realtimepublishers.com®

The Administrator Shortcut Guide™ To

Email Protection

Sybari
Software, Inc.

Paul Robichaux

Copyright Statement

Chapter 3: Server-Side Antivirus Protection

Recent outbreaks of viruses, worms, and blended threats provide evidence that there is much more to virus protection than installing antivirus software on a client computer and hoping for the best. Some of the more notable *blended threats* such as Nimda, the Code Red worm, BugBear, SoBig, and Blaster have caught many network administrators by surprise. Blended threats are threats that combine characteristics of viruses, worms, and Trojan horses in one nasty package.

In most organizations, virus protection is not a single action that administrators perform but rather a combination of procedures and protection. Security experts call this layering *defense in depth*—the point is to harden your systems by putting up multiple barriers. The first two chapters of this guide discussed the basics of viruses and worms and the basics of protecting Microsoft clients against email-based threats. This chapter builds on the knowledge you have gained from the previous three chapters and focuses on protection of the Exchange server.

Protecting your Exchange servers from viruses, worms, Trojan horses, and blended threats is not simply a process of picking any virus protection software and assuming you are protected. Servers must be properly patched, Exchange must be properly configured, and the software that you pick for your Exchange servers must be able to accurately detect viruses and protect against malicious attachments.

Basics for Protecting Your Organization

Regardless of which virus protection mechanism you choose for your organization, true protection involves much more than simply picking the right antivirus software. Protection measures need to include properly configuring the Exchange server, protecting the network with a firewall, using more than a single virus protection system, keeping software updated, and blocking specific files.

> Many of the recommendations in this section will affect the functionality of your messaging system; thus, you should thoroughly discuss potential changes within the IT department and properly publish them to the user community.

Properly Configuring the Firewall

Protecting your network against hostile email content is not often associated with proper firewall configuration. However, there are several firewall configuration measures you can take in order to better protect your organization against viruses and other hostile mail content. The following list highlights suggestions for firewall implementation and configuration:

- Only servers that absolutely *must* be exposed to the Internet should be, such as servers that accept inbound SMTP mail or that provide access to Internet protocols (HTTP, POP3, or IMAP4). If your firewall allows reverse proxying of ports, use that option instead of directly opening each port. Open only the ports that are necessary.

- Require SSL for inbound IMAP, POP, and OWA connections. Doing so will cause some users to complain, but if you don't, your users' credentials may be transmitted in plain text, visible to any attacker. Properly and thoroughly documenting the setup and use of SSL and properly notifying users before SSL is required can help to mitigate some of these complaints.
- Outbound SMTP mail should only be accepted from authorized servers, such as the Exchange servers that host an SMTP Connector or your SMTP content/virus inspection gateway. This configuration will prevent viruses such as SoBig that run their own SMTP engines from sending viruses to users outside of your organization.
- Outbound POP3 and IMAP4 requests to ISP servers outside of your organization should be restricted. Doing so will prevent users from retrieving mail to their desktops from other mail services. This restriction might be an annoyance for some users; you can recommend that they use Web mail clients to these ISPs.
- Direct, inbound RPC requests from the Internet should be blocked for MAPI clients; if a remote MAPI client wants to use Outlook as a MAPI client remotely, they should connect to your organization via a VPN, Microsoft's Internet Security and Acceleration (ISA) Server, or Exchange 2003's RPC-over-HTTP feature. In years past, some organizations chose to open RPCs directly to their Exchange servers; doing so is not a good practice because of the vulnerabilities in various implementations of RPC.
- Exchange front-end servers that reside in a perimeter or DMZ network should be restricted to only the connectivity on the internal network necessary. Be careful to open only the minimum set of ports. Better yet, move the front-end servers to the internal network so that you do not have to open as many ports between the DMZ and the internal network. The most secure method is to configure a solution that allows front-end servers to be accessible only via a reverse proxy.
- If your firewall software has plug-ins available that will perform virus or content inspection on inbound HTTP, SMTP, or other traffic, you should consider using these as an additional layer of defense.

Beware of Cisco's PIX MailGuard, which doesn't work all that well with Exchange. For more information, see the Microsoft article "XCON: Cannot Send or Receive E-mail Messages Behind a Cisco PIX Firewall."

Avoid Directly Publishing Exchange Server Resources

Though this topic might seem more inline with a good security strategy overall than for virus and worm protection, avoiding directly publishing Exchange Server resources is still relevant. The Nimda and Code Red worms managed to spread by connecting to unpatched NT and Win2K servers running IIS. In many organizations, this server was sitting in the DMZ. In cases with worms such as the Blaster worm, a single workstation or server could become infected on the internal network; in a many cases, such occurred because someone plugged in an infected notebook to an internal network. Once these servers were infected, these worms gained access to the internal network and began to spread to the servers and the desktop computers on the internal network. Once one computer on the internal network is infected, you will see almost an exponential infection rate internally!

You can allow your remote users to use Exchange features such as OWA, POP3, or IMAP4 from the Internet without ever directly accessing a Windows IIS server. To do so, you employ some type of reverse proxy solution, which is the type of solution that Microsoft recommends as the most secure method of publishing OWA for Internet users.

Reverse proxy technology acts in the opposite way that a regular proxy server behaves. A regular proxy server (forward proxy) receives requests from a client (usually HTTP), then forwards those request on to the destination server. A reverse proxy examines inbound IP requests (HTTP, POP3, IMAP4, and so on), often performs some type of content inspection or URL inspection on the request, repackages the request, and directs it on to the intended Web server. The only host that has direct access to the back-end servers is the reverse proxy server.

The most secure method of implementing a reverse proxy solution is to put all of your Exchange servers (front-end and back-end) on the internal network and to put the reverse proxy solution in the perimeter network. Figure 3.1 shows an example implementation of a reverse proxy solution for OWA clients.

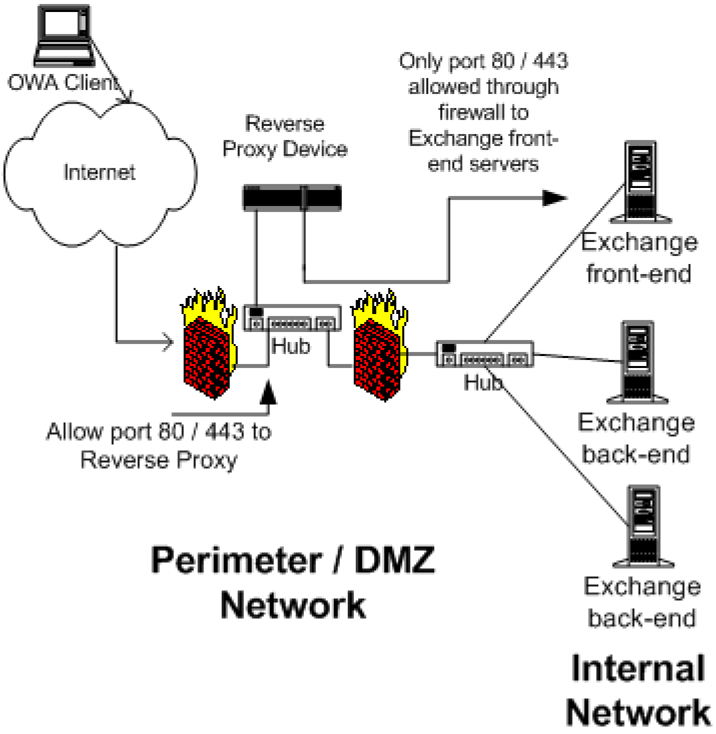


Figure 3.1: Example OWA solution using a reverse proxy device.

Employing a Multi-Layered Virus Protection Strategy

No single antivirus scanning engine catches 100 percent of viruses. Occasionally, even the most accurate scanning engine allows a virus or worm to sneak by. Viruses can sneak in to your organizations from many different directions. For these reasons, I recommend that you implement a multi-tiered approach to scanning for viruses. In a multi-tiered approach, you implement at least one additional method of scanning on your network. I recommend the three-layer approach that Figure 3.2 illustrates.

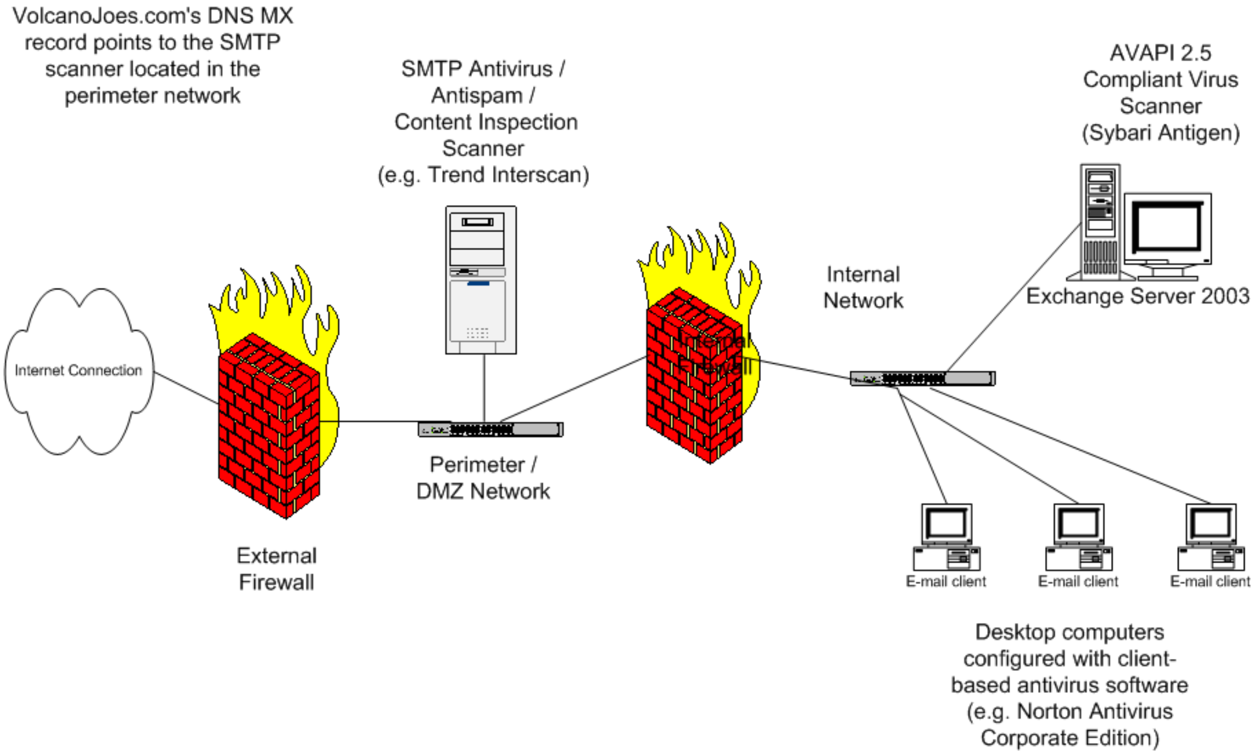

VolcanoJoes.com's DNS MX record points to the SMTP scanner located in the perimeter network
SMTP Antivirus / Antispam / Content Inspection Scanner (e.g. Trend Interscan)
AVAPI 2.5 Compliant Virus Scanner (Sybari Antigen)
Internal Network
Exchange Server 2003
Internet Connection
Internal Firewall
Perimeter / DMZ Network
External Firewall
E-mail client
E-mail client
E-mail client
Desktop computers configured with client-based antivirus software (e.g. Norton Antivirus Corporate Edition)

Figure 3.2: Multi-layer email virus scanning solution.

Figure 3.2's network has three *separate* antivirus systems at work, each from a different vendor and each using a different scanning engine and set of signatures. Inbound mail is delivered to an SMTP scanning system located in the DMZ; no inbound SMTP traffic ever goes directly to the Exchange server. The Exchange server runs a separate scanning engine specifically designed to scan the Exchange server information store. Finally, each desktop client on the network has client-based scanning software. This setup gives you better protection by ensuring that a single vendor's failure to update their signatures in time to catch a new threat won't leave your network entirely unsupported.

Differing Scanning Policies

You might want to consider implementing different scanning and attachment policies for email that arrives from the Internet as opposed to mail that is to be delivered internally. Implementing a multi-tier approach such as the one shown in Figure 3.2 allows you to do so.

For example, on the SMTP scanning system that handles mail that is arriving from the Internet, you could ban all types of attachments except for office automation applications (Word, Excel, PowerPoint, and so on). However, on the Exchange server, you could allow files that might be more dangerous, such as ZIP files, compiled Help (.CHM) files, and the like.

Some companies block ZIP attachments using the logic that the file might contain hostile content. Although this is certainly true, ZIP files remain a valid way to get other content into an organization and usually should not be blocked. Most virus scanning software has the ability to open and scan ZIP attachments anyway. A better policy towards ZIP files is to quarantine them when they cannot be scanned or if they contain an infected file.

Updating the Software

One of the common reasons that the most invasive worms have spread so quickly is that they have taken advantage of vulnerabilities in the Windows OS, IIS, or the Web browser. Keeping the OS and IIS up to date and properly patched is critical. One of the most important and difficult decisions that an administrator must make is which patches to apply and how quickly.

A couple of security fixes and updates are usually released each week for the various Windows platforms. The Nimda and Code Red worms exploited a weakness in IIS; unfortunately, a patch for this weakness had been released nearly 6 months before the authors of these worms unleashed their wrath on email users and administrators. The Blaster worm exploited a weakness in the entire NT family (NT, Win2K, Windows XP, and WS2K3) for which a patch had been offered a few weeks earlier.

So how do you make good decisions about deploying these updates? After all, most of these updates require reboots and, consequently, at least a few minutes of downtime for each server. Keep an eye on the patches that are released and the vulnerabilities that exist:

- Subscribe to Microsoft’s Security Notification service at http://www.microsoft.com/security.
- Regularly visit a third-party notification site such as Carnegie Mellon’s CERT Coordination Center at http://www.cert.org and the SANS Institute at http://www.sans.org.
- If a security threat makes it to national or local news, investigate it immediately. Major media organizations tend to publish sensationalistic, technically inaccurate reports, but sometimes these reports are the first notice you get of a new vulnerability.
- Check multiple sources for information—don’t depend on any single source for your news about vulnerabilities.

When you receive notification of new updates and fixes, evaluate each one to determine whether the update or fix applies to your environment. Fixes related to Windows Media Player or DirectX are non-critical for servers and can be deferred until the next scheduled reboot. Fixes relating to Internet Explorer (IE) can be deferred to your next scheduled downtime; after all, you should not be surfing the Internet from the console of your Exchange servers. Patches that enhance functionality can be deferred indefinitely.

However, fixes that affect IIS, core Windows functionality, or RPCs (including fixes that affect Exchange Server security problems) should be applied at the next available opportunity. Even if your next scheduled downtime is not for a couple of weeks, you should take the time to reboot each server after you’ve informed users that you’re going to do so—when users know about downtime, it is far less convenient than a virus outbreak that shuts out users from their email for hours!

☞ Don’t sacrifice reliability or security for better availability. An hour of unscheduled downtime is far more inconvenient than even several hours of scheduled downtime.

Applying Exchange Restrictions

Most experienced Exchange administrators are firm believers in placing as many limits and restrictions on the user community as possible. These limits should be as unobtrusive as possible and be implemented while keeping in mind that users must be able to continue to do their jobs.

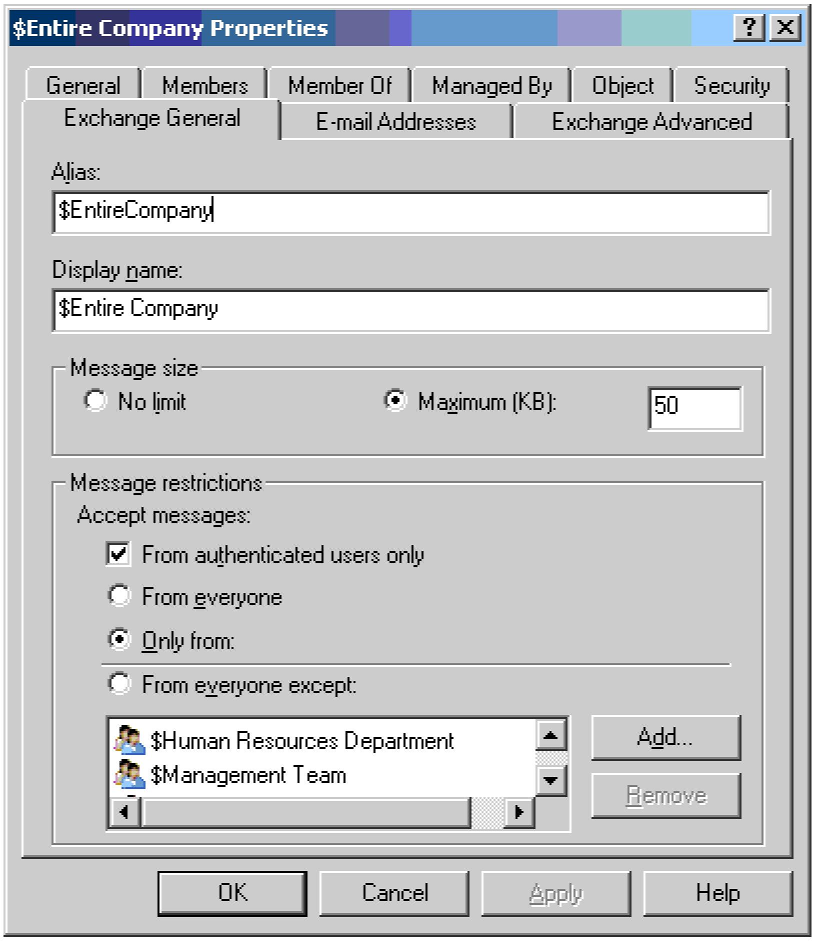
Dummy Entries Offer No Protection to Your Address Book

Tips and hints for protecting your organization from email replicating viruses have emerged since the first such virus hit in 1999. The Melissa virus sent itself to the first 50 entries in the Exchange Global Address List (GAL), so many administrators created 50 “dummy” mailboxes that would be sorted to top of the GAL. Later email-based viruses merely picked names at random or didn’t even use the GAL—worms such as SoBig, BugBear, Nimda, and Blaster don’t even need Exchange to replicate. These worms can scan emails in your Inbox, files on your hard drive, or local pages in your Web browser cache looking for email address to send messages to or from which to claim that the message was sent.

Another incorrect tip instructs users and administrators to put an entry into their address books that starts with !0000, 0000, AAAAAAA, or other sequences of letters, numbers, and characters. These tactics do not work against modern viruses, so don’t bother.

Protecting Mail-Enabled Groups

Mail-enabled groups (distribution lists) are the easiest way for a virus or worm to send itself to a large number of users with a single recipient. In Exchange 2000, Microsoft implemented a couple of features for protecting mail-enabled groups, and mail-enabled group protection was again extended in Exchange Server 2003. Figure 3.3 shows the Exchange general property page for a mail-enabled group in AD 2003 and Exchange 2003.



$Entire Company Properties

Alias: $EntireCompany

Display name: $Entire Company

Message size

○ No limit ● Maximum (KB): 50

Message restrictions

Accept messages:

☑ From authenticated users only

○ From everyone

● Only from:

○ From everyone except:

$Human Resources Department

$Management Team

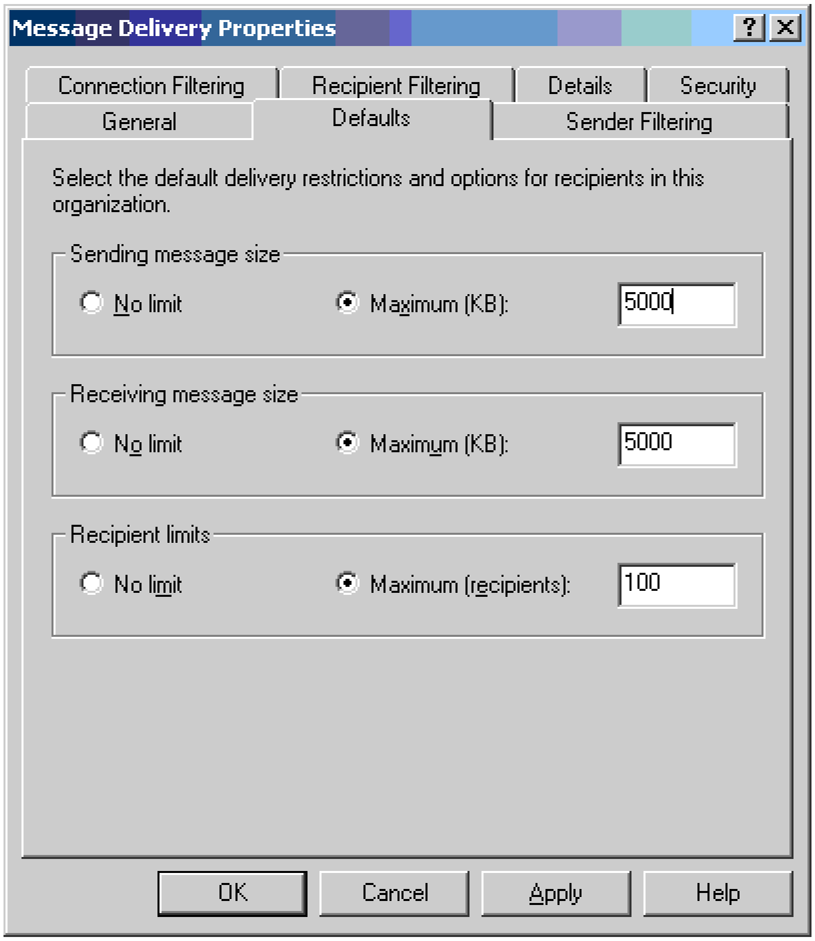
Figure 3.3: Exchange general properties for a mail-enabled group.

Some of the features of a mail-enabled group that can help prevent mail abuse or hostile content from spreading include:

- Configure the message size limit to prevent large messages from blasting your distribution lists. I advise setting this limit to a reasonably small amount, especially if the group membership is very large.
- Set a group's restrictions so that only authenticated users can send mail to the group (this option is available in Exchange 2003). Doing so will prevent an anonymous user from connecting to the server via SMTP and sending messages to a mail-enabled group.
- Restrict a group so that it will only accept messages from specific users or groups. Doing so is extremely useful for groups that have large memberships and company-wide groups.

Restricting Message Size and Recipient Count

Exchange 2000 and Exchange 2003 have another set of features that help reduce hostile email content from spreading too quickly and can help prevent users from abusing their email privileges—the Message Delivery Properties, which Figure 3.4 shows. You can find these settings in Exchange System Manager in the Global Settings container.



Select the default delivery restrictions and options for recipients in this organization.

Sending message size

○ No limit ● Maximum (KB): 5000

Receiving message size

○ No limit ● Maximum (KB): 5000

Recipient limits

○ No limit ● Maximum (recipients): 100

Figure 3.4: Global message delivery restrictions.

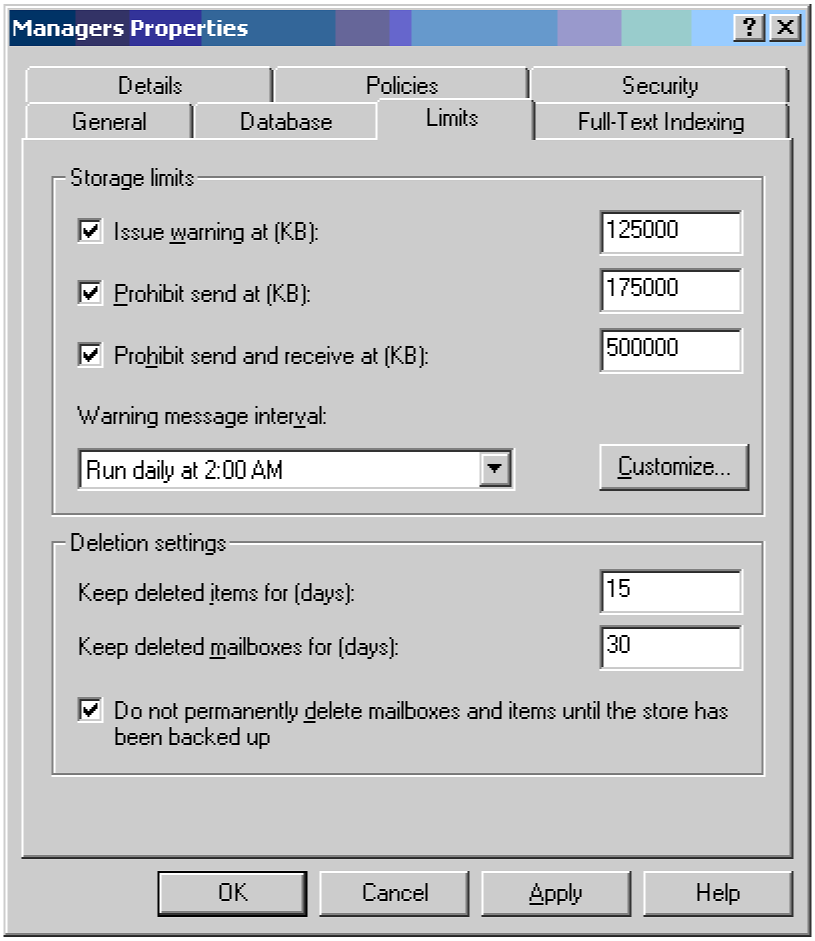
The restrictions that Figure 3.4 show allow the administrator to globally restrict the maximum incoming and outgoing message sizes as well as the maximum number of recipients per message. Each of these settings can be overridden on a user-by-user basis for VIPs or users that require larger messages or more recipients per message. The maximum number of recipients per messages is the maximum number of recipients in the To, Cc, and Bcc lines; the total number of recipients in a group is included in this count. If a restriction of 100 recipients per messages is enforced, then a virus or worm will not be able to send to a distribution list with 101 recipients. Of course, this offers no protection from worms that send to a single recipient at a time.

Limiting Mailbox Storage

Mailbox size does not necessarily relate directly to viruses spreading through an organization, but if your organization is hit by a worm or virus that is quickly spreading, it is possible that mailboxes may become extremely large. Excessive mailbox growth *will* lead to a server shutting down due to a lack of disk space.

To help thwart such attacks, place limits on all mailbox stores. When calculating these limits, be generous and allow users enough space to properly do their jobs. These limits should be published so that the users are aware of them. Even if you don't intend for your users to be subject to the limits, setting a 1GB per mailbox limit can help protect your server from running out of space during a virus outbreak. A Prohibit Send and Receive limit should take into consideration the maximum number of mailboxes on the mailbox store and the total amount of mail storage on the server.

Figure 3.5 shows the Limits tab of a mailbox store, which you can also set through Exchange Mailbox Store Policies.



Storage limits

☑ Issue warning at (KB): 125000

☑ Prohibit send at (KB): 175000

☑ Prohibit send and receive at (KB): 500000

Warning message interval: Run daily at 2:00 AM

Deletion settings

Keep deleted items for (days): 15

Keep deleted mailboxes for (days): 30

☑ Do not permanently delete mailboxes and items until the store has been backed up

Figure 3.5: Mailbox store storage restrictions.

Scanning and Blocking File Attachments

Develop a list of forbidden file attachment types for your organization that is published to your users. In the early days of email replicating viruses, IT departments were continually adjusting this list to include the seemingly ever-increasing list of possibly dangerous file types. Blocking some of these files is politically difficult, as many users need access to certain file types.

> ☞ Some server-based antivirus software gives you the choice of scanning all file attachments or only specific attachment types. Scan all files.

Which file types should be included in this forbidden list of attachment types? The answer is hotly debated. Table 3.1 contains the standard list of attachment types that I ask my clients to block at their perimeter network scanner or on their Exchange server. I think this list still allows maximum functionality while protecting against most threats.

Attachment Extension	**Description**
asp	Active Server Pages scripts
bat	DOS batch files
chm	Compiled HTML Help files
cmd	Windows Command scripts
com	DOS program files
eml	Embedded email files
exe	Executables
htm/html	HTML files
Js	JavaScript files
pif	DOS/Windows 3.1 Program Information Files
pl	Perl script files
reg	Windows registry script files
scr	Screen saver files
shs	Shell Scrap files
vb	Visual Basic files
vbs	Visual Basic Script files
wsc	Windows Script Component
wsh	Windows Script Host scripts

Table 3.1: Significant file attachment types that should be blocked.

> In Chapter 2, we explored the file types that Microsoft considers Level-1 attachments (which we also discussed in Chapter 2).

If your antivirus software offers the functionality, configure the software to automatically send a message to the sender of a message that includes a file attachment that is not allowed. Instruct the sender about how to get the attachment to the user.

The Exchange Antivirus API

With Exchange 5.5 SP2 and later, the only way to scan for a virus in the Exchange information store is to use MAPI programming calls. Essentially, Exchange-aware antivirus software had to log on to each mailbox, then wait for a MAPI notification that a new message had arrived. Once the messages arrived, the antivirus scanning software could then scan the message, assuming the software was not busy scanning other messages. If a virus was detected, the message was opened, the virus was removed, and the message was re-saved. However, because this process took place mailbox-by-mailbox, messages that were sent to 50 people had to be scanned 50 times. Organizations often suffered as a result of the shortcomings of this method.

Another limitation of MAPI-based scanning is that MAPI can only send 64 new mail notifications to the antivirus software at any one time. Thus, if a virus outbreak occurs and the server is receiving hundreds of messages in a short period of time, many messages will hit the mailbox and the antivirus software will not have a chance to scan the message before a quick user opens the message and spreads the virus.

Microsoft had a painful demonstration of the shortcomings of the MAPI-scanning approach with the outbreaks of viruses such as Melissa in 1999. The Exchange team developed an API that would allow third-party vendors to hook messages as they arrived and before they are placed in the user's mailbox. This API is known as the Antivirus API or AVAPI 1.0; you will also see AVAPI referred to as VAPI.

As usual, new products generate more feature requests. As vendors developed solutions using this API, customers and vendors realized the limitations of this first API. AVAPI 1.0 only allowed for scanning of the attachments in the message and not the message body itself; embedded viruses such as BubbleBoy could still slip through. In addition, the message had to be delivered to the information store; AVAPI had no method of inspecting the message in the SMTP or MTA queues.

In 2001, Microsoft released a new virus scanning API for use with Exchange 2000 SP1 and later called AVAPI 2.0. This version addressed many of the issues surrounding the capabilities of AVAPI 1.0-based products by allowing the scanner access to recipient information and the ability scan for embedded viruses. AVAPI 2.0 also allowed scanning of not only the EDB database file but also the STM database file.

With the release of Exchange 2003, Microsoft has published yet another antivirus API, AVAPI 2.5, which further extends the abilities of earlier versions. This version allows the scanning software to scan messages not only in the information store but also in the SMTP queues on SMTP bridgehead servers or SMTP front-end servers.

Learning More About the Exchange AVAPI

For more information about the Exchange AVAPI and virus scanning on Exchange servers, see the Microsoft articles "Overview of Exchange Server 2003 and Antivirus Software" and "XADM: Understanding Virus Scanning API 2.0 in Exchange 2000 Server SP1."

Designing a Server-Based Protection Scheme

All Exchange servers need an Exchange-aware antivirus software package installed and running. Exchange server-based antivirus scanning software used to be considered a luxury, but now it is essential for the security and reliability of your messaging system. Pricing varies from vendor to vendor and can depend on a variety of things such as the number of users, software subscription service (free updates), add-on packages such as anti-spam/junk mail scanning, and the number of scanning engines, if applicable. Retail pricing for Exchange AVAPI products range from less than $25US per seat to $35US per seat when purchasing 100 seats. You should include these estimated costs in any budget you put together for Exchange services. The following list highlights characteristics and features that you should consider when evaluating Exchange AVAPI software:

- Automatic updates of antivirus software
- Ability to configure blocked attachment list
- Customizable notifications
- Multiple scanning engines
- The ability to scan zip and other compressed files
- Anti-spam features or plug-in that enables anti-spam features
- Ability to kick off a manual scan of existing messages
- Quarantine where files that could not be scanned or viruses can be stored in case they need to be examined or released later
- Remote management of the software
- Manually initiated scans of the existing data in the mailbox stores
- For Exchange 2000, the product should support AVAPI 2.0, and for Exchange 2003, the product should support AVAPI 2.5
- Ability to handle encrypted and password-protected files
- Adequate notification of the appropriate people in your organization when viruses are detected
- Comprehensive reporting features
- Outbreak monitoring features—will the product proactively notify you if it detects a potential outbreak and do the configurable notification features run scripts?

Multiple Scanning Engines

No single antivirus scanning engine and set of signatures is 100 percent effective all the time. Some Exchange AVAPI-based scanners have the capability to use more than one scanning engine; Sybari's Antigen, for example, allows as many as five different scanning engines to be enabled. This functionality greatly increases the likelihood that all viruses will be detected and removed.

Exchange-Aware Antivirus Vendors

There are many Exchange-aware antivirus products available. To get a better idea of their strengths and weaknesses, search the Exchange Usenet newsgroups and mailing lists for discussions about virus protection and recommended products. The following list provides vendor names and Web sites of products that were designed for Exchange:

- Sybari at http://www.sybari.com
- FRISK Software at http://www.f-prot.com
- GeCAD Software at http://www.ravantivirus.com
- Kaspersky Lab at http://www.kaspersky.com
- McAfee Security at http://www.mcafeeb2b.com
- Norman Data Defense Systems at http://www.norman.com
- Panda Software at http://www.pandasoftware.com
- Softwin at http://www.bitdefender.com
- Symantec at http://www.symantec.com
- Trend Micro at http://www.trendmicro.com

File-Based Virus Scanners

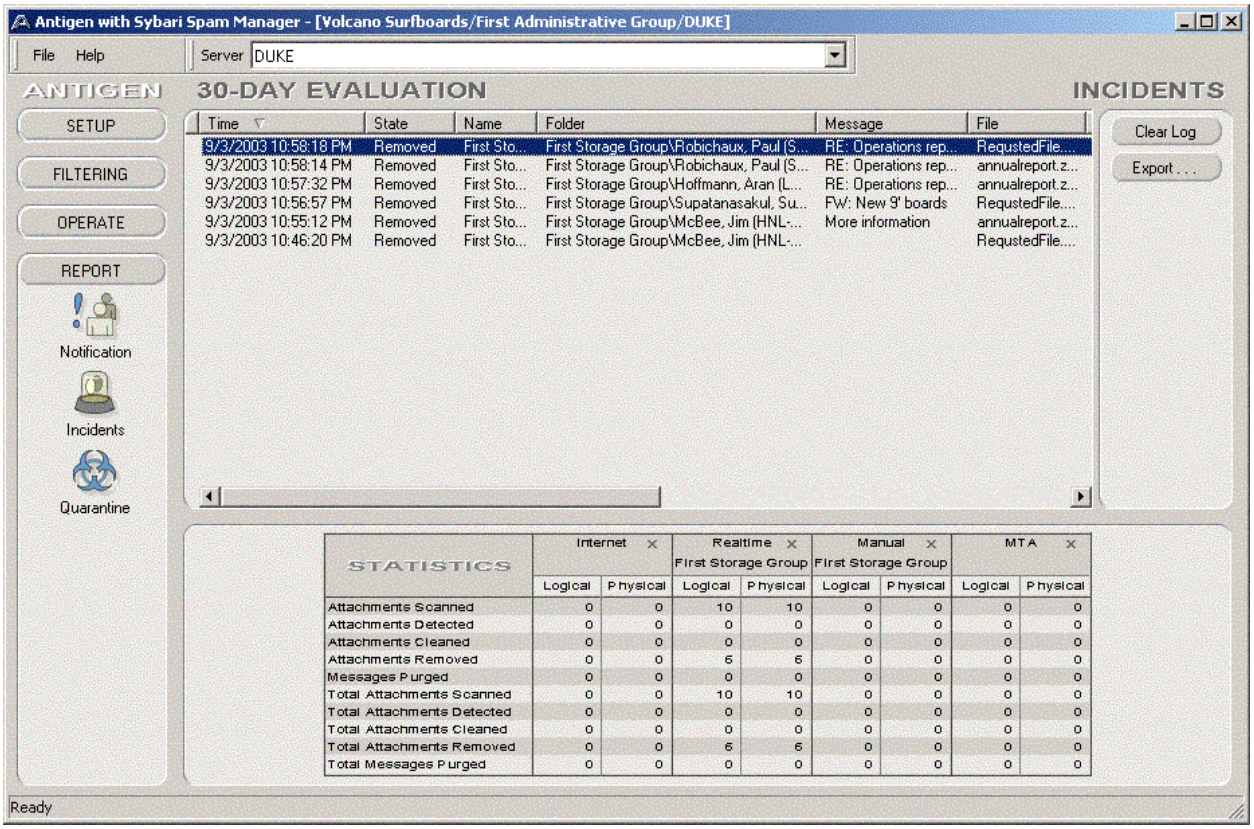
Many administrators implement a file-based antivirus scanning system on their Exchange servers. If you choose to do so, keep the following considerations in mind:

- The file-based scanner *must* be excluded from scanning any directories that contain Exchange data and transaction logs, including the following directories
  - \exchsrvr\mtadata
  - \exchsrvr\mdbdata
  - \exchsrvr\*ServerName*.log (message tracking log files)
  - \exchsrvr\mailroot
  - \exchsrvr\imcdata
  - \exchsrvr\srsdata
  - Wherever your SMTP (and X.400 MTA) queues are located
- If the Exchange Installable File System (ExIFS) drive (the M drive) is enabled, the file-based virus scanner must *never* scan this drive.
- File-based virus scanners are not a substitute for an Exchange AVAPI-based scanner.
- Test the interaction of the two A/V scanners before you put them into production.
- Be prepared to disable the file scanner if you are performing an upgrade, disaster recovery, or database maintenance operation.
- Don't be surprised if Microsoft Product Support Services asks you to completely remove the product (not just disable it) if you are having problems.

Monitoring Exchange Server Virus Protection

Most Exchange server antivirus products have reporting features that allow you to run reports on the number of viruses received, blocked attachments, and quarantined messages. I recommend running these reports between weekly and monthly intervals and keeping a record of past reports. These reports are useful and provide management with proof that the antivirus software is of value to the organization.

Most vendors provide canned reports and easy-to-read screens that give you the most recent virus statistics at a glance. Figure 3.6 shows the Sybari Antigen product's Incidents screen that details the most recent viruses detected and where they were detected. As with most products, this screen can be exported.



Server: DUKE

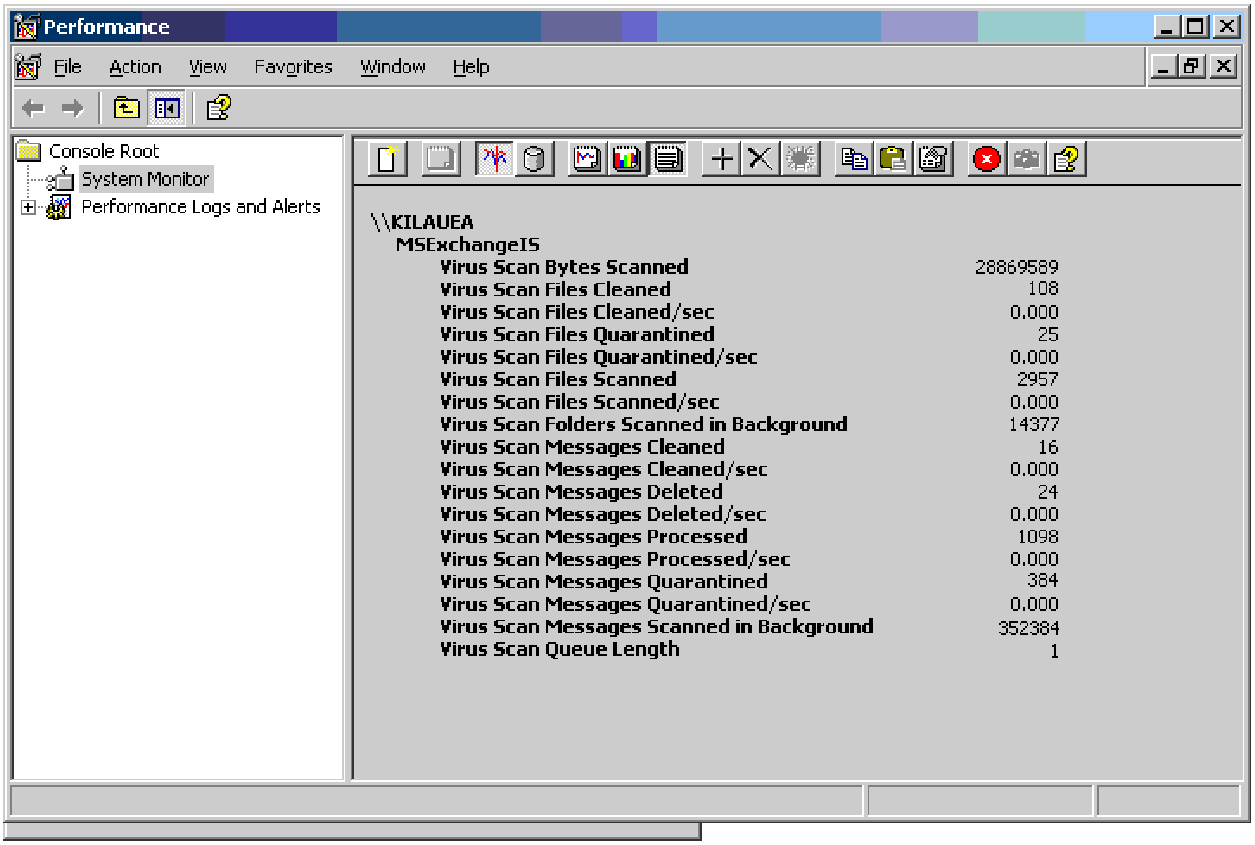
Time	State	Name	Folder	Message	File
9/3/2003 10:58:18 PM	Removed	First Sto...	First Storage Group\Robichaux, Paul (S...	RE: Operations rep...	RequstedFile....
9/3/2003 10:58:14 PM	Removed	First Sto...	First Storage Group\Robichaux, Paul (S...	RE: Operations rep...	annualreport.z...
9/3/2003 10:57:32 PM	Removed	First Sto...	First Storage Group\Hoffmann, Aran (L...	RE: Operations rep...	annualreport.z...
9/3/2003 10:56:57 PM	Removed	First Sto...	First Storage Group\Supatanasakul, Su...	FW: New 9' boards	RequstedFile....
9/3/2003 10:55:12 PM	Removed	First Sto...	First Storage Group\McBee, Jim (HNL-...	More information	annualreport.z...
9/3/2003 10:46:20 PM	Removed	First Sto...	First Storage Group\McBee, Jim (HNL-...		RequstedFile....

STATISTICS	Internet		Realtime First Storage Group		Manual First Storage Group		MTA	
	Logical	Physical	Logical	Physical	Logical	Physical	Logical	Physical
Attachments Scanned	0	0	10	10	0	0	0	0
Attachments Detected	0	0	0	0	0	0	0	0
Attachments Cleaned	0	0	0	0	0	0	0	0
Attachments Removed	0	0	6	6	0	0	0	0
Messages Purged	0	0	0	0	0	0	0	0
Total Attachments Scanned	0	0	10	10	0	0	0	0
Total Attachments Detected	0	0	0	0	0	0	0	0
Total Attachments Cleaned	0	0	0	0	0	0	0	0
Total Attachments Removed	0	0	6	6	0	0	0	0
Total Messages Purged	0	0	0	0	0	0	0	0

Figure 3.6: The incidents report screen from Antigen.

Monitoring Windows Performance Counters

The Exchange AVAPI also includes additional performance monitor counters that are most useful when put into System Monitor's report view, as Figure 3.7 shows. This type of report is useful to provide evidence to management that although viruses aren't reaching users, viruses are still arriving in the mail system. These counters reset each time the store is stopped and restarted.


Performance
File Action View Favorites Window Help
Console Root
System Monitor
Performance Logs and Alerts

```
\\KILAUEA
  MSExchangeIS
      Virus Scan Bytes Scanned                            28869589
      Virus Scan Files Cleaned                                 108
      Virus Scan Files Cleaned/sec                           0.000
      Virus Scan Files Quarantined                              25
      Virus Scan Files Quarantined/sec                       0.000
      Virus Scan Files Scanned                                2957
      Virus Scan Files Scanned/sec                           0.000
      Virus Scan Folders Scanned in Background               14377
      Virus Scan Messages Cleaned                               16
      Virus Scan Messages Cleaned/sec                        0.000
      Virus Scan Messages Deleted                               24
      Virus Scan Messages Deleted/sec                        0.000
      Virus Scan Messages Processed                           1098
      Virus Scan Messages Processed/sec                      0.000
      Virus Scan Messages Quarantined                          384
      Virus Scan Messages Quarantined/sec                    0.000
      Virus Scan Messages Scanned in Background             352384
      Virus Scan Queue Length                                    1
```

Figure 3.7: AVAPI performance monitor statistics.

Most of the statistics you can track from System Monitor are reasonably self-explanatory. Table 3.2 provides descriptions of these statistics; all of these counters are found under the MSExchangeIS object.

Counter	Description
Bytes Scanned	Total size of all messages and attachments that the AVAPI has scanned for viruses
Files Cleaned	Total number of file attachments that had viruses but were successfully cleaned and released to the intended recipient
Files Cleaned/sec	Current scanning activity for file attachments
Files Quarantined	Total number of file attachments moved to quarantine
Files Quarantined/sec	Number of file attachments quarantined per second
Files Scanned	Total number of file attachments scanned
Files Scanned/sec	Number of file attachments scanned per second
Folders Scanned in Background	Total number of folders scanned during a background or scheduled antivirus scan
Messages Cleaned	Total number of messages that have been cleaned
Messages Cleaned/sec	Number of messages cleaned per second
Messages Deleted	Total number of messages deleted as the result of a rule such as a forbidden attachment rule (Exchange 2003 only)
Messages Deleted/sec	Number of messages deleted per second (Exchange 2003 only)
Messages Processed	Total number of messages that have been processed
Messages Processed/sec	Number of messages processed per second
Messages Quarantined	Total number of message that have been put in quarantine
Messages Quarantined/sec	Number of messages that are put in to the quarantine per second
Messages Scanned in Background	Number of messages scanned during a background scan of the information store; these scans can be kicked off manually or on a schedule
Queue Length	Current number of messages waiting to be scanned; if the queue always has more than one or two messages waiting, you have performance problems on your server

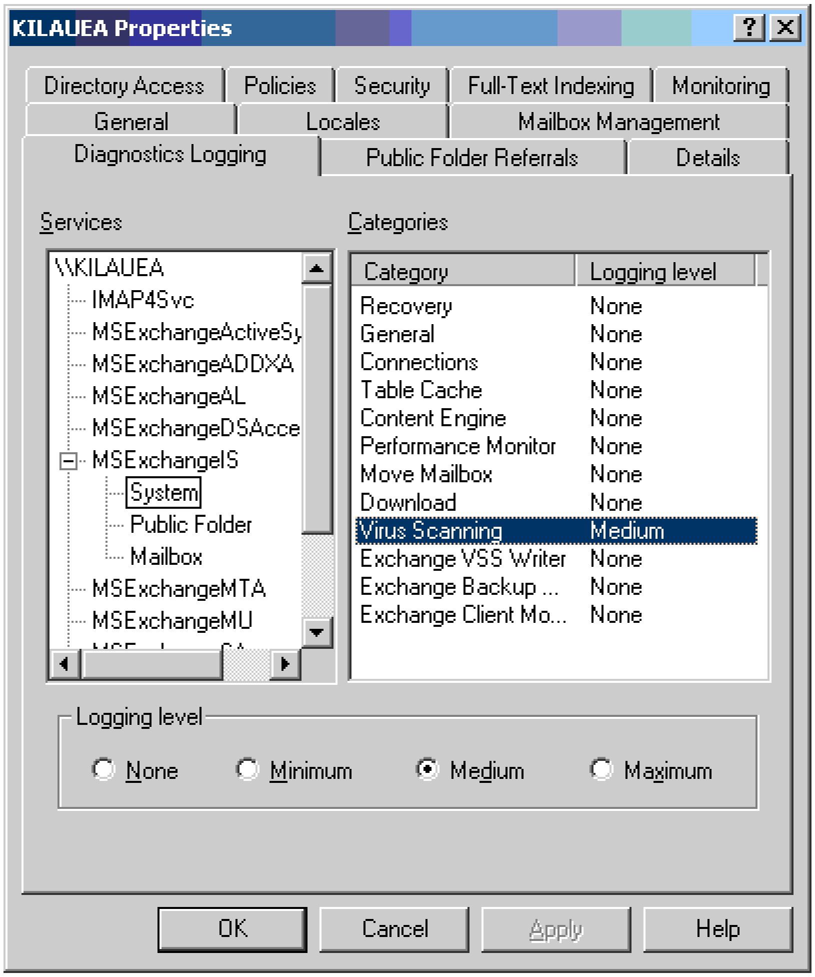
Table 3.2: AVAPI System Monitor counters.

☞ If you want to be notified of a potential outbreak of a known virus, you could set a threshold of viruses detected per second by using the Performance Logs and Alerts console and the Messages Cleaned/sec or Messages Quarantined/sec counters.

Examining the Windows Application Event Log

The Exchange AVAPI provides useful diagnostics logging capabilities for virus scanning and detection operations. The information you will receive from the event logs might not be as comprehensive as the information you will be able to access directly from the antivirus software’s reporting tools, but the information in the Application event log is available to any event log monitoring tools.

To enable this logging level, you must turn on the Virus Scanning diagnostic logging for each Exchange Server. Figure 3.8 shows the Diagnostics Logging property page for an Exchange Server 2003 system called KILAUEA. Locate the Virus Scanning category under MSExchangeIS, System, and set the value to a medium logging level.



Category	Logging level
Recovery	None
General	None
Connections	None
Table Cache	None
Content Engine	None
Performance Monitor	None
Move Mailbox	None
Download	None
Virus Scanning	Medium
Exchange VSS Writer	None
Exchange Backup ...	None
Exchange Client Mo...	None

Logging level

○ None ○ Minimum ● Medium ○ Maximum

Figure 3.8: Enabling Virus Scanning diagnostics logging.

Once diagnostics logging is enabled, you will see events in the Application event log that report on virus detection. Table 3.3 shows some of the more common events you may see for AVAPI 2.0 and later scanning software. All of these events are from the source MSExchangeIS and category Virus Scanning; however, some of the events in this table will only be available if you set the logging level to maximum. Not all AVAPI antivirus software packages will generate all of these error messages.

Event ID	Severity	Explanation
9572	Warning	A virus has been discovered. Message was cleaned successfully. Details can be found in the event description.
9565 and 9566	Error	An error occurred during the initialization of the virus scanner due to an invalid configuration parameter. Review the event details for more information.
9568	Error	An error occurred in one of the virus scanning components. Review the event details for more information.
9569 and 9570	Error	An error occurred when scanning a message. This error could be the result of the message being corrupted or it could be a problem with the virus scanning software. Confirm that you have the latest scanning engine and updates. This error might also result from the configuration of the antivirus software.
9571	Error	An error occurred while scanning a message and the scanning software is unloading. This error is fairly serious. Confirm software and scanning engine updates. Consult the event details for more information.
9573	Warning	A virus has been discovered. The message could not be cleaned so the message was quarantined. Details can be found in the event description.
9574	Informational	AVAPI virus scanning software has been loaded.
9575	Informational	AVAPI virus scanning software has been stopped.
9575	Informational	AVAPI virus scanning software has been restarted.
9578	Informational	Scanning software is starting a background or scheduled task to scan the database specified in the event details.
9580	Informational	If diagnostics logging is turned off, you will see this message when the scanning software is started. This message simply tells you that the scanning software has started but that you will see no additional diagnostics logging information.
9581	Error	Virus scanner failed to start during initialization routine, see event description for more information.

Table 3.3: Events generated in the Application event log by AVAPI-aware antivirus products.

Errors indicating that the antivirus software is not working properly or failing to scan messages can be serious; especially if the scanning engine has stopped altogether, which means that a virus could sneak through. If you are seeing these problems, try the following:

- Restart the antivirus software
- Update the scanning engine
- Update the antivirus signatures
- Reboot the server
- Determine whether the problem is with one specific message or with all messages

Though not as common as it once was, virus signatures can be corrupted when they are downloaded from the vendor. A corrupted signature database will cause the virus scanner software to fail.

Containing a Virus Outbreak

You are driving to work and the morning news mentions a new and dangerous virus. You wonder if the story is hype or if the virus is real threat. You arrive at work and find your boss and 30 new voicemail messages waiting for you. Your Inbox has 2500 copies of this new virus. A virus has managed to get into your organization through mechanism you had not previously thought of, and your organization is too large to go from user to user advising the users on what to do next.

Your first and most immediate task must be to stop further exposure. First, stop all SMTP services on your Exchange Server, perimeter SMTP gateways, and stop the Exchange MTAs.

> By stopping SMTP, you have stopped *all* mail flow. Evaluate whether this step is right for the situation—especially if you need to send a message to the user community about what to do next.

Once SMTP and the MTAs are stopped, it is time to assess the situation quickly. By stopping SMTP and the MTAs, you have stopped the virus from spreading, but you have also stopped email from flowing.

Next, before you even get back in touch with your boss, force virus signature updates from the vendor's update site. If the virus has already been announced on the news, your vendor should know about it and have something on the Web site. If the virus is only a few hours old, signatures may not be available for a few more hours, so you have more work to do. In this case, consider the following factors:

- How bad is the outbreak? Is it all servers and all locations?
- How long can you remain offline (without email flowing)?
- Does this situation warrant a shutdown?
- Are the WAN links clogged?
- Do the SMTP queue and MTAData directories have many copies of this message?
- Is there something recognizable or unique about the virus such as a subject, attachment name, or attachment type?

If you are in a larger organization, you are probably going to have to make a recommendation to your boss about what to do next. A complete shutdown is not a very popular option. Upper management and your users do not appreciate or understand how the virus managed to hinder email flow, just the fact that email is down. The pressure is now on and you need to get mail flowing again as soon as possible.

Locking Users Out of the Exchange Server

Locking your users out of the Exchange server is not going to be advisable under most circumstances, but it might be the only way to subdue the virus or worm that is taking advantage of your disk storage and bandwidth. For POP3, IMAP4, HTTP, and NNTP clients, doing so is a simple matter of disabling the appropriate services:

- Microsoft Exchange POP3
- Microsoft Exchange IMAP4
- NNTP
- World Wide Web Publishing Service

For MAPI clients, it is a little different; you could simply disable the information store service, but doing so will prevent you from extracting any messages using ExMerge. On Exchange 2000 SP1 and later, you can create a registry key that will disable certain versions of MAPI clients; in this case, you are interested in disabling all versions except the Exchange server components themselves. Open the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem key, and create` a value of type REG_SZ called Disable MAPI Clients. In this value, enter in the data field

```
-6.0.0, 7.0.0-
```

Then stop and restart the Microsoft Exchange Information Store service. Doing so prohibits any version of the MAPI client except 6.0.0 through 7.0.0 from connecting to the information store; this will be the Exchange components (and ExMerge, if running from the Exchange server's console).

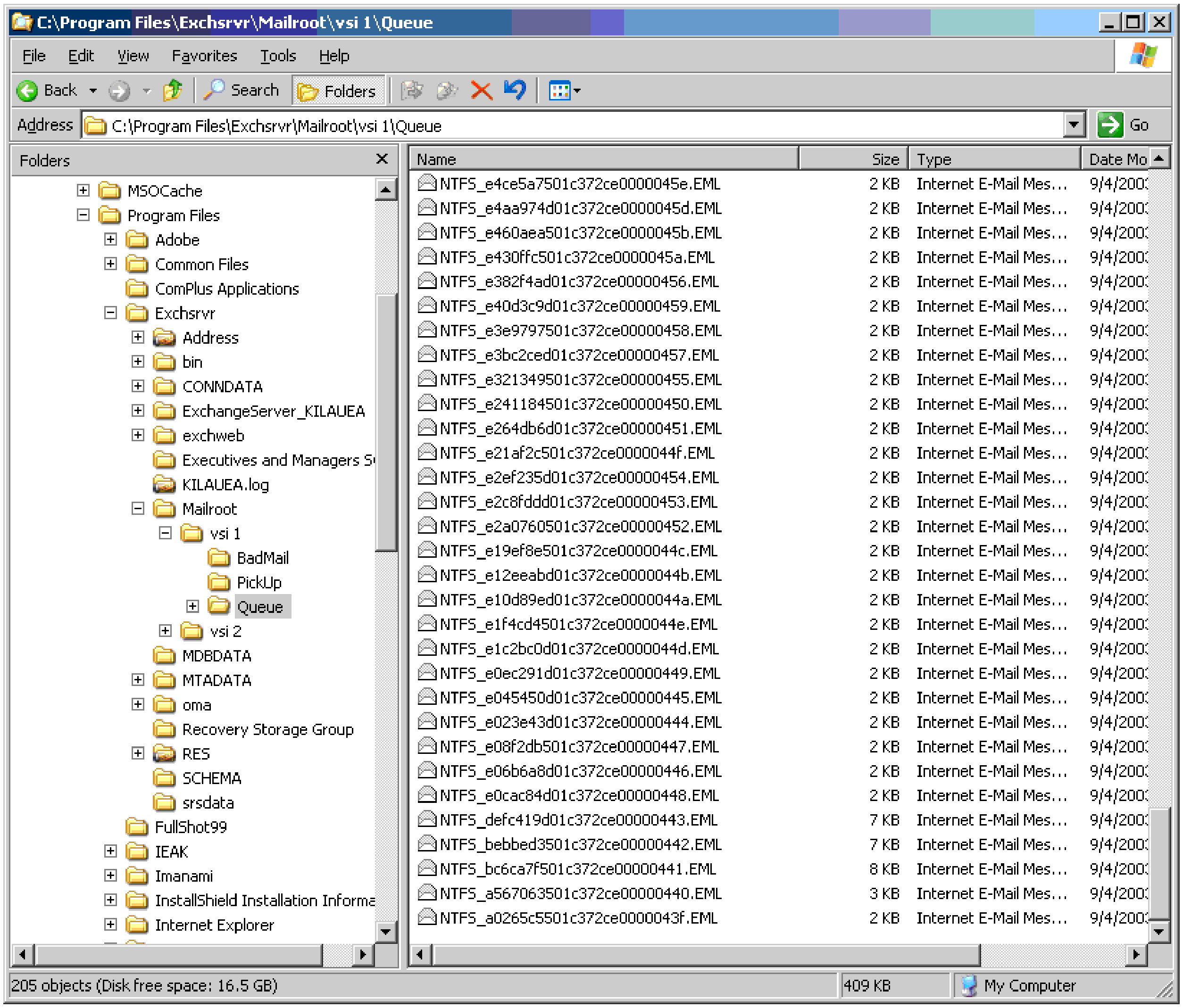
📖 For more information, see the Microsoft article "XADM: Feature to Disable MAPI Clients."

☞ Once you are ready to allow users back on to the servers on which you have disabled the MAPI clients, delete the Disable MAPI Clients registry key and restart the information store.

Cleaning Up Queue Directories

If you examine the \Exchsrvr\Mailroot\vsi 1\queue directory, you will find all the inbound messages that had not been processed when you shut down the SMTP service. It would be easy to delete every file in this directory, but you don't know viruses from valid messages merely by looking at the file names. If you have truly been in the middle of a major outbreak, the Advanced Queuing Engine will probably have been overwhelmed and you might have thousands (or tens of thousands) of files in this directory. The same holds true for the \Exchsrvr\MTAData directory, if you are using the Exchange MTA.

Figure 3.9 shows the queue directory of an Exchange 2003 SMTP virtual server; this directory contains a few hundred messages that were the result of a minor virus outbreak. However, not all of these messages are viruses, so I'm going to use Windows' built-in FINDSTR to remove only the viruses.



Name	Size	Type	Date Mo
NTFS_e4ce5a7501c372ce0000045e.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e4aa974d01c372ce0000045d.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e460aea501c372ce0000045b.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e430ffc501c372ce0000045a.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e382f4ad01c372ce00000456.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e40d3c9d01c372ce00000459.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e3e9797501c372ce00000458.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e3bc2ced01c372ce00000457.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e321349501c372ce00000455.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e241184501c372ce00000450.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e264db6d01c372ce00000451.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e21af2c501c372ce0000044f.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e2ef235d01c372ce00000454.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e2c8fddd01c372ce00000453.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e2a0760501c372ce00000452.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e19ef8e501c372ce0000044c.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e12eeabd01c372ce0000044b.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e10d89ed01c372ce0000044a.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e1f4cd4501c372ce0000044e.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e1c2bc0d01c372ce0000044d.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e0ec291d01c372ce00000449.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e045450d01c372ce00000445.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e023e43d01c372ce00000444.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e08f2db501c372ce00000447.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e06b6a8d01c372ce00000446.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_e0cac84d01c372ce00000448.EML	2 KB	Internet E-Mail Mes...	9/4/200
NTFS_defc419d01c372ce00000443.EML	7 KB	Internet E-Mail Mes...	9/4/200
NTFS_bebbed3501c372ce00000442.EML	7 KB	Internet E-Mail Mes...	9/4/200
NTFS_bc6ca7f501c372ce00000441.EML	8 KB	Internet E-Mail Mes...	9/4/200
NTFS_a567063501c372ce00000440.EML	3 KB	Internet E-Mail Mes...	9/4/200
NTFS_a0265c5501c372ce0000043f.EML	2 KB	Internet E-Mail Mes...	9/4/200

205 objects (Disk free space: 16.5 GB)   409 KB   My Computer

Figure 3.9: Virus explosion in the queue directory!

The first task is to find something unique about the virus; hopefully so unique that it will not occur in normal messages in the queue directory. In this example, I'm going to search for the Love Bug virus; Love Bug included in the subject line ILOVEYOU. Thus, the simple command

```
Findstr /c:ILOVEYOU c:\program files\exchsrvr\mailroot\vsi
1\queue\*.eml
```

will search for files containing the target string and list those that it finds. At that point, you can inspect the files to confirm that they're infected, and move them to another directory or remove them altogether. (You can also use Windows' search command to search the files; this method is slower than FINDSTR, but the search tool shows all the results at once so you can simply hit Ctrl+A, followed by Shift+Del, to remove all the suspect files.)

Cleaning the MTAData directory

A few years ago, Microsoft wrote a utility called findbin.exe for the specific purpose of finding viruses in queue directories. It was released by Microsoft's support services initially, then later, when the Love Bug virus hit, it was included in the ILOVEYOU.ZIP cleanup kit.

> 🖫 You can find a link to findbin.exe at in http://www.somorita.com/webcasts.

Findbin.exe is an extremely simple program. You supply it with a hexadecimal string of data that represents something unique about a virus along with a list of files to look through. If findbin finds that string in any of the specified files, it will move those files to a directory specified in the command. Using the ILOVEYOU example again, I'll walk through the process of cleaning the MTAData directory with findbin. Because the MTA queue files are in binary format, I need the hexadecimal equivalent of my unique string; thus, I need to convert ILOVEYOU to hexadecimal, which is 494C4F5645594F.

> ☞ Don't convert to hexadecimal often? Visit http://www.asciitable.com.

If the MTA is not already stopped, you will need to stop it before you can clean up the messages in this directory, so make sure the Microsoft Exchange MTA Stacks service is stopped. Next, I'm going to put findbin.exe into the path on the Exchange server (probably the \WINNT directory), and create a subdirectory in the queue folder called VirusMsg into which findbin.exe will move any viruses messages it finds. I'm going to make my current directory the MTAData directory so that I don't have to type long paths in the command-line options, then, I will type

```
    FINDBIN 494C4F5645594F DB*.DAT VIRUSMSG
```

Doing so should move all the infected MTA data files into the VirusMsg directory. Once this is done and before I restart the MTA, I will run the MTACHECK program to make sure that the MTA database is in good shape.

Getting Rid of the Virus from the Stores

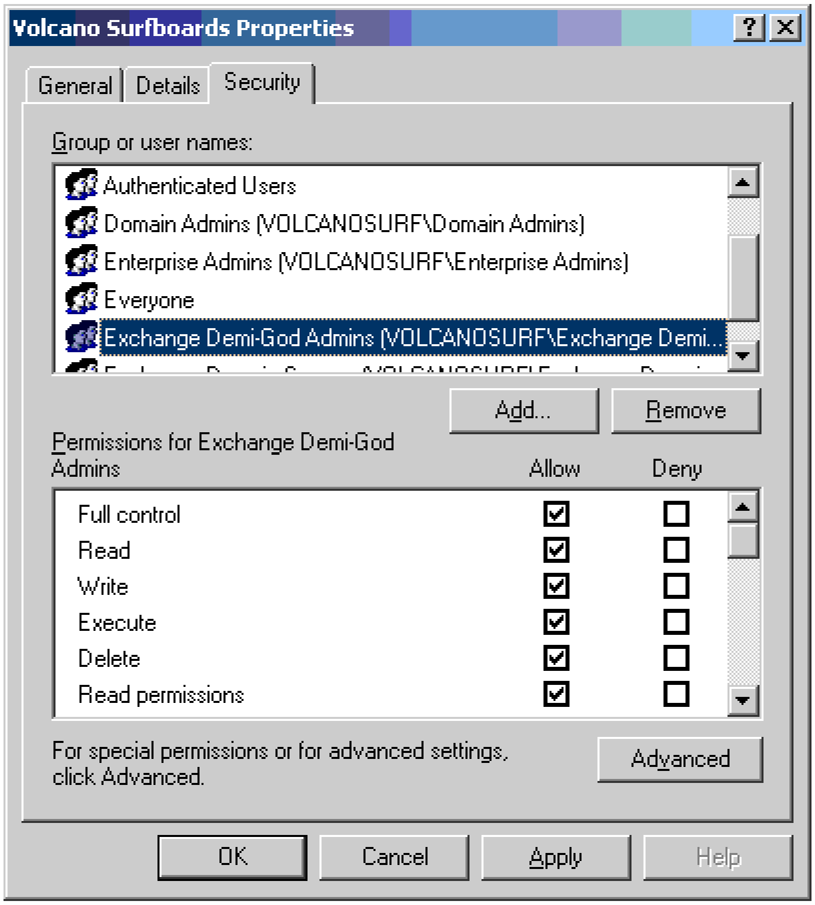
Regardless of how many times you tell people to delete a message that has a virus, a few of your users are going to open the message anyway. Part of an effective removal strategy is to make sure that the virus is completely eradicated from the information store. Theoretically, once your virus signatures are finally updated, they will catch any viruses that anyone tries to open, but it is a good backup to at least attempt to remove the virus from users' mailboxes. To do so, you can use the ExMerge utility.

> 🖫 You can download ExMerge from http://www.microsoft.com/exchange/tools/2003.asp, then place it in the \Exchsrvr\bin directory.

The first thing you will need is a user account that has permissions to open all the users' mailboxes. I won't explore the political or security dangers of creating this user, just keep in mind that this user must be protected from unauthorized use because it has the permissions to access anyone's email. This user cannot be a member of the Domain Admins or Enterprise Admins groups because these groups are automatically blocked from being able to open users' mailboxes.

First, create a global security group, for example, Exchange Demi-God Admins, then create a user—ExchSuperAdmin—that has a strong password. This user should be a member of the global security group because you will assign permission to the group rather to an individual user.

Open Exchange System Manager while logged on as an Administrator that has Full Exchange Admin permissions, and display the properties of the Organization or an Administrative group. If the Security property page is not visible in ESM, you will need to enable it in the registry by opening the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\ExAdmin registry key.` In this key, create a REG_DWORD value called ShowSecurityPage, and set it to 1. When you close and reopen Exchange System Manager, the Security property page should be visible. On the Security property page, add the Exchange Demi-God Admins group and give it Full Control (as Figure 3.10 shows). If you use the Delegation Wizard, the Receive As and Send As permissions are automatically denied and the user account you're creating will not be able to open other users' mailboxes.



Group or user names:

- Authenticated Users
- Domain Admins (VOLCANOSURF\Domain Admins)
- Enterprise Admins (VOLCANOSURF\Enterprise Admins)
- Everyone
- Exchange Demi-God Admins (VOLCANOSURF\Exchange Demi...

Permissions for Exchange Demi-God Admins

	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Execute	☑	□
Delete	☑	□
Read permissions	☑	□

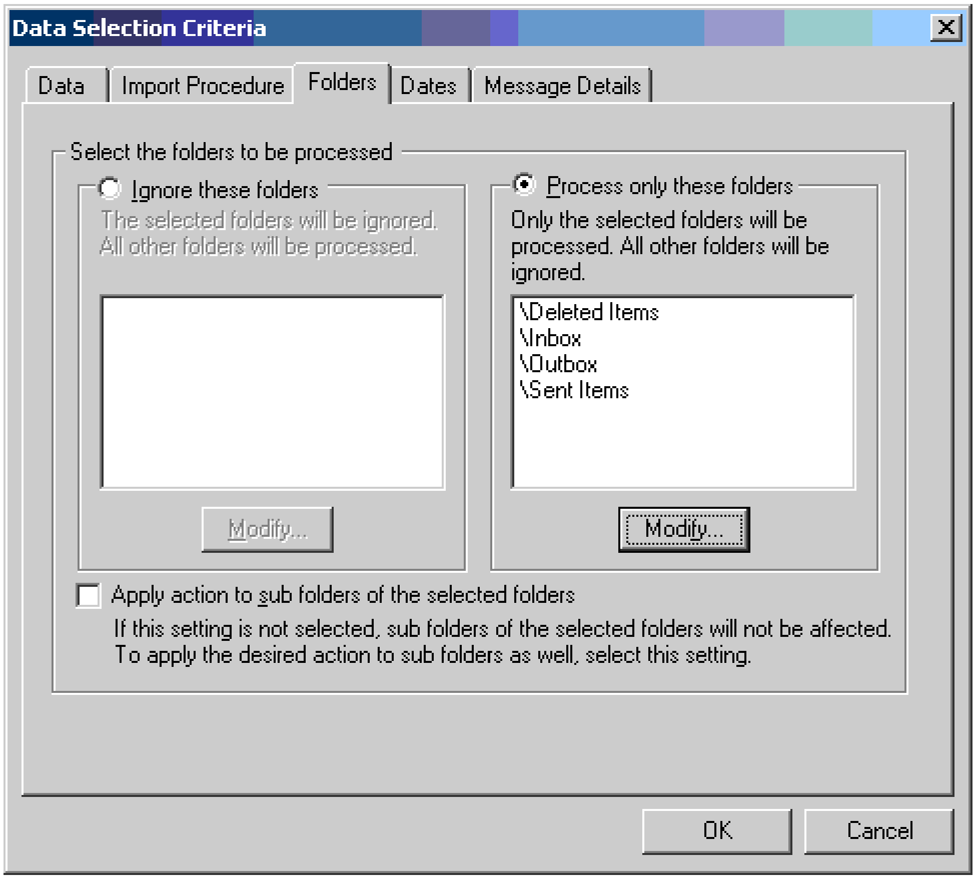
For special permissions or for advanced settings, click Advanced.

Figure 3.10: Granting a group Full Control permissions.

If your Exchange server is running on a domain controller, you should also make your ExchSuperAdmin user a member of an operators group such as Server Operators; otherwise it will not be able to log on to the console of the Exchange server. Once your user has sufficient permissions to access everyone’s mail messages, it is time to use the ExMerge utility. Before you start, ensure that you have isolated a unique characteristic about the virus-infected messages, such as a subject or attachment name.

I use the archive feature to archive mail that meets a certain criteria to PST files. That way, if I accidentally removed an important message, I have a copy of the PST file. Also, I recommend performing the cleaning with ExMerge in two steps. First, look through only the Inbox, Outbox, Deleted Items, and Sent Items folders to help ensure speed when removing messages. I perform a second pass later, once the server is back online and users are working, that extracts the virus from any other folder to which it might have been moved. The following steps walk you through the process of extracting virus-infected messages that have a subject of ILOVEYOU from the Inbox, Outbox, Sent Items, and Deleted Items folders:

1. Run the ExMerge Wizard, and click Next.
2. Select the Extract or Import (two-step procedure) radio button, and click Next.
3. Select the Step 1: Extract data from an Exchange Server Mailbox radio button, and click Next.
4. In the Source Server dialog box, enter the name of the Exchange server, the name of domain controller, and click Options.
5. On the Import Procedure property page, click the Archive Data to Target Store radio button.
6. On the Folders tab, select the *Process only these folders* radio button, then click Modify. Add the folders you want to process to this list (see Figure 3.11).



Data Selection Criteria

Data | Import Procedure | Folders | Dates | Message Details

Select the folders to be processed

○ Ignore these folders

The selected folders will be ignored. All other folders will be processed.

● Process only these folders

Only the selected folders will be processed. All other folders will be ignored.

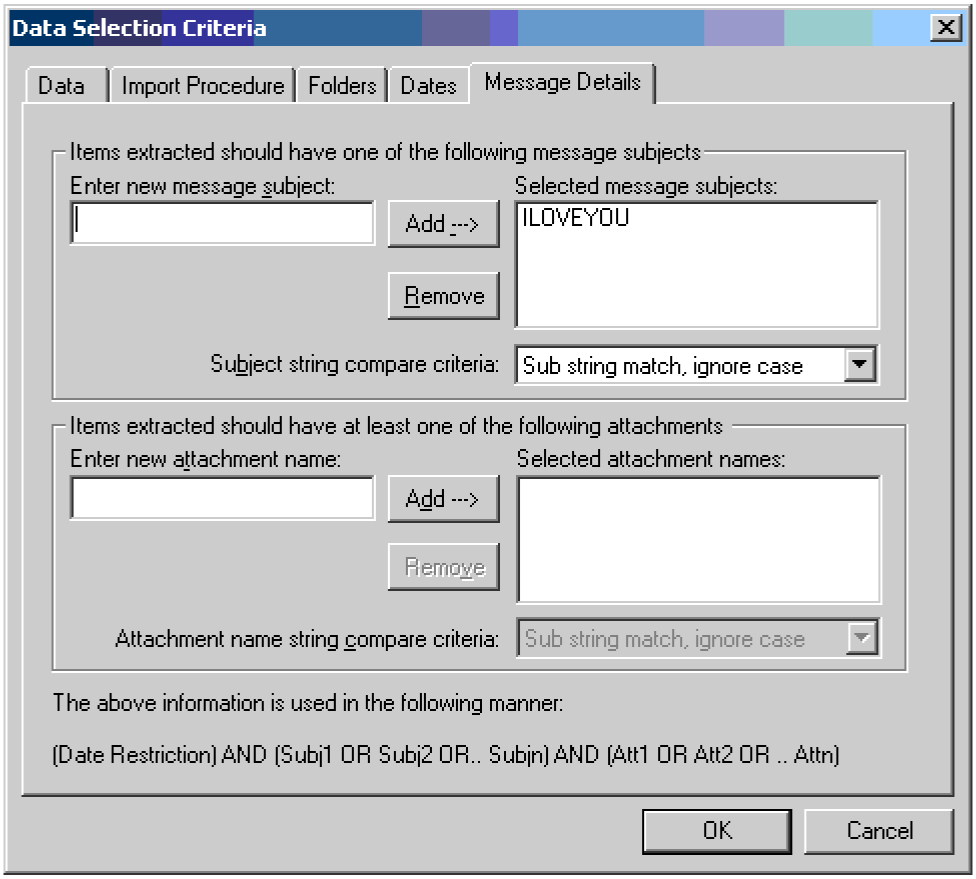
\Deleted Items
\Inbox
\Outbox
\Sent Items

□ Apply action to sub folders of the selected folders

If this setting is not selected, sub folders of the selected folders will not be affected. To apply the desired action to sub folders as well, select this setting.

Figure 3.11: ExMerge's Folder's tab lets you specify which folders you will process.

7. Optionally, you can specify a date range on the Dates tab if the virus has just hit. Doing so will reduce the likelihood that you will accidentally remove valid messages.
8. On the Message Details tab (see Figure 3.12), specify the unique characteristic of the message that you want to remove from the folders. If you leave this blank, ExMerge will remove *all* messages from the specified folders. In this example, I have added ILOVEYOU to the list of selected subjects.



Items extracted should have one of the following message subjects

Enter new message subject:

Selected message subjects: ILOVEYOU

Subject string compare criteria: Sub string match, ignore case

Items extracted should have at least one of the following attachments

Enter new attachment name:

Selected attachment names:

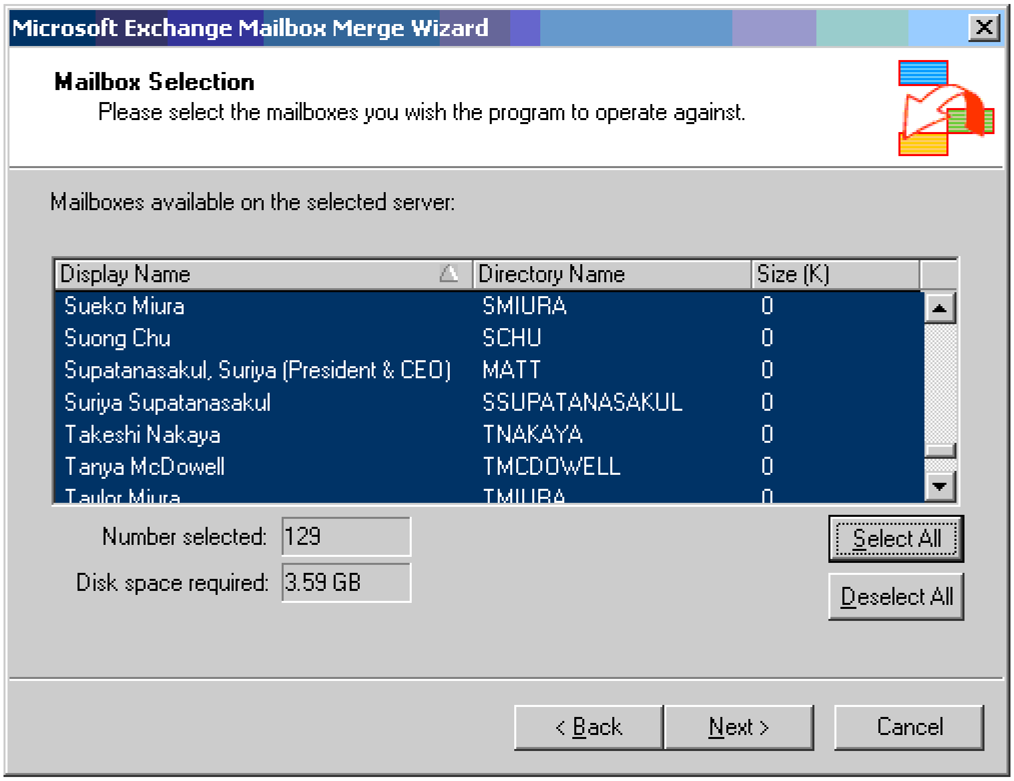
Attachment name string compare criteria: Sub string match, ignore case

The above information is used in the following manner:

(Date Restriction) AND (Subj1 OR Subj2 OR.. Subjn) AND (Att1 OR Att2 OR .. Attn)

Figure 3.12: Specifying a message subject or attachment name.

9. When finished with the Options, click OK and Next.
10. In the Database Selection dialog box, select the mailbox stores you want to process, then click Next.
11. On the Mailbox Selection listing (see Figure 3.13), select the mailboxes you want to process. If you are extracting a virus, you will probably want to click Select All. When finished selecting mailboxes, click Next.



Microsoft Exchange Mailbox Merge Wizard

Mailbox Selection

Please select the mailboxes you wish the program to operate against.

Mailboxes available on the selected server:

Display Name	Directory Name	Size (K)
Sueko Miura	SMIURA	0
Suong Chu	SCHU	0
Supatanasakul, Suriya (President & CEO)	MATT	0
Suriya Supatanasakul	SSUPATANASAKUL	0
Takeshi Nakaya	TNAKAYA	0
Tanya McDowell	TMCDOWELL	0
Taylor Miura	TMIURA	0

Number selected: 129

Disk space required: 3.59 GB

Figure 3.13: Selecting mailboxes to process.

12. Specify the default locale; if you don’t know what this means, then leave the selection as English (US), then click Next.
13. Specify a path for the location to the PST files you are about to create. The location should be a drive with enough space to accommodate all of the PSTs. Don’t panic if the estimated amount of space required seems excessive; ExMerge tends to exaggerate about how much space it thinks it will need. And, remember, you are only extracting a few messages. When finished, click Next twice to commence with the extraction.

This procedure should extract the messages you specified from the mailbox stores. A log file will be recorded in the directory from which you ran ExMerge called ExMerge.log. You should scan this log for any errors.

ExMerge works great as long as the information store service is running and the mailbox store is mounted. Ontrack’s PowerControls tool allows you to mount a mailbox store and access mailbox data even when the mailbox store is dismounted or the information store service is stopped. You can find more information about PowerControls at http://www.ontrack.com/powercontrols.

Best Practices for Virus Protection

If you follow good procedures and have a well-thought through antivirus protection scheme in place, you should be safe from most outbreaks. The following list provides best practices for preventing viruses from attacking your organization from the Exchange server perspective:

- Keep your antivirus scanning engine and virus signatures updated daily.
- Implement a multi-tier protection scheme in which at least all inbound mail is scanned by at least two separate virus scanning engines.
- Publish and implement on your perimeter SMTP gateway and Exchange servers a list of forbidden attachments.
- Do not assign administrative or operator account mailboxes. All IT users should have a non-privileged account for regular office automation tasks and a separate account with elevated privileges for administrative tasks; the administrative accounts should never have mailboxes.
- *Quickly* evaluate each security fix and critical update from Microsoft to determine whether it applies to your organization and, if so, how soon should it be applied. Do *not* procrastinate. Although it is true that Microsoft hotfixes sometimes cause new problems, you have to decide whether that small risk is better than the much larger risk imposed by failing to quickly apply critical fixes.
- Develop an escalation procedure that helps you to deal quickly and efficiently with a virus that sneaks in due to out-of-date signatures or previously unknown vulnerabilities.
- Create a separate mailbox that is used for antivirus reports. Monitor this mailbox at least weekly and don’t forget to archive it.
- Run weekly reports of viruses detected and messages processed.

Summary

It is no secret that computer viruses, worms, and Trojan horses have become the scourge of every computer user and administrator. Countless hours of downtime and dollars have been lost due to viruses; billions of dollars are spent in the fight against viruses. In Chapter 1, we covered some of the basics of viruses, worms, and Trojan horses and explored a little history. The evolution of this malware clearly shows that the authors of these afflictions are becoming more creative and their spawn is more dangerous than ever.

Virus protection must start with the client computer. An end user or administrator can easily introduce viruses to a corporate network in a variety of ways including floppy, CD-ROM, external POP3 or IMAP4 mail servers, USENET newsgroups, instant messaging clients, Web mail, or email from an Exchange server. Viruses and worms that can enter a network through mobile devices or PDAs have already been discovered and future malware of this class will only be worse.

In Chapter 2, we explored virus and worm protection from the perspective of the client. Virus protection on the client-side must include not only up-to-date antivirus software but also an up-to-date OS and email client. Exchange Server can also be used to further secure clients by restricting MAPI client versions to only approved versions and centrally configuring Outlook 2000 SP3 and later mail security features.

In Chapter 3, we have explored the challenge associated with protecting email on the server. When possible, a virus perimeter should be built around the server in the form of correctly configured firewalls, SMTP virus and content scanning, and properly configured email clients. The Exchange server should also have antivirus software, preferably Exchange-aware antivirus software that uses AVAPI for Exchange for accessing data in the Exchange server.

The key to effective email protection is continued vigilance. You can never get complacent in the battle against malware—just when you thought you had considered everything, someone will prove you wrong.