



# **Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide**

**For Unified Contact Center Enterprise**

Release 9.0(2)  
September 2014

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <http://www.cisco.com/go/trademarks>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

*Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide: For Unified Contact Center Enterprise. September 5, 2014*

Copyright © 2006–2014, Cisco Systems, Inc. All rights reserved.

# Contents

- About This Guide ..... 4
- Configuring Your Browser ..... 4
  - Configuring Internet Explorer 9 or Internet Explorer 10 ..... 5
  - Configuring Internet Explorer 8 ..... 14
  - Configuring Pop-Up Blockers..... 23
- Configuring Java on Your Desktop ..... 23
- Configuring MeadCo’s Security Manager ..... 25
  - Enabling the Automatic Download of ActiveX Controls ..... 25
  - Installing MeadCo’s Security Manager..... 26
- Logging In..... 26

Welcome to Cisco® Interaction Manager™, multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A unified suite of the industry’s best applications for web and email interaction management, it is the backbone of many innovative contact center and customer service helpdesk organizations.

Cisco Interaction Manager includes a common platform and one or both of the following applications:

- ▶ Cisco Unified Web Interaction Manager (Unified WIM)
- ▶ Cisco Unified E-Mail Interaction Manager (Unified EIM)

## About This Guide

---

*Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide* helps you set up your web browser, and Java for Unified WIM and Unified EIM. Users must configure their desktops according to the procedures described in this guide before logging in to the system.

### Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis, or the title of a published document.
<b>Bold</b>	Labels of items on the user interface, such as buttons, boxes, and lists. Or, text that must be typed by the user.
<code>Monospace</code>	A file name or command. Or, text that must be typed by the user.
<i>Variable</i>	User-specific text, provided by the user.

*Document conventions*

## Configuring Your Browser

---

You can use a 32-bit or 64-bit version of Internet Explorer to access the Unified WIM and Unified EIM application. Note that the MeadCo’s Security Manager ([page 25](#)), a browser add-on used to enable the advanced page-pushing feature in Unified WIM, is available only on 32-bit version of Internet Explorer. If you plan to use the MeadCo capabilities, you must use the 32-bit version of the browser.

This section describes the procedures for configuring the web browser. It includes:

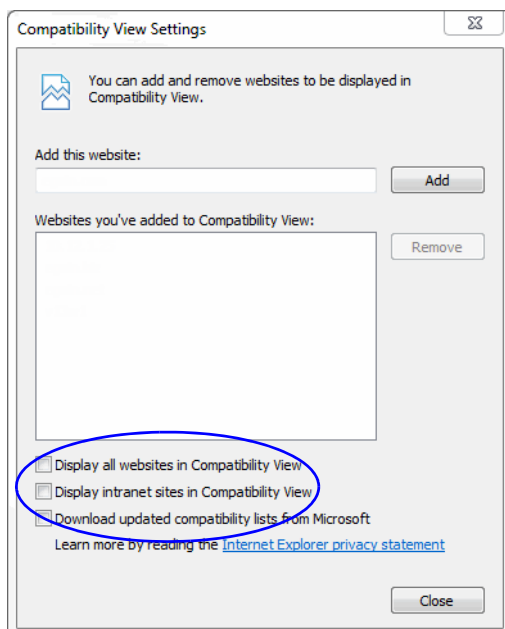
- ▶ [“Configuring Internet Explorer 9 or Internet Explorer 10” on page 5](#)
- ▶ [“Configuring Internet Explorer 8” on page 14](#)
- ▶ [“Configuring Pop-Up Blockers” on page 23](#)

## Configuring Internet Explorer 9 or Internet Explorer 10

The screens used in this section are from Internet Explorer 10. The screens you will see for Internet Explorer 9 may be slightly different.

### To configure your browser for Unified WIM and Unified EIM:

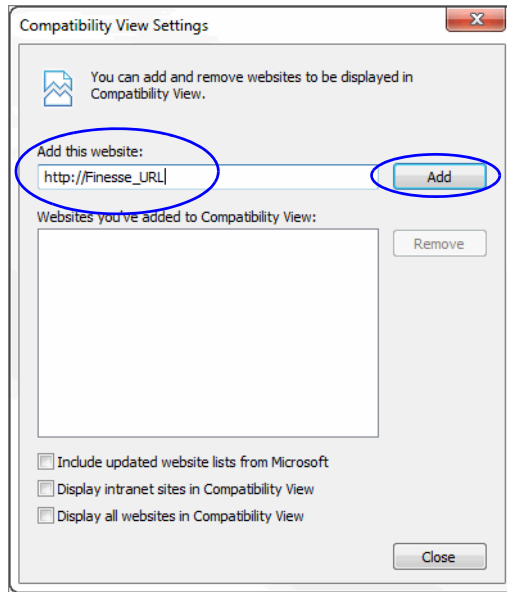
1. Open Internet Explorer.
2. On the Internet Explorer toolbar, click the **Help** button and select **About Internet Explorer**.
3. In the About Internet Explorer window, verify that the version number is **9.0.x** or **10.0.x**. If you need to get the correct version, download it from the Microsoft web site.
4. On the Internet Explorer toolbar, click the **Tools** button and select **Compatibility View Settings**.
5. In the Compatibility View Settings window that appears, do the following:
  - a. Uncheck the following options to turn off the compatibility view mode.
    - Display all websites in Compatibility View
    - Display intranet sites in Compatibility View
    - Download updated compatibility lists from Microsoft (In Internet Explorer 9, this options is called Include updated website lists from Microsoft)



*Turn off the compatibility view settings*

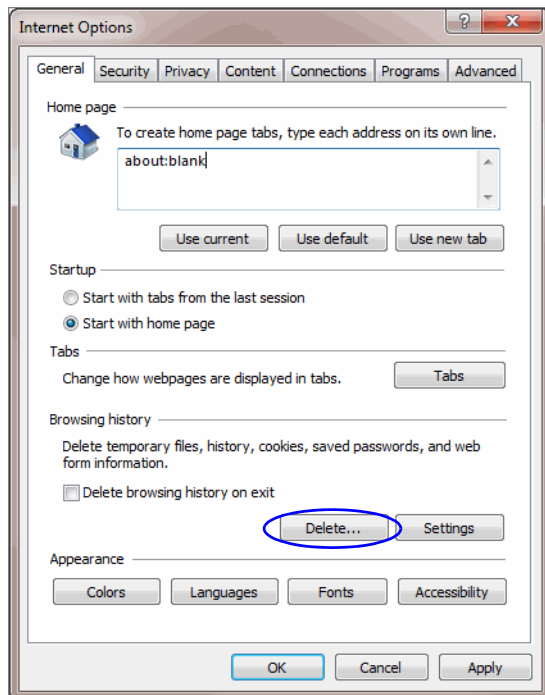
- b. If you have embedded the Unified EIM and WIM application in Finesse, and you are using Finesse 10.0(1) SU1 ES1 or Finesse 10.5(1) ES1, you need to enable the compatibility mode setting for accessing Finesse.

- In the **Add this website** field provide the Finesse URL and click the **Add** button.



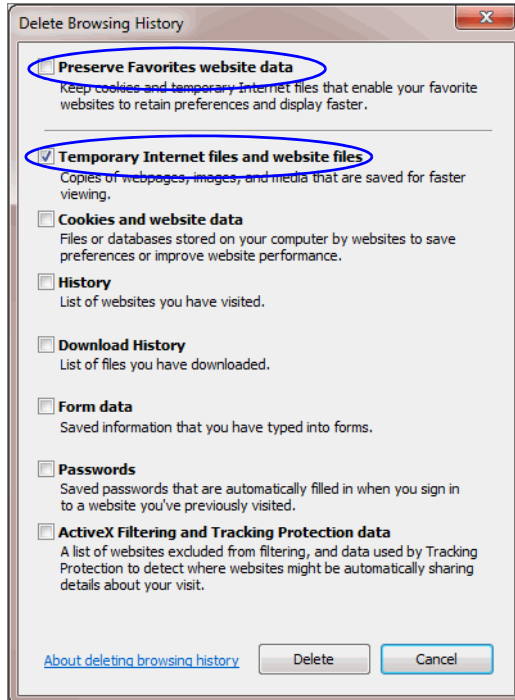
*Add the Finesse URL to compatibility view settings*

6. On the Internet Explorer toolbar, click the **Tools** button and select **Internet Options**.  
The Internet Options window appears.
7. On the General tab, do the following:
  - a. In the Browsing history section, click the **Delete** button.



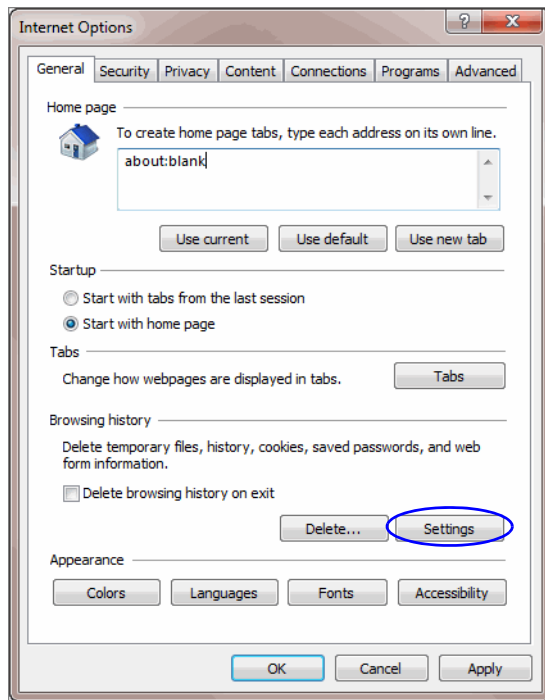
*Click the **Delete** button*

- b. In the Delete Browsing History window, do the following:
- i. Uncheck the **Preserve Favorites website data** option.
  - ii. Select the **Temporary Internet files and Website files** option and click the **Delete** button. In Internet Explorer 9, this options is called **Temporary Internet Files**.



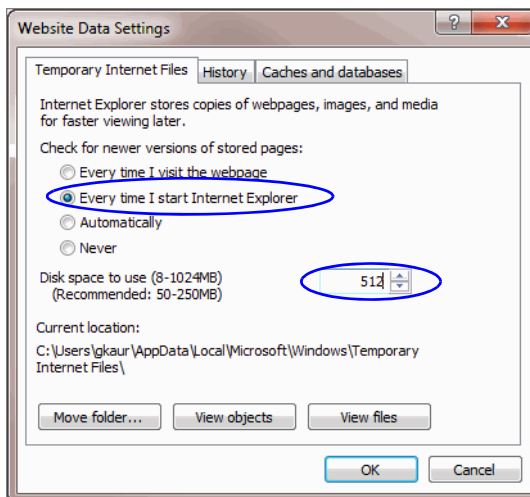
*Delete temporary internet files*

- c. In the Browsing history section, click the **Settings** button.



Click the **Settings** button

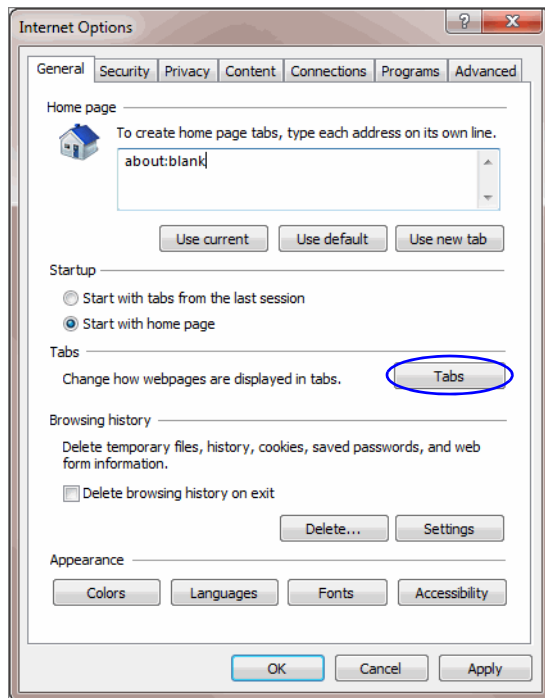
- d. In the Settings window, in the Temporary Internet files section, set the following options and click **OK**.
- Select **Every time I start Internet Explorer** as the option for checking newer versions of stored pages.
  - Specify at least 512 MB as the disk space to use for temporary internet files.



Configure temporary internet file settings

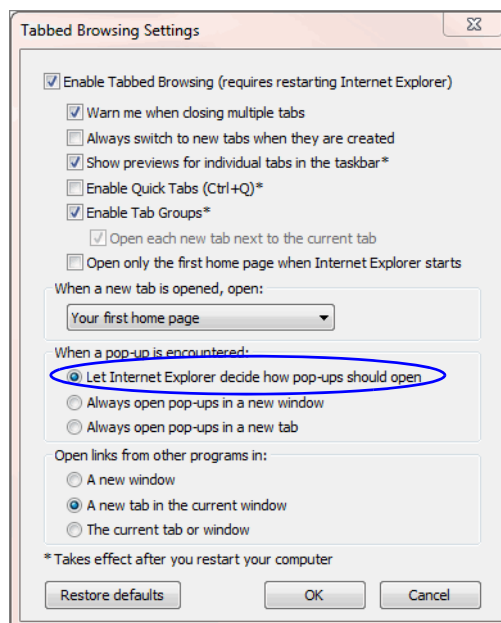


- e. In the Tabs section, click the **Tabs** button. In Internet Explorer 9, this button is called **Settings**.



Click the *Settings* button

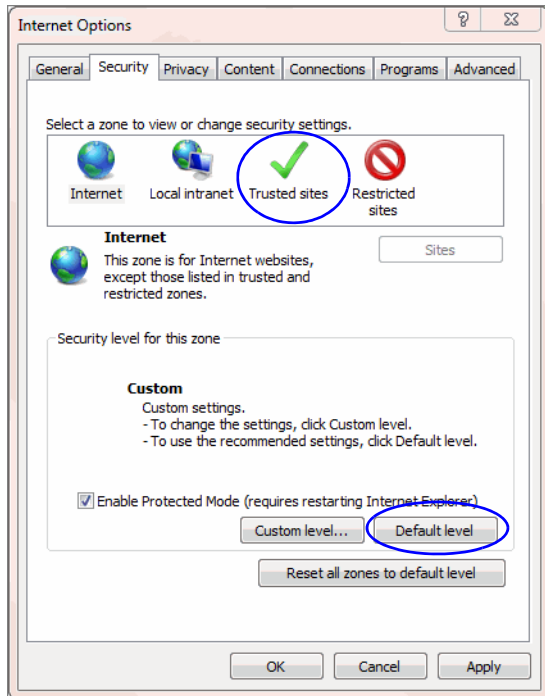
- f. In the Settings window, in the When a pop up is encountered: section, select the **Let Internet Explorer decide how pop-ups should open** option and click OK.



Configure the *When a pop up is encountered:* setting

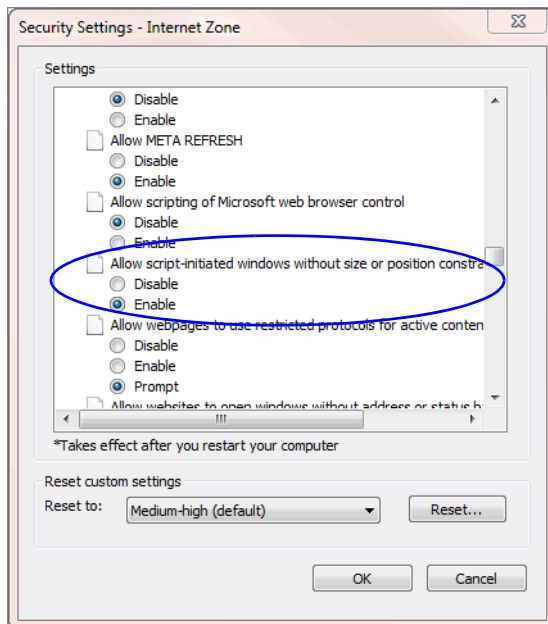
8. On the Security tab, perform the following tasks:
- Select the **Trusted sites** zone, and restore default settings by clicking the **Default level** button.

If the **Default level** button is disabled, then default settings are already in use.



*Configure trusted sites settings*

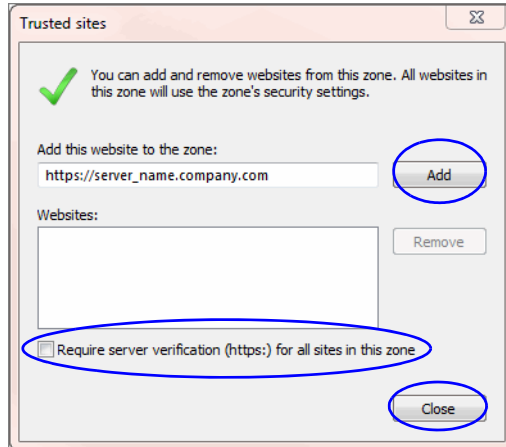
- b. Next, select the **Trusted sites** zone, and click the **Custom level** button.
- c. In the Security Settings window, enable the following settings:
  - In the Miscellaneous section, enable the **Allow script-initiated windows without size or position constraints** setting.



*Enable the Allow script-initiated windows without size or position constraints setting*

If you plan to use MeadCo for Unified WIM, you need to configure some additional settings. For details, see “[Configuring MeadCo’s Security Manager](#)” on page 25.

- d. Then, select the **Trusted sites** zone and click the **Sites** button.
- e. In the Trusted sites window, perform the following tasks:
  - i. Clear the **Require server verification (https:) for all sites in this zone** option.
  - ii. In the **Add this website to the zone** text box, type the Internet address for the application and click the **Add** button. Click **Close**.



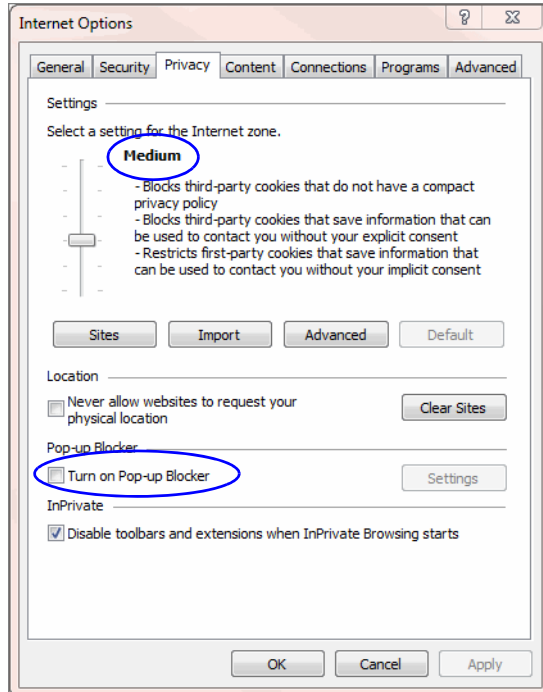
*Add the URL for the application to the trusted web sites list*

9. On the Privacy tab, perform the following tasks:
  - a. In the Settings section, set the Cookies setting to **Medium**.

- b. In the Pop-up Blocker section, clear the **Turn on Pop-up Blocker** option.

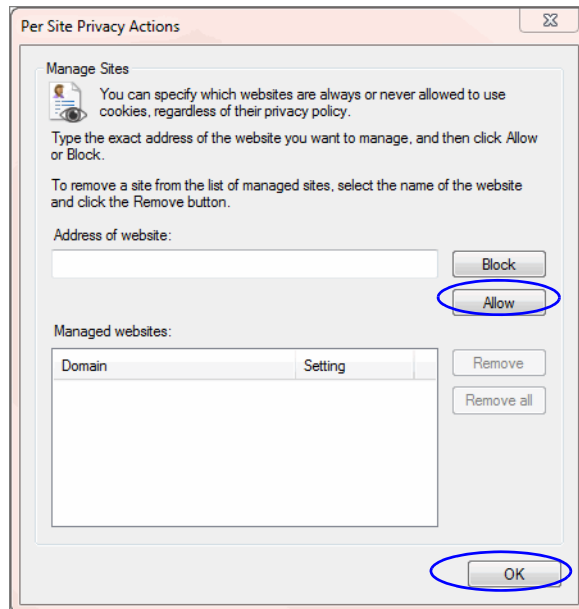


**Important:** If you use additional pop-up blockers, you must configure them to allow pop-up windows for the Unified WIM and Unified EIM URL (see [“Configuring Pop-Up Blockers”](#) on page 23).



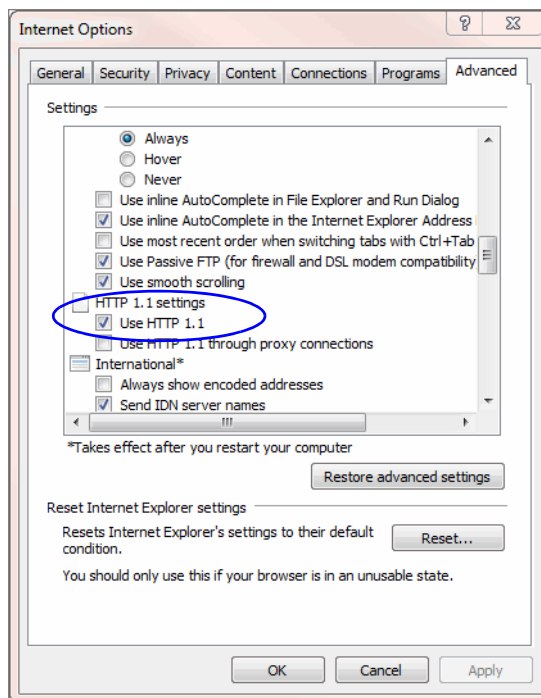
*Configure pop-up blocker setting*

- c. Skip this step if you have not embedded the Unified EIM and WIM application in Finesse. If you are using Finesse, in the Settings section, click the **Sites** button.
- In the Per Site Privacy Actions window, in the **Address of website** field, enter the fully qualified hostname of the Unified EIM and WIM web server and click **Allow**.
  - Now enter the Finesse hostname and click **Allow**. Click **OK** to close this window.



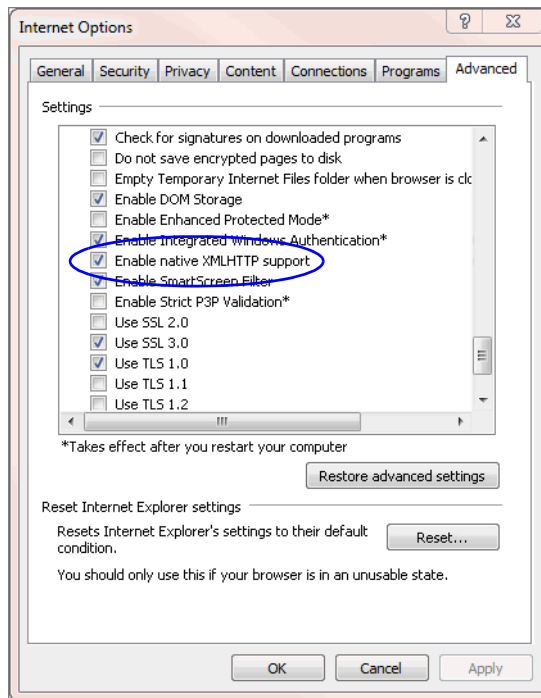
*Manage per site privacy actions*

10. On the Advanced tab, perform the following tasks:
  - a. In the HTTP 1.1 Settings section, ensure that the **Use HTTP 1.1** option is selected. If you cannot use HTTP 1.1 on your desktop, IIS compression settings must be modified on the web server. Contact your system administrator for help.



*Verify HTTP 1.1 setting*

- b. In the Security section, ensure that the **Enable Native xmlHTTP** support option is selected.



*Verify the Native xmlHTTP support setting*

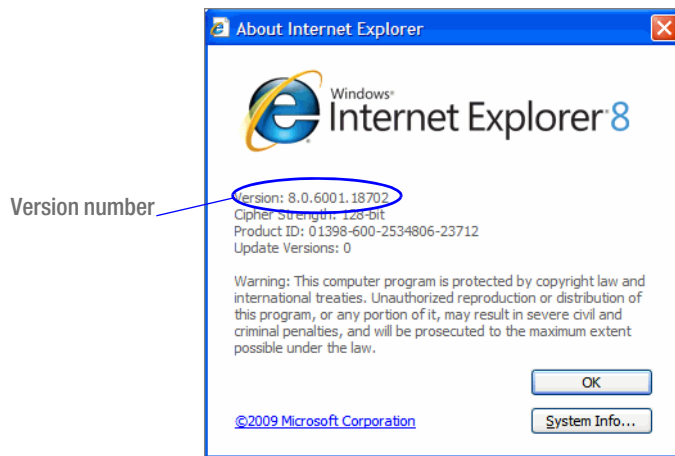
11. Click **OK** in the Internet Options window to close it.

## Configuring Internet Explorer 8

### To configure your browser for Unified WIM and Unified EIM:

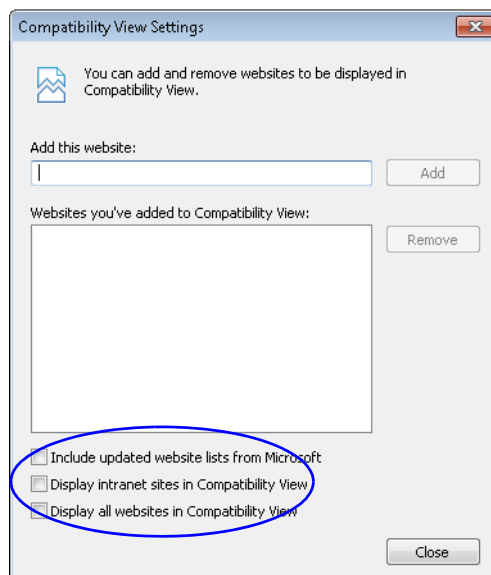
1. Open Internet Explorer.
2. On the Internet Explorer toolbar, click the **Help** button and select **About Internet Explorer**.

3. In the About Internet Explorer window, verify that the version number is **8.0.x**. If you need to get the correct version, download it from the Microsoft web site.



*Verify browser version*

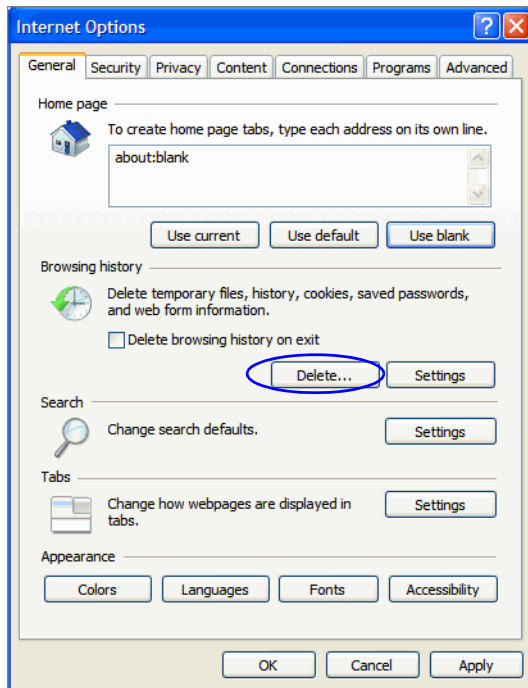
4. On the Internet Explorer toolbar, click the **Tools** button and select **Compatibility View Settings**.
5. In the Compatibility View Settings window that appears, uncheck the following options to turn off the compatibility view mode.
  - Include updated website lists from Microsoft
  - Display intranet sites in Compatibility View
  - Display all websites in Compatibility View



*Turn off the compatibility view settings*

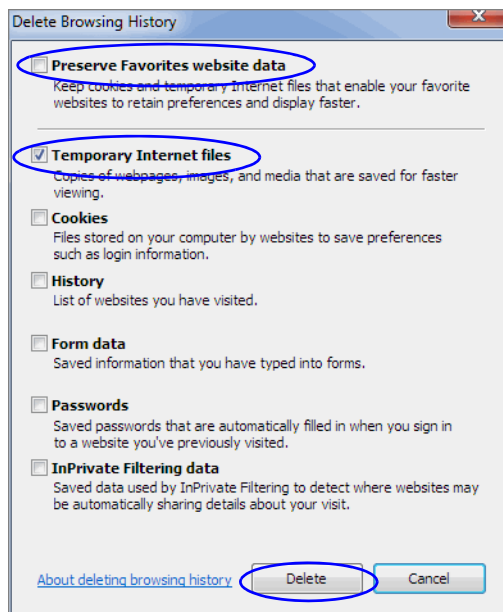
6. On the Internet Explorer toolbar, click the **Tools** button and select **Internet Options**.  
The Internet Options window appears.

7. On the General tab, do the following:
  - a. In the Browsing history section, click the **Delete** button.



Click the **Delete** button

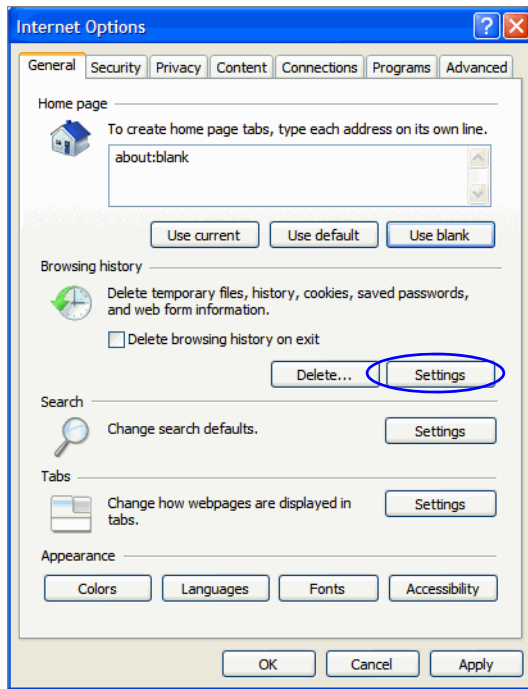
- b. In the Delete Browsing History window, do the following:
      - i. Uncheck the **Preserve Favorites Website Data** option.
      - ii. Select the **Temporary Internet Files** option and click the **Delete** button.



Delete temporary internet files

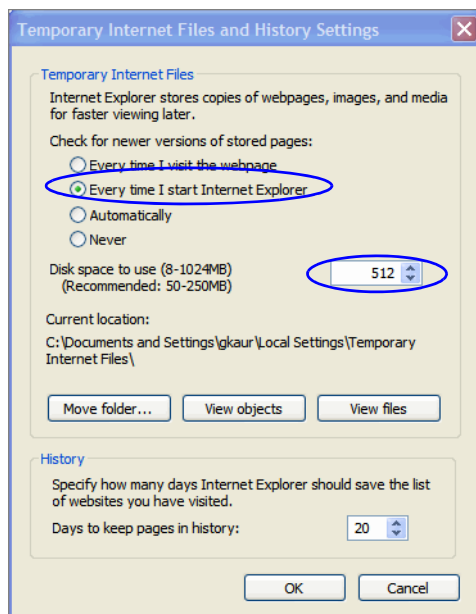


- c. In the Browsing history section, click the **Settings** button.



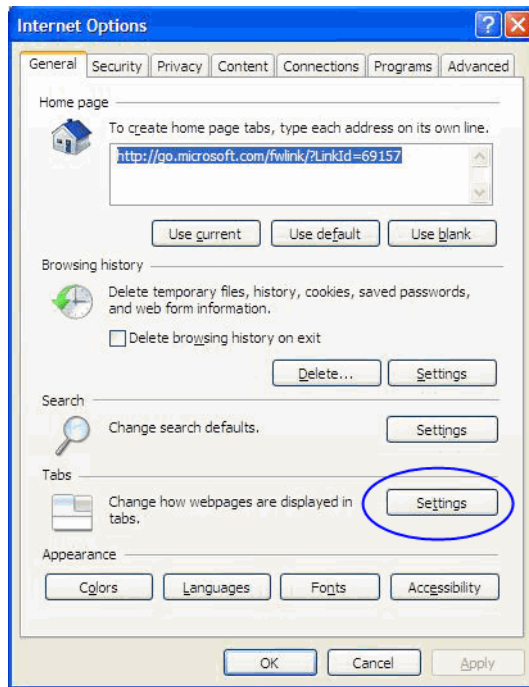
Click the **Settings** button

- d. In the Settings window, in the Temporary Internet files section, set the following options and click **OK**.
- Select **Every time I start Internet Explorer** as the option for checking newer versions of stored pages.
  - Specify at least 512 MB as the disk space to use for temporary internet files.



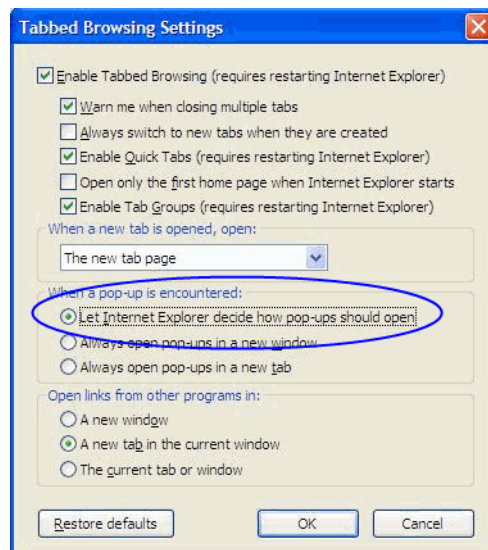
Configure temporary internet file settings

- e. In the Tabs section, click the **Settings** button.



Click the **Settings** button

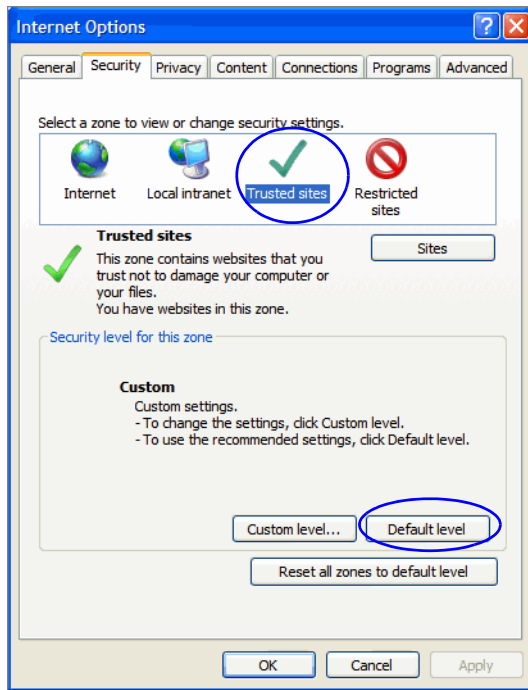
- f. In the Settings window, in the When a pop up is encountered: section, select the **Let Internet Explorer decide how pop-ups should open** option and click OK.



Configure the *When a pop up is encountered:* setting

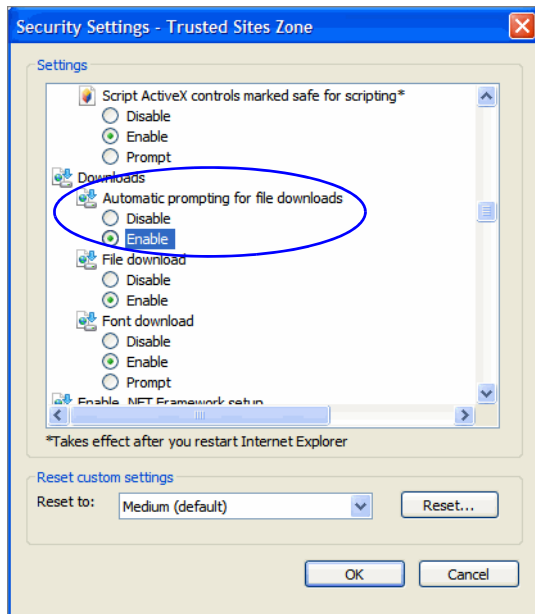
8. On the Security tab, perform the following tasks:
- Select the **Trusted sites** zone, and restore default settings by clicking the **Default level** button.

If the **Default level** button is disabled, then default settings are already in use.



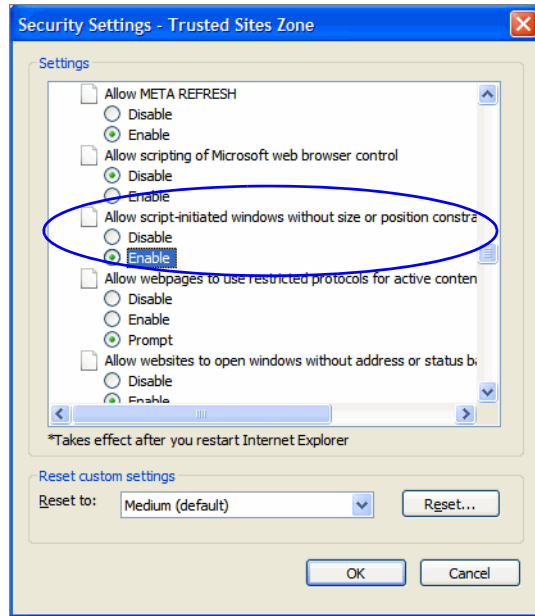
*Configure trusted sites settings*

- b. Next, select the **Trusted sites** zone, and click the **Custom level** button.
- c. In the Security Settings window, enable the following settings:
  - In the Downloads section, enable the **Automatic prompting for file downloads** setting.



*Enable the Automatic prompting for file downloads setting*

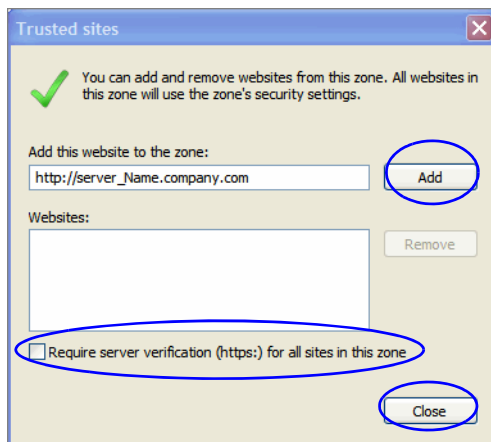
- In the Miscellaneous section, enable the **Allow script-initiated windows without size or position constraints** setting.



*Enable the Allow script-initiated windows without size or position constraints setting*

If you plan to use MeadCo for Unified WIM, you need to configure some additional settings. For details, see [“Configuring MeadCo’s Security Manager” on page 25](#).

- Then, select the **Trusted sites** zone and click the **Sites** button.
- In the Trusted sites window, perform the following tasks:
  - Clear the **Require server verification (https:) for all sites in this zone** option.
  - In the **Add this website to the zone** text box, type the Internet address for the application and click the **Add** button. Click **Close**.



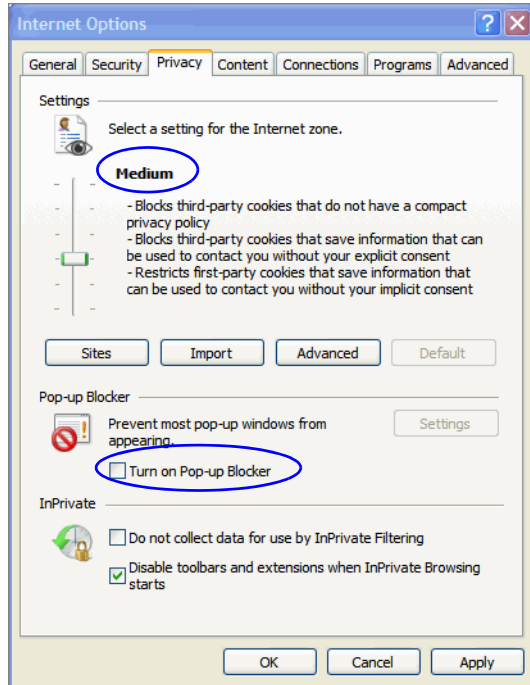
*Add the URL for the application to the trusted web sites list*

- On the Privacy tab, perform the following tasks:
  - In the Settings section, set the Cookies setting to **Medium**.

- b. In the Pop-up Blocker section, clear the **Turn on Pop-up Blocker** option.

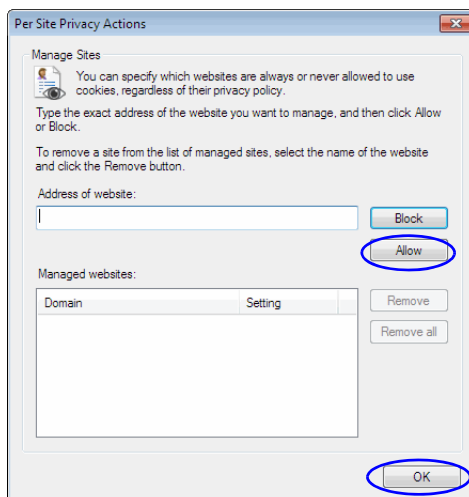


**Important:** If you use additional pop-up blockers, you must configure them to allow pop-up windows for the Unified WIM and Unified EIM URL (see “Configuring Pop-Up Blockers” on page 23).



*Configure pop-up blocker setting*

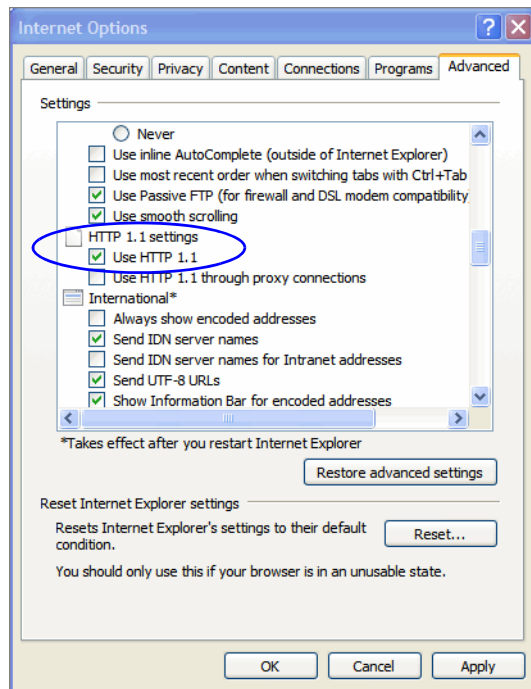
- c. Skip this step if you have not embedded the Unified EIM and WIM application in Finesse. If you are using Finesse, in the Settings section, click the **Sites** button.
- i. In the Per Site Privacy Actions window, in the **Address of website** field, enter the fully qualified hostname of the Unified EIM and WIM web server and click **Allow**.
  - ii. Now enter the Finesse hostname and click **Allow**. Click **OK** to close this window,



*Configure per site privacy actions*

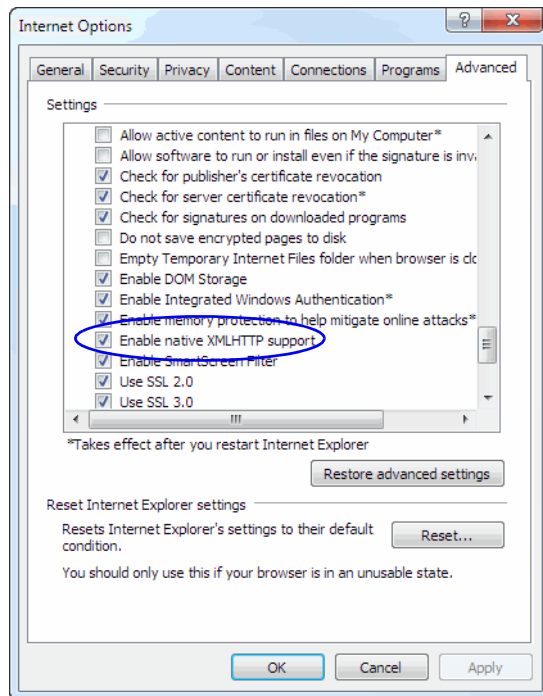
10. On the Advanced tab, set the following:

- a. In the HTTP 1.1 Settings section, ensure that the **Use HTTP 1.1** option is selected. If you cannot use HTTP 1.1 on your desktop, IIS compression settings must be modified on the web server. Contact your system administrator for help.



*Verify HTTP 1.1 setting*

- b. In the Security section, ensure that the **Enable Native xmlHTTP support** option is selected.



*Verify the Native XMLHttpRequest support setting*

11. Click **OK** in the Internet Options window to close it.

## Configuring Pop-Up Blockers

- ▶ If you use external pop-up blockers such as those available in the Google and Yahoo toolbars, configure them to allow pop-up windows for your Unified WIM and Unified EIM installation URL.

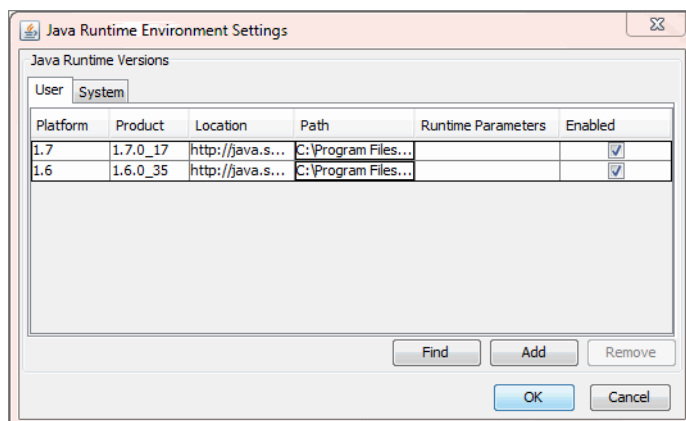
## Configuring Java on Your Desktop

From the user desktop, ensure that the Java 1.6 (Updates 30 to 43) or Java 1.7 (Updates 11 to 17) is being used. For 64-bit browser, you must have the 64-bit JRE enabled on your system. If you are using a 32-bit browser, you must have the 32-bit JRE (x86) enabled on your system. In 64-bit Operating Systems, the Java Control Panel does not display 32-bit versions of JRE. Follow the steps on [page 24](#) to ensure that you have the correct 32-bit JRE version.

### To configure Java on your desktop:

1. Close all open Internet Explorer browsers.
2. Go to **Start > Control Panel**.
3. Double-click **Java**.
4. In the Java Control Panel window, go to the Java tab and click the **View** button.

- In the Java Runtime Environment Settings window, verify that JRE 1.6 (Updates 30 to 43) or Java 1.7 (Updates 11 to 17) is enabled.

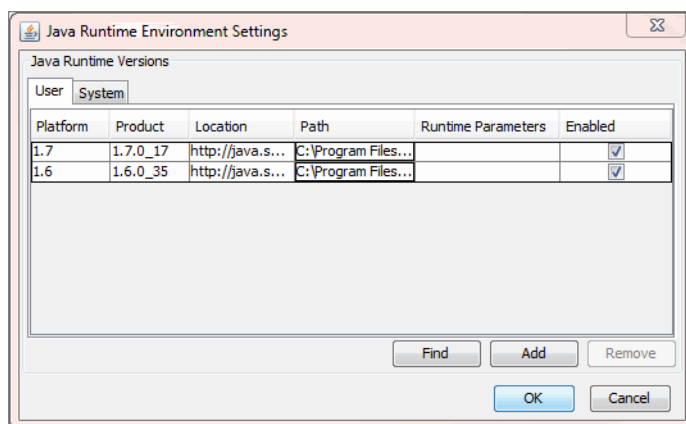


*Verify that the correct version of Java is enabled*

- Click **OK** to close the window.

### To configure Java on desktops that have 32-bit Internet Explorer browsers installed on 64-bit Operating Systems:

- Close all open Internet Explorer browsers.
- Go to **C:\Program Files (x86)\Java\jre6\bin** or **C:\Program Files (x86)\Java\jre7\bin**
- Double-click **javacpl.exe**.
- In the Java Control Panel window, go to the Java tab and click the **View** button.
- In the Java Runtime Settings window that opens, verify that JRE 1.6 (Updates 30 to 43) or Java 1.7 (Updates 11 to 17) is enabled.



*Verify that the correct version of Java is enabled*

- Click **OK** to close the window.



# Configuring MeadCo's Security Manager

MeadCo's Security Manager is required to enable the page-pushing feature in Unified WIM. Organizations that want to use this feature should set the **Chat - MeadCo download on Agent Console** department-level setting to **Enable** to ensure that users are prompted to download the control.

Users who are assigned Unified WIM licenses are asked to install this control when they first log in to the Agent Console.

Note that the MeadCo add-on works only on 32-bit version of Internet Explorer.

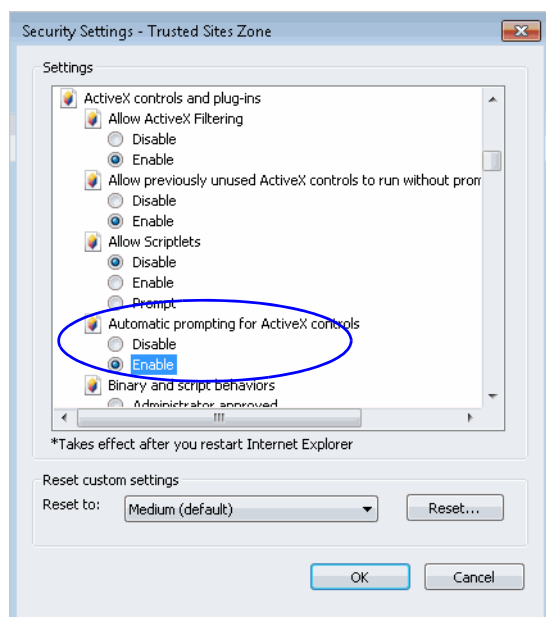


**Important:** Before installing MeadCo, you need to enable an ActiveX controls setting on user desktops.

## Enabling the Automatic Download of ActiveX Controls

### To enable the automatic download of ActiveX controls:

1. Open Internet Explorer.
2. On the Internet Explorer toolbar, click the **Tools** button and select **Internet Options**.
3. In the Internet Options window, on the Security tab, select the **Trusted sites** zone, and click the **Custom level** button.
4. In the Security Settings - Trusted Sites Zone window, in the ActiveX controls and plug-ins section, enable the **Automatic prompting for ActiveX controls** setting. Click **OK**.

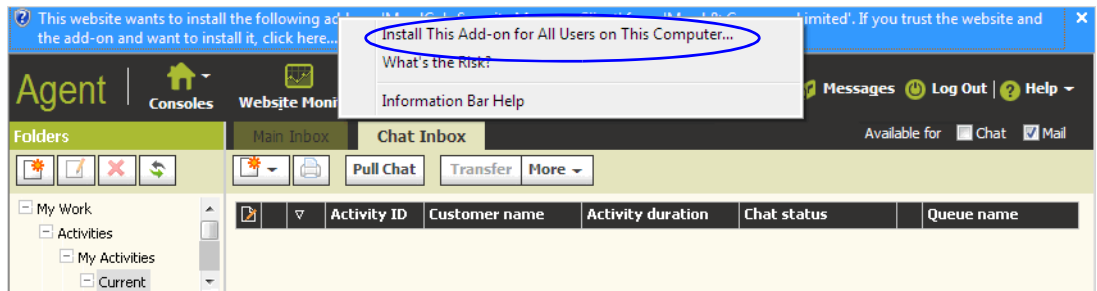


*Enable the automatic download of ActiveX controls*

# Installing MeadCo's Security Manager

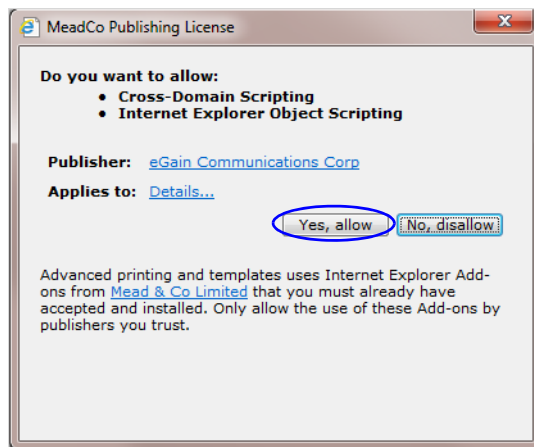
## To install MeadCo's Security Manager:

1. Log in to the Unified WIM and Unified EIM application. For details, see “Logging In” on page 26.
2. In the Consoles window, select **Agent** to go to the Agent Console.
3. If MeadCo's Security Manager is not installed, a related message appears near the title bar. Click the message and select **Install This Add-on for All Users on This Computer**. When you select this option, you are prompted to log out of the application.



Select the *Install ActiveX Control* option

4. Log out and log in again. Go to the Agent Console.
5. In the MeadCo Publishing License window, click the **Yes, allow** button to complete the installation.



Allow cross-domain and Internet Explorer object scripting

## Logging In

The application allows users to log in to the application using the same user account from different browser sessions and desktops. Designed to provide greater flexibility for authors and administrators, this feature is not

meant for use by agents. Users performing agent and supervision tasks from the Agent Console should not use the same user account more than once at the same time.

**To log in to the business partition from your browser window:**

1. Type the URL provided by your system administrator in the browser. The URL is typically in the following format: `http://Web_Server/Partition_Virtual_Directory` where *Web\_Server* is your web server and *Partition\_Virtual\_Directory* is the virtual directory created for the business partition.
2. In the Login window, type your user name and password.
3. Click the **Log In** button.