



Release Notes for *Cisco Unified Contact Center Management Portal Release 7.1(1)*

August 25, 2006

Contents

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Related Documentation, page 2](#)
- [New and Changed Information, page 2](#)
- [Important Notes, page 4](#)
- [Resolved Caveats in This Release, page 5](#)
- [Open Caveats in This Release, page 7](#)
- [Obtaining Documentation, page 7](#)
- [Documentation Feedback, page 8](#)
- [Product Alerts and Field Notices, page 9](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 11](#)

Introduction

This is the first release of Cisco Unified Contact Center Management Portal, which is a suite of components that form part of Cisco IPCC Hosted Edition. The rest of this document discusses the features, technical information and caveats associated with Unified Contact Center Management Portal Release 7.1(1).



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

**Note**

For the most up-to-date version of these release notes, go to the Cisco Web page:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html

System Requirements

For hardware and third-party software specifications for Releases 7.0(0) and 7.1(1), refer to the *Hardware and System Software Specification (Bill of Materials): Cisco ICM/IPCC Enterprise & Hosted Edition, Releases 7.0(0) and 7.1(1)*, which is accessible from
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Related Documentation

- Documentation for Cisco IPCC Hosted Edition, including Cisco Unified Contact Center Management Portal, is accessible from
http://www.cisco.com/en/US/products/sw/custcosw/ps5053/tsd_products_support_series_home.html
- For additional information on Cisco IPCC/ICM Enterprise and Hosted Editions, see the *Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0)B* and the *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*, which are accessible from
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html
- Technical Support documentation and tools can be accessed from
<http://www.cisco.com/en/US/support/index.html>
- The Product Alert tool can be accessed through
<http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice>

New and Changed Information

The following sections describe new features and changes that are pertinent to this release.

- [Overview, page 2](#)
- [User Documentation, page 4](#)

Overview

Since this is a first release, the entire release is new, and there have been no changes from a previous release. Detailed information on Unified Contact Center Management Portal Release 7.1(1) can be found in the documentation set, which is discussed in [User Documentation, page 4](#).

Cisco Unified Contact Center Management Portal is a suite of components that form part of Cisco IPCC Hosted Edition. Unified Contact Center Management Portal serves two mutually supportive purposes:

- **Simplify** the operations and procedures for performing basic tasks such as Move/Add/Modify Agents, Skill Groups, Teams and other common administrative functions.

- **Provide a common web user interface** within the product solution set. Currently, IPCC Hosted Edition and CallManager use different interfaces. Simple tasks therefore require performing multiple tasks in both products to achieve a single goal, for example, adding an agent. By providing a web-based unified interface for common administrative tasks, the value of the solution increases, by decreasing the amount of time, knowledge, training and resources currently required to administer the solution set.

Unified Contact Center Management Portal components comprise a module that is integrated with IPCC Hosted Edition. IPCC Hosted Edition customers can optionally include the Unified Contact Center Management Portal to satisfy particular business requirements.

Primary Functionality

- **Unified Configuration**, that is, tenant provisioning of both the applicable IPCC Hosted Edition CICM and CallManager components through a single task-based web interface.
- **Hierarchical Administration**, for example:
 - The Service Provider Administrator can add a Tenant.
 - The Tenant Administrator can add a Skill Group.
 - The Tenant Supervisor can add an Agent.
- **Audit Trails** on configuration changes and usage.

In terms of configuration, the Unified Contact Center Management Portal differentiates between commissioning and provisioning.

- **Commissioning** consists of operations that install and initially configure a system of components. These operations are typically done by the Service Provider using existing setup and configuration tools. Examples include installing PGs and configuring PGs and Network Trunk Groups.
- **Provisioning** consists of day to day configuration operations performed by a tenant. Examples include Move/Add/Modify Agents, Skill Groups and Teams.

The Service Providers will use the existing IPCC Hosted Edition and CallManager tools (installers and configuration tools) to commission a system. Service Providers will use the Unified Contact Center Management Portal Provisioning System to define tenants and set up tenant permissions. Tenants will then use the Unified Contact Center Management Portal Provisioning System to provision their specific site.

Unified Contact Center Management Portal provides a provisioning layer on top of IPCC Hosted Edition 7.1. It works with the standard IPCC Hosted Edition, a new single-instance IPCC Hosted Edition Deployment, and CallManager.

Unified Contact Center Management Portal provides its own provisioning database that includes a rich, hierarchical permissions model. Provisioning changes are stored in the Unified Contact Center Management Portal system and then exported to IPCC Hosted Edition and CallManager.

Additionally, the Unified Contact Center Management Portal system can read existing configuration data from IPCC Hosted Edition and CallManager, store them in the Unified Contact Center Management Portal database and reconcile differences between them. This enables Service Providers to make configuration changes using existing IPCC Hosted Edition and CallManager tools and propagate these changes into the Unified Contact Center Management Portal system.

Deployment Specifics

Unified Contact Center Management Portal platform deployments are limited to standard IPCC Hosted Edition deployments with the following restrictions:

- Each Tenant must have its own:
 - CICM instance.
 - Dedicated Admin Workstation Real Time Distributor server.



Note Multiple Distributor instances on a single server are NOT allowed.

- WebView instance for reporting purposes.
- The Unified Contact Center Management Portal is only supported on IPCC Hosted Edition 7.1 and above.
- Current IPCC Enterprise Edition customers can deploy the Unified Contact Center Management Portal in their system to provide particular features—thereby converting that system to a NAM-less IPCC Hosted Edition model. (However, multi-level access/ partitioning is not currently provided for reporting or agent statistics).

User Documentation

This section briefly describes the Unified Contact Center Management Portal documentation set.

- *Installation Guide for Unified Contact Center Management Portal*—describes the installation procedures for the various components that make up Unified Contact Center Management Portal.
- *User Manual for Unified Contact Center Management Portal*—explains how to use Unified Contact Center Management Portal to view and alter your system.
- *Administration Manual for Unified Contact Center Management Portal*—contains information needed to configure and administer Unified Contact Center Management Portal.
- *Troubleshooting Guide for Unified Contact Center Management Portal*—provides information to help troubleshoot problems you may encounter when you install, configure, or use Unified Contact Center Management Portal.

Important Notes

The following sections contain important restrictions and requirements that apply to Unified Contact Center Management Portal Release 7.1(1).

- [Multi-tenant Unified CallManager, page 4](#)
- [Microsoft Windows Hotfix Required, page 5](#)

Multi-tenant Unified CallManager

Unified Contact Center Management Portal Release 7.1(1) does not support multi-tenant Unified CallManager.

Microsoft Windows Hotfix Required

Before installation, Windows Update should be run and all required updates installed. In particular, the hotfix located at <http://www.microsoft.com/downloads/details.aspx?familyid=8B4E6B93-1886-4D47-A18D-35581C42ECA0&displaylang=en> must be downloaded. Without this patch the application installers may not execute correctly.

Resolved Caveats in This Release



Note

Since this is the first release of Cisco Unified Contact Center Management Portal there are, in fact, no resolved caveats, that is, there are no bugs from an earlier release that could have been fixed.

Resolved caveats are no longer listed in these Release Notes. Instead, you can find the latest resolved caveat information through Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.



Tips

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure



Tips

To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

- Step 1** Log on with your Cisco.com user ID and password.
- Step 2** Click the **Launch Bug Toolkit** hyperlink.
- Step 3** If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco ICM/IPCC Enterprise and Hosted Editions, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Unified Intelligent Contact Management Enterprise** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Unified Intelligent Contact Management Enterprise**.

Step 4 Click **Next**. The Cisco Unified Intelligent Contact Management Enterprise search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Select the Cisco Unified Intelligent Contact Management Enterprise Version:

- Choose the major version for the major releases.

A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information.

A revision release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

b. Choose the Features or Components to query; make your selection from the "Available" list and click **Add** to place your selection in the "Limit search to" list.

To query for all caveats for a specified release, choose "All Features" in the left window pane.



Note The default value specifies "All Features" and includes all of the items in the left window pane.

c. Enter keywords to search for a caveat title and description, if desired.



Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

d. Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the Fixed check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

Step 6 Bug Toolkit returns the list of caveats on the basis of your query. You can modify your results by submitting another query and using different criteria.

Open Caveats in This Release

This section contains a list of defects that are currently pending in Unified Contact Center Management Portal Release 7.1(1). Defects are listed by component and then by identifier.



Tips

If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 1 Open Caveats for Cisco Unified Contact Center Management Portal Release 7.1(1)

Identifier	Component	Headline
CSCse98884	ccmp	Network VRU Script List - New button returns Error:404
CSCse99020	ccmp	Install of win2k3 +sp1 missing windows installer V3.1
CSCsf03172	ccmp	DN: UI allows > max char allowed for unique name and DN fields
CSCsf04171	ccmp	Monitor Details Web Page for Provisioning Server fails to display
CSCsf04189	ccmp	Minor Updates within DB installer
CSCsf04210	ccmp	A supervisor is allowed to create an agent on a different peripheral
CSCsf05971	ccmp	Multiple Controls error with duplicate users listed

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 websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, 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/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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.

Product Alerts and Field Notices

Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Product Alert and Cisco Field Notice mechanisms. You can register to receive Product 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.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.htm

The link on this page has the current PGP key ID in use.

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 Website

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

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website 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 & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down 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)—Your 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 operation 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 your network is impaired, but 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.

- 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>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)