Learn   Discover ⌄   Product documentation ⌄   Development languages ⌄   Topics ⌄   Sign in

ⓘ We're no longer updating this content regularly. Check the **Microsoft Product Lifecycle** for information about how this product, service, technology, or API is supported.   Return to main site   ✕

Internet Explorer security zones registry entries for advanced users

Article • 10/13/2020 • **2 contributors**

In this article

Privacy settings

Security Zone settings

TemplatePolicies

ZoneMap

Show 4 more

> ⚠ **Warning**
>
> The retired, out-of-support Internet Explorer 11 desktop application has been permanently disabled through a Microsoft Edge update on certain versions of Windows 10. For more information, see **Internet Explorer 11 desktop app retirement FAQ** ⧉ .

This article describes how and where Internet Explorer security zones and privacy settings are stored and managed in the registry. You can use Group Policy or the Microsoft Internet Explorer Administration Kit (IEAK) to set security zones and privacy settings.

Original product version: Internet Explorer 9, Internet Explorer 10
Original KB number: 182569

Privacy settings

Internet Explorer 6 and later versions added a Privacy tab to give users more control over cookies. This tab (select**Tools**, and then select**Internet options**) provides flexibility for blocking or allowing cookies, based on the website that the cookie came from or the type of cookie. Types of cookies include first-party cookies, third-party cookies, and cookies that do not have a compact privacy policy. This tab also includes options to control website requests for physical location data, the ability to block pop-ups, and the ability to run toolbars and extensions when InPrivate browsing is enabled.

There are different levels of privacy on the Internet zone, and they are stored in the registry at the same location as the security zones.

You can also add a Web site to enable or to block cookies based on the Web site, regardless of the privacy policy on the Web site. Those registry keys are stored in the following registry subkey:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\P3P\History
```

Domains that have been added as a managed site are listed under this subkey. These domains can carry either of the following DWORD values:

0x00000005 - Always Block

0x00000001 - Always Allow

Security Zone settings

For each zone, users can control how Internet Explorer handles higher-risk items such as ActiveX controls, downloads, and scripts. Internet Explorer security zones settings are stored under the following registry subkeys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`
- `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`

These registry keys contain the following keys:

- TemplatePolicies
- ZoneMap
- Zones

> ⓘ **Note**
>
> By default, security zones settings are stored in the `HKEY_CURRENT_USER` registry subtree. Because this subtree is dynamically loaded for each user, the settings for one user do not affect the settings for another.

If the **Security Zones: Use only machine settings** setting in Group Policy is enabled, or if the `Security_HKLM_only` DWORD value is present and has a value of **1** in the following registry subkey, only local computer settings are used and all users have the same security settings:

`HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`

With the `Security_HKLM_only` policy enabled, HKLM values will be used by Internet Explorer. However, the HKCU values will still be displayed in the zone settings on the **Security** tab in Internet Explorer. In Internet Explorer 7, the **Security** tab of the **Internet Options** dialog box displays the following message to indicate that settings are managed by the system administrator:

> Some settings are managed by your system administrator   If the **Security Zones: Use only machine** settings setting is not enabled in Group Policy, or if the `Security_HKLM_only` DWORD value does not exist or is set to **0**, computer settings are used together with user settings. However, only user settings appear in the **Internet Options**. For example, when this DWORD value does not exist or is set to **0**, `HKEY_LOCAL_MACHINE` settings are read together with `HKEY_CURRENT_USER` settings, but only `HKEY_CURRENT_USER` settings appear in the **Internet Options**.

TemplatePolicies

The `TemplatePolicies` key determines the settings of the default security zone levels. These levels are Low, Medium Low, Medium, and High. You can change the security level settings from the default settings. However, you cannot add more security levels. The keys contain values that determine the setting for the security zone. Each key contains a Description string value and a Display Name string value that determine the text that appears on the Security tab for each security level.

ZoneMap

The `ZoneMap` key contains the following keys:

- Domains
- EscDomains
- ProtocolDefaults
- Ranges

The `Domains` key contains domains and protocols that have been added to change their behavior from the default behavior. When a domain is added, a key is added to the `Domains` key. Subdomains appear as keys under the domain where they belong. Each key that lists a domain contains a DWORD with a value name of the affected protocol. The value of the DWORD is the same as the numeric value of the security zone where the domain is added.

The `EscDomains` key resembles the Domains key except that the `EscDomains` key applies to those protocols that are affected by the Internet Explorer Enhanced Security Configuration (IE ESC). IE ESC is introduced in Microsoft Windows Server 2003 and applies to server operating systems only.

The `ProtocolDefaults` key specifies the default security zone that is used for a particular protocol (ftp, http, https). To change the default setting, you can either add a protocol to a security zone by selecting **Add Sites** on the **Security** tab, or you can add a DWORD value under the Domains key. The name of the DWORD value must match the protocol name, and it must not contain any colons (:) or slashes (/).

The `ProtocolDefaults` key also contains DWORD values that specify the default security zones where a protocol is used. You cannot use the controls on the **Security** tab to change these values. This setting is used when a particular Web site does not fall in a security zone.

The `Ranges` key contains ranges of TCP/IP addresses. Each TCP/IP range that you specify appears in an arbitrarily named key. This key contains a `:Range` string value that contains the specified TCP/IP range. For each protocol, a DWORD value is added that contains the numeric value of the security zone for the specified IP range.

When the Urlmon.dll file uses the MapUrlToZone public function to resolve a particular URL to a security zone, it uses one of the following methods:

- If the URL contains a fully qualified domain name (FQDN), the Domains key is processed.

  In this method, an exact site match overrides a random match.

- If the URL contains an IP address, the `Ranges` key is processed. The IP address of the URL is compared to the `:Range` value that is contained in the arbitrarily named keys under the `Ranges` key.

> ⓘ **Note**
>
> Because arbitrarily named keys are processed in the order that they were added to the registry, this method may find a random match before it finds a match. If this method does find a random match first, the URL may be executed in a different security zone than the zone where it is typically assigned. This behavior is by design.

Zones

The `Zones` key contains keys that represent each security zone that is defined for the computer. By default, the following five zones are defined (numbered zero through four):

```
Console                                                    ⧉ Copy

Value  Setting
------------------------------
0       My Computer
```

```
1       Local Intranet Zone
2       Trusted sites Zone
3       Internet Zone
4       Restricted Sites Zone
```

> ⓘ **Note**
>
> By default, My Computer does not appear in the Zone box on the Security tab as it is locked down to help improve security.

Each of these keys contains the following DWORD values that represent corresponding settings on the custom Security tab.

> ⓘ **Note**
>
> Unless stated otherwise, each DWORD value is equal to zero, one, or three. Typically, a setting of zero sets a specific action as permitted, a setting of one causes a prompt to appear, and a setting of three prohibits the specific action.

Console   🗐 Copy

```
Value  Setting
----------------------------------------------------------------------
1001   ActiveX controls and plug-ins: Download signed ActiveX controls
1004   ActiveX controls and plug-ins: Download unsigned ActiveX controls
1200   ActiveX controls and plug-ins: Run ActiveX controls and plug-ins
1201   ActiveX controls and plug-ins: Initialize and script ActiveX controls not
1206   Miscellaneous: Allow scripting of Internet Explorer Web browser control '
1207   Reserved #
1208   ActiveX controls and plug-ins: Allow previously unused ActiveX controls t
1209   ActiveX controls and plug-ins: Allow Scriptlets
120A   ActiveX controls and plug-ins: ActiveX controls and plug-ins: Override Pe
120B   ActiveX controls and plug-ins: Override Per-Site (domain-based) ActiveX r
1400   Scripting: Active scripting
1402   Scripting: Scripting of Java applets
1405   ActiveX controls and plug-ins: Script ActiveX controls marked as safe for
1406   Miscellaneous: Access data sources across domains
1407   Scripting: Allow Programmatic clipboard access
1408   Reserved #
1409   Scripting: Enable XSS Filter
1601   Miscellaneous: Submit non-encrypted form data
1604   Downloads: Font download
1605   Run Java #
1606   Miscellaneous: Userdata persistence ^
1607   Miscellaneous: Navigate sub-frames across different domains
1608   Miscellaneous: Allow META REFRESH * ^
1609   Miscellaneous: Display mixed content *
160A   Miscellaneous: Include local directory path when uploading files to a ser
1800   Miscellaneous: Installation of desktop items
1802   Miscellaneous: Drag and drop or copy and paste files
1803   Downloads: File Download ^
1804   Miscellaneous: Launching programs and files in an IFRAME
1805   Launching programs and files in webview #
1806   Miscellaneous: Launching applications and unsafe files
1807   Reserved ** #
1808   Reserved ** #
1809   Miscellaneous: Use Pop-up Blocker ** ^
180A   Reserved #
180B   Reserved #
180C   Reserved #
180D   Reserved #
180E   Allow OpenSearch queries in Windows Explorer #
180F   Allow previewing and custom thumbnails of OpenSearch query results in Wir
1A00   User Authentication: Logon
1A02   Allow persistent cookies that are stored on your computer #
1A03   Allow per-session cookies (not stored) #
1A04   Miscellaneous: Don't prompt for client certificate selection when no cert
1A05   Allow 3rd party persistent cookies *
1A06   Allow 3rd party session cookies *
1A10   Privacy Settings *
1C00   Java permissions #
```

```
1E05   Miscellaneous: Software channel permissions
1F00   Reserved ** #
2000   ActiveX controls and plug-ins: Binary and script behaviors
2001   .NET Framework-reliant components: Run components signed with Authentico
2004   .NET Framework-reliant components: Run components not signed with Authent
2007   .NET Framework-Reliant Components: Permissions for Components with Manife
2100   Miscellaneous: Open files based on content, not file extension ** ^
2101   Miscellaneous: Web sites in less privileged web content zone can navigate
2102   Miscellaneous: Allow script initiated windows without size or position co
2103   Scripting: Allow status bar updates via script ^
2104   Miscellaneous: Allow websites to open windows without address or status b
2105   Scripting: Allow websites to prompt for information using scripted window
2200   Downloads: Automatic prompting for file downloads ** ^
2201   ActiveX controls and plug-ins: Automatic prompting for ActiveX controls *
2300   Miscellaneous: Allow web pages to use restricted protocols for active con
2301   Miscellaneous: Use Phishing Filter ^
2400   .NET Framework: XAML browser applications
2401   .NET Framework: XPS documents
2402   .NET Framework: Loose XAML
2500   Turn on Protected Mode [Vista only setting] #
2600   Enable .NET Framework setup ^
2702   ActiveX controls and plug-ins: Allow ActiveX Filtering
2708   Miscellaneous: Allow dragging of content between domains into the same wi
2709   Miscellaneous: Allow dragging of content between domains into separate wi
270B   Miscellaneous: Render legacy filters
270C   ActiveX Controls and plug-ins: Run Antimalware software on ActiveX contro

       {AEBA21FA-782A-4A90-978D-B72164C80120} First Party Cookie *
       {A8A88C49-5EB2-4990-A1A2-0876022C854F} Third Party Cookie *

* indicates an Internet Explorer 6 or later setting
** indicates a Windows XP Service Pack 2 or later setting
# indicates a setting that is not displayed in the user interface in Internet Ex
^ indicates a setting that only has two options, enabled or disabled
```

Notes about 1200, 1A00, 1A10, 1E05, 1C00, and 2000

The following two registry entries affect whether you can run ActiveX controls in a particular zone:

- 1200 This registry entry affects whether you can run ActiveX controls or plug-ins.
- 2000 This registry entry controls binary behavior and script behavior for ActiveX controls or plug-ins.

Notes about 1A02, 1A03, 1A05, and 1A06

The following four registry entries take only effect if the following keys are present:

- {AEBA21FA-782A-4A90-978D-B72164C80120} First Party Cookie *
- {A8A88C49-5EB2-4990-A1A2-0876022C854F} Third-Party Cookie *

Registry entries

- 1A02 Allow persistent cookies that are stored on your computer #
- 1A03 Allow per-session cookies (not stored) #
- 1A05 Allow third party persistent cookies *
- 1A06 Allow third party session cookies *

These registry entries are located in the following registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\<ZoneNumber>
```

In this registry subkey, <ZoneNumber> is a zone such as 0 (zero). The `1200` registry entry and the `2000` registry entry each contain a setting that is named Administrator approved. When

this setting is enabled, the value for the particular registry entry is set to **00010000**. When the Administrator approved setting is enabled, Windows examines the following registry subkey to locate a list of approved controls:

`HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\AllowedControls`

Logon setting (1A00) may have any one of the following values (hexadecimal):

| Console | Copy |

```
Value       Setting
-------------------------------------------------------------
0x00000000  Automatically logon with current username and password
0x00010000  Prompt for user name and password
0x00020000  Automatic logon only in the Intranet zone
0x00030000  Anonymous logon
```

Privacy Settings (1A10) is used by the Privacy tab slider. The DWORD values are as follows:

Block All Cookies: 00000003
High: 00000001
Medium High: 00000001
Medium: 00000001
Low: 00000001
Accept all Cookies: 00000000

Based on the settings in the slider, it will also modify the values in {A8A88C49-5EB2-4990-A1A2-0876022C854F}, {AEBA21Fa-782A-4A90-978D-B72164C80120}, or both.

The Java Permissions setting (1C00) has the following five possible values (binary):

| Console | Copy |

```
Value        Setting
----------------------
00 00 00 00  Disable Java
00 00 01 00  High safety
00 00 02 00  Medium safety
00 00 03 00  Low safety
00 00 80 00  Custom
```

If Custom is selected, it uses {7839DA25-F5FE-11D0-883B-0080C726DCBB} (that is located in the same registry location) to store the custom information in a binary.

Each security zone contains the Description string value and the Display Name string value. The text of these values appears on the Security tab when you select a zone in the Zone box. There is also an Icon string value that sets the icon that appears for each zone. Except for the My Computer zone, each zone contains a `CurrentLevel`, `MinLevel`, and `RecommendedLevel` DWORD value. The `MinLevel` value sets the lowest setting that can be used before you receive a warning message, `CurrentLevel` is the current setting for the zone, and `RecommendedLevel` is the recommended level for the zone.

What values for `Minlevel`, `RecommendedLevel`, and `CurrentLevel` mean the following:

| Console | Copy |

```
Value (Hexadecimal) Setting
----------------------------------
0x00010000          Low Security
0x00010500          Medium Low Security
0x00011000          Medium Security
0x00012000          High Security
```

The `Flags` DWORD value determines the ability of the user to modify the security zone's properties. To determine the `Flags` value, add the numbers of the appropriate settings together. The following `Flags` values are available (decimal):

```Console
Value  Setting
----------------------------------------------------------------
1      Allow changes to custom settings
2      Allow users to add Web sites to this zone
4      Require verified Web sites (https protocol)
8      Include Web sites that bypass the proxy server
16     Include Web sites not listed in other zones
32     Do not show security zone in Internet Properties (default setting for My
64     Show the Requires Server Verification dialog box
128    Treat Universal Naming Connections (UNCs) as intranet connections
256    Automatically detect Intranet network
```

If you add settings to both the `HKEY_LOCAL_MACHINE` and the `HKEY_CURRENT_USER` subtrees, the settings are additive. If you add Web sites to both subtrees, only those Web sites in the `HKEY_CURRENT_USER` are visible. The Web sites in the `HKEY_LOCAL_MACHINE` subtree are still enforced according to their settings. However, they are not available, and you cannot modify them. This situation can be confusing because a Web site may be listed in only one security zone for each protocol.

References

For more information about changes to functionality in Microsoft Windows XP Service Pack 2 (SP2), visit the following Microsoft Web site:

Part 5: Enhanced Browsing Security

For more information about URL security zones, visit the following Microsoft Web site:

About URL Security Zones

For more information about how to change Internet Explorer security settings, visit the following Microsoft Web site:

Change security and privacy settings for Internet Explorer 11 ⧉

For more information about Internet Explorer Local Machine Zone Lockdown, visit the following Microsoft Web site:

Internet Explorer Local Machine Zone Lockdown

For more information about values associated with the actions that can be taken in a URL security zone, see URL Action Flags.