CISCO

Cisco Unified Web and E-Mail Interaction Manager Release Notes

For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.2(1)
August 2007

Contents

This is the first release of Cisco Interaction Manager 4.2(1) for integration with Cisco Unified Contact Center Enterprise (Unified CCE) 7.1.3. 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)

> **Important:** **In this release, Unified CCE and Unified SCCE are not integrated with Unified WIM.**

Cisco Unified Web and E-Mail Interaction Manager Release Notes provides an overview of the release and a list of open caveats. It also includes information about the Bug Toolkit, documentation, and support resources.

About this release

Cisco Unified Contact Center solutions provide an open, strategic platform that allows you to move your organization beyond today's call center to the next phase of customer care, a customer interaction network. The Cisco Interaction Manager–Unified CCE integration offers new and exciting capabilities for contact centers, helping users effectively handle large volumes of customer interactions, whether voice phone calls, email, or web chats, with the help of common data and knowledge resources.

> **Important:** **In this release, label-based routing (also referred to as non-IPTA routing) is not supported.**

Localized versions

Cisco Interaction Manager is available in five Western European languages other than English: Dutch, French, German, Italian and Spanish. The localized versions include user interface (UI) screens and the ability to handle email, chat, and knowledge base article content in these languages.

The document set is only available in English. Localized online help is planned for a future release.

Open caveats

The following table contains a list of caveats currently pending in Cisco Interaction Manager Release 4.2(1). For the latest status of all open caveats, access the Cisco Bug Toolkit as described in the section "Using Cisco Bug Toolkit" on page 7.

Identifier	Severity	Headline	Workaround
CSCsj72942	S3	Sun JRE does not get loaded due to several Java Virtual Machines (JVMs) running in the same process.	▹ Remove unused plugins in the browser. ▹ Use a newly initiated browser session to access the Login page.

Identifier	Severity	Headline	Workaround
CSCsj72980	S4	Localized Help is not available.	Localized online help is planned for a future release
CSCsj79566	S4	Sometimes, login doesn't work when the Enter key is pressed to activate the selected Log in button. The mouse event is not captured in this case.	▶ Double-click the browser title bar, which then resizes the window and triggers the mouse event.
CSCsj86522	S3	Some department level settings are not visible as preferences even though they are configured to be reset at a lower level.	–
CSCsj86535	S3	When a user with permissions to transfer to more than 800 users opens the transfer window, the window and user list appear empty.	▶ Assign permissions in smaller batches.
CSCsj86550	S3	Find and replace across folders does not work for ``macroname.	–
CSCsj86559	S3	If an attribute of an access link is modified, emails go into the exception queue. The corresponding parameter of the usage link disappears.	▶ Open the usage link and reselect the input parameter. Then stop and start the Workflow Engine process and instance.
CSCsj86567	S3	Agents who are assigned Chat licenses may see the following error while working for long periods on non-chat activities in the main inbox. *Chat Applet connection was temporarily lost. You need to click the Yes button to refresh the window to restore the connection now, or click the No button to refresh later.*	▶ Refresh the window.
CSCsk15210	S3	When a user with permissions to administer more than 10,000 users clicks the Users node, it takes more than 15 minutes to display the user list.	▶ Create multiple departments. For each department, run the Cisco Interaction Manager Integration Wizard and map a maximum of 500 users.
CSCsk15215	S3	When a user with permissions to administer more than 20,000 user groups clicks the Groups node, the operation times out.	▶ Create multiple departments. For each department, run the Cisco Interaction Manager Integration Wizard and map a maximum of 500 user groups.

Special note for integrations with Cisco Unfiied System Contact Center Enterprise

The following issues are noticed only in deployments where Cisco Interaction Manager is integrated with Cisco Unified System Contact Center Enterprise (Unified SCCE), formerly called System IPCC. Cisco Technical Assistance Center (TAC) has fixes available for all of these issues.

Identifier	Severity	Headline	Workaround
CSCsj73017	S2	Agents who belong to the "Cisco Interaction Manager-Picks-the-Agent" user group cannot log in to Unified SCCE.	▸ Contact Cisco TAC to obtain the fix.
CSCsj74879	S3	The Media Routing Domain (MRD) associated with a skill group can be changed from Unified SCCE.	▸ Contact Cisco TAC to obtain the fix.
CSCsj78522	S2	The interruptible value of an Email MRD cannot be changed from Unified SCCE.	▸ Contact Cisco TAC to obtain the fix.

Configuring integrations with Unified SCCE

This section decribes procedures for configuring deployments where Cisco Interaction Manager is integrated with Unified SCCE.

Configuring application instance

To configure the application instance for the integration:

1. Log in to Cisco Interaction Manager as a partition administrator.

2. Go to the Administration Console.

3. In the Tree pane, browse to **Partition:** *Your partition* > **Settings** > **Partition.**

4. In the List pane, select **Partition Settings Group.**

5. In the Properties pane, click the Attributes tab.

6. Locate the **Application Instance** communication setting. Set the value to be "IPCCAdmin". If you had used the Integration Wizard earlier, this value should already be set. In that case, verify that the value is "IPCCAdmin".

Configuring Listener instance

To configure the Listener instance:

1. In the Unified SCCE Web Administration tool, navigate to the **System Management** > **Machine Management** > **IPCC Network** page.

   a. Note the name or IP address of the IPCC Machine that is Side A and has the role Agent/IVR Controller.

    b.   Note the name or IP address of the IPCC Machine that is Side B and has the role Agent/IVR Controller.

2. Log in to Cisco Interaction Manager as a partition administrator.

3. Go to the System Console.

4. In the Tree pane, browse to **Partition:** *Your partition* > **Services** > **Listener** > **Listener.**

5. In the List pane, select **Listener-instance.**

6. In the Properties pane, configure the following properties:

    ❍   **Primary CTI Server:Port:** Type the Side A Agent/IVR Controller machine name or IP address that you noted in step 1a, followed by ":" (colon) and then the number "42027".

    ❍   **Secondary CTI Server:Port:** Type the Side B Agent/IVR Controller machine name or IP address that you noted in step 1b, followed by ":" (colon) and then the number "43027". If there is no B side, enter the same information you entered in step 6 above.

Configuring External Agent Assignment Service instance

To configure the External Agent Assignment Service (EAAS) instance:

1. Log in to Cisco Interaction Manager as a partition administrator.

2. Go to the Administration Console.

3. In the Tree pane, browse to **Partition:** *Your partition* > **Settings** > **Partition.**

4. In the List pane, select **Partition Settings Group.**

5. In the Properties pane, click the Attributes tab.

6. Locate the **MR Connection Port** communication setting. Set its value to "2000".

Using Cisco Bug Toolkit

If you are a registered Cisco.com user, you can find the latest information about resolved, open, and closed caveats for Cisco Interaction Manager by using the Bug Toolkit, an online tool that allows you to query caveats according to your own needs. By using the Bug Toolkit, you can find caveats of any severity for any release. The Bug Toolkit may also provide a more current listing than this document provides.

To access the Bug Toolkit, you need:

▸ Internet connection

▸ Web browser

▸ Cisco.com user ID and password

To use the Bug Toolkit:

1. Go to this URL to access the Bug Toolkit:

    http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

2. Log in with your Cisco.com user ID and password.

3. To access Cisco Interaction Manager caveats, take either of these actions:

   ❍ To access a particular caveat when you know its identifier, enter the identifier in the **Search for Bug ID** field and click **Go.**

   ❍ To access all caveats, follow these steps:

      i. From the **Select Product Category** list, choose **Voice and Unified Communications.**

      ii. From the **Select Product** list, choose **Cisco Unified E-Mail Interaction Manager** or **Cisco Unified Web Interaction Manager.**

      iii. From the **Software Versions** list, choose the desired Unified EIM or WIM release.

      iv. Select the desired **Advanced Options** button. If you choose custom settings, enter appropriate custom information.

      v. Click **Search.**

      A list of caveats that match your search criteria appear. To see details about any caveat, click its Bug ID number or click its **Info** link.

Document set

Unified Web and E-Mail Interaction Manager documentation is available in the `Documents` folder on the product CD. It includes the following documents:

▸ *Cisco Unified Web and E-Mail Interaction Manager System Requirements*

▸ *Cisco Unified Web and E-Mail Interaction Manager Installation Guide*

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

▸ *Cisco Unified Web and E-Mail Interaction Manager Administration Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager Agent Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager Reports Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager Supervision Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager System Console User's Guide*

▸ *Cisco Unified Web and E-Mail Interaction Manager Tools Console User's Guide*

The latest versions of all Cisco documentation can be found online at http://www.cisco.com

▸ All Unified EIM documentation can be found online at
   http://www.cisco.com/en/US/products/ps7236/tsd_products_support_series_home.html

▸ All Unified WIM documentation can be found online at
   http://www.cisco.com/en/US/products/ps7233/tsd_products_support_series_home.html

▸ In particular, Release Notes for these products can be found at
   http://www.cisco.com/en/US/products/ps7236/prod_release_notes_list.html

▸ For general access to Cisco Voice and Unified Communications documentation, go to
   http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

Obtaining documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco web sites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Field alerts and field notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

Cisco product security overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting security problems in Cisco products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com
  An emergency is either a condition in which a system is under <u>active</u> attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non emergencies.

- For non emergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302

- 1 408 525-6532

> **Tip:** We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
>
> http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
>
> The link on this page has the current PGP key ID in use. If you do not have or use PGP, contact PSIRT at the aforementioned email addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining technical assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation web site

The Cisco Technical Support & Documentation web site provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The web site is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation web site requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

> **Note:** Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support and Documentation web site by clicking the **Tools & Resources** link under **Documentation & Tools**. Choose **Cisco Product Identification Tool** from the Alphabetical Index dropdown list, or click the **Cisco Product Identification Tool** link under **Alerts & RMAs**. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a service request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly. To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of service request severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

- Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

- Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

- Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

- Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining additional publications and information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine
  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html