realtimepublishers.com®

The Administrator Shortcut Guide™ To

Email Protection

Sybari
Software, Inc.

Paul Robichaux

Copyright Statement

Chapter 2: Protection at the Client Level

In the first chapter, we explored many of the risks to which networked computers are exposed. Even if a computer is not networked, if the users of that computer share media (floppies, CD-ROMs, DVDs, or tapes) that have infected files, the computers can be infected by viruses, worms, or Trojan horses.

Your virus protection strategy is not complete until you have protected not only the email server, but also the client. In this chapter, I'll cover how to protect Windows-based clients that are using Microsoft Outlook or Outlook Express and connecting to a Microsoft Exchange Server. Why? Protecting clients and leaving the server unprotected gives you a reasonable degree of security, but the reverse isn't true. Client protection is the fundamental first step toward building a strong, layered defense against viruses. Many of the techniques discussed in this chapter are specific to Exchange environments, while others are generic and the principles can be applied to most any environment.

Virus Entry Points

Before I delve into client protection, let's first explore some of the different ways that malware (viruses, worms, and Trojan horses) can make their way into your organization. Although many of these entry points are the result of users introducing a virus to the environment, some of them are a result of carelessness on the part of the systems or network administrators. The widespread perception is that the most common way viruses are transported is via an infected email message or an infected attachment. However, probably the most common way that viruses are spreading in 2003 is by exploiting vulnerabilities in OSs and Web servers. Nimda, Code Red, Klez, and the SQL Slammer prove that such blended virus/worm threats can be devastating. However, there are many ways for malware to spread:

- Through users who accidentally introduce viruses, worms, and Trojan horses by introducing outside, unscanned media (floppy, CD-ROM, DVD, or tape)
- By way of users who download viruses, worms, and Trojan horses from Internet Web sites either unknowingly or by downloading shareware or infected software from file sharing services or 'warez sites
- Via users who use their external POP3, IMAP4, or Web mail accounts to retrieve personal email—without it being scanned for malware—from outside of the organization
- Through users that connect to the network remotely from computers that are unprotected, such as a laptop or home computer

> ☞ Some antivirus software vendors allow a user to install a copy of the company software on a single home computer—check your software's license agreement.

Penny-Wise and Pound Foolish

Company X had purchased antivirus software for its Exchange Server system and the company's firewall had a virus scanning component. Only a few computers actually had antivirus client software installed, and the software was what had shipped with the client computers. In an effort to save money, the IT department reasoned that client software was not necessary on the company's desktop computers. They rationalized this decision by stating that viruses entered the organization through the email system.

During the first year after this server-protection-only strategy was implemented, numerous viruses entered the organization via documents on floppy disks and by way of users who brought their notebooks in and out of the office. Often, the only time a virus was detected was when a user emailed a document infected with a macro virus. The internal network was also infected with the Nimda worm/virus twice due to users plugging infected notebook computers into the company network.

Securing the Desktop—Client Protection 101

Users are remarkably ingenious when it comes to figuring out how to completely mess up their desktop computers. Even the most technically inept user can (unintentionally) figure out a way to require a visit from the Help desk. The more technically savvy the user is, the more difficult the problem can be to track down. In the process of exchanging documents, adding software, changing settings, and reading email from outside sources, users can introduce viruses from outside extremely easily. The desktop client must be secured in order to prevent viruses from being introduced into your organization.

Choosing Antivirus Client Software

There are many antivirus client software vendors targeting the desktop market. Each of these products has strengths and weaknesses. You must evaluate the client software based on your specific needs and decide which vendors meet your requirements for desktop scanning. The following list highlights a few guidelines for picking client software for an organization with more than 100 seats. The ideal client should be:

- Capable of automatically updating its virus signatures on a schedule you set (or at least on a daily basis)
- *Email aware*, meaning that it understands email client software (such as Outlook and Outlook Express); for SMTP, POP3, and IMAP4 clients, the software must be able to scan inbound and outbound message traffic
- Configurable to scan different types of files—not just executables
- Capable of scheduled weekly hard disk scans
- Capable of detecting blended threats and other forms of malware (in addition to viruses)
- Able to allow centralized administration of client configuration and scanning rules
- Automatically configured to scanning removable media for viruses when inserted
- Able to perform real-time scans of the file system so that if hostile content is written to or read from the file system, the scanner will detect it

- Optimized and designed for organizations of your size and needs—some antivirus clients are designed for organizations with centralized administration, while others are designed for small offices or home use
- Designed for a corporate environment, including reporting software that allows the administrator to monitor client software version, signatures, and outbreaks

> ☞ Client software that can quickly update its signatures during a virus outbreak is very helpful. A desktop client that can only access signatures once per day or once per week will be dangerously exposed during more virulent and fast-spreading virus outbreaks. Some blended threats, such as Nimda and SQL Slammer, infected computers world-wide within 15 minutes of their initial release into the wild. McAfee estimates that there are approximately 300 new viruses per month. Of course, you probably won't want to pull down multiple updates per day in normal operation, but you want the ability to do so when a fast-spreading virus is about.

Common Vendors of Antivirus Client Software

You should give careful consideration to whichever antivirus client software you are planning to use. It should meet both your security and administrative needs. Table 2.1 lists some of the more common vendors of antivirus software. This list is alphabetical and is not an endorsement of a specific product nor is it all-inclusive.

Vendor	Web address
AVG Anti-virus	http://www.grisoft.com
BitDefender	http://www.bitdefender.com
Computer Associates	http://www.ca.com
FRISK Software	http://www.f-prot.com
Kapersky Lab	http://www.kapersky.com
Network Associates	http://www.mcafee.com
Norman Virus Control	http://www.norman.com
Panda Software	http://www.pandasoftware.com
Sophos	http://www.sophos.com
Symantec	http://www.symantec.com
Trend Micro	http://www.trendmicro.com

Table 2.1: Common antivirus vendors.

> 📖 For comparisons and tests of various antivirus products, visit http://www.av-test.org. This Web site is a joint project of the University of Magdeburg and GEGA IT-Solutions. Products are tested on a variety of Windows and non-Windows platforms to determine performance and detection for not only viruses found in the wild but also for "zoo" (lab) viruses. In April of 2003, PC Magazine published a review of corporate antivirus software solutions; you can find this review at http://www.pcmag.com/article2/0,4149,978683,00.asp.

General Recommendations

This chapter focuses mostly on the use of Microsoft Outlook 2000 and later as an email client. Many of the suggestions for tightening security for Outlook (such as restricting Internet Explorer—IE—Security Zones) applies to Outlook Express as well as Outlook. Outlook and Outlook Express present interesting targets for malware authors because of the number of different programmatic interfaces that are available and the proliferation of these clients.

However, this attraction to Outlook and Outlook Express by malware authors does not mean that other email clients are not at risk. Although the rest of this chapter does focuses on these Microsoft platforms, I wanted to take a brief opportunity to provide some solid suggestions for protecting other email client software. These tips (some of them are pretty obvious) apply whether you are using a Macintosh, Linux, or other desktop platform and regardless of the email client you are using:

- Regularly fix bugs and close known vulnerabilities
- Update the Web browser—the version should be fairly recent and you should have all the latest fixes; if the vendor is no longer releasing fixes for the version of the browser you are using, it is time to upgrade
- Update the email client—most email clients (including many of the public domain clients and shareware clients) are updated periodically with security fixes and feature updates
- Disable an email client's scripting interface (regardless of the email client that you are using) as a good security precaution against virus outbreaks—different clients have different recommendations for making the client software more secure

Netscape Mail

Disabling the scripting interface in Netscape Mail will help tighten the security of that email client. To disable scripting, launch the Netscape Mail client, select Edit, then Preferences. Select Category, then Advanced, clear the *Enable Javascript for Mail and News* check box, and click OK to close the dialog box.

📖 You can find more information about the Netscape Mail program on the Web at http://channels.netscape.com/ns/browsers/mail.jsp.

Qualcomm Eudora

Qualcomm makes a few recommendations for tightening security and improving virus protection in the Eudora mail client. First the company recommends that you disable allowing executables in the mail client. To so, select Tools, Options—Viewing Mail, and clear the *Allow Executables in HTML Content* check box. The company also recommends that you configure Eudora with a different directory than the default for the Attach directory.

📖 For documentation regarding the directory change check out http://www.eudora.com/techsupport/kb/2020hq.html. You can also find more information about Eudora at (http://www.eudora.com and http://www.eudora.com/security.html).

Outlook Security Update

Over the past several years, Microsoft has made quite a few security improvements in Outlook. One of the most significant of these changes is the Outlook Security Update, originally released for Outlook 98 and Outlook 2000. If you are running Outlook 98 or Outlook 2000, you should apply this update to your desktop clients as soon as possible.

> 📖 You can find the update for Outlook 2000 at http://office.microsoft.com/downloads/2000/Out2ksec.aspx (note that Outlook 2000 SR1 must be installed). For more information about the update for Outlook 97, 98, and 2000, see the Microsoft article "Outlook E-mail Attachment Security Update."

> ✎ The Office 2000 Service Pack 2 (SP2) and SP3 both include the security features that were introduced in the Outlook Security Update. Outlook 2002 and Outlook 2003 also include the security fixes.

Understanding the Outlook Security Update

The Outlook Security Update made a number of changes to Outlook to improve Outlook's resistance to viruses. These attachment security features are an attempt to protect users from accidentally opening malware attachments and to protect users' address books against attacks by macro viruses that try to mail themselves to everyone in an address list. These measures can help to slow the spread of email-based viruses within an organization.

> ☞ Notify your user community of the new restrictions that the Outlook Security Update or a newer version of Outlook will impose. Some users may need to be able to access restricted files via their email, so they'll need to think of other ways to accomplish this task.

The security update has changed slightly between the original version and Outlook 2000 SP3; I am going to discuss the features in the later version, which I strongly recommend that you apply.

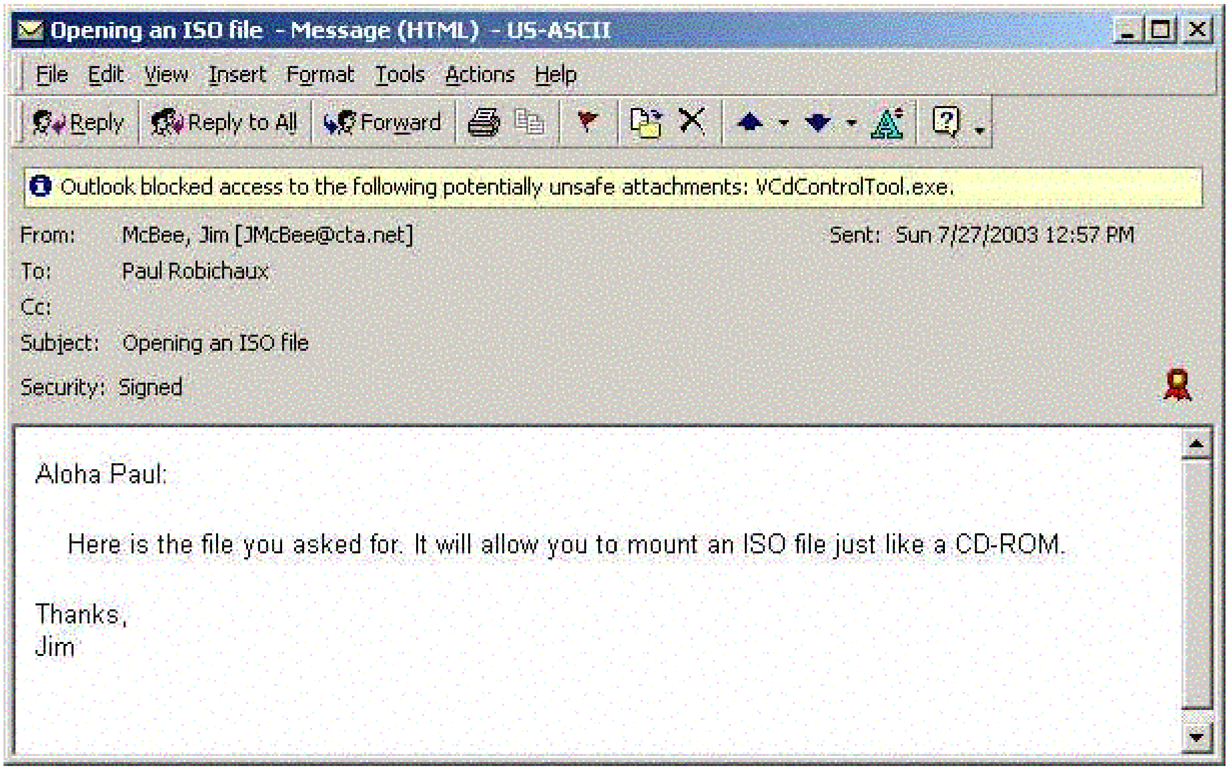
By default, when the update is installed, the security features are all enabled. Later in this chapter, I will review some features that will allow you to centrally control these restrictions using the Outlook Security Features Administrative Package from the Office Resource Kit. These new security features include:

- Defining a specific set of attachments as potentially unsafe and preventing users from either opening the attachment or saving it to disk. These attachments are known as Level-1 attachments.
- Warning users when they attempt to send an attachment categorized as a Level-1 attachment that the attachment might be potentially unsafe.
- Giving users the ability—through the registry editor—to "demote" specific Level-1 attachment types to Level-2 attachments. Level-2 attachments can be saved to the hard disk, but not opened directly through Outlook.

- Implementing add-in and third-party application security; if an application attempts to programmatically access Outlook using the Outlook object model, Simple MAPI, or Collaborative Data Objects (CDO), the add-in can automatically be denied access to Outlook or the user can be prompted to allow the add-in to access Outlook messages, features, and the address book.
- Allowing specific add-ins and extensions to be defined as safe; thus, the user will not be warned each time the add-in accesses Outlook. This feature is useful when the add-in is used for each message sent or received.

Prior to installing the security update for all of your users, run some tests on custom forms and Outlook add-ins in your environment. It is entirely possible that this patch will change the behavior of these forms and add-ins or that the users may see additional prompts that they had not seen prior to the update being installed. If you have custom forms that contain scripts, you might need to change the behavior of these forms and make sure that they are published to the organization forms library.

The patch defines for Outlook two types of attachments: Level-1 and Level-2. Users are prohibited from opening or saving attachments in the Level-1 attachment list. Though the attachments are still in the message, the user sees a note directly below the button bar indicating that the message contains a potentially unsafe attachment (see Figure 2.1).



Outlook blocked access to the following potentially unsafe attachments: VCdControlTool.exe.

From: McBee, Jim [JMcBee@cta.net]   Sent: Sun 7/27/2003 12:57 PM
To: Paul Robichaux
Cc:
Subject: Opening an ISO file
Security: Signed

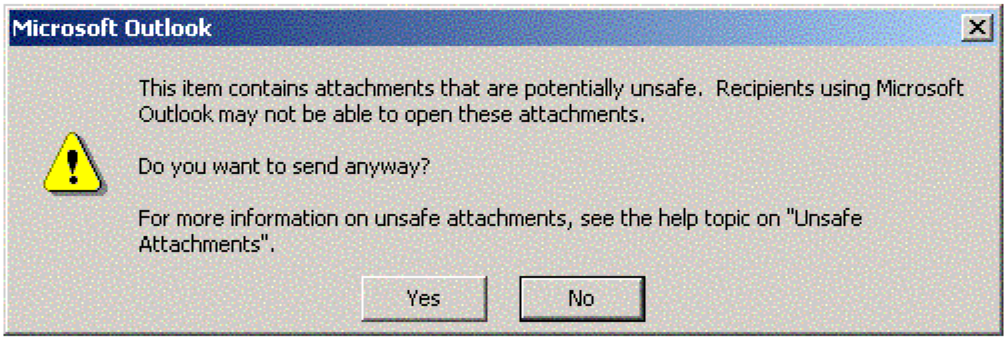
Aloha Paul:

Here is the file you asked for. It will allow you to mount an ISO file just like a CD-ROM.

Thanks,
Jim

Figure 2.1: Once the Outlook Security Update is installed, users no longer have access to unsafe attachments.

If the user attempts to forward the message, the potentially unsafe attachment will be stripped from the forwarded message. However, Outlook will allow the user to send the message as long as they click Yes in the warning dialog box that Figure 2.2 shows (the warning dialog box will appear slightly different with different versions of Outlook and depending on whether the Outlook Assistant is enabled).



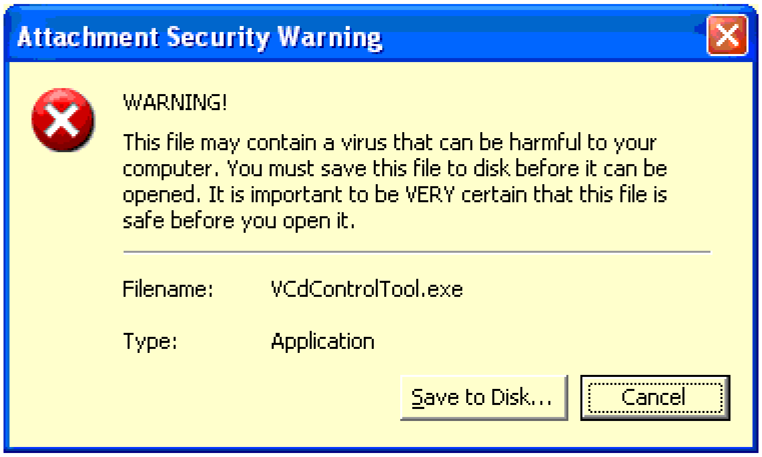
This item contains attachments that are potentially unsafe. Recipients using Microsoft Outlook may not be able to open these attachments.

Do you want to send anyway?

For more information on unsafe attachments, see the help topic on "Unsafe Attachments".

Figure 2.2: Outlook warning message for unsafe attachments.

As I mentioned earlier, users or administrators can demote some attachments from Level-1 to Level-2 attachments. Once an attachment is considered a Level-2 attachment, the user can save the attachment to disk, but they will still receive a warning indicating that the attachment is potentially unsafe if they attempt to open it directly from within Outlook. Figure 2.3 shows this warning (this image is from Outlook 2002).



WARNING!

This file may contain a virus that can be harmful to your computer. You must save this file to disk before it can be opened. It is important to be VERY certain that this file is safe before you open it.

Filename: VCdControlTool.exe

Type: Application

Figure 2.3: Warning a user that he or she cannot open a potentially unsafe attachment.

☞ In many email environments, some attachments are automatically blocked from being sent and received by the firewall, SMTP scanner, or the mail-server antivirus scanning software. A very good practice is to instruct users to rename their potentially unsafe attachments—such as renaming VBS attachments to VB_ or to use a zip utility. Some antivirus and scanning software may still detect the attachment type if it has been renamed or compressed, so this solution will not work for everyone.

So what is considered a blocked attachment? Table 2.2 provides the Level-1 attachment types that are blocked.

> ✐ You can find a comprehensive list of the blocked attachment types in Appendix B of the Microsoft whitepaper “Outlook 98/2000 Email Security Update” at http://www.microsoft.com/office/ork/2000/download/OutSecWP.doc.

Attachment Extension	Description
Ade	Microsoft Access project extensions
Adp	Microsoft Access project
App	Microsoft Visual FoxPro application
Asx	Windows Media audio or video shortcut
Bas	Visual Basic module
bat	Batch file
chm	Compiled HTML help file
cmd	Windows command script
com	MS-DOS program
cpl	Control Panel applet
crt	Security certificate
csh	KornShell script
exe	Executable program
fxp	Microsoft Visual FoxPro compiled program
hlp	Windows Help file
hta	HTML program
inf	Setup information file
ins	Internet Naming Service
isp	Internet communication settings
js	JavaScript file
lnk	Windows shortcut link
jse	JScript Encoded Script file
ksh	KornShell script file
lnk	Shortcut
mda	Microsoft Access add-in program
mdb	Microsoft Access program
mdt	Microsoft Access workgroup information
mdw	Microsoft Access workgroup information
mde	Microsoft Access MDE database
mdz	Microsoft Access wizard program
msc	Microsoft MMC document
msi	Windows Installer package
msp	Windows Installer patch
Mst	Visual Test source files
ops	Office XP settings
pcd	Photo CD image

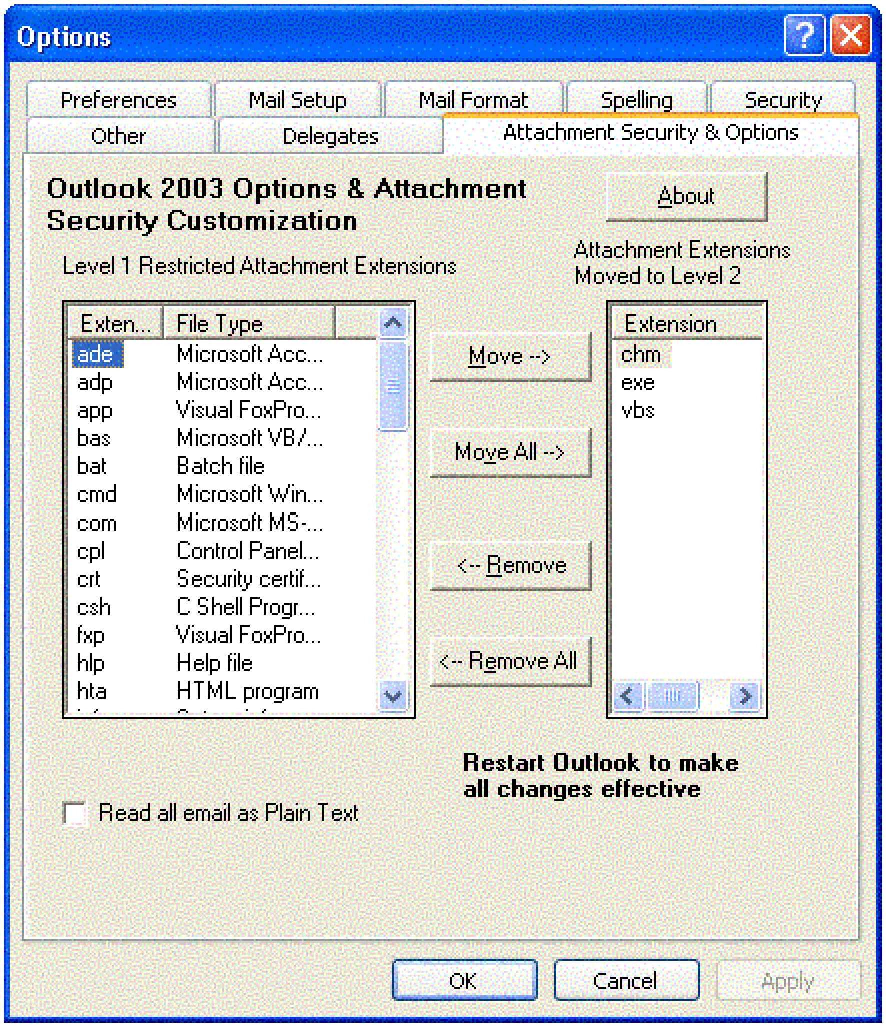
pif	Program information file for DOS programs
prf	Microsoft Outlook profile settings (Outlook 2002 only)
prg	Microsoft Visual FoxPro program
pst	Microsoft Outlook Personal Folders file
reg	registry entries
scf	Windows Explorer command (Outlook 2002 only)
scr	Screensaver file
sct	Windows Script component
shb	Shell scrap object
shs	Shell scrap object
url	Internet shortcut
vb	Visual Basic script
vbe	Visual Basic script encoded script file
vbs	Visual Basic script
wsc	Windows Script component
wsf	Windows Script file
wsh	Windows Scripting Host settings file

Table 2.2: Level-1 attachments blocked by Outlook 2000 SP3 and later.

This list of attachments can be modified by the administrator. As additional attachments present a risk to your organization, the administrator can add attachments to the Level-1 or Level-2 list.

Alternatively, in a standalone environment, or when you need to allow specific users access to certain attachment types, you can download an excellent piece of shareware from Slovak Technical Services that allows you to easily change an attachment from a Level-1 attachment to a Level-2 attachment (see Figure 2.4).

> You can find Outlook 2003 Options and Attachment Security Customizations tool on the Web at http://www.slovaktech.com/attachmentoptions.htm.



Outlook 2003 Options & Attachment Security Customization

Level 1 Restricted Attachment Extensions

Exten...	File Type
ade	Microsoft Acc...
adp	Microsoft Acc...
app	Visual FoxPro...
bas	Microsoft VB/...
bat	Batch file
cmd	Microsoft Win...
com	Microsoft MS-...
cpl	Control Panel...
crt	Security certif...
csh	C Shell Progr...
fxp	Visual FoxPro...
hlp	Help file
hta	HTML program

Attachment Extensions Moved to Level 2

Extension
chm
exe
vbs

Restart Outlook to make all changes effective

□ Read all email as Plain Text

Figure 2.4: Outlook 2003 Options & Attachment Security Customization from Slovak Technical Services.

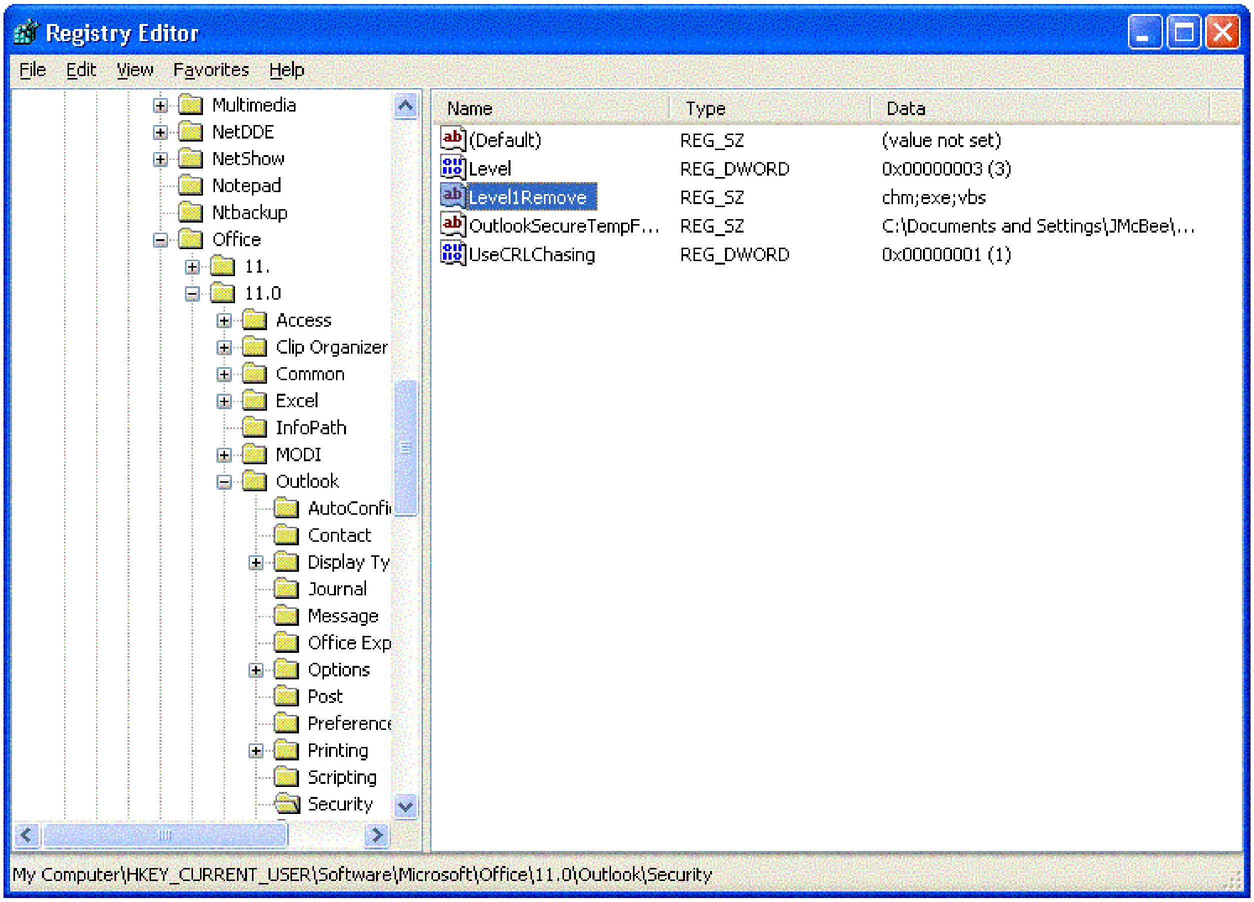
If users are allowed to move some attachments from the Level-1 category to the Level-2 category, then save the attachments to disk, there is still some risk that the attachment contains hostile content. This risk emphasizes the need not only for client-based antivirus software, but also for the need to train users to recognize the signs of potentially hostile content:

- If you don’t know the sender, don’t open the attachment.
- Do not open attachments if you are not expecting an attachment from that user.
- If you receive an attachment from a user that usually does not send you programs or other files that require that the attachment first be saved to the file system, check with that person first before running it.
- Avoid opening attachments that arrive with a message that is trying to entice you to open the attachment (for example, “This is really funny” or “Thought you would enjoy this”).

- Be very careful about attachments that look like documents. By default Windows will “hide” extensions of known file types. A malicious attachment could say something like PerformanceReview.doc.exe. The last extensions (EXE, in this case) would be hidden from Windows. When you save this file to the hard disk, then click on it to open it, the executable would run.
- When in doubt, call the Help desk.

Demoting Attachments to Level-2

If a user has read/write access to the correct registry keys, the user can edit the values that control whether a potentially dangerous attachment is considered a Level-1 or Level-2 attachment. However, this ability is only possible with Outlook 2000 SP3 and later; earlier versions of the Outlook Security Update do not support making these changes. To move a Level-1 attachment to Level-2, locate the following registry key (substitute X for 9.0 for Outlook 2000, 10.0 for Outlook 2002, and 11.0 for Outlook 2003): HKEY_CURRENT_USER\Software\Microsoft\Office\X\Outlook\Security. Create a new value named Level1Remove of type REG_SZ. Enter into that value the extensions (separated by semicolons) of attachments that should not be Level-1 attachments. For example, VBS;CMD;BAT would allow VBScripts, batch files, and command files to be saved to the file system. Figure 2.5 illustrates this registry modification.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Level	REG_DWORD	0x00000003 (3)
Level1Remove	REG_SZ	chm;exe;vbs
OutlookSecureTempF...	REG_SZ	C:\Documents and Settings\JMcBee\...
UseCRLChasing	REG_DWORD	0x00000001 (1)

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security

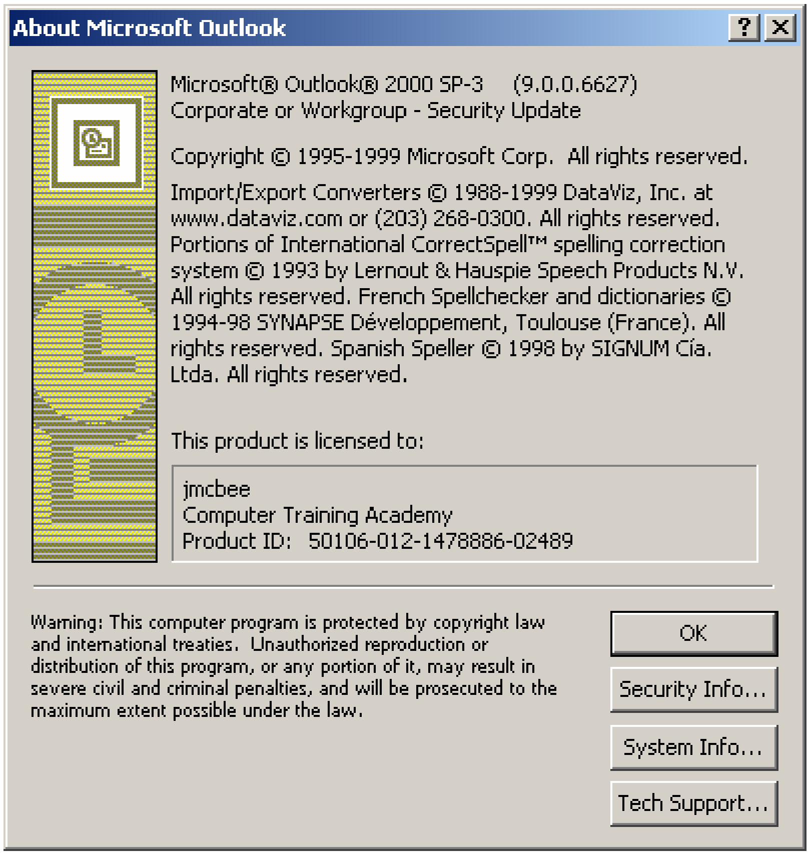
Figure 2.5: Removing CHM, EXE, and VBS file attachments from Level-1.

You might find tips on the Internet suggesting you can get around the Outlook Security Update features by hex-editing outllib.dll or replacing that DLL with one from an earlier version. This workaround is dangerous and if problems arise, Microsoft will not support you.

Installing the Office Update for Outlook 2000

No matter which version of Outlook you're using, I strongly recommend installing the latest service pack. You can confirm that the security fix is in place in Outlook by clicking Help, About. The About Microsoft Outlook dialog box (see Figure 2.6) should indicate Corporate or Workgroup—Security Update directly below the version information. You'll see the same text in the About Microsoft Outlook dialog box of Outlook XP and Outlook 2003.

Microsoft publishes a fairly comprehensive set of documents about deploying Outlook 2000 and later, including information about how to create an administrative shared folder that can be used for mass deployments. You can find this information, along with a link to all of the files necessary (including the Windows installer patch file), at http://www.microsoft.com/office/ork/xp/journ/o2ksp3a.htm.



Microsoft® Outlook® 2000 SP-3 (9.0.0.6627)
Corporate or Workgroup - Security Update

Copyright © 1995-1999 Microsoft Corp. All rights reserved.

Import/Export Converters © 1988-1999 DataViz, Inc. at www.dataviz.com or (203) 268-0300. All rights reserved. Portions of International CorrectSpell™ spelling correction system © 1993 by Lernout & Hauspie Speech Products N.V. All rights reserved. French Spellchecker and dictionaries © 1994-98 SYNAPSE Développement, Toulouse (France). All rights reserved. Spanish Speller © 1998 by SIGNUM Cía. Ltda. All rights reserved.

This product is licensed to:

jmcbee
Computer Training Academy
Product ID: 50106-012-1478886-02489

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 2.6: The About Microsoft Outlook screen indicates whether the security update has been applied.

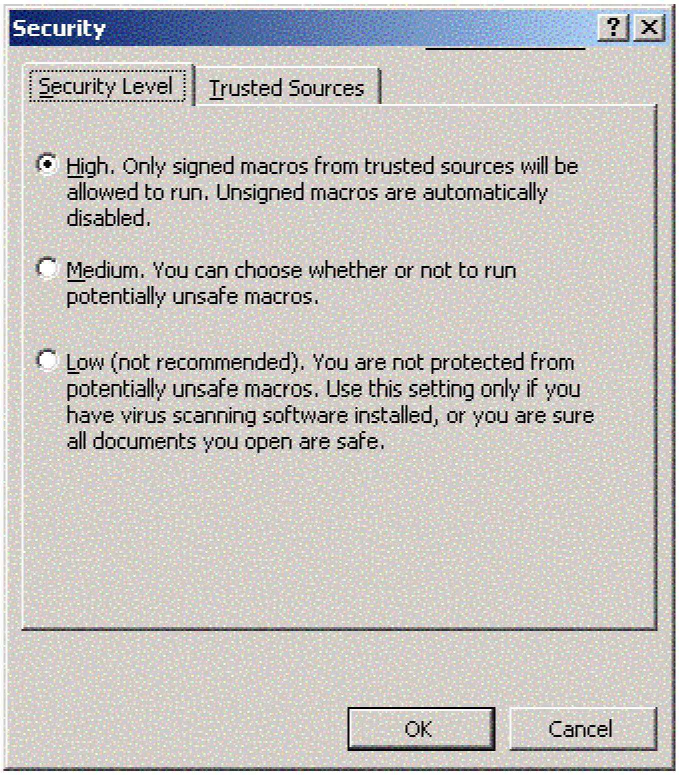
Desktop Configuration Best Practices

Regardless of the client OS or desktop platform, there are several things that you as an administrator should always do. These include:

- Use client-side antivirus software from a different vendor than you use on your Exchange Server systems. Doing so gives you a better chance of catching new viruses because you've now got two (or more) sets of signatures in use during scans.
- Users should never log on to their computers as either a Domain Admin or local Administrator (of course, you should tightly restrict who has these privileges in the first place!).
- Install the current service pack for your version of Internet Explorer (IE—SP2 for IE 5.5, or SP1 for IE 6.0) plus all current hotfixes. Regularly use Windows Update, the Microsoft Baseline Security Analyzer, the Microsoft Software Update Service, or another patch-management tool to keep your systems up to date.
- Only administrators should have NTFS permissions to modify the \Windows and \Program Files folders.
- Use a firewall or scanner that can check the content of incoming attachments.
- Prohibit the use of file-sharing services such as Kazaa, Grokster, and Morpheus on your network.
- Prevent workstations from downloading POP3 or IMAP4 mail from personal ISPs; it may be easiest to do so at the network firewall.
- Configure workstations so that they cannot establish outbound virtual private network (VPN) sessions or inbound VPN/RAS sessions.

Outlook Macro Security

Many of the very first email-based viruses as well as many of the annoying viruses that spread through Windows during the mid-1990s were actually macros. The Microsoft Office family allows developers (and unfortunately virus writers) to write macros using Visual Basic for Applications (VBA). These macros can be embedded into documents, spreadsheets, presentations, and email forms. However, Outlook has three levels of Macro security that let you restrict which macros may be run. You can view these settings in Outlook by clicking Tools, Macro, Security (Figure 2.7 shows the Security dialog box from Outlook 2000—the only change in this screen for Outlook 2003 is that the property tab Trusted Sources is now called Trusted Publishers).



● High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.

○ Medium. You can choose whether or not to run potentially unsafe macros.

○ Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe.

Figure 2.7: Outlook Macro security settings.

Even though the default setting is High, inevitably a user will attempt to run a form that contains an untrusted macro and get an error message. The user will then navigate to the macros security settings and drop the configuration to Low, which is not a good idea and may expose the user to future hostile content. Most users are probably not in a position to determine whether a macro should really be trusted, further they are not in a position to determine trusted publishers.

☞ The Outlook macro security settings only apply to VBA macros, not to VBScripts embedded in custom forms.

If your organization is using VBA macros, you should get your macro digitally signed and added to the Trusted Sources list. Macros that can be placed in the Trusted Sources list must be digitally signed. Outlook will not allow you to publish trusted sources that are not digitally signing their macros. The Exchange organization forms library is considered a trusted source for VBA macros.

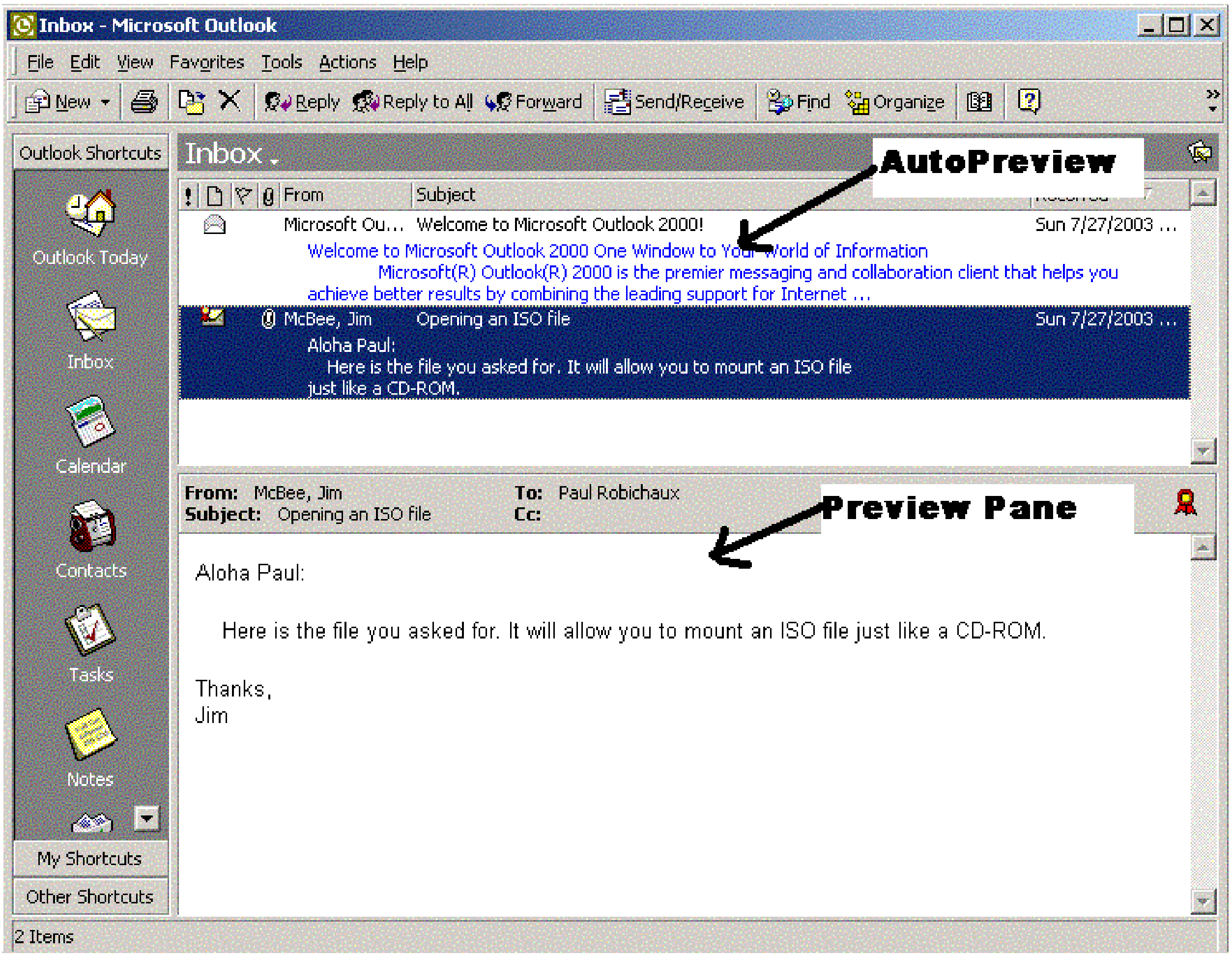
☞ The Outlook macro security settings can be enforced through an AD Group Policy Object (GPO). To do so, you will need the administrative templates from the Office Resource Kit (ORKTOOLS.EXE) found at http://www.microsoft.com/office/ork/xp/appndx/appc00.htm.

Quelling Active Content

I first saw the term *active content* used by security guru Russ Cooper on his Web site (http://www.ntbugtraq.com). He used the term active content with respect to an email message that contains anything besides a plain-text message. This content could be Microsoft Rich Text Formatting, HTML messages, scripts, forms, or ActiveX objects and can be embedded in a message. This content can easily be used for malicious purposes—not only for viruses, but also for worms and Trojan horses, all of which are frequently spread due to the ability of Microsoft's Outlook and Outlook Express clients to support active content.

The Preview Pane

A common question is whether the Preview Pane (called the Reading Pane in Outlook 2003) is vulnerable. The preview pane (if enabled) is the portion of the Outlook window that shows the currently highlighted messages (as Figure 2.8 shows). The short answer is, yes, messages with hostile content can execute if viewed in the preview pane. Viruses and worms such as Klez, Zoher, and HLLW.Pluto can take advantage of the fact that a message is viewed in the Preview Pane.



AutoPreview

Microsoft Ou... Welcome to Microsoft Outlook 2000! Sun 7/27/2003 ...

Welcome to Microsoft Outlook 2000 One Window to Your World of Information
Microsoft(R) Outlook(R) 2000 is the premier messaging and collaboration client that helps you achieve better results by combining the leading support for Internet ...

McBee, Jim Opening an ISO file Sun 7/27/2003 ...

Aloha Paul:
Here is the file you asked for. It will allow you to mount an ISO file just like a CD-ROM.

From: McBee, Jim **To:** Paul Robichaux
Subject: Opening an ISO file **Cc:**

Preview Pane

Aloha Paul:

Here is the file you asked for. It will allow you to mount an ISO file just like a CD-ROM.

Thanks,
Jim

Figure 2.8: The Outlook AutoPreview feature and the Preview Pane.

With Outlook Express and Outlook 98, active content in the preview pane was executed based on the security settings in the IE security zones. Starting with Outlook 2000, ActiveX controls and active scripting items are considered to be disabled in the Preview Pane even if they are enabled in the security zone settings. This configuration will tighten security on potentially harmful message content in the Preview Pane. In certain cases, Outlook will display a dialog box indicating that items in the message can't be displayed in the Preview Pane and telling you to open the message to see all its contents.

Is the Outlook AutoPreview Feature Vulnerable?

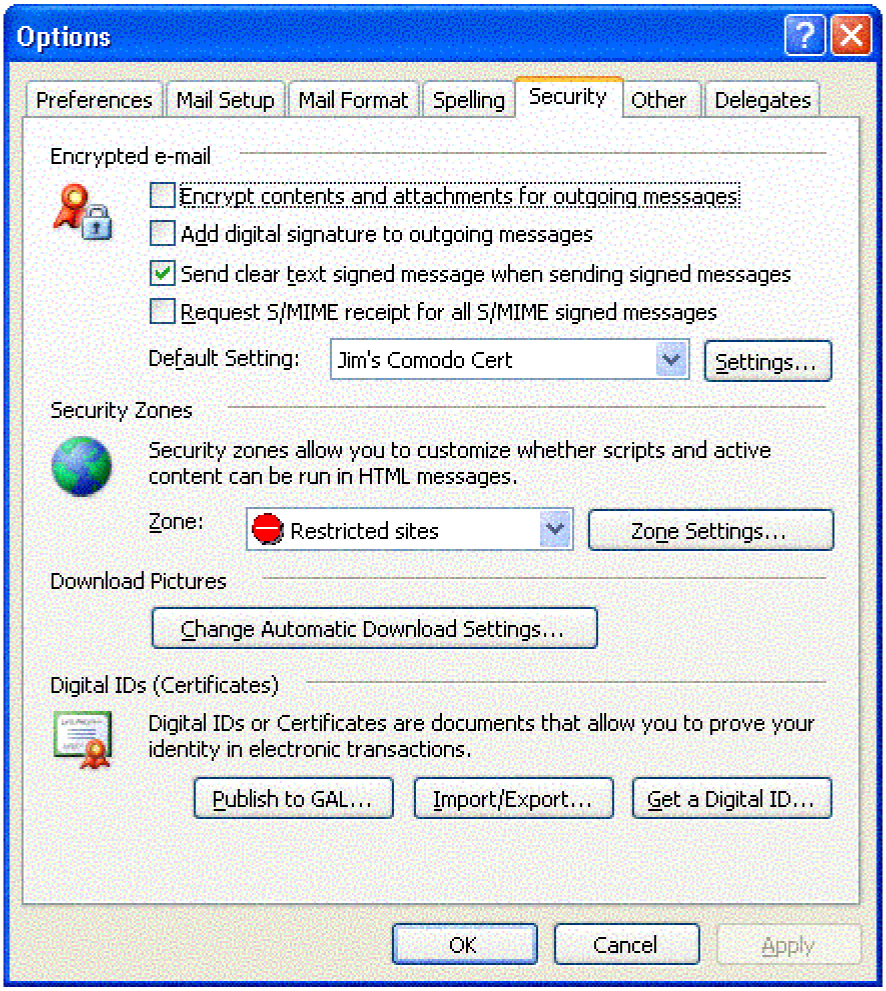
The Outlook AutoPreview feature (which you access by selecting AutoPreview from the Outlook View menu) enables all versions of Outlook to display the first three lines of read (or unread) messages. This text normally appears in blue. When Outlook examines the message, it takes the first three lines of the message text and displays them. It makes no effort to interpret HTML codes, forms, or execute scripts; thus, the AutoPreview pane is safe and not subject to some of the dangers of active content.

☞ If you are running Outlook 2002 or Outlook 2003, the Preview (Reading) Pane can be disabled through an AD GPO.

Viewing the Message

Once a message with active content is opened, the active content (scripts, formatting, links, and s on) are executed and the message is viewed the way the sender intended for it to be viewed. The IE security zone settings enforce how the active content will be executed; the security zone settings also control how IE handles potentially unsafe Internet content. You can configure Outlook to use one of two IE zones when opening messages with active content: the Internet zone or the restricted zone.

For Outlook 2000 with the email security update and later, the default zone is the restricted sites zone. You can change this setting on the Security tab of the Outlook Options dialog box (which you access by selecting Tools, Options, Security), though it is recommended that you leave the zone as restricted sites. Figure 2.9 shows the Outlook 2003 Security options.



☐ Encrypt contents and attachments for outgoing messages

☐ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting: Jim's Comodo Cert

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

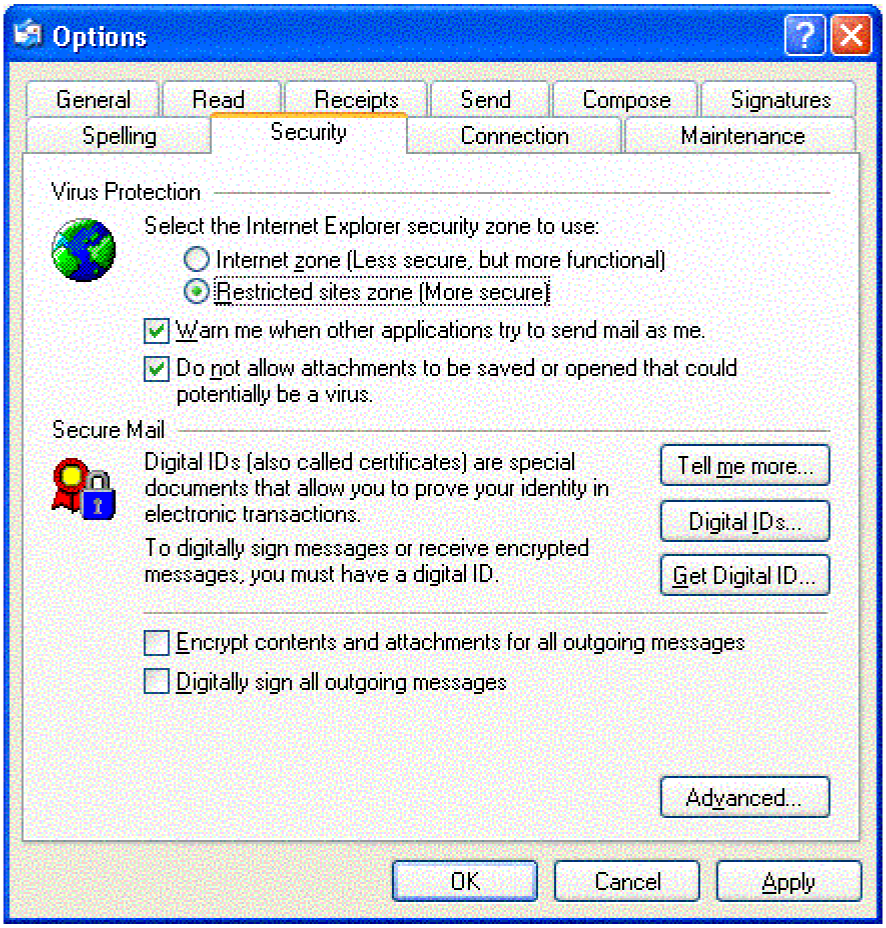
Zone: Restricted sites

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Figure 2.9: Outlook 2003 Security Options.

Outlook Express is configured similarly to Outlook in that you can designate whether email messages are treated as if they are in the Internet zone or the restricted sites zone. Figure 2.10 shows the Tools, Options, Security property options from Outlook Express. Outlook Express should always be configured in the restricted sites zone.

There are two extra check boxes in Outlook Express that you do not find in regular Outlook: the *Warn me when other applications try to send mail as me* check box and the *Do not allow attachments to be saved or opened that could potentially be a virus* check box. Users should be strongly discouraged from clearing these two check boxes because doing so will lower security on Outlook Express attachments.



Virus Protection

Select the Internet Explorer security zone to use:

○ Internet zone (Less secure, but more functional)

● Restricted sites zone (More secure)

☑ Warn me when other applications try to send mail as me.

☑ Do not allow attachments to be saved or opened that could potentially be a virus.

Secure Mail

Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.

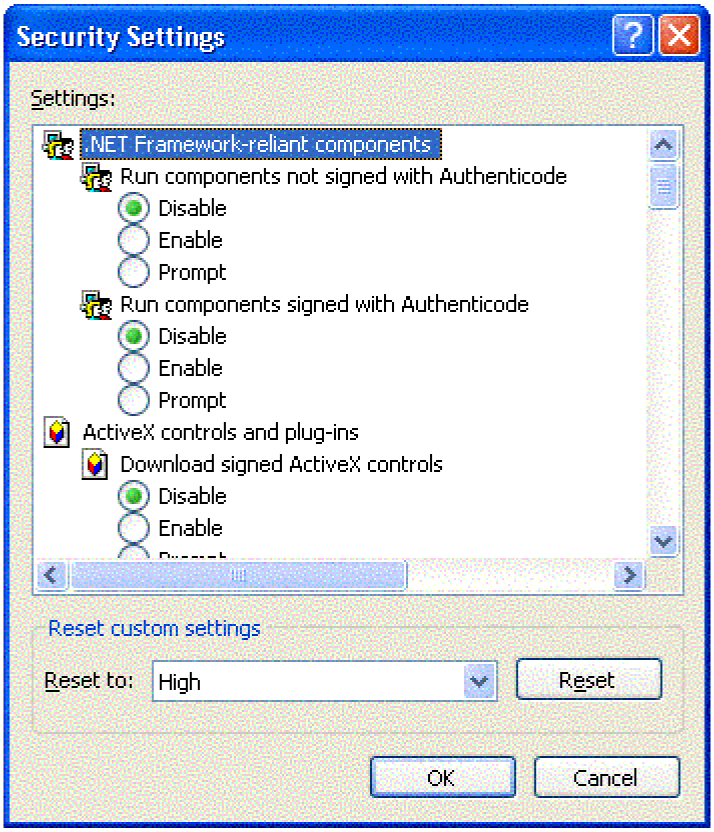
To digitally sign messages or receive encrypted messages, you must have a digital ID.

☐ Encrypt contents and attachments for all outgoing messages

☐ Digitally sign all outgoing messages

Figure 2.10: Outlook Express security options.

The zone settings can either be edited through Outlook or through IE. From within Outlook, select Tools, Options, Security, and click Zone Settings. From within IE, select Tools, Internet Options, Security. Figure 2.11 shows the Security Settings dialog box from the restricted sites security zone.



Settings:

- .NET Framework-reliant components
  - Run components not signed with Authenticode
    - ● Disable
    - ○ Enable
    - ○ Prompt
  - Run components signed with Authenticode
    - ● Disable
    - ○ Enable
    - ○ Prompt
- ActiveX controls and plug-ins
  - Download signed ActiveX controls
    - ● Disable
    - ○ Enable

Reset custom settings

Reset to: High

Figure 2.11: Changing the security settings for the restricted sites security zone.

> ☞ You can configure the security zone settings centrally using an AD GPOs. The settings are found in the User Configuration of the policy in the Windows Settings, Internet Explorer Maintenance, Security section of the policy. You can also deploy custom security zone settings using the Internet Explorer Administration Kit (IEAK).

Determining which security settings are right for your restricted sites security zone will depend on your organization. Table 2.3 contains a list of custom settings that you can apply to your restricted sites zone to lock down the configuration as tightly as possible.

Option	Recommended Setting
Run components not signed with Authenticode (.NET Framework)	Disable
Run components signed with Authenticode (.NET Framework)	Disable
Download signed ActiveX controls	Disable
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe	Disable
Run ActiveX controls and plug-ins	Disable
Script ActiveX controls marked as safe for scripting	Disable
Allow cookies that are stored on your computer	Disable
Allow per-session cookies (not stored)	Disable
File download	Disable
Font download	Disable

Java permissions	Disable Java
Access data sources across domains	Disable
Don’t prompt for client certificate selection when no certificates or only one certificate exists	Disable
Drag and drop or copy and paste files	Disable
Installation of desktop items	Disable
Launching programs within an IFRAME	Disable
Navigate sub-frames across different domains	Disable
Software channel permissions	High safety
Submit non-encrypted form data	Disable
UserData persistence	Disable
Active Scripting	Disable
Allow past operations via script	Disable
Scripting of Java applets	Disable
Logon	Anonymous logon

Table 2.3: Restricted sites security zone settings for secure Outlook configuration.

The settings in this table apply to any site that is in the restricted sites zone, not just to Outlook. The restricted sites zone is just that—it is a zone that contains sites from which you can trust the content.

Reading Messages as Plain Text

I like Rich Text and HTML formatting in messages. Embedding text formatting, font changes, tables, and graphics into some messages can make them more effective. Unfortunately, as with many other useful technical features, HTML mail has been exploited to deliver malware—it seems like someone always comes along and spoils the party by misusing cool features. If you do not have a complete warm-and-fuzzy feeling after performing the other security steps in this chapter, another, and more extreme, step is to force Outlook to display all unsigned messages as plain text. This feature is only available with Outlook 2002 SP1 and later.

To enable this feature, you must make a registry change. Locate the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\10.0\Outlook\Options\Mail key. In this registry key, add a new REG_DWORD value called ReadAsPlain; set the data for this value to 1. Once enabled and the Outlook client is restarted, the following changes will be noticed for messages that do not have a digital signature:

- Images are now attachments
- Message content loses its formatting (font changes, colors, and so on)

This setting will affect messages both in the Preview Pane and when the message is opened in Outlook. The message is not converted to plain text in the mailbox store, but merely displayed in plain text; the message retains its full content in the mailbox store.

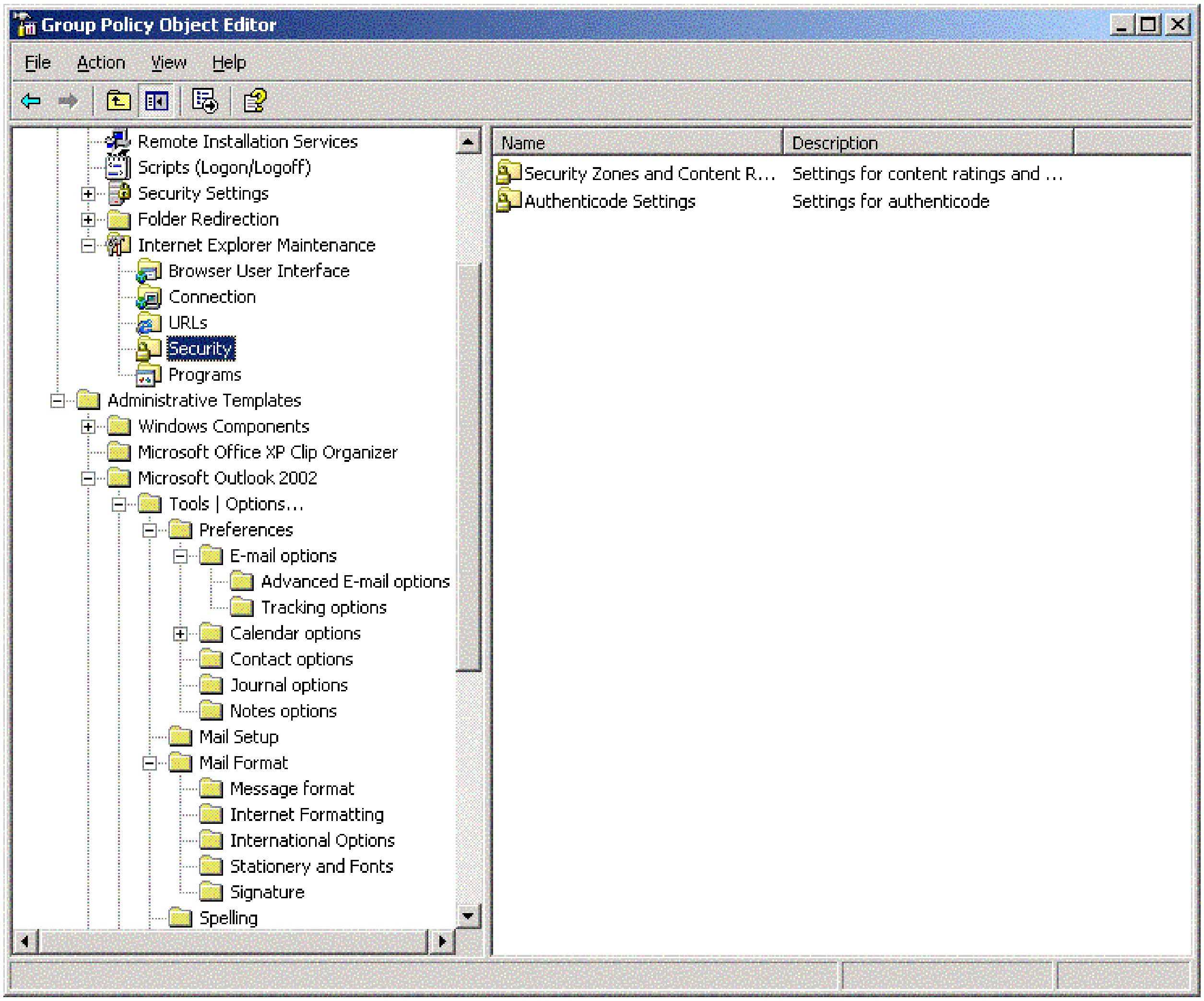
Centralizing Some Client Security Features

If you are the administrator of a few dozen client computers, you probably don't mind manually configuring the security settings and applying updates to these computers. The primary consideration in such situations are your time and making sure that you apply the settings consistently. However, as those few dozen machines turn in to a few hundred or more, manually applying anything is not going to cut it. In this scenario, learning some features of Windows, AD, and Exchange can make your life a lot easier.

AD to the Rescue!

If you are not already familiar with AD GPOs, there is no time like the present. There are a number of things you can do through AD GPOs that can help you to fight viruses and make your email clients more secure:

- The Software Settings GPO option will allow you to automatically deploy antivirus software and Outlook updates to client workstations. As long as the software you want to install is packaged as a Windows Installer (.MSI) file, you can install it to any AD site, domain, or organizational unit (OU).
- Windows startup and shutdown scripts will let you install software and updates that do not have MSI files.
- All versions of Outlook have ADM files (administrative templates) that you can load into a GPO (using the GPO's Administrative Templates component). These ADM files let you apply Outlook settings and prevent end users from changing them via GPO. Outlook 2000, 2002, and 2003 ADM files are found in the Office Resource Kit tools bundle (ORKTOOLS.EXE) for the version of Office that you're running; Outlook 97 and 98 can be found in the Outlook administration kit.
- In the User Configuration node of the GPO, under Windows Settings, Internet Explorer Maintenance, Security (see Figure 2.12), you can deploy custom IE security zones.



Name	Description
Security Zones and Content R…	Settings for content ratings and …
Authenticode Settings	Settings for authenticode

Figure 2.12: Setting security zone information through a GPO.

Using the Outlook Security Features Administrative Package

With the introduction of the Outlook Security Update, there came a need to control the Outlook security features centrally. The Outlook Security Features Administrative Package contains the tools necessary to control these security settings through a form in an Exchange public folder. This public folder can be on an Exchange 5.5, 2000, or 2003 server; Outlook 2000 SR2 and later are hardwired to look for this folder and honor settings found therein.

> ✎ The administrative package will only work if you are using Outlook as the email client and the Outlook mail delivery option is configured to deliver mail to the Exchange server's Inbox.

You can find this package on the Office 2002 resource kit CD-ROM in the \ORK\Files\PFiles\ORKTools\ORK10\Tools\Admpack directory or you can download it from http://www.microsoft.com/office/ork/xp/appndx/appa11.htm.

Before you install the Outlook Security Features Administrative Package, be warned that many of the check boxes and items in the templates actually serve to **lower** security, not improve it. Use it with extreme caution.

Run the ADMPACK.EXE utility and specify a directory to which the files should be installed. Doing so should decompress four files:

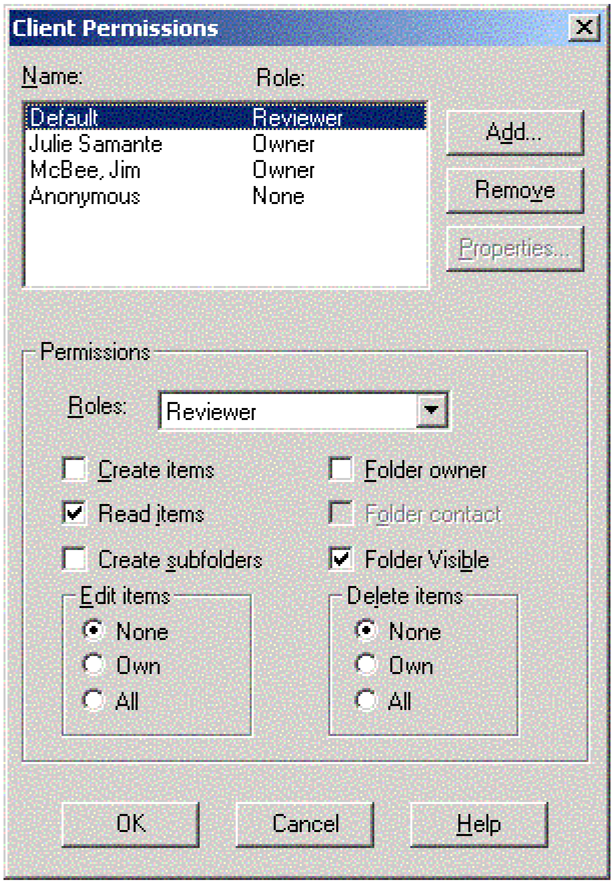
- The readme.doc file contains documentation for how to use the administrative package.
- OutlookSecurity.oft is an Outlook item template that you will need to open and add to the Outlook Security Settings public folder in order to configure the security settings.
- Comdlg32.ocx is a program that is necessary to specify trusted COM add-ins. This file must be copied to the administrator's workstation and placed in the \windows\system32 or \winnt\system32 directory. This ocx file must be registered by typing

  ```
  regsvr32.exe comdlg32.ocx.
  ```

- Hashctl.dll is a dll that is necessary to specify trusted COM add-ins. This file must be copied to the administrator's workstation and placed in the \windows\system32 or \winnt\system32 directory. This dll file must be registered by typing

  ```
  regsvr32.exe hashctl.dll.
  ```

Next, create a folder in the root of the public folder hierarchy called either Outlook Security Settings (for Outlook 2000) or Outlook 10 Security Settings (for Outlook XP and Outlook 2003). This folder must be exactly one of these two names and it must be in the root of the public folder tree. You can have both folders, in which case you can apply separate settings to the two client families; however, doing so might end up causing confusion for your users and thus hassles for you. Change the folder's permissions so that the administrator has full control of the folder, Default has Reviewer permission, and Anonymous has None, as Figure 2.13 illustrates.



Name:	Role:
Default	Reviewer
Julie Samante	Owner
McBee, Jim	Owner
Anonymous	None

Permissions

Roles: Reviewer

□ Create items □ Folder owner

☑ Read items □ Folder contact

□ Create subfolders ☑ Folder Visible

Edit items: ● None ○ Own ○ All

Delete items: ● None ○ Own ○ All

Figure 2.13: Client permissions for the Outlook Security Settings folder.

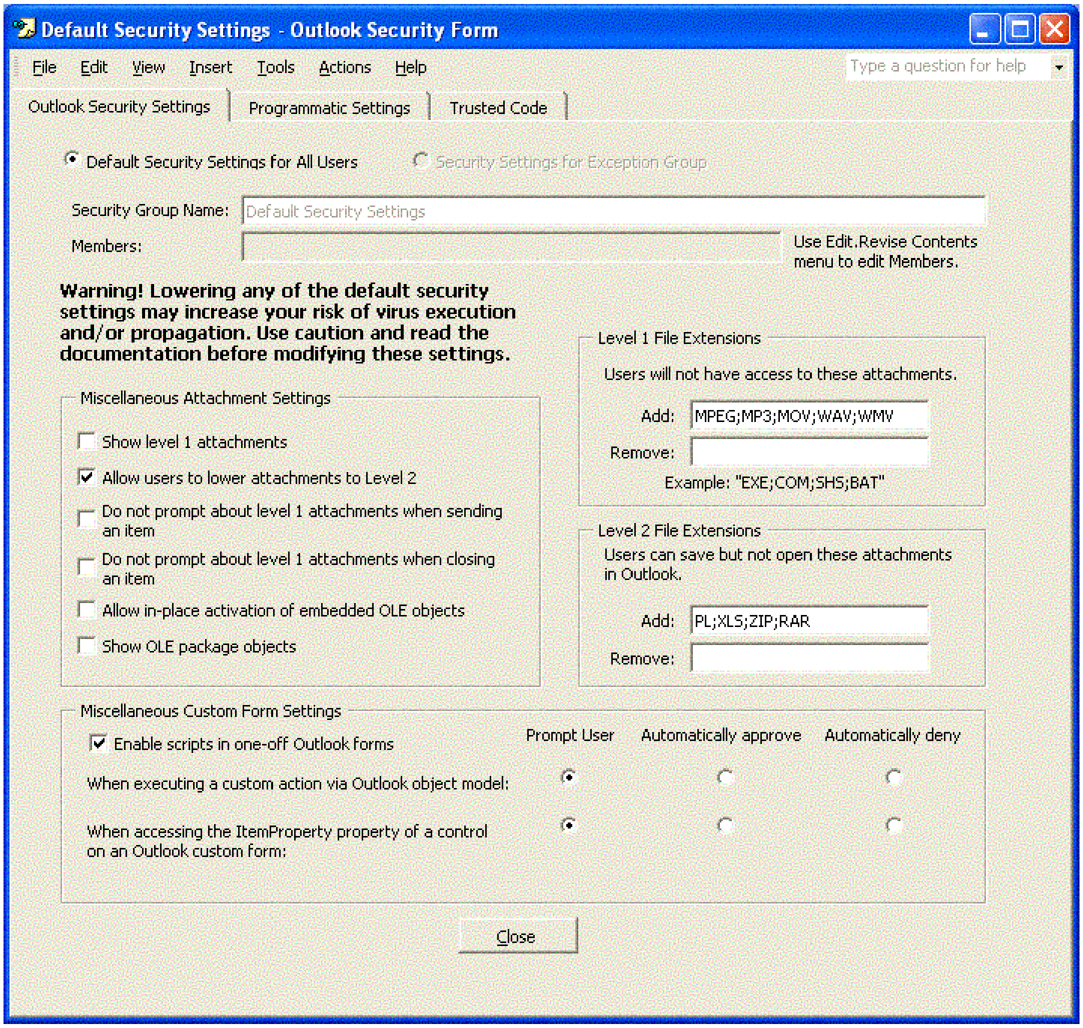
You now need to get the form published into the public folder's forms list. To do so, follow these steps:

1. On the client computer on which you registered the hashctl.dll and comdlg32.ocx files, double-click the OutlookSecurity.oft file.
2. Specify the folder name you created in the root of the public folder tree. You should now see the Default Security Settings form.
3. From the form's Tools menu, select Forms, Publish Form.
4. In the Look In drop-down list box, select the name of the public folder (Outlook Security Settings or Outlook 10 Security Settings)
5. In the Display Name enter

   ```
   Outlook Security Form
   ```

   the Form Name will automatically be filled in.
6. Click Publish.
7. Close the form without saving changes.

You are now ready to create custom Outlook security settings. To create a new form, highlight the Outlook Security Settings folder, and select Actions, New Outlook Security Form. Figure 2.14 shows the Outlook Security Settings property tab of this form. This page mostly controls access to attachments and which attachments are considered Level-1 or Level-2 attachments.


Default Security Settings - Outlook Security Form
File Edit View Insert Tools Actions Help
Type a question for help
Outlook Security Settings
Programmatic Settings
Trusted Code
Close

● Default Security Settings for All Users ○ Security Settings for Exception Group

Security Group Name: Default Security Settings

Members:

Use Edit.Revise Contents menu to edit Members.

Warning! Lowering any of the default security settings may increase your risk of virus execution and/or propagation. Use caution and read the documentation before modifying these settings.

Miscellaneous Attachment Settings

- □ Show level 1 attachments
- ☑ Allow users to lower attachments to Level 2
- □ Do not prompt about level 1 attachments when sending an item
- □ Do not prompt about level 1 attachments when closing an item
- □ Allow in-place activation of embedded OLE objects
- □ Show OLE package objects

Level 1 File Extensions

Users will not have access to these attachments.

Add: MPEG;MP3;MOV;WAV;WMV

Remove:

Example: "EXE;COM;SHS;BAT"

Level 2 File Extensions

Users can save but not open these attachments in Outlook.

Add: PL;XLS;ZIP;RAR

Remove:

Miscellaneous Custom Form Settings

☑ Enable scripts in one-off Outlook forms

	Prompt User	Automatically approve	Automatically deny
When executing a custom action via Outlook object model:	●	○	○
When accessing the ItemProperty property of a control on an Outlook custom form:	●	○	○

Figure 2.14: The Outlook Security Settings form.

As I previously mentioned, understanding these settings is important before you implement this template because most configuration options on this template reduce security rather than increasing it.

📖 Much of the Outlook Security Settings template refers to Level-1 attachments. See Table 2.2 earlier in this chapter for a partial listing of the attachments that are considered Level-1 by default.

When you create a form, you are either creating a form that will apply to everyone or a form that applies to a specific group of users. If the radio button *Default Security Settings for All Users* is selected, the form applies to everyone. However, if you create a form in which the *Security Settings for Exception Group* option is selected, you will be able to specify a list of email aliases in the Members list to which this template is specifying exceptions to the default. The Miscellaneous Attachment Settings section of this form controls the types of attachments to which the user has access. Table 2.4 lists these settings and provides a description of each.

Setting	Description
Show level 1 attachments	The setting name is deceiving. If selected, this setting **allows** users access to the attachment. Selecting this check box will *lower* attachment security!
Allow users to lower attachments to Level 2	Lets the user demote Level-1 attachments to Level-2 attachments by either changing the registry value that contains these attachments or by using a third-party tool (such as Slovak Technical Services' Attachment Options tool). Without this setting, users can still make the client-side changes, but Outlook will ignore them. Selecting this check box may allow users to *lower* attachment security that you did not want lowered.
Do not prompt about level 1 attachments when sending an item	Disables the warning users receive when they send a message that includes a Level-1 attachment. Selecting this check box stops the warning messages; users should always get warning messages to remind them before they send potentially unsafe attachments.
Do not prompt about level 1 attachments when closing an item	Disables the warning users get when they close a message that includes a Level-1 attachment. Selecting this check box stops the warning messages; users should always be reminded when they are storing a potentially unsafe message.
Allow in-place activation of embedded OLE objects	Enables the ability for OLE embedded attachments to be opened if the user double-clicks the attachment (such as an Excel spreadsheet or PowerPoint presentation). If Word is selected as the email editor, embedded Word documents will always open regardless of this setting. This setting can compromise attachment security if any malware has managed to propagate as an OLE attachment.
Show OLE package objects	Allows the OLE objects that have been packaged to show. This setting exists because it is easy to change the icon of an embedded package and thus disguise something that might really be dangerous.

Table 2.4: Miscellaneous attachment settings.

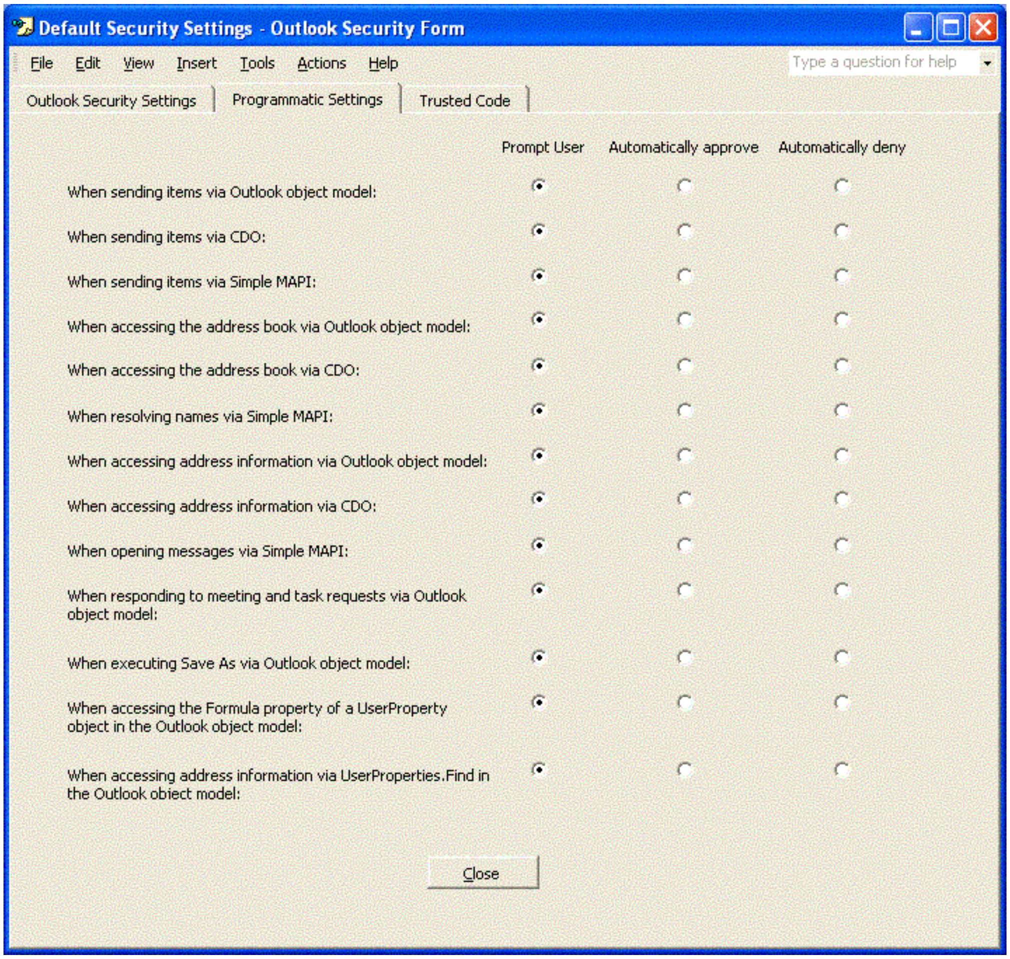
On the right side of the template are the Level-1 and Level-2 File Extensions sections. From these sections, you can add or remove extensions from the default Level-1 file list. As you will recall, Level-1 attachments cannot be opened or saved from within the Outlook client. The Level-2 list is for files that must be saved to the hard disk or shared storage before they can be opened. This setting is useful if you decide that document types that can have embedded macros (DOC, XLS, PPT, and so on) should be saved to hard disk and not retrieved directly from the email message.

At the bottom of the form is the Miscellaneous Custom Form Settings section. These settings control the behavior of Outlook when custom controls are added to an Outlook form. Table 2.5 lists the settings and describes what each setting does.

Setting	Description
Enable scripts in one-off Outlook forms	A one-off form is a form that is contained within the message rather than in a personal, folder, or organization forms library. This setting enables the use of one-off forms if your users receive messages that include the form itself. Ideally, forms should be stored in a trusted location (such as the Exchange organization forms library), but this setting may have to be enabled if your users receive messages that include forms from outside organizations. If this occurs regularly, take steps to get copies of the forms, validate them, and store them in your own organization forms library.
When executing a custom action via the Outlook object model	This setting specifies what happens when a custom form is using the Outlook object model: • Prompt User—The user receives a dialog box that states that the Outlook object model is being used by a program and asks whether this is okay. • Automatically approve—Custom forms can automatically access the Outlook object model. • Automatically deny—Custom forms will automatically be blocked from using the Outlook object model.
When accessing the ItemProperty property of a control on an Outlook custom form	This setting specifies what happens when a custom control is included in a form, and the control attempts to access the address field of the message: • Prompt User—The user receives a dialog box that states that a program is attempting to access properties which could give that program access to the address book. • Automatically approve—Custom forms can automatically access the Outlook ItemProperty. • Automatically deny—Custom forms will automatically be blocked from using the Outlook ItemProperty.

Table 2.5: Miscellaneous custom form settings.

The next dialog box on the Outlook Security Settings template is the Programmatic Settings, which Figure 2.15 shows. The default setting for each of these programmatic settings is to allow the user to designate whether the Outlook add-in or third-party application works.



Default Security Settings - Outlook Security Form
File Edit View Insert Tools Actions Help
Type a question for help
Outlook Security Settings
Programmatic Settings
Trusted Code
Close

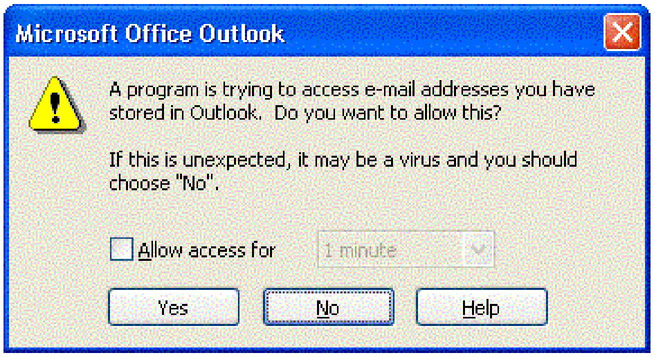
	Prompt User	Automatically approve	Automatically deny
When sending items via Outlook object model:	●	○	○
When sending items via CDO:	●	○	○
When sending items via Simple MAPI:	●	○	○
When accessing the address book via Outlook object model:	●	○	○
When accessing the address book via CDO:	●	○	○
When resolving names via Simple MAPI:	●	○	○
When accessing address information via Outlook object model:	●	○	○
When accessing address information via CDO:	●	○	○
When opening messages via Simple MAPI:	●	○	○
When responding to meeting and task requests via Outlook object model:	●	○	○
When executing Save As via Outlook object model:	●	○	○
When accessing the Formula property of a UserProperty object in the Outlook object model:	●	○	○
When accessing address information via UserProperties.Find in the Outlook object model:	●	○	○

Figure 2.15: Programmatic Settings options.

The Programmatic Settings page lets the administrator specify the behavior of Outlook when third-party add-ins, forms, and external applications attempt to use CDO, the Outlook object model, or MAPI functions. The default configuration for each of these 13 settings is to prompt the user when one of these actions is taking place. How you configure these settings is determined by whether you trust your users to think before they allow a program to use the Outlook address book, and so on. For organizations that are connected to public email systems, these settings should never be configured to Automatically approve.

There are three options for each of these settings:

- Prompt user—The user receives a message stating that a particular application is attempting to use a programmatic feature of Outlook. The user can either say it is okay or deny the operation. Some of the prompts allow the user to specify how long the application can have access to Outlook (see Figure 2.16).
- Automatically approve—External applications will automatically be allowed programmatic access to Outlook.
- Automatically deny—External applications will automatically be blocked from programmatic access to Outlook.



A program is trying to access e-mail addresses you have stored in Outlook. Do you want to allow this?

If this is unexpected, it may be a virus and you should choose "No".

□ Allow access for 1 minute

Figure 2.16: Outlook users are prompted when an external program programmatically attempts to access Outlook.

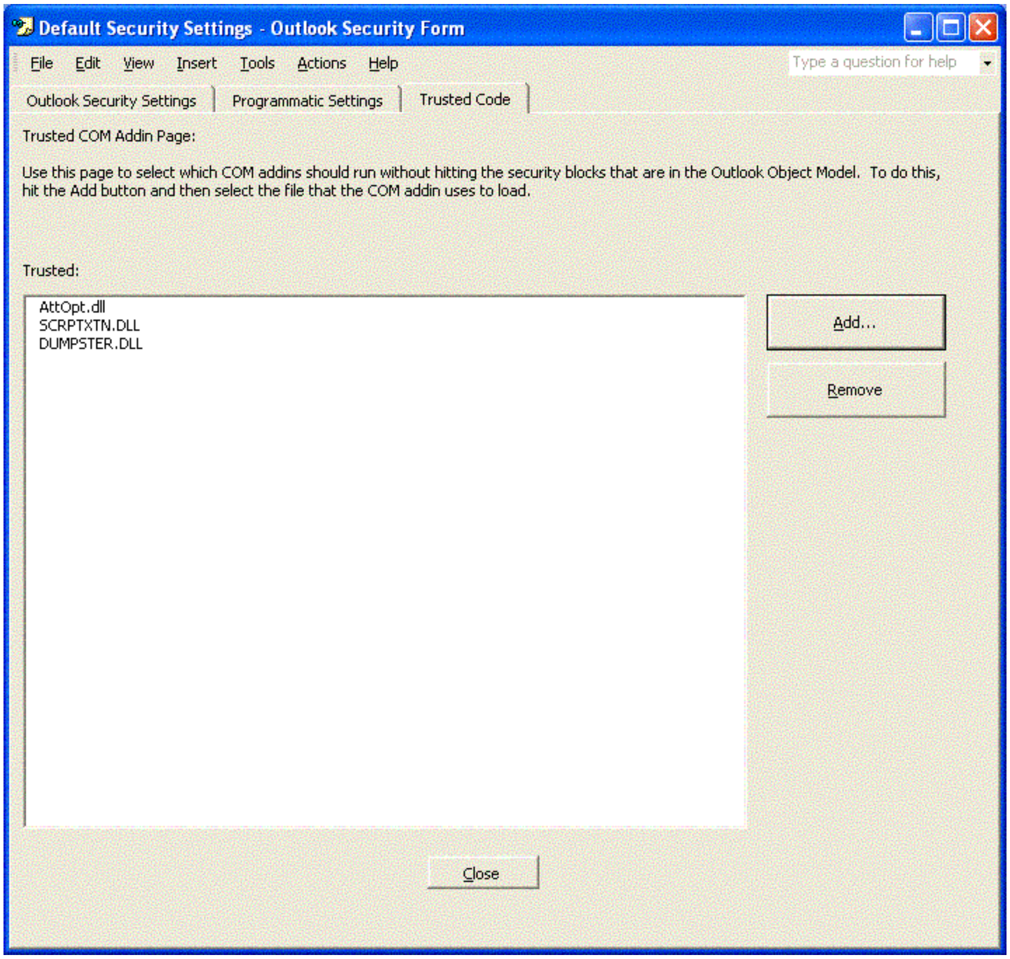
Table 2.6 provides information about each of the settings.

Setting	Description
When sending items via Outlook object model	Affects behavior of Outlook when an application attempts to programmatically use the Outlook object model to send a message
When sending items via CDO	Affects the behavior of Outlook when an application attempts to send mail programmatically using CDO
When sending items via Simple MAPI	Affects the behavior of Outlook when an application uses Simple MAPI function calls to send a message
When accessing the address book via Outlook object model	Affects the behavior of Outlook when an application attempts to gain access to the Outlook address book via the Outlook object model
When accessing the address book via CDO	Affects the behavior of Outlook when an application attempts to gain access to the Outlook address book via CDO
When resolving names via Simple MAPI	Affects the behavior of Outlook when an application attempts to gain access to the Outlook address book via Simple MAPI
When accessing address information via Outlook object model	Affects the behavior of Outlook when an application attempts to gain access to a message's addressing properties (To, From, CC, and so on) via the Outlook object model
When accessing address information via CDO	Affects the behavior of Outlook when an application attempts to gain access to a message's addressing properties (To, From, CC, and so on) via CDO
When opening messages via Simple MAPI	Affects the behavior of Outlook when an application attempts to gain access to a message's addressing properties (To, From, CC, and so on) via Simple MAPI
When responding to meeting and task requests via Outlook object model	Affects the behavior of Outlook when an application attempts to manipulate meeting and task requests via the Outlook object model
When executing Save As via the Outlook object model	Affects the behavior of Outlook when an application attempts to use the Save As feature using the Outlook object model
When accessing the Formula property of a UserProperty object in the Outlook object model	Affects the behavior of Outlook when an application attempts to access the UserProperty object's Formula property using the Outlook object model

Table 2.6: Programmatic settings options.

For more information about CDO, MAPI, and the Outlook object model, visit http://msdn.microsoft.com/office.

Finally, the Trusted Code property page is used to specify custom and third-party add-ins that should be trusted by Outlook. These trusted COM add-ins can run without hitting the restrictions placed on them through the Programmatic Settings Outlook object model restrictions. Figure 2.17 shows the Trusted Code list. Simply specify the names of the DLLs that are provided by the vendor or developer of the third-party COM add-in.



Trusted COM Addin Page:

Use this page to select which COM addins should run without hitting the security blocks that are in the Outlook Object Model. To do this, hit the Add button and then select the file that the COM addin uses to load.

Trusted:

AttOpt.dll
SCRPTXTN.DLL
DUMPSTER.DLL

Figure 2.17: Trusted Code list.

Where Are My Custom Settings?

There is one final step that you need to take in order to make the Outlook Security Settings work for Outlook clients. You need a registry setting that instructs Outlook to check the public folder for the Outlook Security Settings templates. Locate the HKEY_CURRENT_USER\Software\Policies\Microsoft\Security registry key (you might need to create the Security subkey if it does not exist). In this key, create a REG_DWORD value called CheckAdminSettings. Set the data to one of three settings:

- A value of 0—Use the default settings, which means it does not consult the public folders
- A value of 1—Use the custom settings found in the Outlook Security Settings folder
- A value of 2—Use the custom settings found in the Outlook 10 Security Settings folder

Final Thoughts About Outlook Security Settings

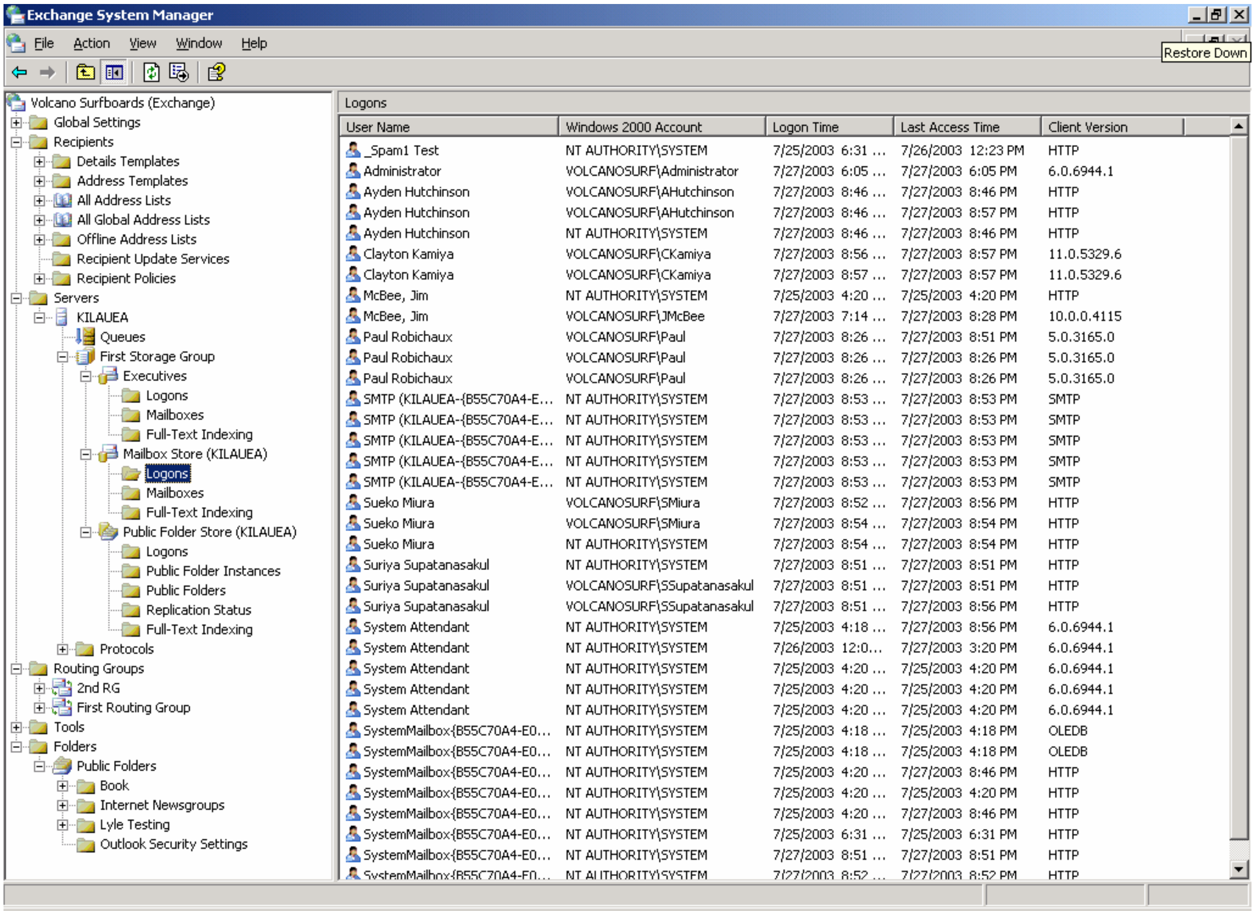
A couple of parting thoughts about the Outlook Security Settings feature that I want you to keep in mind when you implement this feature:

- Many of these settings can easily undo any additional security settings that you may have gained with the Outlook Security Update or by installing later versions of Outlook
- The template should work fine for Outlook 2000 SP3 and later
- The public folder that holds this template should be replicated so that it is accessible in all Exchange sites or routing groups
- When you save a template, you are prompted for your credentials twice; enter your credentials both times
- Finally, test your features thoroughly on a test system before introducing it into production; make sure that all custom messaging applications work properly

Using Exchange Server to Control Outlook Client Versions

Exchange 2000 SP1 introduced a new feature that allows the administrator to restrict access to the Exchange Server system based on the MAPI version of the Outlook client. This feature is also supported on Exchange Server 2003. I find this feature extremely useful if I decide that I only want a specific set of client versions to be allowed to use the Exchange Server. For example, perhaps I only want Outlook clients that are running Outlook 2000 SP3 or later to be able to use Exchange; this configuration will help to guarantee that client-side precautions are being taken. You can even constrain the versions so that only a specific range of versions are allowed and nothing later than that version. This configuration can ensure that no one installs an Outlook client that has not yet been approved and tested (for example, if you want to prohibit anyone from installing a beta version of Outlook 2003).

The feature must be enabled in the registry of each Exchange Server, and you must know the exact MAPI versions of the client according to the Exchange Server. Simply looking in the Outlook client's Help, About screen will not give you the information you need. I found this information by connecting to the Exchange Server using different versions of the MAPI client, then recording the information found in the Exchange mailbox store's Logons container (see Figure 2.18).



User Name	Windows 2000 Account	Logon Time	Last Access Time	Client Version
_Spam1 Test	NT AUTHORITY\SYSTEM	7/25/2003 6:31 ...	7/26/2003 12:23 PM	HTTP
Administrator	VOLCANOSURF\Administrator	7/27/2003 6:05 ...	7/27/2003 6:05 PM	6.0.6944.1
Ayden Hutchinson	VOLCANOSURF\AHutchinson	7/27/2003 8:46 ...	7/27/2003 8:46 PM	HTTP
Ayden Hutchinson	VOLCANOSURF\AHutchinson	7/27/2003 8:46 ...	7/27/2003 8:57 PM	HTTP
Ayden Hutchinson	NT AUTHORITY\SYSTEM	7/27/2003 8:46 ...	7/27/2003 8:46 PM	HTTP
Clayton Kamiya	VOLCANOSURF\CKamiya	7/27/2003 8:56 ...	7/27/2003 8:57 PM	11.0.5329.6
Clayton Kamiya	VOLCANOSURF\CKamiya	7/27/2003 8:57 ...	7/27/2003 8:57 PM	11.0.5329.6
McBee, Jim	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/25/2003 4:20 PM	HTTP
McBee, Jim	VOLCANOSURF\JMcBee	7/27/2003 7:14 ...	7/27/2003 8:28 PM	10.0.0.4115
Paul Robichaux	VOLCANOSURF\Paul	7/27/2003 8:26 ...	7/27/2003 8:51 PM	5.0.3165.0
Paul Robichaux	VOLCANOSURF\Paul	7/27/2003 8:26 ...	7/27/2003 8:26 PM	5.0.3165.0
Paul Robichaux	VOLCANOSURF\Paul	7/27/2003 8:26 ...	7/27/2003 8:26 PM	5.0.3165.0
SMTP (KILAUEA-{B55C70A4-E...	NT AUTHORITY\SYSTEM	7/27/2003 8:53 ...	7/27/2003 8:53 PM	SMTP
SMTP (KILAUEA-{B55C70A4-E...	NT AUTHORITY\SYSTEM	7/27/2003 8:53 ...	7/27/2003 8:53 PM	SMTP
SMTP (KILAUEA-{B55C70A4-E...	NT AUTHORITY\SYSTEM	7/27/2003 8:53 ...	7/27/2003 8:53 PM	SMTP
SMTP (KILAUEA-{B55C70A4-E...	NT AUTHORITY\SYSTEM	7/27/2003 8:53 ...	7/27/2003 8:53 PM	SMTP
SMTP (KILAUEA-{B55C70A4-E...	NT AUTHORITY\SYSTEM	7/27/2003 8:53 ...	7/27/2003 8:53 PM	SMTP
Sueko Miura	VOLCANOSURF\SMiura	7/27/2003 8:52 ...	7/27/2003 8:56 PM	HTTP
Sueko Miura	VOLCANOSURF\SMiura	7/27/2003 8:54 ...	7/27/2003 8:54 PM	HTTP
Sueko Miura	NT AUTHORITY\SYSTEM	7/27/2003 8:54 ...	7/27/2003 8:54 PM	HTTP
Suriya Supatanasakul	NT AUTHORITY\SYSTEM	7/27/2003 8:51 ...	7/27/2003 8:51 PM	HTTP
Suriya Supatanasakul	VOLCANOSURF\SSupatanasakul	7/27/2003 8:51 ...	7/27/2003 8:51 PM	HTTP
Suriya Supatanasakul	VOLCANOSURF\SSupatanasakul	7/27/2003 8:51 ...	7/27/2003 8:56 PM	HTTP
System Attendant	NT AUTHORITY\SYSTEM	7/25/2003 4:18 ...	7/27/2003 8:56 PM	6.0.6944.1
System Attendant	NT AUTHORITY\SYSTEM	7/26/2003 12:0...	7/27/2003 3:20 PM	6.0.6944.1
System Attendant	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/25/2003 4:20 PM	6.0.6944.1
System Attendant	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/25/2003 4:20 PM	6.0.6944.1
System Attendant	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/25/2003 4:20 PM	6.0.6944.1
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 4:18 ...	7/25/2003 4:18 PM	OLEDB
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 4:18 ...	7/25/2003 4:18 PM	OLEDB
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/27/2003 8:46 PM	HTTP
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/25/2003 4:20 PM	HTTP
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 4:20 ...	7/27/2003 8:46 PM	HTTP
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/25/2003 6:31 ...	7/25/2003 6:31 PM	HTTP
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/27/2003 8:51 ...	7/27/2003 8:51 PM	HTTP
SystemMailbox{B55C70A4-E0...	NT AUTHORITY\SYSTEM	7/27/2003 8:52 ...	7/27/2003 8:52 PM	HTTP

Figure 2.18: Determining the MAPI client version.

The MAPI version number looks much like an IP address, except that each decimal place is a 16-bit number, so the range can be between 0 and 65,535. The number is in the form of *W.X.Y.Z.* Table 2.7 shows the MAPI client version. The value you actually need in the registry is in the Value Required to Restrict Logon column. When determining which version number to put in to the Disable MAPI Clients registry value, use only the W.Y.Z format (leave out the X).

Table 2.7 is by no means inclusive of all MAPI clients because each service release and security fix may update this version number. In addition, the version in Help, About does not always agree with the version the server sees.

Client	Help About Version	MAPI Version	Value Required to Restrict Logon
Exchange 4 Inbox Client	4.0.993.3	4.0.993.3	4.993.3
Exchange 5 Inbox Client	5.0.1457.3	5.0.1457.3	5.1457.3
Outlook 97 (from Office 97 CD-ROM)	8.02.4212	5.0.1457.3	5.1457.3
Outlook 97 8.03 (with Exchange 5.5)	8.03.4629	5.0.1960.0	5.1960.0
Outlook 98	8.5.5104.6	5.0.2178.0	5.2178.0
Outlook 2000 (with Office 2000)	9.0.0.2711	5.0.2819.0	5.2819.0
Outlook 2000 SR-1	9.0.0.3821	5.0.3121.0	5.3121.0
Outlook 2000 SR-1 (after Office 2000 SP2 applied)	9.0.0.4527	5.0.3144.0	5.3144.0
Outlook 2000 SR-1 with the Security Update	9.0.0.5414	5.0.3158.0	5.3158.0
Outlook 2000 SP3	9.0.0.6627	5.0.3165.0	5.3165.0
Outlook 2002	10.2627.2625	10.0.0.2627	10.0.2627
Outlook 2002 SP1	10.3513.3501	10.0.0.3416	10.0.3416
Outlook 2002 SP2	10.4219.4219	10.0.0.4115	10.0.4115
Outlook 2003 SP2 January 2003 Update	10.4712.4219	10.0.0.4115	10.0.4115
Outlook 2003 Beta 2	11.5329.5329	11.0.5329.6	11.5329.6
Exchange 2000 SP1 components	N/A	6.0.4712.0	6.4712.0
Exchange 2003 components	N/A	6.0.6944.1	6.6944.1

Table 2.7: MAPI client and Outlook versions.

To restrict access to MAPI clients you will need to locate the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\Parameters System registry key. In this key, create a valued named Disable MAPI Clients of type REG_SZ. You then populate this value with the list of MAPI client versions that are not allowed to access the server.

> ☞ The MAPI version 6 components must always be allowed to log on. These are Exchange 2000 and Exchange 2003 components such as the System Attendant.

You can mix and match values in the registry key to allow certain ranges of clients to access the information store. Additionally, you can put in multiple values by separating them with commas. Table 2.8 provides some examples of restrictions you can place on MAPI clients.

Registry Value	Effective Results on MAPI Clients
`-6.0.0, 7.0.0-`	Allows only the Exchange 2000 or Exchange 2003 components to access the information store by blocking all clients before version 6 and all clients after version 7.
`10.0.2627`	Prevents the original release of Outlook XP clients from accessing the store.
-5.3165.0	Prevents any clients prior to Outlook 2000 SP3 from accessing the store.
`4.993.3–5.1457.3`	Prevents Exchange 4, 5, and original Outlook 97 clients from accessing the store.
–-5.3165.0, 10.0.4115 -	Allows only clients between Outlook 2003 SP3 and Outlook 2002 SP2.

Table 2.8: Examples that you can use in the `Disable MAPI Clients` registry value.

Once this registry value is in place and the information store has been stopped and restarted, clients will get a *The attempt to log on to the Microsoft Exchange Server computer has failed* message if they try to access the Exchange Server from a client whose MAPI version you are blocking. If you allow only very specific versions of MAPI clients, you will have to remember to always update this if you update the MAPI client version.

Summary

You can achieve and maintain client-side email security with a minimal loss of functionality as long as you have a good sense of the security components you need to put in place and as long as end users remain diligent to potential security threats. When designing a client-side email scheme, keep the following considerations in mind:

- All client computers should have up-to-date antivirus software installed—no exceptions!
- Desktop OSs should remain reasonably up-to-date on OSs and service packs. If you are running Windows NT Workstation 3.51 or Windows 98, it is time to consider an upgrade. If you have not applied OS and browser critical updates in the past 2 months, it is time to apply them.
- Email client software should be updated with the latest security patches available. If you are running Outlook 97 or Outlook Express 4.0, it is time to consider upgrading.

In the next chapter, we'll explore what you can do to help protect your server—and the messaging resources and services it offers to clients—from viruses, worms, and malware.