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
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.

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

*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.

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](image)

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](image)

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.
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.

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

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

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
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.
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