



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

For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.2(1)
August 2007

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.

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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.

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. (0705R)

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
© 2007 Cisco Systems, Inc. All rights reserved.

Preparing your browser and desktop

- ▶ [About this guide](#)
- ▶ [Verifying browser version](#)
- ▶ [Configuring your browser](#)
- ▶ [Configuring Java runtime parameters](#)
- ▶ [Installing MeadCo's Security Manager](#)

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.

This guide is for installations that are integrated with Cisco Unified Contact Center Enterprise (Unified CCE).

Contents

This guide contains the following procedures:

- ▶ [“Verifying browser version” on page 5](#)
- ▶ [“Configuring your browser” on page 5](#)
- ▶ [“Configuring Java runtime parameters” on page 10](#)
- ▶ [“Installing MeadCo’s Security Manager” on page 11](#)

Document conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	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.
<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.

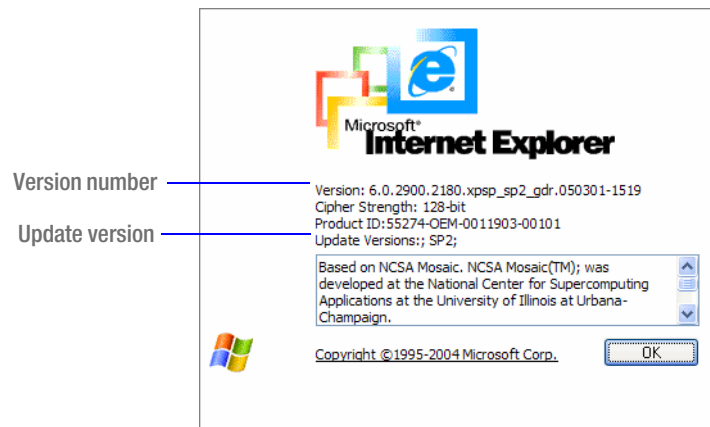
Document conventions

Verifying browser version

Your browser should be Microsoft Internet Explorer 6.0 (Service Pack 2 or higher).

To verify that you are using the correct version:

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** and that the update version is **SP2**. If you need to get the correct version, download it from the Microsoft web site.



Verify browser version

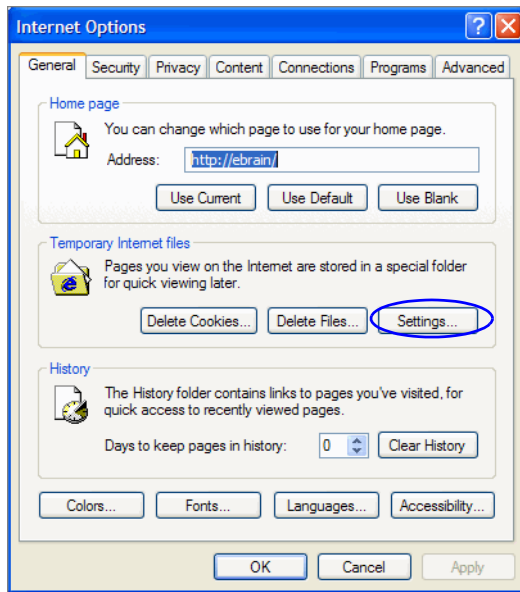
Configuring your browser

To configure your browser for Cisco Interaction Manager:

1. Open Internet Explorer.
2. Go to **Tools** (menu) > **Internet Options**.

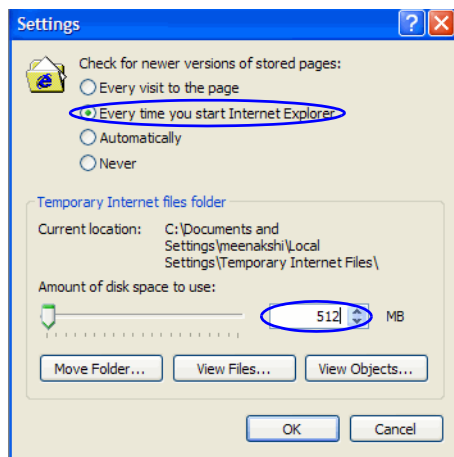
The Internet Options window appears.

3. On the **General** tab, in the **Temporary Internet Files** section, click the **Settings** button.



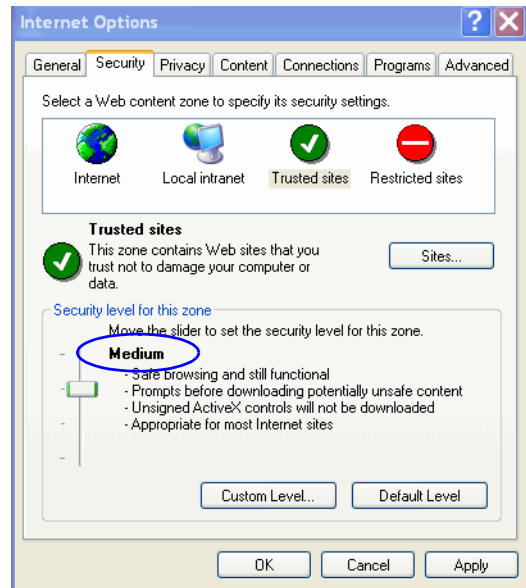
Click the **Settings** button

4. In the Settings window, set the following options and click **OK**.
 - a. Select **Every time you start Internet Explorer** as the option for checking newer versions of stored pages.
 - b. In the **Temporary Internet files folder** section, specify at least 512 MB as the disk space to use.



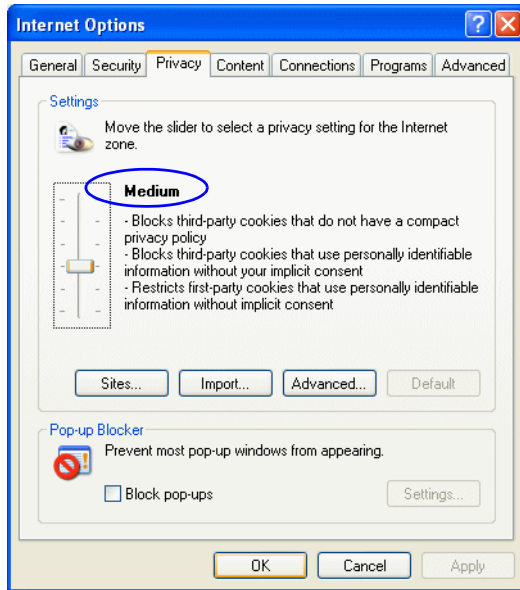
Configure temporary internet file settings

5. On the **Security** tab, perform the following tasks.
 - a. Verify that security level for the **Trusted sites** zone is set to medium or lower.



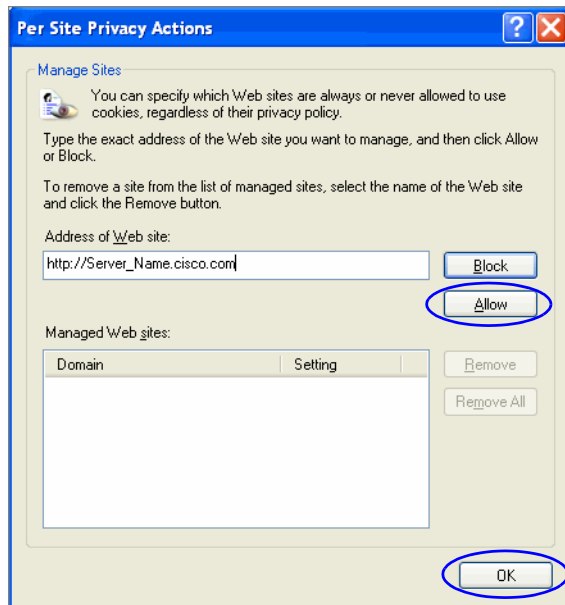
Verify security level for trusted sites is set to medium or lower

- b. Then, select the **Trusted sites** zone and click the **Sites** button.
- c. 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**.
6. On the **Advanced** tab, click the **Restore Defaults** button to restore the default settings.
7. Close Internet Explorer.
8. Reopen Internet Explorer.
9. Go to **Tools** (menu) > **Internet Options**.
10. In the Internet Options window, go to the **Privacy** tab. Perform the following tasks:
 - a. Verify privacy levels are set to medium or lower.



Configure privacy settings

- b. Click the **Sites** button.
- c. In the Per Site Privacy Actions window, perform the following tasks:
 - i. In the **Address of Web site** text box, type the Internet address for the application.
 - ii. Click the **Allow** button. Click **OK**.

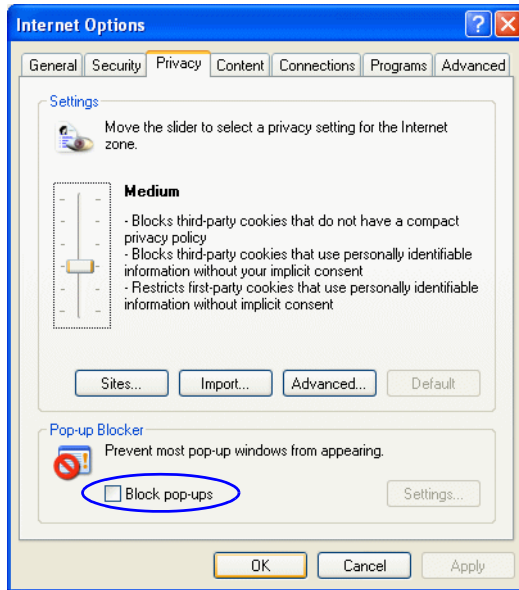


Configure per site privacy settings

- d. Back on the Internet Options window, in the **Pop-up Blocker** section, clear the **Block pop-ups** option.

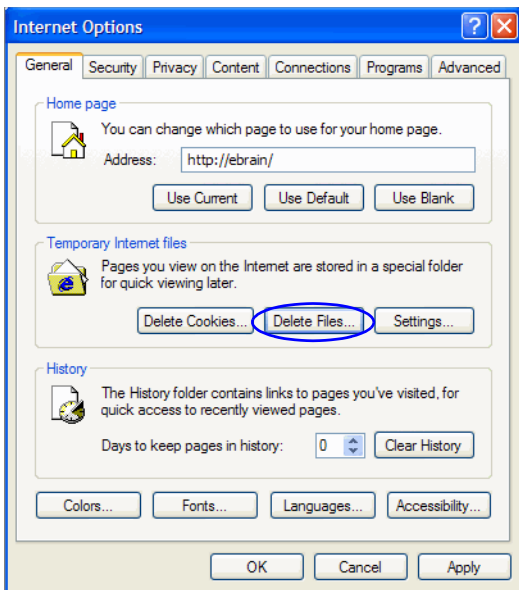


Important: If you use additional pop-up blockers, you must configure them to allow pop-up windows at the Unified WIM and Unified EIM URL (see “Configuring pop-up blockers” on page 10).



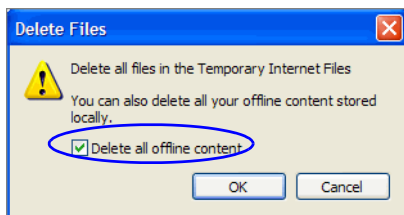
Configure pop-up blocker setting

11. On the General tab, in the **Temporary Internet Files** section, click **Delete Files**.



Delete temporary internet files

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



Delete the offline content stored locally

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

Configuring pop-up blockers

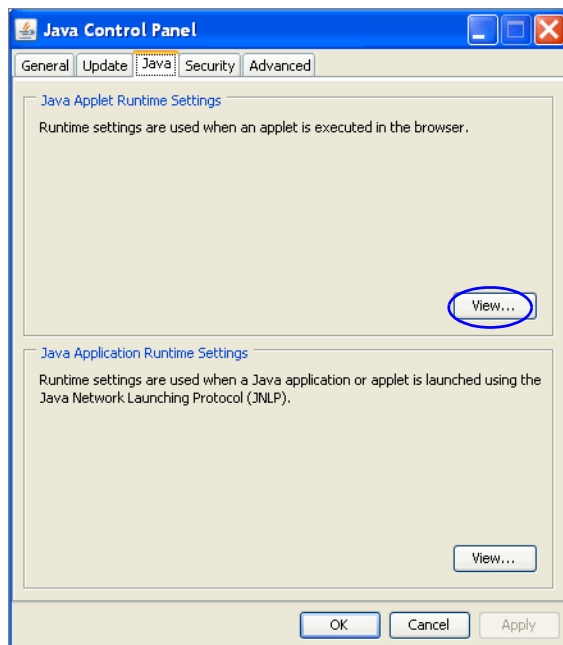
- ▶ If you use an external pop-up blocker such as the Google and Yahoo toolbar, configure it to allow pop-up windows at your Unified WIM and Unified EIM installation URL.

Configuring Java runtime parameters

The application uses Sun JVM for various operations. This section describes the procedure for configuring Java runtime parameters to optimize memory usage by Sun JVM.

To configure Java runtime parameters:

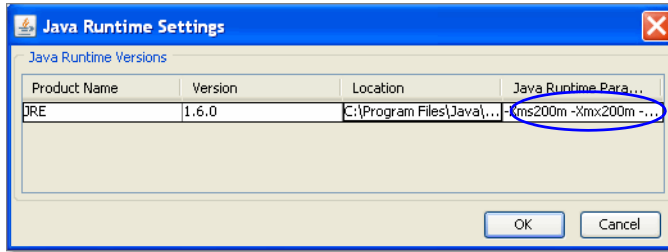
1. Close all open Internet Explorer browsers.
2. Go to **Start > Control Panel**.
3. Double-click **Java**.
4. In the Java Control Panel window, go to the **Java** tab.
5. In the **Java Applet Runtime Settings** section, click the **View** button.



Click the **View** button

6. In the Java Runtime Settings window, locate JRE version 1.6. For that version, 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
```



Copy and paste parameters

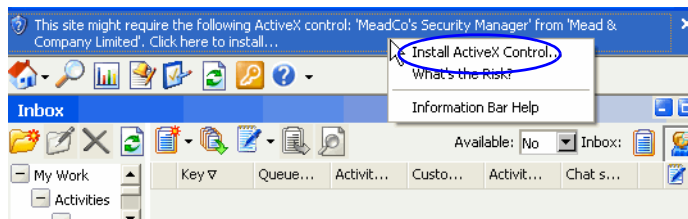
Installing MeadCo's Security Manager

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.

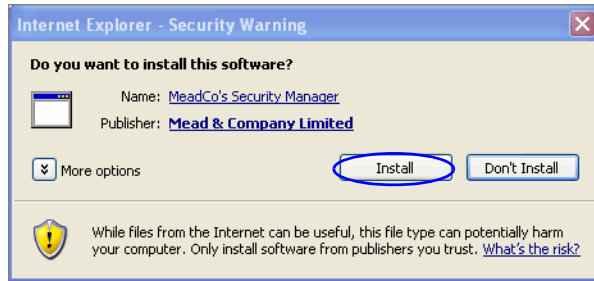
To install MeadCo's Security Manager:

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.



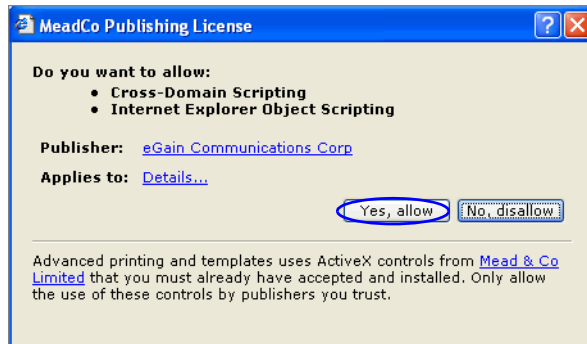
*Select the **Install ActiveX Control** option*

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