Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide
For Unified Contact Center Enterprise

Release 9.0(1)
March 2013
Contents

About This Guide ......................................................... 4
Configuring Your Browser ............................................. 4
 Configuring Internet Explorer 9 .................................... 5
 Configuring Internet Explorer 8 .................................... 12
 Configuring Internet Explorer 7 .................................... 19
 Configuring Pop-Up Blockers ....................................... 25
 Configuring Java on Your Desktop ................................. 25
 Configuring MeadCo’s Security Manager ......................... 27
   Enabling the Automatic Download of ActiveX Controls ...... 28
   Installing MeadCo’s Security Manager ......................... 28
 Logging In .................................................................. 29
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.

<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.</td>
</tr>
<tr>
<td></td>
<td>Or, text that must be typed by the user.</td>
</tr>
<tr>
<td><em>Monospace</em></td>
<td>A file name or command.</td>
</tr>
<tr>
<td></td>
<td>Or, text that must be typed by the user.</td>
</tr>
<tr>
<td><em>Variable</em></td>
<td>User-specific text, provided by the user.</td>
</tr>
</tbody>
</table>

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 28), 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” on page 5
- “Configuring Internet Explorer 8” on page 12
- “Configuring Internet Explorer 7” on page 20
- “Configuring Pop-Up Blockers” on page 26
Configuring Internet Explorer 9

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. 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 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.

   ![Delete button](image)

   **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](image1)

**Delete temporary internet files**

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

![Click the Settings button](image2)

**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

e. In the Tabs section, 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](image)

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](image)
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.

![Security Settings - Internet Zone](image)

*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 28.

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**.

![Trusted sites](image)

*Add the URL for the application to the trusted web sites list*
7. On the Privacy tab, perform the following tasks:

a. 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 26).

---

![Configure pop-up blocker setting](image)

b. Skip this step if you have not embedded the eGain 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 eGain web server and click **Allow**.

ii. Now enter the Finesse hostname and click **Allow**. Click **OK** to close this window,

![Manage per site privacy actions](image)
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](image)

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 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 \textbf{8.0.x}. If you need to get the correct version, download it from the Microsoft web site.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{about_ie.png}
\caption{Verify browser version}
\end{figure}

4. On the Internet Explorer toolbar, click the \textbf{Tools} button and select \textbf{Internet Options}.

The Internet Options window appears.

5. On the General tab, do the following:
   a. In the Browsing history section, click the \textbf{Delete} button.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{internet_options.png}
\caption{Click the Delete button}
\end{figure}

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

![Delete temporary internet files](image1.png)

**Delete temporary internet files**

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

![Click the Settings button](image2.png)

**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.

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

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.

   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 28.

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](image1)

7. On the Privacy tab, perform the following tasks:
   a. In the Pop-up Blocker section, clear the **Turn on Pop-up Blocker** option.

![Configure pop-up blocker setting](image2)

*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 26).
b. Skip this step if you have not embedded the eGain 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 eGain 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

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 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**. If you need to get the correct version, download it from the Microsoft web site.

![Internet Explorer Version Number](image)

**Verify browser version**

4. On the Internet Explorer toolbar, click the **Tools** button and 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.

   ![Internet Options](image1)
   Click the **Delete** button

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

   ![Delete Browsing History](image2)
   Delete temporary internet files
c. In the Browsing history section, click the **Settings** button.

![Settings button](image1.png)

**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.

![Temporary internet file settings](image2.png)

**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](image)

   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](image)
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](image)

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 28.

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 URL for the Unified WIM and Unified EIM application and click the **Add** button. Click **Close**.

   ![Add the URL for the application to the trusted web sites list](image)

7. On the Privacy tab, perform the following tasks:
a. 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 26).

Configure pop-up blocker setting

b. Skip this step if you have not embedded the eGain 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 eGain 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
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 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 (Update 30 or higher) 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 27 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**. In the Java Control Panel window, go to the Java tab.
4. In the Java Applet Runtime Settings section, click the **View** button.
5. In the Java Runtime Settings window, verify that JRE 1.6 (Update 30 or higher) is enabled. Click OK.

![Verify that the latest version of Java is enabled](image)

6. If Java 1.7 is also installed on your machine, in the Java Control Panel window go to the Advanced tab and in the Insecure JRE version section, select the **Allow using insecure JRE versions** option and click Apply.

![Select the Allow using insecure JRE versions option](image)

7. Click OK to close the window.

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

1. Close all open Internet Explorer browsers.
2. Go to `C:\Program Files (x86)\Java\jre6\bin`
3. Double-click `javacpl.exe`.
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 that opens, verify that JRE 1.6 (Update 30 or higher) is enabled. Click OK.

![Java Runtime Environment Settings](image)

*Verify that the latest version of Java is enabled*

7. If Java 1.7 is also installed on your machine, in the Java Control Panel window go to the Advanced tab and in the Insecure JRE version section, select the Allow using insecure JRE versions option and click Apply.

![Java Control Panel](image)

*Select the Allow using insecure JRE versions option*

8. 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](image)

### 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 30.
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.

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.

---

**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.