IEZoneAnalyzer 3.5

A Utility for Analyzing Internet Explorer Security Zone Settings

Aaron Margosis

Microsoft Public Sector Services

22 September 2011

**Contents**

[Overview 2](#_Toc304497772)

[Show Effective Settings 3](#_Toc304497773)

[View/Compare Entire Collections of Settings 5](#_Toc304497774)

[Compare Zone Settings 7](#_Toc304497775)

[Saving Settings and Loading Saved Settings 9](#_Toc304497776)

[The View/Compare Windows 10](#_Toc304497777)

[View Options (Comparer windows) 10](#_Toc304497778)

[Export to Excel 11](#_Toc304497779)

[Export to CSV 11](#_Toc304497780)

[Clipboard Copy 12](#_Toc304497781)

[Find Text 12](#_Toc304497782)

[Column Sorting, Sizing, Re-ordering 12](#_Toc304497783)

[Modeless Operation 12](#_Toc304497784)

[Map URL to Zone 12](#_Toc304497785)

[Zone Map Viewer 13](#_Toc304497786)

[Help/About 15](#_Toc304497787)

[Appendix: Definition of Terms 16](#_Toc304497788)

[Zones and Policies 16](#_Toc304497789)

[Templates 18](#_Toc304497790)

[Local Intranet Zone vs. Trusted Sites Zone 18](#_Toc304497791)

[The "Locked Down" Security Zones 19](#_Toc304497792)

[Appendix: Internet Explorer’s Explicit Security Zone Mappings 21](#_Toc304497793)

[Explicit Site To Zone Rules 22](#_Toc304497794)

[What About “ZoneMapKey”? 23](#_Toc304497795)

# Overview

IEZoneAnalyzer is a utility for viewing and comparing Internet Explorer security zone settings. It is particularly valuable on systems controlled through Group Policy, on which the standard security settings dialog does not allow viewing of settings. IEZoneAnalyzer version 3 represents a total rewrite, adding a tremendous amount of new functionality compared to earlier versions. Note that IEZoneAnalyzer does not require administrative rights. It also does not have an installer – just run the utility directly. IEZoneAnalyzer does require.NET Framework 3.5.

Key features of IEZoneAnalyzer:

* View effective security zone settings for any security zone on the local computer or exported from a remote computer and identify whether each setting was established by policy.
* Compare settings between two or more security zones or templates.
* View and compare entire sets of settings captured on different computers or on a single computer over time (e.g., to determine whether a system has drifted from its baseline settings).
* Export results to Excel or to a Comma Separated Values (CSV) text file.
* Filter comparison results to show only differences or conflicts.
* Sort, reorder and resize result columns.
* Copy selected or all results to the clipboard.

See the Appendix to this documentation for a helpful overview about IE security zones, machine vs. user configuration, policies vs. preferences, precedence order of settings, templates and more.

IEZoneAnalyzer’s main dialog is where you define what settings you want to view or compare. There are three ways to create those definitions, each in its own area of the screen: Show Effective Settings; View/Compare Entire Collections of Settings; and Compare Zone Settings. Each of these is discussed in the next sections of this document. The menu toolbar provides the ability to save current security zone settings to an XML file, and to load previously saved settings for viewing and comparing; and to identify the security zone in which a URL will be rendered.

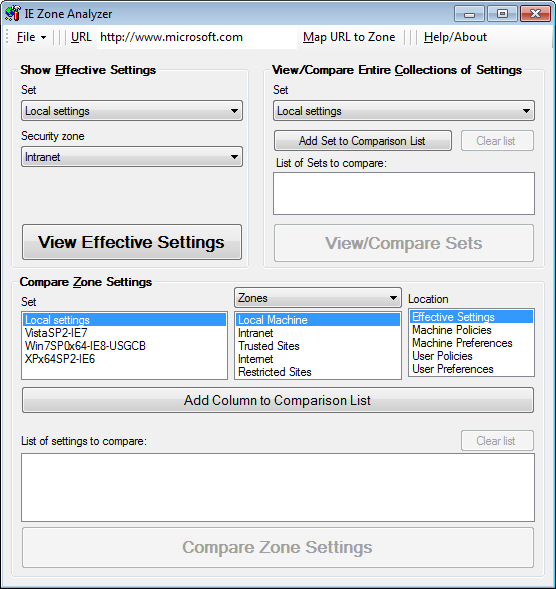


Figure 1. The IEZoneAnalyzer main dialog *(note: 3.5 adds a “Zone Map Viewer” button to the toolbar; not shown here)*

# Show Effective Settings

“Effective Settings” are the security zone settings that apply to a given security zone. They are computed by inspecting the zone’s machine policies, user policies, user preferences and machine preferences, taking into account the precedence order for these settings and whether the Group Policy setting “Security Zones: Use only machine settings” is enabled. The Effective Settings Viewer can show whether intended settings are actually being applied and taking effect.

In the Show Effective Settings area of the IEZoneAnalyzer main dialog, select “Local settings” or a previously saved configuration from the “Set” dropdown list, select a zone from the “Security zone” dropdown list, then click View Effective Settings to display the Effective Settings Viewer. The “Security zone” dropdown list includes the five standard security zones and the five “Locked-Down” security zones. (See Saving Settings and Loading Saved Settings 4 later in this document for information about populating the “Set” dropdown list. See the Appendix for information about the “Locked-Down” zones.)

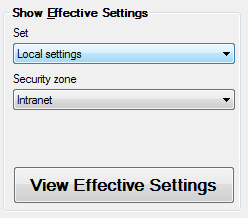


Figure 2. The Show Effective Settings area of the IEZoneAnalyzer main dialog

The Effective Settings Viewer displays each security setting identifier (also known as an “URL Action”), its corresponding description, the effective configured setting, and whether it came from machine policy, user policy, user preferences or machine preferences. The “Use only machine settings” label on the right side of the menu toolbar indicates whether the “Security Zones: Use only machine settings” Group Policy setting is enabled. The Effective Setting Viewer also adds a row representing the collection’s OS version, IE version, and machine name, and “Security Zones: Use only machine settings” setting. In the example in Figure 3, results are shown for the Intranet zone from settings saved from a USGCB-configured Windows 7 computer. See The View/Compare Windows 4 section later in this documentation for information on exporting results to Excel, copying to the clipboard, finding specific text, and sorting, reordering and resizing result columns.

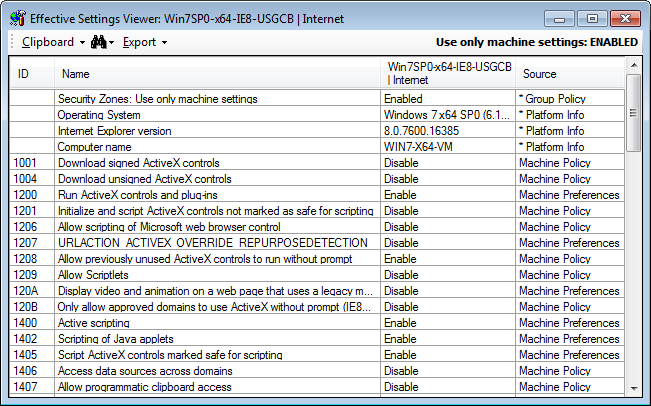


Figure 3. The Effective Settings Viewer

# View/Compare Entire Collections of Settings

This feature lets you see all the current settings from the local computer or all the settings from a previously saved collection. You can also view it side by side with one or more other collections and highlight the differences between them. You can filter the results to show only the differences or conflicts. This can be useful to determine whether a system has drifted from a configured baseline, for example, or to see how default settings have changed between releases of Windows or Internet Explorer.

To view all the settings from a single collection, select it from the “Set” dropdown list in the “View/Compare Entire Collections of Settings” area, click the Add Set to Comparison List to add the collection to the “List of Sets to compare” list box, then click the View/Compare Sets button to launch the Setting Collection Comparer. The “List of Sets to compare” list box identifies the collections that the Setting Collection Comparer will display. To compare two or more sets, select each additional collection of interest from the “Set” dropdown list and click Add Set to Compare List to add each to the list of sets to compare before clicking View/Compare Sets. To remove a set from the comparison list, select it in the list box and press the Del key. Click the “Clear list” button to empty the list.

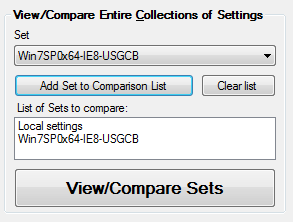


Figure 3. The View/Compare Entire Collections of Settings area of the IEZoneAnalyzer main dialog

The Setting Collection Comparer enumerates all settings in all zones for machine policies, machine preferences, user policies, and user preferences, and then the settings in the five templates ("High", "Medium-high", "Medium", "Medium-low", and "Low"). The Comparer adds a column for each included collection with the collection name in the column header. The cell for a given setting is highlighted in yellow if it has a different value from the corresponding setting in one or more other collections. A cell is highlighted in gray if the collection does not define a value for that setting. (The yellow highlighting can be turned off. See [The View/Compare Windows 4](#_Toc289170131) for details, as well as information about showing only differences or conflicts, exporting results to Excel, and more.)

The Setting Collection Comparer also adds a row representing each collection’s OS version, IE version, and machine name, and whether the setting for “Security Zones: Use only machine settings” is enabled in Group Policy.

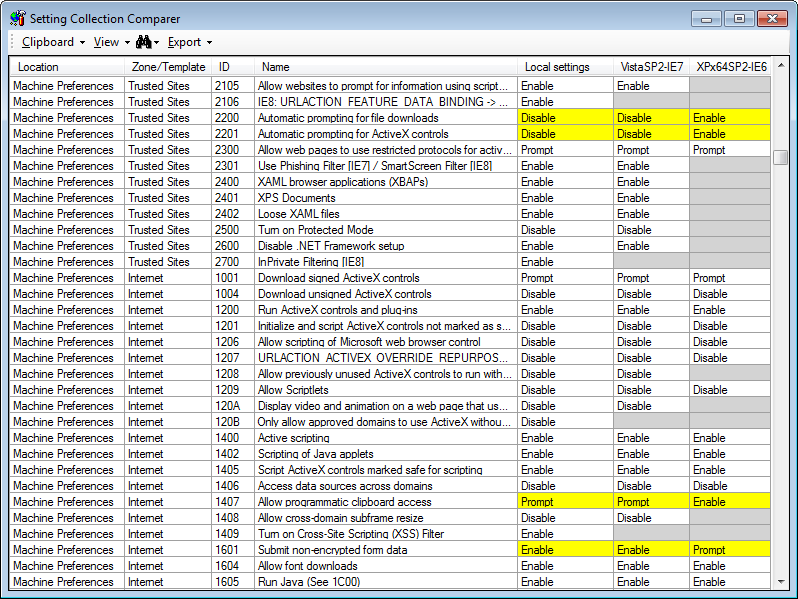


Figure 4. The Setting Collection Comparer

# Compare Zone Settings

The IEZoneAnalyzer “Compare Zone Settings” feature lets you compare two or more security zone settings. Each item to be compared can come from current local settings or from previously saved settings, the effective settings for any zone in those collections or just the settings from a specific source such as machine policies or user preferences, or the settings from a template in any of the collections. Examples that may be of interest:

* Compare the effective settings for the Internet zone from a default configuration to those from a system with security policies applied.
* Compare the effective settings for the Locked-Down Local Machine Zone (LMZL) to those of the Local Machine Zone to see what becomes enabled when the user clicks through the information bar to enable functionality. (See the Appendix for information about the LMZL.)
* Compare the relative security settings of the Intranet zone to those of the Trusted Sites zone.
* Compare the Machine Preferences for a zone to those of the User Preferences for that zone (ordinarily they should be the same).
* Create a table for export to Excel listing the effective settings for all zones and templates.

The “List of settings to compare” list box in the Compare Zone Settings area of the IEZoneAnalyzer main dialog shows the settings that will be compared against each other. To add an item to the list, select a collection from the “Set” list box, a zone or template from the middle dropdown list and list box, “Effective Settings” or a set of policies or preferences, then click “Add Column to Comparison List”. The dropdown list in the middle column changes the items in the middle list box to the five standard zones, the five “Locked-Down” zones, or the five templates. When “Templates” is selected, the “Location” list is dimmed since template settings come from one location. To remove one item from the “List of settings to compare”, select it in the list box and press the Del key. Click the “Clear list” button to remove all items from the list.

Click the Compare Zone Settings button to launch the Zone Settings Comparer with the selected settings.

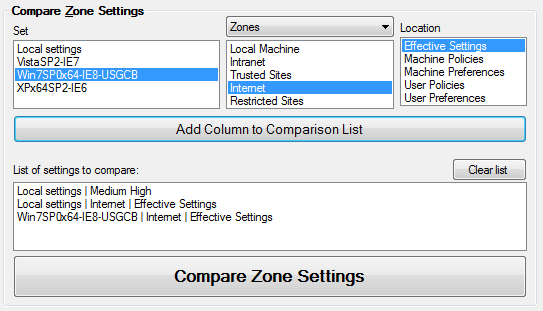


Figure 5. The Compare Zone Settings area of the IEZoneAnalyzer main dialog

The Zone Settings Comparer enumerates all the setting identifiers (“URL actions”) found in the union of the settings and lists them along with corresponding descriptive text. The Comparer adds a column for each included group of settings with the group name in the column header. As with the Setting Collection Comparer, rows are added representing each collection’s OS version, IE version, machine name, and “Security Zones: Use only machine settings” setting. Likewise, the cell for a given setting is highlighted in yellow if it has a different value from the corresponding setting in one or more other collections. A cell is highlighted in gray if the collection does not define a value for that setting. (The yellow highlighting can be turned off. See The View/Compare Windows 4 section for details, as well as information about showing only differences or conflicts, exporting results to Excel, and more.)

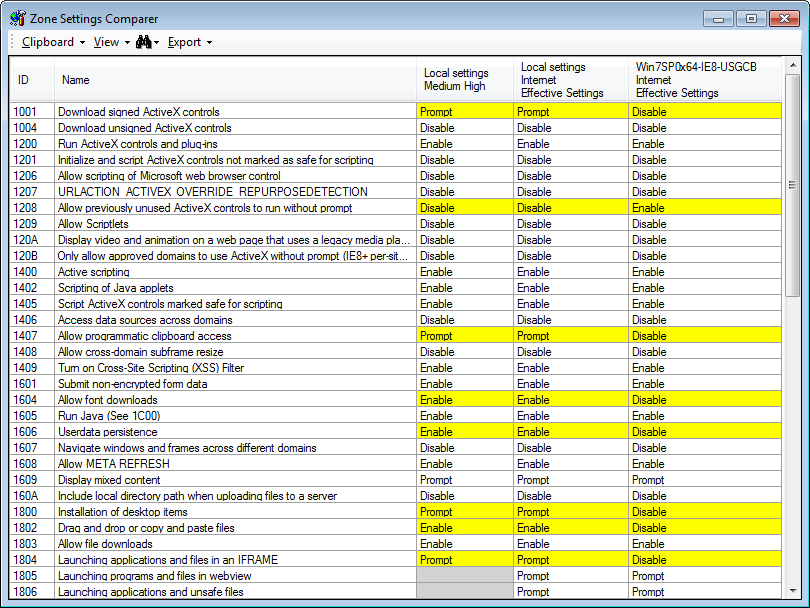


Figure 6. The Zone Settings Comparer

# Saving Settings and Loading Saved Settings

IEZoneAnalyzer lets you capture the current IE security zone settings on the local computer and save them to a file that can be loaded at a later time by IEZoneAnalyzer on the same or a different computer. Choose “Export local settings…” from the File menu and provide a file name. IEZoneAnalyzer creates an “IEZoneAnalyzer” subfolder in your “My Documents” folder and uses it as the default location for its saved files. IEZoneAnalyzer’s default file extension for saved files is \*.IEZoneSettings. The files are actually XML saved as UTF-8, and easily edited with Notepad or another text editor.

To load previously saved files, choose “Import saved settings…” from the File menu. The “Load saved IE security zone settings” dialog lets you select and import multiple files at once. Each file that is loaded is added to the “Set” lists in each of the task areas in the IEZoneAnalyzer main dialog.

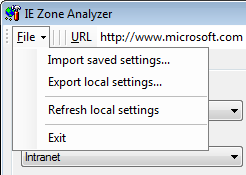


Figure 7. The IEZoneAnalyzer File menu

If local settings change while IEZoneAnalyzer is running, choose “Refresh local settings” from the File menu to reload settings from the registry. Note that if “Local settings” is already in the either of the comparison lists for comparing zone settings or entire collections, you need to remove them from the lists and re-add them to get the refreshed data.

# The View/Compare Windows

The Effective Settings Viewer, Setting Collection Comparer and Zone Settings Comparer share features in common. The two Comparer windows have a few extra features to support comparisons. The features common to all three include:

## View Options (Comparer windows)

The View menu in the Zone Settings Comparer and in the Setting Collection Comparer provides these options:

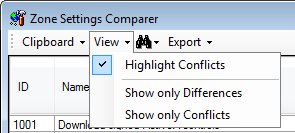


Figure 8. The View menu in the Zone Settings Comparer (also found in the Setting Collection Comparer)

* **Highlight Conflicts**: when checked, this option highlights row cells with yellow to indicate that the row contains two or more defined values that are different from one another. This option is selected by default. (You may want to uncheck this option if you are showing only rows with conflicting values or if the purpose for the data is not to identify differences – for example, if you simply want a list of all settings for all zones.)
* **Show only Differences**: when checked, this option hides all rows in which all values are the same. This option does not hide rows in which one or more of the columns does not define a value (shaded in gray).
* **Show only Conflicts**: when checked, this option shows only those rows in which multiple different values are defined. Unlike “Show only Differences”, this option hides rows in which the only differences are that one or more cells do not have a defined value.

## Export to Excel

Choose Export | to Excel… from the menu toolbar to launch Microsoft Excel 2007 or newer with a new spreadsheet containing all data from the current window, including column headers and cell coloring, and retaining column ordering and sorting. If one of the Comparer windows’ View menu filtering options is in effect, only rows selected for display are written to the spreadsheet. Note that if you don’t want the yellow highlighting of differences across columns, uncheck the View | Highlight Conflicts option in the Comparer window before exporting to Excel.

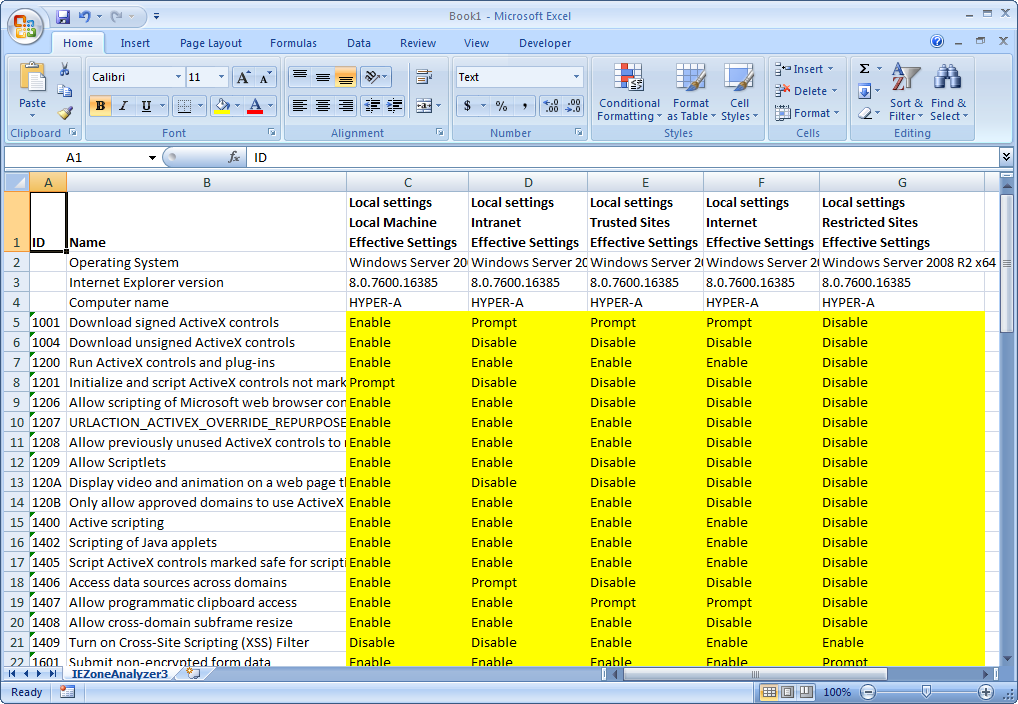


Figure 9. IEZoneAnalyzer data exported to Microsoft Excel 2007

## Export to CSV

Choose Export | to CSV… from the menu toolbar, enter a file name (default extension \*.csv) and press Enter. IEZoneAnalyzer writes the text in the table, including column headers as well as row data, to the Comma-Separated Values (CSV) file you specified, retaining the window’s current column order and sort ordering. If one of the Comparer windows’ View menu filtering options is in effect, only rows selected for display are written to the CSV file. The CSV file can be imported easily into Microsoft Excel or another data store.

## Clipboard Copy

Select one or more rows and press Ctrl+C to copy the selected rows to the clipboard. Press Ctrl+A to select all rows in the window as well as the column headers. Row data copied to the clipboard can be pasted directly as a new table in Microsoft Word or into an Excel spreadsheet. (The Ctrl+A and Ctrl+C options can also be found on under “Clipboard” on the menu toolbar.)

## Find Text

Press Ctrl+F to display the Find dialog enter text to search for and press Enter. IEZoneAnalyzer selects the next row that contains the search text in any column. Press F3 to repeat the previous search without displaying the Find dialog. (These options can also be found under the binoculars icon on the menu toolbar.)

## Column Sorting, Sizing, Re-ordering

Alphabetically sort on any column by clicking on its column header. Toggle the sort order by clicking the column header again.

You can change the order of columns in the View/Compare windows by clicking on a column header and dragging it to a new location.

Click and drag the right border of a column header to change the column’s width. Double-click the right border of a column header to automatically resize the column width to the widest text in the column.

## Modeless Operation

The View/Compare windows are modeless. You do not need to close a View/Compare window to launch another window. Simply select the IEZoneAnalyzer main dialog and launch another viewer. All viewer windows are closed when the main dialog is closed.

# Map URL to Zone

IEZoneAnalyzer’s “Map URL to Zone” feature lets you identify the security zone in which a given URL will be rendered. This can be helpful when trying to determine whether Site to Zone Assignment List policies have been defined and deployed correctly.

In the IEZoneAnalyzer’s main dialog, type the URL into the text area of the menu toolbar and click “Map URL to Zone”. IEZoneAnalyzer displays the URL and its zone in a message box. (If you prefer keyboard shortcuts, Alt+U moves focus to the URL text area, and Alt+M invokes the “Map URL to Zone” feature.)



Figure 10. The URL text area and Map URL to Zone button in the IEZoneAnalyzer main dialog’s menu toolbar.

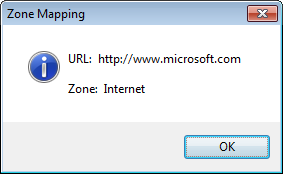


Figure 11. The Map URL to Zone result.

# Zone Map Viewer

IEZoneAnalyzer version 3.5 adds a Zone Map Viewer that shows which web sites have been specifically assigned to security zones. Click on the “Zone Map Viewer” button in the main dialog’s toolbar to display the Zone Map Viewer. You can toggle the Zone Map Viewer between an “Effective Settings” view and a “Raw Settings” view with labeled toolbar buttons.

“Effective Settings” lists the configured web sites and the zones to which they are mapped. The Comments column calls out settings that are applicable only to 32-bit processes or only to 64-bit processes, or that are completely overridden and never take effect. (An Appendix to this document describes the rules that determine whether settings are effective or ignored.) For example, Figure 12 shows a number of site assignments to Trusted Sites that are overridden because they are defined in User Preferences, but overridden both because the “use only machine settings” group policy is in effect and because a Computer Configuration Site-To-Zone Assignment policy is in effect. Figure 12 also shows two overridden settings that are in effect only when Enhanced Security Configuration (ESC) is in effect, which is not the case as shown by the informational lines at the top of the listing. A given site is listed only once in the Effective Settings view. If a site is mapped the exact same way in a registry location that is in effect and in another that is not in use, the “overridden” one is not shown. That is, a setting is shown as “overridden” only if is defined somewhere differently from what is actually in effect.

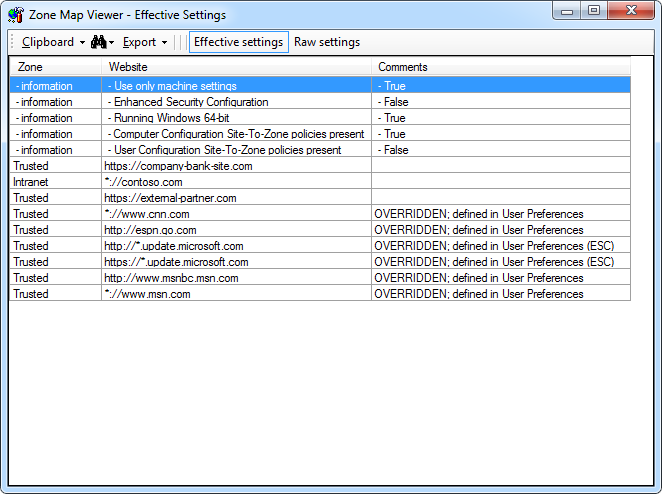


Figure 12. Zone Map Viewer displaying Effective Settings.

The “Raw Settings” view shows all site-to-zone configuration settings, listing where they are defined, the zone each is assigned to, and whether that particular setting is in effect or ignored. Both views show the criteria that are used to determine which ZoneMap settings are in effect and which are ignored (per the rules listed in the Appendix.)

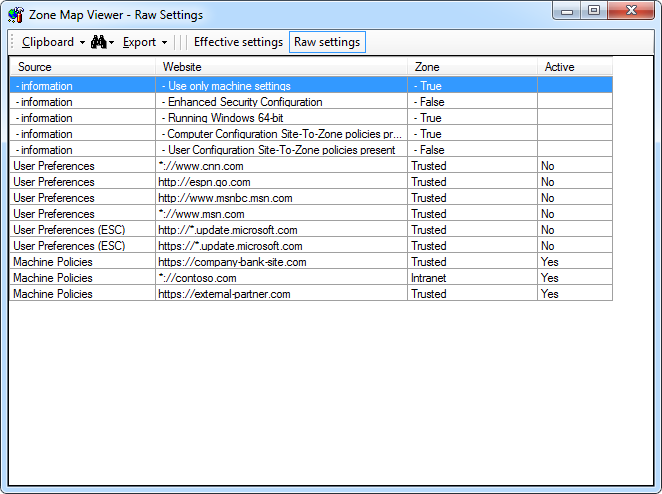


Figure 13. Zone Map Viewer displaying Raw Settings.

As with all other IEZoneAnalyzer views, columns can be sorted, resized and reordered; content can be searched for specific text, copied to the clipboard and exported to CSV and to Excel files. Further, the sort order for the “Website” columns is based on domain names rather than on a strict alphabetic order. For example, all the “microsoft.com” mappings are grouped together, alphabetized by subdomains in reverse order.

# Help/About

Click Help/About in the IEZoneAnalyzer menu toolbar. The Help/About dialog includes hyperlinks to additional useful information.

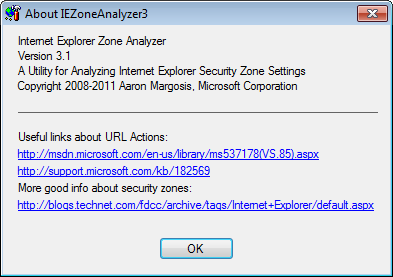


Figure 14. The IEZoneAnalyzer Help/About dialog. (TODO: Get the v3.5 screenshot.)

# Appendix: Definition of Terms

This content is extracted from the blog post, ***FDCC and Internet Explorer 7, Part 1: Security Zones*** (<http://blogs.technet.com/b/fdcc/archive/2008/09/19/fdcc-and-internet-explorer-7-part-1-security-zones.aspx>)

## Zones and Policies

There are many capabilities that can be leveraged by a web browser beyond rendering static HTML. These capabilities can include the ability to run script, to invoke installed mobile code (such as Java or ActiveX), and to manipulate the clipboard. Permission to use some of these capabilities should be granted only to trustworthy content. The concept behind IE security zones is that the source of the content to be rendered by the browser – in other words, where the content came from – can be used to help determine the trustworthiness of that content. Zones that are defined by Internet Explorer include:

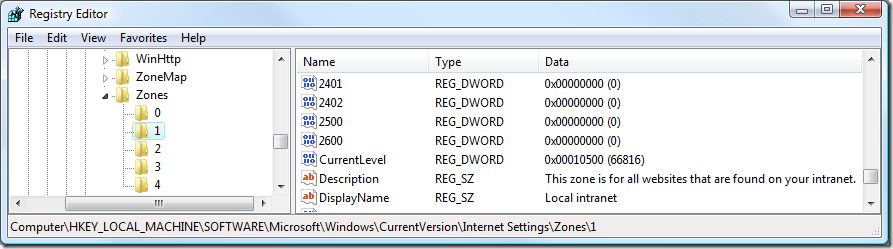
* Local Machine (a.k.a., "Computer" or "My Computer") zone is for content that is already found on the local computer (but not in the Temporary Internet Files cache). In the past this had been considered the most trusted content; this was changed by the "Local Machine Zone Lockdown" feature first introduced in Windows XP SP2, and which is described in more detail below.
* Local Intranet zone is for content found on the organization’s intranet.
* Internet zone is for content found on the Internet – this is considered an untrustworthy source for content.
* Trusted Sites are for external sites that are explicitly determined by the user or by the administrator to be more trustworthy than other content on the internet.
* Restricted Sites are for sites that are explicitly determined by the user or by the administrator to be less trustworthy than other content on the internet.

Registry settings determine which capabilities are permitted for each zone. There are dozens of these settings, which are documented in [KB 182569](http://support.microsoft.com/kb/182569). For example, the value "1201" maps to the permissions for "Initialize and script ActiveX controls not marked as safe." These zone settings can be defined in multiple places, with a hierarchy determining which settings are actually in effect:

* Machine Policies (HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones)
* Machine Preferences (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones)
* User Policies (HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones)
* User Preferences (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones)

Under each of these "Zones" keys are subkeys for each of the security zones:

* 0: Local Machine
* 1: Local Intranet
* 2: Trusted Sites
* 3: Internet
* 4: Restricted Sites

[](http://blogs.technet.com/blogfiles/fdcc/WindowsLiveWriter/FDCCandInternetExplorer7Part1SecurityZon_2D57/RegEditIEZones.png)

The default precedence order for settings for a particular zone is:

* Machine Policies
* User Policies
* User Preferences
* Machine Preferences

Policies always take precedence over Preferences, so if a registry value exists for a capability in a Policies key, it will override a corresponding setting in a Preferences key for that zone. In a default Windows install, no Policies keys are populated, so only Preferences are in effect. The Federal Desktop Core Configuration (FDCC) mandates a bunch of Policies settings, particularly for the Internet zone. Note that all the User Policies keys (starting in HKCU\Software\Policies and HKCU\Software\Microsoft\Windows\CurrentVersion\Policies) are *read-only to non-admin users* – even though they are in HKCU. Policies are hard to enforce if you let users overwrite them.

Also note that the correct way to populate the Policies is through Group Policy interfaces, not by pushing data directly into those registry keys. The Group Policy interfaces (whether programmatic or interactive tools) ensure that the Group Policy stores (registry.pol files) contain the authoritative settings, and that the GP hierarchy (domain vs. OU vs. local policies) is respected. If you apply settings directly into the registry, they will likely get overwritten or deleted upon the next Group Policy refresh.

*By default*, User Preferences take precedence over Machine Preferences. *By default*, Machine Preferences come into play only when a corresponding value does not exist in the User Preferences. However, there is a group policy, "Security Zones: Use only machine settings", which FDCC mandates. With this policy in effect, User Policies and Preferences are ignored – only the Machine Policies and Preferences are used. This helps ensure that non-admin users do not override administrative security choices.

Note that the Security tab of the Internet Properties dialog shows User Preferences *only*. And when Policies are in effect, most or all of the Security tab UI is disabled, with a label at the bottom explaining, "Some settings are managed by your system administrator".

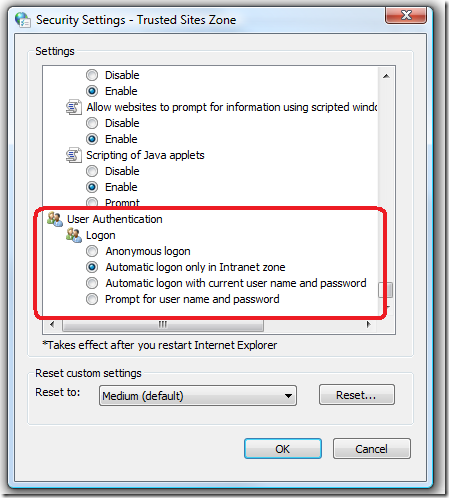
## Templates

"Templates" define a collection of settings that can be applied to a zone as a comprehensive group. These collections appear in the IE Security tab as security levels "High", "Medium-high", "Medium", "Medium-low", and "Low". When you set a particular zone to one of these levels, it copies the settings for that template to the User Preferences for that zone. The Template settings are defined in the registry in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\TemplatePolicies.

## Local Intranet Zone vs. Trusted Sites Zone

Originally, the "Trusted Sites" zone was treated as the most trustworthy of all the zones. It was configured to use the "Low" security level template, while "Local intranet" was set to "Medium-low". Starting with Internet Explorer 7, however, security on "Trusted Sites" was tightened up, and it now defaults to the "Medium" security level template. So now, ***"Local Intranet" has more relaxed permissions than "Trusted Sites"*.** It is recommended to use the "Intranet" zone for internal sites, and "Trusted Sites" for trusted *external* sites.

For organizations that had added their dotted-name intranet sites to the "Trusted Sites" zone and are using default permissions for that zone, one very notable impact is that browsing IIS web sites that use Windows authentication now prompts for credentials rather than just using the Windows logon of the user to flow through. This is because the "Logon options" security setting for "Medium-low" and above sends credentials automatically only in the Intranet zone (see screenshot).

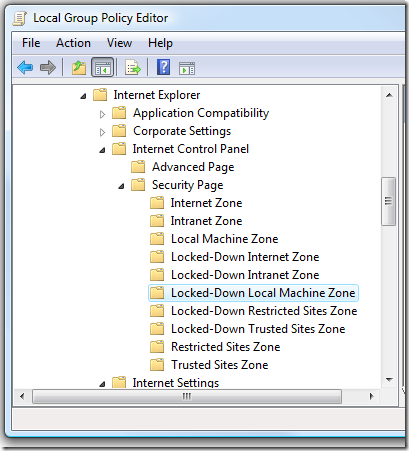
[](http://blogs.technet.com/blogfiles/fdcc/WindowsLiveWriter/FDCCandInternetExplorer7Part1SecurityZon_2D57/LogonOptions.png)

When Trusted Sites was based on the "Low" template, the Logon option defaulted to "Automatic logon with current user name and password." But generally you do not want Internet Explorer to try to log on automatically with the user’s current username and password to an external site, even a "trusted" one.

By default, URLs in which the server name contains dots are assumed to be in the Internet zone, even if they are on your organization’s intranet; e.g., http://hrweb.contoso.com. One way to define the fully-qualified domain names (FQDNs) that should be considered intranet is through the "Site to Zone Assignment List" in Group Policy (Computer Configuration \ Administrative Templates \ Windows Components \ Internet Explorer \ Internet Control Panel \ Security Page). For more information on zone detection algorithms, see this page: <http://msdn.microsoft.com/en-us/library/bb250483(VS.85).aspx>.

## The "Locked Down" Security Zones

Those who have dug into Group Policy for Internet Explorer and/or the details of FDCC configuration have probably noticed that in addition to the standard zones ("Internet", "Intranet", etc.), there are corresponding "Locked-Down" zones, with their own collections of settings:

[](http://blogs.technet.com/blogfiles/fdcc/WindowsLiveWriter/FDCCandInternetExplorer7Part1SecurityZon_2D57/LockedDownZonesInGpEdit.png)

The Policies and Preferences for these zones live in "Lockdown\_Zones" keys near the corresponding machine and User Policies and Preferences:

* Machine Policies: HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\**Lockdown\_Zones**
* Machine Preferences: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\**Lockdown\_Zones**
* User Policies: HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\**Lockdown\_Zones**
* User Preferences: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\**Lockdown\_Zones**

The "Locked-Down Local Machine Zone" is very different from the other "Locked-Down" zones.

The Lockdown\_Zones settings for the Local Machine zone (zone 0) are used by a feature first introduced in Windows XP Service Pack 2 called "Local Machine Zone Lockdown" (LMZL). By default, when a page is opened in the Local Machine zone, it runs with the more restrictive policies/preferences in the Lockdown\_Zones\0 registry keys, rather than the usual Zones\0 settings. By default, the LMZL settings disable ActiveX and script. If the content in the page tries to use ActiveX or script, the information bar prompts the user whether to allow them to run. If the user allows the blocked content, Internet Explorer then uses the less-restrictive, normal Local Machine zone policies/preferences from that point forward for the lifetime of that browser tab (for IE7+) or browser window (IE6).

You can find more information about LMZL on the following pages:

* <http://technet2.microsoft.com/WindowsVista/en/library/44a2d577-3ee5-4b44-9af7-aaebcfcf41341033.mspx>
* <http://technet2.microsoft.com/windowsserver/en/library/aebcfc94-25d5-4f41-93cc-7fb6e031de401033.mspx>

The Lockdown\_Zones settings for the other zones (Intranet, Internet, etc.) are used to support a feature called "Network Protocol Lockdown" (NPL). This can be used to force content received over less-commonly used URL schemes to be provided restricted permissions. http: and https: are the most common URL schemes. Less common schemes include ftp:, file:, mailto:, shell:, and application-defined pluggable protocols. NPL restrictions are off by default, but administrators may choose to enable lockdown zones for specific applications and URL schemes to help reduce attack surface.

More information about NPL can be found here:

* <http://technet2.microsoft.com/windowsserver/en/library/44a1af75-935b-4cc2-97cd-da3b7e8bfc891033.mspx>

# Appendix: Internet Explorer’s Explicit Security Zone Mappings

Internet Explorer applies a set of rules to associate web sites (URLs) with security zones, based on criteria such as whether the server has a dot in its name. In addition, group policies, computer settings and user preferences can be used to map specific URLs to specific zones. For example, you could explicitly add “https://www.contoso.com” to the Trusted Sites zone. Such site-to-zone mappings are defined under one or more ZoneMap key hierarchies in the registry. There are five different locations where ZoneMap key hierarchies can be defined, but only one or two of them will be in effect at any particular point in time. Exactly which settings under which ZoneMap keys are effective depends on a number of circumstances:

* Whether Site-To-Zone-Assignment lists are configured in Computer Configuration and/or User Configuration group policies;
* Whether the “Security Zones: Use only machine settings” group policy is configured (a.k.a., Security\_HKLM\_only);
* Whether Internet Explorer’s Enhanced Security Configuration (ESC) is enabled (Server only);

and, quite surprisingly:

* Whether or not the program is a 32-bit process on 64-bit Windows; a.k.a., “Windows On Windows 64” or WOW64.

Yes, that’s right – in some circumstances, a 32-bit process and a 64-bit process on the same computer can see the same site mapped to different security zones.

Also, my testing indicates that there is a bug that results in all URLs being treated as “Internet” zone when both ESC *and* a Computer or User Site-To-Zone-Assignment list are enabled.

## Explicit Site To Zone Rules

The rules for selecting ZoneMap keys are listed below. Each table shows some combination of the four circumstances described in the overview; following each table is the key or keys that are in effect in those circumstances. There are separate settings under each ZoneMap key for “ESC on” and “ESC off”. If ESC is on, only those settings under the EscDomains and EscRanges subkeys are used; if ESC is off, only the settings under the Domains and Ranges subkeys are used.

Note that in the tables below, WOW64 set to “Yes” means a 32-bit process on a 64-bit version of Windows. WOW64 set to “No” means either a 32-bit process on a 32-bit version of Windows or a 64-bit process on a 64-bit version of Windows.

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Yes** | **Cleared** | **Absent** | **Absent** |

Combines results from

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(preference is given to HKCU)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **No** | **Cleared** | **Absent** | **Absent** |

Combines results from

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(preference is given to HKCU)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Yes** | **Set** | **Absent** | **Either** |

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(User site-to-zone assignments are ignored if present)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **No** | **Set** | **Absent** | **Either** |

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(User site-to-zone assignments are ignored if present)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Either** | **Either** | **Present** | **Absent** |

HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Either** | **Cleared** | **Present** | **Present** |

Combines results from

HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(preference is given to HKCU)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Either** | **Set** | **Present** | **Either** |

HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

(User site-to-zone assignments are ignored if present)

|  |  |  |  |
| --- | --- | --- | --- |
| *WOW64* | *Security\_HKLM\_only* | *Computer Site-To-Zone* | *User Site-To-Zone* |
| **Either** | **Cleared** | **Absent** | **Present** |

HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

## What About “ZoneMapKey”?

IT administrators trying to apply site-to-zone settings by directly manipulating registry values often discover two “ZoneMapKey” registry keys that appear to be more interesting than they actually are: specifically, HKCU\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMapKey and HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMapKey. Values under these keys look like the site-to-zone assignments applied through group policy, and in fact they are. However, these keys are not used directly by Internet Explorer, and if you directly set values there, they will have no effect. The ZoneMapKey entries are just a temporary writing place for the Group Policy engine, which writes entries there as specified by Group Policy, and then parses them into corresponding ZoneMap subkey settings that *are* used by Internet Explorer.