

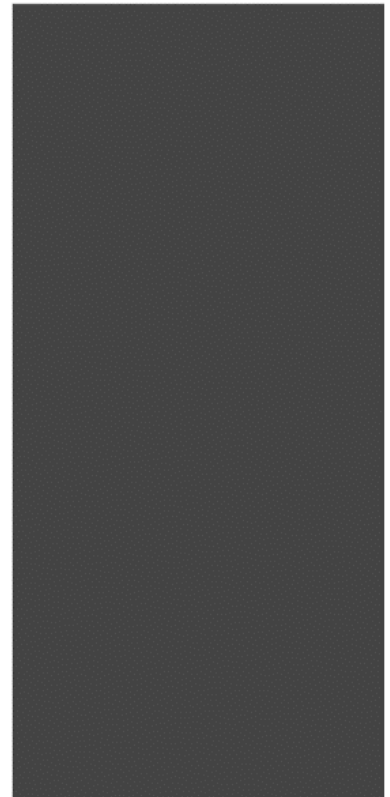
FEDERAL
RESERVE



FINANCIAL
SERVICES

Microsoft Internet Explorer[®] v9.0 Quick Set-Up for FedLine Web[®] and/or FedLine Advantage[®]

User Guide



CONTENTS

Preface.....	3
Section I.....	4
Internet Explorer Security Defaults	4
Setting up the Internet Explorer Trusted Web Content Zone	6
Internet Explorer Privacy Defaults.....	10
Java™ Environment	11
User Credentials	11
Section II	12
Accessing FedLine Web	12
Check Imaging Services Customers	12
Contacting Customer Support	12
Appendix A – Web Content Zone Default Values.....	13
“Internet” Web Content Zone Default Values.....	13
“Local Intranet” Web Content Zone Default Values.....	18
“Trusted Sites” Web Content Zone Default Values	23
“Restricted Sites” Web Content Zone Default Values	28

PREFACE

This set-up guide provides the basic information you need to successfully configure your Internet Explorer® v9.0 browser¹, download the requisite files, and perform the tasks necessary to use the FedLine Web® and/or FedLine Advantage® access solution(s).

LEGAL NOTICES

This information is provided solely as a convenience to Federal Reserve Bank customers. The Federal Reserve Banks do not have any obligation for and do not make any warranty or representation of any kind with respect to any and/or all aspects of non-Federal Reserve Bank software and/or equipment, including but not limited to its security attributes and/or compatibility with Federal Reserve Bank systems. Use of electronic connections to access Federal Reserve Financial Services and other applications provided by the Federal Reserve Banks is governed by the Federal Reserve Banks' Operating Circular 5.

The copyright in Microsoft Internet Explorer v9.0 software is owned by Microsoft Corporation. Use of Microsoft Internet Explorer v9.0 software is governed by terms and conditions provided by Microsoft. Federal Reserve Bank customers are responsible for obtaining any necessary permission or license to use Microsoft Internet Explorer v9.0 software. Nothing in this document should be construed to transfer any rights to use Microsoft Internet Explorer v9.0 software.

The Federal Reserve Banks encourage organizations to follow their established organizational security policies and procedures. The appropriate management and technical support personnel at the organization should be consulted prior to making any configuration changes

The Financial Services logo, "FedLine", "FedLine Web" and "FedLine Advantage" are registered service marks of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at www.FRBservices.org.

"Microsoft", "Internet Explorer", "Windows" and "Windows Vista" are registered trademarks of Microsoft Corporation in the United States and/or other countries.

"Java" is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

¹FedLine Web and FedLine Advantage require browsers to be configured to use 128-bit encryption. If you are unsure of the encryption level of your browser or how to upgrade, please contact the Customer Contact Center listed in Section II.

SECTION I

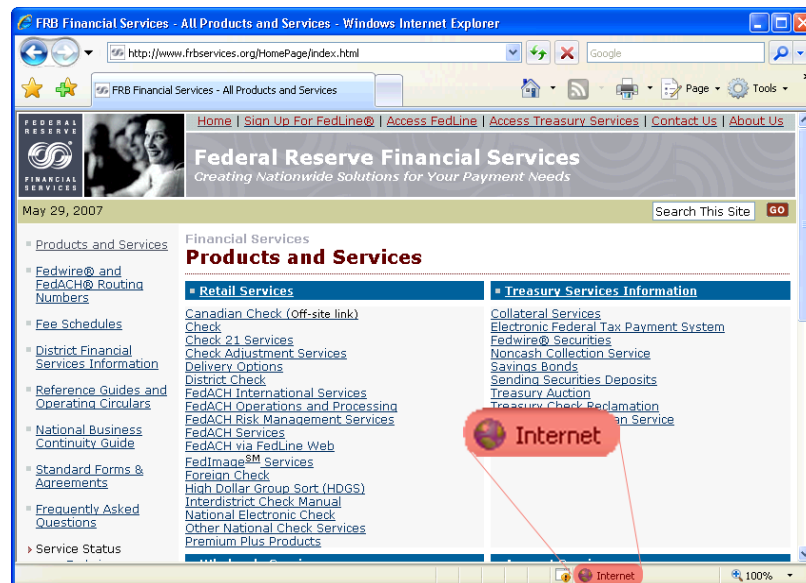
INTERNET EXPLORER SECURITY DEFAULTS

Internet Explorer v9.0 supports four “Web Content Zones,” as defined by Microsoft. The four Web Content Zones are Internet, Local Intranet, Trusted Sites and Restricted Sites. These different zones allow a user to select a different level of security for different Web sites. Most public Internet sites fall into Microsoft’s “Internet” content zone. By default, Federal Reserve Bank Web sites also fall into the “Internet” content zone.

Access for each content zone can be customized as desired, by you or your organization’s network administrators. Internet Explorer v9.0 allows Web Content Zone settings to be changed at any time.

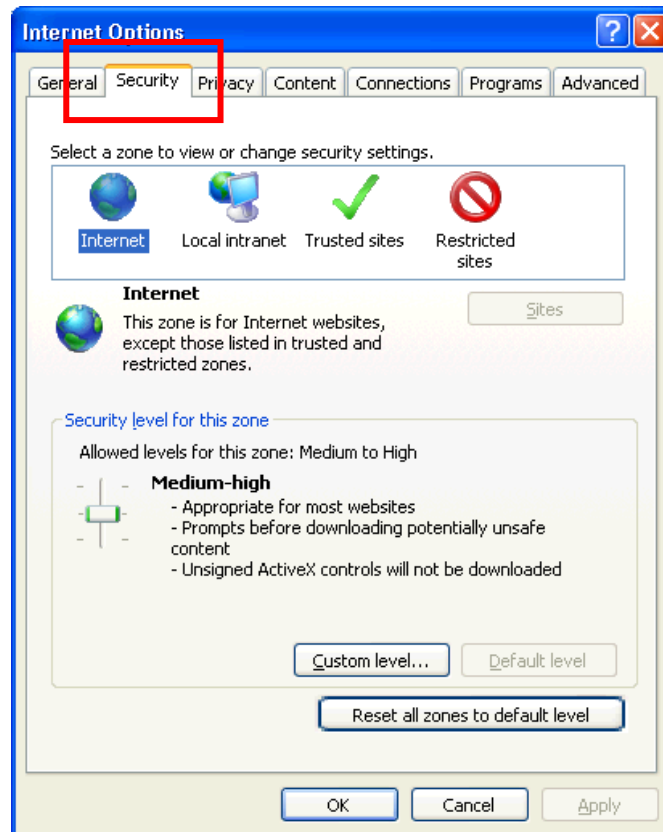
Federal Reserve Bank Web sites will initially launch in the Internet content zone and should function effectively using the zone’s default values. However, newer releases of Internet Explorer have introduced technologies, such as pop-up blockers and more stringent access controls, which may adversely impact your FedLine experience over the “Internet” zone. Therefore, you also may choose to run a Federal Reserve Bank Web site in the “Trusted sites” content zone, as defined by Microsoft. This zone allows for a greater degree of access and performance for Web-based applications and Web pages.

To determine the content zone in which your Federal Reserve Web sites are running, look at the status bar in the lower right-hand corner of the browser window. If the status bar is not visible, select “View” from the menu bar at the top of the browser window, and then click on “Status Bar.”



[FIGURE 1. WEB CONTENT ZONE INDICATOR]

If a Federal Reserve Bank Web site is not functioning correctly, you may need to make changes to the content zone settings. To view the content zones, select “Tools” from the menu bar at the top of the browser window, and then select Internet Options. Select the “Security” tab. The Internet Options window shown below will be displayed.



[FIGURE 2. INTERNET OPTIONS, SECURITY TAB]

Appendix A indicates the default values for each of the four Web content zones. You can use these default values to determine which settings have been changed within your browser.

The Federal Reserve Banks encourage organizations to follow their established organizational security policies and procedures. The appropriate management and technical support personnel at the organization should be consulted prior to making any configuration changes.

SETTING UP THE INTERNET EXPLORER TRUSTED WEB CONTENT ZONE

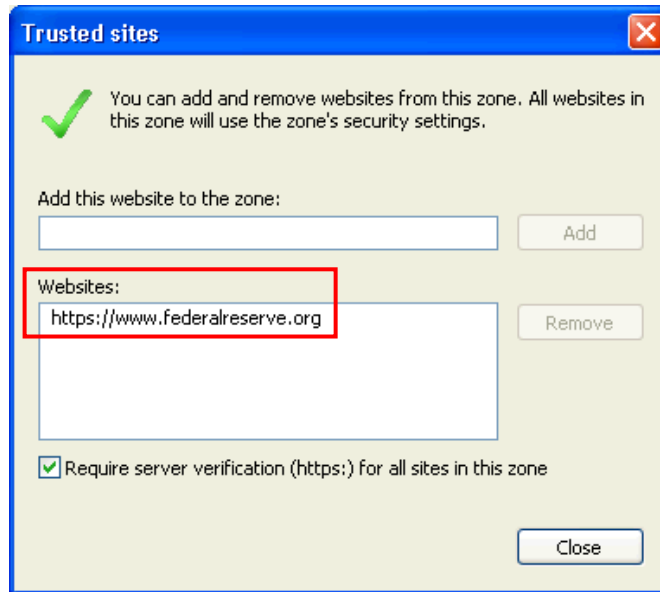
This content zone contains sites you trust. For example, trusted sites are allowed to download files and are not impacted by the pop-up blocker technology in newer versions of Internet Explorer. The default security level for the Trusted web content zone is Low.

1. Launch Internet Explorer and select “Internet Options” item from the Tools menu, then click on the “Security” tab:



[FIGURE 3. INTERNET OPTIONS, SECURITY TAB]

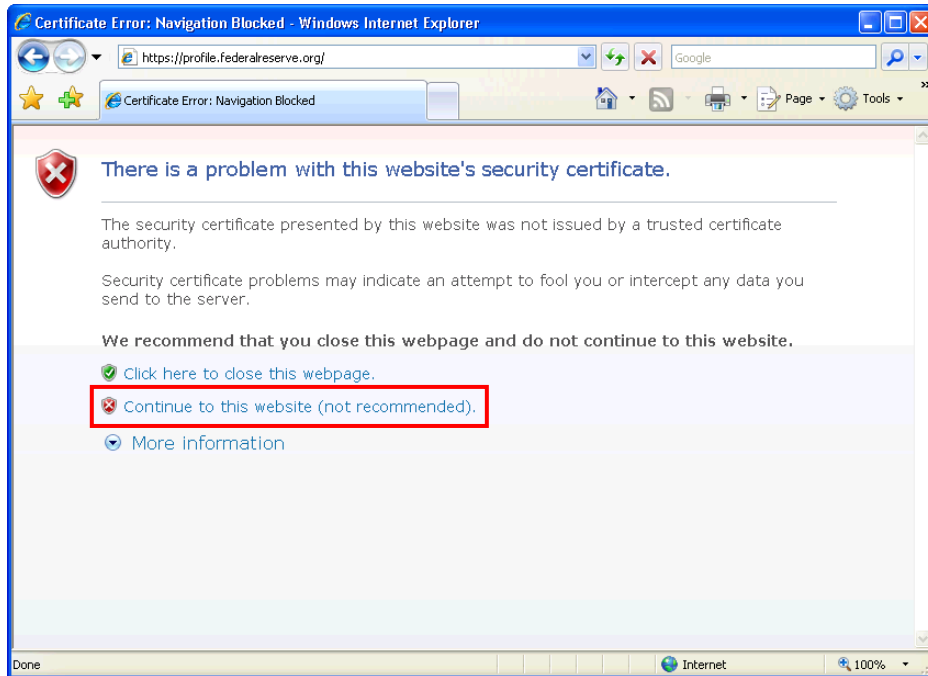
2. Click on the “Trusted sites” icon and then click on the “Sites...” button (Figure 3). A dialog window will display. Enter <https://www.federalreserve.org> then click on the “Add” button to save that setting. A populated window is shown below:



[FIGURE 4. INTERNET OPTIONS, TRUSTED SITES DIALOG BOX]

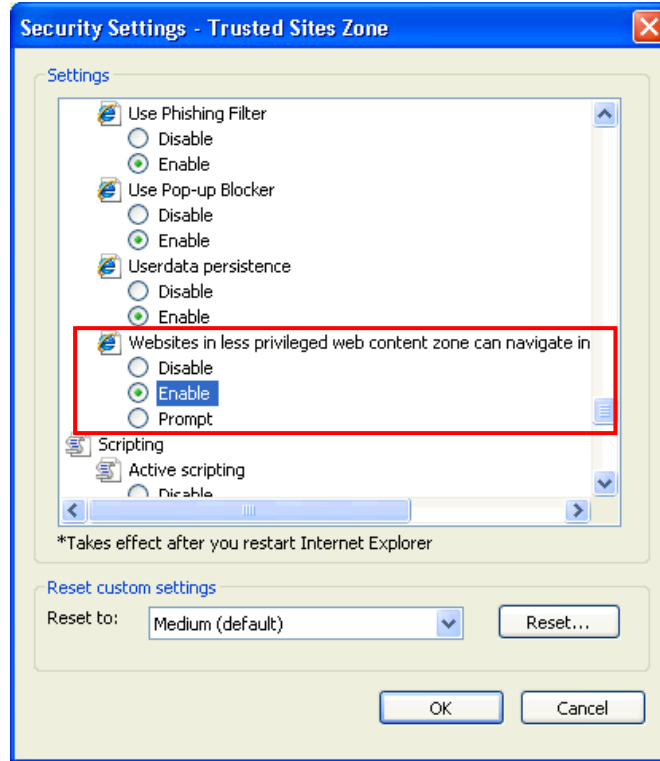
3. Click on the “Close” button to close the “Trusted sites” dialog window.
4. **Important Note: You may also want to consider completing steps 4a and 4b below. Before completing these steps, make sure the changes do not conflict with your organization’s existing security policy.**

If your organization chooses not to change these settings, Subscribers may receive the following security warning when clicking the “Access FedLine Home” button from www.FRBservices.org. This security warning might appear slightly different on different versions of the Internet Explorer browser but is still only a general warning for any site that issues SSL certificates for encryption. **After you have read the Security Warning, click “Continue to this website (not recommended)” if you would like to continue.** You must click “Continue to...” to access FedLine Home



[FIGURE 5. WARNING MESSAGE IN INTERNET EXPLORER v7/8/9]

- 4a. From the Security tab of the Internet Properties control panel, click on the “Custom Level...” button in the Trusted Sites section. A dialog window will display. Scroll down to the section called “Web sites in less privileged Web content zone can navigate...” and ENABLE this feature.



[FIGURE 6. SECURITY SETTINGS CUSTOM LEVEL DIALOG BOX]

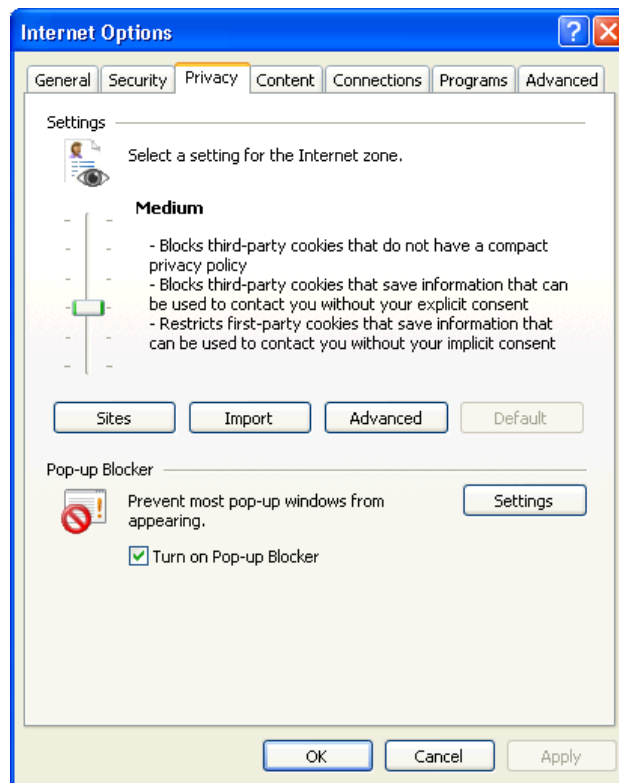
- 4b. Then click on the “OK” button to close the “Security Settings” window. You will be prompted to confirm your changes.
5. Then click on the “OK” button to close the “Internet Options” window.

You are now ready to access the appropriate Federal Reserve Bank Web site.



FedLine Advantage customers are encouraged to complete additional configuration steps, which are included in the FedLine Advantage technical documentation and setup process. Please work with your institution’s End User Authorization Contact (EUAC) to review this material, or you may call the Customer Contact Center (listed in Section II of this document).

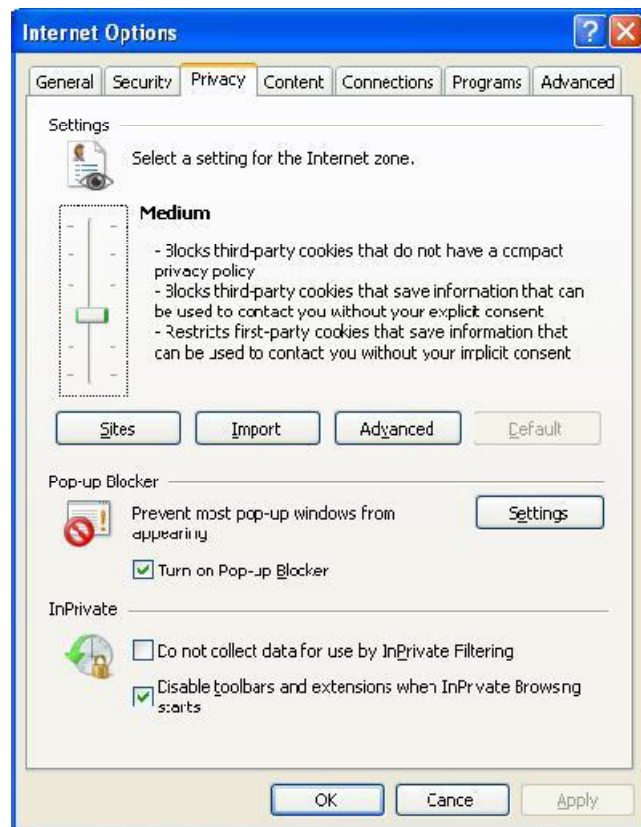
INTERNET EXPLORER PRIVACY DEFAULTS



[FIGURE 7. INTERNET OPTIONS, PRIVACY TAB]

The slider is used to specify the privacy level for the Internet zone. The default setting is “Medium.” If any other level is selected, the default button will be available; otherwise it is grayed out. Moving the slider changes the privacy level and displays a summary of attributes for the selected level.

Internet Explorer v9.0 includes a pop-up blocking feature that can be toggled on and off and configured on the Privacy tab within Internet Options. It is recommended that the URL's used to access the Federal Reserve Bank's financial services applications are added to the Allowed sites list within the Pop-up Blocker Settings dialog box.



[FIGURE 8. INTERNET OPTIONS, PRIVACY TAB, POP-UP BLOCKER SETTINGS]

JAVA™ ENVIRONMENT

If you are a Check Adjustments or Cash Services customer, please view the FedLine Web or FedLine Advantage Hardware and Software Requirements on www.FRBservices.org for the latest information regarding a required Java browser plug-in. This plug-in enables the Java applets used in the Check Adjustment and Cash Services applications.

USER CREDENTIALS

The Federal Reserve Banks use credentials to control access to the Federal Reserve Banks' Financial Services. Subscribers will be issued the appropriate credentials based on the services they access. For more information on requesting and retrieving credentials, please visit www.FRBservices.org and view either the FedLine Web Setup page or FedLine Advantage Setup page.

SECTION II

ACCESSING FEDLINE WEB

After you have completed your FedLine Web setup and acquired the necessary credentials, you will be able to access the Federal Reserve Banks' Financial Services from the following Web site: www.FRBservices.org. Click "Access FedLine" at the top of the screen, and then click "Access FedLine Home." You will be prompted to select the appropriate credential. Once you are connected to FedLine Home, you can select from all of the services that you are authorized to access.

CHECK IMAGING SERVICES CUSTOMERS

Please note: You also will need image-viewing software to utilize the Check Image Retrieval feature. For more information, contact your local Account Executive.

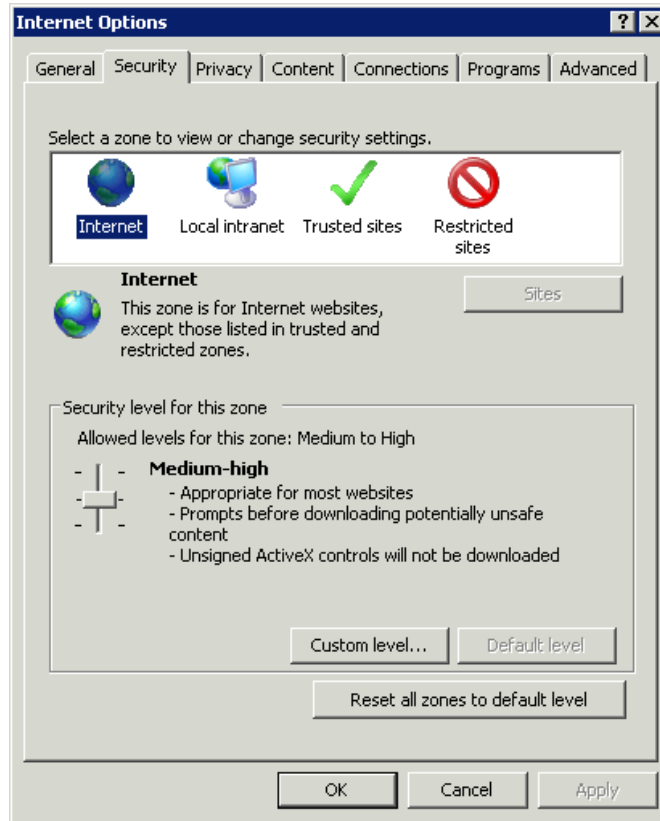
CONTACTING CUSTOMER SUPPORT

If you have a question, contact the Customer Contact Center at (888) 333-7010, Option 1

APPENDIX A – WEB CONTENT ZONE DEFAULT VALUES




Please note that the options displayed are based on the Windows XP Service Pack 3, Windows Vista Service Pack 2 and Windows Server 2003 Service Pack 1 operating systems. Settings may differ depending on operating system, browser patches or other Microsoft Windows system components you have installed.





“INTERNET” WEB CONTENT ZONE DEFAULT VALUES










- .NET Framework
 - Loose XAML
 - Disable
 - Enable
 - Prompt
 - XAML browser applications
 - Disable
 - Enable
 - Prompt
 - XPS documents
 - Disable
 - Enable
 - Prompt

“Internet” Web Content Zone Default Values















-  .NET Framework-reliant components
 -  Run components not signed with Authenticode
 - Disable
 - Enable
 - Prompt
 -  Run components signed with Authenticode
 - Disable
 - Enable
 - Prompt

-  ActiveX controls and plug-ins
 -  Allow previously unused ActiveX controls to run without prom
 - Disable
 - Enable
 -  Allow Scriptlets
 - Disable
 - Enable
 - Prompt
 -  Automatic prompting for ActiveX controls
 - Disable
 - Enable














 -  Binary and script behaviors
 - Administrator approved
 - Disable
 - Enable
 -  Display video and animation on a webpage that does not use
 - Disable
 - Enable
 -  Download signed ActiveX controls
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
 -  Download unsigned ActiveX controls
 - Disable (recommended)
 - Enable (not secure)
 - Prompt

 -  Initialize and script ActiveX controls not marked as safe for sc
 - Disable (recommended)
 - Enable (not secure)
 - Prompt
 -  Run ActiveX controls and plug-ins
 - Administrator approved
 - Disable
 - Enable
 - Prompt
 -  Script ActiveX controls marked safe for scripting*
 - Disable
 - Enable
 - Prompt






“Internet” Web Content Zone Default Values


-  Downloads
 -  Automatic prompting for file downloads
 - Disable
 - Enable
 -  File download
 - Disable
 - Enable
 -  Font download
 - Disable
 - Enable
 - Prompt
-  Enable .NET Framework setup
 - Disable
 - Enable
-  Miscellaneous
 -  Access data sources across domains
 - Disable
 - Enable
 - Prompt
 -  Allow META REFRESH
 - Disable
 - Enable
 -  Allow scripting of Internet Explorer web browser control
 - Disable
 - Enable
 -  Allow script-initiated windows without size or position constraints
 - Disable
 - Enable
 -  Allow webpages to use restricted protocols for active content
 - Disable
 - Enable
 - Prompt
 -  Allow websites to open windows without address or status bar
 - Disable
 - Enable
 -  Display mixed content
 - Disable
 - Enable
 - Prompt
 -  Don't prompt for client certificate selection when no certificate
 - Disable
 - Enable



“Internet” Web Content Zone Default Values

-  Drag and drop or copy and paste files
 - Disable
 - Enable
 - Prompt
-  Include local directory path when uploading files to a server
 - Disable
 - Enable
-  Installation of desktop items
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Launching applications and unsafe files
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Launching programs and files in an IFRAME
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Navigate sub-frames across different domains
 - Disable
 - Enable
 - Prompt
-  Open files based on content, not file extension
 - Disable
 - Enable
-  Software channel permissions
 - High safety
 - Low safety (not secure)
 - Medium safety (recommended)
-  Submit non-encrypted form data
 - Disable
 - Enable
 - Prompt
-  Use Phishing Filter
 - Disable
 - Enable
-  Use Pop-up Blocker
 - Disable
 - Enable
-  Userdata persistence
 - Disable
 - Enable
-  Websites in less privileged web content zone can navigate in
 - Disable
 - Enable
 - Prompt

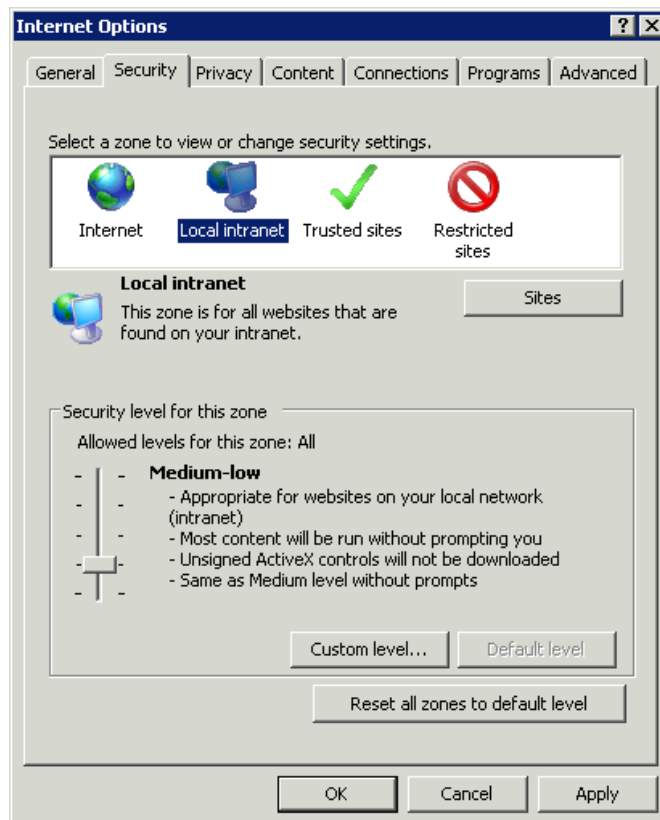
“Internet” Web Content Zone Default Values

-  Scripting
 -  Active scripting
 - Disable
 - Enable
 - Prompt
 -  Allow Programmatic clipboard access
 - Disable
 - Enable
 - Prompt
 -  Allow status bar updates via script
 - Disable
 - Enable
 -  Allow websites to prompt for information using scripted wind
 - Disable
 - Enable

-  Scripting of Java applets
 - Disable
 - Enable
 - Prompt












-  User Authentication
 -  Logon
 - Anonymous logon
 - Automatic logon only in Intranet zone
 - Automatic logon with current user name and password
 - Prompt for user name and password

“LOCAL INTRANET” WEB CONTENT ZONE DEFAULT VALUES










- .NET Framework
 - Loose XAML
 - Disable
 - Enable
 - Prompt
 - XAML browser applications
 - Disable
 - Enable
 - Prompt
 - XPS documents
 - Disable
 - Enable
 - Prompt


“LOCAL INTRANET” WEB CONTENT ZONE DEFAULT VALUES






-  .NET Framework-reliant components
 -  Run components not signed with Authenticode
 - Disable
 - Enable
 - Prompt
 -  Run components signed with Authenticode
 - Disable
 - Enable
 - Prompt
-  ActiveX controls and plug-ins
 -  Allow previously unused ActiveX controls to run without prompt
 - Disable
 - Enable
 -  Allow Scriptlets
 - Disable
 - Enable
 - Prompt
 -  Automatic prompting for ActiveX controls
 - Disable
 - Enable
-  Binary and script behaviors
 - Administrator approved
 - Disable
 - Enable
-  Display video and animation on a webpage that does not use ActiveX
 - Disable
 - Enable
-  Download signed ActiveX controls
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Download unsigned ActiveX controls
 - Disable (recommended)
 - Enable (not secure)
 - Prompt

“LOCAL INTRANET” WEB CONTENT ZONE DEFAULT VALUES





-  Initialize and script ActiveX controls not marked as safe for script execution
 - Disable (recommended)
 - Enable (not secure)
 - Prompt
-  Run ActiveX controls and plug-ins
 - Administrator approved
 - Disable
 - Enable
 - Prompt
-  Script ActiveX controls marked safe for scripting*
 - Disable
 - Enable
 - Prompt





-  Downloads
 -  Automatic prompting for file downloads
 - Disable
 - Enable
 -  File download
 - Disable
 - Enable
 -  Font download
 - Disable
 - Enable
 - Prompt





-  Enable .NET Framework setup
 - Disable
 - Enable

-  Miscellaneous
 -  Access data sources across domains
 - Disable
 - Enable
 - Prompt
 -  Allow META REFRESH
 - Disable
 - Enable
 -  Allow scripting of Internet Explorer web browser control
 - Disable
 - Enable
 -  Allow script-initiated windows without size or position constraints
 - Disable
 - Enable

“LOCAL INTRANET” WEB CONTENT ZONE DEFAULT VALUES

-  Allow webpages to use restricted protocols for active content
 - Disable
 - Enable
 - Prompt
-  Allow websites to open windows without address or status bar
 - Disable
 - Enable
-  Display mixed content
 - Disable
 - Enable
 - Prompt
-  Don't prompt for client certificate selection when no certificate is available
 - Disable
 - Enable

-  Drag and drop or copy and paste files
 - Disable
 - Enable
 - Prompt
-  Include local directory path when uploading files to a server
 - Disable
 - Enable
-  Installation of desktop items
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Launching applications and unsafe files
 - Disable
 - Enable (not secure)
 - Prompt (recommended)

-  Launching programs and files in an IFRAME
 - Disable
 - Enable (not secure)
 - Prompt (recommended)
-  Navigate sub-frames across different domains
 - Disable
 - Enable
 - Prompt
-  Open files based on content, not file extension
 - Disable
 - Enable
-  Software channel permissions
 - High safety
 - Low safety (not secure)
 - Medium safety (recommended)

“LOCAL INTRANET” WEB CONTENT ZONE DEFAULT VALUES

 Submit non-encrypted form data

- Disable
- Enable
- Prompt

 Use Phishing Filter

- Disable
- Enable

 Use Pop-up Blocker

- Disable
- Enable


 Userdata persistence

- Disable
- Enable

 Websites in less privileged web content zone can navigate into

- Disable
- Enable
- Prompt

 Scripting

 Active scripting


- Disable
- Enable
- Prompt

 Allow Programmatic clipboard access


- Disable
- Enable
- Prompt

 Allow status bar updates via script


- Disable
- Enable

 Allow websites to prompt for information using scripted windows

- Disable
- Enable

 Scripting of Java applets

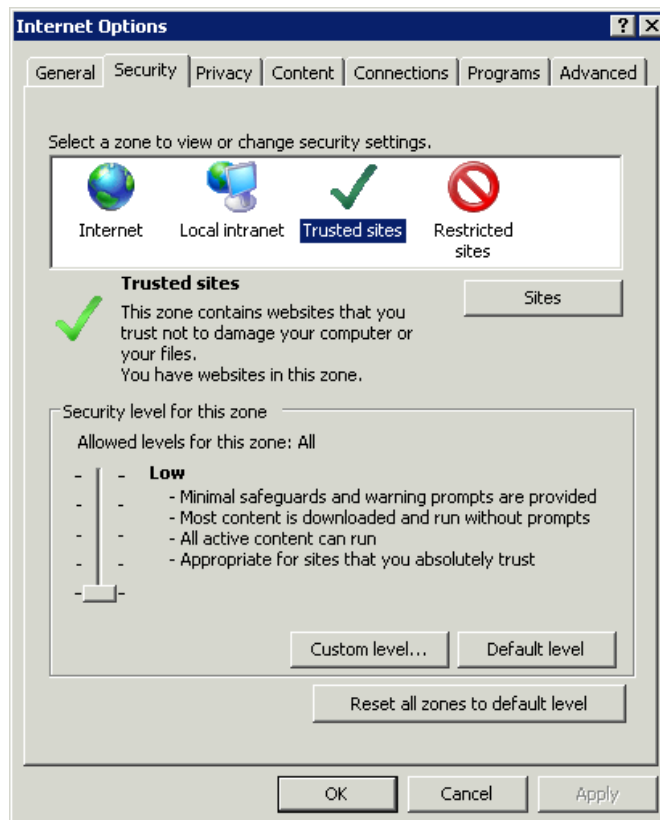
- Disable
- Enable
- Prompt

 User Authentication

 Logon






- Anonymous logon
- Automatic logon only in Intranet zone
- Automatic logon with current user name and password
- Prompt for user name and password





“TRUSTED SITES” WEB CONTENT ZONE DEFAULT VALUES





- .NET Framework
 - Loose XAML
 - Disable
 - Enable
 - Prompt
 - XAML browser applications
 - Disable
 - Enable
 - Prompt
 - XPS documents
 - Disable
 - Enable
 - Prompt















“TRUSTED SITES” WEB CONTENT ZONE DEFAULT VALUES

-  ActiveX controls and plug-ins
 -  Allow previously unused ActiveX controls to run without prompt
 - Disable
 - Enable
 -  Allow Scriptlets
 - Disable
 - Enable
 - Prompt
 -  Automatic prompting for ActiveX controls
 - Disable
 - Enable
 -  Binary and script behaviors
 - Administrator approved
 - Disable
 - Enable













-  Display video and animation on a webpage that does not use
 - Disable
 - Enable
-  Download signed ActiveX controls
 - Disable
 - Enable
 - Prompt
-  Download unsigned ActiveX controls
 - Disable
 - Enable
 - Prompt
-  Initialize and script ActiveX controls not marked as safe for script
 - Disable
 - Enable
 - Prompt

-  Run ActiveX controls and plug-ins
 - Administrator approved
 - Disable
 - Enable
 - Prompt
-  Script ActiveX controls marked safe for scripting*
 - Disable
 - Enable
 - Prompt


“TRUSTED SITES” WEB CONTENT ZONE DEFAULT VALUES

-  Downloads
 -  Automatic prompting for file downloads
 - Disable
 - Enable
 -  File download
 - Disable
 - Enable
 -  Font download
 - Disable
 - Enable
 - Prompt
-  Enable .NET Framework setup
 - Disable
 - Enable
-  Miscellaneous
 -  Access data sources across domains
 - Disable
 - Enable
 - Prompt
 -  Allow META REFRESH
 - Disable
 - Enable
 -  Allow scripting of Internet Explorer web browser control
 - Disable
 - Enable
 -  Allow script-initiated windows without size or position constraints
 - Disable
 - Enable
 -  Allow webpages to use restricted protocols for active content
 - Disable
 - Enable
 - Prompt
 -  Allow websites to open windows without address or status bar
 - Disable
 - Enable
 -  Display mixed content
 - Disable
 - Enable
 - Prompt
 -  Don't prompt for client certificate selection when no certificate is available
 - Disable
 - Enable


“TRUSTED SITES” WEB CONTENT ZONE DEFAULT VALUES


-  Drag and drop or copy and paste files
 - Disable
 - Enable
 - Prompt
-  Include local directory path when uploading files to a server
 - Disable
 - Enable
-  Installation of desktop items
 - Disable
 - Enable
 - Prompt
-  Launching applications and unsafe files
 - Disable
 - Enable
 - Prompt
-  Launching programs and files in an IFRAME
 - Disable
 - Enable
 - Prompt
-  Navigate sub-frames across different domains
 - Disable
 - Enable
 - Prompt
-  Open files based on content, not file extension
 - Disable
 - Enable
-  Software channel permissions
 - High safety
 - Low safety
 - Medium safety
-  Submit non-encrypted form data
 - Disable
 - Enable
 - Prompt
-  Use Phishing Filter
 - Disable
 - Enable
-  Use Pop-up Blocker
 - Disable
 - Enable
-  Userdata persistence
 - Disable
 - Enable


“TRUSTED SITES” WEB CONTENT ZONE DEFAULT VALUES


-  Websites in less privileged web content zone can navigate in
 - Disable
 - Enable
 - Prompt


Scripting

-  Active scripting
 - Disable
 - Enable
 - Prompt


-  Allow Programmatic clipboard access
 - Disable
 - Enable
 - Prompt

-  Allow status bar updates via script
 - Disable
 - Enable

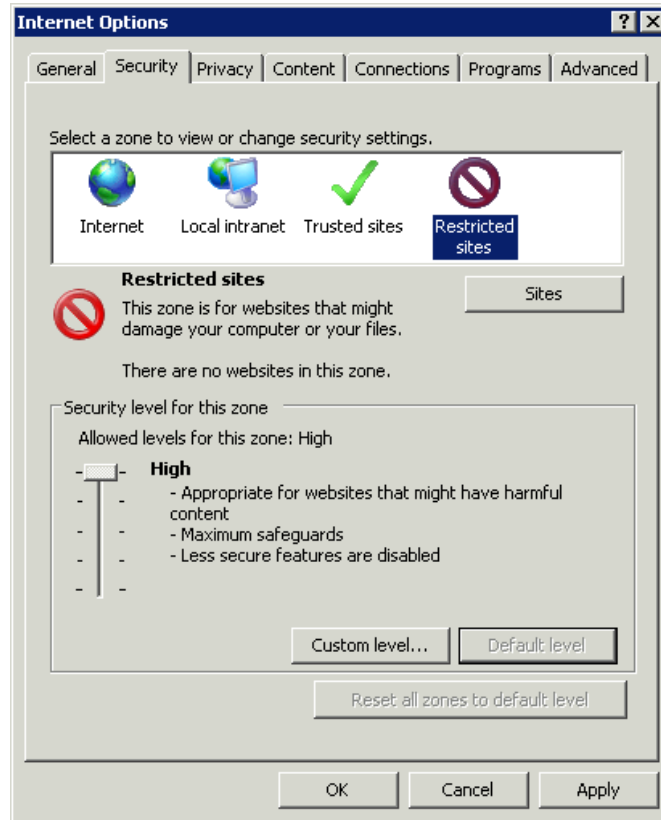
-  Allow websites to prompt for information using scripted windows
 - Disable
 - Enable

-  Scripting of Java applets
 - Disable
 - Enable
 - Prompt

User Authentication




-  Logon
 - Anonymous logon
 - Automatic logon only in Intranet zone
 - Automatic logon with current user name and password
 - Prompt for user name and password






“RESTRICTED SITES” WEB CONTENT ZONE DEFAULT VALUES





- .NET Framework
 - Loose XAML
 - Disable
 - Enable
 - Prompt
 - XAML browser applications
 - Disable
 - Enable
 - Prompt
 - XPS documents
 - Disable
 - Enable
 - Prompt


“RESTRICTED SITES” WEB CONTENT ZONE DEFAULT VALUES


-  .NET Framework-reliant components
 -  Run components not signed with Authenticode
 - Disable
 - Enable
 - Prompt
 -  Run components signed with Authenticode
 - Disable
 - Enable
 - Prompt

-  ActiveX controls and plug-ins
 -  Allow previously unused ActiveX controls to run without prom
 - Disable
 - Enable
 -  Allow Scriptlets
 - Disable
 - Enable
 - Prompt
 -  Automatic prompting for ActiveX controls
 - Disable
 - Enable
 -  Binary and script behaviors
 - Administrator approved
 - Disable
 - Enable













-  Display video and animation on a webpage that does not use
 - Disable
 - Enable

-  Download signed ActiveX controls
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)





-  Download unsigned ActiveX controls
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)





-  Initialize and script ActiveX controls not marked as safe for s
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)





“RESTRICTED SITES” WEB CONTENT ZONE DEFAULT VALUES

-  Run ActiveX controls and plug-ins
 - Administrator approved
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)
-  Script ActiveX controls marked safe for scripting*
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)
-  Downloads
 -  Automatic prompting for file downloads
 - Disable
 - Enable
 -  File download
 - Disable (recommended)
 - Enable (not secure)
 -  Font download
 - Disable
 - Enable
 - Prompt
-  Enable .NET Framework setup
 - Disable
 - Enable
-  Miscellaneous
 -  Access data sources across domains
 - Disable
 - Enable
 - Prompt
 -  Allow META REFRESH
 - Disable
 - Enable
 -  Allow scripting of Internet Explorer web browser control
 - Disable
 - Enable
 -  Allow script-initiated windows without size or position constra
 - Disable
 - Enable





“RESTRICTED SITES” WEB CONTENT ZONE DEFAULT VALUES








-  Allow webpages to use restricted protocols for active content
 - Disable
 - Enable
 - Prompt
-  Allow websites to open windows without address or status bar
 - Disable
 - Enable
-  Display mixed content
 - Disable
 - Enable
 - Prompt
-  Don't prompt for client certificate selection when no certificate is available
 - Disable
 - Enable



-  Drag and drop or copy and paste files
 - Disable
 - Enable
 - Prompt
-  Include local directory path when uploading files to a server
 - Disable
 - Enable
-  Installation of desktop items
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)
-  Launching applications and unsafe files
 - Disable
 - Enable (not secure)
 - Prompt (recommended)

-  Launching programs and files in an IFRAME
 - Disable (recommended)
 - Enable (not secure)
 - Prompt (not secure)
-  Navigate sub-frames across different domains
 - Disable
 - Enable
 - Prompt
-  Open files based on content, not file extension
 - Disable
 - Enable
-  Software channel permissions
 - High safety (recommended)
 - Low safety (not secure)
 - Medium safety (not secure)

“RESTRICTED SITES” WEB CONTENT ZONE DEFAULT VALUES

-  Submit non-encrypted form data
 - Disable
 - Enable
 - Prompt
-  Use Phishing Filter
 - Disable
 - Enable
-  Use Pop-up Blocker
 - Disable
 - Enable
-  Userdata persistence
 - Disable
 - Enable

-  Websites in less privileged web content zone can navigate in
 - Disable
 - Enable
 - Prompt
-  Scripting
 -  Active scripting
 - Disable
 - Enable
 - Prompt
 -  Allow Programmatic clipboard access
 - Disable
 - Enable
 - Prompt
 -  Allow status bar updates via script
 - Disable
 - Enable
 -  Allow websites to prompt for information using scripted windc
 - Disable
 - Enable
 -  Scripting of Java applets
 - Disable
 - Enable
 - Prompt

-  User Authentication
 -  Logon
 - Anonymous logon
 - Automatic logon only in Intranet zone
 - Automatic logon with current user name and password
 - Prompt for user name and password