realtimepublishers.com®

The Definitive Guide™ To

Securing Windows in the Enterprise

SCRIPTLOGIC

Don Jones

Copyright Statement

[**Editor's Note:** This eBook chapter was downloaded from Content Central. To download other chapters from this eBook, please visit http://cc.realtimepublishers.com/portal.aspx?pubid=335.]

Chapter 3: Using Alternative Software to Reduce Your Attack Surface

Attack surface is an IT security term that refers to the number of ways in which a computer can be attacked. For example, a computer running an older operating system (OS) such as MS-DOS has a relatively low attack surface, because the code base for MS-DOS is so much smaller than that of current OSs and few of today's attack techniques would work against it. A computer running Windows XP Professional, in contrast, has a relatively large attack surface simply because it is such a large, complex OS.

As the previous chapter explored, one way to reduce attack surface is to uninstall software that isn't being used, such as unnecessary services. Local firewalls, such as the Windows Firewall, can also reduce your attack surface by blocking attacks' access to specific applications (such as a local Web server). However, it's still possible in many cases for attacks to get through. Suppose that a Windows XP Professional user has the Windows Firewall turned on full-force, and that user attempts to visit a Web site. The firewall will allow the user to visit the site because the traffic is originating locally and that type of traffic isn't blocked by the firewall. The Web site's content, which comes back as a reply to the locally generated traffic, is also allowed. If that content contains an attack—say a virus or other malware—the attack is allowed into the computer where it can do its damage.

Unfortunately, much of Windows XP's bundled software is rife with security vulnerabilities, allowing numerous types of attacks to be effective (this fact applies to earlier versions of Windows, as well). Thus, a further technique of reducing your attack surface—beyond removing unused software and using a local firewall—is to replace this bundled software with less-vulnerable alternatives.

The Bundled Software

The bundled software that this chapter explores is commonly referred to by Microsoft as *middleware*—those applications that Microsoft has controversially bundled into the OS rather than offering them as standalone packages. These applications include:

- Internet Explorer (IE)
- Windows Messenger (this reference doesn't include the similar MSN Messenger, which isn't bundled with Windows and can be easily uninstalled)
- Windows Media Player
- Outlook Express

> There is some discrepancy regarding the definition of *middleware*. In addition to the version used by Microsoft, which is the definition used for this guide, the term middleware is also used to refer to separate products that serve as the glue between two applications.

These applications are worthy of focus because they are installed by default, are somewhat difficult to actually remove if you're not using them, and provide functionality that most users require. For example, most users need a Web browser and an email client; because IE and Outlook Express are bundled, users might be using those applications to provide the functionality they need. Even if these applications are not being used, however, they present a potential security risk.

Dealing with the issue of bundled software is complex, most particularly in the case of IE. To tackle this topic, let's first explore the specific functionality that you will be missing if you eliminate these bundled applications. Second, we'll discover how to actually remove or disable them to the greatest degree possible. Finally, let's look at alternative applications that provide most, if not all, of the same functionality, and any weaknesses (especially in terms of enterprise management) that the alternatives present.

What About Alternatives to Other Applications?

This chapter isn't intended to be Microsoft-centric; it simply focuses on those applications that are preinstalled by Microsoft, less than straightforward to remove, and offer must-have functionality by virtually all modern users. Certainly, there are alternatives to nearly every application that Microsoft offers, and the manufacturers of those alternatives will be more than happy to tell you how their products work, if you're interested. We'll focus on the Microsoft bundled software because its combination of preinstallation, lack of straightforward removal options, and mission-critical functionality places this software into a special category all its own.

What Will You Miss?

Microsoft's bundled applications do, in most cases, provide unique functionality, both in terms of end-user functionality and enterprise manageability. Doing away with the bundled applications will, in most cases, remove that unique functionality. In some cases, this removal might not affect users—Windows Media Player's unique ability to play Windows Media Video (WMV) files, for example, might not matter to your organization; thus, losing that capability might not be a "loss" to you at all. It is important to simply *know* what functionality is going to go missing when you eliminate these bundled applications so that you can make an informed decision about whether losing that functionality is acceptable.

There is also a middle ground where you don't *eliminate* the bundled applications but simply stop using them as the default. For example, you might choose to use an alternative Web browser as your users' default Web browser. Doing so would help eliminate many of the vulnerabilities associated with IE because those vulnerabilities only work if IE is being used to access Web pages containing an exploit. This method doesn't require you to *remove* IE; you can still leave it available to your users for tasks that require IE's unique functionality.

📖 Later in the chapter, I'll explore this middle ground scenario.

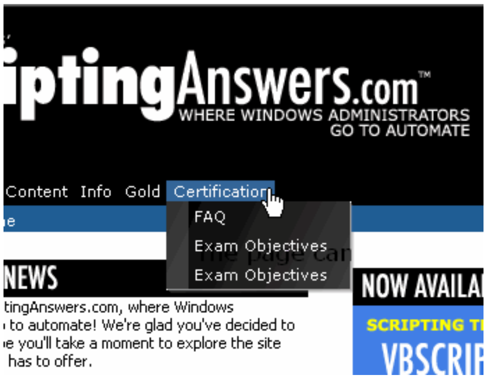
IE

IE has been host to so many security vulnerabilities over the years that it is one of the first bundled applications that enterprises look at for potential removal. Doing so can be difficult. Although few Web sites used by corporate users require IE's unique features, many intranet applications were built around those features.

In terms of user functionality, IE doesn't offer much that can't be replaced by an alternative browser. In fact, most alternatives offer superior user interface (UI) features—such as tabbed browsing—that IE hasn't offered.

> ✎ Microsoft recently announced IE 7.0, which will ship as an update to Windows XP prior to the release of Windows Longhorn; version 7.0 might offer tabbed browsing and other UI enhancements

Most users are receptive to alternative browsers and do well with them; the alternatives work similarly enough to the familiar IE that there is practically no learning curve. There is a small amount of functionality that isn't exactly unique to IE but that IE handles slightly differently than the alternatives. For example, in Figure 3.1 you see a portion of a Web page that is using a Dynamic HTML (DHTML)-generated drop-down menu. Look carefully, and you'll see that the right side of the menu's black background fades into transparency, allowing the underlying page to be glimpsed. This visual effect looks nice, and is essentially unique to IE (at least for now) because it is using Microsoft-designed extensions to Cascading Style Sheets. Although an alternative browser can duplicate the operation of the drop-down menu, it might not duplicate this transparency effect. However, this shortcoming is something few users will notice or mind in most cases.



tingAnswers.com, where Windows
to automate! We're glad you've decided to
e you'll take a moment to explore the site
has to offer.

Figure 3.1: The transparent background of this drop-down menu uses an effect unique to IE.

In terms of developer functionality—that is, functionality that developers of Web applications rely on—IE is rich with unique features. Although the most recent alternative browsers do a good job of replacing most IE-specific functionality, there are three major pieces of functionality that are still unique to IE: VBScript, ActiveX, and XML.

Many Web applications rely on client-side scripts to create robust functionality in their Web applications. For example, the drop-down menu in Figure 3.1 was created by using client-side scripting, a technique referred to as DHTML. Client-side scripting requires a scripting language; while *most* developers will elect to use a language such as JavaScript—which is compatible with most browsers—some developers will use VBScript, a Microsoft-proprietary language that pretty much only works with IE.

JavaScript vs. JScript vs. ECMAScript

For accuracy's sake, I want to point out that JavaScript is a language originally developed by Netscape. It does bear a passing resemblance to Sun Microsystems' Java language, but it's a language in its own right. Ecma International, an industry association focused on IT and communications standardization, adopted JavaScript as a standard language. The specific implementation of JavaScript that was adopted by Ecma is known as ECMAScript (you'll find the specification at http://www.ecma-international.org/publications/standards/Ecma-262.htm).

JScript is the language that is built-in to IE; this Microsoft-developed scripting language is compliant with the ECMAScript standard. Although IE recognizes the use of JavaScript as a client-side language, IE actually executes JavaScript by using the JScript language engine. The practical upshot of all this is that there are three different names for what amounts to the same thing, once you discard the legal and trademark issues involved.

Ditching IE means losing VBScript capabilities. This is where the middle ground scenario, which I'll discuss in more detail later in this chapter, comes into play: *Most* instances where you will need VBScript relate to intranet applications, and presumably (or at least hopefully) you can trust your own intranet applications not to launch attacks against your client computers. That makes IE—and its support for VBScript—safe for internal use where you need it, and still makes it feasible to use an alternative browser for Internet work, where VBScript is less likely to be encountered.

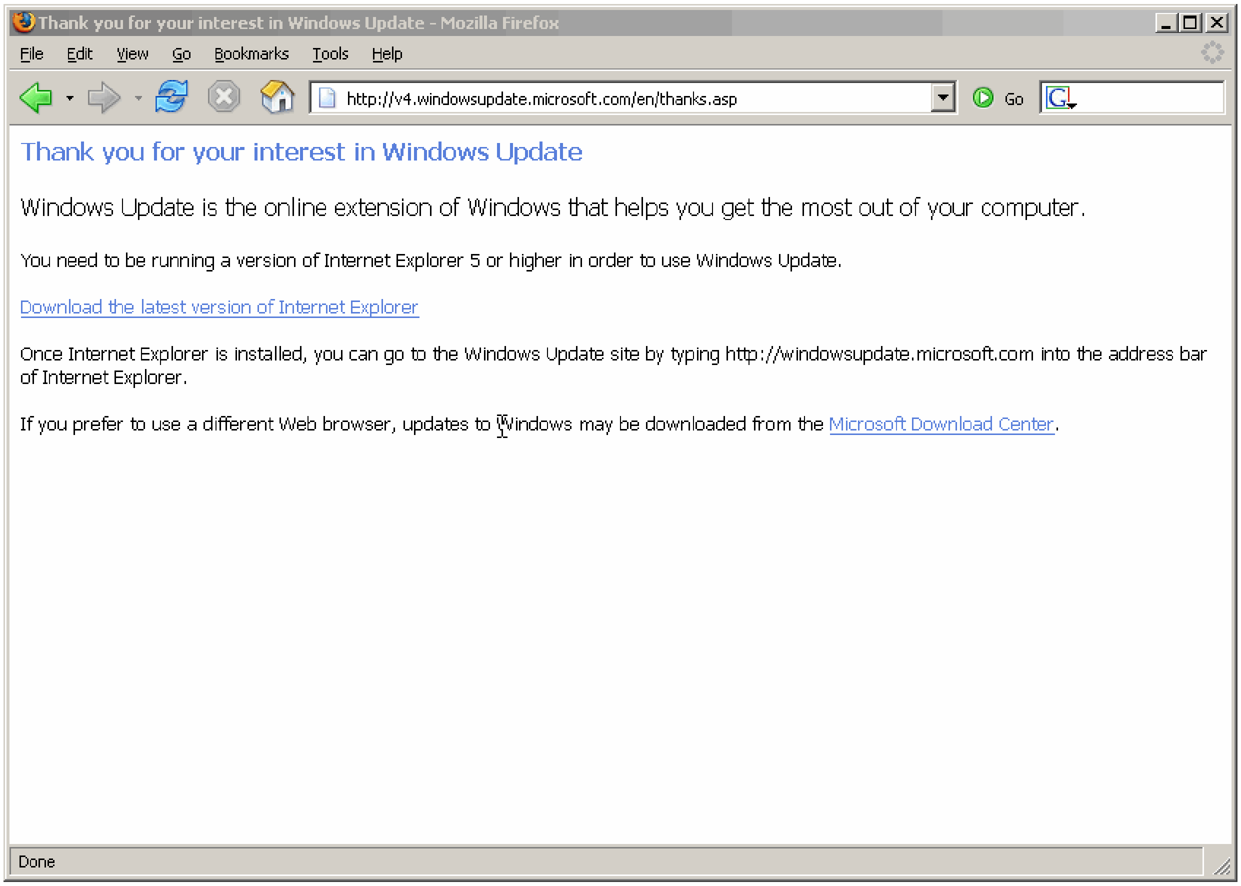
✎ You still might run into Internet situations in which VBScript—and therefore, IE—is needed. Extranets are a good example. Because extranets are often developed as in-house applications, VBScript is more likely to be in use. For example, although much of Microsoft's public Microsoft.com Web site is browseable by non-IE browsers, many of their extranet applications aren't. Microsoft's invoicing Web site, used by Microsoft's vendors to submit invoices to the company, requires a browser that supports IE because it uses VBScript.

By using VBScript in an extranet application, you are essentially forcing your partner companies to use a particular piece of software—in this case, IE—to access your extranet, which is a less-than-ideal business practice. Extranets should be the first applications targeted for revision to remove IE-specific features so that your business partners can make their own decisions about what software to use.

ActiveX is another technology supported exclusively by IE. ActiveX allows small, self-contained applications—ActiveX *controls*—to be downloaded into IE and executed within the IE window. The industry alternative to ActiveX is Java, which provides similar functionality albeit through a radically different technological approach. In other words, while rewriting a Web application to use ECMAScript instead of VBScript is pretty straightforward, rewriting an ActiveX control as a Java applet is anything but straightforward.

Very few legitimate Internet sites rely entirely on ActiveX controls, primarily because ActiveX controls are the source of many of IE's vulnerabilities (there are some notable exceptions, but many sites simply fear using ActiveX controls because of their poor reputation). Losing the ability to use ActiveX controls is, in fact, seen as a *benefit* to many organizations (to organizations that don't have any end-user needs that would require ActiveX, but making this determination in large organizations can be a difficult task).

However, there are drawbacks to losing ActiveX, primarily in relation to Microsoft-based Web sites and functionality. Perhaps the most obvious example is the Windows Update Web site, used to check Windows computers for the latest patches and software updates. The software that performs those checks and downloads and installs new software is an ActiveX control. Try to access Windows Update without an ActiveX-capable browser (in other words, without IE), and you will receive a message like the one that Figure 3.2 shows.


Thank you for your interest in Windows Update - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://v4.windowsupdate.microsoft.com/en/thanks.asp
Go
Done

Thank you for your interest in Windows Update

Windows Update is the online extension of Windows that helps you get the most out of your computer.

You need to be running a version of Internet Explorer 5 or higher in order to use Windows Update.

Download the latest version of Internet Explorer

Once Internet Explorer is installed, you can go to the Windows Update site by typing http://windowsupdate.microsoft.com into the address bar of Internet Explorer.

If you prefer to use a different Web browser, updates to Windows may be downloaded from the Microsoft Download Center.

Figure 3.2: You need IE to access Windows Update.

Workarounds are available and numerous. For example, you could configure your Windows 2000 (Win2K) and Windows XP computers to use Automatic Updates, which will download critical updates without using IE. You could also deploy Microsoft Software Update Services (SUS 1.0, or its successor, which is called Windows Update Services—WUS), which works with Automatic Updates to deploy patches and other updates without the use of IE. However, this workaround applies only to the most obvious example of ActiveX usage; if you have business applications that rely on IE's support for ActiveX, you might need to consider a middle ground solution in which you retain IE for at least some purposes.

A final unique feature in IE is its XML support, which allows the browser to perform client-side manipulation of data. Perhaps the best use of this technology is seen in Exchange Server 2003's Outlook Web Access (OWA), where the Web interface is able to closely resemble the Outlook application. Users can sort their email, for example, by clicking a column, and the browser doesn't need to reload the page; it simply uses IE's XML support to redisplay the page client-side for a faster user experience. Although OWA provides compatibility for other browsers, the user experience is less true to the full Outlook application and feels more like a Web site than an application. In some cases (such as with OWA), giving up IE means giving up a rich user experience; in other instances (such as intranet applications designed for IE), the lack of this robust XML support in an alternative browser might make the alternative browser unfeasible or unusable.

What About IE 7.0?

In the first quarter of 2005, Microsoft announced IE 7.0, a new version of IE that would ship separately from Windows Longhorn (the next version of Windows itself), despite earlier announcements that IE would not ship a new version until the one bundled in Longhorn. Microsoft is touting IE 7.0 as a more secure Web browser; certainly, it has a host of new security features that build upon those added in Windows XP Service Pack 2 (SP2). However, for some organizations, Microsoft's definition of "more secure" might differ from their own.

Microsoft's approach to securing IE—an approach seen in Windows XP SP2 and used in IE 7.0—has primarily been to partially or conditionally block access to potentially vulnerable features or content. Many organizations find this approach to be insufficient and feel that Microsoft should *remove* the potentially vulnerable features. For example, allowing the user to block access to ActiveX controls isn't as secure as removing support for ActiveX controls completely (thus ensuring that ActiveX controls can't be "unblocked"). That backward step in functionality would create significant compatibility issues, however, which is why it is an approach that Microsoft is understandably hesitant to take.

Another problem is that these security updates to IE—in terms of service packs and new versions—are available only to Windows XP, which is not universally deployed. Users of Win2K or Windows 98, for example, must still deal with the less-secure IE they have always had.

Ultimately, Microsoft's updates to IE do (and will continue to) make it less susceptible to attack, while preserving the unique functionality that IE offers. However, alternative browsers continue to offer a more secure alternative simply by not having the functionality that is so often exploited. Additionally, because alternative browsers are less tightly integrated with Windows itself, any vulnerabilities in those browsers will likely be a problem only for the browser—unlike IE, through which a browser-based vulnerability can open into the OS as a whole.

Outlook Express

Outlook Express is a Post Office Protocol 3 (POP3) and Internet Messaging Application Protocol (IMAP) client—in short, an email application. It also offers newsreader functionality for participating in Internet (USENET) newsgroups.

The market is flooded with alternatives to Outlook Express, ranging from freely available clients such as certain editions of Eudora to more robust applications. Certainly, Outlook Express does not offer the robust functionality unique to the full Outlook application (which is a part of the Microsoft Office suite). The one piece of nearly unique functionality Outlook Express does offer is security-related—digital signatures and message encryption. Although Outlook Express isn't the only mail client to support digital certificates (the enabling technology behind signatures and encryption), it is one of the few Windows-compatible clients to do so.

Perhaps more important for this discussion, however, is the fact that *very* few organizations rely on Outlook Express. Although alternatives certainly exist, most organizations already have an alternative—such as Outlook, Lotus Notes, or some other messaging client—in place; they simply need to remove Outlook Express to reduce their attack surface.

If It Ain't Broke, Why Fix It?

The following scenario provides an example of why you might want to remove Outlook Express even if you are not using it—suppose you use Lotus Notes and one of your users receives a message with a file attachment. That file attachment has an .eml extension, which by default will open in Outlook Express. If Outlook Express is installed and available, double-clicking the attachment in Notes might open Outlook Express! Thus, Outlook Express could become "in use" even if you're supposedly not using it.

Why would this be a problem? Outlook Express has been subject to several attacks and exploits. For example, the aforementioned .eml attachment might contain a JPEG graphic that exploits a vulnerability in Microsoft's Graphic Device Interface (GDI+) software—a core part of Windows—to crash the computer or execute code. Because Outlook Express is integrated with Windows, Outlook Express uses Windows' GDI+ to display the JPEG graphic, thus making the exploit work. (The GDI+ vulnerability *has* been patched, but organizations have been notoriously inefficient in ensuring that every copy of GDI+ on their computers receives the patch).

Windows Media Player

There is certainly no shortage of media players on the market, but while all of them provide support for industry-standard file formats—such as MP3 audio or MPEG video—they also come with their own proprietary formats. In the case of Windows Media Player, the supported Windows Media formats include WMA, WMV, ASF, and so forth. Bottom line: If you need to access these media formats, you need Windows Media Player.

You might seek to eliminate Windows Media Player by converting any corporate content into other formats, such as Real Media or Apple QuickTime. Certainly many public Web sites offer media in one of these formats along with Windows Media Player, so converting your corporate content might cover the majority of circumstances in which Windows Media Player might need to be used—except, however, when it comes to protected content.

Windows Media has established a significant market lead in Digital Rights Management (DRM). Apple QuickTime doesn't currently offer DRM for video content and doesn't provide third parties with a way to protect audio content. Real Networks offers DRM for Real Media but requires you to purchase a licensing server in order to use the DRM features. Windows Media's DRM can be deployed essentially free of charge because the DRM software development kit is freely available (although you do have to sign a license with Microsoft to obtain it). If your company is dealing with DRM-protected media content, the odds are that you will need to continue using Windows Media Player.

Windows Messenger

There are *two* Microsoft instant messaging clients: Windows Messenger, which comes bundled with Windows, and MSN Messenger, which is downloadable from Microsoft's MSN Web site. Both are similar in look and operation and provide access to Microsoft's instant messaging network. Windows Messenger can also connect to other instant messaging networks, such as those created by Microsoft Live Communications Server or Exchange 2000 Server. MSN Messenger can be easily uninstalled if you don't want to use it; Windows Messenger is somewhat more difficult.

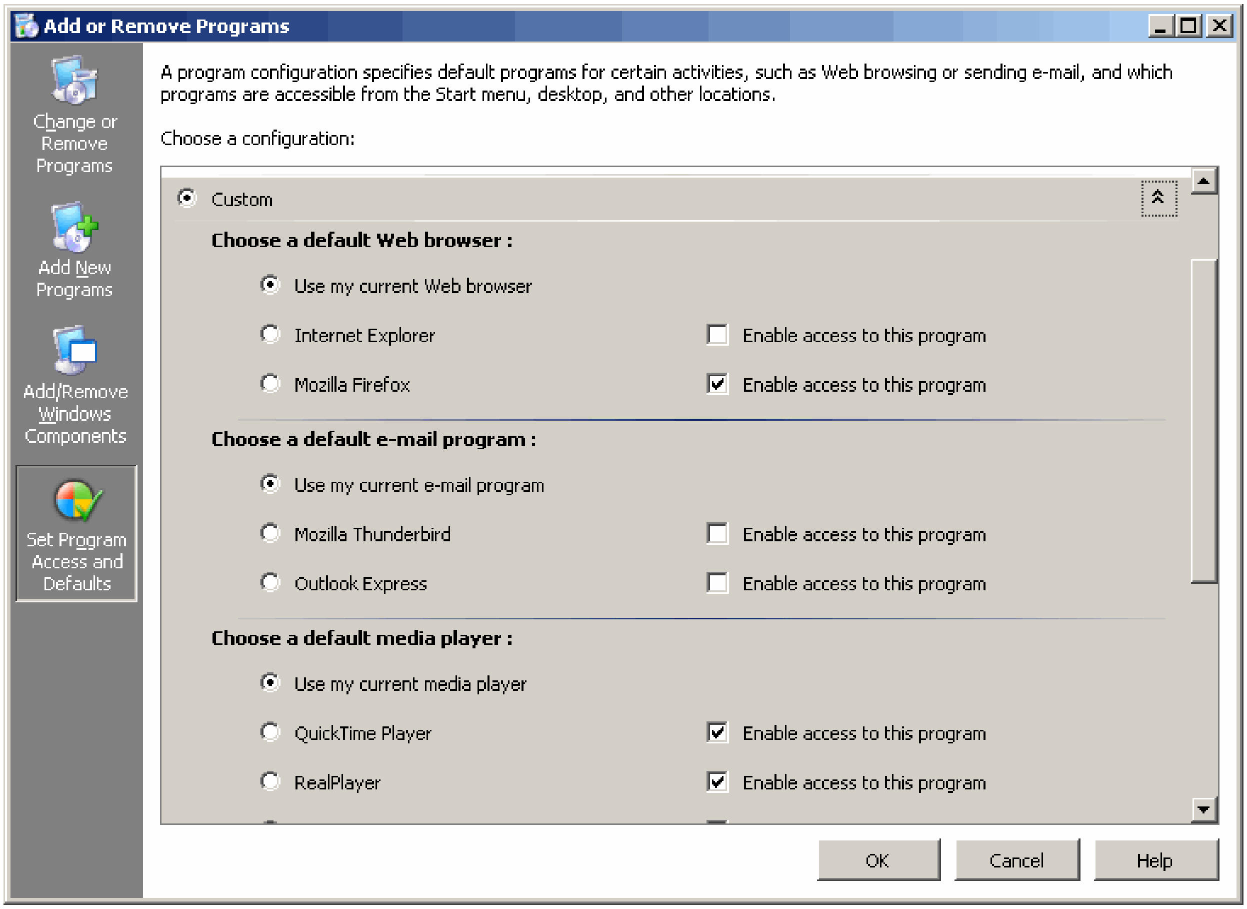
> ✎ When I speak of alternatives to Windows Messenger, I'm referring to instant messaging clients that can connect to Microsoft's public instant messaging network, replacing Windows Messenger's functionality. I am *not* referring to alternative instant messaging networks such as America Online or Yahoo. Although these provide useful functionality and are indeed alternative *networks,* they do not replace the functionality of Windows Messenger by allowing you to connect to *Microsoft's* instant messaging network.

If your users only use public instant messaging networks, they don't lose much by giving up Windows Messenger and using an alternative. If your users rely on an internal instant messaging network (increasingly common in corporate environments), an alternative client might not be able to connect. Instead, you might need to consider an alternative internal instant messaging product, which will come complete with its own server component as well as a new client. Moving to an alternative instant messaging network may or may not change the feature set to which your users have access—some products offer more functionality than Windows Messenger; others offer less.

Removing the Bundled Software

Since the case with the United States Department of Justice in 2003, Microsoft has offered a Program Access and Defaults application, which allows you to set the application used for certain middleware functions. As Figure 3.3 shows, this application also lets you control access and defaults for Web browsing, email, media playing, instant messaging, and your Java virtual machine (JVM).

> ✎ This chapter doesn't discuss Microsoft's JVM because Microsoft is no longer developing the JVM. As a practical matter, you should install Sun Microsystems' JVM and use it to achieve the most recent functionality.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
OK
Cancel
Help

A program configuration specifies default programs for certain activities, such as Web browsing or sending e-mail, and which programs are accessible from the Start menu, desktop, and other locations.

Choose a configuration:

● Custom

Choose a default Web browser :

- ● Use my current Web browser
- ○ Internet Explorer — □ Enable access to this program
- ○ Mozilla Firefox — ☑ Enable access to this program

Choose a default e-mail program :

- ● Use my current e-mail program
- ○ Mozilla Thunderbird — □ Enable access to this program
- ○ Outlook Express — □ Enable access to this program

Choose a default media player :

- ● Use my current media player
- ○ QuickTime Player — ☑ Enable access to this program
- ○ RealPlayer — ☑ Enable access to this program

Figure 3.3: Setting program access and defaults.

This application allows you to determine two things:

- Which application will be used by default for these middleware applications
- Which applications will be accessible by users

For example, you can see in the figure that I've configured Mozilla Firefox to be accessible and disabled access to IE. Firefox is configured as my default browser (which you don't see because this application defaults to "Use my current Web browser," meaning it won't change whatever the current setting is but also won't show you what that current setting is).

This application is, however, misleading. Reading it, you would expect that IE would be turned off, shut down, and possibly even uninstalled. Nothing could be further from the truth: Other applications can launch IE, and, indeed, I can do so manually simply by opening Run from the Start menu, typing

```
iexplore
```

and clicking OK. The "enable access" check box, when cleared, simply removes the IE icon from the Start menu—hardly a security precaution. The application does allude to this "enable" functionality in its description at the top of the window, but doesn't make it clear that "other locations" still allows the application to be executed. In addition, disabling access to an application only removes the default icons that Windows creates for them; you can still easily create your own icons even if access to the application is "disabled." From a security perspective, this application is fairly useless. So how do you go about removing bundled applications if you don't want them?

IE

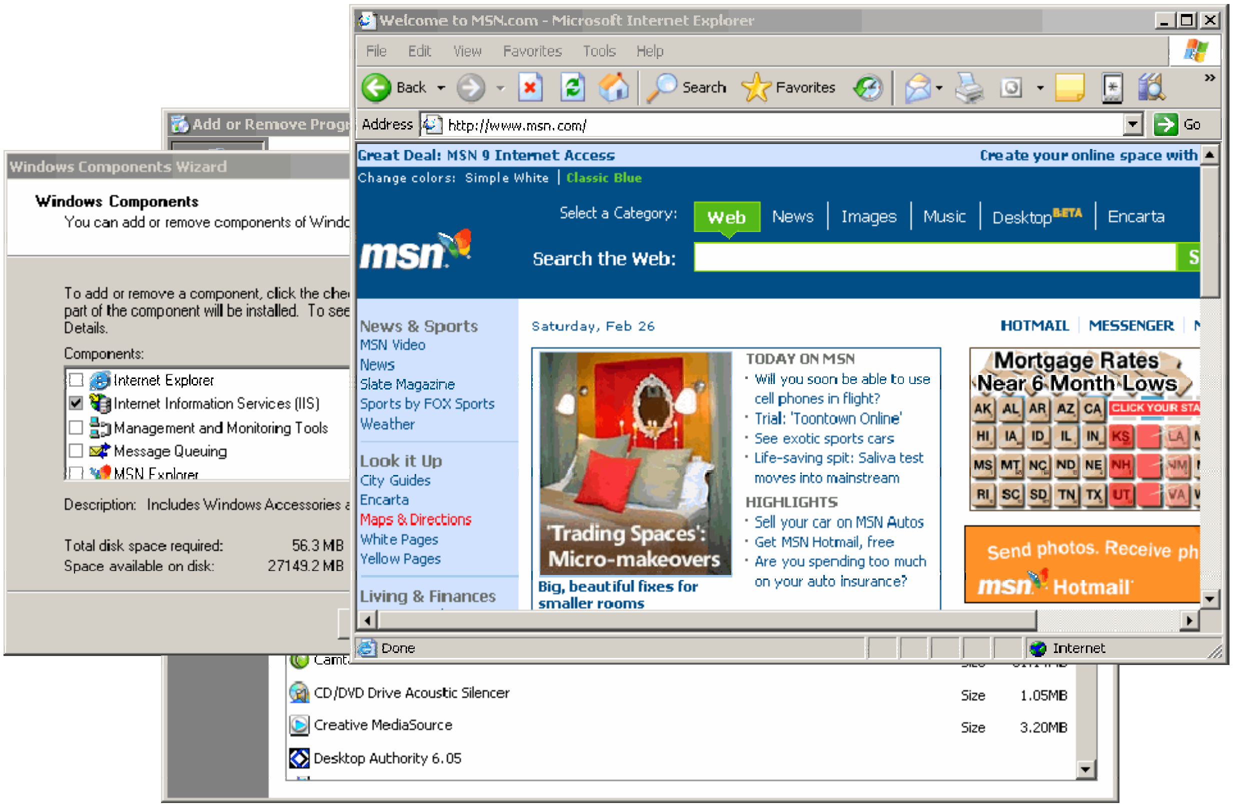
IE is perhaps the toughest bundled application to remove—assuming for the moment that you *do* want to remove it and not go with a middle ground solution, which I'll discuss later in this chapter.

> It is important to voice some cautions and caveats here. Understand that IE is composed of several different bits, some of which are absolutely critical to the operation of many applications. For example, the Microsoft HTML Rendering Engine (MSHTML) is the bit of IE that turns HTML code into a visible Web page; removing MSHTML will break plenty of applications. Iexplore.exe is actually just a wrapper around these several components; removing it doesn't actually remove most of the software that contains IE's vulnerabilities.
>
> Bottom line: Removing *any* portion of IE *might* break *some* applications. Removing anything less than *all* of IE might leave some vulnerabilities in place (if the components you leave in place contain vulnerabilities, of course). So you should carefully test any IE removal with all of your company's applications to determine if anything will be affected.

IE is heavily integrated with Windows and isn't something you can safely just delete on your own. You need an application that understands how IE is built and can safely extract it. One such tool is IEradicator (http://www.litepc.com/ieradicator.html), which can de-register and remove most of the IE components, leaving the ones most commonly used by other applications. The application works with all versions of Windows earlier than Win2K SP2; for Win2K SP2 and later, including Windows XP, use the same company's XPlite and 2000lite software (http://www.litepc.com/xplite.html).

> I need to stress again, however, the importance of testing this process on a representative computer to make sure that none of your applications are adversely affected.

Don't think for a second that going into the Control Panel's Add or Remove Programs utility, selecting Add/Remove Windows Components, and clearing the IE check box will remove anything. As you can see in Figure 3.4, I've "removed" IE, yet you can still see it up and running.



Welcome to MSN.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.msn.com/ Go
Add or Remove Programs
Windows Components Wizard
Done
Internet

Windows Components
You can add or remove components of Windo

To add or remove a component, click the che
part of the component will be installed. To see
Details.

Components:

- ☐ Internet Explorer
- ☑ Internet Information Services (IIS)
- ☐ Management and Monitoring Tools
- ☐ Message Queuing
- ☐ MSN Explorer

Description: Includes Windows Accessories a

Total disk space required:	56.3 MB
Space available on disk:	27149.2 MB

CD/DVD Drive Acoustic Silencer	Size	1.05MB
Creative MediaSource	Size	3.20MB
Desktop Authority 6.05		

Great Deal: MSN 9 Internet Access — Create your online space with
Change colors: Simple White | Classic Blue
Select a Category: Web | News | Images | Music | Desktop BETA | Encarta
Search the Web:

News & Sports: MSN Video, News, Slate Magazine, Sports by FOX Sports, Weather
Look it Up: City Guides, Encarta, Maps & Directions, White Pages, Yellow Pages
Living & Finances

Saturday, Feb 26 — HOTMAIL | MESSENGER

'Trading Spaces': Micro-makeovers
Big, beautiful fixes for smaller rooms

TODAY ON MSN
- Will you soon be able to use cell phones in flight?
- Trial: 'Toontown Online'
- See exotic sports cars
- Life-saving spit: Saliva test moves into mainstream

HIGHLIGHTS
- Sell your car on MSN Autos
- Get MSN Hotmail, free
- Are you spending too much on your auto insurance?

Mortgage Rates Near 6 Month Lows — CLICK YOUR STA

Send photos. Receive ph — msn Hotmail

Figure 3.4: Removing IE only removed its icon, not the application.

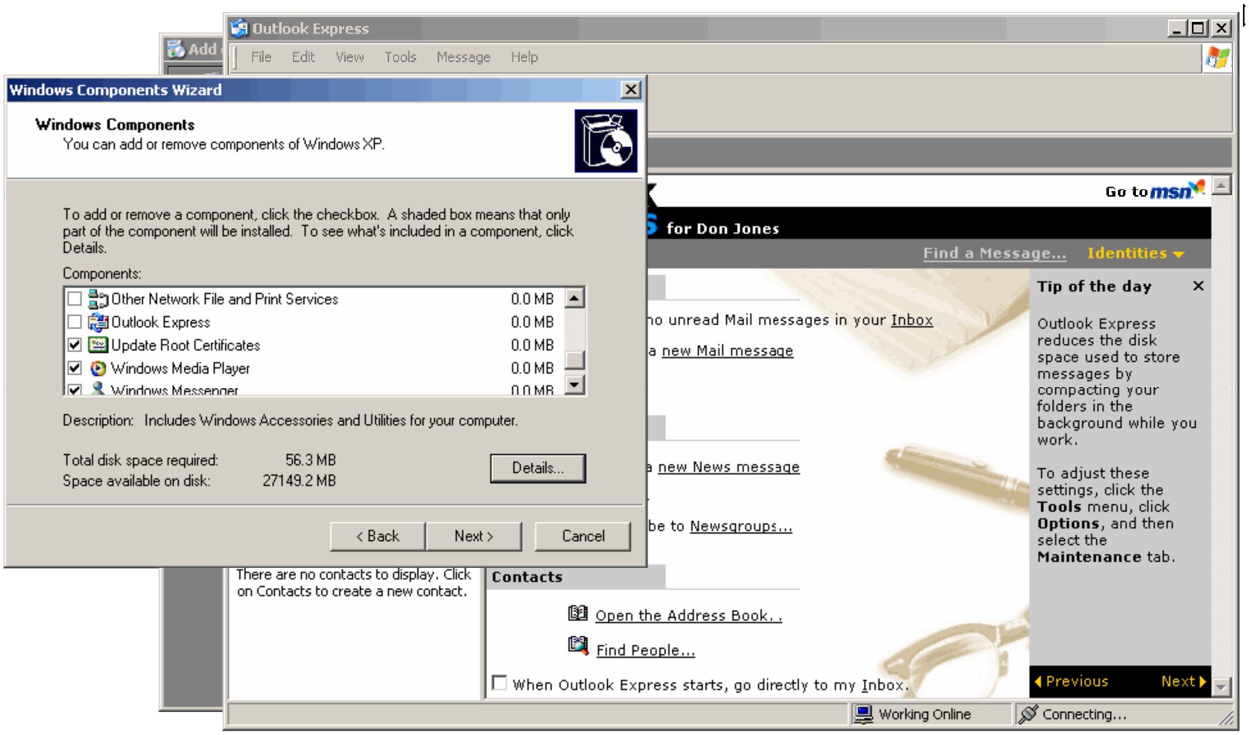
I'm not going to try and tell you that obtaining a tool such as IEradicator or XPlite is the only way to remove IE; obviously, anything an application can do for you, you can do yourself. But IE's roots go deep, and the detailed, step-by-step actions that would be required to remove any part of it with any kind of safety isn't something I'd trust myself to do manually.

> ☞ Be aware that installing a service pack or even certain updates from Microsoft might reinstall portions of IE; test these updates to check their effect and determine whether you will need to subsequently re-un-install IE after applying the update.

Not many companies are able to remove IE without missing some of its functionality. Most companies continue to need it for one reason or another. In many cases, intranet applications requiring ActiveX controls of VBScript were the reason; OWA is another commonly cited reason for keeping IE (OWA in IE really is amazing). That doesn't mean you can't reduce your attack surface by using an alternative browser, though; later in this chapter, I'll discuss coexistence scenarios in which you use IE *only* where doing so is advantageous, and use an alternative elsewhere.

Outlook Express

Like IE, Outlook Express shows up in the Add/Remove Windows Components dialog box, so you would think that clearing the check box and clicking OK would remove it. Not so: Look at Figure 3.5 in which the check box has been cleared, yet Outlook Express is clearly alive and well.



Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Other Network File and Print Services	0.0 MB
□	Outlook Express	0.0 MB
☑	Update Root Certificates	0.0 MB
☑	Windows Media Player	0.0 MB
☑	Windows Messenger	0.0 MB

Description: Includes Windows Accessories and Utilities for your computer.

Total disk space required: 56.3 MB
Space available on disk: 27149.2 MB

for Don Jones

o unread Mail messages in your Inbox
a new Mail message
a new News message
be to Newsgroups...

There are no contacts to display. Click on Contacts to create a new contact.

Contacts
Open the Address Book...
Find People...

□ When Outlook Express starts, go directly to my Inbox.

Tip of the day

Outlook Express reduces the disk space used to store messages by compacting your folders in the background while you work.

To adjust these settings, click the **Tools** menu, click **Options**, and then select the **Maintenance** tab.

Figure 3.5: "Uninstalling" Outlook Express only removes its icons from the Start menu.

Truly uninstalling Outlook Express requires more effort, and you will need to be a local administrator in order to pull it off. You will be renaming several files and folders. What you rename them doesn't matter, so long as you rename them. Start with:

- C:\Program Files\Common Files\Microsoft Shares\Stationery
- C:\Documents and Settings*username*\Application Data\Identities
  or C:\Documents and Settings*username*\Local Settings\Application Data\Identities
- C:\Documents and Settings\username\Application Data\Microsoft\Address Book or C:\Documents and Settings\username\Local Settings\Application Data\Address Book

You will need to delete several registry keys, as well.

> 💣 The usual warnings about registry editing apply here: If you mess up the registry, you may mess up your computer beyond repair.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Outlook Express
- HKEY_LOCAL_MACHINE\Software\Microsoft\WAB
- HKEY_CURRENT_USER\Identities
- HKEY_CURRENT_USER\Software\Microsoft\Outlook Express
- HKEY_CURRENT_USER\Software\Microsoft\WAB
- HKEY_LOCAL_MACHINE \Software\Microsoft\Active Setup\Installed Components\{44BBA840-CC51-11CF-AAFA-00AA00B6015C}
- HKEY_LOCAL_MACHINE \Software\Microsoft\Active Setup\Installed Components\{7790769C-0471-11D2-AF11-00C04FA35D02}

Now you have a bunch of files to rename—I recommend leaving the filenames and adding ".old" to the end (for example, Inetcomm.dll becomes Inetcomm.dll.old) so that you can easily put the files back if desired. You might want to use Windows Explorer's Search function to find these files. Be aware that most of them will also exist in C:\Windows\System32\Dllcache; be sure to rename both copies to have the same new name:

- Inetcomm.dll
- Msoeacct.dll
- Msoert2.dll
- Msoe.dll
- Msoeres.dll
- Msimn.exe
- Oeimport.dll
- Oemiglib.dll
- Oemig50.exe
- Setup50.exe

- Wab.exe
- Wabfind.dll
- Wabimp.dll
- Wabmig.exe
- Csapi3t1.dll
- Directdb.dll
- Wab32.dll
- Wab32res.dll

You might receive a prompt about Windows File Protection. *Do not* provide Windows with a Windows installation CD-ROM; instead, click Cancel in the dialog box. Windows is essentially trying to stop you from doing what you want to do, so you need to override it in this one instance.

You can find more information about this procedure at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q263837, which is a Microsoft article detailing how to uninstall different versions of Outlook Express.

As always, installing a service pack or certain patches will almost certainly reinstall Outlook Express, so you need to test and be prepared to repeat this procedure if necessary.

Windows Media Player

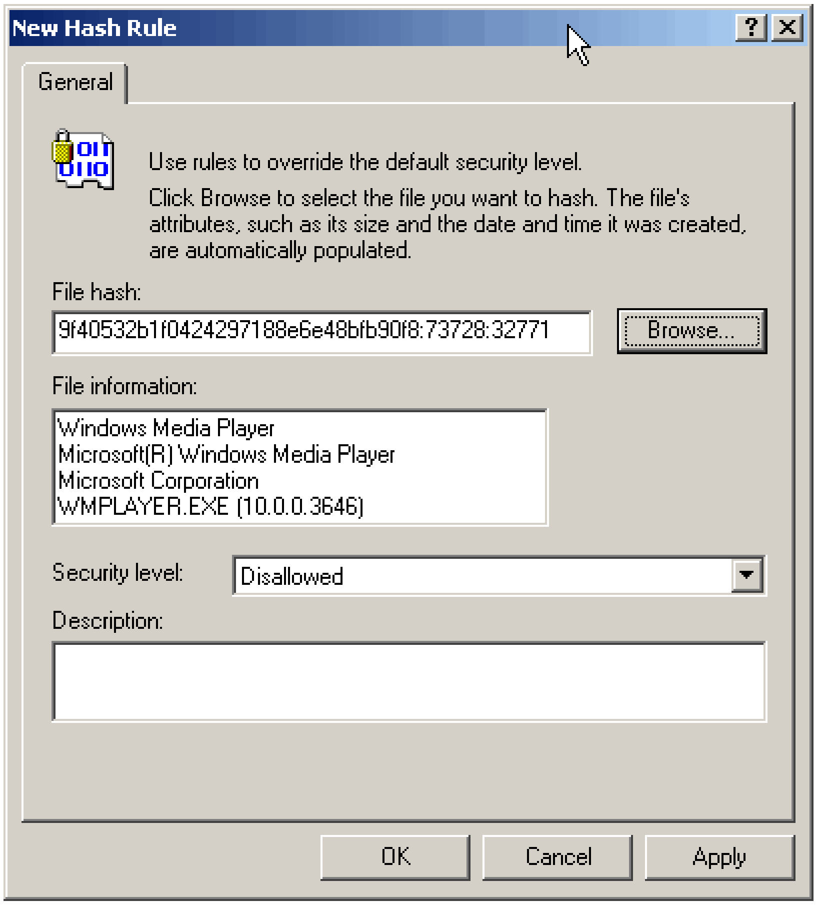
Like IE and Outlook Express, Windows Media Player appears in the Add/Remove Windows Components list with a check box, implying that you can uninstall it by clearing the check box. Think it works? Of course not. Windows Media Player can actually be more difficult to remove than IE, as it's very deeply integrated into the OS. You can typically uninstall a recently installed version (such as Windows Media Player 10), but doing so merely reverts to the previously installed version; it doesn't completely remove all copies of Windows Media Player.

In fact, it is nearly impossible to completely remove Windows Media Player, leaving you with the alternative of making it impossible to run it. To do so, start by installing the latest-available version (from http://www.microsoft.com/windowsmedia; doing so will put Windows Media Player in a more accessible location so that you can perform this trick). Open Windows Media Player's installation folder (typically C:\Program Files\Windows Media Player). The file you are looking for is Wmplayer.exe; edit the security settings on this file so that nobody can access it.

As a backup plan, you might create a special domain group named Windows Media Player and allow only that group to have Full Control over Wmplayer.exe (remove all other users and groups from the file's access control list—ACL). Simply leave the group empty and nobody will have access; should you ever *need* access, you can just add your user account to the group.

Although hardly an *ideal* solution, restricting access to the player at least keeps it from operating. A more centralized method of achieving a similar result would be to use Windows XP and Windows Server 2003 (WS2K3) Software Restriction Policies (SRP), a component of Group Policy. Create a software policy that is a hash rule of Wmplayer.exe, then set the action for that rule to be Disallowed. Figure 3.6 shows just such a rule being configured in a Group Policy Object (GPO); by applying this GPO to your computers, you will prevent Windows Media Player from running.

> ✎ So why not use this same technique on IE and Outlook Express? In the case of Outlook Express, you might, but if you don't need it, why not just get rid of it? I imagine if you had *some* users who needed Outlook Express and others who didn't, and it *had* to be Outlook Express and not some alternative mail client, you could use the SRP or permissions technique to make Outlook Express available to some users. It's main executable—Msimn.exe—can be treated the same way Wmplayer.exe was.
>
> In the case of IE, though, this technique is insufficient. Iexplore.exe doesn't contain much of IE's actual functionality, and restricting access wouldn't stop some other application (or attack) from running IE. The removal technique is much safer, if you can do it.



Use rules to override the default security level.

Click Browse to select the file you want to hash. The file's attributes, such as its size and the date and time it was created, are automatically populated.

File hash:

9f40532b1f0424297188e6e48bfb90f8:73728:32771

File information:

Windows Media Player
Microsoft(R) Windows Media Player
Microsoft Corporation
WMPLAYER.EXE (10.0.0.3646)

Security level: Disallowed

Description:

Figure 3.6: A rule to stop Windows Media Player from running.

Windows Messenger

Windows Messenger is a bit tricky. Although it is not difficult to remove, it does register itself with a half-dozen other programs, including Outlook Express. Simply deleting Windows Messenger will result in delays when those applications launch and try to get in touch with Windows Messenger.

The first step is to hide—not delete—Windows Messenger. To do so, change the registry value HKEY_LOCAL_MACHINE\Software\Microsoft\Outlook Express\Hide Messenger to have a value of 2. Then, execute

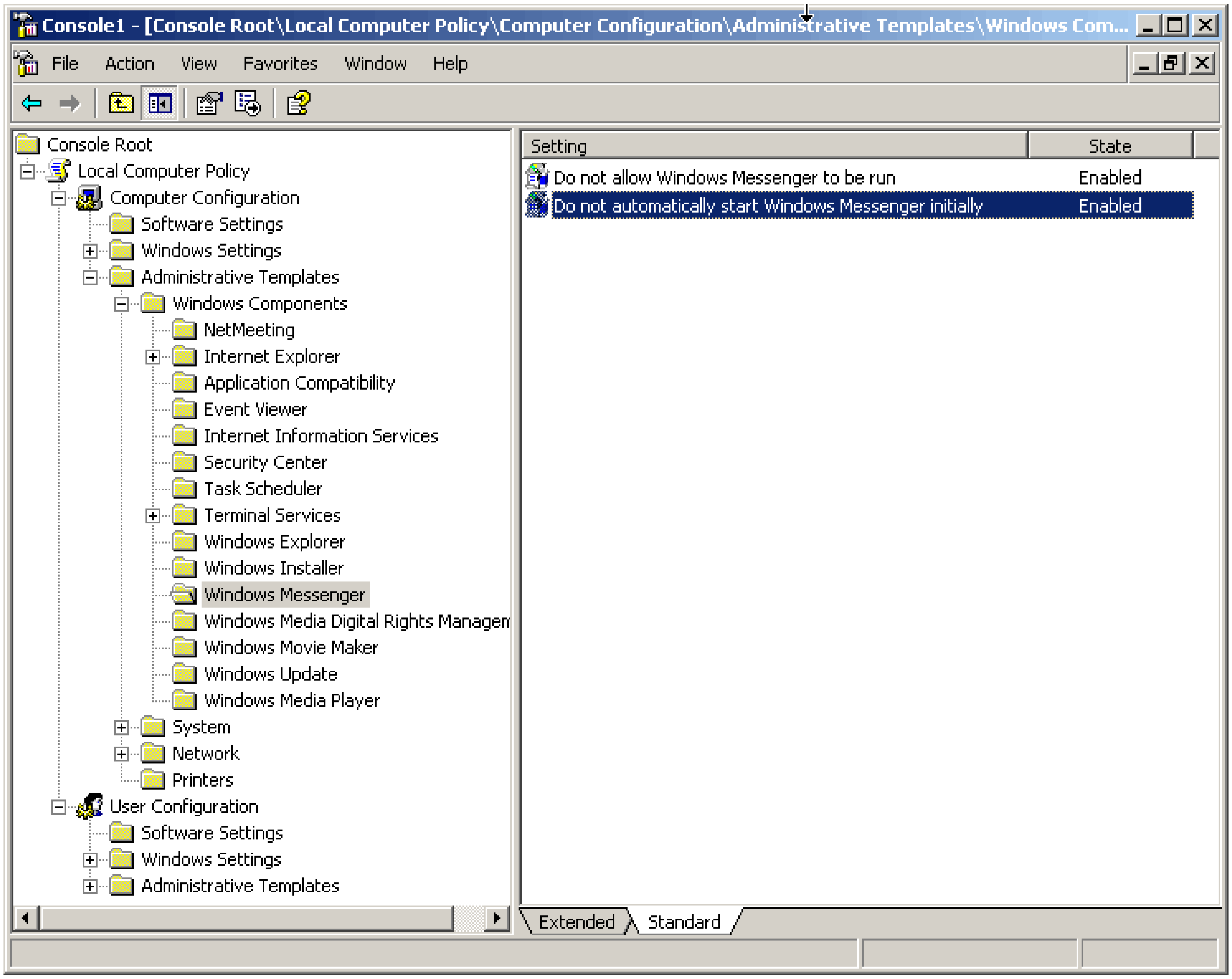
```
Rundll32 advpack.dll,LaunchINFSection
%windir%\inf\msmsgs.inf,BLC.Remove
```

to unregister Windows Messenger and prevent startup delays in other applications. A short VBScript can accomplish the trick easily:

```
On Error Resume Next
Set WSHShell = WScript.CreateObject("WScript.Shell")
val = "HKEY_LOCAL_MACHINE\Software\Microsoft\" & _
 "Outlook Express\Hide Messenger"
setting = 2
cmd = "RunDll32 advpack.dll,LaunchINFSection" & _
 " %windir%\inf\msmsgs.inf,BLC.Remove"
WSHShell.RegWrite val, setting
WshShell.Run(cmd)
```

After that is done, you might also create an SRP (or apply NTFS permissions) to restrict access to Msmsgs.exe, the Windows Messenger executable, in much the same way we did for Wmplayer.exe in the previous section.

Even more simply, you can deploy a GPO that enables the *Do not allow Windows Messenger to be run* setting. This setting works for Windows Messenger 4.0 or later on Windows XP Professional computers. Figure 3.7 shows this GPO policy enabled in a computer's local policy.



Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Com...

Setting	State
Do not allow Windows Messenger to be run	Enabled
Do not automatically start Windows Messenger initially	Enabled

Figure 3.7: Disabling Windows Messenger by using a GPO.

This trick doesn't *remove* Windows Messenger, but it does stop it from running. Windows Messenger doesn't have a lot of subsidiary components that can be run independently, so stopping Windows Messenger from running will pretty much ensure that any vulnerabilities it contains can't be exploited. Fact is, actually getting Windows Messenger completely off of a computer—as with the other bundled software—is difficult enough as to be impractical.

Be sure your users have modified Outlook to clear the *Enable Instant Messaging in Microsoft Outlook* setting *before* you use a GPO to disable Windows Messenger. Otherwise, Outlook will start very slowly.

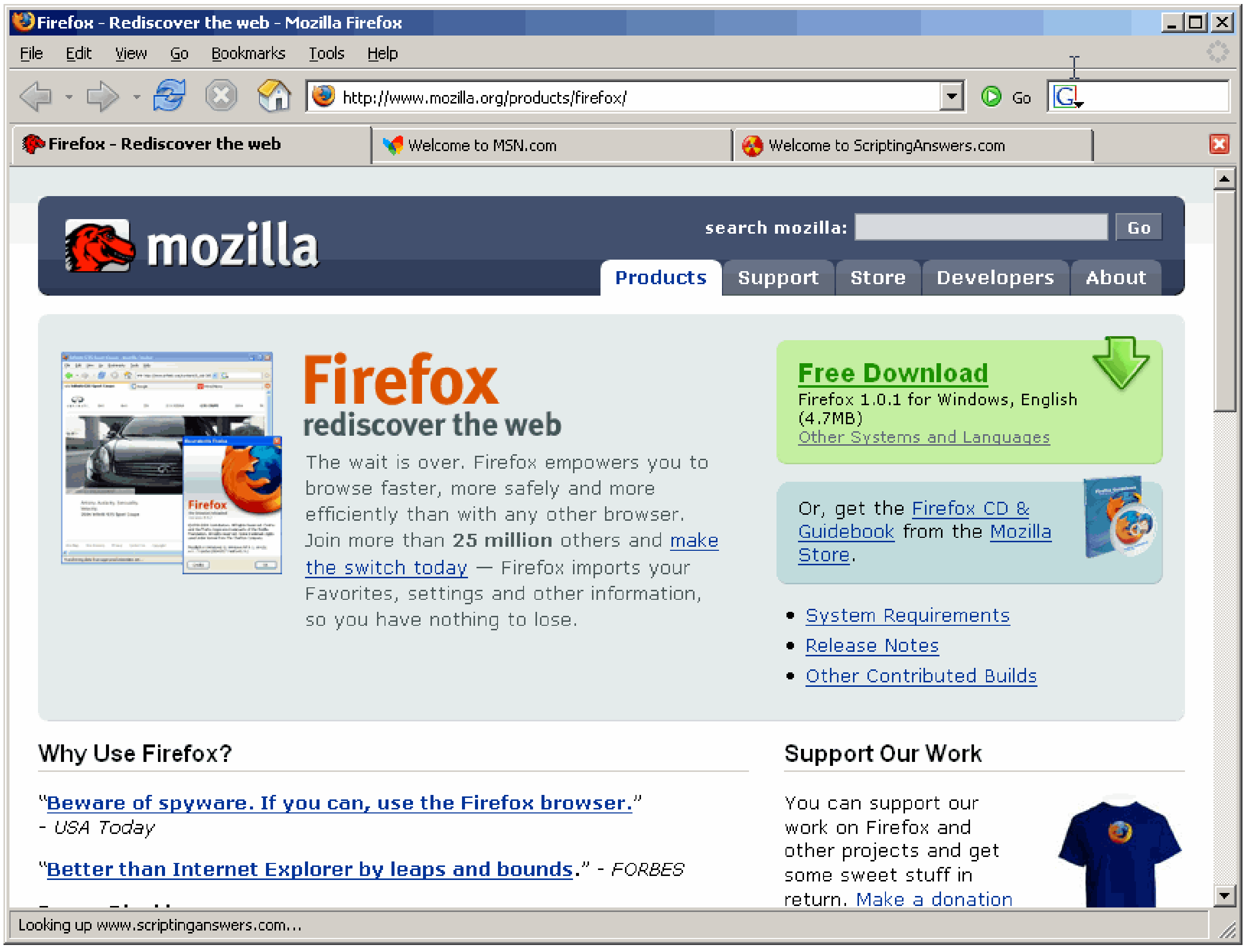
A final technique is to simply rename the folder C:\Program Files\Messenger; call it DisableMessenger or something, instead. Windows will be unable to locate the software, and it will be more difficult for attackers to locate it if they want to run it. Used in conjunction with the GPO method, this will cover most of your bases in ensuring Windows Messenger doesn't allow attackers an entry point into your computers.

The Alternatives

So you’ve disabled and/or removed as much of the bundled software as you can—now what do you do? The next four sections discuss popular alternative software that comes closest to replacing the functionality of Microsoft’s bundled offerings.

Web Browser

The all-time champ of alternative software is the Mozilla Foundation’s Firefox browser (http://www.mozilla.org/firefox), which Figure 3.8 shows.



The wait is over. Firefox empowers you to browse faster, more safely and more efficiently than with any other browser. Join more than **25 million** others and make the switch today — Firefox imports your Favorites, settings and other information, so you have nothing to lose.

Firefox 1.0.1 for Windows, English (4.7MB)
Other Systems and Languages

Or, get the Firefox CD & Guidebook from the Mozilla Store.

- System Requirements
- Release Notes
- Other Contributed Builds

Why Use Firefox?

“**Beware of spyware. If you can, use the Firefox browser.**”
- *USA Today*

“**Better than Internet Explorer by leaps and bounds**.” - *FORBES*

Support Our Work

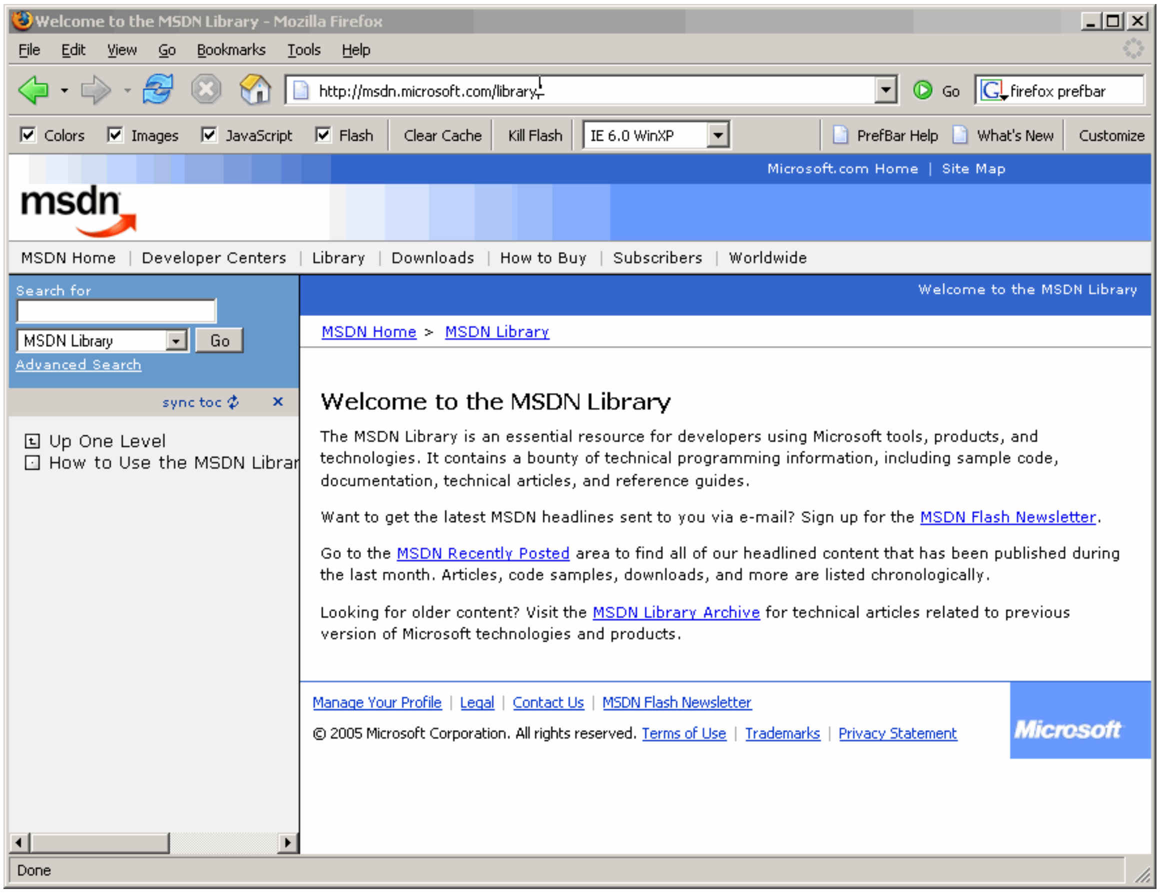
You can support our work on Firefox and other projects and get some sweet stuff in return. Make a donation

Looking up www.scriptinganswers.com...

Figure 3.8: Mozilla Firefox 1.0.

In addition to a host of leading-edge UI features such as tabbed browsing and a built-in pop-up blocker, Firefox supports the latest Cascading Style Sheets and HTML specifications, meaning it can display most any page that IE can. Unlike some other alternatives, Firefox isn’t just a replacement shell that instantiates IE; Firefox uses its own open-source HTML rendering engine (called Gecko).

In something approaching irony, using Firefox to browse many Web sites provides a less satisfactory experience than using IE because of the way the Web sites are programmed, not because of Firefox's functionality. What happens is that the sites check Firefox's *user agent*, a string the browser sends to identify itself, and determines that it can't handle high-end HTML and styles. Thus, the sites then "downgrade" themselves to a less-robust experience. In fact, Firefox *can* handle many of these sites. A Firefox add-in called PrefBar can be used to send an IE 6.0 user agent string, fooling the Web site into giving maximum functionality, as Figure 3.9 shows. You can download PrefBar from http://prefbar.mozdev.org.


Welcome to the MSDN Library - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Clear Cache
Kill Flash
PrefBar Help
What's New
Customize
msdn
Microsoft.com Home | Site Map
MSDN Home | Developer Centers | Library | Downloads | How to Buy | Subscribers | Worldwide
Search for
Go
Advanced Search
sync toc
Up One Level
How to Use the MSDN Librar
Welcome to the MSDN Library
Microsoft
Done

http://msdn.microsoft.com/library

firefox prefbar

☑ Colors ☑ Images ☑ JavaScript ☑ Flash

IE 6.0 WinXP

MSDN Library

MSDN Home > MSDN Library

Welcome to the MSDN Library

The MSDN Library is an essential resource for developers using Microsoft tools, products, and technologies. It contains a bounty of technical programming information, including sample code, documentation, technical articles, and reference guides.

Want to get the latest MSDN headlines sent to you via e-mail? Sign up for the MSDN Flash Newsletter.

Go to the MSDN Recently Posted area to find all of our headlined content that has been published during the last month. Articles, code samples, downloads, and more are listed chronologically.

Looking for older content? Visit the MSDN Library Archive for technical articles related to previous version of Microsoft technologies and products.

Manage Your Profile | Legal | Contact Us | MSDN Flash Newsletter

© 2005 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement

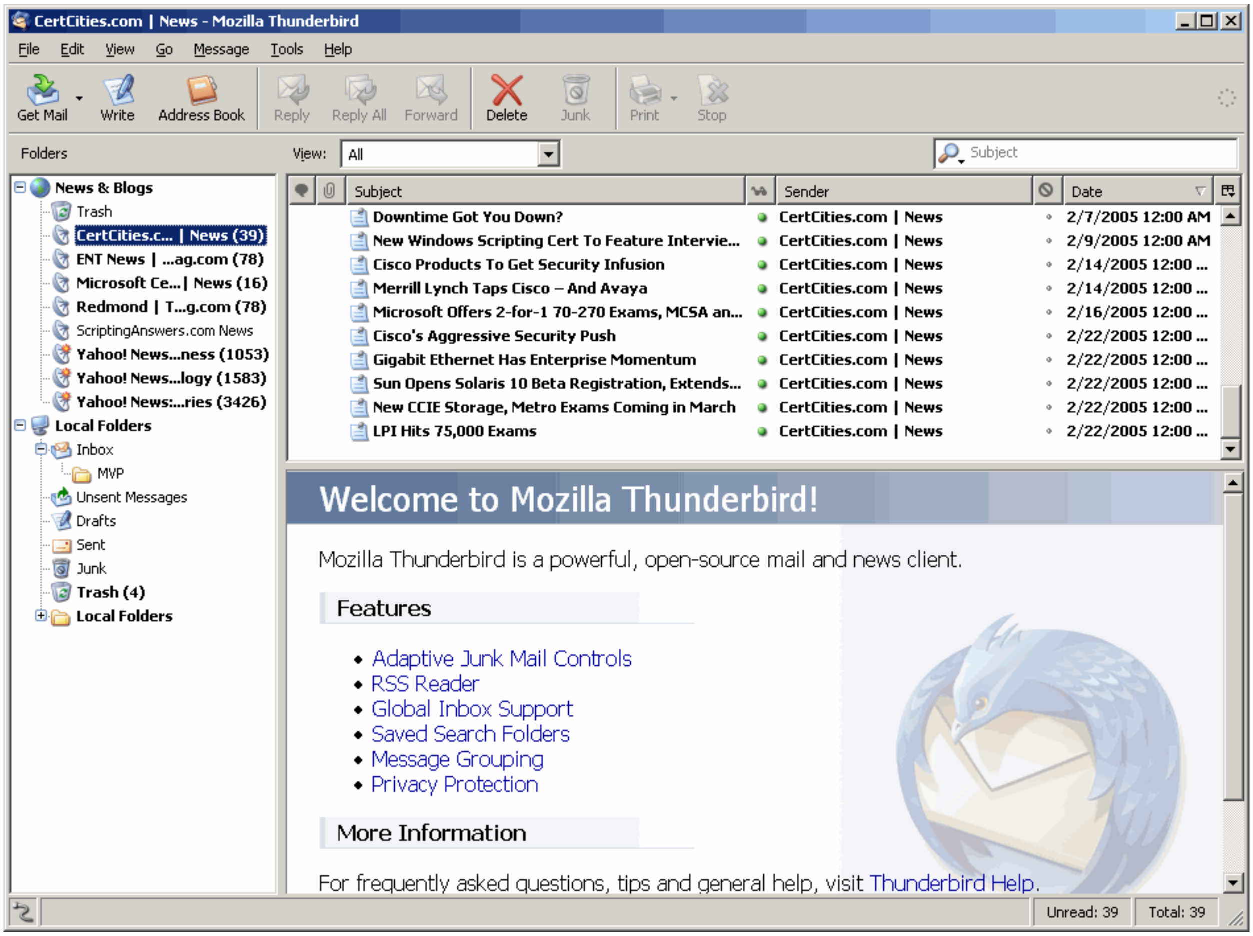
Figure 3.9: Notice the PrefBar set to give the IE 6.0 Windows XP user agent string.

On the downside, Firefox can be more difficult to deploy simply because Mozilla inexplicably doesn't package it in a Windows Installer (MSI) file; it's a standalone installation executable. Of course, if you have a repackaging tool you can create an MSI from it, allowing you to deploy Firefox via GPO, if desired. A more serious downside is that, because Firefox is cross-platform, it stores its settings locally in a file, which is a technique that works for most any platform on which Firefox runs. That makes centralized management of Firefox via GPO—which affects the registry—impossible. You therefore cannot centrally configure browser proxy settings, home pages, and so forth. Hopefully these enterprise-level issues can be addressed in future version of Firefox.

A recently announced new version of Netscape Navigator (which is based on the same core code as Firefox) offers an intriguing alternative for organizations that still need to use IE. This new browser will use the same Gecko engine that Firefox does, but will also offer the option to instantiate IE right within the browser, effectively making the new Navigator both an alternative to IE and a clone of IE. This alternative would allow users to use a single browser to safely surf the Web *and* Web sites that require IE functionality. The browser would "remember" your engine preference on a site-by-site basis, making the process of surfing pretty much transparent. Additional details about this planned release will hopefully be forthcoming, as it seems to offer a good balance between using an alternative browser and needing functionality that is unique to IE.

Email Client

Mozilla Foundation strikes again with Thunderbird, a popular and fully functional alternative to Outlook Express. It includes the usual high-end client features, such as an address book, the ability to access newsgroups (and even RSS news feeds), and so forth. Unlike most alternative mail clients, however, Thunderbird provides full support for digital certificates, meaning you can exchange digitally signed and encrypted emails. You can find Thunderbird at http://www.mozilla.org/thunderbird, and it's shown in Figure 3.10.



Subject	Sender	Date
Downtime Got You Down?	CertCities.com | News	2/7/2005 12:00 AM
New Windows Scripting Cert To Feature Intervie...	CertCities.com | News	2/9/2005 12:00 AM
Cisco Products To Get Security Infusion	CertCities.com | News	2/14/2005 12:00 ...
Merrill Lynch Taps Cisco – And Avaya	CertCities.com | News	2/14/2005 12:00 ...
Microsoft Offers 2-for-1 70-270 Exams, MCSA an...	CertCities.com | News	2/16/2005 12:00 ...
Cisco's Aggressive Security Push	CertCities.com | News	2/22/2005 12:00 ...
Gigabit Ethernet Has Enterprise Momentum	CertCities.com | News	2/22/2005 12:00 ...
Sun Opens Solaris 10 Beta Registration, Extends...	CertCities.com | News	2/22/2005 12:00 ...
New CCIE Storage, Metro Exams Coming in March	CertCities.com | News	2/22/2005 12:00 ...
LPI Hits 75,000 Exams	CertCities.com | News	2/22/2005 12:00 ...

Welcome to Mozilla Thunderbird!

Mozilla Thunderbird is a powerful, open-source mail and news client.

Features

- Adaptive Junk Mail Controls
- RSS Reader
- Global Inbox Support
- Saved Search Folders
- Message Grouping
- Privacy Protection

More Information

For frequently asked questions, tips and general help, visit Thunderbird Help.

Figure 3.10: Mozilla Thunderbird.

However, Thunderbird shares a number of drawbacks with Firefox, including a non-MSI installation package and no real means of centralized enterprise management. Also, Thunderbird is an alternative to Outlook *Express;* it isn't an alternative to Microsoft Outlook and doesn't contain any functionality for native connectivity to Exchange Server. As most enterprises use an enterprise messaging platform that offers its own client—such as Microsoft Exchange Server or Lotus Notes—you are more likely to use those than Outlook Express or any of its alternatives.

Media Player

The main competition for Windows Media Player is Apple QuickTime and RealPlayer, both shown in Figure 3.11.

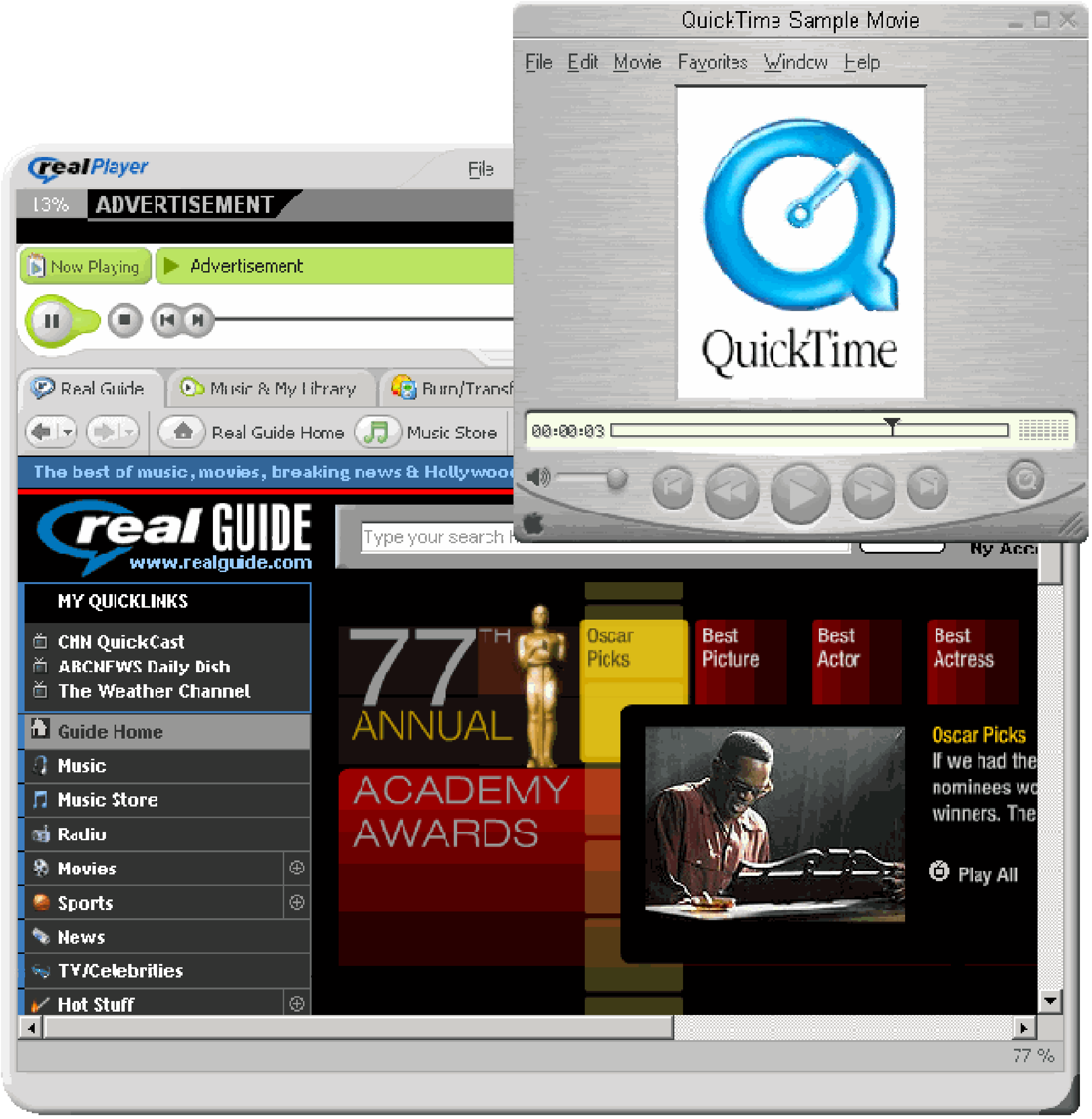


Figure 3.11: Apple QuickTime Player and RealPlayer.

As I said earlier, if you need Windows Media format support, you're stuck with Windows Media Player; if you don't, you can switch. Neither QuickTime nor Real Player, however, offers Windows Installer packages (as with Firefox, however, you can make your own package if you have an MSI packaging tool) and neither offer centralized management via Group Policy. However, for a media player application, neither of these features is likely to be critical.

Instant Messaging

Instant messaging is the next battleground for the corporate desktop. You really have two choices when it comes to alternatives: An alternative client that still allows you to use the Microsoft instant messaging network, or a completely different network—which will come with its own client, and can be a private network if desired.

The most popular alternative client is probably Cerulean Studios' Trillian (http://www.ceruleanstudios.com), a client that is compatible with America Online, ICQ, Microsoft, Yahoo, and Internet Relay Chat (IRC) instant messaging networks, allowing users to participate in one or more networks simultaneously, if desired. Again, third-party software vendors tend to not accommodate Windows-based enterprises in their efforts, and Trillian isn't available in a Windows Installer package and it doesn't support centralized management via GPO.

Why No GPO Functionality?

I don't know why third-party manufacturers don't make their products more manageable via GPO because doing so is simple enough: Simply store the application's settings in a specific area of the registry, then create text-based template files that tell the GPO Editor where those registry settings are and what they do. Doing so wouldn't change the way the application works or prevent it from working outside an Active Directory—AD—environment, so there seems little reason not to do it. Several of these alternative software applications would be more viable if their manufacturers would package them in Windows Installer files (for easier deployment) and make them GPO-manageable (for easier management).

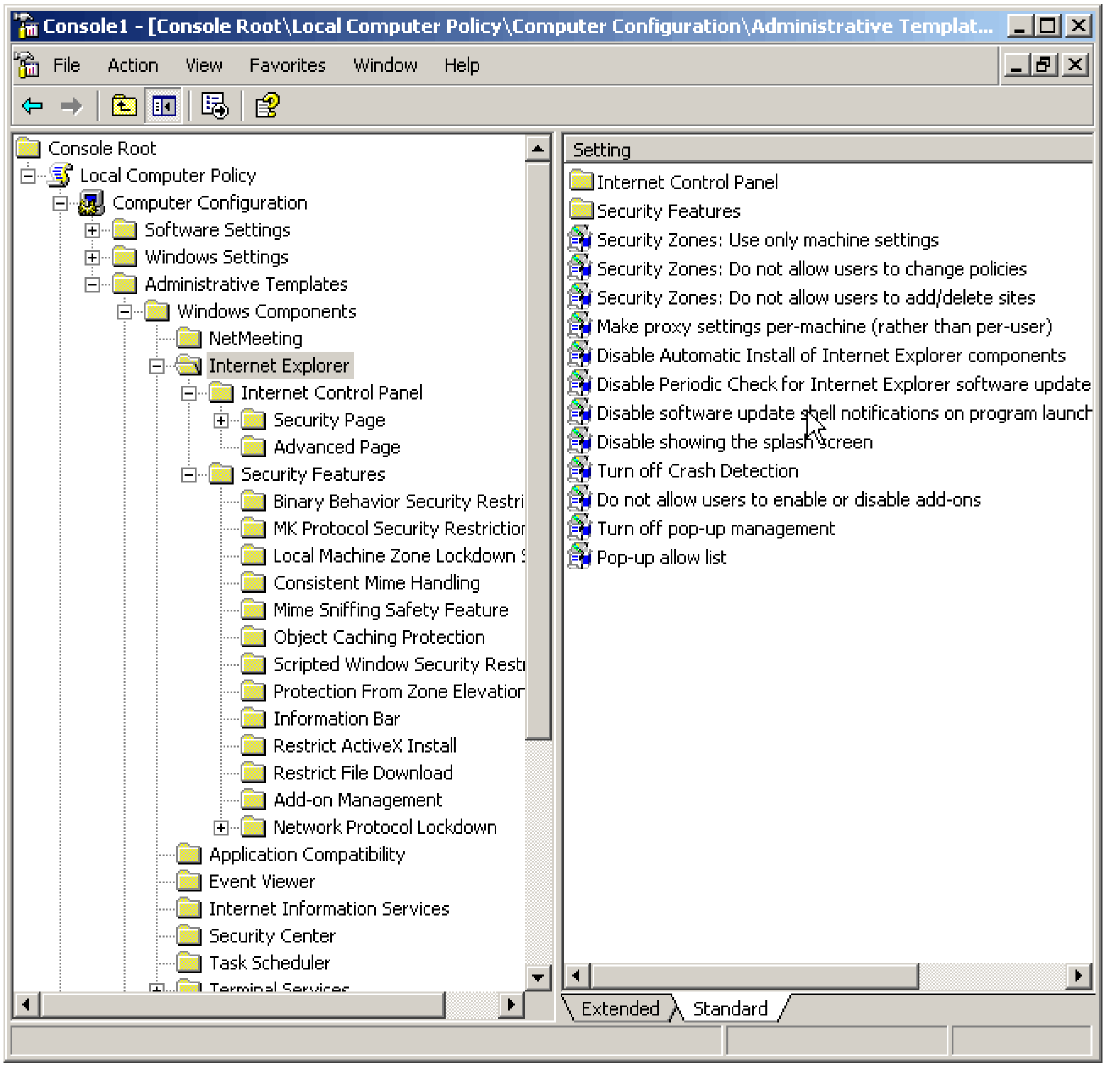
On the other end of the spectrum is a completely alternative instant messaging network, such as public networks from Yahoo or America Online, or your own private instant messaging network. The latter is becoming more popular within companies, as it provides the rapid communications benefits of instant messaging while keeping the corporate network (and its communications) more isolated from public networks. A huge variety of manufacturers offer private instant messaging solutions, including Jabber (http://www.jabber.com). Microsoft even offers Live Communications Server (LCS), a private network that uses the Windows Messenger client. Using LCS offers sufficient security benefits; by disconnecting Windows Messenger from the public network and only allowing it to use your private network, you markedly reduce the opportunities for the client to be attacked and its vulnerabilities to be exploited.

Coexistence: The Middle Ground

Although you can usually make an all-or-nothing decision with regards to Outlook Express, Windows Media Player, and Windows Messenger, IE is nearly always a sticking point. That leaves most companies in an awkward position: Ditch IE completely and risk a loss of functionality or keep using IE despite its shady security past?

There is a middle ground that might be a better choice. Use an alternative browser as users' main choice, and use IE only where needed. For example, if users' primary need for IE is for an intranet application, configure IE to *only* access the intranet, forcing users to employ a less-vulnerable and less-integrated browser in the more dangerous wilds of the Internet.

IE—especially in Windows XP SP2 and later—can be configured via GPO with a number of settings to restrict its behaviors and enhance its security (that is, make exploitable features more difficult, if not impossible, to use). Figure 3.12 shows a Windows XP Professional SP2 computer's local policy (which is the same as the centralized Group Policy that could be used to manage this computer), and all of the IE settings which are available.

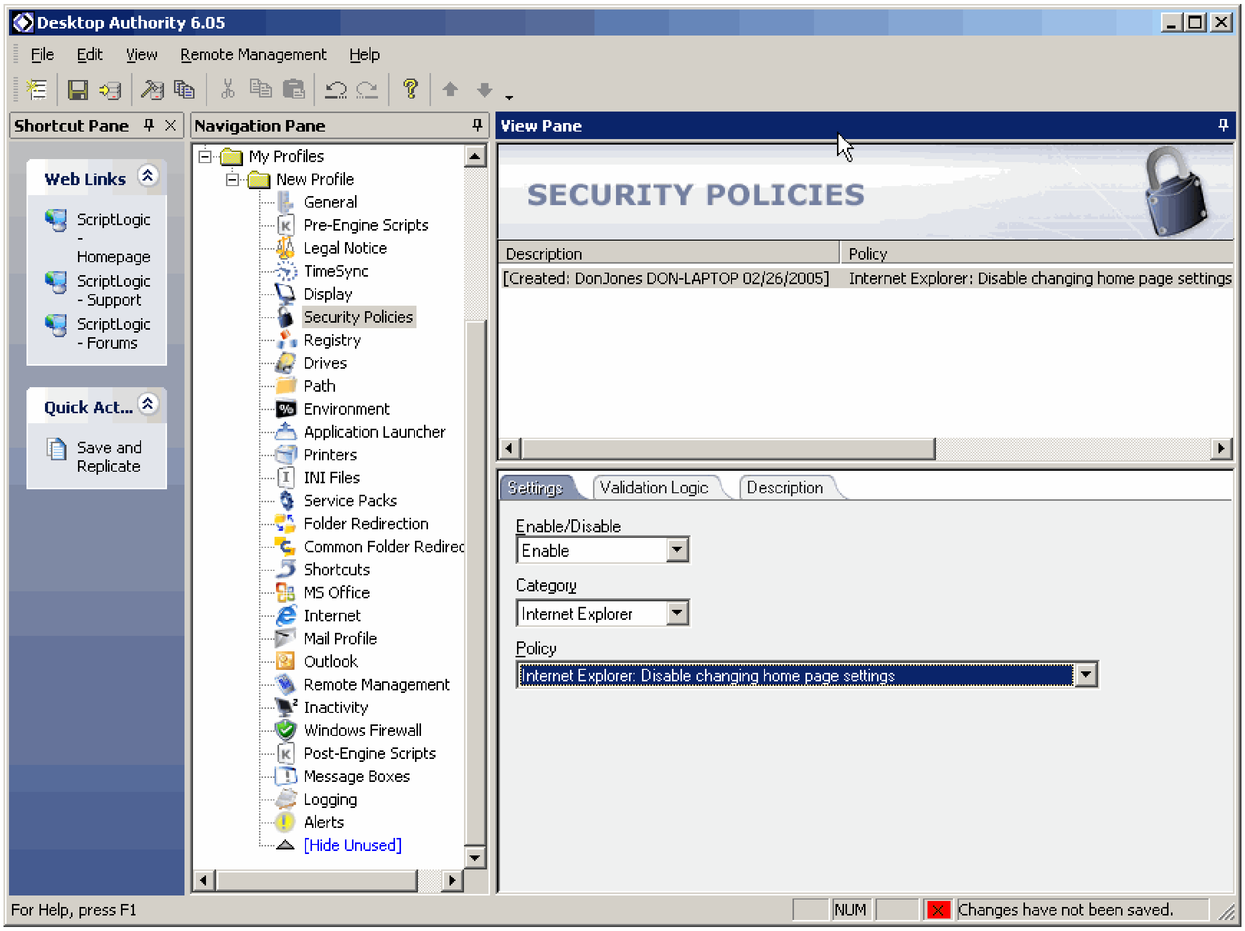

Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templat...
File
Action
View
Favorites
Window
Help
Setting
Extended
Standard

Console Root
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
        - NetMeeting
        - Internet Explorer
          - Internet Control Panel
            - Security Page
            - Advanced Page
          - Security Features
            - Binary Behavior Security Restri
            - MK Protocol Security Restrictior
            - Local Machine Zone Lockdown S
            - Consistent Mime Handling
            - Mime Sniffing Safety Feature
            - Object Caching Protection
            - Scripted Window Security Restr
            - Protection From Zone Elevatior
            - Information Bar
            - Restrict ActiveX Install
            - Restrict File Download
            - Add-on Management
            - Network Protocol Lockdown
        - Application Compatibility
        - Event Viewer
        - Internet Information Services
        - Security Center
        - Task Scheduler
        - Terminal Services

Setting
- Internet Control Panel
- Security Features
- Security Zones: Use only machine settings
- Security Zones: Do not allow users to change policies
- Security Zones: Do not allow users to add/delete sites
- Make proxy settings per-machine (rather than per-user)
- Disable Automatic Install of Internet Explorer components
- Disable Periodic Check for Internet Explorer software update
- Disable software update shell notifications on program launch
- Disable showing the splash screen
- Turn off Crash Detection
- Do not allow users to enable or disable add-ons
- Turn off pop-up management
- Pop-up allow list

Figure 3.12: Managing IE through Group Policy configurations.

You can use third-party tools to provide even more granular configuration. For example, Figure 3.13 shows ScriptLogic Desktop Authority, which can be used to set a few dozen IE-specific settings. This figure shows a policy that removes users' ability to change the browser's home page; combined with other settings, you might configure IE's home page to point directly to an intranet application that relies on IE-specific functionality. By preventing users from changing this location (hiding toolbars, disabling menu options, locking down the home page setting, and so forth), you turn IE into an application-specific tool. Users can use it only to access the one application that requires it and will be forced to use your alternative browser for other Web sites.



Description	Policy
[Created: DonJones DON-LAPTOP 02/26/2005]	Internet Explorer: Disable changing home page settings

Enable/Disable: Enable

Category: Internet Explorer

Policy: Internet Explorer: Disable changing home page settings

Changes have not been saved.

Figure 3.13: Locking down IE's functionality.

If IE will be needed for a broader range of sites, you can lock down problematic functionality, such as the ability to download ActiveX controls or browser helper objects (BHOs) by configuring the appropriate Desktop Authority settings.

Other tools that can help secure IE and restrict its functionality—helping ensure that users only use it where it's absolutely necessary—include Secure Browser by Tropical Software and IE Guardian by Devicode Technology.

Summary

This chapter has presented alternatives for the bundled software included with Windows: IE, Outlook Express, Windows Media Player, and Windows Messenger. We've explored how to remove, disable, or block access to these bundled applications—where possible—and covered some of the weaknesses of the alternatives. In the end, removing or disabling—where possible—Windows' bundled applications will help reduce your computers' attack surface; these bundled applications (particularly IE) are responsible for close to two-thirds of the Windows security vulnerabilities discovered in recent months.

The next chapter looks at securing AD, focusing—as in previous chapters—on often-overlooked areas of security, on consistency and auditing, and so forth. I'll walk through how AD configurations become gradually less secure over time and how you can combat this *security drift*, and I'll address some major weaknesses in AD's security support features, such as reporting.