Understanding Executable Content in Microsoft Products

Overview

Microsoft uses the concept of “unsafe file types” to help better protect users from executable content that an attacker could embed in such files. This document aims to help support personnel and knowledge workers:

* Understand the file types in Microsoft® products that are executable or potentially executable, and thereby might be considered “unsafe”
* Identify these executable file types as well as the potential impact of mishandling executable file types
* Use the safeguards in a number of Microsoft products that protect against mishandling executable file types

**This document discusses executable file types in the following Microsoft products:**

* Microsoft Windows®
  + Microsoft Windows 2000 Service Pack 4 (SP4)
  + Windows XP Service Pack 2 (SP2) and Service Pack 3 (SP3)
  + Windows Server® 2003 Service Pack 1 (SP1) and Service Pack 2 (SP2)
  + Windows Vista® RTM and SP1
  + Windows Server 2008
* Microsoft Internet Explorer® and Windows Internet Explorer®
  + Microsoft Internet Explorer 5
  + Microsoft Internet Explorer 6 RTM and SP1
  + Windows Internet Explorer 7
* Microsoft Office Outlook®
  + Microsoft Outlook 2000 SP3
  + Microsoft Outlook 2002 SP3
  + Microsoft Office Outlook 2003 SP2 and SP3
  + Microsoft Office Outlook 2007 RTM and SP1
* Microsoft Outlook Express and Windows Mail
  + Outlook Express 5
  + Outlook Express 6 RTM and SP1
  + Windows Mail
* Windows Messenger and Windows Live™ Messenger
  + Windows Messenger 4.7
  + Windows Messenger 5.1
  + Windows Live Messenger 8.1

# About Potentially Executable File Types

Many types of files are designed to invoke automated actions during ordinary use of the file, through the use of commands or script code. Obvious examples of this functionality include program files (.exe), batch files (.cmd and .bat), and script files (.vbs and .js). These files are designed for the sole purpose of executing commands. Less obvious examples are file types that allow for embedded script operations, such as Microsoft Access database files (.mdb) or Microsoft Visio templates (.vst).

The ability to perform script actions in applications can be a very powerful productivity tool that helps you customize Microsoft products to solve business problems. However, an attacker can leverage these same technologies to damage a user's computer. For example, an attacker could send executable code through a file attachment to an unwitting recipient in an e-mail message. Opening the attachment would then cause the code to be executed, which could harm the user’s computer or compromise the security of sensitive data.

## What file types are potentially executable?

A file type that is executable has the potential to harm your computer. For example, Visual Basic Scripting Edition (VBScript) files, which have the extension .vbs, can be used to automate tasks on your computer. Because this is an executable file type, an attacker can take advantage of this functionality when the file is opened by the user. As a result, this file type is considered potentially unsafe in many Microsoft products. In contrast, a file type that can be misused to exploit a vulnerability in an application or the operating system is not considered unsafe, because you can eliminate the danger by applying the correct security update[[1]](#footnote-2).

A potentially executable file type can be unsafe in some situations and not in others. Some potentially executable files only apply to certain applications, or in certain versions of Windows. For example, gadget files for the Windows Sidebar introduced in Windows Vista can contain executable code, so files with the .gadget extension are considered potentially executable file types in Windows Vista and Windows Server 2008. They are not considered unsafe for versions of Windows introduced before Windows Vista, because the Windows Sidebar is not a component of those Windows versions.

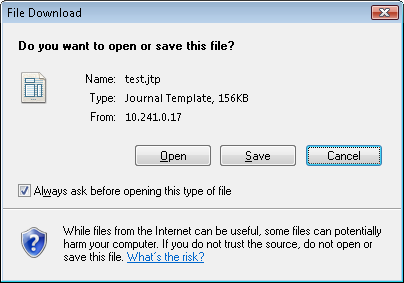
See “” for lists of file types that are considered unsafe in different situations.

## What happens when I encounter a file that is potentially executable?

Potentially executable file types are treated differently in different contexts. In some situations, as with Microsoft Office Outlook, access to the potentially executable file is blocked entirely; in others, the operating system or program displays a dialog box or message warning you of the potential risk.

### Microsoft Internet Explorer and Windows Internet Explorer

Ordinarily, when you click on a link to a downloadable file in Internet Explorer, the browser displays a standard dialog box with a number of options, such as this one from Windows Vista:



The options available in the dialog box vary depending on the versions of Windows and Internet Explorer you are using and the nature of the file. At the very least, you are prompted to save the file to a location on disk, or to cancel the download. If the file is of a type that Windows can open using an installed application, you are also typically given the option to open the file directly. For many file types, the dialog box displays an **Always ask before opening this type of file** check box. If you clear this check box and then open the file, Internet Explorer will automatically open all files of that type in the associated application in the future. In versions of Windows released since Windows XP SP2, the dialog box also includes a general advisory to be cautious about files downloaded from the Internet, accompanied by a graphic of a blue shield with a white question mark.

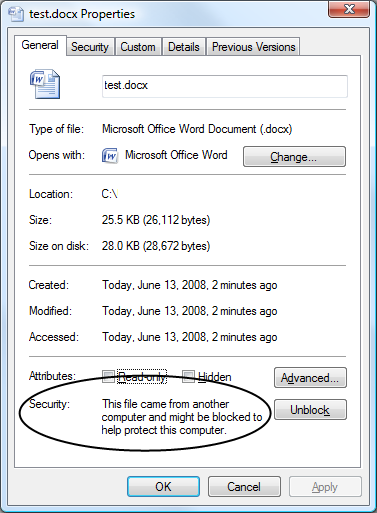
When you try to download a potentially executable file type that Internet Explorer considers potentially unsafe, the dialog box is different:



Here, Internet Explorer gives you a more specific warning that the file you are downloading is of a type that can potentially harm your computer. In recent versions of Windows, the graphic accompanying the warning is a yellow shield with a black exclamation mark. In addition, the dialog box does not give you the option to automatically open files of this type without confirmation in the future.

### Downloaded Files in Windows Explorer

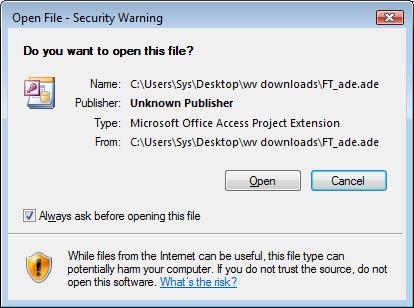
In Windows XP (SP2 and later), Windows Server 2003, Windows Vista, and Windows Server 2008, when you download a file from the Internet, a feature of Windows called the Attachment Execution Service (AES) saves information in the NTFS file system about the security zone from which the file was downloaded. You can see if a particular file has this zone identifier by right-clicking the file in Windows Explorer and then clicking **Properties**.



For more information about security zones, see “How to use security zones in Internet Explorer” (<http://support.microsoft.com/kb/174360>). See also the following for more information about AES: <http://technet.microsoft.com/en-us/library/bb457150.aspx> and <http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%202%20white%20paper.doc>.

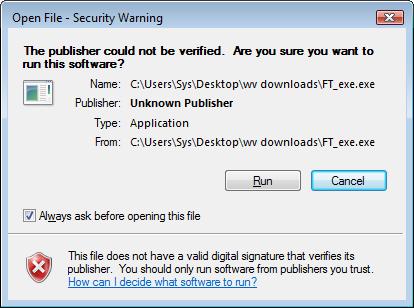
In addition to files you download directly, the AES also adds zone identifier information to any files you extract from compressed folders (extension .zip) or cabinet files (extension .cab) you download from the Internet zone if Windows Explorer is used to perform the file extraction from the compressed archive.

When you attempt to open a registered[[2]](#footnote-3) file type that is downloaded from the Internet zone in Windows Explorer, Windows determines whether the file type is considered potentially unsafe. If it is, Windows displays a warning dialog box. For most file types, including signed executable programs, the dialog box looks similar to this:

****

This dialog box is similar to the one displayed by Internet Explorer when you download a file that is potentially executable, and the warning message is the same. This time, however, the dialog box includes an **Always ask before opening this file** check box, which is checked by default. If you leave the box checked, Windows will display the security warning dialog box every time you open the file. If you clear the check box, you will remove the zone identifier information associated with the file, and Windows will not prompt you about it again.

If the file is of an executable type (such as .exe) and does not include a digital signature that verifies the publisher’s identity, the security warning dialog box is slightly different:[[3]](#footnote-4)



As with other files, clearing the **Always ask before opening this file** check box removes the zone identifier information from the file so that Windows will not prompt you about the file in the future.

### Microsoft E-mail Programs (Outlook, Outlook Express, and Windows Mail)

E-mail messages can include files enclosed as attachments. Unlike files you download from the Internet, you can’t control whether someone sends you files through e-mail. Therefore, instead of simply warning you about executable file types, recent versions of Outlook, Outlook Express, and Windows Mail go a step further and block potentially unsafe file types entirely.

In Outlook 2002 through Outlook 2007, Outlook Express 6,[[4]](#footnote-5) and Windows Mail, when you receive and open a message that includes a potentially unsafe attachment, Outlook displays the Message Bar and informs you that access to the attachment has been blocked.

C:\Users\migrady.REDMOND\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\ouss1.gif

Earlier versions of Outlook and Outlook Express were not as strict with potentially unsafe file types. In Outlook 2000, potentially executable file types are not blocked, but you are required to save potentially unsafe files to disk, rather than opening them directly from within Outlook. (Depending on how your network is configured, you may be required to save some types of files to disk in other versions of Outlook as well. Consult your network administrator for more information.) In Outlook Express 5, you can choose to either save potentially unsafe files or open them directly, but you cannot clear the **Always ask before opening this type of file** check box.

### Windows Messenger and Windows Live Messenger

Users can share files with one another using Windows Messenger and Windows Live Messenger. In Windows Messenger 4.7 and 5.1, when a user attempts to transfer a file to another Windows Messenger user, the Attachment Execution Service (AES) verifies the safety of the file type and blocks the transfer if it is determined to be potentially unsafe. (On Microsoft Windows 2000, which does not include the AES, Windows Messenger 5.1 uses a different mechanism to block files in conjunction with Internet Explorer.)

In Windows Live Messenger 8.1, you can transfer files to another user directly, or you can use a sharing folder. A sharing folder is a synchronized folder that appears on both your computer and your contact’s computer. To copy files to a sharing folder, you drag them from the folder on your computer where they are stored to the sharing folder window.

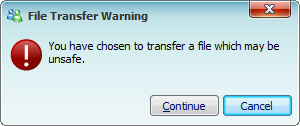
If Windows Live Messenger determines that you are attempting to share a potentially executable file and thereby potentially unsafe type, it blocks you from sharing the file, and your contact will not be able to see or access the file in his or her own sharing folder. Blocked files are indicated in the sharing folder window by a red circle with a white X:



In Windows Live Messenger, you can choose whether to allow or prevent direct transfers of potentially unsafe files. To block potentially unsafe file types, click **Tools**, click **Options**, click **File Transfer**, and then select the **Automatically reject file transfers for known unsafe file types** check box. If transfers of potentially unsafe file types are allowed, when you attempt to send or receive a file of a potentially unsafe type, Windows Live Messenger requires you to install the Windows Live OneCare safety scanner, which will automatically scan the file for viruses before allowing the transfer:



After the safety scanner is installed, when you try to transfer a potentially unsafe file, Windows Live Messenger displays a warning dialog box, but allows you to complete the transfer if you click **Continue**.



## Working with Potentially Executable Files

Many of the file types considered potentially unsafe by one or more Microsoft products contain potentially executable content and are also file types that people use every day to share ideas, collaborate, and get work done. By following a few rules and guidelines, you can share these files safely without worrying about restrictions.

The most important tool you can use when working with files over the Internet is *trust*. When you accept a file you should accept it based on the source and not the file type; there is no such thing as a “safe” file type from an untrusted source. Files that you download or receive from someone you know and trust are less likely to harm you or your computer than files you receive from people or sites you don’t know. However, some viruses have the ability to e-mail copies of themselves to people in a victim’s address book, so you can’t always assume a file is safe just because it comes from someone you know. Expanding on this, it’s also possible to spoof e-mail messages; a good site to reference regarding phishing scams and fraudulent e-mail is: <http://www.microsoft.com/protect/yourself/phishing/identify.mspx> . To protect yourself, only open files you expect to receive, or can confirm independently that your contact intended to send.

Some tips for sharing files safely over the Internet:

* Pay attention to the source of files you download from the Internet. In Internet Explorer, the Address bar and the File Download dialog box give you the location of the page or file you’re accessing. Be cautious about downloading from a Web site if you were referred there by e-mail from an unknown source. Also be wary if the site contains objectionable material, makes offers that seem too good to be true, or does not include a clearly written privacy statement.
* Outlook, Outlook Express, Windows Mail, Windows Messenger, and Windows Live Messenger do not block common Microsoft Office document types, such as .docx and .xls, or common text file types like .txt. These file types are the ones that most people use in their work. However, it is important to keep in mind that some files can contain macros that have the potential to spread viruses (on newer versions of Office, macros are disabled by default and so this is less of a concern). So whenever you receive such files in your e-mail or messaging program, it’s always safer to have up-to-date antivirus running, which can help detect threats like macro viruses.
* Another way to send files of blocked types is to use a zip program to package files before you send them to your contact. In the message, you can password-protect the zip file, include instructions that explain how to extract the files from the zipped package and communicate the password to the recipient out-of-band (e.g. over the phone or Instant Messenger). Of course, recipients should only open .zip files from trusted sources that they expect to receive.
* Instead of sending files in e-mail, you can post them to a secure network share, on your local network, or on the Internet using a service like Windows Live SkyDrive™ (<http://skydrive.live.com>). In your message to the recipients, you can include a link to the share.

For more information about protecting yourself from potentially unsafe files and other dangers online, visit <http://www.microsoft.com/protect>.

# Potentially Executable Content in Microsoft Products

The file type lists presented in this section are the default lists configured for the specified products. These lists should not be assumed to be comprehensive: updates, hotfixes, and other mechanisms may cause extensions to be added or removed from these lists, and your network administrator may choose to modify the lists to suit your organization’s needs. Consult your network administrator for information about any changes that have been made to the unsafe file lists.

## Microsoft Internet Explorer and Windows Internet Explorer

When you attempt to download a file in Internet Explorer, the **File Download** dialog box indicates whether the file type is executable or potentially executable and may be considered potentially unsafe. The appearance of the dialog box varies depending on the versions of Windows and Internet Explorer installed and the behavior modeled below is a Windows installation without Microsoft Office installed. See “Windows Internet Explorer” for more information.

|  | **Normal Dialog Box** | **Potentially Unsafe Dialog Box** |
| --- | --- | --- |
| Microsoft Windows 2000 SP4 (Internet Explorer 5) | 2K-IE5-2 | 2K-IE5-1 |
| Microsoft Windows 2000 SP4 (Internet Explorer 6) | 2K-IE6-2 | 2K-IE6-1 |
| Windows XP SP2 and SP3 | XP-2 | XP-1 |
| Windows Server 2003 SP1 and SP2 | WS-2 | WS-1 |
| Windows Vista RTM and SP1 | WV-2 | WV-1 |

|  |  |  |
| --- | --- | --- |
| Windows Vista SP1 and IE 8 | downlaod.JPG | maldownloadwarn.JPG\* Internet Explorer 8 includes SmartScreen Filter, a feature which detects known-malicious files and interrupts their download. |

The following file types are executable or potentially executable and considered potentially unsafe in one or more versions of Internet Explorer, as noted.

| **Extension** | **Description** | **Potentially Unsafe in…** |
| --- | --- | --- |
| .ade | Access Project Extension | All |
| .adp | Access Project | All |
| .app | Executable Application | All except Microsoft Windows 2000 SP4 |
| .bas | BASIC Source Code | All |
| .bat | Batch Processing | All |
| .cer | Internet Security Certificate File | All |
| .chm | Compiled HTML Help | All |
| .cmd | DOS CP/M Command File, Command File for Windows NT | All |
| .com | Command | All |
| .cpl | Windows Control Panel Extension | All |
| .crt | Certificate File | All |
| .csh | UNIX Shell Script | All except Microsoft Windows 2000 SP4 |
| .der | DER Encoded X509 Certificate File | All |
| .exe | Executable File | All |
| .fxp | FoxPro Compiled Source | All except Microsoft Windows 2000 SP4 |
| .gadget | Sidebar Gadget | Windows Vista, Windows Server 2008 |
| .grp | Microsoft Program Group | All except Microsoft Windows 2000 SP4 |
| .hlp | Windows Help File | All |
| .hta | Hypertext Application | All |
| .inf | Information or Setup File | All |
| .ins | IIS Internet Communications Settings | All |
| .isp | IIS Internet Service Provider Settings | All |
| .its | Internet Document Set | All |
| .js | JavaScript Source Code | All |
| .jse | JScript Encoded Script File | All |
| .ksh | UNIX Shell Script | All except Microsoft Windows 2000 SP4 |
| .lnk | Windows Shortcut File | All |
| .mad | Access Module Shortcut | All except Microsoft Windows 2000 SP4 |
| .maf | Access Form | All except Microsoft Windows 2000 SP4 |
| .mag | Access Diagram Shortcut | All except Microsoft Windows 2000 SP4 |
| .mam | Access Macro Shortcut | All except Microsoft Windows 2000 SP4 |
| .maq | Access Query Shortcut | All except Microsoft Windows 2000 SP4 |
| .mar | Access Report Shortcut | All except Microsoft Windows 2000 SP4 |
| .mas | Access Stored Procedures | All except Microsoft Windows 2000 SP4 |
| .mat | Access Table Shortcut | All except Microsoft Windows 2000 SP4 |
| .mau | Media Attachment Unit | All except Microsoft Windows 2000 SP4 |
| .mav | Access View Shortcut | All except Microsoft Windows 2000 SP4 |
| .maw | Access Data Access Page | All except Microsoft Windows 2000 SP4 |
| .mda | Access Add-in | All except Microsoft Windows 2000 SP4 |
| .mdb | Access Database | All |
| .mde | Access MDE Database File | All |
| .mdt | Access Add-in Data | All |
| .mdw | Access Workgroup Information | All |
| .mdz | Access Wizard Template | All except Microsoft Windows 2000 SP4 |
| .msc | Microsoft Management Console Snap-in Control File | All |
| .msh | Microsoft Shell | All except Microsoft Windows 2000 SP4 |
| .mshxml | Microsoft Shell | All except Microsoft Windows 2000 SP4 |
| .msi | Windows Installer File | All |
| .msp | Windows Installer Update | All |
| .mst | Windows SDK Setup Transform Script | All |
| .ocx | ActiveX Control | Windows XP, Windows Vista, Window Server 2008 |
| .ops | Office Profile Settings File | All except Microsoft Windows 2000 SP4 |
| .pcd | Visual Test | All |
| .pif | MSDOS shortcut | All |
| .prf | PICS Rules File | All except Microsoft Windows 2000 SP4 |
| .prg | Program File | All except Microsoft Windows 2000 SP4 |
| .pst | Outlook Personal Folder File | All except Microsoft Windows 2000 SP4 |
| .reg | Registry Data File | All |
| .scf | Windows Explorer Command | All except Microsoft Windows 2000 SP4 |
| .scr | Windows Screen Saver | All |
| .sct | Windows Script Component | All |
| .shb | Windows Shortcut into a Document | All |
| .shs | Shell Scrap Object File | All |
| .tmp | Temporary File/Folder | All |
| .url | Internet Location | All |
| .vbe | VBScript Encoded Script File | All |
| .vbs | VBScript Script File, Visual Basic for Applications Script | All |
| .vsd | Visio Drawing | Microsoft Windows 2000 SP4 |
| .vsmacros | Visual Studio .NET Binary-based Macro Project | All |
| .vss | Visio Stencil | All |
| .vst | Visio Template | All |
| .vsw | Visio Workspace File | All |
| .ws | Windows Script File | All |
| .wsc | Windows Script Component | All |
| .wsf | Windows Script File | All |
| .wsh | Windows Script Host Settings File | All |
| .zip | Compressed (zipped) Folder | Microsoft Windows 2000 SP4 with Internet Explorer 5 |

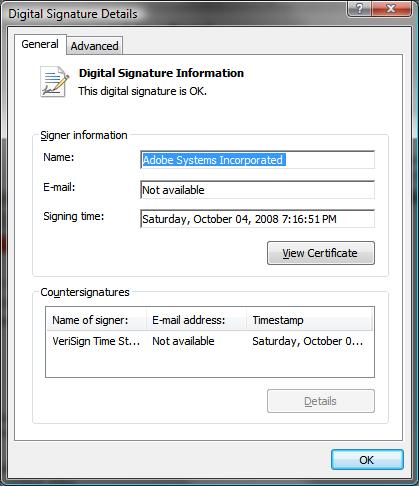
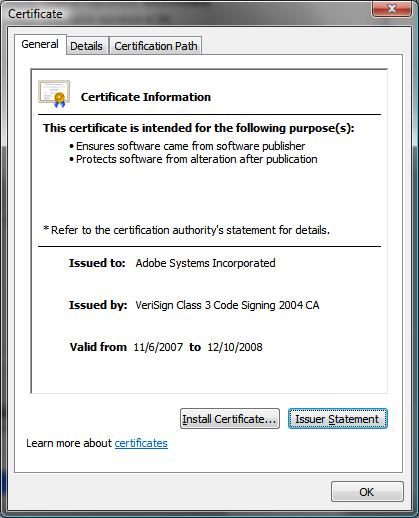
## Windows Explorer (Shell Execution)

Since Windows XP SP2, the Attachment Execution Service (AES) can help verify the origins of downloaded files[[5]](#footnote-6). In Windows Explorer, when you open a potentially unsafe file that has been downloaded from the Internet zone, the **Open File – Security Warning** dialog box displays. The appearance of the dialog box varies depending on the version of Windows installed, and on whether the file is considered an executable type. Microsoft Windows 2000 SP4 does not use AES and does not display these dialog boxes. See “Downloaded Files in Windows Explorer” for more information.

|  | **Unsigned Executable** | **Other Potentially Unsafe File Type** |
| --- | --- | --- |
| Windows XP SP2 and SP3 | XP-15 | XP-17 |
| Windows Server 2003 SP1 and SP2 | WS-15 | **WS-17** |
| Windows Vista RTM and SP1 | WV-15 | **WV-17** |

For reference, digital signatures provide a way to determine the identity of the creator or publisher of a file, to reveal whether the file has been altered since it was signed, and to verify when it was signed. A warning dialog is still displayed, but it’s much less ominous and a hyperlink to the digital certificate is provided, giving the user more confidence that the file is safe to open. Prior to Windows XP SP2, for most users there was no obvious difference between a signed and unsigned executable. But since Windows XP SP2, when opening a program or installing an Internet Explorer add-on, an enhanced message will show. For instance, Internet Explorer will show you are about to install a signed control with an “Internet Explorer Add-on Installer – Security Warning”. If you click on the Publisher’s name you will see “Digital Signature Details” showing that it is trusted (“the digital signature is OK”) and time stamped (“Countersignatures”). Next, if you click “View Certificate” you will see the Certificate itself, indicating the intended purpose(s), the subject name (“Issued to”), and the authority (“Issued by”), and the validity period (“Valid from”). This is all shown below.



Files of the following types are considered potentially executable when downloaded from the Internet zone, and display the **Open File – Security Warning** dialog box as shown in the “Unsigned Executable” column above.

| **Extension** | **Description** |
| --- | --- |
| .bas | BASIC Source Code |
| .bat | Batch Processing |
| .cmd | DOS CP/M Command File, Command File for Windows NT |
| .com | Command |
| .exe | Executable File |
| .hta | Hypertext Application |
| .msi | Windows Installer File |
| .pif | MSDOS shortcut |
| .reg | Registry Data File |
| .scr | Windows Screen Saver |
| .vb | Visual Basic Source |
| .vbs | VBScript Script File, Visual Basic for Applications Script |

Files of the following types are considered potentially executable files when downloaded from the Internet zone, and display the **Open File – Security Warning** dialog box as shown in the “Other Potentially Unsafe File Type” column above.

| **Extension** | **Description** |
| --- | --- |
| .ade | Access Project Extension |
| .adp | Access Project |
| .app | Executable Application |
| .cer | Internet Security Certificate File |
| .chm | Compiled HTML Help |
| .cpl | Windows Control Panel Extension |
| .crt | Certificate File |
| .csh | UNIX Shell Script |
| .der | DER Encoded X509 Certificate File |
| .fxp | FoxPro Compiled Source |
| .gadget (Windows Vista only) | Windows Vista Sidebar Gadget |
| .hlp | Windows Help File |
| .inf | Information or Setup File |
| .ins | IIS Internet Communications Settings |
| .isp | IIS Internet Service Provider Settings |
| .its | Internet Document Set |
| .js | JavaScript Source Code |
| .jse | JScript Encoded Script File |
| .ksh | UNIX Shell Script |
| .mad | Access Module Shortcut |
| .maf | Access Form |
| .mag | Access Diagram Shortcut |
| .mam | Access Macro Shortcut |
| .maq | Access Query Shortcut |
| .mar | Access Report Shortcut |
| .mas | Access Stored Procedures |
| .mat | Access Table Shortcut |
| .mau | Media Attachment Unit |
| .mav | Access View Shortcut |
| .maw | Access Data Access Page |
| .mda | Access Add-in |
| .mdb | Access Database |
| .mde | Access MDE Database File |
| .mdt | Access Add-in Data |
| .mdw | Access Workgroup Information |
| .mdz | Access Wizard Template |
| .msc | Microsoft Management Console Snap-in Control File |
| .msp | Windows Installer Update |
| .mst | Windows SDK Setup Transform Script |
| .ops | Office Profile Settings File |
| .pcd | Visual Test |
| .prf | PICS Rules File |
| .prg | Program File |
| .scf | Windows Explorer Command |
| .sct | Windows Script Component |
| .shb | Windows Shortcut into a Document |
| .shs | Shell Scrap Object File |
| .tmp | Temporary File |
| .vbe | VBScript Encoded Script File |
| .vbs | VBScript Script File, Visual Basic for Applications Script |
| .vdx | Visio 2003 XML Drawing |
| .vsd | Visio Drawing |
| .vsmacros | Visual Studio .NET Binary-based Macro Project |
| .vss | Visio Stencil |
| .vst | Visio Template |
| .vsw | Visio Workspace File |
| .vsx | Visio XML Stencil |
| .vtx | Visio XML Template |
| .ws | Windows Script File |
| .wsc | Windows Script Component |
| .wsf | Windows Script File |
| .wsh | Windows Script Host Settings File |

## Microsoft Office Outlook

In Microsoft Office Outlook, when you receive a message containing an attachment of a potentially unsafe type, you are required to save the file to disk (Outlook 2000), or the attachment is blocked altogether (Outlook 2002 through 2007). In Outlook 2000, the **Attachment Security Warning** dialog box displays when you attempt to open a potentially unsafe attachment. In Outlook 2002 through 2007, the Message Bar displays when you open or preview the message.

|  | **Normal Dialog Box** | **Potentially Unsafe Dialog Box** |
| --- | --- | --- |
| Outlook 2000 | WS-4 | WS-3 |
| Outlook 2002 | 2K-6 | XPSECU08 |
| Outlook 2003 | WS-8 | C:\Users\migrady.REDMOND\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\ouss1.gif |
| Outlook 2007 | WS-10 | blocked.PNG |

The following file types are considered potentially unsafe executable files in one or more versions of Outlook, as noted.

| **Extension** | **Description** | **Blocked in…** |
| --- | --- | --- |
| .ade | Access Project Extension | All |
| .adp | Access Project | All |
| .app | Executable Application | Outlook 2002 and later versions |
| .asp | Active Server Page | Outlook 2002 and later versions |
| .bas | BASIC Source Code | All |
| .bat | Batch Processing | All |
| .cer | Internet Security Certificate File | Outlook 2002 and later versions |
| .chm | Compiled HTML Help | All |
| .cmd | DOS CP/M Command File, Command File for Windows NT | All |
| .com | Command | All |
| .cpl | Windows Control Panel Extension | All |
| .crt | Certificate File | All |
| .csh | UNIX Shell Script | Outlook 2002 and later versions |
| .der | DER Encoded X509 Certificate File | Outlook 2003 SP3 and later versions |
| .exe | Executable File | All |
| .fxp | FoxPro Compiled Source | Outlook 2002 and later versions |
| .gadget | Windows Vista Gadget | Outlook 2003 SP3, Outlook 2007 SP1 |
| .hlp | Windows Help File | All |
| .hta | Hypertext Application | All |
| .inf | Information or Setup File | All |
| .ins | IIS Internet Communications Settings | All |
| .isp | IIS Internet Service Provider Settings | All |
| .its | Internet Document Set | Outlook 2002 and later versions |
| .js | JavaScript Source Code | All |
| .jse | JScript Encoded Script File | All |
| .ksh | UNIX Shell Script | Outlook 2002 and later versions |
| .lnk | Windows Shortcut File | All |
| .mad | Access Module Shortcut | Outlook 2002 and later versions |
| .maf | Access Form | Outlook 2002 and later versions |
| .mag | Access Diagram Shortcut | Outlook 2002 and later versions |
| .mam | Access Macro Shortcut | Outlook 2002 and later versions |
| .maq | Access Query Shortcut | Outlook 2002 and later versions |
| .mar | Access Report Shortcut | Outlook 2002 and later versions |
| .mas | Access Stored Procedures | Outlook 2002 and later versions |
| .mat | Access Table Shortcut | Outlook 2002 and later versions |
| .mau | Media Attachment Unit | Outlook 2002 and later versions |
| .mav | Access View Shortcut | Outlook 2002 and later versions |
| .maw | Access Data Access Page | Outlook 2002 and later versions |
| .mda | Access Add-in | All |
| .mdb | Access Database | All |
| .mde | Access MDE Database File | All |
| .mdt | Access Add-in Data | Outlook 2002 and later versions |
| .mdw | Access Workgroup Information | Outlook 2002 and later versions |
| .mdz | Access Wizard Template | All |
| .msc | Microsoft Management Console Snap-in Control File | All |
| .msh | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .msh1 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .msh1xml | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .msh2 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .msh2xml | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .mshxml | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .msi | Windows Installer File | All |
| .msp | Windows Installer Update | All |
| .mst | Windows SDK Setup Transform Script | All |
| .ops | Office Profile Settings File | Outlook 2002 and later versions |
| .pcd | Visual Test | All |
| .pif | MSDOS shortcut | Outlook 2002 and later versions |
| .plg | Developer Studio Build Log | Outlook 2003 SP3 and later versions |
| .prf | PICS Rules File | Outlook 2002 and later versions |
| .prg | Program File | Outlook 2002 and later versions |
| .ps1 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .ps1xml | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .ps2 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .ps2xml | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .psc1 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .psc2 | Windows PowerShell | Outlook 2003 SP3 and later versions |
| .pst | Outlook Personal Folders File | Outlook 2002 and later versions |
| .reg | Registry Data File | All |
| .scf | Windows Explorer Command | Outlook 2002 and later versions |
| .scr | Windows Screen Saver | All |
| .sct | Windows Script Component | All |
| .shb | Windows Shortcut into a Document | All |
| .shs | Shell Scrap Object File | All |
| .snp | Snapshot File | All |
| .tmp | Temporary File | Outlook 2002 and later versions |
| .url | Internet Location | All |
| .vb | VBScript File | All |
| .vbe | VBScript Encoded Script File | All |
| .vbs | VBScript Script File, Visual Basic for Applications Script | All |
| .vsmacros | Visual Studio .NET Binary-based Macro Project | Outlook 2002 and later versions |
| .vss | Visio Stencil | Outlook 2002 and later versions |
| .vst | Visio Template | Outlook 2002 and later versions |
| .vsw | Visio Workspace File | Outlook 2002 and later versions |
| .ws | Windows Script File | Outlook 2002 and later versions |
| .wsc | Windows Script Component | All |
| .wsf | Windows Script File | All |
| .wsh | Windows Script Host Settings File | All |
| .xnk | Exchange Public Folder Shortcut | Outlook 2003 SP3 and later versions |

## Outlook Express and Windows Mail

In Microsoft Outlook Express and Windows Mail, when you receive a message containing an attachment of a potentially unsafe type, you are prompted to open or save the file (Outlook Express 5), or the attachment is blocked altogether (Outlook Express and Windows Mail). In Outlook Express 5, the **Open Attachment Warning** dialog box does not allow you to clear the **Always ask before opening this type of file** check box when you attempt to open a potentially unsafe attachment. In Outlook Express 6 RTM and SP1 and Windows Mail, the Message Bar displays when you open or preview the message.

|  | **Normal Dialog Box** | **Potentially Unsafe Dialog Box** |
| --- | --- | --- |
| Outlook Express 5 | 2K-14 | 2K-13 |
| Outlook Express 6 RTM and SP1 | WS-12 | oe.png |
| Windows Mail | WV-12 | windowsmail.png |

The following file types are considered potentially unsafe executable files in Outlook Express 5, Outlook Express 6 (**except** on Microsoft Windows 2000 SP4), and/or Windows Mail, as noted. See page 24 for information about Outlook Express 6 SP1 on Microsoft Windows 2000 SP4.

| **Extension** | **Description** | **Blocked in…** |
| --- | --- | --- |
| .ade | Access Project Extension | All |
| .adp | Access Project | All |
| .app | Executable Application | Outlook Express 6, Windows Mail |
| .application | Executable Application | Outlook Express 6 |
| .asa | ASP Configuration File | Outlook Express 6, Windows Mail |
| .asp | Active Server Page | All |
| .bas | BASIC Source Code | All |
| .bat | Batch Processing | All |
| .cdx | FoxPro Compound Index | Outlook Express 6 |
| .cer | Internet Security Certificate File | Outlook Express 6, Windows Mail |
| .chm | Compiled HTML Help | All |
| .cmd | Command File | All |
| .com | Command | All |
| .cpl | Windows Control Panel Extension | All |
| .crt | Certificate File | All |
| .csh | UNIX Shell Script | Outlook Express 6, Windows Mail |
| .der | DER Encoded X509 Certificate File | Outlook Express 6, Windows Mail |
| .exe | Executable File | All |
| .fxp | FoxPro Compound Source | Outlook Express 6, Windows Mail |
| .grp | Windows Program Manager Group | Windows Mail |
| .hlp | Windows Help File | All |
| .hta | Hypertext Application | All |
| .inf | Information or Setup File | All |
| .ins | IIS Internet Communications Settings | All |
| .isp | IIS Internet Service Provider Settings | All |
| .its | Internet Document Set | All |
| .js | JavaScript Source Code | All |
| .jse | JScript Encoded Script File | All |
| .ksh | UNIX Shell Script | Outlook Express 6, Windows Mail |
| .lnk | Windows Shortcut File | All |
| .mad | Access Module Shortcut | Outlook Express 6, Windows Mail |
| .maf | Access Form | Outlook Express 6, Windows Mail |
| .mag | Access Diagram Shortcut | Outlook Express 6, Windows Mail |
| .mam | Access Macro Shortcut | Outlook Express 6, Windows Mail |
| .maq | Access Query Shortcut | Outlook Express 6, Windows Mail |
| .mar | Access Report Shortcut | Outlook Express 6, Windows Mail |
| .mas | Access Stored Procedures | Outlook Express 6, Windows Mail |
| .mat | Access Table Shortcut | Outlook Express 6, Windows Mail |
| .mau | Media Attachment Unit | Outlook Express 6, Windows Mail |
| .mav | Access View Shortcut | Outlook Express 6, Windows Mail |
| .maw | Access Data Access Page | Outlook Express 6, Windows Mail |
| .mda | Access Add-in | Outlook Express 6, Windows Mail |
| .mdb | Access Database | All |
| .mde | Access MDE Database File | All |
| .mdt | Access Add-in Data | All |
| .mdw | Access Workgroup Information | All |
| .mdz | Access Wizard Template | Outlook Express 6, Windows Mail |
| .msc | Microsoft Management Console Snap-in Control File | All |
| .msh | Windows PowerShell | Windows Mail |
| .mshxml | Windows PowerShell | Windows Mail |
| .msi | Windows Installer File | All |
| .msp | Windows Installer Update | All |
| .mst | Windows SDK Setup Transform Script | All |
| .ocx | ActiveX Control | Outlook Express 6, Windows Mail |
| .ops | Office Profile Settings File | All |
| .pcd | Visual Test | All |
| .pif | MSDOS shortcut | All |
| .plg | Developer Studio Build Log | Outlook Express 6 |
| .prf | PICS Rules File | Outlook Express 6, Windows Mail |
| .prg | Program File | Outlook Express 6, Windows Mail |
| .pst | Outlook Personal Folders File | Outlook Express 6, Windows Mail |
| .reg | Registry Data File | All |
| .scf | Windows Explorer Command | Outlook Express 6, Windows Mail |
| .scr | Windows Screen Saver | All |
| .sct | Windows Script Component | All |
| .shb | Windows Shortcut into a Document | All |
| .shs | Shell Scrap Object File | All |
| .tmp | Temporary File | All |
| .url | Internet Location | All |
| .vb | VBScript File | All |
| .vbe | VBScript Encoded Script File | All |
| .vbs | VBScript Script File, Visual Basic for Applications Script | All |
| .vsmacros | Visual Studio .NET Binary-based Macro Project | Outlook Express 6, Windows Mail |
| .vss | Visio Stencil | Outlook Express 5, Outlook Express 6 |
| .vst | Visio Template | Outlook Express 5, Outlook Express 6 |
| .vsw | Visio Workspace File | Outlook Express 5, Outlook Express 6 |
| .ws | Windows Script File | All |
| .wsc | Windows Script Component | All |
| .wsf | Windows Script File | All |
| .wsh | Windows Script Host Settings File | All |

The Internet Explorer 6 SP1 upgrade for Microsoft Windows 2000 SP4 included a version of Outlook Express 6 that blocks all file attachments by default, except for file types associated with Internet Explorer and Windows Media Player. Files that are not blocked open in the associated program without a dialog box.

The following file types are **not** blocked by Outlook Express 6 SP1 on Microsoft Windows 2000 SP4.

| **Extension** | **Description** |
| --- | --- |
| .aif | Audio Interchange File Format |
| .aifc | Compressed Audio Interchange File |
| .aiff | Audio Interchange File Format |
| .asf | Advanced Systems Format |
| .asx | ASF Redirector |
| .au | Audio File |
| .avi | Audio Video Interleave |
| .cdf | Channel Definition Format |
| .cnf | Conference Link |
| .htt | Hypertext Template File |
| .icc | ICC Profile |
| .mv1 | MPEG File |
| .m3u | Media Playlist File |
| .mid | MIDI File |
| .midi | MIDI File |
| .mp2 | MPEG Layer II Compressed Audio File |
| .mp3 | MP3 Audio File |
| .mpa | MPEG Audio File |
| .mpe | MPEG Video File |
| .mpeg | MPEG Video File |
| .mpg | MPEG Video File |
| .mpv2 | MPEG-2 Video Stream |
| .mp2v | MPEG File |
| .rmi | RMID MIDI File |
| .snd | Sound File |
| .wav | WAVE Audio File |
| .wax | Windows Media Audio Redirect |
| .wma | Windows Media Audio File |
| .wmv | Windows Media Video File |
| .wmx | Windows Media Redirect |
| .xml | XML File |
| .xsl | XML Stylesheet |

## Windows Messenger and Windows Live Messenger

Windows Messenger blocks you from sending or receiving potentially unsafe files in instant message conversations. Windows Live Messenger lets you choose whether to allow or prevent direct transfers of potentially unsafe files, but blocks potentially unsafe files you add to sharing folders.

On Microsoft Windows 2000, the list of file types Windows Messenger considers potentially unsafe depends on the version of Internet Explorer installed. All supported editions of Windows XP, Windows Server 2003, and Windows Vista all use the same list of potentially unsafe file types for Windows Messenger 4.7 and 5.1 and Windows Live Messenger 8.1.

| **Extension** | **Description** | **Potentially Unsafe in…** |
| --- | --- | --- |
| .ade | Access Project Extension | All |
| .adp | Access Project | All |
| .app | Executable Application | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .asa | ASP Configuration File | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4, and Windows Live Messenger 8.1 |
| .asp | Active Server Page | All |
| .bas | BASIC Source Code | All |
| .bat | Batch Processing | All |
| .cdx | FoxPro Compound Index | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4, and Windows Live Messenger 8.1 |
| .cer | Internet Security Certificate File | All |
| .chm | Compiled HTML Help | All |
| .cmd | DOS CP/M Command File, Command File for Windows NT | All |
| .com | Command | All |
| .cpl | Windows Control Panel Extension | All |
| .crt | Certificate File | All |
| .csh | UNIX Shell Script | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .der | DER Encoded X509 Certificate File | All except Windows Live Messenger 8.1 |
| .exe | Executable File | All |
| .fxp | FoxPro Compiled Source | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .hlp | Windows Help File | All |
| .hta | Hypertext Application | All |
| .inf | Information or Setup File | All |
| .ins | IIS Internet Communications Settings | All |
| .isp | IIS Internet Service Provider Settings | All |
| .its | Internet Document Set | All |
| .js | JavaScript Source Code | All |
| .jse | JScript Encoded Script File | All |
| .ksh | UNIX Shell Script | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .lnk | Windows Shortcut File | All |
| .mad | Access Module Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .maf | Access Form | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mag | Access Diagram Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mam | Access Macro Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .maq | Access Query Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mar | Access Report Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mas | Access Stored Procedures | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mat | Access Table Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mau | Media Attachment Unit | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mav | Access View Shortcut | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .maw | Access Data Access Page | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mda | Access Add-in | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .mdb | Access Database | All |
| .mde | Access MDE Database File | All |
| .mdt | Access Add-in Data | All |
| .mdw | Access Workgroup Information | All |
| .mdz | Access Wizard Template | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .msc | Microsoft Management Console Snap-in Control File | All |
| .msi | Windows Installer File | All |
| .msp | Windows Installer Update | All |
| .mst | Windows SDK Setup Transform Script | All |
| .ocx | ActiveX Control | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4, and Windows Live Messenger 8.1 |
| .ops | Office Profile Settings File | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .pcd | Visual Test | All |
| .pif | MS-DOS shortcut | All |
| .prf | PICS Rules File | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .prg | Program File | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .pst | Outlook Personal Folders File | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .reg | Registry Data File | All |
| .scf | Windows Explorer Command | All except Windows Messenger 5.1 on Microsoft Windows 2000 SP4 |
| .scr | Windows Screen Saver | All |
| .sct | Windows Script Component | All |
| .shb | Windows Shortcut into a Document | All |
| .shs | Shell Scrap Object File | All |
| .tmp | Temporary File | All |
| .url | Internet Location | All |
| .vb | VBScript File | All |
| .vbe | VBScript Encoded Script File | All |
| .vbs | VBScript Script File, Visual Basic for Applications Script | All |
| .vsd | Visio Drawing | Windows Messenger 5.1 on Microsoft Windows 2000 SP4; Windows Live Messenger 8.1 |
| .vsmacros | Visual Studio .NET Binary-based Macro Project | All |
| .vss | Visio Stencil | All |
| .vst | Visio Template | All |
| .vsw | Visio Workspace File | All |
| .ws | Windows Script File | All |
| .wsc | Windows Script Component | All |
| .wsf | Windows Script File | All |
| .wsh | Windows Script Host Settings File | All |

# Appendix

## Functional Evolution of Identifying and Blocking Potentially Unsafe Files

Starting with Microsoft Windows 2000 SP4, Microsoft began the process of adding warning dialog boxes into the user experience to provide additional information to users that their systems may be put at risk by running certain types of files downloaded from the Internet. The following provides a general overview of the functional evolution of identifying and/or blocking potentially executable or executable content in Windows and Windows applications from Microsoft Windows 2000 SP4 through Windows Vista.

* **Microsoft Windows 2000 SP4**
  + Internet Explorer 5 warns users with a different dialog box when they attempt to download or open a potentially executable file.
  + Outlook Express 5 warns users if they want to save a potentially executable file.
  + Internet Explorer 6 SP1 – Downloadable upgrade with updated list of blocked file types.
  + Outlook Express 6 SP1 – Included in the Internet Explorer 6 SP1 upgrade. Prevents users from downloading potentially unsafe attachments. User is informed of which attachments were blocked.
* **Windows XP SP2 and SP3**
  + Attachment Execution Service (AES) added to assist in the identification of potentially executable files.
  + New zone information added for files in the NTFS file system; the information is set when a file is downloaded to the system from the Web.
  + Additional warning dialog boxes when a downloaded file attempts to launch using the Windows shell.
  + Internet Explorer 6 and Outlook Express 6 ship by default on Windows XP SP2.
* **Windows Server 2003 SP1 and SP2**
  + Includes AES and the NTFS file system zone information.
* **Windows Vista RTM and SP1**
  + Includes an upgraded mail client, Windows Mail, with additional blocked file types.
* **Internet Explorer 5 (IE 5)**
  + Shipped on Microsoft Windows 2000 SP4.
  + Includes static list of blocked file types.
* **Internet Explorer 6 (IE 6)** 
  + Downloadable upgrade for Microsoft Windows 2000 SP4.
  + Blocked file type list updated to match list used in Microsoft Office.
* **Internet Explorer 6 (IE 6) Updates for Windows XP SP2+**
  + Shipped on Windows XP SP2 and Windows Server 2003 SP1 and SP2.
* **Internet Explorer 7 (IE 7)**
  + Shipped on Windows Vista and Windows Server 2008.
  + Downloadable upgrade for Windows XP SP2 and SP3 and Windows Server 2003 SP1 and SP2.
* **Office 2000 SP3**
  + Includes notification of potentially unsafe attachments in Outlook.
  + Supported on Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP1 and SP2.
* **Office 2002 (Office XP) SP3**
  + Outlook now blocks saving of potentially unsafe attachments by default.
  + Additional blocked file types.
  + Supported on Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP1 and SP2.
* **Office 2003 (SP2 and SP3)**
  + Additional blocked file types.
  + Supported on Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1.
* **Office 2007 (base version and SP1)**
  + Additional blocked file types.
  + Supported on Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1.
* **Windows Messenger 4.7**
  + Shipped in Windows XP SP2 and SP3.
  + Blocks the receipt of potentially unsafe attachments.
* **Windows Messenger 5.1**
  + Downloadable for Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP1 and SP2.
  + Blocks the receipt of potentially unsafe attachments.
* **Windows Live Messenger 8.1**
  + Downloadable for Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1.
  + Requires the user to enable an antivirus program to screen the attachments before the downloading of potentially unsafe file types is permitted.

## Notes for Internet Explorer on Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1

Internet Explorer checks whether a given file type is associated with an application before checking the potentially unsafe file type list. For example, the Microsoft Visio file type of .vsd is considered unsafe only if Microsoft Visio is installed on the system. If it is not, Internet Explorer looks at the file contents to determine whether or not the file can be displayed. Text format files are displayed in a browser window. For files that contain binary data, the user is presented with a dialog box giving the option of saving the file to disk.

### Internet Explorer 5 and Internet Explorer 6 SP1 on Microsoft Windows 2000 SP4

* The NTFS file system for Microsoft Windows 2000 SP4 does not support the saving of zone information.

### Internet Explorer 6 on Windows XP SP2 and SP3 and Windows Server 2003 SP1 and SP2

* On Internet Explorer 6, when a user browses to an FTP site on the Web, Internet Explorer uses Windows Explorer as the browser to view the files. If the user uses drag and drop to copy the files locally then NO zone information is saved with these files. In order for zone information to be saved with the file, the user has to double-click on the file and select **Save** from the dialog box.
* On Windows versions after Windows Server 2003, Internet Explorer 6 is not supported.

### Internet Explorer 7 on Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1

* By default, Internet Explorer 7 can browse FTP sites rather than invoke Windows Explorer. If the user right-clicks on a file and selects **Save as** from the context-sensitive menu, then zone information will be saved with the file.
* Internet Explorer 7 is not supported on Windows versions earlier than Windows XP.

## Note on Shell Execute Behavior

### Special note on .cab .and .zip files.

If a .cab or .zip file is downloaded from the web, then the zone information is set on that archive file in the local file system. When these archive files are opened by the Windows shell, the files that are contained within will also be ‘tagged’ with this zone information. For example, if a .zip file is downloaded from the Web and the user tries to launch an .exe file contained within that .zip file, the shell will present the user with a warning dialog box.

## Notes on Windows Messenger

### Windows Messenger 5.1 on Microsoft Windows 2000 SP4

Microsoft Windows 2000 SP4 supports both Internet Explorer 5 and Internet Explorer 6 SP1. If a file is determined to be potentially unsafe, Windows Messenger will block the user from accepting the download.

### Windows Messenger with Internet Explorer 5

On Microsoft Windows 2000, Windows Messenger uses the same list of blocked files as Internet Explorer.

### Internet Explorer 6

The Internet Explorer 6 SP1 release for Microsoft Windows 2000 SP4 changed the potentially unsafe file type list to be consistent with the list used for the Office products. Since Windows Messenger uses this same list, the blocked file behavior also changed. Internet Explorer 6 SP1 includes a total of 54 potentially unsafe file types, or 21 fewer than Internet Explorer 5.

### Windows Messenger 4.7, 5.1, and Windows Live Messenger 8.1 on Windows XP SP2

Windows XP SP2 added the Attachment Execution Service (AES), which is called to verify the safety of a file type. If a file is determined to be potentially executable and thereby potentially unsafe, Windows Messenger will block the user from accepting the download.

On supported editions of Windows XP, all three versions of Windows Messenger exhibit consistent behavior under both Internet Explorer 6 and Internet Explorer 7.

### Attachment save behavior

### Windows Messenger 4.7 and 5.1

When a file is saved after being received, the zone information in the file system is set on that file to indicate the file came from another computer. When viewing the file properties, the user is presented with an “Unblock” button to clear the zone setting on the file.

### Windows Live Messenger 8.1

When a file is saved after being received, the zone information on the file is not set.

### Windows Messenger 5.1, and Windows Live Messenger 8.1 on Windows Server 2003 SP1

The blocked file type list and attachment save behavior for Windows Messenger 5.1 and Windows Live Messenger 8.1 on Windows Server 2003 SP1 and SP2 is the same as on Windows XP SP2 and SP3.

### Windows Live Messenger 8.1 on Windows Vista

The blocked file type list and attachment save behavior for Windows Live Messenger 8.1 on Windows Vista RTM and SP1 is the same as on Windows XP SP2 and SP3.

## Notes on Outlook Express and Windows Mail

### Outlook Express 5 on Microsoft Windows 2000 SP4

This is the version of Outlook Express that ships with Microsoft Windows 2000 SP4. Attachments whose file types are associated with Notepad, Windows and FAX Viewer, or Windows Media Player are opened directly by those applications without a dialog box.

### Outlook Express 6 SP1 on Microsoft Windows 2000 SP4

This version of Outlook Express is included in the Internet Explorer 6 SP1 Upgrade package available for Microsoft Windows 2000 SP4. A change was made in Outlook Express 6 to, by default, block potentially unsafe file type attachments and thereby preventing the user from saving it. This change, however, blocks almost all mail attachments except those files associated with Windows Media Player and Internet Explorer. For the attachments deemed not potentially executable, opening it will launch the associated program without any dialog box.

### Outlook Express 6 on Windows XP SP2 and SP3

This is the version of Outlook Express that ships with Windows XP SP2 and SP3. If a message attachment is determined to be a potentially unsafe file, the attachment is blocked and the user will be unable to open or save the attachment.

### Attachment save behavior

When a mail attachment is saved the zone information in the file system is set on that file to indicate the file came from another computer. When viewing the file properties, the user is presented with an “Unblock” button to clear the zone setting on the file.

### Outlook Express 6 on Windows Server 2003 SP1 and SP2

The blocked file type list and attachment save behavior for Outlook Express 6 on Windows Server 2003 SP1 and SP2 is the same as on Windows XP SP2 and SP3.

### Windows Mail on Windows Vista RTM and SP1

Windows Mail is the new mail client that ships with Windows Vista RTM and SP1. If Windows Mail determines that a message attachment is potentially unsafe, the attachment is blocked and the user is unable to open or save the attachment.

### Attachment save behavior

When a mail attachment is saved the zone information in the file system is set on that file to indicate the file came from another computer. When viewing the file properties, the user is presented with an “Unblock” button to clear the zone setting on the file.

## Notes on Microsoft Office Outlook

### General attachment save behavior for versions of Outlook running on Windows XP SP2 and SP3, Windows Server 2003 SP1 and SP2, and Windows Vista RTM and SP1

When a mail attachment is saved from any of the Office Outlook versions, the zone information in the file system is not set. Because of this, all saved attachments can be launched without the additional dialog box. This behavior differs from the Outlook Express and Windows Mail clients.

### Outlook 2000 SP3 on Microsoft Windows 2000 SP4

Attachments that have file types that are associated with Notepad, Windows Picture and FAX Viewer, Windows Media Player, Internet Explorer, or any of the Office products, are opened directly by those applications without a dialog box.

### Outlook 2002 SP3 on Microsoft Windows 2000 SP4

Attachments that have file types that are associated with Notepad, Windows Picture and FAX Viewer, Windows Media Player, or Internet Explorer are opened directly by those applications without a dialog box. Office file types are no longer opened without a dialog box in Outlook 2002.

### Outlook 2003 SP2 on Microsoft Windows 2000 SP4

Outlook 2003 SP2 behaves in the same manner as Outlook 2002 SP3 in that the saving of potentially unsafe file attachments is blocked.

### Outlook 2003 SP3 on Microsoft Windows 2000 SP4

Outlook 2003 SP3 added an additional file types to the blocked file type list; other behavior and dialog boxes are same as in the previous service pack.

### Outlook 2000 SP3 on Windows XP SP2 and SP3

The list of blocked file types is the same as Outlook 2000 SP2 on Microsoft Windows 2000 SP4.

### Outlook 2002 SP3 on Windows XP SP2 and SP3

The list of blocked file types is the same as Outlook 2002 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2003 SP2 on Windows XP SP2 and SP3

The list of blocked file types is the same as Outlook 2000 SP2 on Microsoft Windows 2000 SP4.

### Outlook 2003 SP3 on Windows XP SP2 and SP3

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2007 on Windows XP SP2 and SP3

The list of blocked file types is essentially the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4, but with the following file type removed from the blocked list: .gadget

### Outlook 2007 SP1 on Windows XP SP2 and SP3

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2000 SP3 on Windows Server 2003 SP1 and SP2

The list of blocked file types is the same as Outlook 2000 SP2 on Microsoft Windows 2000 SP4.

### Outlook 2002 SP3 on Windows Server 2003 SP1 and SP2

The list of blocked file types is the same as Outlook 2002 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2003 SP2 on Windows Server 2003 SP1 and SP2

The list of blocked file types is the same as Outlook 2003 SP2 on Microsoft Windows 2000 SP4.

### Outlook 2003 SP3 on Windows Server 2003 SP1 and SP2

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2007 on Windows Server 2003 SP1 and SP2

The list of blocked file types is essentially the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4, but with the following file type removed from the blocked list: .gadget

### Outlook 2007 SP1 on Windows Server 2003 SP1 and SP2

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2003 SP2 on Windows Vista RTM and SP1

The list of blocked file types is the same as Outlook 2003 SP2 on Microsoft Windows 2000 SP4. Attachments that have file types that are associated with Notepad, Windows Photo Gallery, Windows Media Player, or Internet Explorer are opened directly by those applications without a dialog box.

### Outlook 2003 SP3 on Windows Vista RTM and SP1

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

### Outlook 2007 on Windows Vista RTM and SP1

The list of blocked file types is essentially the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4, but with the following file type removed from the blocked list: .gadget

### Outlook 2007 SP1 on Windows Vista RTM and SP1

The list of blocked file types is the same as Outlook 2003 SP3 on Microsoft Windows 2000 SP4.

1. To ensure that you always have the latest security and other updates for your computer, enable Automatic Updates in Windows or visit <http://update.microsoft.com/microsoftupdate> frequently. For more information on update management, visit <http://technet.microsoft.com/en-us/updatemanagement/default.aspx>. [↑](#footnote-ref-2)
2. File types NOT listed in the system registry are classified as unknown file types and default to a certain behavior. [↑](#footnote-ref-3)
3. On Windows Vista, the User Account Control dialog box may appear instead. [↑](#footnote-ref-4)
4. Attachments are handled differently in Outlook Express for Microsoft Windows 2000 SP4. See page 2 for more information. [↑](#footnote-ref-5)
5. Again, for additional information about changes to AES, see <http://technet.microsoft.com/en-us/library/bb457150.aspx> and <http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%202%20white%20paper.doc>) [↑](#footnote-ref-6)