

Internet Explorer Security

Helping to protect your computer from unsafe software

When you download or run programs from the Internet, you want to know that the program comes from a known, reliable source. Internet Explorer uses Microsoft Authenticode technology to help verify the identity of the program. Authenticode technology checks to see if the program has a valid certificate, that the identity of the software publisher matches the certificate, and that the certificate is still valid. Note that this does not prevent a poorly written program from being downloaded or run on your computer, but it helps reduce the chance of someone misrepresenting a program that is intended to be malicious or intentionally harmful.

You can specify different settings for the way Internet Explorer handles downloading programs and files, depending on the zone they are coming from.

For example, you might be confident that what you download within your corporate intranet is safe. So, you might set your security settings for your Local intranet zone to a low level to allow downloading with little or no prompting. If the source is in the Internet zone or the Restricted sites zone, you might want your security levels set to Medium or High. Then, you'd be prompted with information about the program's certificate before it is downloaded, or you might not be able to download it all.

What are ActiveX controls?

ActiveX controls and web browser add-ons are small programs that are used extensively on the Internet. They can make browsing more enjoyable by providing toolbars, stock tickers, video, animated content, and more. These programs can malfunction, however, or give you content you don't want. In some cases, these programs can be used to collect information from your computer in ways you might not approve of, possibly damage information on your computer, install software on your computer without your consent, or allow someone else to control your computer remotely. Given these risks, you should only install ActiveX controls or add-ons if you completely trust the publisher and the website offering it.

Do you trust the website providing the control?

Don't install an ActiveX control unless you trust the website that is providing it.

CBD KNOWLEDGE BASE

Do you know what the control is for and what it will do to your computer?

The website should tell you what this add-on or ActiveX control is for and provide any special details you need to know before you install it. If this information is not available, you should not install the control.

If you still want to install or run the ActiveX, click the Information bar, and then follow the prompts.

Recommended IE Security Settings

Security Option	High Level
Download signed ActiveX controls	Disable
Download unsigned ActiveX controls	Disable
Initialize and script ActiveX controls not marked as safe	Disable
Run ActiveX controls and plug-ins	Disable
Script ActiveX controls marked safe for scripting	Disable
File Download	Disable
Font Download	Prompt
Java permissions	Disable Java
Access data sources across domains	Disable
Allow META REFRESH	Disable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificates or only one certificate exists	Disable
Drag and drop or copy and paste files	Prompt
Installation of desktop items	Disable
Launching programs and files in an IFRAME	Disable

CBD KNOWLEDGE BASE

Navigate sub-frames across different domains	Disable
Software channel permissions	High safety
Submit nonencrypted form data	Prompt
Userdata persistence	Disable
Active scripting	Disable
Allow paste operations via script	Disable
Scripting of Java applets	Disable
User Authentication—Logon	Prompt for user name and password

Configuring Custom Settings

The custom security options for IE are grouped into the following categories:

- ActiveX Controls and Plug-ins
- Downloads
- Java
- Miscellaneous
- Scripting
- User Authentication

The following sections describe the security options for each security category.

ActiveX Controls and Plug-ins

These options dictate how ActiveX controls and plug-ins are downloaded, run, and scripted.

Note: If an ActiveX control is downloaded from a site different from the page on which it's used, the more restrictive of the two sites' zone settings will be applied. For example, if a user is accessing a Web page within a zone that's set to enable a download, but the code is downloaded from another zone that's set to prompt a user first, the prompt setting is used.

CBD KNOWLEDGE BASE

Download signed ActiveX controls

This option determines whether users may download signed ActiveX controls from a page in the zone. The settings for this option are:

Enable, to download signed controls without user intervention.

Prompt, to query the user whether to download controls signed by publishers who aren't trusted, but still silently download code signed by trusted publishers.

Disable, to prevent signed controls from downloading.

Download unsigned ActiveX controls

This option determines whether users may download unsigned ActiveX controls from the zone. Such code is potentially harmful, especially when coming from an untrusted zone. The settings for this option are:

Enable, to run unsigned controls without user intervention.

Prompt, to query users to choose whether to allow the unsigned control to run.

Disable, to prevent unsigned controls from running.

Initialize and script ActiveX controls not marked as safe

This option determines whether ActiveX control object safety is enforced for pages in the zone. Object safety should be enforced unless all ActiveX controls and scripts that might interact with pages in the zone can be trusted. The settings for this option are:

Enable, to override object safety. ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting isn't recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the **Script ActiveX controls marked safe for scripting** option.

Prompt, to attempt to enforce object safety. However, if the ActiveX control cannot be made safe for untrusted data or scripts, then the user is queried whether to allow the control to be loaded with parameters or scripted.

Disable, to enforce object safety for untrusted data or scripts. ActiveX controls that cannot be made safe aren't loaded with parameters or scripted.

CBD KNOWLEDGE BASE

Run ActiveX controls and plug-ins

This option determines whether ActiveX controls and plug-ins can be run on pages from the specified zone. The settings for this option are:

Enable, to run controls and plug-ins without user intervention.

Prompt, to query users to choose whether to allow the controls and plug-ins to run.

Disable, to prevent controls and plug-ins from running.

Script ActiveX controls marked safe for scripting

This option determines whether an ActiveX control marked safe for scripting can interact with a script. The settings for this option are:

Enable, to allow script interaction without user intervention.

Prompt, to query users to choose whether to allow script interaction.

Disable, to prevent script interaction.

Note that safe-for-initialization controls loaded with PARAM tags are unaffected by this option. This option is ignored when **Initialize and script ActiveX controls that are not marked safe** is set to **Enable**, because the setting bypasses all object safety. You cannot script unsafe controls while blocking the scripting of the safe ones.

Downloads

These options specify how IE handles downloads.

File download

This option controls whether file downloads are permitted from the zone. Note that the zone of the page with the link causing the download determines this option, not the zone from which the file is delivered. The settings for this option are:

Enable, to allow files to be downloaded from the zone.

Disable, to prevent files from being downloaded from the zone.

Font download

This option determines whether pages of the zone may download HTML fonts. The settings for this option are:

Enable, to download HTML fonts without user intervention.

Prompt, to query users to choose whether to allow HTML fonts to download.

Disable, to prevent HTML fonts from downloading.

CBD KNOWLEDGE BASE

Java

These options control the permissions that are granted to Java applets when they're downloaded and run in this zone. You can specify:

The maximum permission level granted to signed applets downloaded from the zone.

The permissions granted to unsigned applets downloaded from the zone.

The permissions granted to scripts on pages in the zone that call into applets.

Note: If a Java applet is downloaded from a different site than the page on which it's used, the more restrictive of the two sites' zone settings will be applied. For example, if a user is accessing a Web page within a zone that's set to allow a download, but the code is downloaded from another zone that's set to prompt a user first, then the prompt setting is used.

Java permissions

The settings for this option are:

Custom, to control permissions settings individually. To view and change custom Java permissions for each security zone, use the IE **Custom Java Security** dialog box. You can also use the IEAK Configuration Wizard and IEAK Profile Manager to edit the advanced Java permissions for each security zone.

Low safety, to enable applets to perform all operations.

Medium safety, to enable applets to run in their *sandbox* (an area in memory outside of which the program cannot make calls), plus capabilities such as *scratch space* (a safe and secure storage area on the client computer) and user-controlled file I/O.

High safety, to enable applets to run in their sandbox.

Disable Java, to prevent any applets from running.

Miscellaneous

These options control whether users can submit nonencrypted form data, launch applications and files from IFRAMEs, install Active Desktop items, drag files, or copy and paste files a zone.

Access data sources across domains

This option controls whether a web page can call data sources from other domains, which is not uncommon. The settings for this option are:

Enable, to allow data sources from other domains automatically.

Prompt, to query users on whether to allow data sources to be used from other domains.

Disable, to prevent data sources from other domains from being used.

CBD KNOWLEDGE BASE

Allow META REFRESH

This option controls whether a web page can redirect your browser to another page after a predefined period of time. The settings for this option are:

Enable, to allow Meta refreshes.

Disable, to prevent Meta refreshes.

Display mixed content

This option controls whether or not IE will display a web page containing content from both secure (https) and nonsecure (http) content. The settings for this option are:

Enable, allow web page with mixed content to display.

Prompt, query user on whether to allow web paged with mixed content to display.

Disable, will not allow web pages with both secure and nonsecure content to display.

Don't prompt for client certificate selection when no certificates exist or only one certificate exists

This option controls whether or not a web site requesting client certificate authentication will prompt the user to select a client certificate to authenticate their identity when no or only one certificate exists. The settings for this option are:

Enable, if none or only one certificate exists web site requesting client certificate authentication will not prompt user to select a client authentication certificate.

Disable, web site requesting client certificate authentication will prompt user to select certification even if none or only one certificate exists.

Drag and drop or copy and paste files

This option controls whether users can drag files or copy and paste files from a source within the zone. The settings for this option are:

Enable, to drag files or copy and paste files from this zone without user intervention.

Prompt, to query users to choose whether to drag or copy files from this zone.

Disable, to prevent dragging files or copying and pasting files from this zone.

CBD KNOWLEDGE BASE

Installation of desktop items

This option controls whether users can install Active Desktop items from this zone. The settings for this option are:

Enable, to install desktop items from this zone without user intervention.

Prompt, to query users to choose whether to install desktop items from this zone.

Disable, to prevent desktop items from this zone from being installed.

Launching programs and files in an IFRAME

This option controls whether applications may be run and files may be downloaded from a floating frame (IFRAME) reference in the HTML of the pages in this zone. The settings for this option are:

Enable, to run applications and download files from IFRAMEs on the pages in this zone without user intervention.

Prompt, to query users to choose whether to run applications and download files from IFRAMEs on the pages in this zone.

Disable, to prevent applications from running and files from downloading from IFRAMEs on the pages in this zone.

Navigate sub-frames across different domains

This option controls whether a web page displayed in a sub-frame can launch from a domain different than the calling web page. The settings for this option are:

Enable, allow web pages to call sub-frame pages originating from different domains.

Prompt, query user to choose whether to allow sub-frames from other domains.

Disable, never allow a web page to call a sub-frame from a different domain.

Software channel permissions

This option controls the permissions given to software distribution channels. The settings for this option are:

Low safety, to allow users to be notified of software updates by email, software packages to be automatically downloaded to users' computers, and software packages to be automatically installed on users' computers.

Medium safety, to allow users to be notified of software updates by email and software packages to be automatically downloaded to (but not installed on) users' computers.

High safety, to prevent users from being notified of software updates by email, software packages from being automatically downloaded to users' computers, and software packages from being automatically installed on users' computers.

CBD KNOWLEDGE BASE

Submit nonencrypted form data

This option determines whether data on HTML forms on pages in the zone may be submitted. Forms sent with SSL encryption are always allowed; this setting only affects non-SSL form data submission. The settings for this option are:

Enable, to allow information using HTML forms on pages in this zone to be submitted without user intervention.

Prompt, to query users to choose whether to allow information using HTML forms on pages in this zone to be submitted.

Disable, to prevent information using HTML forms on pages in this zone from being submitted.

Userdata persistence

This option controls whether or not a web page can store collected user data after the user leaves the web page. The settings for this option are:

Enable, allow web page to store persistent data.

Disable, deny a web page the ability to store persistent user data.

Scripting

These options specify how IE handles scripts.

Active scripting

This option determines whether script code on pages in the zone is run. The settings for this option are:

Enable, to run scripts without user intervention.

Prompt, to query users to choose whether to allow the scripts to run.

Disable, to prevent scripts from running.

Allow paste operations via script

This option controls whether or not a web page script can copy and paste data to the Windows Clipboard application. Several security vulnerabilities are possible if this setting is enabled. The settings for this option are:

Enable, allow a web site script to copy and paste data using the Windows clipboard application.

Prompt, query users to choose whether or not to allow a web site to utilize the Windows Clipboard to copy and paste data.

Disable, prevent web sites from using the Windows Clipboard.

CBD KNOWLEDGE BASE

Scripting of Java applets

This option determines whether applets are exposed to scripts within the zone. The settings for this option are:

Enable, to allow scripts to access applets without user intervention.

Prompt, to query users to choose whether to allow scripts to access applets.

Disable, to prevent scripts from accessing applets.