralized and Distributed Administration	16
Creating an Environment to Support a Mixed Administrative Model	16
Controlling User Administration	18
Summary	18
More Information	19

Chapter 3

Securing Exchange 2000 Servers Based on Role	21
Test Environment	21
Using OWA Front-End and Back-End Servers	22
Securing Server Roles for an Exchange 2000 Environment	22
Active Directory Structure to Support Exchange 2000 Server Roles	24
Importing the Security Templates	25
Exchange Server Policies	28
Exchange Back-End Server Policy	28
OWA Front-End Server Policy	31
Installing and Updating Exchange in an Increased Security Environment	33
Additional Security Measures	35
IIS Lockdown Tool	35
Modifying IIS Lockdown and URLScan Settings for OWA Front-End Servers	37
Dismounting the Mailbox Store and Deleting the Public Folder Store	38
Changing the SMTP Banner	40
Group Lockdown for Exchange Domain Servers	40
Exchange Cluster Considerations	41
Summary	41
More Information	41

Chapter 4

Securing Exchange Communications	43
Securing Communications in Outlook 20002	44
Encrypting the MAPI Connection from Outlook 2002 to Exchange Server	44
Signing and Encrypting Messages	44
Securing OWA Communications	45
Using ISA Server to Secure OWA	45
Securing Communication Between Web Browsers and ISA Servers	47
Encryption Between ISA Servers and OWA Front-End Servers	50
Encryption Between OWA Front-End Servers and Back-End Exchange Servers	51
Securing SMTP Communications	57
Using ISA Server to Secure SMTP	57
Additional Measures to Secure SMTP	58
Summary	59
More Information	60

Appendix A

Managing Security with Windows 2000 Group Policy	61
Importance of Using Group Policy	61
How Group Policy is Applied	62
Group Policy Structure	64
Test Environment	65
Checking Your Domain Environment	66
Verifying DNS Configuration	66
Domain Controller Replication	66
Centralize Security Templates	67
Time Configuration	67
Policy Design and Implementation	69
Server Roles	70
Active Directory Structure to Support the Server Roles	70
Importing the Security Templates	73
Keeping Group Policy Settings Secure	75
Events in the Event Log	76
Verifying Policy Using Local Security Policy MMC	76
Verifying Policy Using Command Line Tools	77
Auditing Group Policy	77
Troubleshooting Group Policy	78
Resource Kit Tools	78
Group Policy Event Log Errors	80
Summary	80
More Information	80

Appendix B

Securing Servers Based on Role	83
Domain Policy	84
Password Policy	84
Account Lockout Policy	85
Member Server Baseline Policy	85
Baseline Group Policy for Member Servers	86
Domain Controller Baseline Policy	98
Domain Controller Baseline Audit and Security Options Policy	98
Domain Controller Baseline Services Policy	98
Other Baseline Security Tasks	100
Securing Each Server Role	102
Windows 2000 Application Server Role	103
Windows 2000 File and Print Server Role	103
Windows 2000 Infrastructure Server Role	103
Windows 2000 IIS Server Role	104

Changes to the Recommended Environment	107
Administration Changes	107
Security Modifications if HFNETCHK is Not Implemented	108
Summary	108
More Information	109

Appendix C

Additional Files Secured	111
---------------------------------	------------

Appendix D

Default Windows 2000 Services	115
--------------------------------------	------------

Appendix E

Additional Services	119
----------------------------	------------

Index	121
--------------	------------

1

Introduction

Welcome to *Security Operations for Microsoft® Exchange 2000 Server*. This guide will help you take steps to ensure that your Exchange 2000 Server environment is as secure as possible and remains secure during day to day operations.

This guide is designed to act as a supplement to *Security Operations for Microsoft® Windows® 2000 Server* (Microsoft Press, ISBN: 0-7356-1823-2). You are strongly advised to read that guide in full before going on to read this guide. Sections of this guide will depend directly on information in *Security Operations for Microsoft Windows 2000*, and this will be indicated in the text where appropriate and the pertinent chapters are included as appendices. You are also advised to read *Microsoft® Exchange 2000 Server Operations* (Microsoft Press, ISBN: 0-7356-1831-3), which will provide you with more information about general Exchange 2000 operations.

Microsoft Operations Framework (MOF)

For operations in your environment to be as efficient as possible, you must manage them effectively. To assist you, Microsoft has developed the Microsoft Operations Framework (MOF). This is essentially a collection of best practices, principles, and models providing you with operations guidance. Following MOF guidelines should help your mission critical production systems remain secure, reliable, available, supportable, and manageable

The MOF process model is split into four integrated quadrants, as follows:

- Changing
- Operating
- Supporting
- Optimizing

Together, the phases form a spiral life cycle (see Figure 1.1) that can apply to anything from a specific application to an entire operations environment with multiple data centers. In this case, you will be using MOF in the context of security operations.

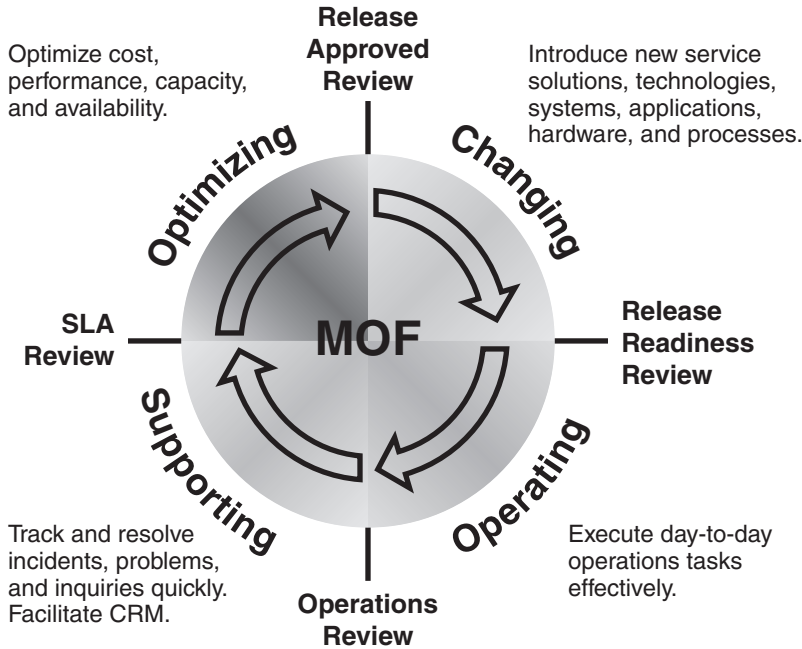


Figure 1.1
MOF lifecycle

The process model is supported by 20 service management functions (SMFs) and an integrated team model and risk model. Each quadrant is supported with a corresponding operations management review (also known as a review milestone), during which the effectiveness of that quadrant’s SMFs are assessed.

It is not essential to be a MOF expert to understand and use this guide, but a good understanding of MOF principles will help you manage and maintain a reliable, available, and stable operations environment.

If you wish to learn more about MOF and how it can assist you in your enterprise, visit the Microsoft Operations Framework website. See the “More Information” section at the end of this chapter for details.

Get Secure and Stay Secure

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

Get Secure

The first phase is called Get Secure. To help your organization achieve an appropriate level of security, follow the Get Secure recommendations in the Microsoft Security Tool Kit, which can be accessed online (see the “More Information” section for details on the tool kit and the STPP).

Stay Secure

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

Scope of This Guide

This guide is focused explicitly on the operations required to create and maintain a secure environment on servers running Exchange 2000. We examine two specific roles defined for servers—OWA front-end servers and back-end servers. We do not discuss how to run Internet Message Access Protocol 4 (IMAP4) or Post Office Protocol 3 (POP3) in a secure manner.

You should use this guide as part of your overall security strategy for Exchange, not as a complete reference to cover all aspects of creating and maintaining a secure environment. The diagram provides a high level view of these areas, the dark shaded box with white text is covered in this guide and the other shaded areas are covered in *Security Operations for Microsoft Windows 2000 Server*.

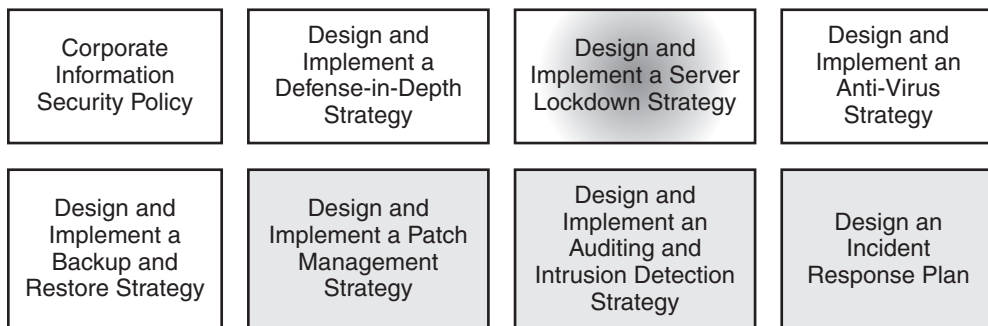


Figure 1.2

Scope of this guide in relation to your overall security strategy for Exchange

Note: *Security Operations for Microsoft Windows 2000 Server* is available online. For further details, see the “More Information” section at the end of this chapter.

The diagram shows the steps required to help make a server secure (Get Secure) and help keep it that way (Stay Secure). It also shows how the chapters of this guide and *Security Operations for Microsoft Windows 2000 Server* will help you achieve those aims.

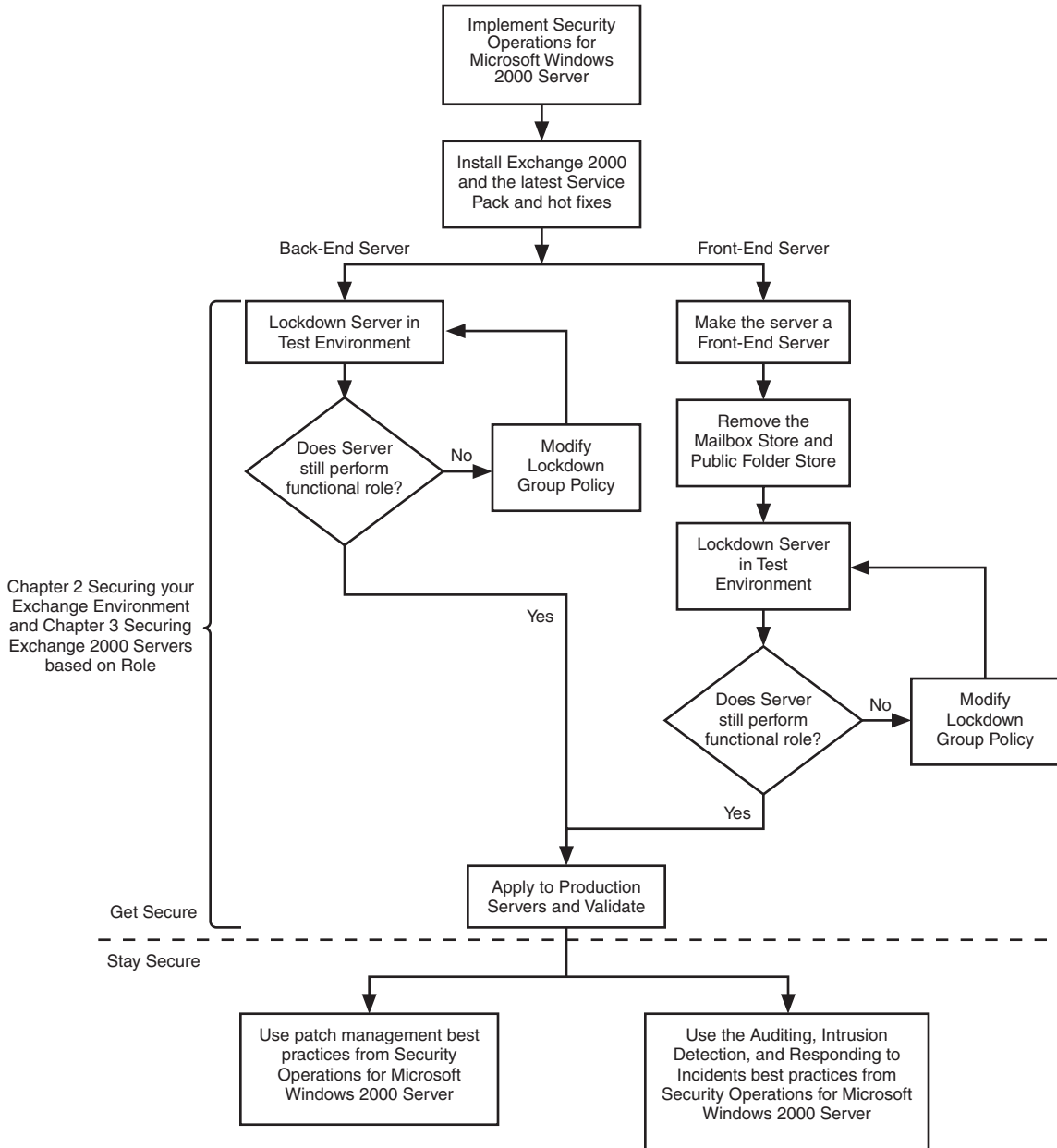


Figure 1.3
Process flowchart showing Get Secure and Stay Secure phases

Chapter Outlines

This guide consists of the following chapters, each of which takes you through a part of the security operations process. Each chapter is designed to be read, in whole or in part, according to your needs.

Chapter 2 – Securing Your Exchange Environment

Exchange is a complex application, with many components that depend on each other. In order to secure Exchange successfully you need to be aware of these relationships and design your security accordingly. This chapter looks at general risks to Exchange 2000 environments. It also introduces the two server roles that appear in the following chapters, back-end and front-end servers, and links in to *Windows 2000 Security Operations* to show how security can be implemented on these server types.

Chapter 3 – Securing Exchange 2000 Servers Based on Role

This chapter deals with securing the back-end server role and the Outlook Web Access (OWA) front-end server role, and examines the steps you need to follow to increase their security. It looks at the changes you need to make to a secure Windows 2000 environment to allow an Exchange 2000 server to run as securely as possible.

Chapter 4 – Securing Exchange Communications

This chapter covers securing communication between clients and Exchange 2000 Server, for example, securing communication between Outlook and Exchange. It examines firewall considerations for OWA server positioning, and looks at securing traffic not only from the OWA server to the client, but also from the OWA server to internal Exchange back-end servers. It also looks at securing SMTP traffic.

Who Should Read This Guide

This guide should be read by anyone who is responsible for securing Exchange 2000 in their organization, and who has a good knowledge of Windows 2000 and the general principles of IT security.

Summary

This chapter has introduced you to this guide and summarized the other chapters in it. It has also introduced the Strategic Technology Protection Program (STTP). Now that you understand the organization of the guide, you can decide whether to read

it from beginning to end, or whether you want to read selected portions. Remember that effective, successful security operations require effort in all areas, not just improvements in one, so you are best advised to read all chapters.

More Information

For more detail on how MOF can assist in your enterprise:

<http://www.microsoft.com/mof>

Information about the Strategic Technology Protection Program:

<http://www.microsoft.com/security/mstpp.asp>

Microsoft Security Tool Kit:

<http://www.microsoft.com/technet/security/tools/stkintr0.asp>

Microsoft Strategic Technology Protection Program Website:

<http://microsoft.com/security/mstpp.asp>

Information on the Microsoft Security Notification Service:

<http://www.microsoft.com/technet/security/bulletin/notify.asp>

Security Operations Guide for Windows 2000 Server

<http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp>

Exchange 2000 Server Operations Guide

<http://www.microsoft.com/technet/prodtechnol/exchange/maintain/operate/opsguide/default.asp>

2

Securing Your Exchange Environment

Many organizations build a number of their critical business processes around the functionality of Microsoft Exchange. It can be very difficult to deal with any period of time without the various services (e-mail, calendaring, contact information, collaborative applications and so on) that Exchange provides.

One area of risk to continued Exchange 2000 operations is malicious attack, either from within your organization or outside. The risk is increased in the case of Exchange because it is so widely accessible. Chances are that almost every person in your organization has access to Exchange, and you may even make it available over the Internet.

In this chapter, we examine many of the steps you can take to minimize the risk of malicious attacks to your Exchange 2000 environment.

Note: As you make changes to your Exchange 2000 environment, it is vital that you thoroughly document each of those changes. For more information on change and configuration management in Exchange, see *Microsoft Exchange 2000 Server Operations*. For further details, see the "More Information" section at the end of this chapter.

General Exchange Security Considerations

When considering how to increase the security of Exchange, it is important to remember that Exchange is actually a number of processes that communicate with each other on local and remote computers. Specifically, Exchange servers need to communicate with other Exchange servers, domain controllers and a number of different clients. IIS is integral to the functionality of Exchange and Exchange

servers can even be accessed through the file system. This series of complicated relationships means that when attempting to lock down Exchange servers you should consider many different components. These include:

- Service security
- File security
- IIS security
- Registry entries
- Underlying Windows 2000 security
- Domain controller/global catalog security
- Active Directory security
- Exchange database security
- Exchange transport mechanisms

Exchange Service Dependencies

The aim of this guide is to help you secure your Exchange 2000 environment as much as possible without affecting the core functionality of Exchange. One key area to look at is Exchange services. Exchange runs on Windows 2000, and requires some Windows 2000 services to be running either to install the product or for it to continue to function properly. Some Exchange services are also dependent on other Exchange services.

The diagram shows the services that run on an Exchange server by default and the dependencies they have on each other.

In this guide we recommend settings for many of these services, which are normally configured to start automatically by default. You will be able to disable some of the services, but this will result in some lack of functionality at the server. You will need to decide whether this loss of functionality is appropriate for your environment.

Exchange Server Service Dependencies

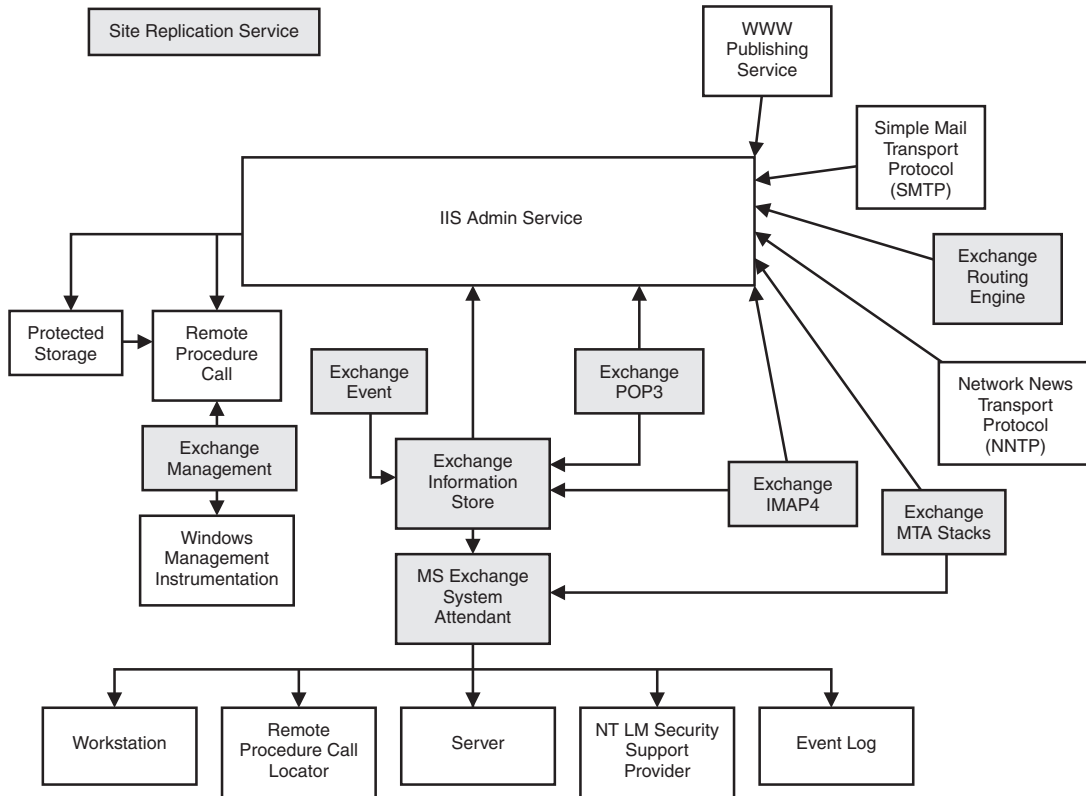


Figure 2.1
Exchange server services dependencies

Installing Exchange

Exchange 2000 is a schema modifying application. This means that when setup /forestprep is run, the schema container is modified. Subsequently, when each Exchange 2000 server is installed, the configuration container is modified to include the appropriate Exchange 2000 objects. In practice this means that the account running setup /forestprep needs schema admin permissions, while any account used to install Exchange requires Exchange Full Administrator permissions.

Note: For more information on Exchange 2000 permissions, see Microsoft Exchange 2000 Internals: Permissions Guide. For further details, see the “More Information” section at the end of this chapter.

As with all aspects of permissions management, you should ensure that administrators only have the rights necessary to do their job. High level permissions should be particularly closely guarded. You should consider keeping the Schema Admins

group empty by default and explicitly add a user to the group in order to run setup /forestprep. Keeping the Schema Admins group empty is a good general practice as it ensures that you are always alerted before any application would modify the schema.

As part of setup /forestprep, the schema administrator has an opportunity to specify an Exchange 2000 administrator account. This account is granted Exchange Full Administrator rights over the Exchange organization and can therefore perform subsequent Exchange installations. One way of minimizing your security risks during installations is to create a specific universal security group that will have the right to install Exchange. You can then define the group as an Exchange Full Administrator. This will allow you to tightly control who can install Exchange by controlling the membership of the group.

Exchange 2000 Patch Management

To keep Exchange as secure as possible over time, you will need to make sure you remain current on the latest patches. There are two elements to this—making sure the operating system is up to date and making sure that Exchange is up to date. If the operating system is vulnerable then Exchange 2000 is also vulnerable, so you should treat the security of the operating system very seriously on Exchange servers.

There are a number of utilities available that will keep you current on Windows 2000 service packs, hotfixes and patches. Microsoft supplies two utilities to help you with this – Hfnetchk and The Microsoft Baseline Security Analyzer.

There are a number of security updates that have emerged since Windows 2000 Service Pack 2. Fortunately, many of these are grouped together as the Security Rollup Package for Windows 2000 see the “More Information” section at the end of this chapter for details. You will also need to ensure that you are fully up to date on IIS vulnerabilities and Internet Explorer vulnerabilities.

Exchange 2000 vulnerabilities are significantly rarer than Windows 2000 vulnerabilities and are not currently reported by the tools mentioned in this section. You should ensure that you are notified of any new patches to your environment by Microsoft. If you subscribe to Microsoft Security Bulletins, you will receive these notifications automatically.

Note: For further details on receiving Microsoft Security Bulletins, see the “More Information” section at the end of this chapter.

Note: For more information on patch management in a Windows 2000 environment, see *Security Operations for Microsoft Windows 2000 Server*.

Note: For further details on the recommended configuration and updates for Exchange 2000, see the “More Information” section at the end of this chapter.

Securing the Client Environment

Exchange 2000 is a client server application. It is therefore very important when considering the overall security of your Exchange environment that you also examine the clients that will be used.

Exchange supports a large number of different clients. As part of your risk management strategy you should examine which are strictly required and limit yourself to those clients. Make sure that you use current and patched versions of the client software, regularly checking for client security updates as these can be just as important as the server.

An important weapon in keeping the client secure is the user. If you educate the user on how to use the client in a responsible manner, it will reduce the risks you face from attack. For example, users should be educated about e-mail viruses, virus hoaxes, chain letters and unsolicited mail.

Note: For information on securing communications between the client and the server, see Chapter 4, “Securing Exchange Communications.”

Protecting Against Address Spoofing

One of the most common ways of attacking an e-mail system is by manipulating the From: field in an e-mail message. Simple Mail Transfer Protocol (SMTP) does not check to verify a user’s identity, but you can perform some actions in Exchange to try and minimize message spoofing.

One of the most insidious problems with address spoofing is external attackers using the e-mail address of an internal user. This can be used in a number of ways, often as a form of social engineering, to persuade another user to give up confidential information, which in turn leads to further attack.

By default, Exchange 2000 will resolve an e-mail address in its address book to the name used in the Global Address List. This can make it very difficult to tell if a message has actually originated outside the organization. You can change the default behavior, so that mail from outside the organization always remains unresolved. If you then educate the users to look for unresolved e-mail addresses, it will help you guard against this form of address spoofing.

Note: For more details on ensuring that mail from outside the Exchange organization remains unresolved, see the Knowledge Base Article Q288635, “XIMS: ResolveP2 Functionality in Exchange 2000 Server.”

If you are receiving messages directly from other domains on the Internet, you can configure your SMTP virtual server to perform a reverse Domain Name System (DNS) lookup on incoming e-mail messages. This verifies that the senders mail

server Internet Protocol (IP) address (and fully qualified domain name) of the sender corresponds to the domain name listed in the message.

Reverse lookup does place an additional load on the Exchange server. It also requires that the Exchange server is able to contact the reverse lookup zones for the sending domain.

Note: For more information on using reverse DNS lookup, see Knowledge Base Article Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server."

Anti-Virus Measures

One of the more significant threats to your environment is viruses transmitted through e-mail. E-mail viruses may attack the computer systems themselves or they may attack the e-mail environment, by flooding the system with messages to the point of overload. You need to ensure that you have adequate protection against viruses in your environment.

You should consider protecting against viruses at the firewall, at or outside the SMTP gateway, at each Exchange server and on every client.

Note: For more information on anti-virus software on Exchange servers, see Knowledge Base Article Q245822, "XGEN: Recommendations for Troubleshooting an Exchange Computer with Antivirus Software Installed."

At the client level, Outlook 2002 blocks many attachments, preventing them from being viewed and therefore potentially causing damage to your environment. However, you should bear in mind that if you also allow the use of Outlook Web Access (OWA), that the OWA client will not block these attachments.

Note: For more information on protecting against virus attack and what to do in the event of an incident, see *Microsoft Exchange 2000 Server Operations*.

Protecting Against Unsolicited Mail (Spam)

Unsolicited mail can be a major problem for many organizations. It is costly in a number of ways, from lost user time dealing with mail, to wasted bandwidth and storage space in carrying and storing unnecessary mail.

Unsolicited mail can be very difficult attack to guard against. However, there are a number of measures you can take which will reduce the amount of unsolicited mail you receive.

Educating Users

The users on your network form a key defense against unsolicited mail. This type of mail is often a result of social engineering on your network, and it is important to educate your users on how to avoid it. For example, your users may receive unsolicited mail that includes a disclaimer, stating that if you wish to be removed from the mailing list you should respond to the mail, with the word REMOVE in the subject line. More often than not this is just a means of verifying that an e-mail address is valid so that the address can then be used again. Users should be educated not to respond to unsolicited e-mail under any circumstances. They should also be educated not to forward on unsolicited mail to co-workers.

Unsolicited Mail Features in Outlook 2002

Outlook 2002 has some built-in features that will help protect your users against unsolicited mail. Outlook can search for certain phrases in e-mail messages and automatically move messages containing these phrases from your **Inbox** to any folder you specify, including a junk e-mail folder created by Outlook or your **Deleted Items** folder.

Outlook stores the list of terms it uses to filter for unsolicited e-mail in a folder called filters.txt. This file contains a list of senders of unsolicited mail. It also contains phrases which, if they appear in the mail, will result in them being treated as unsolicited mail.

When you first begin using these features, you should make sure that your users check for messages that have been removed from the inbox, to ensure that valid messages have not been removed accidentally.

Note: For more details on preventing unsolicited mail in Outlook 2002, see the article “Manage Junk and Adult Content Mail in Outlook 2002” in the Microsoft Office Assistance Center. See the “More Information” section for further details.

Unsolicited Mail Features of Exchange 2000

Features built into Exchange 2000 can help you prevent unsolicited mail. In particular, you can prevent mail from being delivered if there is no sender specified, or if the mail is from a particular domain or domains. You can perform filtering across all Exchange servers, or you can determine specific SMTP virtual servers which will perform filtering.

Note: For more details on filtering unsolicited mail using Exchange 2000 Server, see the Knowledge Base article Q276321, “XADM, How to Filter Junk Mail in Exchange 2000.”

Note: You can guard further against unsolicited e-mail using the message screener. This is covered in Chapter 4, “Securing Exchange Communications.”

Protecting Against Denial-of-Service Attack

Denial-of-service attacks are generally very difficult to guard against. However, there are a number of settings in Exchange that will help you to do so. The message limits parameters configured on the SMTP virtual server, allow you to specify a maximum number of recipients per message, a maximum message size, a maximum number of messages per connection and so on. These limits will help to ensure that a denial-of-service attack using mail transport is very difficult.

Note: For more information on setting message limits, see Knowledge Base article Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server."

Another form of denial-of-service attack could come from sending a large number of mails to a particular server until it runs out of disk space. You can minimize the chance of this happening by setting storage limits on mailboxes and public folders.

Note: For more information on setting storage limits, see Knowledge Base article Q319583, "HOW TO: Configure Storage Limits on Mailboxes in Exchange 2000."

Using Permissions and Administrative Groups to Control Access to Exchange 2000

As with any application in your environment, when you define the permissions for Exchange, you should look at the roles your Exchange administrators will have in the environment and give them only the necessary permissions. To simplify the process, Exchange 2000 uses administrative groups. An administrative group is a collection of Exchange 2000 objects that are collected together for the purpose of managing and delegating permissions. An administrative group may contain policies, routing groups, public folder hierarchies, servers, conferencing objects, and chat networks. For example, if your organization has two sets of administrators that manage two sets of servers running Exchange 2000, you can create two administrative groups that contain those two sets of servers. Based on the administrative model that your organization uses, you can develop an administrative plan that fits your needs.

The easiest way to assign permissions to administrative groups (and to the Exchange organization) is using the Exchange Administration Delegation Wizard. You will need to be logged on as a user with Full Control over the Exchange organization to use the wizard. To start the Exchange Administration Delegation Wizard, you should right-click the organization or administrative group in **Exchange System Manager**, then click **Delegate Control**.

Three administrative roles are provided:

Table 2.1: Administrative Roles in Exchange 2000

Role	Description
Exchange View Only	Grants permissions to list and read the properties of all objects below that container. Unless the administrator will need to modify object properties, always assign this role.
Exchange Administrator	Grants all permissions except for ability to take ownership, change permissions, or open user mailboxes. If the administrator will need to add objects or modify object properties, but will not be required to delegate permissions on the objects, assign this role.
Exchange Full Administrator	Grants all permissions to all objects below that container except for the ability to open user mailboxes or impersonate a user's mailbox, including the ability to change permissions. Assign this role only to administrators who are required to delegate permissions to objects, or to those administrators who will need to add new servers to the administrative group.

In some cases you will find that using the Exchange Administration Delegation Wizard does not provide enough granularity in assigning security. You can modify the security tab on the individual objects within Exchange. However, by default, the security tab is only displayed on the following objects:

- Address Lists
- Global Address Lists
- Databases (Mailbox stores and Public Folder stores)
- Top Level Public Folder Hierarchy

Normally, you will not need to modify the security options on other Exchange objects, however, it is possible to display the security tab on all Exchange objects.

Note: Be careful when changing permissions on Exchange objects. Incorrectly assigning deny permissions can lead to an inability to see Exchange objects in Exchange System Manager.

► **To display the Security tab on all Exchange objects**

1. Start **Regedt32.exe**.
2. Locate the following key in the registry:
HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin
3. On the **Edit** menu, click **Add Value**, and then add the following registry value:
Value Name : ShowSecurityPage
Data Type : REG_DWORD
Value : 1
4. Close **Registry Editor**.

This change takes effect immediately; you do not need to restart Exchange System Manager.

Note: As you are modifying a key within HKEY_CURRENT_USER, the change will only affect the logged on user at the computer you are working on.

Centralized and Distributed Administration

Generally, with respect to administration, there are two core models: centralized and distributed. The type of model you use depends upon the specific needs of your organization.

Centralized Administrative Model

The simplest model is a centralized model. Companies using this model delegate authority for managing their Exchange servers to one person, department or group. To implement this model, create a single administrative group containing all Exchange 2000 objects and assign permissions on the Exchange 2000 organization object.

Distributed Administrative Model

In the distributed model, more than one administrative group is created to represent logical groupings of the organization. These groupings may be geographical, political, or any other logical division of the organization. For example, within the same location, an organization may have three largely autonomous business units. Each business unit has its own IT department and is responsible for maintaining their own IT staff, budget, and responsibilities. Using the distributed administrative model, they can manage their own Exchange administrative tasks.

Mixed Administrative Model

In reality, it's likely that most implementations will neither be purely centralized or distributed, but rather will gravitate towards one model or the other. One useful model is to allow certain configuration choices to be made at the administrative group level, with the more significant ones being made centrally. For example, you may wish to allow administrators of each administrative group to be able to determine time periods for maintenance, but want to ensure that message tracking and mailbox storage limits are enforced throughout the organization.

Creating an Environment to Support a Mixed Administrative Model

There are a number of steps you will need to perform in order to support a mixed administrative model. These include:

- Creating one or more management administrative groups for the items under centralized control.

- Creating Exchange System Policies to centrally control individual settings.
- Assigning the appropriate security to ensure that certain settings cannot be altered by local administrators.

Creating Management Administrative Groups to Centralize Control

Typically, administrative groups are used to manage servers. However, as already mentioned, administrative groups are just a collection of objects that you are placing together for administrative purposes. This can help you to maintain tight administrative control over your Exchange organization. For example, you may determine that you want routine configuration of Exchange servers to be under the control of regional administrators. However, you wish routing decisions and the public folder hierarchy to be under centralized control. To achieve this, you would create a management administrative group and move the routing groups and public folders to that administrative group. If you then control the permissions on the management administrative group appropriately, you can prevent local administrators from changing those elements of Exchange.

Using Exchange System Policies to Enable a Mixed Administrative Model

You can use Exchange 2000 to create policies to control mailbox stores, public folder stores and servers. Policies can be applied to any or all of the corresponding objects in Exchange. If applied with the appropriate security settings, you can use policies to centrally control certain aspects of configuration, while altering other properties locally. Settings which may be configured in this way include message tracking and mailbox limits.

You should consider using system policies in conjunction with a management administrative group. If you place the policies in this group, local administrators will not be able to change the policy settings if they do not have the rights over the management administrative group.

The table shows settings in a simple environment, with two administrative groups for server control. In this example, administrators of each of the London and New York administrative groups have limited control over their servers and are able to make day to day routine changes. However, the servers have policies applied which they cannot alter, nor do they have any control over the management of the public folder hierarchy or routing between servers.

Table 2.2: Example of Mixed Administrative Model for Exchange 2000

Name	Contains	Policies Applied	Permissions
Management	Public Folders Container Routing Groups Container System Policies Container	None	Exchange Management – Allow Full Control Group A Admin – Deny Full Control Group B Admin – Deny Full Control
London	Servers	Server Policy Mailbox Store Policy Public Folder Store Policy	Exchange Management – Allow Full Control Group A Admin – Allow Full Control
New York	Servers	Server Policy Mailbox Store Policy Public Folder Store Policy	Exchange Management – Allow Full Control Group B Admin – Allow Full Control

Controlling User Administration

Under Exchange 2000, mailbox-enabled users, mail-enabled users and mail-enabled contacts are all controlled from Active Directory™ directory services Users and Computers settings. This allows you to delegate administrative authority over users at the organization unit level, separate from the rest of Exchange and give you great granularity of control.

Note: To modify Exchange settings for a user, the administrator must also have at least Exchange View Only Administrator Settings on the Exchange organization.

Summary

There are many elements to increasing the security of an Exchange 2000 environment. First, you need to ensure that the underlying Windows environment is as secure as possible (see *Security Operations for Microsoft Windows 2000 Server* for more details.) Then you will need to take measures to increase the security of Exchange 2000. This chapter and the following chapters will help you with those measures.

More Information

For Microsoft Exchange 2000 Server Operations:

<http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/maintain/operate/opsguide/default.asp>

For Microsoft Exchange 2000 Internals: Permissions Guide:

<http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/deploy/depovg/exchperm.asp>

To receive regular Microsoft Security bulletins:

<http://www.microsoft.com/technet/security/bulletin/notify.asp>

Details on the Security Rollup Package for Windows 2000 Server

<http://www.microsoft.com/technet/security/news/w2ksrp1.asp>

For Security Operations for Microsoft Windows 2000 Server:

<http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp>

Details on the recommended configuration and updates for Exchange 2000:

<http://www.microsoft.com/Exchange/techinfo/deployment/2000/BestConfig.asp>

Details on ensuring that mail from outside the Exchange organization remains unresolved:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288635>

Details on using reverse DNS lookup:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319356>

Details on preventing unsolicited mail using Outlook 2002:

<http://office.microsoft.com/assistance/2002/articles/OIManageJunkAndAdultMail.aspx>

Details on anti-virus software on an Exchange server:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q245822>

Details on filtering unsolicited mail using Exchange 2000 Server:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q276321>

Details on setting storage limits:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319583>

Details on Outlook 2002 security features:

<http://www.microsoft.com/office/techinfo/administration/security.asp>

3

Securing Exchange 2000 Servers Based on Role

In the previous chapter we examined some general recommendations for securing your Exchange 2000 environment. Now we look at the specifics of increasing the security of your Exchange 2000 servers based upon the role they perform in your IT environment.

Ensuring the security of Windows 2000 is fundamental to the security of Exchange 2000, as Exchange 2000 is an application that runs in a Windows 2000 environment. *Security Operations for Microsoft Windows 2000* gives you recommendations for securing particular server roles, and in this chapter we extend the recommendations given in that guide to incorporate Exchange 2000. We specifically examine the OWA front-end server and Exchange back-end server roles.

Note: This chapter is supplemental to the recommendations made in Chapters 3 and 4 of *Security Operations for Microsoft Windows 2000 Server*. For your convenience those chapters have been included at the back of this book as Appendices. For details on the rest of the guide, see the “More Information” section at the end of this chapter.

Test Environment

It is vital that you thoroughly assess any changes to the security of your IT systems in a test environment before you make any changes to your production environment. Your test environment should mimic your production environment as closely as possible. At the very least, it should include multiple domain controllers and each member server role you will have in the production environment.

Testing is necessary to establish that your environment is still functional after you make changes, but is also vital to ensure that you have increased the level of security as intended. You should thoroughly validate all changes and perform vulnerability assessments on the test environment.

Note: Before anyone performs vulnerability assessments in your organization, you should ensure that they have obtained written permission to do so.

Using OWA Front-End and Back-End Servers

By default, every Exchange 2000 server has OWA functionality, allowing users to connect to their Exchange server via Hypertext Transfer Protocol (HTTP). This is possible because the components that make up the OWA solution are installed on an Exchange server in a default installation. However, in most medium to large scale environments it is better to implement a front-end/back-end solution to allow access to OWA. In this case users connect to the front-end server, which then accepts the request, verifies user credentials in Active Directory, and then forwards the request to the appropriate back-end Exchange server. The back-end server provides access to mailboxes and public folders. This provides the following benefits:

- Users do not have to know the name of their local Exchange server in order to access it.
- The name of the servers holding the mailboxes are hidden.
- The front-end servers can be load balanced.
- Secure Sockets Layer (SSL) overhead can be offloaded to the front-end server.
- You can further secure the back-end server behind additional firewalls.

Note: Front-end servers can also be used for connections over POP3 and IMAP4. However, in this guide we are assuming that you will only be enabling HTTP and MAPI connections.

Note: For a detailed discussion of OWA front-end/back-end server environments in Exchange, see the “More Information” section at the end of this chapter.

Securing Server Roles for an Exchange 2000 Environment

For this guide, we have supplied security templates to modify the security on the Exchange 2000 server roles. You will need to import these templates into your Group Policy settings in order for them to be applied to Exchange.

The following table defines the server roles and the templates used to increase their security.

Table 3.1: Exchange 2000 Server Roles

Server Role	Description	Security Templates
OWA Server	Dedicated OWA front-end server for Outlook Web Access	Baseline.inf and OWA front-end Incremental.inf
Exchange 2000 back-end server	Server for mailbox, public folder access and routing	Baseline.inf and Exchange back-end Incremental.inf

In addition to the templates specified above, you will also need to apply an additional security template to your Baseline Group Policy for domain controllers. The settings defined in *Security Operations for Microsoft Windows 2000 Server* do not assume that Exchange will be part of your environment and so therefore require alteration to accommodate Exchange 2000.

To modify your domain controller settings, allowing them to support Exchange operations, we supply a template Exchange DC Incremental.inf. This should be imported into a Group Policy object (GPO) at the Domain Controllers organizational unit (OU). In fact only one setting is changed, the security option shown in the table.

Table 3.2: Security Option on Domain Controllers to Support Exchange 2000

Option	Security Operations for Windows 2000 Server	Security Operations for Exchange 2000 Server
Additional restrictions for anonymous connections	No access without explicit anonymous connections	None. Rely on default permissions
Shut down your system immediately if unable to log security audits	Enabled	Disabled
Account logon event auditing	Success and Failure	Failure
Logon event auditing	Success and Failure	Failure

The anonymous restriction setting needs to be changed because Outlook 2000 and 2002 clients will contact the global catalog server anonymously for information. With the settings defined in *Security Operations for Microsoft Windows 2000 Server*, Outlook users are unable to send internal mail and will have to use external addresses.

Note: For more information on this issue see the Knowledge Base article Q309622, "XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix."

The other settings are modified because of the large number of success logon events that Exchange 2000 generates. If success auditing is enabled for logon events the security log will be rapidly filled.

Note: For more information on this issue see the Knowledge Base article Q316685, "Active Directory-Integrated Domain Name Is Not Displayed in DNS Snap-in with Event ID 4000 and 4013 Messages."

Active Directory Structure to Support Exchange 2000 Server Roles

Security Operations for Microsoft Windows 2000 Server recommends an OU structure that allows you to easily adopt the security templates supplied. The OU structure recommended in that guide can easily be extended to incorporate the two new server roles defined here. Exchange 2000 is an application, so we create an Exchange Servers OU under the Application Servers OU and add further OUs for these server roles under the Exchange Servers OU.

The diagram on the facing page shows the OU structure recommended to accommodate the two new server roles.

Note: Creating the OU structure to support the recommendations in this guide is covered in much more detail in *Security Operations Guide for Microsoft Windows 2000 Server*.

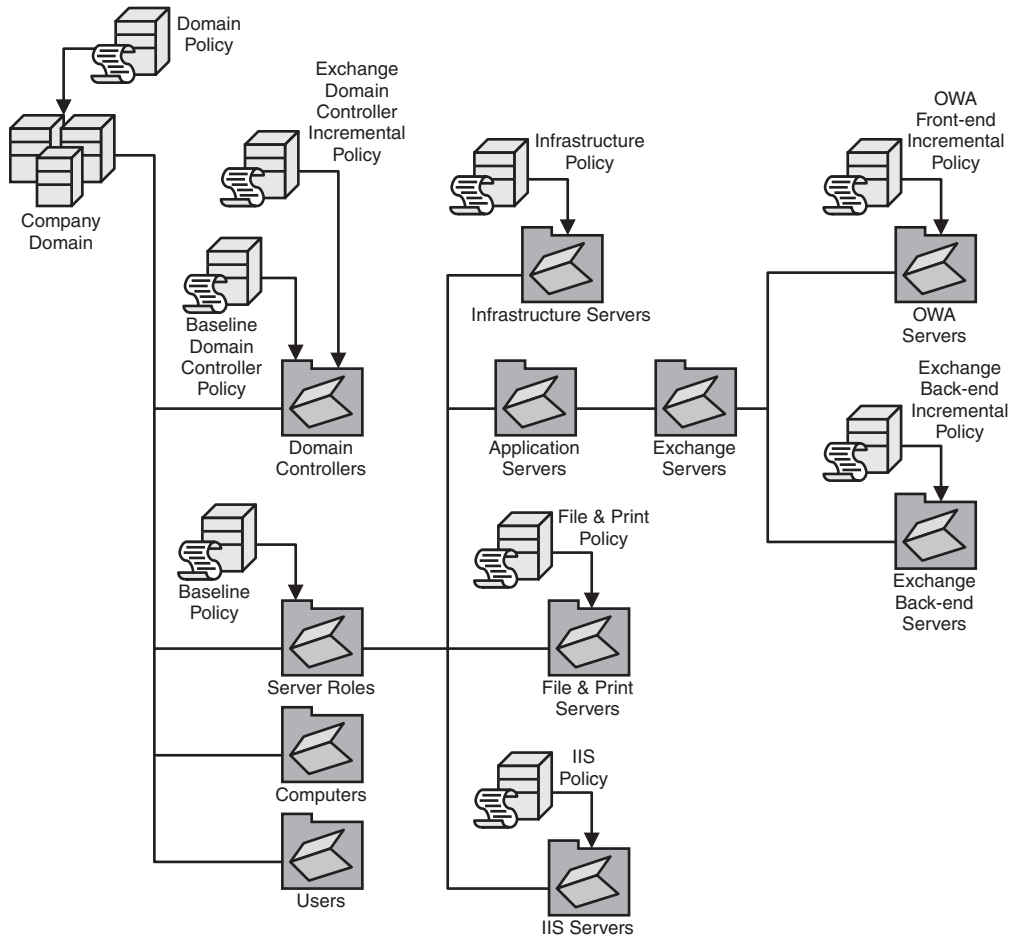


Figure 3.1
OU Structure with the Exchange Server and Application Server OUs added

Importing the Security Templates

The security templates described below are contained in the ExSecurityOps.exe file included with the guide. You will need to extract this file prior to importing the security templates. If you are using Windows 2000, Service Pack 2, you will also need to ensure that you have applied the hotfixes detailed in the following Knowledge Base articles:

- Q295444: SCE Cannot Alter a Service's SACL Entry in the Registry
- Q272560: Race Condition May Lead to Loss of Group Policy Changes

Note: You will have to contact Microsoft Product Support Services (PSS) to obtain the hotfixes discussed in the above Knowledge Base articles. More information on contacting PSS can be found at <http://support.microsoft.com>.

Warning: The security templates in this guide are designed to increase security in your environment. It is quite possible that by installing the templates included with this guide, you will lose functionality in your environment. This could include the failure of mission critical applications. It is therefore ESSENTIAL that you thoroughly test these templates before deploying them in a production environment, and make any changes to them that are appropriate for your environment. Back up each domain controller and server prior to applying new security settings. Make sure the system state is included in the backup, because this is where the registry data is kept, and on domain controllers it also includes all of the objects in Active Directory.

Note: The Domain Controller Baseline Policy and the Member Server Baseline Policy included in *Security Operations for Microsoft Windows 2000* set the LAN Manager Authentication level at NTLMv2 only. For Outlook clients to successfully communicate with Exchange servers and domain controllers they will also have to be configured to use NTLMv2 only.

The following procedure imports the security templates included with the guide into the OU structure suggested in this chapter.

► **To create the Domain Controller Group Policy Object and import the Security Template**

1. In **Active Directory Users and Computers**, right-click **Domain Controllers**, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new Group Policy object.
3. Type **Exchange DC Policy** and press **Enter**.
4. Click **Up** until the **Exchange DC Policy** is at the top of the list.
5. Click **Edit**.
6. Expand **Windows Settings**, right-click **Security Settings**, and select **Import Policy**.

Note: If **Import Policy** does not appear on the menu, close the Group Policy window and repeat steps 4 and 5.

7. In the **Import Policy From** dialog box, navigate to **C:\SecurityOps\Templates**, and double-click **Exchange DC Incremental.inf**.
8. Close **Group Policy** and then click **OK**.
9. Force replication between your domain controllers so that all domain controllers have the policy.

10. Verify in Event Log that the policy was downloaded successfully and that the server can communicate with the other domain controllers in the domain.
11. Restart each domain controller one at a time to ensure that it reboots successfully.

► **To create the Exchange Server Group Policy Objects and Import the Security Templates**

1. In **Active Directory Users and Computers**, expand **Member Servers**, expand **Application Servers**, expand **Exchange Servers**, right-click **OWA Front-End Servers**, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new Group Policy object.
3. Type **OWA Policy** and press **Enter**.
4. Click **Edit**.
5. Expand **Windows Settings**, right-click **Security Settings**, and select **Import Policy**.

Note: If **Import Policy** does not appear on the menu, close the Group Policy window and repeat steps 4 and 5.

6. In the **Import Policy From** dialog box, navigate to **C:\SecurityOps\Templates**, and double-click **OWA Front-end Incremental.inf**.
7. Close **Group Policy** and then click **OK**.
8. Repeat steps 1 through 7 for the **Back-end Servers OU** with **Exchange Back-end Incremental.inf**
9. Force replication between your domain controllers so that all domain controllers have the policy.
10. Move a server for each role into the appropriate OU.
11. On the server download the policy by using the **secedit /refreshpolicy machine_policy /enforce** command.
12. Verify in Event Log that the policy was downloaded successfully and that the server can communicate with the domain controllers and with other servers in the domain. After successfully testing one server in the OU, move the remaining servers in the OU and then apply security.

Note: For more information on verifying the success of the Group Policy download, see Appendix A: “Chapter 3: Managing Security with Windows 2000 Group Policy” of *Security Operations for Microsoft Windows 2000 Server*.

13. Restart each server to ensure that they reboot successfully.

Exchange Server Policies

It is possible to define a large number of security settings in Windows 2000, including auditing, security options, registry settings, file permissions and services. In *Security Operations for Microsoft Windows 2000 Server* we make suggestions for many of these settings and these recommendations do not need to be changed for Exchange 2000. The main area where additional settings are applied is for services, although we also make some file permission changes.

As they reside in OUs below the Member Servers OU, the Exchange servers inherit settings defined in the Member Server Baseline Policy. The Exchange policies modify those settings in two ways. First, some services that are not required for basic Windows 2000 functionality are needed for successful Exchange 2000 operations. Second, Exchange 2000 introduces a number of extra services, not all of which are required to allow the Exchange servers to function in their particular roles.

Note: Although not explicitly mentioned in the Exchange incremental policies, Network News Transfer Protocol (NNTP) is disabled by the Windows 2000 Member Server Baseline Policy. This service is required to install Exchange, but it is not needed for Exchange operations unless you require newsgroup functionality.

Exchange Back-End Server Policy

The Exchange Server Back-end Policy defines settings in two areas — services and file access control lists.

Exchange Back-End Server Services Policy

The table shows the services specified in the Exchange 2000 back-end policy:

Table 3.3: Services Configured in the Exchange Server Back-end Baseline Policy

Service Name	Startup Mode	Reason
Microsoft Exchange IMAP4	Disabled	Server not configured for IMAP4
Microsoft Exchange Information Store	Automatic	Needed to access Mailbox and Public Folder Stores
Microsoft Exchange POP3	Disabled	Server not configured for POP3
Microsoft Search	Disabled	Not required for core functionality
Microsoft Exchange Event Service	Disabled	Only needed for backwards compatibility
Microsoft Exchange Site Replication Service	Disabled	Only needed for backwards compatibility
Microsoft Exchange Management	Automatic	Required for message tracking to function

Service Name	Startup Mode	Reason
Windows Management Instrumentation	Automatic	Required for Microsoft Exchange management
Microsoft Exchange MTA Stacks or if there are X.400 connectors	Disabled	Only needed for backwards compatibility
Microsoft Exchange System Attendant	Automatic	Needed for Exchange maintenance and other tasks
Microsoft Exchange Routing Engine	Automatic	Needed to coordinate message transfer between Exchange servers
IPSEC Policy Agent	Automatic	Needed to implement IPSec policy on server
RPC Locator	Automatic	Needed for communication with domain controllers and clients
IIS Admin Service	Automatic	Required by Exchange routing engine
NTLM Security Support Provider	Automatic	System Attendant depends on this service
SMTP	Automatic	Required for Exchange transport
World Wide Web Publishing Service	Automatic	Required for communication with OWA front-end servers

Note: The Exchange System Attendant depends on the following services to be up and running before it will start:

- Event Log
- NTLM Security Support Provider
- RPC
- RPC Locator
- Server
- Workstation

Key Services That Are Disabled

For the purposes of this guide we have disabled all the services that are not essential for the core functionality of Exchange 2000. In some cases you may need to re-enable services, providing you with the functionality you require in your environment. Here is a description of the key services disabled by the Back-end Server Incremental Policy.

Event Service

Introduced in Exchange Server 5.5, the Exchange Server Event Service supports server-side scripts triggered by folder events, either in public folders or individual mailboxes. Exchange Event Service is provided in Exchange 2000 for backward compatibility with Exchange 5.5 event scripts. New applications written specifically for Exchange 2000 should use native Web Storage System Events instead of Exchange Event Service, as described in the Exchange 2000 Software Development Kit (SDK) available on MSDN, see the “More Information” section for further details.

Microsoft Search

The information store process creates and manages indexes for common key fields for faster lookups and searches of documents that reside in a store. An index allows Outlook users to search for documents more easily. With full-text indexing, the index is built prior to the client search, thus enabling faster searches. Text attachments can be included in the full-text indexing.

Indexing is provided by the Microsoft Search service. Both the Information Store service and the Search service must be running for the index to be created, updated, or deleted.

Microsoft Exchange Site Replication Service

The service responsible for replicating Exchange 5.x site and configuration information to the configuration naming partition of Active Directory when an Exchange 2000 server belongs to an existing Exchange 5.5 site.

Microsoft Exchange MTA Stacks

This is an additional component connecting Exchange 2000 Server to foreign systems. The message transfer agent (MTA) is responsible for the routing of messages through X.400 and gateway connectors to foreign environments. This service maintains its own specific message queues outside the Information Store service in the \Program Files\Exchsrvr\Mtadata directory.

Exchange Back-End Server File Access Control Lists Policy

The Exchange back-end Server Policy modifies access control lists (ACL) on several directories. The table shows the settings that are defined.

Table 3.4: File Access Control Lists Configured by the Exchange Back-end Server Policy

Directory	Old ACL	New ACL	Applied to Subdirectories?
%systemdrive%\inetpub\mailroot	Everyone: Full Access	Domain Admins: Full Access Local System: Full Access	Yes
%systemdrive%\inetpub\nntpfile\	Everyone: Full Access	Domain Admins: Full Access Local System: Full Access	Yes
%systemdrive%\inetpub\nntpfile\root	Everyone: Full Access	Everyone: Full Access	Yes

Note: The settings defined on the nntpfile directory and subdirectories are not strictly required as NNTP does not run on the server. However, we define the setting as it increases restrictions on the file system and is ready to use in case you later decide to enable NNTP.

OWA Front-End Server Policy

The OWA Front-end Policy defines settings in two areas — services and file access control lists.

OWA Front-End Server Services Policy

Since the role of this server is to only support Web-based e-mail, many of the Exchange services installed by the default configuration can be disabled. The table shows the services that are configured in the OWA Front-end Server Policy.

Table 3.5: Services configured in the OWA Front-end Server Policy

Service Name	Startup Mode	Reason
Microsoft Exchange IMAP4	Disabled	OWA server not configured for IMAP4
Microsoft Exchange Information	Disabled	Not required as there is no Mailbox Store or Public Folder Store
Microsoft Exchange POP3	Disabled	OWA server not configured for POP3
Microsoft Search	Disabled	No stores to search
Microsoft Exchange Event	Disabled	Only needed for backwards compatibility
Microsoft Exchange Site Replication Service	Disabled	Only needed for backwards compatibility
Microsoft Exchange Management	Disabled	Required for message tracking
Microsoft Exchange MTA	Disabled	Only needed for backwards compatibility or if there are X.400 connectors
Microsoft Exchange Routing Engine	Automatic	Provides Exchange routing functionality
IPSEC Policy Agent	Automatic	Needed to implement IPSec filter on OWA server
RPC Locator	Automatic	Needed for communication with domain controller and required for system attendant to start
IIS Admin Service	Automatic	Required by MExchange routing engine
World Wide Web Publishing Service	Automatic	Required for client communication with OWA front-end servers

Key Services Disabled in the OWA Front-End Server Policy

As with the back-end configuration, you may need to re-enable some services, providing you with the functionality you require in your environment. Here is a description of the key services disabled by the OWA Front-end Server Incremental Policy.

Microsoft Exchange POP3 and Microsoft Exchange IMAP4

As already mentioned in Chapter 2, you should determine whether you need the full functionality of Exchange in your environment. In many cases you will not have POP3 or IMAP4 clients and so you can ensure that these services are disabled by Group Policy. You should also confirm that you do not have any custom programs running in your environment that require this functionality before you disable it.

System Attendant

On a front-end server, the System Attendant is only required if you wish to make configuration changes to the server. We therefore disable the System Attendant in the template. This means that to make any changes to a server which uses the OWA Front-end Server Policy (including making the server an OWA Front-end server), you need to temporarily start the System Attendant and associated services first.

► To make a change to the configuration of a server with the OWA Front-end Server Group Policy applied

1. Start the **Services** administrative tool.
2. Right-click **NTLM Security Support Provider** and select **Properties**.
3. In the **Startup Type** drop down list box, select **Automatic**.
4. Click **Apply**.
5. Click **Start**.
6. Click **OK**.
7. Repeat steps 2 through 6 for **System Attendant**.
8. Make any configuration changes you require.
9. Start the **Services** administrative tool.
10. Right-click **System Attendant** and select **Properties**.
11. In the **Startup Type** drop down list box, select **Disabled**.
12. Click **Apply**.
13. Click **Stop**.
14. Click **OK**.
15. Repeat steps 2 through 6 for **NTLM Security Support Provider**.

Information Store

The Information Store service is not required since no mail is delivered to this server. With no Information Store service, the M: mapped drive that you normally find on all Exchange 2000 servers will be removed. This is to be expected, as the Exchange installable file system will have nothing to map to.

Microsoft Exchange Management

This service was introduced as part of Exchange 2000 Server, Service Pack 2. The service allows you to specify, through the user interface, which domain controller or global catalog server Exchange 2000 will use when accessing the directory. It is also required for message tracking. You can disable this service without affecting the core functionality of Exchange. However, you will probably find that you require Message Tracking as part of your auditing of Exchange functionality. In this case, the OWA front-end server is used to access mail rather than to route mail, you should not find that the Microsoft Exchange Management Service needs to run on your OWA front-end servers.

SMTP Service

The OWA front-end server does not require SMTP in this case because it is only acting as an OWA server. You will need to enable the SMTP service, if you have configured your front-end server to receive SMTP mail, either to act as a gateway, or as a front-end server for IMAP4 or POP3. If the server will also be an SMTP gateway, the Information Store and System Attendant services are also required.

OWA Front-End Server File Access Control Lists Policy

The policy defines file access control lists in exactly the same way as the Back-end Server Policy. For details, see "Exchange Back-End Server File Access Control Lists Policy" earlier in this chapter.

Installing and Updating Exchange in an Increased Security Environment

If you have followed the procedures specified so far in this chapter, you will have moved existing Exchange servers into the appropriate OUs to increase the level of security in your environment. To maximize your security, new servers must be moved into the appropriate OU prior to installing Exchange. However, while the environment will allow core Exchange services to run, it will not, by default, allow Exchange to install, or allow you to upgrade Exchange to future service packs. To install Exchange or Exchange Service Packs on locked down servers, use the following procedure.

Note: When installing Exchange 2000 on a server that has already been secured, you will receive “Digital Signature Not Found” errors. This is a result of the increased security on the server and can be bypassed.

► **To install Exchange or an Exchange Service Pack on a locked down server**

1. Start the **Services** administrative tool.
2. Right-click **Distributed Transaction Coordinator** and select **Properties**.
3. In the **Startup Type** drop down list box, select **Automatic**.
4. Click **Apply**.
5. Click **Start**.
6. Click **OK**.
7. Repeat steps 2 through 6 for **Network News Transport Protocol (NNTP)** and **Windows Installer**.

Note: If you are performing these steps on a server in the OWA Front-End OU, also repeat steps 2 through 6 for **Windows Management Instrumentation**.

8. Install Exchange 2000 or the latest Exchange 2000 Service Pack.

Note: When installing Exchange 2000, at the end of setup a dialog box may appear indicating a non-fatal setup error occurred because the Microsoft Search service did not start. This is expected when installing an already secured server and can safely be ignored.

9. Start the **Services** administrative tool.
10. Right-click **Distributed Transaction Coordinator** and select **Properties**.
11. In the **Startup Type** drop down list box, select **Disabled**.
12. Click **Apply**.
13. Click **Stop**.
14. Click **OK**.
15. Repeat steps 2 through 6 for **Network News Transport Protocol (NNTP)** and **Windows Installer**.

Note: If you are performing these steps on a server in the OWA Front-End OU, also repeat steps 9 through 14 for **Windows Management Instrumentation**.

Note: The incremental policies for OWA front-end and Exchange back-end servers enable NTLMv2. This allows the Exchange servers to communicate with your secured domain controllers. If you do not place your servers in the appropriate OU prior to installing Exchange, the servers will not be able to contact domain controllers.

Additional Security Measures

In addition to the enhanced security provided by the Group Policy templates, there are additional security measures that should be implemented on Exchange 2000 servers. This section covers those measures.

IIS Lockdown Tool

After the security template is applied to your Exchange 2000 servers, you will need to apply additional security controls on IIS, particularly on your OWA front-end servers. To automate many of the changes to IIS, the IIS Lockdown tool can be used. IIS Lockdown will specify settings needed to harden IIS, but still allow Exchange 2000 to function as either a back-end server or an OWA front-end server.

Note: The IIS Lockdown tool can be obtained from <http://www.microsoft.com/technet/security/tools/tools/locktool.asp>

The IIS Lockdown tool has two modes: an express mode appropriate for most basic Web servers and an advanced mode that allows administrators to pick and choose the technologies the server will support. The tool provides an undo feature that allows the effects of the most recent lockdown to be reversed.

IIS Lockdown also implements URLScan, which screens all incoming requests to an IIS server and only allows those that comply with a specific rule set to pass. This significantly improves the security of the server by helping to ensure that it responds only to valid requests. URLScan allows you to filter requests based on length, character set, content and other factors. A default rule set is provided, which can be customized to meet the needs of a particular server.

► To lockdown Exchange 2000 OWA front-end servers

1. Install and start **IISLockd.exe** on your server.
2. Click **Next**.
3. Read the license agreement, select **I Agree**, and then click **Next**.
4. Select the server template **Exchange 2000 (OWA, PF Management, IM, SMTP, NNTP)**, select the **View Template** check box, and then click **Next**.
5. In the **Internet Services** dialog box, four services will be displayed (Web Service (HTTP), FTP, SMTP, and NNTP). If the check box is dimmed for a specific service, then that service is either not installed or already disabled. Make sure that only **Web Service (HTTP)** is enabled and click **Next** to continue.

Note: If IIS Lockdown is executed after applying the OWA front-end security template from the Group Policy object, then the Web Service (HTTP) should be the only service displayed as enabled while all the other services are disabled.

6. The **Script Maps** dialog box allows you to disable support for specific ISAPI applications by removing their associated script map. The table shows the default settings that are implemented within the Exchange 2000 template. Only Active Server Pages will be enabled. All other script mappings will be disabled. Click **Next**.

Table 3.6: Default Script Mapping Settings in the Exchange 2000 Template for IISLockDown

Type	Entry	Status
Active Server Pages	.asp	Enabled
Index Server Web Interface	.htw, .ide, .idq	Disabled
Server-side Includes	.stm, .shtm, .shtml	Disabled
Internet Data Connector	.idc	Disabled
HTR Scripting	.htr	Disabled
Internet Printing	.printer	Disabled

Note: If you disable support for the .htr script map then the OWA change password feature will not work. This OWA feature is disabled by default by IIS LockDown.

7. The options in the **Additional Security** dialog box allow you to remove the default virtual directories that are created from the default IIS installation, and apply file ACLs to specific directories and to all the system32 executables. Click **Next** to continue.

The table shows the virtual directories that will be removed.

Table 3.7: Virtual Directories Removed by IISLockdown

Name	Virtual Directory	Default Location
IIS Samples	\IISamples	c:\inetput\iissamples
IISHelp	\IISHelp	c:\winnt\help\iishelp
MSADC	\MSADC	c:\program files\common files\system\msadc
Scripts	\Scripts	c:\inetpub\scripts
IISAdmin	\IISAdmin	c:\winnt\system32\inetsrv\iisadmin

To restrict access to the file system, IIS Lockdown will create two new local groups on the OWA server called Web Anonymous Users and Web Applications. It will place any anonymous users or anonymous application accounts in the applicable group. Typically, IUSR_<computername> will be placed in the Web Anonymous Users group and IWAM_<computername> will be placed in the

Web Applications group. IIS Lockdown will then set permission denying write access for these groups to the specific directories

C:\inetpub\wwwroot

C:\Program Files\Exchsrvr\ExchWeb

and also denying execute access to all system utilities, such as cmd.exe, in the c:\winnt\system32 folder. Remember that Group Policy from the baseline template will apply a specific access control entry (ACE) to the executables in the system directory allowing only Administrators Full Control and no other users or groups will be defined. These settings will override the IIS Lockdown setting when Group Policy is reapplied.

8. You will now be prompted to install the **URLScan**. By default it is already checked to be installed. Click **Next**.
9. Review the tasks to be performed and then click **Next**.
10. The **Installing Unknown Software Package** dialog box appears because of the increased security, click **Yes**.
11. IIS Lockdown will produce a report detailing the changes that were made and if there are any errors to report. You will see errors in the report that IIS Lockdown failed to ACL some NTFS directories. These directories are the mailbox and public folders that were deleted as part of the OWA server configuration. Click **Next**.
12. Click **Finish**.

Note: To run IIS Lockdown on an Exchange 2000 back-end server, repeat the above procedure and in step 5 ensure that HTTP and SMTP are enabled.

Modifying IIS Lockdown and URLScan Settings for OWA Front-End Servers

You may need to modify the default IIS Lockdown and URLScan settings for your environment. The URLScan settings are stored in the URLScan.ini file located in <WinDir>\System32\Inetsrv\Urlscan. If you encounter any issues with OWA and UrlScan is enabled, examine the Urlscan.log file in <WinDir>\System32\Inetsrv\Urlscan for the list of requests that are being rejected.

Note: For information on troubleshooting and configuring IIS Lockdown and URLScan, see the Knowledge Base article Q309677, "XADM: Known Issues and Fine Tuning When You Use the IIS Lockdown Wizard in an Exchange 2000 Environment."

Change Password Support in OWA

By default, IIS Lockdown disabled .httr files. When this file type is disabled, the OWA Change Password feature does not function. If .httr files are disabled, you should also hide the Change Password button in OWA to avoid user confusion and help desk calls.

Note: For information on disabling the Change Password button in OWA, see the Knowledge Base article, "Q297121 XWEB: How to Hide the "Change Password" Button on the Outlook Web Access Options Page."

Blocked E-Mail

The [DenyUrlSequences] section of the URLScan.ini file, lists characters that are explicitly blocked can potentially affect access to OWA. Any e-mail subject or mail folder name that contains any of the following character sequences is blocked:

- ..
- ./
- \
- %
- &

Note: The "." in the URLScan.ini file will block e-mail messages with a subject line that ends with a period character.

Dismounting the Mailbox Store and Deleting the Public Folder Store

As the role of the OWA front-end server is to forward requests to the back-end servers, you do not need Exchange Server mailboxes or public folders on the OWA front-end servers. The back-end Exchange server will manage them. You can therefore dismount and delete these stores.

► To dismount and delete the mailbox and public folder databases

1. Start the **Services** administrative tool.
2. Right-click **NTLM Security Support Provider** and select **Properties**.
3. In the **Startup Type** drop down list box, select **Automatic**.
4. Click **Apply**.
5. Click **Start**.
6. Click **OK**.
7. Repeat steps 2 through 6 for **System Attendant**.

8. Start **Exchange System Manager** on the OWA front-end server.
9. Expand **Servers**, expand the **OWA front-end server**, and then expand **First Storage Group**.
10. If the mailbox store is mounted, right-click **Mailbox Store**, select **Dismount Store**, and then click **Yes** to dismount the mailbox store.
11. Right-click **Mailbox Store** and select **Properties**.
12. Select the **Database** tab, click the **Do not mount this store at start-up** check box, and then click **OK**.
13. If the public folder store is mounted, right-click **Public Folder Store**, select **Dismount Store**, and then click **Yes** to dismount the public folder store.
14. Right-click **Public Folder Store** and select **Delete**.
15. Click **Yes**, click **OK**, select a back-end server, and then click **OK**.
16. Click **Yes** to delete the public folder store, and then click **OK** to close the message.
17. Restart the OWA Server.

Note: You do not need to disable the NTLM Security Support Provider and the System Attendant again as this will happen automatically when the server is rebooted.

Note: The private store needs to be mounted if you have SMTP running on the front-end server.

Note: Once the mailbox store and public folder store are dismounted, the M: mapped drive that you normally find on all Exchange 2000 servers will be removed. This is to be expected, as the Exchange installable file system will have nothing to map to.

You will notice event errors (Event ID 101) in the system log indicating that the path to a specific virtual directory is invalid. These virtual directories, "public, Exchange, and Exadmin", will also display a status of "Stop" in the Internet Services Manager console. These errors will be produced after the Exchange Server is installed on the IIS server and then the server is rebooted. After a reboot, the IIS (W3SVC) service will start up before the Exchange Information Store service starts. The Information Store service is responsible for creating the mapped virtual drive (M:) that these 3 virtual directories are assigned to and since the mapped drive is not created yet, IIS will produce the error messages. Since the Information Store service is disabled when security is applied through Group Policy, the mapped virtual drive will never be mounted and these errors will continue to appear in the Event Log. However, they are completely harmless.

Note: For more information on the Event Log ID 101, see Knowledge Base article Q259373, "XADM: W3SVC Logs Event ID 101 in the System Event Log."

Changing the SMTP Banner

The less information you provide an attacker, the more difficult it is to attack your system. One way an attacker may attempt to gain information about which version of Exchange is being run is to use Telnet to connect to the SMTP service. By default, when you connect to the SMTP service on an Exchange server, the following banner is displayed:

```
220 hostname . domain .com Microsoft ESMTP MAIL Service, Version: 5.0.2195.1600
ready at current date and time.
```

You should consider changing this on all back-end Exchange servers so that it does not display the specific version. You may also wish to include a legal statement that unauthorized use of the SMTP service is prohibited.

► To modify the Windows 2000 SMTP banner

1. Using a metabase editing tool such as MetaEdit, locate:
Lm\Smtpsvc\ virtual server number.
2. Click **Edit** , click **New** , and then click **String**.
3. Verify that the entry in the **ID** box is **Other**, and then type **36907 (decimal)** on the right side of the **ID** box.
4. In the **Data** box, type the banner that you want to be displayed.
5. Stop, and then restart the SMTP virtual server or the SMTP service.

To confirm that the banner has been changed, Telnet to port 25 of the virtual server (the default setting). The "ESMTP MAIL Service, Version: 5.0.2195.1600" banner should no longer be displayed. However the fully qualified domain name (as it was entered in the SMTP service properties) and the date and time are still displayed.

Group Lockdown for Exchange Domain Servers

As part of a default installation, an Exchange Domain Servers group is created for each domain within the forest. This group contains the computer accounts for each Exchange server within a given domain. By default the Exchange Domain Servers groups are granted access to all Exchange public folder and mailbox stores in the forest. You can restrict access to mailbox stores to only the local server that hosts the stores by running the EDSLock script.

Note: For further details on the EDSLock script see Knowledge Base article Q313807, "XADM: Enhancing the Security of Exchange 2000 for the Exchange Domain Servers Group."

Exchange Cluster Considerations

Exchange 2000 in a clustered environment is not within the scope of this guide. However, it is clear that you will need to make certain changes to the security settings shown here to allow Exchange 2000 to work in a clustered environment. These include:

- Enabling NTLM on the cluster servers and domain controllers as NTLMv2 is not supported on Windows 2000 clusters, see the Knowledge Base article Q272129, "Cluster Service Does Not Start on "Joining" Node in Windows 2000".
- Modifying the setting for the NTLM Security Support Provider (NTLMSSP) in the Security Template for your Exchange back-end servers. NTLMSSP must be set to 0:

```
MACHINE\System\CurrentControlSet\Control\LSA\MSV1_0\NtlmMinServerSec=4,0
```
- Enabling the Cluster service in the Security template for your Exchange back-end servers.
- Not implementing IPSec for OWA front-end/back-end communication as IPSec is not supported on clusters, see Knowledge Base article 306677, "IPSec Is Not Designed for Failover."

Summary

Increasing the security of your Exchange Servers is a vital part of securing your enterprise. If you follow the advice listed in this and the previous chapter, along with increasing the security of your Windows 2000 environment, you will significantly reduce the risk of successful attack against your Exchange environment.

More Information

For the complete *Security Guide to Microsoft Windows 2000 Server*:

<http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp>

For a detailed discussion of OWA front-end/back-end server environments in Exchange:

<http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2KFrontBack.asp>

Details on the effects of Windows 2000 security fixes on the global catalog server:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309622>

Details on enabling success auditing for logon events filling the security log:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316685>

For a detailed discussion of native Web Storage System Events:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wss/wss/_exch2k_welcome_to_exchange.asp?frame=true

To obtain the IIS Lockdown tool:

<http://www.microsoft.com/technet/security/tools/tools/locktool.asp>

Details on troubleshooting and configuring IIS Lockdown and URLScan:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309677>

Details on disabling the Change Password button in OWA:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q297121>

Details on the Event Log ID 101:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q259373>

Details on the EDSLock script:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313807>

Details on NTLMv2 not supported on Windows 2000 clusters:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q272129>

Details on not implementing IPSec for OWA front-end/back-end communication:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306677>

4

Securing Exchange Communications

When you increase the security of any network, you should not only examine the security of the computers themselves, but also the data that travels between them. As with any system, the best approach is to look at the functionality that is available, and examine what you require, considering the risk posed by each piece of functionality.

In this guide we are assuming that you require the ability to a) send and receive e-mail over the Internet and b) access Exchange over the Internet using Outlook Web Access. If you do not require these pieces of functionality, you will be able to lock down your systems more. On the other hand, if you require POP3 and IMAP4 functionality, you will need to open up the environment to accommodate them.

The front-end/back-end environment suggested in this guide will allow you to send mail to and from the Internet, and to offer Exchange access over the Internet. This chapter looks at how to secure that communication, and also examines securing communication at the client.

Note: It is possible to access Outlook over the Internet by using an Exchange remote procedure call (RPC) application filter provided with ISA Server. This method of accessing Exchange is not covered in this guide. See the “Configuring and Securing Microsoft Exchange 2000 Server and Clients” white paper and the *Microsoft Exchange 2000 Server Hosting Series* (Microsoft Press, ISBN: 0-7356-1829-1 and 0-7356-1830-5) listed in the “More Information” section.

Securing Communications in Outlook 2002

There are a number of measures you can take in Outlook 2002 to increase the security of your communications. These include:

- Encrypting the MAPI connection from Outlook 2002 to the Exchange server
- Signing and encrypting messages using S/MIME certificates

Encrypting the MAPI Connection from Outlook 2002 to Exchange Server

Windows 2000 has a built-in security feature allowing for 128-bit encryption of RPC communication. MAPI connections take place over RPC and so you can take advantage of this feature to increase the security of your connection from the Outlook 2002 client to the Exchange server.

► **To enable RPC encryption of the of the MAPI connection from Outlook 2002 to Exchange server**

1. In Outlook 2002, click **Tools**, and then **E-mail accounts**.
2. Click **Next**.
3. Ensure the Exchange server is selected, and click **Change**.
4. Click **More Settings**.
5. Click the **Advanced** tab.
6. Check **When using the Network**.
7. Click **OK**.
8. Click **Next**.
9. Click **Finish**.

Note: You can also specify this setting when setting up User profiles in Outlook 2002.

RPC encryption only encrypts the data from the MAPI client to the Exchange server. It does not encrypt the messages themselves.

Signing and Encrypting Messages

Outlook 2002 has the ability to sign and encrypt messages for delivery to internal or external recipients. For this encryption you will need a certificate. If you want to deliver signed and/or encrypted e-mail to Internet recipients, you will need to use a recognized certificate (known as a Digital ID) from a third-party vendor.

Once you have a certificate installed on the client, you can begin to send signed and encrypted messages using S/MIME. You can only send encrypted mail to other

users if you have access to their public key. This is achieved by having the other user send you a signed message and then adding that user to your contacts. You will now have their public key available.

Note: For more information on signing and encrypting messages see Knowledge Base article Q286159, "Encryption and Message Security Overview."

Key Management Service

If you wish to routinely send signed and encrypted messages between users inside your Exchange organization, you should consider using the Key Management service provided with Exchange 2000. This service uses Windows 2000 Certificate Services and provides access to public keys with secure, centralized access to private keys. This gives clients seamless access to signed and encrypted messages, allowing them to send these messages to any other security-enabled recipient in the global address list (GAL).

Note: If you use Key Management Server with a certificate authority (CA) that is subordinate to a third-party CA, you can integrate your Key Management service with others on the Internet.

Securing OWA Communications

Upon initial review, communications with OWA are very simple. Web browsers communicate with OWA servers for e-mail. This occurs over port 80, or port 443 if the communication is secure. However, that is not the end of the story. While clients do connect to front-end servers over port 80 or port 443, those front-end servers then need to communicate with domain controllers in their domain to authenticate the users. They also need to communicate with Exchange back-end servers to actually access information from the appropriate mailbox or public folder.

OWA front-end servers can be secured by placing them inside a perimeter network (also known as DMZ), with the back-end server inside the inner firewall. However, in order for this to work, a large number of ports have to be opened on the inner firewall.

Using ISA Server to Secure OWA

To minimize the ports you need to open on the inner firewall, you can use an application layer firewall, such as Microsoft Internet Security and Acceleration (ISA) Server. ISA Server allows you to position both your SMTP server and your OWA front-end server behind the firewall. Using Server Publishing and Web Publishing rules, ISA Server will impersonate internal servers to the outside world without placing those servers in the DMZ.

Note: For a list of the ports used for communication between front-end and other servers, see the “Exchange 2000 Front-end and Back-end Topology” white paper listed in the “More Information” section at the end of the chapter.

The diagram shows an ISA Server publishing an OWA Server to OWA clients on the Internet:

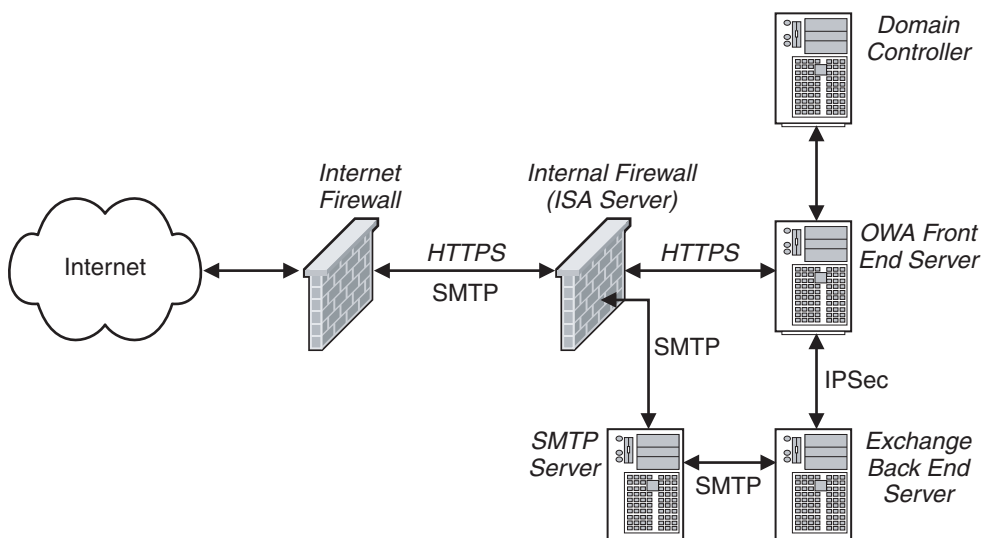


Figure 4.1

Secure Firewall Structure

Note: In this configuration, external DNS entries for the front-end OWA server will need to refer to the IP address published on the ISA Server, not the address of the OWA front-end server.

Note: If you are not able to change your existing two firewall infrastructure to accommodate ISA Server, you can place ISA Server inside your current inner firewall and pass TCP port 443 through to the ISA server.

Firewalls will help protect your servers from being attacked. However, you also need to protect the data that is traveling to and from your servers. When Web browser clients on the Internet access Exchange via OWA using HTTP, the following occurs:

- An HTTP request is sent to the ISA Server from the Web browser. If permitted by the ISA publishing rules, the requests are passed to the OWA front-end servers.

- ISA Server establishes a new HTTP connection to the front-end server with its own IP address as the source IP address.
- The HTTP requests are processed on the OWA front-end server. As part of the processing, the OWA front-end server:
 - authenticates the user and contacts against the global catalog server to determine the location of the user mailbox.
 - resolves the IP address of the user mailbox server.
- The OWA front-end server establishes a new HTTP session to the back-end Exchange server.

As part of the configuration of IIS to support OWA you need to enable basic authentication. Integrated Windows authentication will not work as the only protocol being used for communication is either HTTP or HTTPS, and you must not use anonymous access as this will open up your e-mail environment to anyone on the Internet.

Basic authentication means that over an HTTP connection, passwords and e-mail will pass over the Internet in an unencrypted form. If no additional encryption methods are used, these packets continue to travel unencrypted between the ISA Server and the OWA front-end server in clear text. After OWA performs authentication, the same unencrypted information, including passwords, will be sent over HTTP between OWA front-end server and back-end server. To prevent this from happening, it is vital to encrypt the user credentials along the entire path between the Web browser and the back-end Exchange server. This can be accomplished by:

- Securing communication between Web browsers and ISA Server using SSL encryption
- Securing communication between ISA Server and OWA front-end servers using SSL.
- Securing communication between OWA front-end servers and back-end Exchange servers using IPSec encryption.

We will examine each of these in turn.

Securing Communication Between Web Browsers and ISA Servers

To encrypt the data between Web browsers and an ISA Server using SSL, you need to install an SSL certificate on the ISA Server and the appropriate SSL listener. Your certificate should be issued by a globally trusted CA because it will be used by external Web clients that may not be part of your organization's infrastructure.

Configuring ISA Server to Support SSL Communications

ISA Server can be configured in a number of ways to accept SSL requests from Web browsers. It can:

- Receive SSL communications and pass them on to servers inside the firewall.
- Decrypt SSL communications and pass them on unencrypted to the back-end.
- Decrypt SSL communications and re-encrypt them before passing them on to the back-end.

Note: Decrypting and re-encrypting SSL communication requires ISA Server SP1 or later. The below procedures will not work correctly unless ISA Server SP1 or later is installed.

Of these three methods, the most secure is to decrypt the packets and re-encrypt them again, because this allows the ISA Server to inspect the data for vulnerabilities. It also protects the data from attack inside the ISA Server.

Note: The laws of certain countries may prevent you from decrypting data and inspecting it at an intermediary point in your network. You should check the legal implications of this solution before adopting it.

Note: To improve the performance and reduce the overhead of SSL, you should consider using SSL accelerator network adapters.

To successfully encrypt the data, you should ensure the following:

- The ISA Server certificate for OWA needs to have the common name, also known as friendly name, that matches the Fully Qualified Domain Name (FQDN) used by the Web browsers to reference OWA resources. For example, if the OWA URL used by the client is **https://mail.nwtraders.com/exchange** the certificate common name should be **mail.nwtraders.com**.
- The certificate must be imported into the *Personal* computer store of the ISA Server or servers publishing the OWA resources. When importing the certificate into your ISA Server, make sure that **Mark the private key as exportable** is enabled.
- To avoid accidental transmission of clear text passwords, ISA Server should allow only secure channel and reject clear text HTTP connections for the published OWA site.

ISA Server uses a Web Publishing Rule to make the OWA server available to Internet clients. However, before creating the Web Publishing Rule, Web Publishing itself must be prepared on the ISA Server. This is done by configuring **Incoming Web Requests** and **Outgoing Web Requests**.

Note: Before completing the following procedure, you need to import your external certificate.

► **To configure Incoming Web Requests**

1. Start **ISA Management**.
2. Right-click your ISA Server and select **Properties**.
3. Click the **Incoming Web Requests** tab.
4. Select **Configure listeners individually per IP Address**, and then click **Add**.
5. Select your ISA Server and select the external IP address of your ISA Server.
6. Select **Use a server certificate to authenticate web clients**.
7. Click **Select** and select the certificate for the FQDN clients will be using to access the SSL site.
8. Click **OK**.
9. Select **Enable SSL Listeners**.
10. Click **OK**.
11. Click **OK**.
12. Click **Save the changes and restart the service(s)**, and then Click **OK**.

► **To configure Outgoing Web Requests**

Note: Performing the following procedure will prevent users on the internal network from using the ISA Server as a proxy server to access web sites on the Internet. This procedure is not needed to make OWA available through ISA but is included for additional security.

1. Start **ISA Management**.
2. Right-click your ISA Server and select **Properties**.
3. Click the **Outgoing Web Requests** tab.
4. Select **Configure listeners individually per IP Address**, ensure no IP addresses are listed, and then click **OK**.
5. Click **Save the changes and restart the service(s)**, and then Click **OK**.

You are now in a position to configure Web Publishing to support OWA.

► **To configure Web Publishing for OWA**

1. In **ISA Management**, expand your ISA Server, and then expand **Publishing**.
2. Right-click **Web Publishing Rules**, select **New**, and then select **Rule**.
3. Provide a name, such as *OWA-<FQDN of OWA Front-end Server>* and then click **Next**.
4. Verify **All destinations**, and then click **Next**.
5. Verify **Any request** is selected, and then click **Next**.

6. Select **Redirect the request to this internal Web server (name or IP Address)**, click **Browse** and select your OWA front-end server.
7. Select **Send the original host header to the publishing server instead of the actual one (specified above)**, and then click **Next**.
8. Click **Finish**.
9. In the folder pane click **Web Publishing Rules**, then double-click the new rule.
10. Click the **Bridging** tab.
11. Select **Require secure channel (SSL) for published site**, select **Require 128-bit encryption**, and then click **OK**.

Note: You will also need to configure appropriate rules for port 80 and port 443 on the appropriate routers and firewalls in your environment.

Note: For more information on publishing SMTP and OWA using ISA Server, see Knowledge Base articles Q290113, "How to Publish Outlook Web Access Behind ISA Server" and Q308599, "How to Configure ISA Server to Publish Exchange for OWA."

Encryption Between ISA Servers and OWA Front-End Servers

To encrypt HTTP traffic between ISA Server and an OWA front-end server, you need to install an SSL certificate on the OWA front-end servers. ISA Servers and OWA front-end servers are part of your organization's infrastructure, so the OWA front-end certificate can be issued by your organization's internal root CA or any of its trusted subordinate certificate authorities.

► To request a certificate for your OWA front-end server

Note: The following steps assume you have a CA installed in your environment.

1. Start **Internet Services Manager** on your OWA front-end server.
2. Right-click **Default Web Site**, and then click **Properties**.
3. Click the **Directory Security** tab, and then click **Server Certificate**.
4. Click **Next**, click **Create a new certificate**, and then click **Next**.
5. Click **Send the request immediately to an online certificate authority** option button, and then click **Next**.
6. In the **Name** field, type a name, and then click **Next**.
7. In the **Organization** field, type your organization name.
8. In the **Organizational unit** field, type your organization unit name, and then click **Next**.
9. In the **Common name** field, type the FQDN of your OWA front-end server, and then click **Next**.

10. Type the state and city information, and then click **Next**.
11. In the **Certification authorities** drop-down list box, verify that your certificate authority is selected, and then click **Next**.
12. Click **Next** to submit the request, and then click **Finish** to complete the wizard.
13. On the **Directory Security** tab, in the **Secure communications** group box, click **Edit**.
14. Select **Require secure channel (SSL)**, select **Require 128-bit encryption**, and then click **OK**.
15. On the **Directory Security** tab, in the **Anonymous access and authorization control** group box, click **Edit**.
16. Select **Basic authentication (password is sent in clear text)**, and then click **Yes** to acknowledge the warning.
17. Clear all other options, and then click **OK**.
18. Click **OK**.
19. Click **OK** to close the **Inheritance Overrides** dialog box, and then close **Internet Services Manager**.

Note: The common name is the FQDN of the OWA server because this matches the OWA Publishing Rule Property on the ISA Server. ISA Server checks the validity of the OWA Web certificate, along with the certificate trust chain verification and certificate expiration date, during the publishing process.

Encryption Between OWA Front-End Servers and Back-End Exchange Servers

You cannot encrypt data between OWA front-end servers and back-end servers using SSL. However, as both front-end and back-end servers are running Windows 2000, you can use IPSec for this encryption. IPSec has the benefit of being significantly faster than SSL.

Note: To improve performance and reduce the overhead of IPSec, you should consider using specialized network adapters which offload IPSec processing to the adapter.

IPSec allows you to control which protocols are accepted by the network adapter, blocking or allowing certain ports, and encrypting others. In the case of front-end/back-end server communication, you need to ensure that port 80 is encrypted.

IPSec is controlled through IPSec policies which are defined within Windows 2000 Group Policy.

Table 4.1: IPSec Policy Settings

Policy	Settings
OWA front-end	Port 80 Outbound – Encrypt Port 80 Inbound – Block
Back-end	Port 80 Inbound – Encrypt

It is possible to block inbound requests from the front-end server, because the front-end server initiates all communications with the back-end server. Blocking these requests will avoid accidental transmission of user credentials in clear text and minimize the risk of buffer overflow attacks on the front-end server.

Creating the OWA Front-End Server IPSec Policy

The first policy to create and configure is for the OWA front-end server.

► To create the outbound TCP 80 filter

1. Start **Active Directory Users and Computers**.
2. Expand **Member Servers**, expand **Application Servers**, and then expand **Exchange 2000**.
3. Right-click the **OWA Front-end Servers OU**, and then click **Properties**.
4. Click the **Group Policy** tab.
5. Select the **OWA Front End Incremental GPO**.
6. Click **Edit**.
7. Expand **Windows Settings, Security Settings**, and then right-click **IP Security Policies on Active Directory**.
8. Click **Manage IP filter lists and filter actions**.
9. Click **Add**.
10. In the **Name** box, type **Outbound TCP 80 – OWA FE**.
11. In the **Description** box, type **This filter matches outbound TCP 80 traffic on the OWA front-end server**.
12. Click **Add**, and then click **Next**.
13. In the **Source Address** drop-down list box, verify **My IP Address** is displayed, and click **Next**.
14. In the **Destination Address** drop-down list box, verify **Any IP Address** is displayed, and click **Next**.
15. In the **Select a protocol type** drop-down list box, select **TCP**, and click **Next**.
16. In the **Set the IP protocol port**, verify **From any port** is selected, select **To this port** and type **80**.
17. Click **Next**, and then click **Finish**.
18. Click **Close** to close the IP Filter List window.

► **To create the inbound TCP 80 filter**

1. Click **Add**.
2. In the **Name** box, type **Inbound TCP 80 – OWA FE**.
3. In the **Description** box, type **This filter matches inbound TCP 80 traffic on the OWA front-end server**.
4. Click **Add**, and then click **Next**.
5. In the **Source address** drop-down list box, select **Any IP Address**, and then click **Next**.
6. In the **Destination address** drop-down list box, select **My IP Address**, and then click **Next**.
7. In the **Select a protocol type** drop-down list box, select **TCP**, and click **Next**.
8. In the **Set the IP protocol port**, verify **From any port** is selected, select **To this port**, and then type **80**.
9. Click **Next**, and then click **Finish**.
10. Click **Close**.
11. Click **Close**.

► **To create the block action to be used with the inbound TCP port 80 filter**

1. From the Group Policy window, right-click **IP Security Policies on Active Directory**, and then select **Manage IP filter lists and filter actions**.
2. Click the **Manage Filter Actions** tab.
3. Click **Add**, and then click **Next**.
4. In the **Name** box, type **Block**, and then click **Next**.
5. Select **Block**, and then click **Next**.
6. Click **Finish**.

► **To create the encrypt action to be used with the outbound TCP port 80 filter**

1. Click the **Manage Filter Actions** tab.
2. Click **Add**, and then click **Next**.
3. In the **Name** box, type **Encrypt**, and then click **Next**.
4. Select **Negotiate security**, and click **Next**.
5. Select **Do not communicate with computers that do not support IPSec**, and then click **Next**.
6. Verify **High (Encapsulated Secure Payload)** is selected, and then click **Next**.
7. Click **Edit Properties**, and then click **Finish**.
8. Click **Add**.
9. Select **Custom (for expert users)**, and then click **Settings**.

10. Verify only **Data integrity and encryption (ESP)** is selected.
11. In the **Encryption algorithm**, select **3DES**.
12. Click **OK**.
13. Click **OK**.
14. Select **Custom**, and then click **Move up**.
15. Click **OK**.
16. Click **Close**.

► **To create the IP Security policy, apply the filters and specify the actions**

1. Right-click **IP Security Policies on Active Directory**, select **Create IP Security Policy**, and then click **Next**.
2. In the **Name** box, type **Block-Encrypt TCP 80 traffic – OWA FE**, and click **Next**.
3. Verify **Activate the default response rule** is selected, and click **Next**.
4. Verify **Windows 2000 default (Kerberos V5 protocol)** is selected, and click **Next**.
5. Verify **Edit properties** is selected, and click **Finish**.
6. On the **Rules** tab, click **Add**, and then click **Next**.
7. Verify **This rule does not specify a tunnel** is selected, and click **Next**.
8. Verify **All network connections** is selected, and click **Next**.
9. Verify **Windows 2000 default (Kerberos V5 protocol)** is selected, and click **Next**.
10. In the **IP filter lists** select **Inbound TCP 80 – OWA FE**, and then click **Next**.
11. In the **Filter Actions** box, click **Block**, and then click **Next**.
12. Verify **Edit properties** is cleared, and click **Finish**.
13. On the **Rules** tab, click **Add**, and then click **Next**.
14. Verify **This rule does not specify a tunnel** is selected, and click **Next**.
15. Verify **All network connections** is selected, and click **Next**.
16. Verify **Windows 2000 default (Kerberos V5 protocol)** is selected, and click **Next**.
17. In the **IP filter lists** select **Outbound TCP 80 – OWA FE**, and then click **Next**.
18. In the **Filter Actions** box, click **Encrypt**, and then click **Next**.
19. Verify **Edit properties** is cleared, and then click **Finish**.
20. Click **Close**.

► **To apply the outbound filter to Group Policy**

1. In the **Group Policy contents** pane, right-click **Block-Encrypt TCP 80 traffic – OWA FE**, and then click **Assign**.
2. Close **Group Policy**, and then click **OK**.

► **To apply Group Policy to the OWA front-end server**

1. On the OWA front-end server start a **Command Prompt**.
2. Type `secedit /refreshpolicy machine_policy /enforce`, and press ENTER.
3. Restart the server.

Creating the Back-End Server IPsec Policy

The policy on the back-end server encrypts inbound port 80 traffic.

► **To create the Inbound TCP 80 filter**

1. Start **Active Directory Users and Computers**.
2. Expand **Member Servers**, expand **Application Servers**, and then expand **Exchange 2000**.
3. Right-click the **Back-end Servers OU**, and then click **Properties**.
4. Click the **Group Policy** tab.
5. Select the **Back End Incremental GPO**.
6. Click **Edit**.
7. Expand **Windows Settings, Security Settings**, and then right-click **IP Security Policies on Active Directory**.
8. Click **Manage IP filter lists and filter actions**.
9. Click **Add**.
10. In the **Name** box, type **Inbound TCP 80 – BE**.
11. In the **Description** box, type **This filter matches inbound TCP 80 traffic on the Back-end Server**.
12. Click **Add**, and then click **Next**.
13. In the **Source Address** drop-down list box, verify **My IP Address** is displayed and click **Next**.
14. In the **Destination Address** drop-down list box, verify **Any IP Address** is displayed, and click **Next**.
15. In the **Select a protocol type** drop-down list box, select **TCP**, and click **Next**.
16. In the **Set the IP protocol port**, verify **From any port** is selected, select **To this port**, and type **80**.
17. Click **Next**, and then click **Finish**.
18. Click **Close** to close the IP Filter List window.

► **To create the IP Security policy, apply the filters and specify the actions**

1. Right-click **IP Security Policies on Active Directory**, select **Create IP Security Policy**, and then click **Next**.
2. In the **Name** box, type **Encrypt TCP 80 traffic – BE**, and click **Next**.

3. Verify **Activate the default response rule** is selected, and click **Next**.
4. Verify **Windows 2000 default (Kerberos V5 protocol)** is selected, and click **Next**.
5. Verify **Edit properties** is selected, and click **Finish**.
6. On the **Rules** tab, click **Add**, and then click **Next**.
7. Verify **This rule does not specify a tunnel** is selected, and click **Next**.
8. Verify **All network connections** is selected, and click **Next**.
9. Verify **Windows 2000 default (Kerberos V5 protocol)** is selected, and click **Next**.
10. In the **IP filter lists**, select **Inbound TCP 80 – BE**, and then click **Next**.
11. In the **Filter Actions** box, click **Encrypt**, and then click **Next**.
12. Verify **Edit properties** is cleared, and click **Finish**.
13. Click **Close**.

► **To apply the inbound filter to Group Policy**

1. In the Group Policy contents pane, right-click **Encrypt TCP 80 traffic – BE**, and then click **Assign**.
2. Close **Group Policy**, and then click **OK**.

► **To apply Group Policy to the back-end server**

1. On the OWA front-end server start a **Command Prompt**.
2. Type **secdit /refreshpolicy machine_policy /enforce**, and press ENTER.
3. Restart the server.

Note: You may wish to also apply IPSec settings at each local computer. This ensures that IPSec will still be used, even in the event of a problem accessing Group Policy from the domain controller.

Monitoring IP Security Connections

After you have configured IPSec, it is a good idea to verify its functionality by auditing IPSec-related events and by using the IP Security Monitor tool.

► **To start and configure the IP Security Monitor**

1. On either the OWA front-end or the back-end server, to start the IP Security Monitor tool, click **Start**, click **Run**, and in the **Open** box, type **ipsecmon**.
2. Click **Options** and change the **default Refresh Seconds** value from **15** to **1**.
3. Click **OK**.

► **To verify successful configuration of IPSec**

1. Generate traffic between the OWA front-end and back-end servers by having a user send e-mail using OWA.

2. Switch to IP Security Monitor, which should show the traffic between your OWA front-end server and the back-end server is encrypted.

Note: For more information on IPSec, see the “Step-by-Step Guide to Internet Protocol Security (IPSec)”, see the “More information” section for details.

Securing SMTP Communications

Every Exchange back-end server will run SMTP, as it is responsible for mail transport between Exchange servers and across the Internet. In this section we will look at how to provide SMTP communications to your network while minimizing the risk of attack to your organization.

Using ISA Server to Secure SMTP

As with your OWA front-end server, it is possible to minimize the number of ports open on your inner firewall by using the capabilities of ISA Server. In this case you can use the ISA Server Publishing feature to publish your SMTP server, positioning the Exchange server itself behind the firewall. ISA Server will impersonate the internal SMTP server without you having to place Exchange inside the perimeter network.

Note: In this configuration, external DNS entries for SMTP will need to refer to the IP address published on the ISA Server, not the address of the SMTP server.

Note: If you are not able to change your existing two firewall infrastructure to accommodate ISA Server, you can place ISA Server inside your current inner firewall and pass TCP port 25 through to the ISA Server.

Note: If you are going to implement any form of authentication over port 25, you should enable SSL authentication for SMTP.

Note: You cannot publish outgoing SMTP on an ISA Server if the server is an active member of an ISA array.

Using Content Filtering with the Message Screener

Content filtering enables the SMTP filter, which accepts incoming traffic on port 25, inspects it, and passes it on only if the rules allow it. The filter can accept or reject messages based on the username or domain name of the sender, attachments or keywords and even provide some protection against buffer overflow attacks.

However, for the SMTP filter to have full functionality, you should also install the Message Screener.

Message Screener is a separate utility supplied with ISA Server. It can be installed in a number of different configurations; however the most secure implementation of the message screener is to place it on a server running IIS with an SMTP virtual server. This virtual server would then communicate with Exchange in order to send and receive e-mail. This has the advantage of further isolating your Exchange server from the edge of the internal network.

Note: For information on deploying Message Screener, see the Knowledge Base article Q315132, "HOW TO: Configure SMTP Message Screener in ISA Server 2000." For more details, see the "More Information" section at the end of this chapter.

Additional Measures to Secure SMTP

Publishing SMTP through ISA Server and using the SMTP filter with Message Screener will help you protect your Exchange SMTP servers. However, there are some other actions you should consider.

Using a Separate SMTP Gateway

As part of your defense-in-depth strategy, you may wish to protect your Exchange back-end servers from SMTP attack by using a separate SMTP gateway inside your network. All incoming mail from the Internet would encounter this server before any of the Exchange servers. This server would not be part of any Windows 2000 domain and would therefore not be running Exchange. The advantage of this is that an external attacker trying to use SMTP to attack Exchange servers would encounter the separate SMTP server first. Taking down the SMTP server may shut down your ability to send e-mail over the Internet, but you will still be able to send internal e-mail. You could also run anti-virus software on this server.

Note: For more information on setting up and configuring an SMTP virtual server see Knowledge Base article Q308161, "HOW TO: Set Up and Configure an SMTP Virtual Server in Windows 2000."

Preventing Mail Relay

Mail relaying is the process of using an interim server to accept and then resend mail to recipients on another server. It can be used for legitimate means. For example, roaming users may wish to connect to your SMTP server in order to send mail when they are outside your network.

If you choose to allow limited relaying from outside your network, you should be very sure to regulate what is done, and ensure authentication from those users who

need to take advantage of it (authentication is enabled by default). If you open up SMTP relaying too widely, you will soon find very large amounts of mail passing through your SMTP server, which will affect the performance of your environment and add to the amount of unsolicited mail on the Internet. You may also find that you become listed on spam block-lists which may prevent your legitimate mail getting to its destination.

Even authorized mail relaying can cause problems for your mail server. Attackers use the fact that your mail server accepts authenticated requests to attempt a dictionary attack against the server.

A good approach to protecting your server is to disable relaying as much as possible. External users do not need to connect directly to your SMTP server in order to send mail, as they can use OWA.

To protect your Exchange Servers against mail relay, you consider the following measures on your internal SMTP virtual servers:

- Allowing only anonymous connection to your SMTP Servers.
- Preventing computers which successfully authenticate from relaying.
- Allowing only SMTP connections from specific IP addresses.

You will need to open up this configuration a little on SMTP Servers at the gateway. The exact settings will depend on your message flow and the configuration of your ISP's mail server. However, the best way to increase your security is to lock down your systems completely to prevent relaying and then finding the minimum settings required to allow e-mail to flow successfully.

Note: SMTP for authenticated computers is required if you are going to support IMAP and POP3. If you choose to enable these protocols, you should consider creating a separate virtual server for this traffic and using SSL to protect the virtual server.

Note: For more information on preventing unwanted SMTP relaying in Exchange, see the TechNet article, "Controlling SMTP Relaying in Microsoft Exchange" and Knowledge Base article Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000."

Summary

You cannot consider Exchange to be as secure as possible unless you take measures to secure its data flow. If you are allowing OWA over the Internet, this is particularly important, as without security in place, passwords are passed as clear text over the Internet and inside your internal network. Use the guidelines in this chapter to increase the security of your Exchange communications.

More Information

Configuring and Securing Microsoft Exchange 2000 Server and Clients:

<http://www.microsoft.com/isaserver/techinfo/deployment/ISAandExchange.asp>

Microsoft Exchange 2000 Server Hosting Series:

<http://www.microsoft.com/technet/prodtechnol/exchange/plan/hostedexch/aspintro.asp>

or

From Microsoft Press

Volume 1: Planning (ISBN: 0-7356-1829-1) and Volume 2: Deployment (ISBN: 0-7356-1830-5)

Details on signing and encrypting messages:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q286159>

For a detailed discussion of front-end/back-end server environments in Exchange:

<http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2KFfrontBack.asp>

Details on publishing SMTP and OWA using ISA Server:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q290113>

and

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q308599>

Step-by-Step Guide to Internet Protocol Security (IPSec) is available at:

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.asp>

Details on configuring the Message Screener included in Microsoft ISA Server:

<http://www.microsoft.com/serviceproviders/webhosting/HowTo/P116785.asp>

and

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315132>

Information on controlling SMTP relaying with Microsoft Exchange:

<http://www.microsoft.com/technet/security/prodtech/mailexch/excrelay.asp>

Details on setting up and configuring an SMTP virtual server:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q308161>

Details on preventing unsolicited mail using Outlook 2002:

<http://office.microsoft.com/assistance/2002/articles/OlManageJunkAndAdultMail.aspx>

Details on preventing unsolicited commercial e-mail:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319356>

Appendix A

Managing Security with Windows 2000 Group Policy

After you have determined the level of risk appropriate for your environment and established your overall security policy, it is time to start securing your environment. In a Windows 2000-based environment, this is mainly achieved through Group Policy.

In this chapter we will show how to set up Group Policy objects (GPOs) with security templates to define security settings in your Windows 2000-based environment and we will discuss a simple organizational unit (OU) structure that will support the use of these GPOs.

Warning: Before implementing the security templates discussed in this chapter in a production environment, you must first test the security templates thoroughly in a lab to ensure your servers continue to function as expected.

Importance of Using Group Policy

The goal of security policies is to define the procedures for configuring and managing security in your environment. Windows 2000 Group Policy can help you to implement technical recommendations in your security policy for all the workstations and servers in your Active Directory domains. You can use Group Policy in conjunction with your OU structure to define specific security settings for certain server roles.

If you use Group Policy to implement security settings, you can ensure that any changes made to a policy will apply to all servers using that policy and that new servers will automatically obtain the new settings.

How Group Policy is Applied

To use Group Policy safely and efficiently, it is very important to understand how it is applied. A user or computer object can be subject to multiple GPOs. These are applied sequentially, and the settings accumulate, except in the case of a conflict, where, by default, settings in later policies override those in earlier ones.

The first policy to be applied is the local GPO. Every computer running Windows 2000 has a local GPO stored on it. By default, only nodes under Security Settings are configured. Settings in other parts of the local GPO's namespace are neither enabled nor disabled. The local GPO is stored on each server in %systemroot%\System32\GroupPolicy.

After the local GPO, subsequent GPOs are applied at the site, domain, parent OU and finally child OU. The diagram shows how each policy is applied:

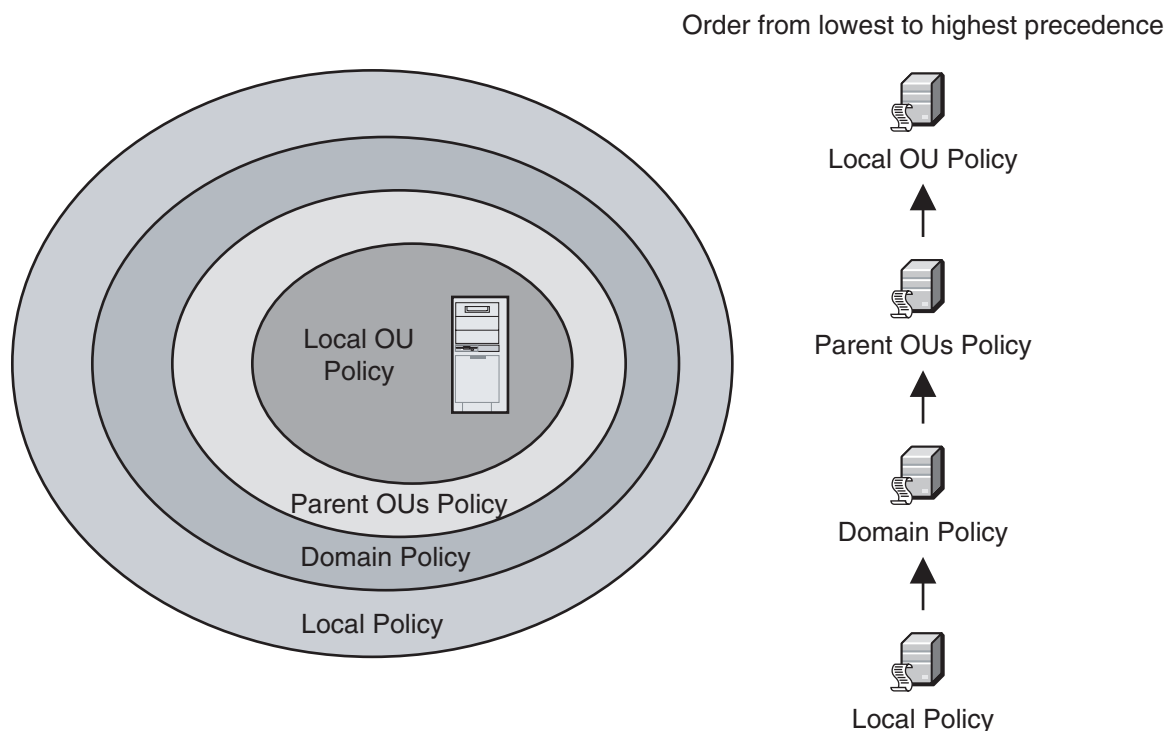


Figure A.1

GPO application hierarchy

If there are multiple GPOs defined at each level, an administrator will set the order in which they are applied.

A user or computer will apply the settings defined in a Group Policy if a) the Group Policy is applied to their container and b) they appear in the Discretionary Access Control List (DACL) for the GPO with at least **Apply Group Policy** permission.

Note: By default, the built-in group, Authenticated Users, has the **Apply Group Policy** permission. This group contains all domain users and computers

Ensuring Group Policy is Applied

Group Policy settings are located (in part) in Active Directory. This means that changes to Group Policy are not applied immediately. Domain controllers first need to replicate Group Policy changes to other domain controllers. This will take up to 15 minutes within a site and significantly longer to replicate to other sites. Once changes have been replicated, there is a further time period (five minutes for domain controllers and 90 minutes plus or minus an offset of 30 minutes for other computers) before the changes in the policy are refreshed on the destination computer.

If you wish, you can force either of these actions to occur immediately.

► To force domain controller replication

1. Open **Active Directory Sites and Services**, expand **Sites**, expand the <site name>, and then expand **Servers**.
2. Expand both <DC name 1> and <DC name 2> and then, for each server select **NTDS Settings**.
3. In the right pane, right-click the connection object name and select **Replicate Now**. This will force replication immediately between both domain controllers.
4. Repeat steps 2 and 3 for each domain controller.

► To refresh policy manually on a server

At the server command prompt, type **Secedit /refreshpolicy machine_policy /enforce**. This command tells the server to check Active Directory for any updates to the policy and, if there are any, to download them immediately.

► To verify the effective policy settings

1. Start **Local Security Policy**.
2. Under **Security Settings**, click **Local Policies**, and then click **Security Options**.
3. In the right pane, view the **Effective Settings** column to verify that the correct security settings have been applied.

Note: As you will be applying security settings using Group Policy, it is very important you have a thorough understanding of their properties and interactions. The Microsoft white paper – Windows 2000 Group Policy, provides more detailed information on how they are deployed. For more details, see the “More Information” section at the end of this chapter.

Group Policy Structure

Group Policy configuration settings are stored in two locations:

- GPOs – located in Active Directory
- Security template files – located in the local file system

Changes made to the GPO are saved directly in Active Directory, whereas changes made to the security template files must then be imported back into the GPO within Active Directory before the changes can be applied.

Note: This operations guide provides you with templates which can be used to modify your GPOs. If you make changes and modify the GPOs directly, they will be out of sync with the template files. You would therefore be advised to modify the template files and import them back into the GPO.

Windows 2000 comes with a number of security templates. The following templates can be applied in a low security environment.

- Basicwk.inf – for Windows 2000 Professional
- Basicsv.inf – for Windows 2000 Server
- Basicdc.inf – for Windows 2000-based domain controllers

To implement higher security to Windows 2000-based computers, further templates are provided. These provide additional security settings to the basic templates:

- Securedc.inf and Hisecdc.inf – for domain controllers
- Securews.inf and Hisecws.inf – for member servers and workstations

These templates are considered incremental templates because the basic templates must be applied before the incremental templates can be added. For this guide we have created new security templates, using Hisecdc.inf and Hisecws.inf as the starting points. The aim is to create a very restrictive environment, which you can then selectively open up to provide the functionality you require, while still keeping security of premium importance.

Note: The Windows 2000 default security templates are stored as .inf files in the %SystemRoot%\Security\Templates folder.

Security Template Format

Template files are text-based files. Changes to the template files can be made from the MMC snap-in Security Templates or by using a text editor such as Notepad. The following table shows how the policy sections maps to sections of the template files.

Table A.1: Security Template Sections Corresponding to Group Policy Settings

Policy Section	Template Section
Account Policy	[System Access]
Audit Policy	[System Log] [Security Log] [Application Log]
User Rights	[Privilege Rights]
Security Options	[Registry Values]
Event Log	[Event Audit]
Restricted Groups	[Group Membership]
System Services	[Service General Setting]
Registry	[Registry Keys]
File System	[File Security]

Some sections within the security template file, such as the [File Security] and [Registry Keys], contain specific access control lists (ACLs). These ACLs are text strings, defined by the Security Descriptor Definition Language (SDDL). More information on editing security templates and on SDDL can be found on MSDN. For further details, see the “More Information” section at the end of this chapter.

Test Environment

It is vital that you thoroughly assess any changes to the security of your IT systems in a test environment before you make any changes to your production environment. Your test environment should mimic your production environment as closely as possible. At the very least, it should include multiple domain controllers and each member server role you will have in the production environment.

Testing is necessary to establish that your environment is still functional after you make changes, but is also vital to ensure that you have increased the level of security as intended. You should thoroughly validate all changes and perform vulnerability assessments on the test environment.

Note: Before anyone performs vulnerability assessments in your organization, you should ensure that they have obtained written permission to do so.

Checking Your Domain Environment

Before implementing Group Policy in your production environment, it is important that the domain environment is stable and working properly. Some of the key areas in Active Directory that should be verified are DNS servers, domain controller replication, and time synchronization. You should also use a test environment to help ensure a stable production environment.

Verifying DNS Configuration

Name resolution by DNS is critical for servers and domain controllers to function properly. When multiple DNS servers are implemented for a domain, each DNS server should be tested. You should perform the following tests:

- On domain controllers:
 - Run `dcdiag /v` and `netdiag /v` using the verbose option to test DNS on each domain controller and review the output for any errors. DCDIAG and NETDIAG can be found on the Windows 2000 installation CD under the Support Tools directory.
 - Stop and start the Net Logon service and check the Event Log for any errors. The Net Logon service will dynamically register the service records in DNS for that domain controller and will produce error messages if it is not able to successfully register DNS records. These service records can be found in the file `netlogon.dns` located in the `%SystemRoot%\System32\Config` directory.
- On member servers, verify that DNS is operating correctly by using `nslookup` or running `netdiag /v`.

Domain Controller Replication

It is important that replication between multiple domain controllers is working properly before implementing Group Policy. If replication is not working correctly then changes made to Group Policy will not be applied to all domain controllers. This can create inconsistency between servers that are looking for Group Policy updates on domain controllers. Servers will be updated if they are pointing to the domain controller that the change was made on, while servers pointing to domain controllers that are still waiting for the Group Policy to be replicated will not be updated.

Forcing and Verifying Replication using Repadmin

Repadmin is a command-line tool included in the Support directory on the Windows 2000 CD. You can use repadmin to determine the directory replication partners of the destination server, and then issue a command to synchronize the source server with the destination server. This is done using the object globally unique identifier (GUID) of the source server.

► **To use repadmin to force replication between two domain controllers**

1. At a command prompt from a domain controller, type the following:

```
repadmin /showreps <destination_server_name>
```

2. Under the Inbound Neighbors section of the output, find the directory partition that needs synchronization and locate the source server with which the destination is to be synchronized. Note the object GUID value of the source server.

3. Initiate replication by entering the following command:

```
repadmin /sync
```

```
<directory_partition_DN> <destination_server_name> <source_server_objectGuid>
```

Note: Once you have the object GUID of each domain controller, you could create a batch script that uses the repadmin tool to initiate replication between servers and provide status on whether the replication is successful.

Centralize Security Templates

It is very important that the security templates used for production are stored in a secure location that can only be accessed by the administrators responsible for implementing Group Policy. By default, security templates are stored in the %SystemRoot%\security\templates folder on each domain controller. This folder is not replicated across multiple domain controllers. Therefore you will need to select a domain controller to hold the master copy of the security templates so that you do not encounter version control problems with the templates.

Time Configuration

It is very important that system time is accurate and that all servers are using the same time source. The Windows 2000 W32Time service provides time synchronization for Windows 2000-based computers running in an Active Directory domain. The W32Time service ensures that Windows 2000-based clients' clocks are synchronized with the domain controllers in a domain. This is necessary for Kerberos authentication, but the time synchronization also assists in event log analysis.

The W32Time service synchronizes clocks using the Simple Network Time Protocol (SNTP) as described in RFC 1769. In a Windows 2000 forest, time is synchronized in the following manner:

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

To ensure that the time is accurate, the PDC emulator in the forest root domain should be synchronized to an external SNTP time server. You can configure this by running the following net time command, where <server_list> is your server list:

```
net time /setsntp:<server_list>
```

Note: If your PDC emulator in the forest root is behind a firewall, you may have to open UDP port 123 on the firewall to allow the PDC Emulator to connect to an Internet-based SNTP time server.

If your network uses older Windows operating systems, on these computers, clocks can be synchronized using the following command in a logon script where <timecomputer> is a domain controller on the network:

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

Note: Computers running an operating system other than Windows should also synchronize their clocks to external time sources to allow logging events to be analyzed, based on time. For more information see the Microsoft Knowledge Base article Q216734, "How to Configure an Authoritative Time Server in Windows."

Policy Design and Implementation

If you are going to use Group Policy effectively, you must carefully determine how it will be applied. To simplify the process of applying and checking Group Policy security settings, we recommend that you apply security settings at two levels:

- **Domain Level.** To address the common security requirements, such as account policies and audit policies that must be enforced for all servers.
- **OU Level.** To address specific server security requirements that are not common to all the servers in the network. For example, the security requirements for infrastructure servers differ from those for servers running IIS.

Group Policy settings that affect security are divided into multiple sections.

Table A.2: Sections of Group Policy and Their Purpose

Policy Section	Description
Account Policy\Password Policy	Password age, length and complexity configured
Account Policy\Account Lockout Policy	Lockout duration, threshold and reset counter configured
Account Policy\Kerberos Policy	Ticket lifetimes configured
Local Policies\Audit Policy	Enable/Disable recording of specific events
Local Policies\User Rights and so on	Define rights such as log on locally, access from network
Local Policies\Security Options	Modify specific security related registry values
Event Log	Success and Failure monitoring enabled
Restricted Groups	Administrators can control who belongs to a specific group
System Services	Controls Startup Mode for each service
Registry	Configure permissions on registry keys
File System	Configure permissions on folders, subfolders and files

All computers have a predefined local policy. When an Active Directory domain is initially created, default domain and domain controller policies are also created. Before you modify any default policies, it is important to document the settings they contain, so that you can easily return to the previous state in the event of a problem.

Server Roles

For this guide, we have defined several server roles and have created security templates to increase the security for these roles.

Table A.3: Windows 2000 Server Roles

Server Role	Description	Security Templates
Windows 2000 Domain Controller	An Active Directory domain controller	BaselineDC.inf
Windows 2000 Application Server	A locked down member server on which a service, such as Exchange 2000, can be installed. To allow the service to function correctly, security will have to be loosened.	Baseline.inf
Windows 2000 File and Print Server	A locked down file and print server.	Baseline.inf and File and Print Incremental.inf
Windows 2000 Infrastructure Server	A locked down DNS, Windows Internet Name Service (WINS), and DHCP server.	Baseline.inf and Infrastructure Incremental.inf
Windows 2000 IIS Server	A locked down IIS Server.	Baseline.inf and IIS Incremental.inf

The security requirements for each of these roles are different. Appropriate security settings for each role are discussed in detail in Appendix B, “Securing Servers Based on Role.”

Note: This guide assumes that servers perform specific defined roles. If your servers do not match these roles, or you have multipurpose servers, you should use the settings defined here as a guideline for creating your own security templates. However, you should bear in mind that the more functions each of your servers perform, the more vulnerable they are to attack.

Active Directory Structure to Support the Server Roles

As already mentioned, you can apply Group Policy in many different ways, using multiple GPOs and at many different levels of hierarchy. For this guide, we have defined a number of Group Policy settings that you can use to secure the various server roles. You will need to ensure that your Active Directory structure allows you to apply these settings.

To help you secure your Windows 2000-based environment, we have predefined some security templates that can be imported into GPOs. However, if you are going to use these as is, you will need to make sure that you have the appropriate Active Directory structure. The GPOs defined in this guide are designed to be used with the OU structure shown in the diagram.

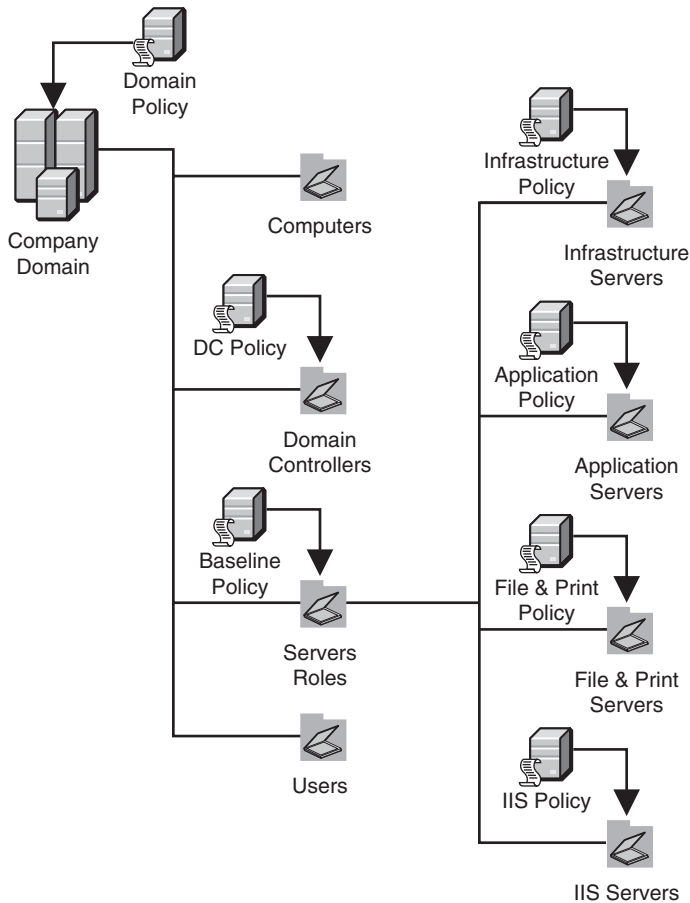


Figure A.2
OU structure for use with defined GPOs

Note: The domain structure is not important here, as domain and OU Group Policy only apply in the domain in which they were defined. The site structure is also unimportant as we do not define GPOs at the site level in this guide.

► **To create the OU structure**

1. Start **Active Directory Users and Computers**.
2. Right-click the domain name, select **New**, and then select **Organizational Unit**.
3. Type **Member Servers** and then click **OK**.
4. Right-click **Member Servers**, select **New**, and then select **Organizational Unit**.
5. Type **Application Servers** and then click **OK**.
6. Repeat steps 5 and 6 for **File & Print Servers**, **IIS Servers**, and **Infrastructure Servers**.

It is worth looking at the OU structure in some more detail.

Domain Level Policy

When a Windows 2000 domain is built, a default domain policy is created. For security settings that you want to apply to the whole domain, you can either:

- Create an additional policy and link it above the default policy
- Modify the existing default policy

Modifying the existing policy is generally simpler, however the advantage of creating an additional domain policy instead of modifying the default policy is that if there are problems with the additional policy, it can be disabled, leaving the default domain policy to resume control.

Remember that domains often contain client computers and users as well as servers. So if you are specifically looking to lock down servers, it will often be impractical to define the specific settings at the domain level. In practice, it is usually best to restrict your server security settings to those that must be set at the domain level.

In this operations guide, we do not define specific settings at the domain level, as many, such as password length, will change according to the overall security policy of your organization. We do however make some general recommendations, which can be found in Appendix B, "Securing Servers Based on Role."

Note: The password and account policy will ONLY affect domain accounts if they are set at the domain level (which means that you can only configure one password and account policy per domain). If these policies are set at the OU level or anywhere else, they will only affect local accounts. For more information, review the Knowledge Base article Q259576, "Group Policy Application Rules for Domain Controllers."

Member Servers OU

Many of the security settings you define for member servers should apply across every member server role. To simplify this process, we have created a baseline security template called `Baseline.inf` that you can import into a GPO and apply to the Member Servers OU. These settings will apply both to the Member Servers OU and any child OUs.

Domain Controllers OU

Windows 2000 already comes with a Domain Controllers OU. When a server becomes a domain controller, it is automatically placed here and you should not remove it, as it can cause user log on and access problems.

With this guide, we provide you with a security template called `BaselineDC.inf`, that you can import into a GPO and apply to the Domain Controller OU. You may choose to apply this in addition to the Default Domain Controllers GPO, or simply modify the settings in the Default Domain Controllers GPO.

Individual Server Role OUs

The individual server role OUs are child OUs to the Member Server OU. This means that by default these servers will all take on the settings defined in your Member Server Baseline Policy.

If you use the baseline policy to secure your member servers, you will need to make alterations which will apply to each individual server role. You can do this by assigning GPOs to each server role OU.

With this guide, we provide security templates that you can import into GPOs for each server role OU. Server roles are discussed in more detail in Appendix B, "Securing Servers Based on Role."

Importing the Security Templates

The following procedure imports the security templates included with this guide into the OU structure suggested in this chapter. Before implementing the following procedure on a domain controller, you must extract the contents of the `SecurityOps.exe` file included with this guide.

Warning: The security templates in this guide are designed to increase security in your environment. It is quite possible that by installing the templates included with this guide, you will lose some functionality in your environment. This could include the failure of mission critical applications. It is therefore ESSENTIAL that you thoroughly test these templates before deploying them in a production environment, and make any changes to them that are appropriate for your environment. Back up each domain controller and server prior to applying new security settings. Make sure the system state is included in the backup, because this is where the registry data is kept, and on domain controllers it also includes all of the objects in Active Directory.

Note: Before continuing, if you are using Windows 2000 Service Pack 2, you will need to apply the hot fix discussed in Knowledge Base article Q295444, "SCE Cannot Alter a Service's SACL Entry in the Registry." If this fix is not applied, the Group Policy templates will not be able to disable any services.

► **Importing the Domain Controller Baseline Policy**

1. In **Active Directory Users and Computers**, right-click **Domain Controllers**, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new Group Policy object.
3. Type **BaselineDC Policy** and press **Enter**.
4. Right click **BaselineDC Policy** and select **No Override**.

Note: This is required because the default domain controller policy configures all audit policy settings to No Auditing, with the exception of account management. Because the default domain controller policy has a higher precedence, the No Auditing setting will become the effective setting.

5. Click **Edit**.
6. Expand **Windows Settings**, right-click **Security Settings**, and select **Import Policy**.

Note: If Import Policy does not appear on the menu, close the Group Policy window and repeat steps 4 and 5.

7. In the **Import Policy From** dialog box, navigate to **C:\SecurityOps\Templates**, and double-click **BaselineDC.inf**.
8. Close **Group Policy** and then click **Close**.
9. Force replication between your domain controllers so that all domain controllers have the policy.
10. Verify in Event Log that the policy was downloaded successfully and that the server can communicate with the other domain controllers in the domain.
11. Restart each domain controller one at a time to ensure that it reboots successfully.

► **Importing the Member Server policies**

1. In **Active Directory Users and Computers**, right-click **Member Servers**, and then select **Properties**.
2. On the **Group Policy** tab, click **New** to add a new Group Policy object.
3. Type **Baseline Policy** and press **Enter**.
4. Click **Edit**.
5. Expand **Windows Settings**, right-click **Security Settings**, and select **Import Policy**.

Note: If Import Policy does not appear on the menu, close the Group Policy window and repeat steps 4 and 5.

6. In the **Import Policy From** dialog box, navigate to **C:\SecurityOps\Templates**, and double-click **Baseline.inf**.
7. Close **Group Policy** and then click **Close**.
8. Repeat steps 1 through 7 using the following OU and security template files:

OU	Security Template
File & Print Servers	File and Print Incremental.inf
IIS Servers	IIS Incremental.inf
Infrastructure Servers	Infrastructure Incremental.inf

9. Force replication between your domain controllers so that all domain controllers have the policy.
10. Move a server for each role into the appropriate OU and on the server download the policy by using the **secedit** command.
11. Verify in Event Log that the policy was downloaded successfully and that the server can communicate with the domain controllers and with other servers in the domain. After successfully testing one server in the OU, move the remaining servers in the OU and then apply security.
12. Restart each server to ensure that they reboot successfully.

Keeping Group Policy Settings Secure

If you are applying security settings using Group Policy, it is important to ensure that the settings themselves are as secure as possible. This is generally achieved by ensuring that the permissions on both the GPOs and the OUs and domains on which they are applied are set appropriately. The templates included with this guide do not modify the default Active Directory permissions, so you will need to modify these permissions manually.

Group Policy settings defined at higher level containers can potentially be overwritten by settings at lower level containers. Using the **No Override** option on the GPO prevents settings on a higher level container from being overwritten.

Note: Do not set **No Override** on the member server baseline policy. Doing so will prevent the server role policies from enabling the appropriate services and settings.

As well as separating the server roles at the OU level, you should also create separate corresponding administrator roles, assigning them administrative rights over only the corresponding OUs. This ensures that if an attacker manages to gain IIS server admin rights, they do not have access to infrastructure servers and so on.

Only domain level administrators and above should have the rights to change the membership of an OU. If an OU level administrator can remove a server from that OU, they will be able to change the security settings on those servers.

Once policy has been applied to the servers, your work has not ended. You should check your servers on a regular basis to be sure that:

- The correct policy is applied to the server
- An administrator has not changed a setting in the policy and reduced the level of security on your servers
- Any policy updates or changes have been applied to all servers

Verifying that the settings in the GPO have been applied to your servers as expected will allow you to have confidence that your servers are properly secured. There are several methods that can be used to examine the Group Policy on a server in order to verify the policy is correctly set.

Events in the Event Log

If the policy is downloaded successfully, an Event Log event with the following information appears:

Type: Information

SourceID: SceCli

Event ID: 1704

Message String: Security policy in the Group Policy objects are applied successfully

It may take a few minutes for this message to appear after applying the policy. If you do not receive the successful Event Log message, you need to run **secedit / refreshpolicy machine_policy /enforce** and then restart the server to force the policy download. Check the Event Log again after the restart to verify the successful download of the policy.

Note: If services are set to Disabled in a GPO and the server is rebooted once, the services will typically have restarted before the settings defined in the GPO take effect. If you reboot the server a second time, this will ensure that the services set to Disabled are not started.

Verifying Policy Using Local Security Policy MMC

Another method for verifying that the policy has been applied successfully is to review the effective policy setting on the local server.

► **To verify the effective policy settings**

1. Start the **Local Security Policy MMC**.
2. Under **Security Settings**, click **Local Policies**, and then click **Security Options**.

3. In the right pane, view the **Effective Setting** column.

The Effective Setting column should display the settings that are configured in the template for the role of the selected server.

Verifying Policy Using Command Line Tools

There are also two command line tools that can be used to verify policy settings.

Secedit

This tool is included in Windows 2000 and can be used to display differences between the template file and the computer's policy. To compare a template with the current policy on a computer, use the following command line:

```
secedit /analyze /db secedit.sdb /cfg <template name>
```

Note: If you apply the templates included with this guide and then run the above command, an access is denied error will be generated. This is expected due to the additional security applied. A log file will still be generated with the results of the analysis.

Gpresult

The *Windows 2000 Server Resource Kit* (Microsoft Press; ISBN: 1-57231-805-8) includes a tool called GPResult that can be used to display the policies currently applied to a server. To obtain a list of the policies applied to a server, use the following command line:

```
Gpresult /c
```

Note: Gpresult is covered in more detail in the "Troubleshooting Group Policy" section later in this chapter.

Auditing Group Policy

It is possible to audit changes to your Group Policy. Auditing policy changes can be used to keep track of who is changing, or attempting to change, policy settings. Auditing the success and failure of policy changes is enabled in the baseline security templates.

Troubleshooting Group Policy

Even though Group Policy is automatically applied, it is possible that the resulting Group Policy on a server is not as expected, mainly because Group Policy can be configured at multiple levels. This section provides some guidelines that can be used to troubleshoot Group Policy.

Note: If you are having a specific problem with Group Policy not covered in this chapter, be sure to check the Microsoft Knowledge Base. Some key Knowledge Base articles related to Group Policy are detailed in the “More Information” section at the end of this chapter as well as the “Troubleshooting Group Policy” whitepaper.

Resource Kit Tools

GPResult and GpoTool are two *Windows 2000 Server Resource Kit* tools that will help you troubleshoot Group Policy problems.

Note: These tools are also available online, see the “More Information” section at the end of this chapter for details.

GPResult

This tool provides a list of all the GPOs that have been applied to a computer, what domain controller the GPOs came from, and the date and time the GPOs were last applied.

When running GPResult on a server to ensure it has the correct GPOs, use the `/c` switch to display information on computer settings only.

When GPResult is used with the `/c` switch, it provides the following general information:

- Operating System
 - Type (Professional, Server, domain controller)
 - Build number and Service Pack details
 - Whether Terminal Services is installed and, if so, the mode it is using
- Computer Information
 - Computer name and location in Active Directory (if applicable)
 - Domain name and type (Windows NT or Windows 2000)
 - Site name

GPRresult with the /c switch also provides the following information about Group Policy:

- The last time policy was applied and the domain controller that applied policy, for the user and computer
- The complete list of applied Group Policy objects and their details, including a summary of the extensions that each Group Policy object contains
- Registry settings that were applied and their details
- Folders that are redirected and their details
- Software management information detailing assigned and published applications
- Disk quota information
- IP Security settings
- Scripts

GpoTool

This command-line tool allows you to check the health of the Group Policy objects on domain controllers including:

- **Check Group Policy object consistency.** The tool reads mandatory and optional directory services properties (version, friendly name, extension GUIDs, and Windows 2000 system volume (SYSVOL) data (Gpt.ini)), compares directory services and SYSVOL version numbers, and performs other consistency checks. Functionality version must be 2 and user/computer version must be greater than 0 if the extensions property contains any GUID.
- **Check Group Policy object replication.** It reads the GPO instances from each domain controller and compares them (selected Group Policy container properties and full recursive compare for Group Policy template).
- **Display information about a particular GPO.** Information includes properties that cannot be accessed through the Group Policy snap-in such as functionality version and extension GUIDs.
- **Browse GPOs.** A command-line option can search policies based on friendly name or GUID. A partial match is also supported for both name and GUID.
- **Preferred domain controllers.** By default, all available domain controllers in the domain will be used; this can be overwritten with the supplied list of domain controllers from the command line.
- **Provide cross-domain support.** A command-line option is available for checking policies in different domains.
- **Run in verbose mode.** If all policies are fine, the tool displays a validation message; in case of errors, information about corrupted policies is printed. A command-line option can turn on verbose information about each policy being processed.

Use the following command line to obtain details of a Group Policy as well as if any errors in the policy are detected:

```
GP0Too1 /gpo:<gpo name>
```

Group Policy Event Log Errors

Some Group Policy Event Log errors indicate specific problems with your environment. Here are two that will prevent Group Policy from being properly applied:

- On a domain controller, warning event 1202 combined with error event 1000. This generally means that a domain controller has been moved from the Domain Controllers OU to another OU which does not have the Default Domain Controllers GPO linked.
- When an administrator attempts to open one of the default GPOs, the following error is returned:

Failed to open Group Policy Object

You may not have appropriate rights.

Details: Unspecified Error

In the event log, events 1000, 1001 and 1004 appear. This is due to a corrupt registry.pol file. By deleting the registry.pol file under SYSVOL, rebooting and making a change to the server, the errors should disappear.

Summary

Windows 2000 Group Policy is a very useful way to provide consistent settings across your Windows 2000-based environment. To deploy it effectively, you should ensure that you are aware of where GPOs are applied, that all of your servers are receiving the appropriate settings, and that you have defined appropriate security on the GPOs themselves.

More Information

For more information from Symantec on corporate security policies, see:

<http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html>

Microsoft Whitepaper on Group Policy:

<http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp>

Microsoft Whitepaper on Troubleshooting Group Policy:

<http://www.microsoft.com/Windows2000/techinfo/howitworks/management/gptshoot.asp>

Knowledge Base articles on Group Policy Troubleshooting:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q250842>

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q216359>

Administrative Template File Format:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/policy/policyref_17hw.asp

Security Descriptor Definition Language:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/acctrl_757p.asp

Additional tools and Group Policy information are available in:

The Windows 2000 Server Resource Kit (Microsoft Press; ISBN: 1-57231-805-8)

or online at:

<http://www.microsoft.com/windows2000/techinfo/reskit/default.asp>

Appendix B

Securing Servers Based on Role

In the previous chapter we looked at how Group Policy can be used to define security settings on your servers. In this chapter we get into specifics, looking at baseline policies that can be defined for all member servers and domain controllers in the enterprise and then further modifications you would apply for specific server roles.

This approach allows administrators to lock down their servers using centralized baseline policies, applied consistently across all servers in the enterprise. The baseline policies allow only minimal functionality, but do allow servers to communicate with other computers in the domain and be authenticated against domain controllers. From this more secure state additional incremental policies can be applied, allowing each server to only perform the specific tasks defined by their role. Your risk management strategy will determine whether making these changes is appropriate for your environment.

This operations guide partitions policy implementation in the following way:

- **Domain Wide Policy.** Address common security requirements, such as account policies that must be enforced for all servers and workstations.
- **Domain Controller Policy.** Policies that apply to the Domain Controllers OU. Specifically, the configuration settings impact audit policy, security options, and service configuration.
- **Member Server Baseline Policy.** Common settings for all member servers including audit policies, service configuration, policies that restrict access to the registry, file system, as well as other specific security settings, such as clearing the virtual memory page file on system shut down.
- **Server Role Policy.** Four distinct server roles are defined: application servers, file and print servers, infrastructure servers, and IIS servers. Specific security needs and configurations are described for each role.

This chapter deals with these policies and other settings that should be defined for particular server roles. For more information on how Group Policy is used to apply security settings, see Appendix A, "Managing Security with Windows 2000 Group Policy."

Domain Policy

In this operations guide, we do not enforce specific settings at the domain level, as many of these settings, such as password length, will change according to the overall security policy of your organization. It is, however, very important that you define these settings appropriately.

Password Policy

By default, a standard password policy is enforced for all servers in the domain. The table lists the settings for a standard password policy, and recommended minimums for your environment.

Table B.1 Password Policy Default and Recommended Settings

Policy	Default Setting	Recommended Minimum Setting
Enforce password history	1 password remembered	24 passwords remembered
Maximum password age	42 days	42 days
Minimum password age	0 days	2 days
Minimum password length	0 characters	8 characters
Password must meet complexity requirements	Disabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled

Complexity Requirements

When the **Password must meet complexity requirements** setting of Group Policy is enabled, it requires passwords to be at least 6 characters in length (although we recommend you set this to 8 characters). It also requires that passwords contain characters from at least three of these classes:

- English upper case letters A, B, C, ... Z
- English lower case letters a, b, c, ... z
- Westernized Arabic numerals 0, 1, 2, ... 9
- Nonalphanumeric characters such as punctuation symbols

Note: A password policy should not only be enforced on servers running Windows 2000, but also on any other devices requiring a password for authentication. Network devices, such as routers and switches, are very susceptible to attack if they are using simple passwords. Attackers may try to gain control of these network devices in order to bypass firewalls.

Account Lockout Policy

An effective account lockout policy will help prevent an attacker from successfully guessing the passwords of your accounts. The table lists the settings for a default account lockout policy and recommended minimums for your environment.

Table B.2: Account Policy Default and Recommended Settings

Policy	Default Setting	Recommended Minimum Setting
Account Lockout Duration	Not Defined	30 minutes
Account Lockout Threshold	0	5 invalid logon attempts
Reset account lockout after	Not Defined	30 minutes

With the recommended minimums listed here, an account that has five invalid logon attempts within 30 minutes is locked out for 30 minutes (after which it will be reset back to 0 bad attempts and log on can be attempted again). The account can only be activated before the 30 minutes are up if an administrator resets the lockout. To increase the level of security in your organization, you should consider increasing the account lockout duration and decreasing the account lockout threshold.

Note: The password and account policy **must** be set at the domain level. If these policies are set on the OU level or anywhere else in Active Directory, they will affect local accounts and not domain accounts. It is only possible to have one domain account policy, for more information see Knowledge Base article Q255550, "Configuring Account Policies in Active Directory."

Member Server Baseline Policy

Once you have configured settings at the domain level, it is time to define common settings for all your member servers. This is done through a GPO at the Member Server OU, known as a baseline policy. A common GPO automates the process of configuring specific security settings on each server. You will also need to manually apply some additional security settings that cannot be done using group policies.

Baseline Group Policy for Member Servers

The configuration of the baseline policy used in this guide is drawn from the hisecws.inf policy included with server and workstation installs. Some of the areas that hisecws.inf addresses include:

- **Audit Policy.** Determines how auditing is performed on your servers.
- **Security Options.** Determines specific security settings using registry values.
- **Registry Access Control Lists.** Determines who can access the registry.
- **File Access Control Lists.** Determines who can access the file system.
- **Service Configuration.** Determines which services are started, stopped, disabled, and so on.

For this guide we have altered hisecws.inf to make it more secure. The Member Server Baseline Policy, baseline.inf, will help to create a server that is significantly more resistant to attack in production environments.

Hisecws.inf has been altered by adding:

- Registry values pertaining to security
- Service configuration
- Tighter file access control lists
- Enhanced auditing configuration

Member Server Baseline Auditing Policy

The settings for the application, security, and system event logs, are configured in the policy and applied to all member servers in the domain. The size for each of the logs is set at 10 megabyte (MB), and each log is configured to not overwrite events. Therefore, it is important for an administrator to regularly review and archive or clear the logs as appropriate.

Note: If a management system regularly monitors the logs for specific events, and extracts and forwards details to a management database, you will capture the necessary data and therefore can set the log files to overwrite.

The table shows the settings defined in the Member Server Baseline Auditing Policy.

Table B.3: Member Server Baseline Audit Policy Settings

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure
Restrict guest access to the application log	Enabled
Restrict guest access to the security log	Enabled
Restrict guest access to the system log	Enabled
Retention method for application log	Do not overwrite events (clear log manually)
Retention method for security log	Do not overwrite events (clear log manually)
Retention method for system log	Do not overwrite events (clear log manually)
Shut down the computer when the security audit log is full	Not Defined

Note: The retention method policy settings **Manually** is shown, which means do not overwrite events (clear log manually).

Member Server Baseline Security Options Policy

The following security options are configured in the baseline group policy.

Table B.4: Member Server Baseline Security Options Policy Settings

Option	Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Disabled
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon time expires	Not Defined (see note)
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory page file when system shuts down	Enabled
Digitally sign client communication (always)	Enabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Enabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 responses only, refuse LM & NTLM
Message text for users attempting to log on	
Message title for users attempting to log on	

Option	Setting
Number of previous logons to cache (in case domain controller is not available)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to drives and folders	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM drive access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled
Secure system partition (for RISC platforms only)	Not defined
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled (see the second note)
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (for example, Symbolic Links)	Enabled
Unsigned driver installation behavior	Do not allow installation
Unsigned non-driver installation behavior	Warn but allow installation

Note: The default domain policy configures **Automatically log off users when logon time expires** to disabled. To configure this option you must edit the default domain policy and therefore it is not defined in the baseline policies included with this guide.

Note: If you significantly increase the number of objects you audit, you run the risk of filling the security log and thus forcing a shutdown of the system. The system will then not be usable until an administrator clears the log. To prevent this, you should either disable the shutdown option listed in the table, or preferably, increase the security log size.

Some of the options set here need further discussion as they directly affect the way servers communicate with each other in the domain and can also have an impact on server performance.

Additional Restrictions for Anonymous Connections

By default, Windows 2000 allows anonymous users to perform certain activities such as enumerating the names of domain accounts and network shares. This allows an attacker to view these accounts and share names on a remote server without having to authenticate with a user account. To better secure anonymous access, **No access without explicit anonymous permissions** can be configured. The effect of this is to remove the Everyone group from the anonymous users token. Any anonymous access to a server will not be allowed, and will require explicit access to any resources.

Note: For details on the effect this may have in your environment, see Knowledge Base article Q246261, "How to Use the RestrictAnonymous Registry Value in Windows 2000."

LAN Manager Authentication Level

The Microsoft Windows 9x and Windows NT® operating systems cannot use Kerberos for authentication, and so, by default, they use the NTLM protocol for network authentication in a Windows 2000 domain. You can enforce a more secure authentication protocol for Windows 9x and Windows NT by using NTLMv2. For the logon process, NTLMv2 introduces a secure channel to protect the authentication process.

Note: If you do use NTLMv2 for legacy clients and servers, Windows 2000-based clients and servers will continue to authenticate with Windows 2000 domain controllers using Kerberos. For information on enabling NTLMv2, see Knowledge Base article Q239869, "How to Enable NTLM 2 Authentication for Windows 95/98/2000/NT." Windows NT 4.0 requires service pack 4 to support NTLMv2 and Windows 9x platforms need the directory service client installed in order to support NTLMv2.

Clear Virtual Memory Page File When System Shuts Down

Important information kept in real memory may be dumped periodically to the page file. This helps Windows 2000 handle multitasking functions. If you enable this option, Windows 2000 clears the page file when the system is shut down, removing all information stored there. Depending on the size of the page file, it could take several minutes before the system is completely shut down.

Digitally Sign Client/Server Communication

Implementing digital signing in high security networks helps to prevent impersonation of clients and servers (known as session hijacking or man in the middle attack). Server message block (SMB) signing authenticates both the user and the server hosting the data. If either side fails the authentication, data transmission will not take place. When SMB signing is implemented, there will be a performance overhead of up to 15 percent in order to sign and verify each packet between the servers. For more information on the performance overhead impact, see Knowledge Base article Q161372, "How to Enable SMB Signing in Windows NT."

Additional Security Options

For this guide, additional registry values were added to the baseline security template file that are not defined within the Administrative Template (ADM) file. This means that when you load the MMC Security Templates snap-in and view the baseline.inf template, the registry values in tables B.5–B.11 are not represented. Instead, these settings can be added to the .inf file using a text editor and will be applied to the server when the policy is downloaded.

Note: For more information on the relationship between .inf and .adm files, see Knowledge Base article Q228460, "Location of ADM (Administrative Template) Files in Windows."

These settings are embedded within the Baseline.inf security template in order to automate the changes. If the policy is removed, these settings are not automatically removed with it and must be manually changed.

Security Considerations for Network Attacks

Some denial of service attacks can pose a threat to the TCP/IP stack on Windows 2000-based servers. These registry settings help to increase the resistance of the Windows 2000 TCP/IP stack to standard types of denial of service network attacks. Information on these settings can be found in Knowledge Base article Q315669, "HOW TO: Harden the TCP/IP Stack in Windows 2000 Against Denial of Service."

The following registry keys have been added to the template file as subkeys of `HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\`:

Table B.5: TCP/IP Parameters Added to the Registry by the Member Server Baseline Policy

Key	Format	Value (Decimal)
EnableICMPRedirect	DWORD	0
EnableSecurityFilters	DWORD	1
SynAttackProtect	DWORD	2
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery	DWORD	0
KeepAliveTime	DWORD	300,000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
NoNameReleaseOnDemand	DWORD	1
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5

Windows Sockets applications such as FTP servers and Web servers have their connection attempts handled by `Afd.sys`. `Afd.sys` has been modified to support large numbers of connections in the half open state without denying access to legitimate clients. This is accomplished by allowing the administrator to configure a dynamic backlog. The new version of `Afd.sys` supports four new registry parameters that can be used to control the dynamic backlog behavior. For more details on these settings, see Knowledge Base article Q142641, "Internet Server Unavailable Because of Malicious SYN Attacks."

The following registry keys have been added to the template file as subkeys of `HKLM\System\CurrentControlSet\Services\AFD\Parameters\`:

Table B.6: Afd.sys Settings Added to the Registry by the Member Server Baseline Policy

Key	Format	Value (Decimal)
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000

Disable Auto Generation of 8.3 Filenames

Windows 2000 supports 8.3 file name formats for backward compatibility with 16-bit applications. This means that an attacker only needs 8 characters to refer to a file that may be 20 characters long. If you avoid using 16-bit applications you can turn this feature off. Disabling short name generation on an NTFS partition also increases directory enumeration performance.

The following registry key has been added to the template as a subkey of `HKLM\System\CurrentControlSet\Control\FileSystem\`:

Table B.7: Setting to Remove 8.3 Filename Creation Added to the Registry by the Member Server Baseline Policy

Key	Format	Value (Decimal)
NtfsDisable8dot3NameCreation	DWORD	1

Note: If you apply this setting to an existing server that already has files with auto generated 8.3 file names, it does not remove them. To remove existing 8.3 file names, you will need to copy those files off the server, delete the files from the original location, and then copy the files back to their original locations.

Disable Lmhash Creation

Windows 2000-based servers can authenticate computers running all previous versions of Windows. However, previous versions of Windows do not use Kerberos for authentication, so Windows 2000 supports Lan Manager (LM), Windows NT (NTLM) and NTLM version 2 (NTLMv2). The LM hash is relatively weak compared to the NTLM hash and therefore prone to rapid brute force attack. If you do not have clients that require LM authentication you should disable the storage of LM hashes. Windows 2000 Service Pack 2 provides a registry setting to disable the storage of the LM hashes.

The following registry key has been added to the template as a subkey of `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\`:

Table B.8: Setting to Disable Lmhash Creation Added to the Registry by Member Server Baseline Policy

Key	Format	Value (Decimal)
NoLMHash	DWORD	1

Note: To disable the storage of LM hashes with this registry setting you must be running Windows 2000 Service Pack 2 or later.

For more information, see the Microsoft Knowledge Base article Q147706, "How to Disable LM Authentication on Windows NT."

Configuring NTLMSSP Security

The NTLM Security Support Provider (NTLMSSP) allows you to specify the minimum required security setting for server side network connections by applications.

The Member Server Baseline Policy ensures that the connection will fail if message confidentiality is in use but 128-bit encryption is not negotiated.

The following registry key has been added to the template as a subkey of **HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**:

Table B.9: Setting to Configure NTLMSSP Security added to the registry by the Member Server Baseline Policy

Key	Format	Value (Hex)
NtlmMinServerSec	DWORD	0x20000000

Disabling Autorun

Autorun begins reading from a drive as soon as media is inserted in it. As a result, the setup file of programs and the sound on audio media starts immediately. To prevent a possible malicious program from starting when media is inserted the Group Policy disables Autorun on all drives.

The following registry key has been added to the template as a subkey of **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer**:

Table B.10: Setting to Disable Autorun on all Drives, Added to the Registry by the Member Server Baseline Policy

Key	Format	Value (Hex)
NoDriveTypeAutoRun	DWORD	0xFF

Member Server Baseline Registry Access Control Lists Policy

The Member Server Baseline Policy does not change the registry ACLs defined in hisecws.inf. You should perform careful testing in your environment before you make any changes.

The ACLs defined in hisecws.inf mainly change the Power Users group, which is created by default for backward compatibility with Windows NT 4.0–based environments. The template ensures that Power Users has the same permissions as the Users group on Windows 2000.

Note: The Power Users group is not defined on domain controllers.

Member Server Baseline File Access Control Lists Policy

To further secure the file system, you should ensure that more restrictive permissions are applied to directories and files common to all member servers in the domain. The Member Server Baseline Security Template incorporates all the file access control lists provided with the hisecws.inf template and adds settings for a number of folders and files.

Note: For details on the default registry and file permissions in Windows 2000, see the “Default Access Control Settings in Windows 2000” white paper available on TechNet. The “More Information” section at the end of this chapter has the link to the white paper.

The table shows the additional folders secured by the Member Server Baseline Policy in addition to those defined by the settings in hisecws.inf.

Table B.11: Settings to Secure Key Directories Defined in the Member Server Baseline Policy

Folders Secured	Permissions Applied
%systemdrive%\	Administrators: Full control System: Full control Authenticated Users: Read and Execute, List Folder Contents, and Read
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	Administrators: Full control Creator/Owner: Full control System: Full control
%systemdrive%\Inetpub	Administrators: Full control System: Full control Everyone: Read and Execute, List Folder Contents, and Read

Note: %SystemRoot% defines the path and folder name where the Windows system files are located and %SystemDrive% defines the drive containing %systemroot%.

There are also a large number of files installed on the server that should be locked down further. The Member Server Baseline Policy will alter the ACLs on the default Windows startup files and also on many of the executables that can be run from the command prompt. The files affected are listed in Appendix C.

Member Server Baseline Services Policy

When Windows 2000 Server is first installed, default services are created and are configured to run when the system starts. Some of these services do not need to run in many environments, and as any service is a potential point of attack, you should disable unnecessary services.

The Member Server Baseline Policy only enables the services required for a Windows 2000 member server to participate in a Windows 2000 domain and provide basic management services.

Table B.12: Services Enabled by the Member Server Baseline Policy

Service	Startup Type	Reason for inclusion in Member Server Baseline
COM+ Event Services	Manual	Allows management of Component Services
DHCP Client	Automatic	Required to update records in Dynamic DNS
Distributed Link Tracking Client	Automatic	Used to maintain links on NTFS volumes
DNS Client	Automatic	Allows resolution of DNS names
Event Log	Automatic	Allows event log messages to be viewed in Event log
Logical Disk Manager to date	Automatic	Required to ensure dynamic disk information is up to date
Logical Disk Manager Administrative Service	Manual	Required to perform disk administration
Netlogon	Automatic	Required for domain participation
Network Connections	Manual	Required for network communication
Performance Logs and Alerts	Manual	Collects performance data for the computer, writes it to log or triggers alerts
Plug and Play	Automatic	Required for Windows 2000 to identify and use system hardware
Protected Storage	Automatic	Required to protect sensitive data such as private keys
Remote Procedure Call (RPC)	Automatic	Required for internal processes in Windows 2000
Remote Registry Service	Automatic	Required for hfnetchk utility (see Note)
Security Accounts Manager	Automatic	Stores account information for local security accounts
Server	Automatic	Required for hfnetchk utility (see Note)
System Event Notification	Automatic	Required to record entries in the event logs

Service	Startup Type	Reason for inclusion in Member Server Baseline
TCP/IP NetBIOS Helper Service	Automatic	Required for software distribution in Group Policy (may be used to distribute patches)
Windows Management Instrumentation Driver	Manual	Required to implement performance alerts, using Performance Logs and Alerts
Windows Time	Automatic	Required for Kerberos authentication to consistently function
Workstation	Automatic	Required to participate in a domain

Note: Hfnetchk is a tool which allows you to verify which patches are installed on each of the servers in your organization.

These settings assume a pure and standard Windows 2000-based environment (with the exception of the hfnetchk tool). If your environment involves Windows NT 4.0 (or you have other tools on all your member servers) you may require other services for compatibility purposes. If you do enable other services, these may in turn have dependencies that require further services. Services needed for a specific server role can be added in the policy for that server role.

Appendix D shows all the services present in a default installation of Windows 2000 and Appendix E shows the additional services that may be added to a default installation.

Key Services Not Included in the Member Server Baseline

The goal of the Member Server Baseline Policy is to be as restrictive as possible. For this reason several services are disabled that may be required in your environment. Some of the more common ones are listed here.

SNMP Service

In many cases, management applications require an agent to be installed on each server. Typically, these agents will use SNMP to forward alerts back to a centralized management server. If management agents are required then you should check to see if they need the SNMP service started.

WMI Services

The Windows Management Instrumentation (WMI) service is disabled in the Member Server Baseline Policy. To manage logical disks using computer management, you need to enable the WMI service. Many other applications and tools also use WMI.

Messenger Service and Alert Service

Although not explicitly dependent on one another, these services work together to send administrative alerts. The Messenger service will send alerts triggered by the Alert service. If you are using Performance Logs and Alerts to trigger alerts, you will need to enable these services.

Domain Controller Baseline Policy

All domain controllers created in the domain are automatically assigned to the Domain Controllers OU. Domain controllers should never be moved out of the Domain Controllers OU as there are specific security ACLs applied to this OU.

The Domain Controllers OU is a top level OU and so will not take on the settings defined in your Member Server Baseline Policy. For this reason, we have created a separate Domain Controller Baseline Policy.

Configuration settings implemented in the Domain Controller Baseline Policy affects the following sections of the policy:

- Audit Policy
- Security Options
- Service Configuration

Note: File ACLs, with the exception of the System32 files listed in Appendix C, and registry ACLs are not included in this Group Policy, as they are defined and implemented when the server running Windows 2000 is promoted to a domain controller. A security template called Defltdc.inf is applied during the promotion of a Windows 2000-based server to a domain controller. This template applies ACLs to the file system and registry keys for the additional services created to support a domain controller.

Domain Controller Baseline Audit and Security Options Policy

The audit policy and security options configured for the domain controllers are identical to the baseline policy (see the “Member Server Baseline Policy” section for details on these settings.)

Domain Controller Baseline Services Policy

The services configured for startup are those defined in the member server baseline configuration, plus additional services needed to support the domain controller functions.

Table B.13: Services Enabled by the Domain Controller Baseline Services Policy, in Addition to Those Set by the Member Server Baseline Policy

Service	Startup Type	Reason for inclusion in Domain Controller Baseline
Distributed File System	Automatic	Required for Active Directory Sysvol share
DNS Server	Automatic	Required for Active Directory integrated DNS
File Replication	Automatic	Needed for file replication between domain controllers
Kerberos Key Distribution Center	Automatic	Allows users to log onto the network using Kerberos v5
NT LM Security Support Provider	Automatic	Allows clients to log on using NTLM authentication
RPC Locator	Automatic	Allows the domain controller to provide RPC name service

Key Services Not Included in the Domain Controller Baseline Policy

The goal of the Domain Controller Baseline Policy is to be as restrictive as possible. For this reason several services are disabled that may be required in your environment. Some of the more common ones you may require are listed here.

Simple Mail Transport Protocol (SMTP)

Intersite replication can occur using either RPC or SMTP. If you use SMTP for replication in your environment, you will need to enable the SMTP Service.

Intersite Messaging

This service is used for mail-based replication between sites. Each transport to be used for replication is defined in a separate add-in dynamic link library (DLL). These add-in DLLs are loaded into Intersite Messaging. Intersite Messaging directs send requests and receive requests to the appropriate transport add-in DLLs, which then route the messages to Intersite Messaging on the destination computer. If you use SMTP for replication in your environment, you will need to enable this service.

IIS Admin Service

If the SMTP service is started then the IIS Admin service also needs to be started as the SMTP service is dependent on the IIS Admin service.

Distributed Link Tracking Server Service

This service is used to track files on NTFS volumes throughout a domain and is contacted by computers running the Distributed Link Tracking Client service. These computers will periodically continue to attempt to contact the Distributed Link Tracking Server service even after it is disabled.

Note: If you run the dcdiag utility from the Windows 2000 Support Tools, it will check for all services which normally run on domain controllers to be started. As some services are disabled in the Domain Controller Baseline Policy, dcdiag will report errors. This is to be expected and does not indicate a problem with your configuration.

Other Baseline Security Tasks

It is not possible to perform all the tasks required to increase the security of your member servers and domain controllers using Group Policy. There are a number of additional steps you should take to increase the overall level of security on all of your servers.

Securing Built-in Accounts

Windows 2000 has a number of built-in user accounts, which cannot be deleted, but can be renamed. Two of the most commonly known built-in accounts on Windows 2000 are Guest and Administrator. By default, the Guest account is disabled on member servers and domain controllers. You should not change this setting. The built-in Administrator account should be renamed and the description altered to prevent attackers from compromising a remote server using a well known name. Many malicious scripts use the built-in administrator account as a first attempt for compromising the server.

Note: The built-in administrator account can be renamed using Group Policy. We have not implemented this setting in the baseline policies because you should choose a name which is not well known.

Securing Local Administrator Account

Every member server has a local accounts database and a local administrator account that provides full control over the server. This account is therefore very important. You should rename this account, and ensure that it has a complex password. You should also ensure that local administrator passwords are not replicated across member servers. If they are, an attacker who gains access to one member server will be able to gain access to all others with the same password.

You should not make local administrator accounts part of the Domain Admins group as this extends their capabilities beyond what is necessary to administer member servers. For the same reason, it is important to ensure that only local accounts are used to administer your member servers.

Securing Service Accounts

Windows 2000 services typically run under the Local System account, but they can also be run under a domain user or local account. You should use local accounts whenever possible over domain user accounts. A service runs under the security context of its service account, so if an attacker compromises a service on a member server, the service account can potentially be used to attack a domain controller. When determining which account to use as a service account, you should make sure that the assigned privileges are limited to what is required for the successful operation of the service. The table below explains the privileges inherent to each type of service account.

Table B.14: Privileges of Windows 2000 Accounts in Different Environments

Authentication when running service on Windows 2000-based computers	Intraforest only, all Windows 2000-based servers	Multiforest application with NTLM trusts between domains
Local user service account	No network resources, local access only under account's assigned privileges	No network resources, local access only under account's assigned privileges
Domain user service account	Network access as domain user, local access under user's privileges	Network access as domain user, local access under user's privileges
LocalSystem	Network access as machine account authenticated user, local access under LocalSystem	No network resources spanning forests, local access under LocalSystem

All Windows 2000 default services run under **LocalSystem** and you should not change this. Any additional services added to the system requiring the use of domain accounts should be evaluated carefully before they are deployed.

Validating the Baseline Configuration

After security has been applied for the first time to a server, it is good practice to validate that the specific security settings have been configured correctly. The Microsoft Security Baseline Analyzer Tool will perform a series of tests against your servers, and warn you of any security problems you may encounter.

Validate Port Configuration

It is important to validate the final port configuration and to understand which TCP and UDP ports your servers running Windows 2000 are listening on. After applying the baseline policies, the netstat command can be run to show what ports the server

is still listening on for each network interface card. The table shows the expected output netstat for a member server with the Member Server Baseline Policy applied:

Table B.15: Ports a Member Server Will Listen on After the Member Server Baseline Policy is Applied

Protocol	Local Address	Foreign Address	Status
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	<IP Address>:139	0.0.0.0:0	LISTENING
UDP	<IP Address>:137	*.*	N/A
UDP	<IP Address>:138	*.*	N/A
UDP	0.0.0.0:445	*.*	N/A
UDP	0.0.0.0:1027	*.*	N/A
UDP	0.0.0.0:1045	*.*	N/A

Securing Each Server Role

Once you have applied your baseline policies, your servers will be significantly more secure. From this state, you may need to enable additional settings, adding functionality to your baseline. For this guide we have defined four distinct member server roles:

- **Windows 2000 Application Server.** The most secure and locked down of the server roles. The goal of the secure application server role is to provide a very locked down server on which you can install an application, such as Exchange or SQL. This server role is designed so that all it can do is communicate with domain controllers for authentication purposes. This role is the basis for the other roles.
- **Windows 2000 File and Print Server.** Designed to greatly increase the security of servers acting as file and print servers.
- **Windows 2000 Infrastructure Server.** Designed to greatly increase the security of servers acting as DNS, DHCP, and WINS servers.
- **Windows 2000 IIS Server.** Designed to greatly increase the security of servers acting as IIS servers. This role uses a modified version of the application server policy as well as using the IIS Lockdown and URLScan tools.

Note: The application server role is deliberately very restricted. In order to install and run certain applications you may well have to alter the security settings from what is defined here.

Note: It is possible to modify the templates included with this guide to build templates for other roles. If this is done, it is important to fully test the modified template to ensure it provides the level of security desired.

Windows 2000 Application Server Role

Settings for the Application Server role will depend on the particular application you are deploying. For this reason, the settings are unchanged from the member server baseline. Therefore the application server role is very restricted—to install and run certain applications you will need to alter the security settings from the defaults defined here. The easiest way to accomplish this, is to create a new OU for the application under the Application Servers OU. Then create a Group Policy that modifies the baseline settings and import the policy into the new OU.

Windows 2000 File and Print Server Role

File and print services are generally accessed and used by all users in a corporate environment, so ensuring that this server role is as secure as possible can be very challenging. The File and Print Server Policy:

- Enables the Spooler service, which is used for printing.
- Disables the security policy setting: **Digitally sign client communication (always)**. If this is not disabled, clients will be able to print, but not able to view the print queue. When attempting to view the print queue they will receive the message: “Unable to connect. Access denied.”

Note: The Spooler service is used on any computer that initiates a print job, as well as print servers. The default settings for the member server and domain controller baselines mean that you will not be able to issue print jobs from these computers.

Windows 2000 Infrastructure Server Role

The Infrastructure Server role supports DNS, DHCP and WINS network services. For all three services to execute on one member server, the infrastructure policy enables the following services in addition to the Member Server Baseline Policy.

Table B.16: Services Added by the Infrastructure Server Role Policy

Service	Startup Type	Reason for inclusion in Infrastructure Server Role Policy
DHCPServer	Automatic	To provide DHCP services to clients
DNS	Automatic	To provide DNS services to clients
NTLMSSP	Automatic	To provide security to RPC programs that use transports other than named pipes
WINS	Automatic	To provide WINS services clients

Windows 2000 IIS Server Role

The IIS server role provides Web server functionality to a Windows 2000-based server. The IIS server role Group Policy adds following services to the Member Server Baseline Policy.

Table B.17: Services added by the IIS Server Role Policy

Service	Startup Type	Reason for inclusion in IIS Server Role Policy
IISAdmin	Automatic	Administration of the Web Server
W3SVC	Automatic	Provides Web Server Functionality

In addition, the IIS server role Group Policy configures the **SynAttackProtect** registry value to 1.

The IISLockdown tool

IIS servers provide a great deal of functionality. However, to make your IIS servers as secure as possible, you should restrict this functionality to only that which is required. The easiest way to do this is with the IISLockdown tool. IISLockdown is a highly configurable utility that allows you to specify the nature of your Web server. It will then remove any functionality that is not required for the particular Web server. You should, of course, test thoroughly any changes before implementing them in a production environment.

Note: IISLockdown is available as part of the Security Toolkit and on the Microsoft Security Website. Further details can be found in the “More Information” section at the end of this chapter.

IISLockdown can perform many steps to help secure web servers. These can include:

- Locking files
- Disabling services and components
- Installing URL Scan
- Removing unneeded Internet Server Application Programming Interface (ISAPI) DLL script mappings
- Removing unneeded directories
- Changing ACLs

You can use IIS Lockdown to secure many types of IIS server role. For each server, you should pick the most restrictive role that meets the needs of your Web server.

► **To secure a Static Web Server with IIS Lockdown**

1. Start **IISLockd.exe**.
2. Click **Next**.
3. Select **I agree**, and then click **Next**.
4. Select **Static Web server**, and then click **Next**.
5. Ensure **Install URLScan filter on the server** is selected and then **Next**.
6. Click **Next**.
7. If the **Digital Signature Not Found** dialog box appears, click **Yes**.
8. Click **Next**.
9. Click **Finish**.

If you set up IIS Server as a Static Web Server, the following changes are made:

- The Index Server Web Interface (.idq, .htw, .ida) script map is disabled
- The Internet Data Connector (.idc) script map is disabled
- The Server side includes (.shtml, .shtm, .stm) script map is disabled
- The .HTR scripting (.htr) script map is disabled
- The Active Server Pages (.asp) script map is disabled
- The Internet printing (.printer) script map is disabled
- The printer virtual directory is removed
- Web Distributed Authoring and Versioning (WebDAV) is disabled
- File permissions are set to prevent anonymous IIS users from writing to content directories
- File permissions are set to prevent anonymous IIS users from running system utilities
- The URLScan filter is installed on the server
- The Scripts virtual directory is removed
- The MSADC virtual directory is removed
- The IIS Samples virtual directory is removed
- The IISAdmin virtual directory is removed
- The IISHelp virtual directory is removed

Other IIS Server Role Security Settings

The IIS Lockdown tool significantly increases the security of your IIS servers. However, there are further steps you can take to further secure your servers running Windows 2000 IIS service.

Setting IP Address/DNS Address Restrictions

This setting ensures that only systems with particular IP addresses or DNS names can access the web server. Setting IP address and DNS address restrictions is not typically done, but it is one option available to restrict Web sites to certain users. However, if DNS names are used instead of IP addresses in the restrictions, IIS has to do a DNS lookup, which can be time consuming.

Disabling the Default IIS Anonymous Account

On Member Servers running IIS, the default anonymous account used to access IIS is a local account, named **IUSR_computername**. For additional security, you should consider disabling the default account and replacing it with another local account, adhering to strong password guidelines. This will make it more difficult for an attacker to guess the name of the account.

Note: You can delete the **IUSR_computername** account, however disabling the account instead leaves it as a decoy account.

Implementing IPSec Filters for Multihomed Web Servers

The IPSec policy engine that comes with Windows 2000 is a useful tool to increasing the overall security of your Web architecture, particularly the security of your Web servers. The IPSec policy is usually used to create a secure communication path between two host sites or two remote sites. However, it can also be used for its protocol/port filtering capabilities.

You can use filter lists in conjunction with filter actions to control the traffic to and from your Web server. For example, you could create two filter lists, one for traffic from all destinations coming to Port 80, another for traffic from all destinations to all ports. You would then define filter actions to allow the traffic matching the first filter list through and to block traffic matching the second filter list.

IPSec policies are implemented using Group Policy. We have not incorporated them in the policies included in this guide, as they will be implemented differently according to the specifics of your environment.

Changes to the Recommended Environment

The goal of the recommendations listed in this chapter is to create a significantly more secure environment for Windows 2000-based servers. However, some of the changes may not be appropriate for your organization. Here we look at two cases where 1) more administrative capability is required, and 2) where the Hfnetchk utility will not be used.

Administration Changes

The default baseline policies for member servers and domain controllers will eliminate some of the remote (and some of the local) administrative functionality from your environment. Remote management using the Microsoft Management Console (MMC) computer management snap-in will not work with the default baseline policies because some MMC related services are disabled.

The baseline policies enable the Server service and Remote Registry service. This will allow the computer management snap-in to remotely connect to other computers and administer these elements:

- Shared Folders
- Local users and groups
- Under Storage Management, everything except Logical Drives and Removable Storage
- Services Device Manager
- Event Viewer
- Performance Logs and Alerts

WMI is not enabled in the baseline policies. This prevents these elements from being administered:

- WMI
- Under Storage Management, Logical Drives

If you need to administer these, locally or remotely, you should enable the WMI service.

Removable Storage cannot be accessed remotely with just the Member Server Baseline Policy services started. If the Removable Storage service is not started on the remote server then the remote server will produce a DCOM error message in the event log stating that the service is not available.

Note: When enabling the above services to allow administration, enable the services only in the incremental server role policies that require the services.

Note: Some administration tools may require you to make security modifications on the client from which you are running the tool. For example, some tools may use NTLM authentication and the baseline policy configures the servers to only accept NTLM v2. See the “LAN Manager Authentication Level” section in this chapter for more information on configuring this.

Security Modifications if HFNETCHK is Not Implemented

Hfnetchk is a tool which allows you to verify which patches are installed on each of the servers in your organization. We highly recommend that you use a tool such as Hfnetchk as it will help you increase the overall level of security in your environment.

However, if you do not implement Hfnetchk, you can disable the Remote Registry service and Server service in the Member Server Baseline Policy. In the Domain Controller Baseline policy you can disable the Remote Registry service.

If you do disable these services in the Member Server Baseline Policy, you will need to enable them in some of the server roles:

Table B.18: Services that Must be Added to Server Role GPOs if Remote Registry and Server Services are Disabled in the Member Server Baseline Policy

Server Role	Service to be Enabled	Reason
File and Print Server	Server	To provide File sharing capabilities
Infrastructure Server	Server	To allow WINS to function properly
Infrastructure Server	Remote Registry	To allow the WINS Manager to view the state of the WINS Server

If you do disable the Server and Remote Registry services, you will also lose almost all of your remote administration capabilities.

Summary

Windows 2000-based servers provide a great deal of functionality out of the box. However, much of this functionality is not required for all servers. By defining the tasks that your servers perform, you can disable those elements you do not require, and therefore increase the security in your environment. If you implement the steps suggested in this chapter, you will go a long way toward making your environment significantly more secure.

More Information

For more information from Symantec on the fundamentals of security, see:

<http://securityresponse.symantec.com/avcenter/security/Content/security.articles/fundamentals.of.info.security.html>

Information on securing the Windows 2000 TCP/IP Stack:

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/website/dosrv.asp>

Default Access Control Settings in Windows 2000 white paper:

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/featusability/secdefs.asp>

Microsoft Security Toolkit:

<http://www.microsoft.com/security/mstpp.asp>

Glossary of Windows 2000 Services:

<http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp>

Appendix C

Additional Files Secured

Files secured by the Member Server Baseline Policy, in addition to the access control lists provided with the hisecws.inf template.

File	Baseline Permissions
%SystemDrive%\Boot.ini	Administrators: Full control System: Full control
%SystemDrive%\Ntdetect.com	Administrators: Full control System: Full control
%SystemDrive%\Ntldr	Administrators: Full control System: Full control
%SystemDrive%\Io.sys	Administrators: Full control System: Full control
%SystemDrive%\Autoexec.bat	Administrators: Full control System: Full control Authenticated Users: Read and Execute, List Folder Contents, and Read
%SystemDrive%\Config.sys	Administrators: Full control System: Full control Authenticated Users: Read and Execute, List Folder Contents, and Read
%SystemRoot%\system32\Append.exe	Administrators: Full control
%SystemRoot%\system32\Arp.exe	Administrators: Full control
%SystemRoot%\system32\At.exe	Administrators: Full control
%SystemRoot%\system32\Attrib.exe	Administrators: Full control
%SystemRoot%\system32\Caccls.exe	Administrators: Full control
%SystemRoot%\system32\Change.exe	Administrators: Full control
%SystemRoot%\system32\Chcp.com	Administrators: Full control

(continued)

File	Baseline Permissions
%SystemRoot%\system32\Chglogon.exe	Administrators: Full control
%SystemRoot%\system32\Chgport.exe	Administrators: Full control
%SystemRoot%\system32\Chguser.exe	Administrators: Full control
%SystemRoot%\system32\Chkdsk.exe	Administrators: Full control
%SystemRoot%\system32\Chkntfs.exe	Administrators: Full control
%SystemRoot%\system32\Cipher.exe	Administrators: Full control
%SystemRoot%\system32\Cluster.exe	Administrators: Full control
%SystemRoot%\system32\Cmd.exe	Administrators: Full control
%SystemRoot%\system32\Compact.exe	Administrators: Full control
%SystemRoot%\system32\Command.com	Administrators: Full control
%SystemRoot%\system32\Convert.exe	Administrators: Full control
%SystemRoot%\system32\Cscript.exe	Administrators: Full control
%SystemRoot%\system32\Debug.exe	Administrators: Full control
%SystemRoot%\system32\Dfscmd.exe	Administrators: Full control
%SystemRoot%\system32\Diskcomp.com	Administrators: Full control
%SystemRoot%\system32\Diskcopy.com	Administrators: Full control
%SystemRoot%\system32\Doskey.exe	Administrators: Full control
%SystemRoot%\system32\Edlin.exe	Administrators: Full control
%SystemRoot%\system32\Exe2bin.exe	Administrators: Full control
%SystemRoot%\system32\Expand.exe	Administrators: Full control
%SystemRoot%\system32\Fc.exe	Administrators: Full control
%SystemRoot%\system32\Find.exe	Administrators: Full control
%SystemRoot%\system32\Findstr.exe	Administrators: Full control
%SystemRoot%\system32\Finger.exe	Administrators: Full control
%SystemRoot%\system32\Forcedos.exe	Administrators: Full control
%SystemRoot%\system32\Format.com	Administrators: Full control
%SystemRoot%\system32\Ftp.exe	Administrators: Full control
%SystemRoot%\system32\Hostname.exe	Administrators: Full control
%SystemRoot%\system32\lisreset.exe	Administrators: Full control
%SystemRoot%\system32\Ipconfig.exe	Administrators: Full control
%SystemRoot%\system32\Ipxroute.exe	Administrators: Full control
%SystemRoot%\system32\Label.exe	Administrators: Full control

File	Baseline Permissions
%SystemRoot%\system32\Logoff.exe	Administrators: Full control
%SystemRoot%\system32\Lpq.exe	Administrators: Full control
%SystemRoot%\system32\Lpr.exe	Administrators: Full control
%SystemRoot%\system32\Makecab.exe	Administrators: Full control
%SystemRoot%\system32\Mem.exe	Administrators: Full control
%SystemRoot%\system32\Mmc.exe	Administrators: Full control
%SystemRoot%\system32\Mode.com	Administrators: Full control
%SystemRoot%\system32\More.com	Administrators: Full control
%SystemRoot%\system32\Mountvol.exe	Administrators: Full control
%SystemRoot%\system32\Msg.exe	Administrators: Full control
%SystemRoot%\system32\Nbtstat.exe	Administrators: Full control
%SystemRoot%\system32\Net.exe	Administrators: Full control
%SystemRoot%\system32\Net1.exe	Administrators: Full control
%SystemRoot%\system32\Netsh.exe	Administrators: Full control
%SystemRoot%\system32\Netstat.exe	Administrators: Full control
%SystemRoot%\system32\Nslookup.exe	Administrators: Full control
%SystemRoot%\system32\Ntbackup.exe	Administrators: Full control
%SystemRoot%\system32\Ntsd.exe	Administrators: Full control
%SystemRoot%\system32\Pathping.exe	Administrators: Full control
%SystemRoot%\system32\Ping.exe	Administrators: Full control
%SystemRoot%\system32\Print.exe	Administrators: Full control
%SystemRoot%\system32\Query.exe	Administrators: Full control
%SystemRoot%\system32\Rasdial.exe	Administrators: Full control
%SystemRoot%\system32\Rcp.exe	Administrators: Full control
%SystemRoot%\system32\Recover.exe	Administrators: Full control
%SystemRoot%\system32\Regedit.exe	Administrators: Full control
%SystemRoot%\system32\Regedt32.exe	Administrators: Full control
%SystemRoot%\system32\Regini.exe	Administrators: Full control
%SystemRoot%\system32\Register.exe	Administrators: Full control
%SystemRoot%\system32\Regsvr32.exe	Administrators: Full control
%SystemRoot%\system32\Replace.exe	Administrators: Full control

(continued)

File	Baseline Permissions
%SystemRoot%\system32\Reset.exe	Administrators: Full control
%SystemRoot%\system32\Rexec.exe	Administrators: Full control
%SystemRoot%\system32\Route.exe	Administrators: Full control
%SystemRoot%\system32\Routemon.exe	Administrators: Full control
%SystemRoot%\system32 Router.exe	Administrators: Full control
%SystemRoot%\system32\Rsh.exe	Administrators: Full control
%SystemRoot%\system32\Runas.exe	Administrators: Full control
%SystemRoot%\system32\Runonce.exe	Administrators: Full control
%SystemRoot%\system32\Secedit.exe	Administrators: Full control
%SystemRoot%\system32\Setpwd.exe	Administrators: Full control
%SystemRoot%\system32\Shadow.exe	Administrators: Full control
%SystemRoot%\system32\Share.exe	Administrators: Full control
%SystemRoot%\system32\Snmp.exe	Administrators: Full control
%SystemRoot%\system32\Snmptrap.exe	Administrators: Full control
%SystemRoot%\system32\Subst.exe	Administrators: Full control
%SystemRoot%\system32\Telnet.exe	Administrators: Full control
%SystemRoot%\system32\Termsrv.exe	Administrators: Full control
%SystemRoot%\system32\Tftp.exe	Administrators: Full control
%SystemRoot%\system32\Tintadmin.exe	Administrators: Full control
%SystemRoot%\system32\Tintsess.exe	Administrators: Full control
%SystemRoot%\system32\Tintsvr.exe	Administrators: Full control
%SystemRoot%\system32\Tracert.exe	Administrators: Full control
%SystemRoot%\system32\Tree.com	Administrators: Full control
%SystemRoot%\system32\Tsadmin.exe	Administrators: Full control
%SystemRoot%\system32\Tscon.exe	Administrators: Full control
%SystemRoot%\system32\Tsdiscn.exe	Administrators: Full control
%SystemRoot%\system32\Tskill.exe	Administrators: Full control
%SystemRoot%\system32\Tsprof.exe	Administrators: Full control
%SystemRoot%\system32\Tsshutdn.exe	Administrators: Full control
%SystemRoot%\system32\Usrmgr.com	Administrators: Full control
%SystemRoot%\system32\Wscript.exe	Administrators: Full control
%SystemRoot%\system32\Xcopy.exe	Administrators: Full control

Appendix D

Default Windows 2000 Services

The Default column shows the service startup for a Windows 2000-based server. The Baseline column shows the configure startup for each service after the Member Server Baseline Policy is applied.

Service	Full Name	Default	Baseline
Alerter	Alerter	Automatic	Disabled
AppMgmt	Application Management	Manual	Disabled
ClipSrv	ClipBook	Manual	Disabled
EventSystem	COM+ Event System	Manual	Manual
Browser	Computer Browser	Automatic	Disabled
DHCP	DHCP Client	Automatic	Automatic
Dfs	Distributed File System	Automatic	Enabled only in the DC role
TrkWks	Distributed Link Tracking Client	Automatic	Automatic
TrkSrv	Distributed Link Tracking Server	Manual	Disabled
MSDTC	Distributed Transaction Coordinator	Automatic	Disabled
DNSSCache	DNS Client	Automatic	Automatic
EventLog	Event Log	Automatic	Automatic
Fax	Fax Service	Manual	Disabled
NtFrs	File Replication	Manual	Disabled
IISADMIN	IIS Admin Service	Automatic	Disabled
Cisvc	Indexing Service	Manual	Disabled

(continued)

Service	Full Name	Default	Baseline
SharedAccess	Internet Connection Sharing	Manual	Disabled
IsmServ	Intersite Messaging	Disabled	Disabled
PolicyAgent	IPSEC Policy Agent(IPSEC Service)	Automatic	Disabled
Kdc	Kerberos Key Distribution Center	Disabled	Enabled only in the DC role
LicenseService	License Logging Service	Automatic	Disabled
Dmservr	Logical Disk Manager	Automatic	Automatic
Dmadm	Logical Disk Manager Administrative Service	Manual	Manual
Messenger	Messenger	Automatic	Disabled
Netlogon	Net Logon	Automatic*	Automatic
Mnmsrvc	NetMeeting Remote Desktop Sharing	Manual	Disabled
Netman	Network Connections	Manual	Manual
NetDDE	Network DDE	Manual	Disabled
NetDDEdsdm	Network DDE DSDM	Manual	Disabled
NtLmSsp	NTLM Security Support Provider	Manual	Disabled
SysmonLog	Performance Logs and Alerts	Manual	Manual
PlugPLay	Plug and Play	Automatic	Automatic
Spooler	Print Spooler	Automatic	Enabled only in the File and Print role
ProtectedStorage	Protected Storage	Automatic	Automatic
RSVP	QoS Admission Control (RSVP)	Manual	Disabled
RasAuto	Remote Access Auto Connection Manager	Manual	Disabled
RasMan	Remote Access Connection Manager	Manual	Disabled
RpcSs	Remote Procedure Call (RPC)	Automatic	Automatic
Rpclocator	Remote Procedure Call (RPC) Locator	Manual	Enabled only in the DC role
RemoteRegistry	Remote Registry Service	Automatic	Automatic
NtmsSvc	Removable Storage	Automatic	Disabled
RemoteAccess	Routing and Remote Access	Disabled	Disabled

Service	Full Name	Default	Baseline
Seclogon	RunAs Service	Automatic	Disabled
SamSs	Security Accounts Manager	Automatic	Automatic
Lanmanserver	Server	Automatic	Automatic
SMTPSVC	Simple Mail Transport Protocol (SMTP)	Automatic	Disabled
ScardSvr	Smart Card	Manual	Disabled
ScardDrv	Smart Card Helper	Manual	Disabled
SENS	System Event Notification	Automatic	Automatic
Schedule	Task Scheduler	Automatic	Disabled
LmHosts	TCP/IP NetBIOS Helper Service	Automatic	Automatic
TapiSrv	Telephony	Manual	Disabled
TintSvr	Telnet	Manual	Disabled
TermService	Terminal Services	Disabled	Disabled
UPS	Uninterruptible Power Supply	Manual	Disabled
UtilMan	Utility Manager	Manual	Disabled
MSIServer	Windows Installer	Manual	Disabled
WinMgmt	Windows Management Instrumentation	Manual	Disabled
WMI	Windows Management Instrumentation Driver Extensions	Manual	Manual
W32Time	Windows Time	Automatic*	Automatic
LanmanWorkstation	WorkStation	Automatic	Automatic
W3svc	World Wide Web Publishing Service	Automatic	Enabled only in the IIS role

* - Automatic for a server in the domain. Manual if server belongs to a workgroup.

Appendix E

Additional Services

The following table lists additional services that are included with Windows 2000 Server and Advanced Server and can be added to a default installation.

Service	Full Name	Baseline
BINLSVC	Boot Information Negotiation Layer	Disabled
CertSvc	Certificate Services	Disabled
ClusSvc	Cluster Service	Disabled
DHCPServer	DHCP Server	Enabled only in the Infra role
DNS	DNS Server	Enabled only in the Infra and DC roles
MacFile	File Server for Macintosh	Disabled
MSFTPSVC	FTP Publishing Service	Disabled
NWCWorkstation	Gateway Service for Netware	Disabled
IAS	Internet Authentication Service	Disabled
MSMQ	Message Queuing	Disabled
NntpSvc	Network News Transport Protocol (NNTP)	Disabled
NSLService	On-Line Presentation Broadcast	Disabled
MacPrint	Print Server for Macintosh	Disabled
RSVP	QoS RSVP	Disabled
Remote_Storage_Engine	Remote Storage Engine	Disabled

(continued)

Service	Full Name	Baseline
Remote_Storage_File_System_Agent	Remote Storage File	Disabled
Remote_Storage_Subsystem	Remote Storage Media	Disabled
Remote_Storage_User_Link	Remote Storage Notification	Disabled
NwSapAgent	SAP Agent	Disabled
SimpTcp	Simple TCP/IP Services	Disabled
Groveler	Single Instance Storage Groveler	Disabled
LDAPSVCX	Site Server ILS Service	Disabled
SNMP	SNMP Service	Disabled
SNMPTRAP	SNMP Trap Service	Disabled
LPDSVC	TCP/IP Print Server	Disabled
TermServLicensing	Terminal Services Licensing	Disabled
TFTPD	Trivial FTP Daemon	Disabled
WINS	Windows Internet Name Service (WINS)	Enabled only in the Infra role
nsmonitor	Windows Media Monitor Service	Disabled
nsprogram	Windows Media Program Service	Disabled
nsstation	Windows Media Station Service	Disabled
nsunicast	Windows Media Unicast Service	Disabled

Index

A

- access control lists. *See* ACLs
- account lockout policy, 85
- accounts, administrator, securing
 - local, 100
- ACLs, 65
 - registry, 94
- Active Directory, structure of, 70
- address spoofing, preventing, 11
- administration, models of, 16
- administrative roles in
 - Exchange 2000, 15
- administrator accounts, securing
 - local, 100
- administrators, setting permissions for, 14
- advanced mode of IIS
 - Lockdown, 35
- anonymous connections, disallowing, 90
- authentication, 47
 - LAN Manager, 93
- Autorun, disabling, 94

B

- back-end Exchange servers
 - encrypting with OWA front-end servers, 51
- baseline policy
 - domain controller, 98
 - member server, services enabled, 96
- blocked e-mail, 38

C

- Centralized Administrative model, 16
- centralizing control, 17
- changing Exchange 2000, 7
- client environment, securing, 11
- configuring ISA servers, 48

- content filtering, 57
- controlling
 - permissions, 9
 - user administration, 18
- creating
 - IPSec policy for OWA back-end servers, 55
 - IPSec policy for OWA front-end servers, 52
 - Management Administrative groups, 17

D

- default script mapping settings in
 - Exchange 2000, 36
- deleting the public folder store, 38
- denial-of-service attacks, 14
- digital signing, 91
- dismounting the mailbox store, 38
- Distributed Administrative model, 16
- DNS configuration, verifying, 66
- domain controller settings, modifying, 23
- domain controllers
 - applying Group Policy changes on, 63
 - replication, 66
- domain environment, evaluating, 66

E

- encrypting, 51
 - between ISA servers and OWA front-end servers, 50
 - MAPI connections, 44
 - messages, 44
- errors, Event Log, Group Policy, 80
- Event Log errors, Group Policy, 80

- Exchange 2000, 17
 - administrative roles in, 15
 - administrator accounts, rights of, 10
 - back-end Server Policy, 30
 - changing, 7
 - clusters, 41
 - default script mapping settings in, 36
 - installing, 9
 - installing and updating in
 - increased security environment, 33
 - risks to, 7
 - server roles in, 22
 - service dependencies, 8
 - Exchange Administration
 - Delegation Wizard, 14
 - modifying, 15
 - Exchange domain servers, group lockdown in, 40
 - Exchange Server Event Service, 29
 - Exchange Server policies, 28
 - back-end, 28
 - express mode of IIS Lockdown, 35

F

- filtering, 13
 - content, 57
- firewalls, 46

G

- globally unique identifier (GUID), 67
- GPOs, 61
 - precedence, 62
- GPResult tool, 77
- group lockdown for Exchange domain servers, 40

Group Policy

- baseline, for member servers, 86
 - changes, applying, 63
 - changes, auditing, 77
 - configuration settings, 64
 - Event Log errors, 80
 - troubleshooting, 78
- Group Policy objects. *See* GPOs
- Group Policy settings, securing, 75

I

- IIS Lockdown, 35
- modifying, 37
- importing security templates, 25
- Information Store service, 33
- installing
- Exchange 2000, 9
 - Exchange 2000 in an increased security environment, 33
- Intersite Messaging, 99
- IP Security connections,
- monitoring, 56
- IPSec policy, 106
- creating for OWA back-end servers, 55
 - creating for OWA front-end servers, 52
 - settings, 52
- ISA servers, 45
- configuring, 48
 - encrypting with OWA front-end servers, 50
 - securing communication with Web browsers, 47
 - using to secure SMTP, 57

J

- junk e-mail. *See also* spam
- managing in Outlook, 13
 - preventing in Exchange 2000, 13

K

- Key Management service, 45

L

- LAN Manager authentication, 93
- local administrator accounts
- securing, 100

M

- mail relay, preventing, 58
- mailbox store, dismounting, 38
- Management Administrative groups, creating, 17
- MAPI connections, encrypting, 44
- message transfer agent (MTA), 30
- messages, signing/encrypting, 44
- Microsoft Exchange Management, 33
- Microsoft Internet Security and Acceleration Server. *See* ISA servers
- Microsoft Management Console (MMC), 107
- Microsoft Operations Framework (MOF), 1
- Microsoft Search, 30
- Microsoft Windows 2000 Group Policy, 61
- security templates, 64
- Mixed Administrative model, 16
- enabling with Exchange system policies, 17
 - supporting, 16
- models of administration
- centralized, 16
 - distributed, 16
 - mixed, 16
- modifying
- domain controller settings, 23
 - Exchange Administration Delegation Wizard, 15
 - IIS Lockdown, 37
 - the SMTP banner, 40
 - URLScan settings, 37
- MOF, process model, 1
- monitoring IP Security connections, 56

O

- organizational units. *See* OUs
- OU structure, 24
- OUs, 61
- Domain Controllers, 73
 - individual server role, 73
 - Member Servers, 72
 - structure, 72
 - structure, creating, 72
- OWA, securing with ISA server, 45
- OWA back-end Servers, creating
- IPSec policy for, 55
- OWA communications, securing, 45
- OWA front-end and back-end servers, using, 22
- OWA front-end servers
- creating IPSec policy for, 52
 - encrypting with back-end Exchange servers, 51
 - encrypting with ISA servers, 50
 - modifying IIS Lockdown and URLScan settings for, 37
 - services policy, 31

P

- password policy, 84
- Password Support in OWA, 38
- patch management, 10
- permissions, setting for administrators, 14
- permissions, controlling, 9
- policies
- Exchange Server, back end, 28
 - OWA front-end server services, 31
- preventing
- address spoofing, 11
 - mail relay, 58
- protecting
- against spam, 12
 - against viruses, 12
- protocols
- SMTP, 99
 - SNTP, 68
- public folder store, deleting, 38

R

registry values, added to security template, 91

Repadmin tool, 67

Reverse lookup, 12

S

searching, 30

Secedit tool, 77

securing

 communication between ISA servers and Web browsers, 47

 OWA communications, 45

 SMTP with ISA server, 57

securing the client environment, 11

Security Descriptor Definition Language (SDDL), 65

security measures, testing, 65

security policy

 account lockout, 85

 domain controller, 83

 domain wide, 83

 member server, 83

 password, 84

 server role, 83

security settings

 domain level, 69

 OU level, 69

security templates

 disadvantages of, 73

 format, 65

 importance of testing, 61

 importing, 73

 registry values added to, 91

security templates, importing, 25

server message block (SMB), 91

server roles, 102

server roles in Exchange 2000, 22

servers

 applying Group Policy changes on, 63

 multipurpose, 70

service dependencies in Exchange 2000, 8

service management functions (SMFs), 2

services, disabled, 29, 32

settings, domain controller, modifying, 23

signing messages, 44

Simple Network Time Protocol, 68

SMTP

 gateway, using inside

 networks, 58

 securing with ISA server, 57

SMTP banner, modifying, 40

SMTP service, 33

spam. *See also* junk e-mail

 educating users about, 12

 protecting against, 12

spiral life cycle, 2

Strategic Technology Protection Program (STPP), 2

supporting a Mixed Administrative model, 16

System Attendant, 32

system policies, 17

T

test environment, 21

testing, importance of, 65

time synchronization, 67

U

Unsolicited mail. *See* spam

URL Scan settings, modifying, 37

user administration, controlling, 18

Using OWA front-end and back-end servers, 22

V

virtual memory, 91

viruses, protecting against, 12

W

Windows Management

 Instrumentation (WMI), 97

