⌕   Microsoft   Sign in

Support ⌄

Information about the Attachment Manager in Microsoft Windows

▶ *Applies To*

Summary

This article describes Attachment Manager in Windows. This article includes the methods to configure Attachment Manager and the workarounds for two issue with Attachment Manager.

Introduction

The Attachment Manager is included in Microsoft Windows to help protect your computer from unsafe attachments that you might receive with an e-mail message and from unsafe files that you might save from the Internet.

If the Attachment Manager identifies an attachment that might be unsafe, the Attachment Manager prevents you from opening the file, or it warns you before you open the file. For more information about Attachment Manager, go to the "More Information" section.

Workarounds when you cannot download a file or a program

Many people encounter issues when they try to download a file or a program from the Internet. This could be caused by a number of reasons. Here we provide two general solutions for you to try if you are getting an error that your download is blocked, or if you get "virus scan failed" or "virus detected" messages.

You cannot download any file if the "File download" option is disabled in the Internet security settings. Follow these steps to check the Internet security settings:

1. Start the **Internet Properties** window.
   Windows 7

   a. Click **Start**, click **All Programs**, and then open the **Accessories** folder.

   b. Click **Run**.

   c. Type inetcpl.cpl, and then click **OK**.

   Windows 8 or 10

   a. From the Start screen, type inetcpl.cpl, and then press Enter.

2. In the **Internet Properties** window, click the **Security** tab, click the **Ineternet** zone (globe icon), and then click the **Custom level** button.

3. In the **Security Settings** window, scroll down to **Downloads** > **File download**.

4. Click to select **Enable**.

5. Scroll down the list further to **Miscellaneous** > **Launching applications and unsafe files**.

6. Click to select **Prompt (recommended)**.

7. Click **OK**.

You may receive a "Virus scan failed" or "Virus detected" error message when you try to open or save a file or a program from Internet. In most cases, it is not caused by the Windows operating system, but by the antivirus software. If you are certain that the source you are trying to open is safe and trusted, try the following workaround to disable the virus scanning temporarily, and then enable the virus scanning immediately after you complete downloading the program or file. You have to be very cautious about using this workaround. Otherwise, you may be exposed to virus attacks.

1. Start Registry Editor.
   Windows 7

   a. Click **Start**, click **All Programs**, and then open the **Accessories** folder.

   b. Click **Run**.

   c. Type regedit.exe, and then click **OK**.

   Windows 8 or 10

   a. From the Start screen, type regedit.exe, and then press Enter.

2. Locate the following registry subkeys:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments

   If you do not see the Attachments subkey, create it by right clicking **Policies**, select **New**, click **Key**, and then type Attachments as the key name.
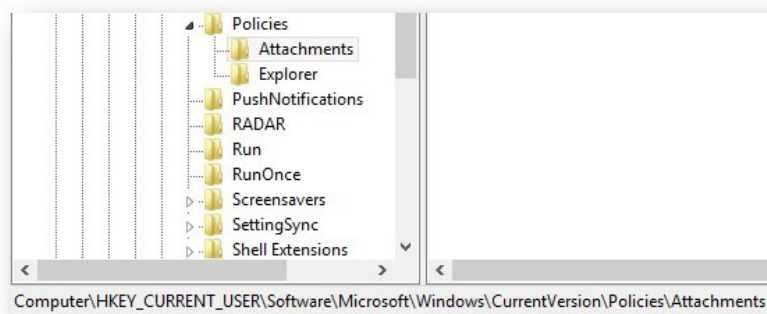
3. Right click **Attachments**, select **New**, and then click **DWORD (32-bit) Value**.

4. Type ScanWithAntiVirus as the value name, and then press Enter.

5. Right-click the new **ScanWithAntiVirus** DWORD value, and then click **Modify**.

6. In the **Value data** box, type 1, and then click **OK**.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ScanWithAntiVirus	REG_DWORD	0x00000001 (1)

7. Exit Registry Editor.

8. Log off and log in Windows to make the change take effect.

9. Open or save the program or file that you failed before.

Note We suggest you change the value of **ScanWithAntiVirus** subkey to 3 to enable the virus scan right after you completely open or save the program or file.

Configuring the Attachment Manager

There are several features of the Attachment Manager that can be configured by using Group Policy or the local registry.

This policy setting lets you manage the default risk level for file types. To fully customize the risk level for file attachments, you may also have to configure the trust logic for file attachments:

- High Risk
  If the attachment is in the list of high risk file types and is from the restricted zone, Windows blocks the user from accessing the file. If the file is from the Internet zone, Windows prompts the user before accessing the file.

- Moderate Risk
  If the attachment is in the list of Moderate Risk file types, Windows will not prompt the user before accessing the file, regardless of the file's zone information.

- Low Risk
  If the attachment is in the list of low risk file types, Windows will not prompt the user before accessing the file, regardless of the file's zone information.

If you enable this policy setting, you can specify the default risk level for file types. If you disable this policy setting, Windows sets the default risk level to moderate. If you do not configure this policy setting, Windows sets the default risk level to moderate.

Group Policy	Registry Subkey	Registry Entry	Entry Value
User Configuration\Administrative Templates\Windows	HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Policies\Associations	DefaultFileTypeRisk	High (6150) or

Components\Attachment Manager		Moderate (6151) or Low (6152)

Note The default value of the DefaultFileTypeRisk registry entry is Moderate (6151).

This policy setting lets you manage whether Windows marks file attachments that have information about their zone of origin. These zones or origin are Internet, intranet, and local. This policy setting requires the NTFS file system to function correctly and will fail without notice on systems that use FAT32. By not preserving the zone information, Windows cannot make appropriate risks assessments. If you enable this policy setting, Windows does not mark file attachments by using their zone information. If you disable this policy setting, Windows marks file attachments by using their zone information. If you do not configure this policy setting, Windows marks file attachments by using their zone information.

Group Policy	Registry Subkey	Registry Entry	Entry Value
User Configuration\Administrative Templates\Windows Components\Attachment Manager	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments	SaveZoneInformation	On (1) or Off (2)

Note The default value of the DefaultFileTypeRisk registry entry is Off (2).

Hide mechanisms to remove zone information

This policy setting lets you manage whether users can manually remove the zone information from saved file attachments by clicking
Unblock on the file's **Properties** tab or by clicking to select a check box in the **Security Warning** dialog box. Removing the zone information lets users open potentially dangerous file attachments that Windows has blocked users from opening. If you enable this policy setting, Windows hides the check box and the **Unblock** button. If you disable this policy setting, Windows shows the check box and the **Unblock** button. If you do not configure this policy setting, Windows shows the check box and the **Unblock** button.

Group Policy	Registry Subkey	Registry Entry	Ent Val

User Configuration\Administrative Templates\Windows Components\Attachment Manager	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments	HideZoneInfoOnProperties	Of (0) or On (1

Note The default value of the **DefaultFileTypeRisk** registry entry is Off (0).

These policy settings let you configure the list of low, moderate, and high risk file types. The High list takes precedence over the Moderate and Low risk inclusion lists. Also, an extension is listed in more than one inclusion list. If you enable this policy setting you can create a custom list of low, moderate, and high risk file types. If you disable this policy setting, Windows uses its built in list of file types. If you do not configure this policy setting, Windows uses its built in list of file types.

Group Policy	Registry Subkey	Registry Entry	Entry Value
User Configuration\Administrative Templates\Windows Components\Attachment Manager	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations	HighRiskFileTypes ModRiskFileTypes LowRiskFileTypes	

This policy setting lets you configure the logic that Windows uses to determine the risk for file attachments. Preferring the file handler instructs Windows to use the file handler data over the file type data. For example, it instructs Windows to trust Notepad.exe, but do not trust .txt files. Preferring the file type instructs Windows to use the file type data over the file handler data. For example, trust .txt files, regardless of the file handler. Using both the file handler and type data is the most restrictive option. Windows chooses the more restrictive recommendation. This causes users to see more trust prompts than selecting the other options. If you enable this policy setting, you can select the order in which Windows processes risk assessment data. If you disable this policy, Windows uses its default trust logic which prefers the file handler over the file type.

Group Policy	Registry Subkey	Registry Entry	Entry Value
User Configuration\Administrative Templates\Windows Components\Attachment Manager	HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Policies\Attachments	UseTrustedHandlers	File Type (1) or Handler (2) or Both (3)

Note The default value of the **DefaultFileTypeRisk** registry entry is Handler (2).

This policy setting lets you manage the behavior for notifying registered antivirus programs. If multiple programs are registered, they will all be notified. If the registered antivirus program already performs on-

access checks or scans files as they arrive on the computer's e-mail server, additional calls would be redundant. If you enable this policy, Windows tells the registered antivirus program to scan the file when a user opens a file attachment. If the antivirus program fails, the attachment is blocked from being opened. If you disable this policy, Windows does not call the registered antivirus programs when file attachments are opened. If you do not configure this policy, Windows does not call the registered antivirus programs when file attachments are opened.

Group Policy	Registry Subkey	Registry Entry	Entry Value
User Configuration\Administrative Templates\Windows Components\Attachment Manager	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments	ScanWithAntiVirus	Off (1) or Optional (2) or On (3)

Note The default value of the DefaultFileTypeRisk registry entry is Off (1). When the value is set to Optional (2), all scanners are called even after one reports a detection.
For more information, click the following article number to view the article in the Microsoft Knowledge Base:

182569 Internet Explorer security zones registry entries for advanced users

More Information

The following determine whether you are prevented from opening the file or whether you are warned before you open the file:

- The type of program that you are using.

- The file type that you are downloading or trying to open.

- The security settings of the Web content zone that you are downloading the file from.

  Note You can configure the Web content zones in Microsoft Internet Explorer on the **Security** tab. To view the Web content zones, click **Tools**, click **Internet Options**, and then click the **Security** tab. The following are the four Web content zones:

  - Internet

  - Local intranet

  - Trusted sites

  - Restricted sites

The Attachment Manager uses the IAttachmentExecute application programming interface (API) to find the file type, to find the file association, and to determine the most appropriate action.

Microsoft Outlook Express and Microsoft Internet Explorer use the Attachment Manager to handle e-mail

attachments and Internet downloads.

The Attachment Manager classifies files that you receive or that you download based on the file type and the file name extension. Attachment Manager classifies files types as high risk, medium risk, and low risk. When you save files to your hard disk from a program that uses the Attachment Manager, the Web content zone information for the file is also saved with the file. For example, if you save a compressed file (.zip) that is attached to an e-mail message to your hard disk, the Web content zone information is also saved when you save the compressed file. When you try to extract the contents from the compressed file, or if you try to run a file, you cannot. The Web content zone information is saved together with the files only if the hard disk uses the NTFS file system.

You can open a blocked file from a known source if you want to. To open a blocked file, follow these steps:

1. Right-click the blocked file, and then click
   Properties.

2. In the **General** tab, click
   Unblock.

High-risk file types	⌄
Medium-risk file types	⌄
Low-risk file types	⌄

📶 SUBSCRIBE RSS FEEDS

Need more help?

How can we help you?   →

Want more options?

🌐 Discover   👥 Community

Explore subscription benefits, browse training courses, learn how to secure your device, and more.

Microsoft 365   Microsoft 365 training   Microsoft security   Accessibility center
subscription benefits

Was this information helpful? | Yes | | No |

What's new

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap   Contact Microsoft   Privacy   Terms of use   Trademarks   Safety & eco   Recycling   About our ads   © Microsoft 2024