



# Slowing and Stopping E-Mail Transmitted Viruses in an Exchange 2003 Environment

Product Version:	Exchange Server 2003
Reviewed By:	Exchange Product Development
Latest Content:	<a href="http://www.microsoft.com/exchange/library">www.microsoft.com/exchange/library</a>
Author:	John Speare
Published:	May 2004



**Microsoft**

## **Copyright**

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.

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.

©2004 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Outlook, Windows, Windows NT, and Windows Server 2003 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.

## **Acknowledgments**

**Project Editor:** Alison Hirsch

**Contributing Editors:** Lee Ross

**Contributing Writer:** Ross Smith IV

**Technical Reviewers:** Alan Abrahams, Simon Attwell, Karim Batthish, Rich Benack, Tom Frankum, Chris Graham, Harry Katz, Dennis Morgan, Michael Nelte, Ross Smith IV, Michael Surkan, Mark Swift

**Graphic Design:** Kristie Smith

**Production:** Joe Orzech, Sean Pohilla

# Table of Contents

<b>Introduction .....</b>	<b>1</b>
<b>Recommended Actions and Configurations .....</b>	<b>3</b>
Understanding Malicious Software and Microsoft Security Bulletins .....	3
Desktop Client Configuration.....	4
Configure Windows Firewall or Other Personal Firewall Software .....	4
Taking Steps to Secure Outlook.....	5
Secure Outlook Web Access.....	7
End User Awareness Training.....	8
Exchange Server Configurations .....	9
Deploy Antivirus Software at the SMTP Gateway or on the Mailbox Servers .....	9
Restrict Anonymous Access to SMTP.....	10
<b>Optional Configurations.....</b>	<b>13</b>
Lock Down TCP Port 25 .....	13
Using IPsec to Lock Down TCP Port 25 .....	13
Creating the Block TCP 25 Policy .....	14
Disable Exchange Access to Non-secured Versions of Outlook .....	17
Run the Internet Security and Acceleration Server SMTP Filter .....	19
Use Restricted Distribution Groups.....	19
<b>What to Do When a Virus Attack Occurs.....</b>	<b>21</b>
Understanding the "On with no exceptions" Mode Functionality of Windows Firewall ....	21
Cleaning the Exchange Environment .....	22
Stopping Internet Mail Flow.....	22
Stopping Internal Mail Flow .....	23
Isolate and Clean Infected Servers.....	23
Apply Antivirus Software Updates .....	26
Clean User Workstations .....	26
Reestablish User Access to Mailboxes .....	26
Reestablish Mail Flow Connectivity.....	26
<b>Accessibility .....</b>	<b>27</b>



# Introduction

Viruses and worms transmitted by e-mail have become a destructive reality that many administrators of Microsoft® Exchange battle.

This document has been created to help guide the Exchange administrator in fortifying an Exchange environment against e-mail transmitted viruses and worms. This document includes some practical hands-on procedures. However, its main purpose is to join a set of recommendations from the Exchange product team with implementation details that already exist in several locations on the Microsoft.com Web site.

If you are a messaging administrator who is responsible for mail flow at the implementation level, this document is critical because its recommendations and information will help you provide a higher level of service to your clients. If you are a messaging architect, this information will be helpful to you when planning a messaging topology and solution. If you are a desktop administrator, review this article for suggestions for maintaining a virus-free computing environment for your clients. If you are a member of the messaging team, the decision you make about antivirus software should fit into the overall antivirus solution deployed on the desktops. If you are a network or firewall administrator for Microsoft Active Directory® directory service, you may also benefit from understanding the recommendations in this document.

This document is divided into three main sections:

- **Recommended Actions and Configurations** This section provides the recommendations that you should implement to help minimize the impact of viruses and worms in the e-mail environment.
- **Optional Configurations** This section discusses some lower priority or alternate configuration suggestions that you should implement if you are unable to implement all the recommendations in the first section.
- **What to Do When a Virus Attack Occurs** This section gives a suggested set of recommendations and procedures for handling a virus outbreak. It is critical that you read this section and create a plan before an actual outbreak occurs.

This document provides a collection of recommendations with pointers to implementation details. Each subsection of this document begins with a short description of the recommendation or configuration. This description is followed by a set of recommendations and a list of resources for the implementation details related to the recommendations. If specific implementation details are not available elsewhere, this document provides the details.



# Recommended Actions and Configurations

The recommendations in this section will help stop and slow the spread of e-mail-transmitted viruses. These recommendations concern the following:

- Understanding malicious software and Microsoft security bulletins
- Configuring desktop clients, including firewalls
- Taking steps to help secure Outlook
- Taking steps to help secure Outlook Web Access
- Training the end user to be aware of malicious software
- Configuring your Exchange servers

**Note**

This document has been written with the supposition that antivirus software is running on all desktop computers in your organization. Therefore, this document does not discuss deployment of antivirus software on the client desktops. However, strategies for running antivirus software in the Exchange server environment are discussed.

---

## Understanding Malicious Software and Microsoft Security Bulletins

There are many classes of malicious software, also known as malware. In general, this document refers to malware that is transmitted through e-mail and that is self-propagating as viruses and worms. It is helpful to understand the basic terminology used for various types of malicious software.

After you have a basic understanding of the different types of malicious software, visit the Microsoft Security Bulletin Search Web site and verify that all Microsoft software running in your organization is up-to-date.

**Recommendations**

- Learn how to distinguish a virus from a worm from a Trojan horse and so on.
- Learn how to keep Microsoft software current with the latest updates. This is one of the most important actions you can take to help slow and stop viruses.

**Resources**

- For more information about how the types of malicious software are defined, see the "Defining Malware: FAQ" Web site (<http://go.microsoft.com/fwlink/?LinkId=28397>).
- For security bulletins, see the "Microsoft Security Bulletin Search" Web site (<http://go.microsoft.com/fwlink/?LinkId=12322>).

# Desktop Client Configuration

The most recent releases and service packs of Microsoft Windows® and Microsoft Office Outlook® include many security and virus-fighting enhancements. For example, beginning with Outlook 2002, attachment blocking and Object Model Guard are included and enabled by default. Windows XP Service Pack 2 (SP2) includes Windows Firewall, formerly Internet Connection Firewall, built into the network properties page. In some cases, functionality can be applied to earlier versions of Microsoft software through updates. However, to help maintain a secure environment, it is recommended that you run the latest versions of Windows and Outlook. This section gives recommendations for client updates that are specific to Windows and Outlook, with links to more in-depth implementation details.

In addition to keeping Windows and Outlook up-to-date, it is critical that your antivirus signatures are up-to-date across your organization. Also, implementing an aggressive update management solution for the software in your organization is extremely important. For more information about update management for Microsoft software, see *Understanding Patch and Update Management: Microsoft's Software Update Strategy* (<http://go.microsoft.com/fwlink/?LinkId=28377>).

---

## Configure Windows Firewall or Other Personal Firewall Software

Windows XP SP2 includes Windows Firewall (formerly Internet Connection Firewall), which allows users to block traffic on seldom-used ports by selecting a single check box. Running Windows Firewall or other third-party personal firewall software on client computers is critical to help slow or stop many viruses. For example, when the MyDoom worm infects a computer, TCP ports 3127 through 3198 will respond to inbound requests. Their response allows the potential for an attacker to connect to the computer and use the computer as a proxy to access network resources. Installing and configuring a firewall on client computers blocks the effectiveness of this type of worm.

### Note

Windows has provided three different firewall solutions. Internet Connection Firewall and Basic Firewall are components of the Routing and Remote Access service in Windows Server 2003™. Windows XP and Windows XP SP1 include Internet Connection Firewall, which is a Control Panel feature that you can use to set restrictions on the traffic that is allowed to enter your network from the Internet. Windows Firewall refers to the firewall that is included with Windows XP SP2.

By default, Internet Connection Firewall is disabled in Windows XP and Windows XP SP1. By default, in Windows XP SP2, Windows Firewall is enabled for all connections. In addition, Windows Firewall can now be managed by Group Policy objects (GPOs), allowing administrators to configure different levels of protection based on the location of mobile computers. For example, consider a scenario where a laptop is connected to an enterprise's domain. The port restrictions may be less restrictive than if the laptop was connected to a public wireless Internet access point.

It is important to recognize that there are hundreds of applications that use various ports to communicate. Some examples of applications that define their own ports include instant messaging, peer-to-peer file sharing and communication software, and line-of-business applications. Running Windows Firewall or other personal firewall software may cause these applications to fail. Make sure you review all firewall documentation carefully. Test the configuration before deploying it across your organization.

### Recommendations

- Upgrade all Windows clients to Windows XP SP2, or deploy other third-party personal firewall software.
- Develop a standardized set of allowed ports. If you are deploying the Windows XP Windows Firewall, define the allowed ports for the "Domain" and "Mobile" cases.

- Deploy firewall configurations to all clients. If you are deploying the Windows XP Windows Firewall, deploy the client configuration through Group Policy objects.

#### Resources

- For more information about updates to Windows Firewall in Windows XP SP2, see *Changes to Functionality in Microsoft Windows XP Service Pack 2* (<http://go.microsoft.com/fwlink/?LinkId=28379>).
- For more information about using Group Policy objects to deploy and configure Windows Firewall in your enterprise, see *Deploying Windows Firewall Settings for Microsoft® Windows® XP with Service Pack 2* (<http://go.microsoft.com/fwlink/?LinkId=28380>).

---

## Taking Steps to Secure Outlook

As mentioned previously, upgrading to the latest version of Outlook and regularly obtaining updates provides your client desktops with the most up-to-date virus protection for Outlook.

Attachment blocking and Object Model Guard are important functionality in Outlook that help slow or stop the spread of viruses. This section explains how these two features protect the Outlook client and explains which versions of Outlook can be updated to include the features.

#### Note

Although this section discusses how to apply security updates to earlier versions of Outlook, be aware that Outlook 2000 Service Pack 3 (SP3) is the earliest version of Outlook that Microsoft Product Support Services (PSS) supports. For more information about Office and PSS support, see Office Family Products Support Lifecycle FAQ Web site (<http://go.microsoft.com/fwlink/?LinkId=28381>).

---

## Attachment Blocking in Outlook

One common method virus writers use to transport viruses is to include the virus in an attachment. For example, a virus can be delivered by attaching an executable program (.exe) to an e-mail message. In some cases, viruses can be delivered by embedding them in a macro, which appears to users as a safe document (such as a Microsoft Word or Excel file).

Attachment blocking functionality is one of the most effective deterrents against viruses spread by e-mail. By default, Outlook 2003 and Outlook 2002 include attachment blocking functionality to protect against such viruses. To enable attachment blocking on Outlook 2000, Outlook 98, and Outlook 97, you must download and install the security update specific to the version you want to protect. By default, the latest service packs to supported versions of Outlook block 71 types of attachments.

Attachment blocking is essential for all e-mail clients today. However, you must still educate your users to not open attachments from unknown senders. For more information about educating users, see "End User Awareness Training" later in this document.

---

## Object Model Guard

Object Model Guard protects access to address book data, recipient data on an item, and programmatic sending of e-mail messages in Outlook. Object Model Guard applies to the Outlook object model and to Simple MAPI. When Object Model Guard is enabled, the user is prompted if any application tries to send an e-mail message from the mailbox profile. The same behavior occurs when non-Outlook processes try to access the address book. The user can set a timed interval for a specified process to access the object model or the Outlook address book. It is important to understand that Object Model Guard does not prevent a user from sending a virus. Rather, it blocks automated processes from accessing the object model and the address book.

By default, Object Model Guard is installed and enabled in Outlook 2003 and Outlook 2002. To enable Object Model Guard in Outlook 2000 or Outlook 98, you must download the security update specific to the version you want to protect. Object Model Guard is not included in the Outlook 97 security update.

### Recommendations

- Upgrade to Outlook 2003, or if running Outlook 2002, make sure to keep it up-to-date with the latest service pack and updates.
- If you are running a version of Outlook other than Outlook 2003 or Outlook 2002, download and deploy the security update for Outlook 2000 or Outlook 98. If you are running Outlook 97, upgrade to a version of Outlook that supports Object Model Guard. Outlook 2000 SP3, which includes the security update, is the earliest version of Outlook that Microsoft supports.

### Resources

- For more information about Object Model Guard and attachment blocking in Outlook 2003 and Outlook 2002, see the "How Outlook helps to protect your computer from viruses" Web site (<http://go.microsoft.com/fwlink/?LinkId=28382>).
- For more information about customizing the Outlook 2000 or Outlook 98 security updates, see the "Customizing the Outlook 98/2000 E-mail Security Update" Web site (<http://go.microsoft.com/fwlink/?LinkId=28383>).
- For more information about deploying and administering the Outlook security updates, see the "Microsoft Office Resource Kit Toolbox" Web site (<http://go.microsoft.com/fwlink/?LinkId=28384>).
- For more information about helping to secure Outlook 98, see the following:
  - *Outlook 98 Update E-mail Security* (<http://go.microsoft.com/fwlink/?LinkId=28385>)
  - *Outlook 98 Update: Java Permissions Security* (<http://go.microsoft.com/fwlink/?LinkId=28386>)
  - *Outlook 98 E-mail Security Update International Releases* (<http://go.microsoft.com/fwlink/?LinkId=28387>)
- For more information about helping to secure Outlook 2000, see the following:
  - *Outlook 2000 SR1: Extended E-mail Security Update* (<http://go.microsoft.com/fwlink/?LinkId=28388>)
  - *Microsoft Outlook 2000 SR1 E-mail Security Update for MultiLanguage Pack* (<http://go.microsoft.com/fwlink/?LinkId=28389>)
  - Microsoft Knowledge Base article 263297, "OL 2000: Administrator Information About the Outlook E-mail Security Update" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=263297>)
  - *Office 2000 Update: Service Pack 3 (SP3)*, which includes the Outlook 2000 extended e-mail security update. It is the earliest version of Office that PSS supports. (<http://go.microsoft.com/fwlink/?LinkId=28390>)

# Secure Outlook Web Access

If you are using Outlook Web Access in your organization, review attachment blocking and Internet Explorer security zone configuration.

---

## Attachment Blocking in Outlook Web Access

In Exchange 2000 Service Pack 2 (SP2), Outlook Web Access introduced the ability to block attachments by file type and Multipurpose Internet Mail Extensions (MIME) type. By default, in Outlook Web Access 2003 and Outlook Web Access for Exchange 2000, attachment blocking is enabled. With this default configuration, users can send any attachment type, but they will not receive dangerous file types, such as .exe, .bat, and .vbs files. The default list of blocked file types in Outlook Web Access includes the default list that is used by Outlook 2003, plus XML files and specific MIME types.

Attachment blocking in Outlook Web Access is configured on the Exchange server through the registry. The configuration can be deployed as a Group Policy object (GPO) to ensure consistency.

If you allow access to mailboxes from the Internet through Outlook Web Access, you may not have administrative control of the computers that are accessing mail. In some cases, such as when users are accessing Outlook Web Access from the Internet, you may want to restrict users' ability to download any attachments from such computers. In this case, you can set a registry key on the Exchange front-end servers that will block all attachments in Outlook Web Access when the computer accesses Exchange through specific front-end servers.

---

## Internet Explorer Security Zone Configuration

Because Outlook Web Access is an application running in Internet Explorer, it is important to consider the configuration of Internet Explorer in the context of fighting viruses. It is recommended that you configure the Internet Explorer security zones to be as restrictive as the functionality your clients' requirements will allow. At a minimum, deploy Internet Explorer 6.0 SP1 in its default configuration, which sets the Internet zone at a Medium level of security and the intranet zone at a Medium-Low level.

Outlook Web Access and Outlook Web Access with the S/MIME control have been designed and engineered with strict attention to Web-based vulnerabilities, such as cross-site scripting, IFRAME manipulation, and other known, malicious HTML-based activity. Specifically, Outlook Web Access runs and displays only known safe HTML elements, attributes, and style information, therefore blocking against the malicious use of HTML in previously unknown ways.

Running Outlook Web Access with the S/MIME control also adds an extra layer of security around message attachments. Mail attachments downloaded with the S/MIME control are deleted more thoroughly (memory address space is zeroed, or nulled, after deletion) than those that are downloaded with Outlook Web Access without the S/MIME control. The Exchange 2003 SP1 version of Outlook Web Access S/MIME control setup is a Microsoft Windows Installer file. Therefore, it can be deployed through Microsoft Systems Management Server (SMS) or another enterprise management program.

**Note**

Because the S/MIME control is an installable component, it may not be practical or possible to run it in all deployment scenarios, such as public kiosks and other scenarios where the client computer is not centrally administrable.

It is recommended that you run Outlook Web Access with the S/MIME control. The S/MIME control only runs on Internet Explorer 6 or later and on Windows 2000 or later. The S/MIME control does not run on other Web browsers or earlier operating systems. As mentioned previously, update management of all software running in your organization is an extremely important part of the fight against viruses and worms. Internet

Explorer updates are managed through Windows Update. By keeping Windows up-to-date, you also have the latest updates for Internet Explorer.

### Recommendations

- Deploy the Exchange 2003 version of Outlook Web Access and the latest version of Internet Explorer.
- The default file and MIME-type block list is likely sufficient for your organization. However, you may want to review, update, and deploy the blocked file and MIME types for Outlook Web Access. Maintain consistency between the blocked file types in Outlook Web Access with the file types that are blocked in Outlook.
- In some cases, where you cannot control the computer accessing Outlook Web Access from the Internet, consider blocking all attachments.
- Define the correct level of security for Internet Explorer in your organization, and deploy a standardized configuration to the desktops.
- Deploy the Outlook Web Access S/MIME control to all clients that access mail through Outlook Web Access, even if your organization does not use S/MIME.

### Resources

- For more information about deploying and upgrading to Exchange 2003 and Outlook Web Access, see the *Exchange Server 2003 Deployment Guide* (<http://go.microsoft.com/fwlink/?linkid=21768>).
- For more information about deploying Internet Explorer, see the "Microsoft Internet Explorer 6.0 Administrative Kit Service Pack 1" Web site (<http://go.microsoft.com/fwlink/?LinkId=28391>), and then click "Redistributing Internet Explorer."
- For more information about reviewing and updating blocked file and MIME types in Outlook Web Access, see the *Exchange 2003 Security Hardening Guide* (<http://go.microsoft.com/fwlink/?linkid=25210>).
- For more information about blocking all attachments from front-end server connections in Outlook Web Access, see Microsoft Knowledge Base article 823486, "Administrative and Registry Key Settings for Exchange Server 2003 Outlook Web Access" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=823486>).
- For more information about understanding, configuring, and deploying security zones in Internet Explorer, see the "Microsoft Internet Explorer 6.0 Administration Kit Service Pack 1" Web site (<http://go.microsoft.com/fwlink/?LinkId=28391>), and then click "Security."

---

## End User Awareness Training

Generally, viruses and worms get into your network through unsolicited e-mail messages, also known as spam. Educating users about how to deal with spam effectively can help reduce the chance that viruses and worms get into your organization. Spam is frequently a result of social engineering tactics employed against your users. For example, your users may receive spam that includes a disclaimer stating something that is similar to the following:

**If you wish to be removed from this mailing list, you should respond to the mail with the word "Remove" in the subject line.**

Although this is a legitimate tool for some reputable companies, it is frequently a means of verifying that an e-mail address is valid so that the address can be used again. It is likely that the address will be sold to other spammers now that it has been validated.

Attachments are the most important education area for users. Help them to understand what types of attachments are safe to open. Almost every virus transmitted by e-mail relies on users opening some kind of malicious attachment to initiate the virus. Some file formats, such as .zip files that are protected with a password, may be allowed and antivirus file scanners cannot scan them. Also, users should know about double-extension attachments, such as executables with a .jpg extension (Filename.exe.jpg), which pass through the attachment blocking as a .jpg file, but may contain malicious code in the executable.

**Note**

Educating users is not a substitute for running antivirus client software on the desktop.

**Recommendation**

- Educate users about how to combat spam and viruses.

**Resource**

- For more information about what users can do to combat spam, viruses, and worms, see *Fighting unwanted e-mail (spam)* (<http://go.microsoft.com/fwlink/?LinkId=24701>).

---

## Exchange Server Configurations

Deploying antivirus software and making sure TCP port 25 is not available as an open relay for viruses are two main configuration areas that you must address for your Exchange environment.

Before you review the configuration recommendations, keep in mind several important policy recommendations:

- Do not run e-mail clients on the Exchange server. If you are running an e-mail client on a computer that is running Exchange and it becomes infected, an infected client becomes an infected mail server.
- Do not browse the Internet from the Exchange computer for the same reasons. A general best practice in reducing the attack surface is to minimize the applications running on an Exchange server.
- Keep your Exchange servers up-to-date with the latest security updates from Microsoft.
- Lock down your Exchange servers by following the recommendations in the *Exchange Server 2003 Security Hardening Guide* (<http://go.microsoft.com/fwlink/?linkid=25210>).

---

## Deploy Antivirus Software at the SMTP Gateway or on the Mailbox Servers

At a minimum, you must deploy antivirus software designed for messaging systems at either the Simple Mail Transfer Protocol (SMTP) gateway or at the Exchange servers that host mailboxes. The two resources listed in the following Resources section explain the strategies you can use in planning your messaging antivirus deployment and the different types of message scanning available. The types of antivirus software you choose and where the software is deployed are determined by the balance between the cost you are willing to tolerate and the risk you are willing to assume.

For example, some organizations run antivirus messaging software at the SMTP gateway, antivirus file-level scanning at the Exchange server, and antivirus client software on the user desktop. This approach provides messaging-specific protection at the gateway, general file-level protection at the mail server, and protection at the client. Other organizations may assume greater cost and security by running the same scheme with the addition of antivirus software compatible with Exchange VSAPI 2.5 on the Exchange mailbox server.

### Recommendations

- Run client antivirus software on the desktop. If you are running antivirus software designed for messaging systems (it can parse and scan MIME) at the gateway or on the Exchange server, running a file-level scanner at the desktop is sufficient.
- At a minimum, deploy antivirus software designed for messaging systems at either the SMTP gateway or at the Exchange servers that host mailboxes. For the most protection, run antivirus software at the gateway that scans the inbound MIME messages, and a scanner on the Exchange Server that uses VSAPI 2.5.

### Resources

- For information about planning an antivirus software strategy, see the *Exchange Server 2003 Security Hardening Guide* (<http://go.microsoft.com/fwlink/?linkid=25210>).
- For a description of different types of antivirus software that you can run in an Exchange messaging environment, see the Microsoft Knowledge Base article 823166, "Overview of Exchange Server 2003 and Antivirus Software" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=823166>).
- For more information about why running mail clients on an Exchange server is not recommended, see the Microsoft Knowledge Base article 266418, "XCCC: Microsoft Does Not Recommend Installing Exchange 2000 Server and Outlook 2000 or Later on the Same Computer" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=266418>).
- For more information about antivirus vendors who are Microsoft partners, see the "Exchange Partners: Antivirus" Web site (<http://go.microsoft.com/fwlink/?LinkId=16226>).

---

## Restrict Anonymous Access to SMTP

By default, Exchange 2003 sets up in a secure mode for anonymous SMTP access. Anonymous or open relay is disabled, and non-authenticated mail submitted to Exchange 2003 from within the organization is not displayed as resolved on the Outlook client. Therefore, restricting anonymous access to SMTP is partially done by default, in that anonymous relaying is disabled. However, internal anonymous SMTP access is not disabled. This section gives recommendations for reviewing and verifying your relay configuration and further restricting internal anonymous SMTP access.

---

### Anonymous Relay

It is essential that you do not allow anonymous relaying on your SMTP virtual servers. Relaying is when someone uses your Exchange server to send mail to an external domain. An open relay allows someone sending spam to use your external SMTP servers to send messages on their behalf. This activity will likely cause your gateway servers to be listed as a spam relay on Internet block lists.

In its default configuration, Exchange allows only authenticated users to relay mail. Only authenticated users can use Exchange to send mail to an external domain. If you modify the default relay settings to allow unauthenticated users to relay, or if you allow open relaying to a domain through a connector, unauthorized users or malicious worms can use your Exchange server to send spam. Your server may be block-listed and be prevented from sending mail to legitimate remote servers. To prevent unauthorized users from using your Exchange server to relay mail, at a minimum, use the default relay restrictions.

If you have legitimate reasons for relaying, you should follow the guidelines for making sure that security is preserved in your implementation. This is mainly done by leaving the deny all defaults and adding only the IP addresses from which you will accept relayed mail, and disabling access for authenticated users.

Review how built-in accounts (local Administrator) and other users are used on your gateway servers. It is unlikely that you are using the built-in accounts for any kind of relaying. If you are relaying, the relaying is

probably by a known set of users or computers. Restricting relay rights to explicit users and computers or to an IP address is recommended.

Configuring explicit permission to relay will further help to fortify your server. Malicious users may use a brute-force attack to try to obtain the passwords for built-in accounts or for user accounts found on the Internet so that they can use your server as a spam proxy. Therefore, the default setting that allows any authenticated computer to relay is not recommended for computers that are accessible from the Internet. Disabling this setting is recommended.

---

## Anonymous SMTP Access

Exchange 2003 does provide the ability for client-side users to recognize spoofed mail by displaying the actual SMTP address of nonauthenticated mail as opposed to the display name as it appears in the global address list (GAL). However, disabling anonymous SMTP access on all internal Exchange servers is recommended. The Outlook behavior concerning nonauthenticated (or potentially spoofed) mail is subtle. It takes an attentive and experienced user to recognize that an actual SMTP address means that the sender did not authenticate. Therefore, disabling anonymous access ensures that only authenticated users can submit messages within your organization. Additionally, requiring authentication forces client programs such as Outlook Express and Outlook in Internet Mode (Post Office Protocol version 3, or POP3, or Internet Message Access Protocol version 4rev1, or IMAP4) to authenticate before sending mail.

### Recommendations

- Review your relay configuration. Configure all SMTP virtual servers such that only explicit users, computers, or IP addresses are allowed to relay to other organizations.
- Disable the ability for all authenticated computers to relay.
- Disable anonymous SMTP access on all internal Exchange servers.

### Resources

- For information about securing SMTP relaying and routing, see "Securing Your Exchange Server" in the *Exchange Server 2003 Transport and Routing Guide* (<http://go.microsoft.com/fwlink/?linkid=26041>).
- For more information about how to control relaying, see Microsoft Knowledge Base article 304897, "XIMS: Microsoft SMTP Servers May Seem to Accept and Relay E-Mail Messages in Third-Party Tests" (<http://go.microsoft.com/fwlink/?LinkId=3052&kbid=304897>).



# Optional Configurations

The recommendations in this section are important. However, they are not as critical as the recommendations in the previous section. If you follow the guidelines in the previous section, following these optional configuration guidelines will provide an extra layer of protection against the spread of viruses.

---

## Lock Down TCP Port 25

As viruses and worms become more sophisticated, SMTP (typically port 25) is becoming a more common transport mechanism for malicious purposes. One example of this sophistication is the w32.hllw.gaobot.dk worm. This worm is a Trojan horse that installs pieces of an SMTP mail service on the victim's computer. This installation allows the worm to send spam from the computer. To disable the effectiveness of such worms and viruses, you can configure your network such that SMTP traffic is only allowed to travel between Exchange servers, domain controllers, and other computers that require SMTP.

Because of the management overhead in restricting SMTP traffic, you may only consider this implementation if you are not running or cannot run a personal firewall on the desktop computers. Running antivirus software in addition to a personal firewall on the desktop will help to keep the majority of worms and viruses out of your network, or at least debilitate them to the extent that they are easier to remove after an isolated infection.

---

## Using IPSec to Lock Down TCP Port 25

Only certain systems in an environment listen and respond to requests on TCP port 25. In a Microsoft environment, only servers running Internet Information Services (IIS), domain controllers, and Exchange servers typically use TCP port 25. When you block the listening of TCP port 25 on all other systems, you help to increase the security of your environment by removing one attack vector that malicious code can use.

This section provides a generic set of procedures for setting up Internet Protocol security (IPSec) to block TCP port 25. IPSec is a set of technologies included in the Windows Server operating system that allows administrators to run specific actions such as authentication, block traffic, and encrypt traffic based on filters ("all traffic on TCP 25").

The procedures are based on the architecture defined in the *Windows Server 2003 Security Guide* and the *Exchange Server 2003 Security Hardening Guide*. Additionally, these procedures also assume that all workstations are in a central organizational unit (named *Workstations*) within a domain. If your architecture is not configured according to the recommended deployments in the *Windows Server 2003 Security Guide* and the *Exchange Server 2003 Security Hardening Guide*, use this procedure as a foundation for testing and building your own IPSec policies. In either case, complete testing is recommended before you deploy the IPSec policies.

It is important to recognize the potential impact that deploying the policy may have in your organization. Implemented as described, the policy blocks all SMTP traffic to and from all the computers in the *Workstation* organizational unit. If your organization uses IMAP or POP for e-mail, these clients will not work. Additionally, any other applications, such as line-of-business tools and automated mailers may also fail if SMTP is blocked.

**Note**

IPSec policies through Group Policy are inheritable, but they do not merge. Where more than one IPSec Group Policy is applied, the last Group Policy applied to a computer takes effect.

---

## Creating the Block TCP 25 Policy

You must complete all of the following tasks to create a policy to block TCP port 25 through IPSec and Group Policy:

1. Create the base Group Policy object.
2. Create the filter lists.
3. Create a block action.
4. Create and assign the IPSec policy.
5. Apply the IPSec Group Policy to other organizational units (optional).

**Note**

The procedures specify naming conventions in ***bold italic***. As you work through the procedures, notice that the policies, descriptions, and filters that are named in earlier procedures are referenced in subsequent procedures (again in ***bold italic***).

---

## Create the Base Group Policy Object

The account that you use to perform this procedure must be a member of the Domain Admins security group in the domain where the policy will run.

### To create the base Group Policy object

1. Open the **Active Directory Users and Computers** snap-in.
2. Right-click the *Workstations* organizational unit, and then select **Properties**.
3. Select the **Group Policy** tab.
4. Click **New**, and then name the Group Policy **Block TCP25 Policy**.

---

## Create Filter Lists

You must create one filter list to block inbound SMTP connection requests and one filter list to block outbound SMTP connection requests.

### To create the inbound SMTP filter list

1. In **Group Policy Object Editor**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
2. Right-click **IP Security Policies on Active Directory**, and then select **Manage IP Filter lists and filter actions**. The **Manage IP filter lists and filter actions** property page is displayed.

3. On the **Manage IP Filter Lists** tab, click **Add**. The **IP Filter List** page is displayed.
4. In the **Name** field, enter *Inbound TCP 25*. In the **Description** field, enter *This filter responds to inbound requests on TCP 25*, and then click **Add**.
5. On the **IP Filter Wizard Welcome** page, click **Next**.
6. On the **IP Filter Description and Mirrored property** page, enter a filter description, and then click **Next**.

**Note**

If you do not enter a description here, future troubleshooting with the Network Diagnostics tool (netdiag.exe) will not display the name of the filter.

7. On the **IP Traffic Source** page, select **Any IP Address** and then click **Next**.
8. On the **IP Traffic Destination** page, select **My IP Address** and then click **Next**.
9. On the **IP Protocol Type** page, select **TCP** and then click **Next**.
10. On the **IP Protocol Port** page, select **From any port** and **To this port**, and then enter **25** in the open field. Click **Next**.
11. On the finish page, click **Finish**. On the **IP Filter List** page, click **OK**.

**To create the outbound SMTP filter list**

- Follow the procedure for creating the inbound SMTP filter list, with the following exceptions:
  - a. In step 4, in the **Name** field, enter *Outbound TCP 25*. In the **Description** field, enter *This filter responds to outbound requests on TCP 25*.
  - b. In step 7, on the **IP Traffic Source** page, select **My IP Address**.
  - c. In step 8, on the **IP Traffic Destination** page, select **Any IP Address**.

## Create a Block Action

In the previous procedures, you defined two filters. To make these filters block SMTP traffic on the target computers, you must specify the action to take on these filters. This procedure explains how to specify the block action.

**To create a block action**

1. In **Group Policy Object Editor**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
2. Right-click **IP Security Policies on Active Directory**, and then select **Manage IP Filter lists and filter actions**. The **Manage IP filter lists and filter actions** property page is displayed.
3. Click the **Manage Filter Actions** tab, and then click **Add**. The **Filter Action Wizard** is displayed.
4. On the **Welcome to the IP Security Filter Action Wizard** page, click **Next**.
5. On the **Filter Action Name** page, enter *Block* in the **Name** field, *Blocks traffic* in the **Description** field, and then click **Next**.
6. On the **Filter Action General Options** page, select **Block**, and then click **Next**.
7. Click **Finish**.

## Create and Assign the IPSec Policy

So far, you have created the base Group Policy object, defined the SMTP filters, and specified the block action to take on the filters. Now you must create and assign the IPSec policy.

### To create the IPSec policy

1. In **Group Policy Object Editor**, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.
2. Right-click **IP Security Policies on Active Directory**, and then select **Create IP Security Policy**. The IP Security Policy Wizard is displayed.
3. On the **Welcome to the IP Security Policy Wizard** page, click **Next**.
4. On the **IP Security Policy** page, enter **Block TCP 25 Policy** in the **Name** field, enter **This policy blocks TCP 25** in the **Description** field, and then click **Next**.
5. On the **Requests for Secure Communication** page, clear the **Activate the default response rule** check box, and then click **Next**.
6. On the **Completing the IP Security Policy Wizard** page, leave the check box, **Edit properties** selected (checked), and then click **Finish**. The **Block TCP 25 Policy Properties** page will be displayed.
7. On the **Rules** tab, click **Add**. The Security Rule Wizard is displayed.
8. On the **Welcome to the Create IP Security Rule Wizard** welcome page, click **Next**.
9. On the **Tunnel Endpoint** page, leave the default selection **This rule does not specify a tunnel**, and then click **Next**.
10. On the **Network Type** page, leave the default selection **All network connections**, and then click **Next**.
11. On the **IP Filter List** page, select **Inbound TCP 25**, and then click **Next**.
12. On the **Filter Action** page, select **Block**, and then click **Next**.
13. On the **Completing the Security Rule Wizard** page, clear the check box **Edit properties**, and then click **Finish**.
14. You must now specify the Outbound TCP 25 filter. Follow steps 7 through 13. However, in step 11, select **Outbound TCP 25**.

### To assign the IPSec policy

1. In **Group Policy Object Editor**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, and then click **IP Security Policies on Active Directory**.
2. In the details pane, right-click the **Block TCP 25 Policy**, and then select **Assign**.

The policy will be applied after replication between domain controllers is complete, and the client computers check for the new policy updates, which defaults at 90 minutes.

To force the policy on Windows Server 2003 and Windows XP, run the following command on the **Run** line:

```
gpupdate /force
```

To force the policy on Windows 2000, run the following command on the **Run** line:

```
secedit /refreshpolicy machine_policy /enforce
```

## Applying the IPSec Policy on Other Organizational Units

This section explains how you can apply the Block Inbound TCP 25 Policy filter to other organizational units in your enterprise. This procedure uses the Print organizational unit from the *Windows Server 2003 Security Guide* architecture as an example. Consider running this policy on organizational units in your enterprise that do not contain domain controllers, Exchange servers, or other computers that require SMTP inbound connectivity.

### To apply the IPSec policy on other organizational units

1. Open **Active Directory Users and Computers** using an account with Domain Admin privileges.
2. Right-click the *Member Servers\Print* organizational unit, and then select **Properties**.
3. On the **Group Policy** tab, click **Add**.
4. In the **Add a Group Policy Object Link** dialog box, click the **All** tab, select *Block TCP25 Policy*, and then click **OK**.

### Resources

Although the procedures given earlier in this document will accomplish the basic lockdown of TCP port 25 using IPSec, it is recommended that you become familiar with IPSec and the other services, like authentication and encryption, that can be provided by IPSec. The following documents are introductory in scope:

- *What Is IPSec?*  
(<http://go.microsoft.com/fwlink/?LinkId=28392>)
- *The IPSec process*  
(<http://go.microsoft.com/fwlink/?LinkId=28393>)
- *Security information for IPSec*  
(<http://go.microsoft.com/fwlink/?LinkId=28394>)
- *Creating, modifying, and assigning IPSec policies*  
(<http://go.microsoft.com/fwlink/?LinkId=28395>)

---

## Disable Exchange Access to Non-secured Versions of Outlook

After you have updated to Outlook 2003 or Outlook 2002, or you have installed Outlook 2000 Service Release 1 (SR1) or the security update for Outlook 98 as recommended earlier, you can lock out access to Exchange from earlier versions of Outlook that have not been updated. Locking out earlier versions of Outlook that do not support attachment blocking and Object Model Guard helps provide a known level of client security for MAPI client connections.

### Recommendation

- At a minimum, disable access to Outlook 98 (with no security update installed) and earlier versions.

### Resource

- For more information about how to disable access to Exchange based on the Outlook build number, see the Microsoft Knowledge Base article 288894, "XADM: Feature to Disable MAPI Client Access" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=288894>).

Table 1 shows the major versions of Outlook along with their build number (as specified on Emsmbd32.dll) and the corresponding MAPI number that you should enter when specifying the build in the registry key that is referenced in Knowledge Base article 288894.

**Table 1 Build numbers and corresponding MAPI version numbers for relevant versions of Outlook**

Version	Build number	MAPI number
Exchange 2003 or Exchange 2000	6.1.0–6.9999.0	6.x
Outlook 2003	11.0.5604.0	11.5604
Outlook 2002 SP3	10.0.6515.0	10.0.6515
Outlook 2002	10.0.2627.1	10.0.2627
Outlook 2000 SP3	5.5.3165.0	5.3165.0
Outlook 2000 SR1a	5.5.3121.0	5.321.0
Outlook 98, with security update installed	5.5.2652.57	5.2652.57
Outlook 98	5.5.2178.0	5.2178.0

To help protect against all outdated versions of Outlook (Outlook 98 with no security update installed, and earlier versions), disallow all versions of Outlook with build numbers equal to or less than 5.5.2178.0 from connecting to Exchange. The value data as specified in the Microsoft Knowledge Base article 288894 are the following:

```
Value name: Disable MAPI Clients
Value type: REG_SZ
Value data: -5.2178.0
```

If you are blocking ranges of Outlook clients, be sure to leave the 6.0 range open for Exchange administration. Specifically, do not block any values from 6.1.0 to 6.9999.0. All versions of Exchange 2000 and later use a 6.0.0 range for administration. The following table shows the registry key value to enter to block specific ranges of Outlook clients against computers running Exchange 2000 or later.

**Table 2 Registry key values to block ranges of Outlook clients**

To allow	Set the registry key to
Only Outlook 2003	-6.0.0;10.0.0-11.5603.0
Outlook 2002 SP3 and later	-6.0.0;10.0.0-10.0.6514;11.0.0-11.5603.0
Outlook 2000 SP3 and later	-5.3164.0;10.0.0-10.0.6514;11.0.0-11.5603.0
Outlook 98 with security update installed and later	-5.2652.56;5.3000.0-5.3164.0;10.0.0-10.0.6514;11.0.0-11.5603.0

Microsoft Product Support Services does not support Outlook clients that are earlier than Outlook 2000 SP3. Outlook 2000 SP3 contains the Outlook 2000 security update.

Exchange 2000 servers require that the store process be restarted after a change is made to this registry value. However, in the original released version of Exchange 2003 and later versions, implementation of this parameter is dynamically applied within 15 minutes of the change.

# Run the Internet Security and Acceleration Server SMTP Filter

In addition to the social engineering tactics that spam relies on (such as a message with a subject line of "I love you"), many viruses also rely on limitations or inherent weaknesses in the services that they attack. You can configure Microsoft Internet Security and Acceleration (ISA) Server 2004 to run with an SMTP filter that combats spam, viruses, and buffer overflows. Fighting spam may help reduce the surface area for a virus to spread. The SMTP filter is an application layer filter that is run at the corporate firewall. The SMTP filter allows you to specify keywords that, if found in a message, can trigger an action. At the same time, ISA Server inspects the SMTP communications for anomalies in the application layer header and data sections of a communication.

Application layer filtering firewalls build on the features of the conventional stateful filtering firewalls and enforce both valid connection states and valid application layer communications. Attackers use a variety of application layer specific methods to exploit known and unknown weaknesses in server services to disable servers or take control of them. An application layer filtering firewall can examine the application layer commands and data. Then, the firewall can determine whether the content or commands being sent to a server on the corporate network are or are not valid connection attempts.

## Recommendation

- If you are running ISA Server at your gateway, or within your organization, add an extra layer of SMTP filtering.

## Resource

- For more information about deploying application filtering with ISA Server, see Chapter 2 of *Introducing the ISA Server 2000 Application Layer Filtering Kit* (<http://isaserver.org/articles/spamalfkit.html>).

### Note

Web addresses can change, so you might be unable to connect to the Web site mentioned here.

---

# Use Restricted Distribution Groups

As mentioned previously, many strategies for blocking spam also help in slowing or stopping the spread of viruses. Another effective deterrent against spam is to use restricted distribution groups in your Exchange organization. A restricted distribution group allows only authenticated users to send messages. This restriction is especially important because, if spammers know the alias of a distribution group, they can reach many of your employees with a single e-mail message. Restricting distribution groups is especially effective for large lists that contain many nested distribution groups.

### Note

Be aware that many spammers use dictionary attacks as a mechanism to reach recipients. A dictionary attack uses software that opens a connection to the target mail server and then rapidly submits millions of random e-mail addresses. This technique is effective because distribution groups are frequently represented by an alias that is a common word.

### **To set a distribution group as restricted**

1. In **Active Directory Users and Computers**, open the property page of the distribution group.
2. Click the **Exchange General** tab, and then select the **From authenticated users only** check box.

#### **Resource**

- For more information about restricting submissions to distribution lists, see "Securing Your Exchange Server" in the *Exchange Server 2003 Transport and Routing Guide* (<http://go.microsoft.com/fwlink/?linkid=26041>).

# What to Do When a Virus Attack Occurs

Following the recommendations in this document will help you to reduce the attack surface available to authors of malicious code. Unfortunately, even with precautions, your organization may still become the victim of a virus attack transmitted through e-mail.

This section provides more detailed information about what you can do when a virus is in your organization. The two main actions you need to take are the following:

1. Use the "On with no exceptions" mode functionality of Windows Firewall.
2. Clean the Exchange environment.

**Note**

If you implement the recommendations in the Recommended Actions and Configurations section in this document, it is unlikely that a virus transmitted by e-mail will be robust enough to require shutting down mail services. However, in the event of such a virus, you may have to shut down mail flow to and from the Internet until the threat is contained.

---

## Understanding the "On with no exceptions" Mode Functionality of Windows Firewall

As mentioned previously, Windows XP SP2 includes an update to Windows Firewall. In addition to the features mentioned previously, Windows Firewall includes an "On with no exceptions" operational mode where all excepted ports are locked down. An excepted port is a static port that is allowed to accept anonymous connections from the network during typical operation. In this mode, excepted ports are closed in addition to the generally closed ports in Windows Firewall. If a virus is running in your organization and it requires one of the excepted ports to communicate, running Windows Firewall in the "On with no exceptions" mode will impair its effectiveness. Like the other features of Windows Firewall in Windows XP SP2, the "On with no exceptions" mode can also be toggled through Group Policy.

**Recommendations**

- Review the documentation in the Resource section about how to specify and deploy the Windows Firewall "On with no exceptions" mode through Group Policy.
- Deploy third-party products with similar lock-down functionality if you are not using Windows Firewall.

**Resource**

- For more information about using Group Policy objects to deploy Windows Firewall in your enterprise, see *Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2* (<http://go.microsoft.com/fwlink/?LinkId=28380>).

# Cleaning the Exchange Environment

Review and understand the recommendations in this section before a virus attack occurs. If an outbreak occurs, implement these recommendations as appropriate, according to the level of infection within your system.

## **Important**

Although this section discusses shutting off mail flow, shutting off mail flow every time there is an e-mail transmitted virus is not recommended, especially if such an outbreak occurs during peak mail usage, and the level of disruption caused by the virus does not warrant such a severe response. However, there may be virus outbreaks that are so disruptive that they may warrant shutting off mail flow. This section is written for such an outbreak.

The approach given here assumes a widespread infection like that found in a "Melissa" or "ILOVEYOU" type of outbreak. Your objectives in responding to such an outbreak are to shut off mail flow to and from the Internet, clean and isolate servers, run antivirus software updates, and then reestablish mail flow. To achieve these objectives, follow these steps:

1. Stop Internet mail flow on gateway servers.
  - a. Clean mail queues.
  - b. Disinfect servers.
2. Stop internal mail flow.
3. Isolate and clean infected mailbox servers.
  - a. Disable user access to mailboxes.
  - b. Clean SMTP and MTA queues.
  - c. Clean mailboxes.
  - d. Disinfect servers.
4. Apply antivirus software updates.
  - a. Apply the most recent antivirus definitions to all antivirus products (for example, at file-level, AVAPI, gateways, and mailbox servers).
  - b. Run antivirus tools to verify that the computers are clean.
5. Clean user workstations and update antivirus software definitions.
6. Reestablish user access to mailboxes.
7. Reestablish Internet mail flow connectivity.

The following sections describe these steps in more detail.

---

## Stopping Internet Mail Flow

In some outbreaks, the most effective way to slow viruses both in your organization and to the Internet beyond is to stop all mail flow to and from the Internet.

The recommended method for stopping mail flow to the Internet is to disable the SMTP connections that connect your organization to the Internet. You can do this by setting the connection time on the connectors to **Never run**.

## To stop the mail flow on a connector

1. In **Exchange System Manager**, right-click the connector where you want to disable mail flow, and then click **Properties**.
2. On the **Delivery Options** tab, select **Never run** from the **Connection time** menu, and then click **Apply**. Perform this procedure on each connector to the Internet.

---

## Consolidate Internet-facing Exchange Servers

For maximum efficiency and easier isolation during a virus outbreak, you might consider grouping all Internet-facing Exchange servers into a single routing group. If there is an Internet virus outbreak, this routing group can be disconnected from the rest of the organization, allowing for cleanup to occur without affecting internal mail traffic. In the context of controlling virus outbreaks, this type of routing group organization is much easier to lock down than a model where each routing group has an Internet mail connector (IMC) bridgehead. In the latter case, the IMC passes traffic directly to other servers in the routing group. If an infected message arrives from the Internet with recipients destined to multiple mailbox servers on it, the multiple servers are infected immediately.

If you use a dedicated routing group for all Internet mail connections, all mail flows through the connector to the next hop. You can stop that mail flow by stopping the connector, thus allowing you to clean both the internal routing groups and the Internet-facing routing group in isolation.

This approach also gives you the flexibility to optionally allow Internet mail to flow inbound into the Internet-facing routing group and queue until mail service is restored. However, if the Internet routing group is severely infected, you might clean up the internal routing groups first, and then create a temporary outbound routing group to allow mail to flow through the alternate connection.

---

## Stopping Internal Mail Flow

The same procedure for stopping Internet mail flow applies to stopping internal mail flow. Set the **Connection time** on the **Delivery Options** tab of the connector to **Never run**.

Although the procedure itself is straightforward, you must give careful thought to the order in which you stop mail flow. Presumably, you will be stopping the mail flow to clean and disinfect the Exchange computers. It is critical that you develop an order of operations for taking the servers offline, cleaning and disinfecting them, and bringing them back online in such a way that isolates them from the risk of being reinfected. This plan is dependant on the topology of your Exchange routing groups and mail flow through other connectors, such as x400 and SMTP connectors.

---

## Isolate and Clean Infected Servers

When internal Exchange servers are infected, you can take the following steps to remove the infection:

1. Disable user access to Exchange.
2. Clean the messaging infrastructure:
  - a. Freeze and unfreeze the queue.
  - b. Find and delete infected messages.

## Disabling User Access to Exchange

In some outbreaks, it may become necessary to prevent users from using Exchange while the server is disinfected. Preventing user access helps to make sure that the server stays disinfected while the virus is removed from your organization. It is likely that, as part of the mailbox cleaning, you will need to run a disinfecting tool against the Exchange store. Therefore, you must keep the store mounted and running. The recommended method for disabling user access to the Exchange computer is to disconnect the physical connection to the network by unplugging the Ethernet cable.

---

## Cleaning the Messaging Infrastructure

After you have identified the message or messages that contain viruses, you must clean, or disinfect, your messaging infrastructure. Cleaning the messaging infrastructure involves cleaning the queues, cleaning the mailboxes, and then disinfecting the servers.

---

### Cleaning the Queues

The first step in cleaning the messaging infrastructure is to clean the queues. For each server, this task involves freezing the queue, finding the offending messages, and deleting them.

#### Freeze and Unfreeze the Entire Queue

When you freeze (stop) an entire queue, all messages that are currently in the queue will not be delivered. Frozen queues can continue to accept messages, but the messages will not be delivered until the queue is unfrozen (restarted). The messages inside a frozen queue will not be in a frozen state themselves.

#### To stop or restart the transfer of all messages in a queue

1. In Exchange System Manager, navigate to Queue Viewer by doing one of the following:
  - If you do not have routing or administrative groups defined, expand **Servers**, expand the server you want, and then click **Queues**.
  - If you do not have routing groups defined, expand **Administrative Groups**, expand **Administrative Group Name**, expand **Servers**, expand the server you want, and then click **Queues**.
2. Click to select the queue that you want to stop or restart.

**Note**

X.400 queues cannot be frozen.

3. Right-click the queue, and then point to one of the following options:
  - **Freeze Messages** Messages will be trapped inside the queue. No delivery will occur until the messages are unfrozen. For example, if one or more large messages have temporarily blocked the queue, you can freeze the large messages to allow Exchange to transfer the other messages. Then, with more resources available, Exchange will be able to send the larger messages.
  - **Unfreeze Messages** Remove the temporary hold on the transfer of messages.

#### Finding and Deleting Messages

The Find Messages button in Queue Viewer helps you to search for messages by specifying search criteria, such as the sender or recipient and the message state (such as frozen). You can also specify the number of messages you want your search to return.

## To find and delete specific messages in the SMTP queue

1. In **Exchange System Manager**, navigate to Queue Viewer by doing one of the following:
  - If you do not have routing or administrative groups defined, expand **Servers**, expand the server you want, and then click **Queues**.
  - If you do not have routing groups defined, expand **Administrative Groups**, expand *Administrative Group Name*, expand **Servers**, expand the server you want, and then click **Queues**.
2. Click **Disable Outbound Mail** to stop the outbound flow of messages from this computer.
3. In the details pane, click the queue where you want to search for messages. You must run this procedure on all queues.
4. Click **Find Messages**.
5. Select the search criteria you want, and then click **Find**.

### Note

The message field that is most likely to identify the virus is **Subject**. Because there is no mechanism to search on the subject, you must set the field **Number of messages to be listed in the search** to its maximum value, and then set the field **Show messages whose state is** to **All messages**. These settings will return all messages (up to 10,000) in the queue. You can now sort the messages by the subject by clicking **Subject** in the **Search Results** section of the dialog box.

6. Select the messages you want to delete, right-click, and then click **Delete (no NDR)**.  
This will delete the messages from the queue without notifying the sender. The message will not be delivered.

---

## Cleaning Mailboxes

After you delete the virus messages from the queues, you must disinfect the mailboxes. The best way to perform this task is with a third-party antivirus solution. For information about antivirus products that work with Exchange 2003, see the "Exchange Partners: Antivirus" Web site (<http://go.microsoft.com/fwlink/?LinkId=16226>).

If your antivirus software does not include the functionality for deleting messages from the Exchange store, you must run the Mailbox Merge Wizard (ExMerge.exe) to delete the offending messages. For more information about deleting virus messages from Exchange by using ExMerge.exe, see the Microsoft Knowledge Base article 328202, "HOW TO: Remove a Virus-Infected Message from Mailboxes by Using the ExMerge.exe Tool" (<http://go.microsoft.com/fwlink/?linkid=3052&kbid=328202>).

---

## Disinfecting Servers

After you delete the messages containing viruses from your Exchange servers, and before you bring the servers back online, you must disinfect the servers. In this context, disinfecting the servers implies a file-level scan to make sure the server itself is not infected with the virus. You can do this manually by following the instructions that are available on any number of virus-related Web sites for the given virus, or by running file-level antivirus software on the Exchange computer and updating the virus signature.

## Apply Antivirus Software Updates

As soon as your antivirus vendor releases an updated definition file that protects against further infection, deploy the update. Make sure that you deploy the definition update to the following layers:

- Message gateway servers
- Exchange servers
- Client workstations

---

## Clean User Workstations

Depending on the type of infection, client workstations may have also been targeted. If this is the case, follow the recommendations of your antivirus vendor to remove the infection. Most antivirus vendors now provide detection and removal tools to isolate and clean infected files. Also, be sure that you deploy the latest antivirus definition file that is applicable to your antivirus software.

---

## Reestablish User Access to Mailboxes

When your environment is free from infection, you can reestablish user access to their mailboxes. You can do this by reconnecting the Exchange server to your network.

---

## Reestablish Mail Flow Connectivity

When your environment is free from infection, you can reestablish mail flow connectivity in your internal network and to the Internet. Use the following procedure to reestablish mail flow.

### To reestablish the mail flow on a connector

1. In **Exchange System Manager**, right-click the connector on which you want to disable mail flow, and then click **Properties**.
2. On the **Delivery Options** tab, select **Always** (or the applicable time frame) from the **Connection time** menu, and then click **Apply**.

Perform this procedure on each connector that was previously set to **Never**.

# Accessibility

For information about accessibility for people with disabilities, see the "Microsoft Accessibility" Web site (<http://go.microsoft.com/fwlink/?LinkId=22008>).



**Does this article help you?** Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this article?

Mail feedback to <mailto:exchdocs@microsoft.com>.

For the latest information about Exchange, see the following Web sites:

- "Exchange 2003 Technical Documentation Library"  
<http://go.microsoft.com/fwlink/?LinkId=21277>
- "Downloads for Exchange 2003"  
<http://go.microsoft.com/fwlink/?LinkId=21030>
- "Welcome to the Exchange Server Community"  
<http://go.microsoft.com/fwlink/?linkid=14927>
- "Exchange 2000 and 2003 - All Technical Articles and Books / Updated"  
<http://go.microsoft.com/fwlink/?LinkId=10687>