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

For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.2(5)
October 2008

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 UCB's 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

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.

Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide: For Unified Contact Center Enterprise and Hosted and Unified ICM
© 2008 Cisco Systems, Inc. All rights reserved.

Preparing your browser and desktop

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 Sun JVM 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.

Contents

This guide contains the following procedures:

Document conventions

This guide uses the following typographical conventions.

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

Document conventions

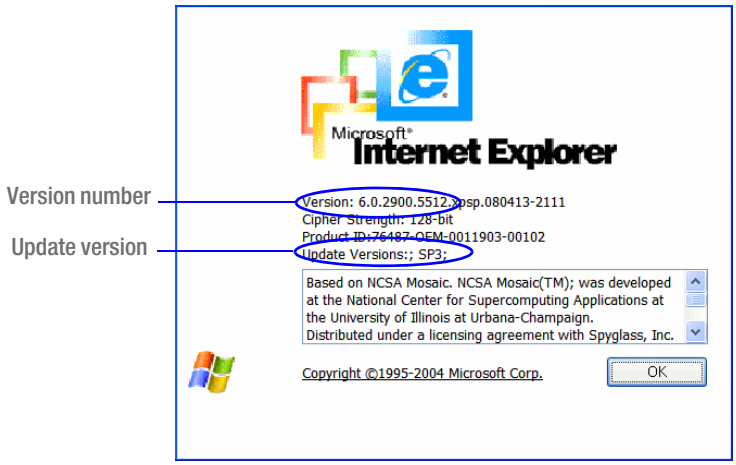
Configuring your browser

This section describes the procedures for configuring Internet Explorer 6 and Internet Explorer 7.

Configuring Internet Explorer 6

To configure your browser for Cisco Interaction Manager:

1. Open Internet Explorer.
2. Go to **Help** (menu) **> About Internet Explorer.**
3. In the About Internet Explorer window, verify that the version number is **6.0.x** with the update version is **SP3.** If you need to get the correct version, download it from the Microsoft web site.

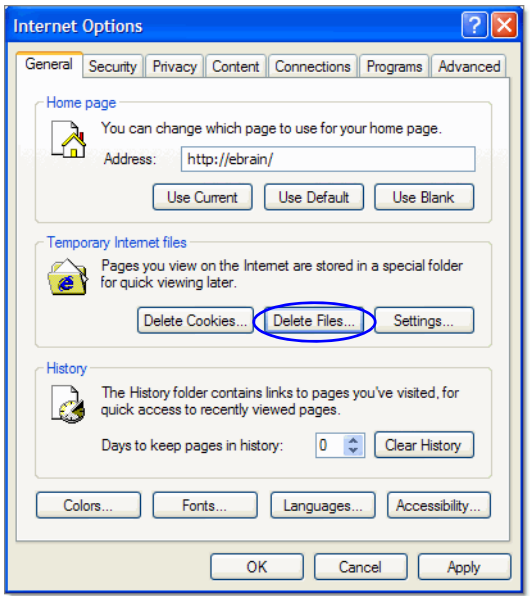


Verify browser version

4. Go to **Tools** (menu) **> Internet Options.**

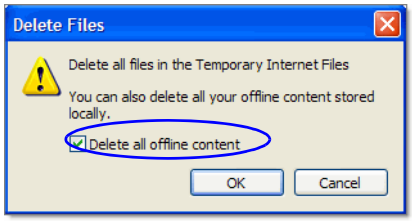
   The Internet Options window appears.
5. On the General tab, do the following:

a. In the Temporary Internet Files section, click the **Delete Files** button.



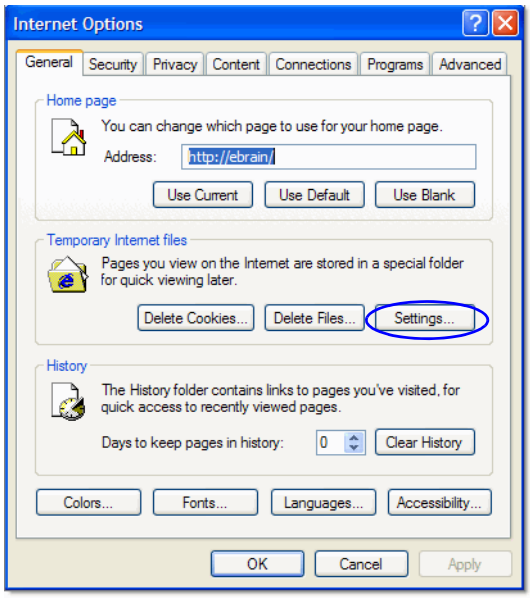
Delete temporary internet files

b. In the Delete Files window, select the **Delete all offline content** option, and click **OK.**



Delete the offline content stored locally

c. In the Temporary Internet Files section, click the **Settings** button.

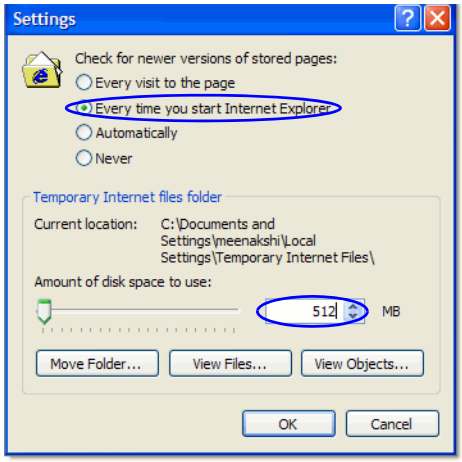


*Click the **Settings** button*

d. In the Settings window, set the following options and click **OK.**

i. Select **Every time you start Internet Explorer** as the option for checking newer versions of stored pages.

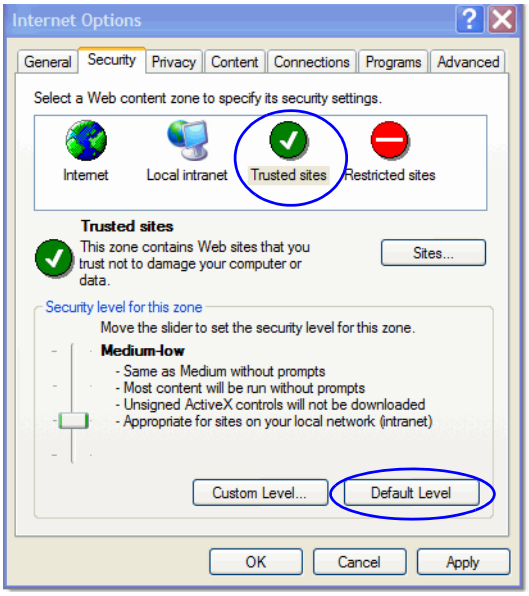
ii. In the Temporary Internet files folder section, specify at least 512 MB as the disk space to use.



Configure temporary internet file settings

6. On the Security tab, perform the following tasks:

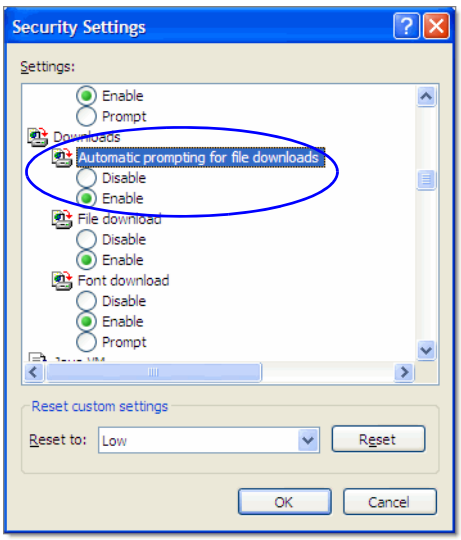
a. Select the **Trusted sites** zone, and restore default settings by clicking the **Default Level** button. If the **Default Level** button is disabled, then default settings are already in use.



Configure trusted sites settings

b. Next, select the **Trusted sites** zone, and click the **Custom level** button.

c. In the Security Settings window, in the Downloads section, enable the **Automatic prompting for file downloads** setting. Click **OK.**



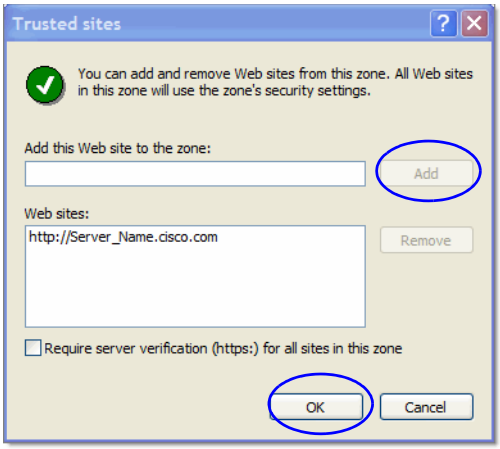
*Enable the **Automatic prompting for file downloads** setting*

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 (http:) for all sites in this zone** option.

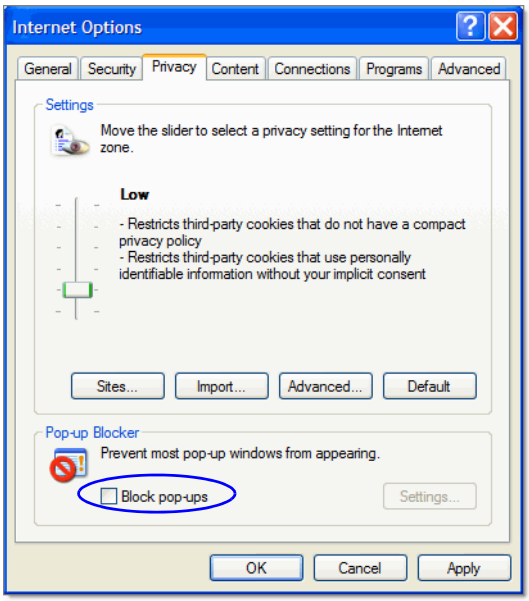
ii. In the **Add this Web site to the zone** text box, type the Internet address for the application and click the **Add** button. Click **OK.**



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

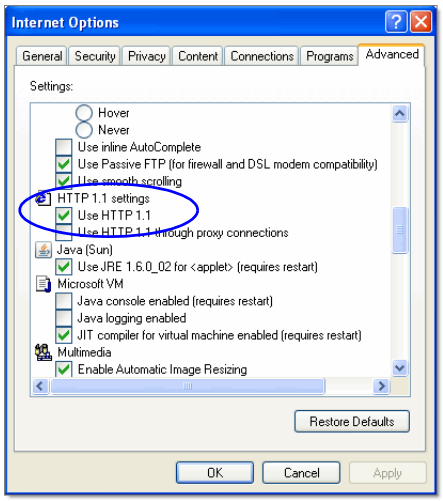
7. On the Privacy tab, in the Pop-up Blocker section, clear the **Block pop-ups** option.

> Important: **If you use additional pop-up blockers, you must configure them to allow pop-up windows at the Unified WIM and Unified EIMURL (see** "Configuring pop-up blockers" on page 16**).**



Configure pop-up blocker setting

8. On the Advanced tab, in the HTTP 1.1. Settings section, ensure that the Use HTTP 1.1 option is selected.



Verify HTTP 1.1 setting

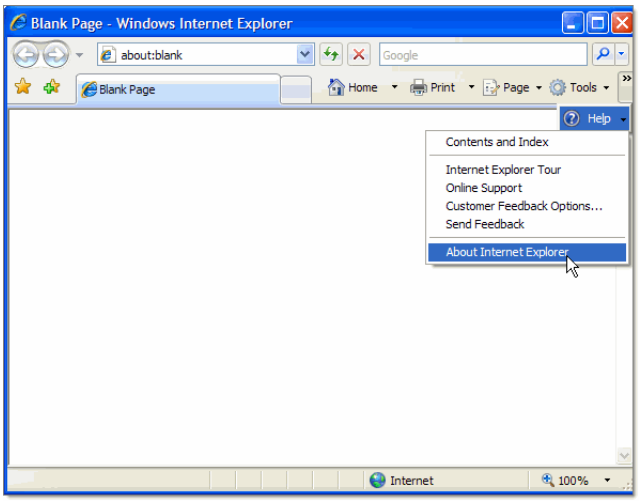
If you cannot use HTTP 1.1 on your desktop, IIS compression settings must be modified on the web server. Contact your system administrator for help.

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

Configuring Internet Explorer 7

To configure your browser for Cisco Interaction Manager:

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

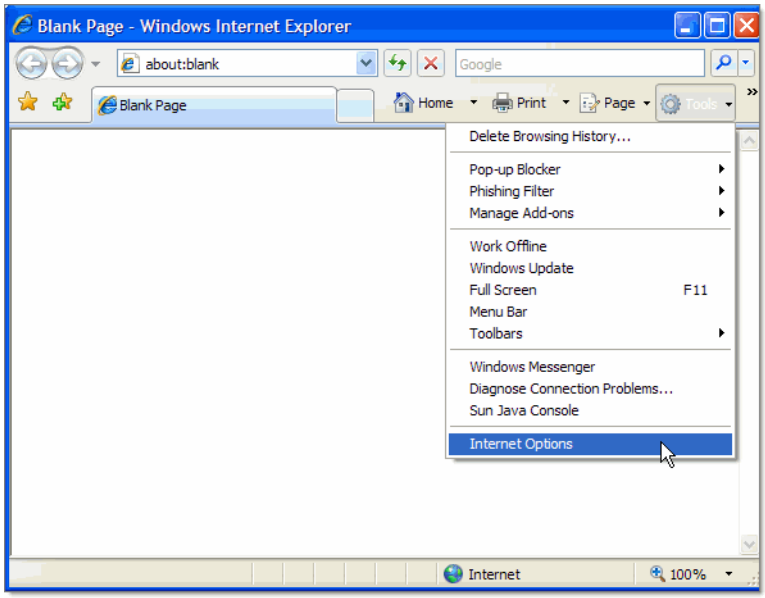


*Select **About Internet Explorer***

3. In the About Internet Explorer window, verify that the version number is **7.0.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 **Internet Options.**

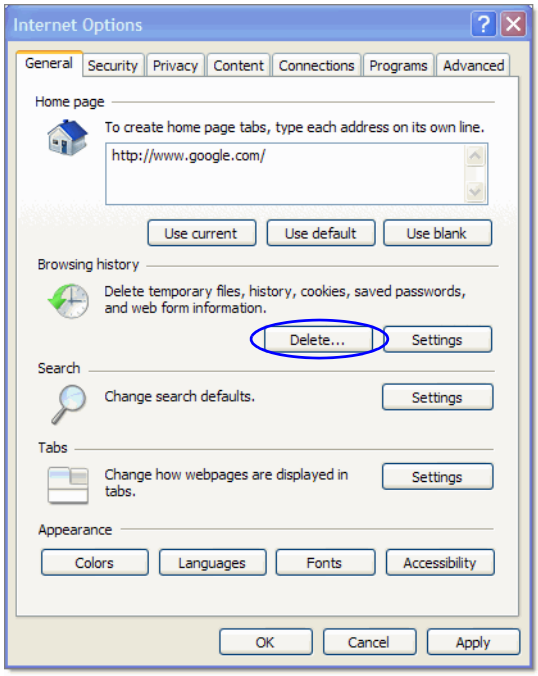


*Select **Internet Options***

The Internet Options window appears.

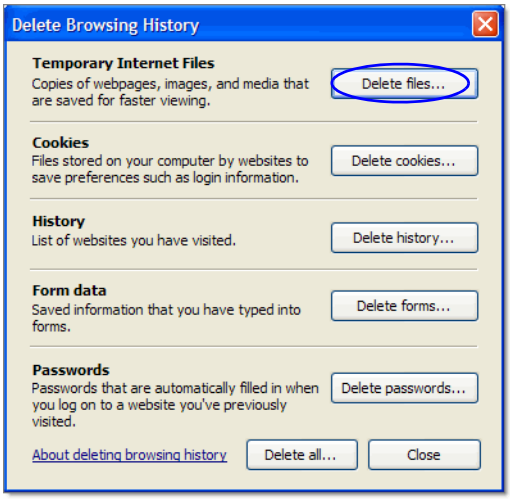
5. On the General tab, do the following:

   a. In the Browsing history section, click the **Delete** button.



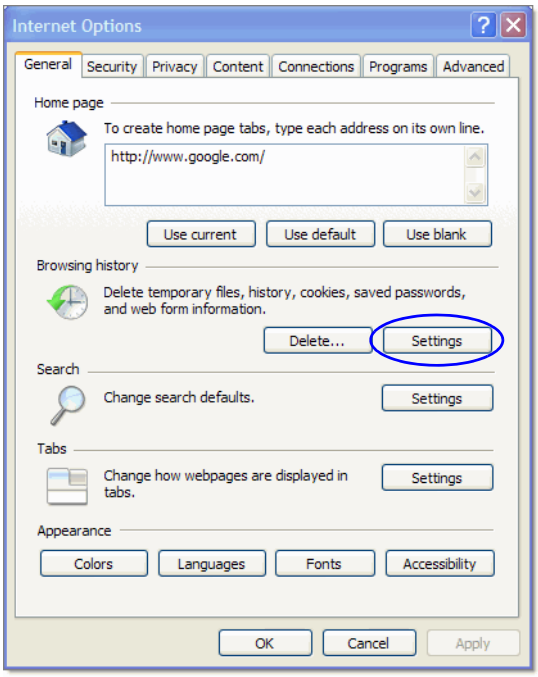
*Click the **Delete** button*

   b. In the Delete Browser History window, in the Temporary Internet Files section, click the **Delete files** button. Click **Close.**



Delete temporary internet files

c. In the Browser history section, click the **Settings** button.

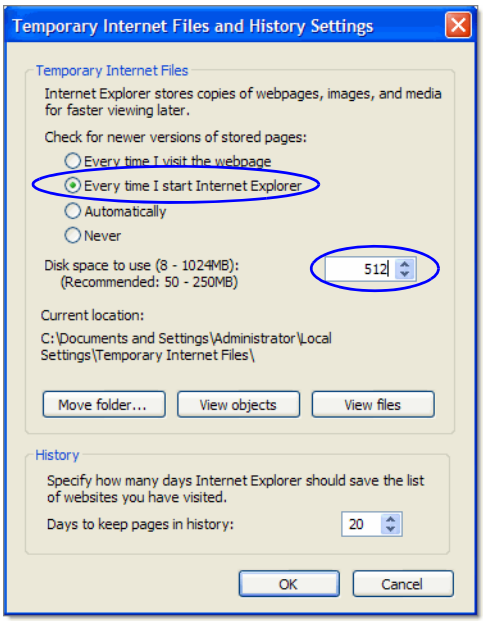


*Click the **Settings** button*

d. In the Settings window, in the Temporary Internet files section, set the following options and click **OK.**

i. Select **Every time I start Internet Explorer** as the option for checking newer versions of stored pages.

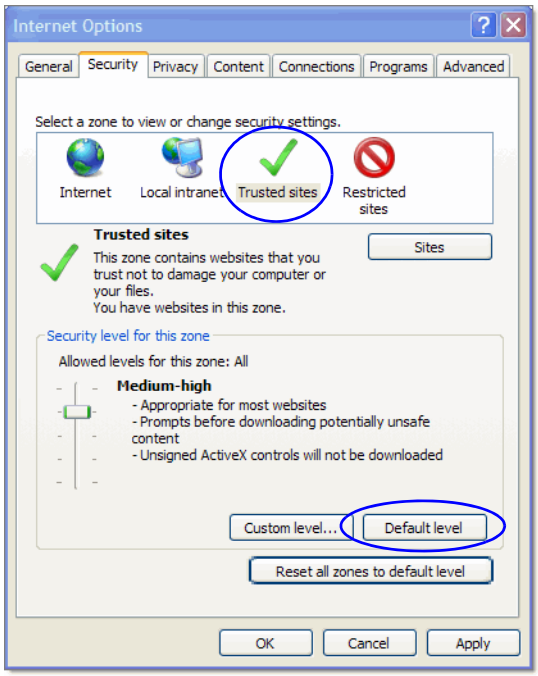
ii. Specify at least 512 MB as the disk space to use for temporary internet files.



Configure temporary internet file settings

6. On the Security tab, perform the following tasks:

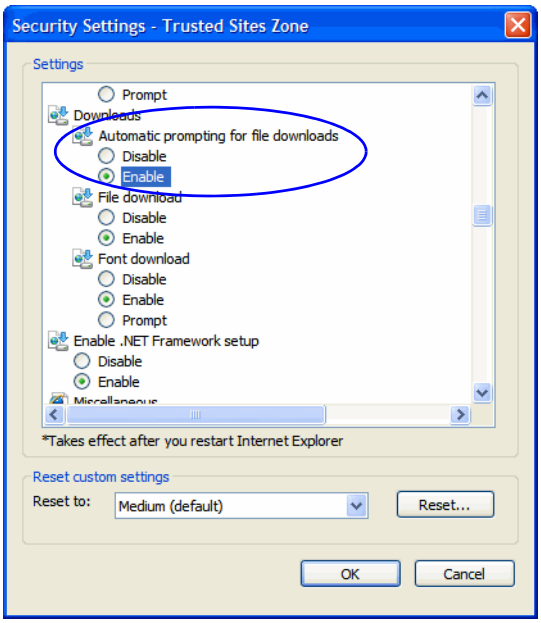
   a. Select the **Trusted sites** zone, and restore default settings by clicking the **Default level** button. If the **Default level** button is disabled, then default settings are already in use.



Configure trusted sites settings

   b. Next, select the **Trusted sites** zone, and click the **Custom level** button.

   c. In the Security Settings window, in the Downloads section, enable the **Automatic prompting for file downloads** setting. Click **OK.**



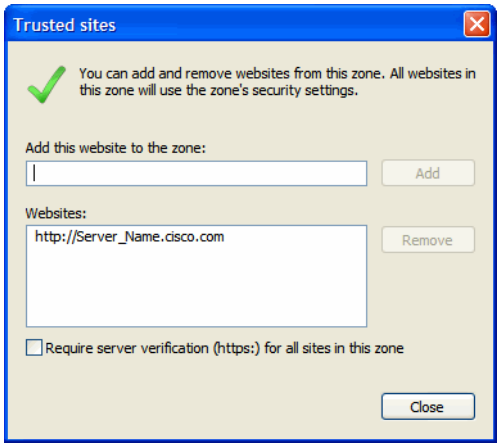
*Enable the **Automatic prompting for file downloads** setting*

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 (http:) for all sites in this zone** option.

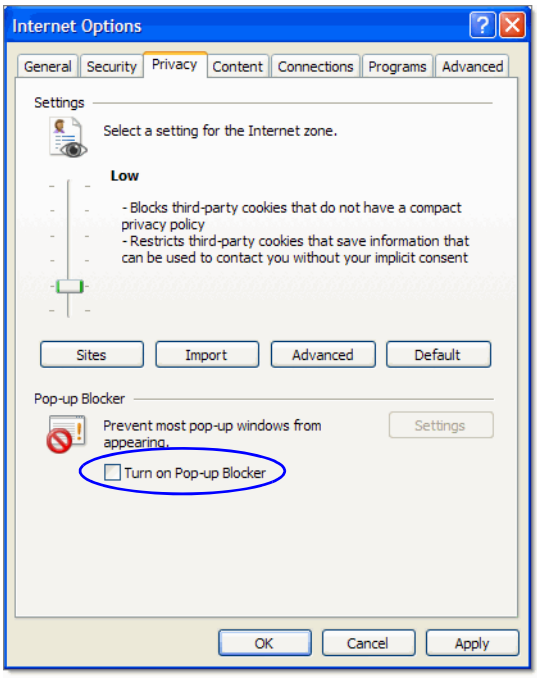
ii. In the **Add this website to the zone** text box, type the Internet address for the application click the **Add** button. Click **Close.**



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

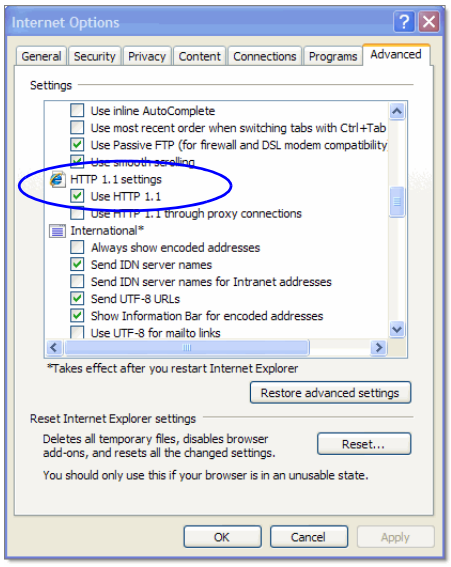
7. On the Privacy tab, in the Pop-up Blocker section, clear the **Turn on Pop-up Blocker** option.

Important: **If you use additional pop-up blockers, you must configure them to allow pop-up windows at the Unified WIM and Unified EIM (see** "Configuring pop-up blockers" on page 16**).**



Configure pop-up blocker setting

8. On the Advanced tab, in the HTTP 1.1. Settings section, ensure that the Use HTTP 1.1 option is selected.



Verify HTTP 1.1 setting

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.

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

Configuring pop-up blockers

- If you use an external pop-up blocker such as the Google and Yahoo toolbar, configure it to allow pop-up windows at your Unified WIM and Unified EIM installation URL.

Configuring Java runtime parameters

The application uses Sun JVM for various operations. This section describes three different procedures for configuring Java runtime parameters to optimize memory usage by Sun JVM. You can use any one of the following methods to configure Java runtime parameters.

- Before a user logs into the system, the application prompts the user to allow the application to automatically optimize Java runtime parameters. For details, see "Configuring Java runtime parameters while logging in" on page 17.
- You can also use the Client JRE Configuration Utility that is packaged with the product to configure Java runtime parameters. For details, see "Configuring Java runtime parameters using the Client JRE Configuration Utility" on page 17.
- From the client desktop, you can also configure these parameters from the Control Panel. For details, see "Configuring Java runtime parameters from the Control Panel" on page 17.

Configuring Java runtime parameters while logging in

Before a user logs into the system, the application prompts the user to allow the application to automatically optimize Java runtime parameters.

To configure Java runtime parameters while logging in:

1. Click **OK** when the application displays the following message:

   ```
   This application uses Java. The Java Runtime memory parameters on your desktop
   are not optimized for this application. Please click OK to configure the
   parameters.
   ```

2. The application configures the required Java runtime parameters automatically and confirms that the parameters have been configured.

   If the application fails to configure the parameters, contact your system administrator.

Configuring Java runtime parameters using the Client JRE Configuration Utility

Use the Client JRE Configuration Utility that is packaged with the product to configure Java runtime parameters.

To configure Java runtime parameters using the Client JRE Configuration Utility:

1. From the *Cisco_Home*`\Utilities` directory, copy the `clientjreconfig` folder and its contents to the client desktop. The folder includes the following files: `JRERuntimeParam.class`, `JREVersions.properties`, `readme.txt`, and `setJREParam.bat`.
2. Open the `setJREParam.bat` file in a text editor and make the following changes:
   a. Locate the line `SET JAVA_HOME=`*<JAVA_HOME>*
   b. Replace *<JAVA_HOME>* with the path where the latest version of JRE 1.6 is installed. For example, *C:\Program Files\java\jre1.6*.
   c. Save the file.
3. Double-click the `setJREParam.bat` file to set the Java runtime parameters on the user desktop.

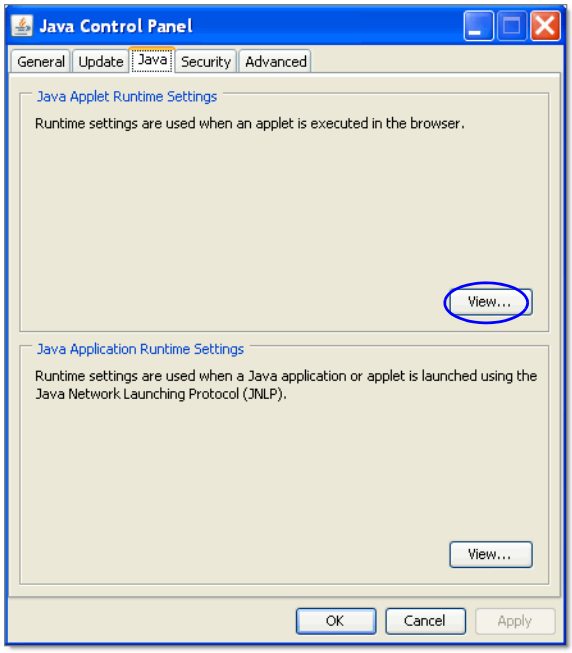
Configuring Java runtime parameters from the Control Panel

From the client desktop, configure the Java parameters from the Control Panel.

To configure Java runtime parameters from the Control Panel:

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.

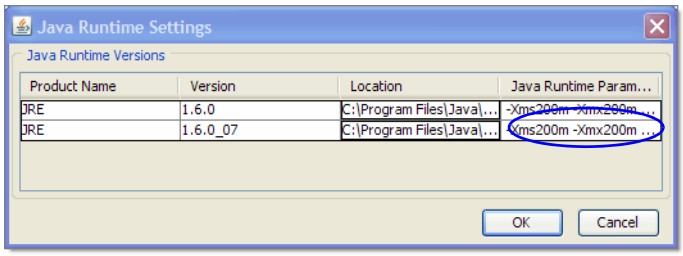
5. In the Java Applet Runtime Settings section, click the **View** button.



*Click the **View** button*

6. In the Java Runtime Settings window, locate JRE version 1.6.0_04, 1.6.0_05, 1.6.0_06, or 1.6.0_07. For the latest version found, in the **Java Runtime Parameters** column, copy and paste the following parameters, and then click **OK**.

```
-Xms200m -Xmx200m -XX:NewSize=48M -XX:MaxNewSize=48M -XX:SurvivorRatio=4 -XX:PermSize=40m -XX:MaxPermSize=40m -Djavaplugin.classloader.cache.enabled=false
```



Copy and paste parameters

Installing MeadCo's Security Manager

MeadCo's Security Manager is required to enable the page-pushing feature in Unified WIM. Users who are assigned chat licenses are asked to install this control when they first log in to the Agent Console.

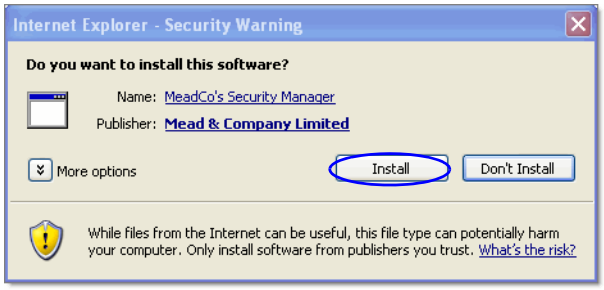
Organizations that do not want to use this feature should set the **Chat - MeadCo download on Agent Console** department-level setting to **No,** in which case users will not be prompted to download the control.

To install MeadCo's Security Manager:

1. Type the Cisco URL in your web browser.
2. In the login window, provide your user name and password. Click **Log In.**
3. In the Consoles window, select **Agent** to go to the Agent Console.
4. If MeadCo's Security Manager is not installed, a related message appears near the title bar. Click the message and select **Install ActiveX Control.** When you select this option, you are prompted to log out of the application.

*Select the **Install ActiveX Control** option*

5. Log out and log in again. Go to the Agent Console.
6. In the Agent Console, you are prompted to install MeadCo's Security Manager. Click the **Install** button.



Install MeadCo's Security Manager

7. 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

Important: **While logging in, use only one user account at a time on a particular desktop. For example, if you have an agent and an author account, log out of one account before logging in to the other account on the same desktop.**

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. Click the **Log In** button.

To log in to the business partition using Cisco Agent Desktop:

- Cisco Interaction Manager integrates with the lower pane of the Cisco Agent Desktop. As an agent, you can configure a task button to launch external applications and use it to log into Unified WIM and Unified EIM.