# Release Notes for *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*

**June 11, 2007**

## Contents




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

# Introduction

ICM/IPCC software Release 7.1(1) supports ICM and IPCC Hosted & Enterprise Editions. This document discusses new features, changes, and caveats for Release 7.1(1) of ICM/IPCC Enterprise and Hosted software.

This document is a supplement to the *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0)* available at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html

These Release Notes should be used in conjunction with the above Release Notes.

## About Release 7.1(1)

Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) is a minor release. New as of Release 7.1(1), a minor release is an incremental set of defect fixes and a limited set of new functionality delivered in an automated installer.

As of ICM Release 7.1(X) Service Releases are being renamed as Maintenance Releases.

A minor release is incremental, cumulative to the base release of the Major release. A minor release can be returned to its pre-installation state. All ongoing maintenance release content present at the point of the minor release ship date is contained within the minor release. The only exception is where a minor release development/testing schedule overlaps with that of a maintenance release. Engineering specials released prior to the code freeze date are also part of the minor release content (resolved caveats included are highlighted in the release notes).

Minor Release 7.1(1) can be installed over ICM/IPCC 7.0(0), or ICM/IPCC 7.0(0) SR1-SR3. The Release 7.1(1) Installer performs a check that prevents it from installing on systems running ICM/IPCC 7.0(0) with service releases after SR3.

The minor release is available on CD and as downloadable installers from cisco.com.

For additional information on the Cisco software support methodology, refer to the *ICM/IPCC Enterprise Maintenance Support Strategy*, available at:
http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml (requires login).

ICM/IPCC 7.0(0) must be installed prior to installing Release 7.1(1). For an explanation of the specifications for ICM/IPCC Enterprise & Hosted Edition Release 7.0(0) , refer to the C*isco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, which is accessible from:
http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

Release Notes for *Cisco CTI Object Server*, *Cisco Agent Desktop*, *Cisco E-Mail Manager Option*, *Cisco Support Tools,* and *Cisco Web Collaboration Option* (including *Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender*) are separate documents and are not included as part of these Release Notes.

For a detailed list of language localizations implemented for different portions of this release, refer to the Cisco Unified ICM/Contact Center Product and System Localization Matrix available at:
http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps1846/c1225/ccmigration_09186a008068770f.xls

**Note** The most up-to-date version of these release notes is available on the web at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html

## A Note about Product Naming

Cisco IPCC Enterprise Edition is being renamed to Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE).

Cisco IPCC Hosted Edition is being renamed Cisco Unified Contact Center Hosted (abbreviated as Unified CCH).

These new names are introduced in this release for Agent and Supervisor product opening-screens and in documentation that has been revised for Release 7.1(1), but they do not yet appear throughout the user interface or documentation. These release notes use the previous naming convention.

# System Requirements

For hardware and third-party software specifications for Release 7.1(1), refer to the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, which is accessible from
http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

Release 7.1(1) updates are also available for CTI OS and Cisco Agent Desktop. Cisco E-Mail Manager and Cisco Web Collaboration Option remain at Release 5.0.

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* for information on agent desktop and PG software versions supported during 7.1(1) migration, as well as other important upgrade considerations.

Installation of Release 7.1(1) has a prerequisite of a Release 7.0(0) base installation (including any of Release 7.0(0) SR1, SR2, or SR3), as described in the above document.

# Related Documentation

Documentation for Cisco ICM/IPCC Enterprise and Hosted Editions, as well as most related documentation, is accessible from
http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

- Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) - http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html
- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).
- Also related is the documentation for Cisco CallManager.
- 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

Intelligent Contact Management (ICM) and IP Contact Center (IPCC) software Release 7.1(1) is a minor release that contains fixes and a limited set of new functionality. All previous maintenance releases to Release 7.0(0) (through Service Release 3)[1] are included in Release 7.1(1). Release 7.1(1) is incremental and cumulative, and can be rolled back.

Release 7.1(1) introduces the following new features:

- Cisco Unified Mobile Agent
- ECC Variable Persistence Selection
- Support Tools Node Agent automatically installed.
- Support for the InstallShield Silent Installation (not supported for CAD).
- System IPCC Localization Support
- Support for Cisco CVP NetworkVRU Type 10
- ICM ID Finder Tool Enhancement
- Technical Changes and Notes, page 8, also provide information on new features that are technical in nature.

If you are also deploying CTI OS, the respective Release 7.1(1) provides the following new features (Details available in the *CTI OS Release Notes for Release 7.1(1)*):

- Citrix MetaFrame Presentation Server 4.0 Support
- Mobile Agent Support
- Support for Up To 1500 Agents
- Silent Install
- Silent Monitoring Architecture Changes

If you are also deploying Cisco Agent Desktop (CAD), the respective Release 7.1(1) provides the following new features (details available in the *Cisco Agent Desktop Release Notes for Release 7.1(1)*):

- Cisco Agent Desktop–Browser Edition (CAD-BE), a browser-based version of Cisco Agent Desktop
- Cisco Agent Desktop includes up to 6 tabbed browser windows
- Cisco Supervisor Desktop includes a supervisor workflow email alert action— email alerts that notify supervisors whenever skill group thresholds for Number of Calls Waiting and Oldest Call in Queue are not met
- Cisco Supervisor Desktop includes an integrated browser window
- Cisco Unified Mobile Agent is supported for use with Cisco Agent Desktop and CAD-BE
- Cisco Unified Intelligent Contact Management (ICM) reason codes are integrated into CAD
- Reason codes, wrap-up data, and phone books are assigned on both the global and work flow group levels

1. Release 7.1(1) also contains a subset of the fixes that are available in Maintenance Release 4.

- Cisco Agent Desktop can receive messages from third party applications via the new remote access IPC Receive event.

## Cisco Unified Mobile Agent

ICM 7.1(1) introduces support for Contact Center agents working remotely. This feature makes it possible for ICM/IPCC Enterprise to support agents using phones not directly controlled by ICM/IPCC Enterprise. This could be an agent:

- Outside the contact center, calling from an analog phone at home or a cell phone.
- Inside the contact center, calling from an IP phone connected to a PBX not controlled by Unified CCE or an associated CallManager.

For more information see the *Cisco Unified Mobile Agent Guide for Unified CCE*.

## ECC Variable Persistence Selection

Release 7.1(1) introduces support for setting the persistent or non-persistent nature of Expanded Call Context (ECC) Variables. When configuring ECC Variables in the ICM Configuration Manager (**Tools > List Tools > Expanded Call Variable List**) there is now a checkbox labeled **Persistent**. When this checkbox is selected, the ECC Variable data is written to the Logger Database.

This feature allows you to decrease the load on the database by selecting only those variables that you require to be persistent across restarts and at the end of a call. Non-persistent variables are held in memory and their value is cleared at the completion of the call.

Persistent ECC variables are known as "Call Variables" in System IPCC and are configurable in the System IPCC Web Administration tool. They are configured there under **Contact Management > Call Variables**.

After the upgrade to Release 7.1(1), all ECC variables from the Release 7.0(0) installation are marked as persistent. ECC Variables created after the upgrade to Release 7.1(1) are not persistent by default. New ECC Variables created in Release 7.1(1) can be made persistent using the methods described above.

## Support Tools Node Agent Automatically Installed

When the Release 7.1(1) Installer is invoked, it in turn invokes the Support Tools Node Agent installer in a silent mode, causing the Node Agent to be installed on the server.

This feature makes the process of deploying Support Tools easier.

Support Tools version 2.0(1) is backwards compatible with Support Tools Server 1.0(1). However, to get the full functionality of the 2.0(1) Support Tools Node Agent you must also upgrade your Support Tools Server to version 2.0.

**Note** Although the Support Tools Node Agent is installed, it is not started, unless subsequently configured to do so.

## Support for InstallShield Silent Installation

This release includes support for Installshield's Silent Install mode. Silent Install allows automated installation of software without the need for user input, based on configuration files. See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* for details.

**Note** Silent Install support applies to the 7.1(1) installers for ICM/IPCC and CTI OS only; Silent Install is not supported with CAD 7.1(1).

## System IPCC Localization Support

The prior Release 7.0(0) System IPCC restriction on English-only localization has been lifted and there is now installation support for full local language selection. All languages available to the ICM are now available on System IPCC platforms.

## Support for Cisco CVP NetworkVRU Type 10

Release 7.1(1) supports a new NetworkVRU, known as Type 10. Type 10 is designed to simplify the configuration requirements in Cisco Customer Voice Portal (CVP) Comprehensive Model deployments. It can be used for:

- calls which originate from a TDM VRU or ACD and need to be transferred to CVP for self service or queuing; and
- calls which originate from an IPCC Call Manager and need to be transferred to CVP for self service or queuing.

The Type 10 NetworkVRU has the following behaviors:

- There is a Handoff of routing client responsibilities to the CVP switch leg;
- There is an automatic transfer to the CVP VRU leg, making for a second transfer in the case of VRU, ACD or Call Manager originated calls;
- For CallManager originated calls, the correlation-id transfer mechanism is used; the correlation-id is automatically added to the end of the transfer label defined in the Type 10 NetworkVRU configuration;
- The final transfer to the CVP VRU leg is similar to a Type 7 transfer, in that a RELEASE message will be sent to the VRU prior to any subsequent transfer.

In CVP implementations, a single Type 10 NetworkVRU should be defined, and all CVP Micro-application scripts should be associated with it. It requires one label for the CVP Switch leg routing client, which transfers the call to the CVP VRU leg. If calls are transferred to CVP from Call Manager, it also needs another label for the Call Manager routing client. That label transfers the call to the CVP Switch leg. The ICM Router sends that label to Call Manager with a correlation-id concatenated to it. Call Manager must be configured to tolerate these arbitrary extra digits.

The CVP Switch leg peripheral should be configured to point to the same Type 10 NetworkVRU. Also, all incoming dialed numbers for calls which are to be transferred to CVP should be associated with a Customer Instance which points to the same Type 10 NetworkVRU.

For calls which originate at a Call Routing Interface VRU or at a TDM ACD, a TranslationRouteToVRU node should be used to transfer the call to CVP's Switch leg peripheral. For all other calls, a SendToVRU node should be used, or a node which contains automatic SendToVRU behavior, such as the queuing nodes, or RunExternalScript.

If you plan to use blind transfer with Cisco Unified CallManager 5.0, the following configuration changes need to be made:

- Uncheck the "Wait for Far End H.245 Terminal Capability Set" parameter in CCMAdmin for the CVP gateway device.

- Change the value of the CCM H323 Service Parameter called "Send H225 User Info Message" to the value "H225 Info for Call Progress".

### ICM ID Finder Tool Enhancements

In Release 7.1(1), the ICM ID Finder tool is enhanced to provide the ICM application path of the component ID. Documentation is now available on use of the tool. See ICM ID Finder Tool, page 23.

## Installation

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* for information on how to plan for and deploy release 7.1(1), including information on agent desktop and PG software versions supported during 7.1(1) migration.

**Note** The Install Guide instructs you to stop CSA during the installation. If the confirmation dialog is not displayed when attempting to stop the CSA service on a machine that has had users logged into it via a session of Remote Desktop Connection, the CSA service can not be stopped. The Installer appears to be hung while displaying the "Stopping CSA" dialog. Use the Task Manager to disconnect and logoff any users that are currently, or have previously been, connected to the system. Before attempting to stop CSA again, either allow the initial request to stop CSA to timeout, or reboot the system.

### System IPCC

For System IPCC, any servers with the following roles must use the same release of software (for example, Release 7.1(1)):

- Central Controller
- Administration & WebView Reporting
- Outbound Controller

For example, if you upgrade your Central Controller servers to Release 7.1(1), then you must upgrade your Administration & WebView Reporting servers and Outbound Controller servers to Release 7.1(1) as well. We also strongly encourage customers to keep their machines with "Agent/IVR Controller" roles (these servers have the IPCC System PG, CTIOS Server and CTI Server) at the same version as the Central Controller if they are on a separate server.

Also, if after installing Release 7.1(1) you decide to roll back to Release 7.0(0), you do not need to delete any System IPCC machines from the database (using the Web Administration tool under *System Management* > *Machine Management* > *Machines*) unless you intend to uninstall Release 7.0(0) as well.

See *Chapter 15* of the *System IPCC Enterprise Installation and Configuration Guide* for information on the install and uninstall of System IPCC.

## Reporting

ICM/IPCC reporting documentation has been expanded for release 7.1(1), and includes the creation of a new *Reporting Guide for Cisco Unified ICM Enterprise & Hosted.*

There are no new reports for Release 7.1(1). However, selected existing reports have been modified to support Mobile Agent reporting. The affected reports are listed below. See the *Mobile Agent Guide for Cisco Unified CC Enterprise* for more information on Mobile Agent reporting support.

Changes have been made to the following reports to reflect additional columns for Mobile Agent (data for these fields is available for IPCC systems only):

- Agent20
- Agtper20
- Agtskg30
- Agteam20
- All Agent Real Time All Fields Reports: agent28, agtper28, agtskg28, agteam28
- Agent03
- Agtper03
- Agteam03

# Technical Changes and Notes

The following changes in Release 7.1(1) are generally of a more technical nature than those above.

- New MDS scalability enhancements consisting of scheduling improvements and the default deferral of the internal peer health sanity message are included in this release.
- The JDK and JRE used in ICM 7.1(1) are updated to JDK1.4.2_10 and JRE 1.4.2_10 respectively. The Release 7.1(1) installer installs the new version of JDK and JRE wherever necessary.
- The Import/Export functionality of the ICMDBA utility has been modified to pertain to ICM Configuration data only. To import or export ICM Historical data, users should use Microsoft SQL Server's Database Backup and Database Restore utilities.
- Release 7.1(1) introduces support for redirect interface for outbound option to reduce the time required to set up IPCC consultative transfer to connect agents to customers. In laboratory conditions, the improvement is about 200 milliseconds.
- In Release 7.0(0), the Contact Center SNMP infrastructure was installed on a PG (but not enabled) if CRS was also installed on the PG. This was due to incompatibilities with the CRS sysappl agent. In this situation, Windows SNMP continued to be used to provide SNMP management and represented the shared PG as a CRS only node to SNMP management stations. With release 7.1(1), the Contact Center SNMP infrastructure is enabled if Release 4.6 or greater of CRS is installed on the PG, thus replacing the Windows SNMP infrastructure and providing instrumentation for both the CRS and ICM PG components. SysAppl MIB data continues to be returned by the CRS sysAppl extension agent, not the Contact Center sysAppl agent. Since Release 4.6 of CRS is not yet available, there will be no change to the existing behavior when Release 7.1(1) is installed. However, if CRS is upgraded to Release 4.6 at a later date, the Cisco Contact Center SNMP Management service can be restarted enabling the Contact Center SNMP infrastructure.
- The Queue Node with the ConsiderIf clause was modified to provide improved routing control. This improvement changes the behavior of the queue node when ConsiderIf evaluates to false. If false, and the call is already queued to the target, the call will be dequeued from the target. Formerly, the call was left queued to the target.

- Closed variables have been added for Skill Groups, Peripherals, and Media Routing Domains. This allows administration scripts to turn dequeuing to these objects on and off. The Closed variables default to 0, meaning that the object is open. A script (usually an administration script) can change the state of the Closed variables. If a Closed flag is set to a non-zero integer, then calls will not be dequeued to affected agents, regardless of their state.
- An enhancement has been made to scripting for Outbound Option which allows for the evaluation of the ECC variable "BAResponse", which carries the CPA result of the customer call. Two new IF node configurations are supported:
  - Call.BAResponse="CPA_AnswerMachine"
  - Call.BAResponse="CPA_Voice"

  These IF nodes route to separate External Scripts to allow for different treatment depending on whether voice or an answering machine was detected.
- An enhancement was made to ICMDBA to allow it to better calculate the database size relevant to ECC variables

# ICM Database Schema Changes, Release 7.0(0) to Release 7.1(1)

This section indicates the changes made to the ICM/IPCC Database Schema between Release 7.0(0) and Release 7.1(1). Refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions* for descriptions of the new tables and columns.

The changes to the database schema are made atop of Release 7.0(0), as part of the Release 7.1(1) installer. The EDMT utility is not used for the Release 7.0(0) to Release 7.1(1) upgrade process.

Database changes from Release 7.0(0) to Release 7.1(1) can be rolled back.

## New Fields in Existing Tables:

- Agent_Desk_Settings.RemoteAgentType
- Agent_Desk_Settings.RemoteLoginWithoutDesktop
- Agent_Real_Time.PhoneType
- Agent_Real_Time.RemotePhoneNumber
- Agent_Logout.PhoneType
- Agent_Logout.RemotePhoneNumber
- Call_Type_Half_Hour – addition of 5 fields "Reserved1' – "Reserved5'
- Changed field description in existing table: Expanded_Call_Variable.Persistent description changed to indicate that this is now configurable.

## New Tables listed but not detailed, and noted as 'reserved for future use':

- Agent_Targeting_Rule
- Agent_Targeting_Rule_Member
- Agent_Targeting_Rule_Range
- Agent_Targeting_Rule_Member table
- Agent_Targeting_Rule_Range table

### Additional Database Table Changes

The following changes to the database have occurred:

- Updates to initial data have changed for the *Region* and *Region_Prefix* tables.

# Installation Notes

This section provides important information to be read before installing the Release 7.1(1) update. For additional installation notes see the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).*

## WebView User Information May be Lost

Local WebView user information may be lost during setup on an AW or Logger if the domain controller is unavailable. Verify that the domain controller is available from the server before installing Release 7.1(1). For complete details see the following caveat in Bug Toolkit: CSCse61084

## WebView Favorite, Private and Scheduled Reports May be Lost

WebView favorite, private and scheduled reports may be lost if the NetBIOS domain is different from the Active Directory Domain name. This could happen after upgrading from an NT domain to an Active Directory Domain and changing domain names, but leaving NetBIOS domain at old name. For more details see the following caveat in Bug Toolkit: CSCse50977

# Limitations and Restrictions

Limitations and Restrictions are provided in the following documents:

- The *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0)* available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html
- The *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, updated for Release 7.1(1), available from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm
- The *Software Compatibility Guide for Cisco IPCC Enterprise Edition*, available from: http://cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html
- The *Cisco Unified Mobile Agent Guide for Unified CCE* provides information on limitations in the Mobile Agent feature.
- The *IPCC Solution Reference Network Design (SRND) for Cisco IPCC Enterprise Edition* (Updated for Release 7.1(1)) provides additional limitations and restrictions.

Release 7.1(1) is a cumulative update and may rectify restrictions as documented in the ICM Release 7.0(0) Release Notes.

## Mobile Agent Limitations and Restrictions

In addition to the limitations and restrictions noted in the documents above, the Mobile Agent feature in Release 7.1(1) has the following additional limitations and restrictions:

- Web Callback is not supported for Mobile Agent
- Blended Collaboration is not supported for Mobile Agent

# Important Notes

The following sections contain restrictions that apply to Release 7.1(1):

- Mobile Agent Scalability may be contingent on specific CallManager versions, see the *IPCC Solution Reference Network Design (SRND) for Cisco IPCC Enterprise Edition* for Release 7.1(1) for details.
- Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender, and Cisco Email Manager remain at the Release 5.0 version of their respective products, however, compatibility with these products and Release 7.1(1) has been maintained.

**Note** Limitations ("no more than *N* connections can be made to ...") and scalability ("up to x agents can ...") are discussed in the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*.

# Resolved Caveats in This Release

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.

# Caveats

## Open Caveats in This Release

This section contains a list of defects that are currently pending in ICM/IPCC Enterprise and Hosted Editions 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 ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*

| Identifier | Component | Sev | Headline |
|---|---|---|---|
| CSCse50977 | aw.config.list | 2 | WebView favorite, private and scheduled reports lost w/ upgrade to 7.0 |
| CSCsc49512 | aw.config.list | 2 | User List Tool and Agent Explorer tool are slow to display users |
| CSCsb94170 | cti.international | 2 | CHN: CTIOS Agent and Supervisor Desktops Chinese Labels are Wrong |
| CSCsa65256 | ctios.server | 2 | Possible Memory Leak in CtiosServerNode |
| CSCse05675 | nic.crsp | 2 | CRSPNicV3 fails to send ECC data |
| CSCsd86139 | patch | 2 | Silent patch install can cause incomplete installation |
| CSCse40573 | pg.acmi | 2 | Enabling tracing delays IPCC Express Gateway failover. |
| CSCse46690 | pg.aspect | 2 | CTI Soft phone fails when RONA occurs on Aspect ACD |
| CSCse57091 | pg.definity | 2 | PIM crashes in 'checkcall' generating DR.WTSN log |
| CSCse48237 | pg.dms100 | 2 | In 3 Way Conf Scenario, One Party Drops and OPC Kills Rest of Call Legs |
| CSCsd95261 | pg.dms100 | 2 | DMS100 PIM PIM Asserts in RemoveConfigAgent function |
| CSCse26993 | pg.siemens-rolm | 2 | No monitor data calls/agents at times when PIM failover |
| CSCse11534 | pg.siemens-rolm | 2 | PIMs bouncing btwn PGs and CallBridge Servers |
| CSCsd59723 | security | 2 | User created through user list tool unable to open configuration manager |
| CSCse44161 | setup.webview.ICM | 2 | ICM Setup fails to set Jaguar Service Account correctly |
| CSCsd97211 | aw | 3 | Cisco ICM Services set to automatically start intermitently Do Not Start |
| CSCsb38949 | aw.config | 3 | ICM Instance selection Fault with Bulk Edit and Insertion Tools |
| CSCse25560 | ba.campaignmgr | 3 | Dialer may not attempt to contact a customer if Agents Skip or Reject |
| CSCsd83454 | ba.campaignmgr | 3 | CampaignManager restarts when retrieving more than 17 personal callbacks |
| CSCse48445 | ba.dialer.ipcc | 3 | When Campaign is halted, records are incorrectly set to state C. |
| CSCse20091 | ba.dialer.ipcc | 3 | Dialer sets incorrect call result if customer hangs up during transfer |
| CSCse21575 | ba.dialer.ipcc | 3 | Reservation call to Agent not released after transfer to IVR upon AMD |
| CSCse00026 | ba.dialer.ipcc | 3 | Customer abandoned call during CPA is reported as Cancel |

*Table 1 Open Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*

| Identifier | Component | Sev | Headline |
|---|---|---|---|
| CSCsd99414 | cti.commonitor | 3 | When agt logs off softphone incorrectly, stay in not ready and logged in |
| CSCse33335 | ctios.ctidriver | 3 | CTIOS Driver - Same InvokeID for seperate items |
| CSCse22553 | ctios.ctiosclient | 3 | CTIOS Desktop Agent grays out all buttons after hang up from conference |
| CSCse22916 | ctios.server | 3 | AgentName Lookup failed messages on CTIOSServer startup |
| CSCsd84306 | ctios.softphone | 3 | Agent desk setting for screen not picked up with toolkit phone |
| CSCsb90386 | db.distributor.realtime.feed | 3 | Some Skill Group Real Time Webview reports are lagging / not updating |
| CSCsc62164 | db.icmdba | 3 | ICMDBA Space Used fails on non-English system |
| CSCsc24521 | db.icmdba | 3 | ICMDBA estimator unable to connect via router private address |
| CSCsd29061 | documentation | 3 | Agent in talking state are set to NOT READY after System PG Failover |
| CSCse31894 | inetscripted | 3 | scripts using custom functions reload cannot be modified - diff char set |
| CSCse00353 | ipccwebconfig-ui | 3 | It is unclear how to log in Supervisors to the Web Reskilling tool |
| CSCsd98386 | mds.synchronizer | 3 | Router should promote the most viable Router/Logger pair to active |
| CSCse16836 | nic.icrp | 3 | ICRPnic - CLI Presentation Restricted Indicator is not set by NIC |
| CSCse09642 | nic.ss7innic | 3 | SS7InNic does not properly report Abandon or Disconnect for Leg 1 |
| CSCsd81830 | pg.definity | 3 | PIM not updating trunk grp info to OPC when C_OFFERED missing from Avaya |
| CSCse09232 | pg.eapim | 3 | Skillgroup change doesn't update in Team Real-Time Status for Voice |
| CSCse03974 | pg.neax2400 | 3 | NEC: Newcall/makecall button is disabled |
| CSCse17532 | pg.opc | 3 | Call Variables are not being propagated when using dynamic label |
| CSCsd44013 | pg.opc | 3 | Incorrect Skill Group Assignment after Removing all skills |
| CSCsd75775 | pg.symp | 3 | Symposium PIM error : send_hdx_response: (HDX Error 9) Undefined error |
| CSCse07235 | pg.symp.noseipim | 3 | PIM should retrieve the SkillGroup update set against the Agent |
| CSCsb14877 | pg.vru | 3 | OriginatorType value of 70 appeared in RCD, which should be 0 - 4. |
| CSCse34160 | reporting.webview | 3 | WV reports exported in binary formats (Excel, Dbase...) are corrupted |
| CSCsd79524 | reporting.webview | 3 | Webview Session Timeout Message Incorrect |
| CSCsd75781 | reporting.webview | 3 | WV 'Schedule' category still present if Outbound Opt is not installed |
| CSCsd76723 | reporting.webview | 3 | Periph06:Peripheral Summary not the max calls in progress during period |
| CSCse53569 | router | 3 | router.exe crash |
| CSCse40918 | router | 3 | Need to have router call key, ANI and such details to appear in RT logs |
| CSCse54362 | scripteditor | 3 | JPN: calltracer dialog cut |
| CSCse36468 | scripteditor | 3 | User Variables with Data Type of long evaluates true for characters |
| CSCsd84862 | setup.aw | 3 | Local Setup fails on Limited AW system. |
| CSCsd88706 | sys.nodemanager | 3 | disable Global Performance Monitoring from NM |
| CSCsd02557 | tools | 3 | Support Tool Node Install does not accept Hostname but IP |
| CSCsd02569 | tools | 3 | PG Registry Compare shows A and B separately instead of merging A and B |

*Table 1 Open Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*

| Identifier | Component | Sev | Headline |
|---|---|---|---|
| CSCsd70051 | tools | 3 | Log collection does not compensate for GMT time difference |
| CSCsd17650 | user-interface | 3 | Dashboard does not load after install |
| CSCse50977 | aw.config.list | 2 | WebView favorite, private and scheduled reports lost w/ upgrade to 7.0 |
| CSCsd93156 | setup | 2 | Services fail to start due to login failures after setup finishes |
| CSCse55800 | setup | 2 | Cannot replicate configuration changes from NAM to CICM |
| CSCse61084 | db.upgrade.edmt | 3 | Migrate Users called unnecessarily and could lose user information |
| CSCse56970 | documentation | 3 | Login Fails if Agent wise Desk Setting is not assigned |

# Troubleshooting

Troubleshooting information is available in the product documentation. Additional troubleshooting tips appear below:

## Setup Troubleshooting

### Finding the Release 7.1(1) log

The Release 7.1(1) Installer's setup log is in the following folder on the system drive. (All examples assume system drive is C:). Example: C:\temp\Minor Release ICM7.1(1)

- New log files are created each time the installer is run, with unique IDs of format YYYYMMDDHHMM, is pre-pended to the file name "_Minor Release ICM7.1(1).log". Example: *20060404_112338_Minor Release ICM7.1(1).log*
- JDK/JRE installation logs are embedded within the Minor Release installer's log.
- Support Tools setup log is created or appended to existing log file. Example: *C:\temp\ICM_SupportTools_Setup.log*
- Schema Upgrade/rollback logs. Example: *C:\temp\<server name><instance name><DB name>.log*

### error -9934

**Symptom:** On a AW Client only system, running Configuration Manager may display the error "-9934. Unable to initialize real-time feed for instance."

**Reason:** The real-time feed error is caused by ICM7.0FCS real-time distributor which has not been applied with 7.1(1) release.

**Solution:** Make sure the Release 7.1(1) is applied on the Distributor, Call Router and the Logger, then bring up the Call Router, Logger, and Distributor services.

### Failure to stop Tomcat service

**Symptom:** During the Release 7.1(1) installation or uninstallation, installer attempts to stop the Apache Tomcat Service, if it is running. On some systems, the installer may report a failure to stop the service, and abort the installation.

**Reason:** When stopping service reports error, before passing error on the installer goes into a loop to test for a file lock on tomcat5.exe. It does retries at 5 sec intervals for 3 minutes. If lock does not release in 3 minutes, then error gets passed on.

**Solution:** Go to the system's "Services" console, and manually stop the Tomcat service. Restart the installer.

### Error in log: Failure stopping Jaguar Watchdog

**Symptom:** During the minor release installation or removal, setup automatically stops the Jaguar Watchdog Service. Occasionally, an error message is written to the setup log that stopping the service failed. The installer continues to run.

**Solution:** Look in the Services window to find out if the service is running or not.

### File lock error message

**Symptom:** If an ICM application is running when the installer starts (Script Editor, for example) the operating system applies a lock to files loaded into memory, blocking the update of those files. The installer will abort, explain that an ICM application is currently running, and list the locked files.

**Reason:** Launching install or uninstall without stopping ICM non-service programs. (Note that running ICM services are automatically stopped and will not lead to this message.)

**Solution:** Stop all ICM programs before installing or uninstalling the minor release. If you can't find a running application, try looking for the locked file as a process in Task Manager, and shut it down there.

## Database

### Incompatible Schema Versions

**Symptoms:**

- Logger displays "Major Version Mismatch!"
- You can not run ICM 7.0 with a database schema from ICM 7.1.

**Reason:** This can happen after a temporary uninstall (without schema downgrade), and then running ICM services

**Solution:** Reinstall ICM 7.1(1)

**Note** If you wish to go back to running ICM 7.0(0), you must perform a **permanent** uninstall (with schema rollback).

### Incompatible Schema Versions (other)

**Symptoms:** Logger displays "The sideX Logger cannot come online duplexed because its database is out of date." (sideA or sideB)

**Reason:** This can happen when only one side of a duplexed system is upgraded. Loggers sideA and sideB must be at the same ICM versions

**Solution:** Follow steps outlined in ICM 7.1 Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)

## Recommended Trace setting for Troubleshooting IPCC

The latest up-to-date recommended trace settings for troubleshooting in your IP Contact Center (IPCC) environment can be found on the web at: *http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_tech_note09186a0080094b22.shtml*.

## Mobile Agent

### Additional Trace Levels for Mobile Agent

Additional trace levels for troubleshooting Mobile Agent, in addition to those referenced in the previous section, are provided below:

**JTAPI Gateway:**

There is no separate trace mask for Mobile Agent. To enable trace for Mobile Agent, the following traces can be enabled as needed.

- Procmon <customer instance name> <nodename> jgw<#>
- >>>>trace JT_TPREQUESTS /on
- >>>>trace JT_CONNECTION /on
- >>>>trace JT_MEMORY /on

**EAGTPIM**:

There is no separate trace mask for Mobile Agent. The existing tele_drive_OP_ERR bit is turned on using default trace level.

**CTIOS, CTISever, OPC**:

There is no additional trace mask for Mobile Agent.

### General Mobile Agent Troubleshooting

**Condition:** The user has configured the mobile agent option within the ICM Agent Desk settings page. However the Agent Desktop softphone application does not display any fields on the login dialog for the agent to log in as a mobile agent.

**Problem:** The CTIOS Server was not set up properly during install or the connection profiles defined in the registry are not defined correctly for Mobile Agents. The ShowFieldBitmask value needs to be defined in the connection profile for the appropriate mobile agent settings.

The CTIOS Server connection profiles sent to the CTIOS client desktop contains the information for ShowFieldBitmask which controls what fields are displayed on the login dialog.

**Recommended Action:** Rerun the CTIOS Server setup program, on the Peripheral dialog screen select the Mobile Agent option and the appropriate work mode. The registry is automatically updated with the appropriate values when the CTIOS Server setup program is run.

---

**Condition:** The agent is unable to select a call mode on the login dialog. The call mode field is disabled and set to either call-by-call or nailed connection without the option to change it.

**Problem:** The agent work mode needs to be set to "agent chooses" in order to be able to select the agent call mode.

**Recommended Action:** Rerun the CTIOS Server setup program and select "agent chooses" as the agent work mode on the Peripheral Identifier screen. Mobile Agent also needs to be selected in order to select the call mode. The registry is automatically updated with the appropriate values when the CTIOS Server setup program is run.

---

**Condition:** Call-by-call delivery to mobile agent fails and agent is logged out

**Problem:** Agent call cannot connect due to an invalid phone number.

**Recommended Action:** Check to make sure mobile agent phone number is entered correctly in the phone number field of the agent login UI before logging back in.

---

**Condition:** Call-by-call delivery to mobile agent fails and agent is set to not ready

**Problem:** Agent call cannot connect due to mobile agent phone line busy.

**Recommended Action:** Check agent phone line and make sure line is available.

---

**Conditions:**

- Nailed connection log in fails, AND "ConnFailedEv with cause of RESOURCE_NOT_AVAILABLE" in the JGW log, OR
- Call-by-call Mobile Agent call fails, AND "ConnFailedEv with cause of RESOURCE_NOT_AVAILABLE" in the JGW log

**Problem:** Call cannot connect due to codec mismatch.

**Recommended Action:** Check corresponding voice gateway codec configuration to match the codec setup in PG

---

**Condition:** Login failed: IPCC Error [10151] You haven't configured or have misconfigured the LCP Port on CCM Admin. Login denies. Invalid or missing LCP Port.

**Problem:** Unable to log into device due to an incorrect LCP configuration in CCM.

**Recommended Action:** Check the phone configuration page in CCM. Make sure that the device name of the LCP port starts with "LCP"

---

**Condition:** Login failed: IPCC Error [10152] You haven't configured or misconfigured the RCP Port on CCM Admin. Login Denied. Invalid or missing RCP Port.

**Problem:** Unable to log into a device due to an incorrect RCP configuration in CCM.

**Recommended Action:** Check the phone configuration page in CCM. Make sure that the device name of the RCP port starts with "RCP" and also check the device name of the corresponding LCP port.

---

**Condition:** Login failed: IPCC Error [10153] Mobile agent mode doesn't match the agent desk settings. Login Denied. Mobile agent mode is not allowed.

**Problem:** The agent's desk setting is not configured properly. Either mobile agent is not enabled or the agent work mode does not correspond to the agent call mode selected in the login dialog.

**Recommended Action:** Enable the mobile agent setting in the agent's desk setting. Verify that the agent mode configured in the agent's desk setting is the same as the agent call mode selected in the login dialog.

---

**Condition:** Login failed: IPCC Error [10154] Try to log in CTI PORT device for non-mobile agent or invalid CTI PORT for mobile agent. Login Denied. Agent is not allowed due to incorrect device.

**Problem:** A local agent is not allowed to log into a CTI port. Or if an invalid CTI port is used for login by a mobile agent.

**Recommended Action:** For a local agent, enter the agent's IP phone extension in the "instrument" field of CTI Login dialog box. For a mobile agent, check the CTI port configuration.

## Samples of Mobile Agent Log Content

Agent login - When a mobile agent with agentID:2025 and remote phone number:2090 logs in using assigned local CTI port:5000, the "AgentInstrument" field will contain "5000;2090":

```
16:18:23 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0xa0a5 PeripheralID:5000
AgentState:LOGIN
16:18:23 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0 EventReasonCode:0
16:18:23 SESSION 1: AgentInstrument:"5000;2090" AgentID:"2025" AgentPassword:"2025" )
```

---

An agent event is sent to the agent desktop. The "AgentInstrument" field in all subsequent agent events for that mobile agent with agentID:2025 has 5000 (aka, local CTI Port) as AgentExtension and AgentInstrument:

```
16:18:28 SESSION 1: MsgType:AGENT_STATE_EVENT (MonitorID:0 PeripheralID:5000 SessionID:0x0
16:18:28 SESSION 1: PeripheralType:EnterpriseAgent SkillGroupState:LOGIN StateDuration:0
16:18:28 SESSION 1: SkillGroupNumber:9577 SkillGroupID:5000 SkillGroupPriority:0
AgentState:NOT_READY
16:18:28 SESSION 1: EventReasonCode:0 MRDID:1 NumTasks:0 AgentMode:0 MaxTaskLimit:0
ICMAgentID:13910
16:18:28 SESSION 1: AgetAvailabilityStatus:0 ClientSignature:"CTIOSServer" AgentID:"2025"
16:18:28 SESSION 1: AgentExtension:"5000" AgentInstrument:"5000" )
```

---

Failed agent login - Try to log in a mobile agent (cti port=5001, remote phone=3000, agentID=74003) and agent's desk setting is set to Mobile Agent, but CTI Port Name for 5001 in CCM does not start with "LCP". Peripheral Error Code: PERERR_TELDRIVE_MOBILEAGENT_INCORRECT_LCP=10151:

```
11:19:54 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0x6e78 PeripheralID:5000
AgentState:LOGIN
```

```
11:19:54 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0
EventReasonCode:50004 ForcedFlag:0
11:19:54 SESSION 1: AgentInstrument:"5001;3000" AgentID:"74003" )
11:19:54 Trace: ProcessSetAgentStateRequest - sessionID 1
11:19:54 Trace: *** AddToAssociateAgentList(); ADDED: SessionID=1 AgentID=74003
PeripheralID=5000
11:19:54 Trace: CSTASetAgentState - InvokeID=0x2a00f71b
     Device=5001;3000 AgentMode=LOG_IN AgentID=74003
     AgentGroup=-1(0xffffffff) AgentPassword=)
11:19:54 Trace: PrivateData - EventReasonCode=50004 WorkMode=0 NumAdditionalGroups=0
               PositionID= SupervisorID= ClientAddress=
11:19:54 Trace:
11:19:54 Trace: DEVICE_TARGET_OTS_IND - Instrument= Out-Of-Service NetworkTargetID=-1
11:19:54 SESSION 1: MsgType:SYSTEM_EVENT (PGStatus:NORMAL CCTimestamp:0x43d2e9e5 (01/21/06
21:11:49)
11:19:54 SESSION 1: SystemEventID:Agent Instrument Out-of-Service SystemEventArg1:0x1388
11:19:54 SESSION 1: SystemEventArg2:0xffffffff SystemEventArg3:0x0
EventDeviceType:DEVID_NONE )
11:19:54 Trace:
11:19:54 Trace: CSTAUniversalFailureConfEvent - InvokeID=0x2a00f71b
     Error=GENERIC_UNSPECIFIED_REJECTION
11:19:54 Trace:      PRIVATE_DATA - PeripheralErrorCode=0x27a7(10151)
11:19:54 SESSION 1: MsgType:CONTROL_FAILURE_CONF (InvokeID:0x6e78
FailureCode:CF_GENERIC_UNSPECIFIED_REJECTION
11:19:54 SESSION 1: PeripheralErrorCode:10151 )
```

---

Failed agent login - Try to log in a mobile agent (cti port=5001, remote phone=3000, agentID=74000) while agent's desk setting is not enabled for Mobile Agent. Peripheral Error Code: PERERR_TELDRIVE_MOBILEAGENT_MODE_NOT_ALLOWED=10153:

```
11:12:53 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0x6dd4 PeripheralID:5000
AgentState:LOGIN
11:12:53 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0
EventReasonCode:50004 ForcedFlag:0
11:12:53 SESSION 1: AgentInstrument:"5001;3000" AgentID:"74000" )
11:12:53 Trace: ProcessSetAgentStateRequest - sessionID 1
11:12:53 Trace: *** AddToAssociateAgentList(); ADDED: SessionID=1 AgentID=74000
PeripheralID=5000
11:12:53 Trace: CSTASetAgentState - InvokeID=0x2a00f6ad
     Device=5001;3000 AgentMode=LOG_IN AgentID=74000
     AgentGroup=-1(0xffffffff) AgentPassword=)
11:12:53 Trace: PrivateData - EventReasonCode=50004 WorkMode=0 NumAdditionalGroups=0
               PositionID= SupervisorID= ClientAddress=
11:12:53 Trace:
11:12:53 Trace: CSTAUniversalFailureConfEvent - InvokeID=0x2a00f6ad
     Error=GENERIC_OPERATION_REJECTION
11:12:53 Trace:      PRIVATE_DATA - PeripheralErrorCode=0x27a9(10153)
11:12:53 SESSION 1: MsgType:CONTROL_FAILURE_CONF (InvokeID:0x6dd4
FailureCode:CF_GENERIC_OPERATION_REJECTION
```

```
11:12:53 SESSION 1: PeripheralErrorCode:10153 )
```

Mobile agent transitions to Available state - Mobile agent with agentID:2025 and remote phone number:2090 logged in using local CTI port(5000) sends a request to change its agent state to AS_AVAILABLE.

```
16:18:30 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0xa0bb PeripheralID:5000
AgentState:AVAILABLE
16:18:30 SESSION 1: AgentWorkMode:RA_CALL_BY_CALL NumSkillGroups:0 EventReasonCode:0
AgentInstrument:"5000"
16:18:30 SESSION 1: AgentID:"2025" )
```

An agent event is sent to the agent desktop. Agent event has local CTI Port (5000) as AgentExtension and AgentInstrument.

```
16:18:30 SESSION 1: MsgType:AGENT_STATE_EVENT (MonitorID:0 PeripheralID:5000 SessionID:0x0
16:18:30 SESSION 1: PeripheralType:EnterpriseAgent SkillGroupState:AVAILABLE
StateDuration:0
16:18:30 SESSION 1: SkillGroupNumber:9577 SkillGroupID:5000 SkillGroupPriority:0
AgentState:AVAILABLE
16:18:30 SESSION 1: EventReasonCode:0 MRDID:1 NumTasks:0 AgentMode:1 MaxTaskLimit:1
ICMAgentID:13910
16:18:30 SESSION 1: AgentAvailabilityStatus:1 ClientSignature:"CTIOSServer" AgentID:"2025"
16:18:30 SESSION 1: AgentExtension:"5000" AgentInstrument:"5000" )
```

**Note** If a mobile agent is configured to use nailed connection, disconnecting the nailed connection call causes agent state to transition to AS_LOGGED_OUT.

# Documentation Updates

This section discusses changes and additions to the ICM/IPPC Enterprise and Hosted Editions software documentation set.

## Documentation Availability

The following documentation for ICM/IPCC Enterprise and Hosted Editions Release 7.1(1) is available from the following sources:

- Documentation for ICM/IPCC Enterprise and Hosted Editions (excluding System IPCC, CAD, and CTI OS) is available on the Cisco ICM/IPCC Release 7.1(1) Documentation CD.
- Documentation for System IPCC Enterprise Release 7.1(1) is available on the System IPCC Enterprise Release 7.1(1) product software CD.
- Documentation for CTI OS Release 7.1(1) is available on the CTI OS Release 7.1(1) product software CD.
- Documentation for CAD Release 7.1(1) is available on the CAD Release 7.1(1) product software CD.

**Note** All of the above documentation, plus additional titles, is available for download from cisco.com at: http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

The Cisco ICM/IPCC Release 7.1(1) documentation CD and the System IPCC Enterprise Release 7.1(1) product CD contain both Release 7.1(1) and 7.0(0) documentation as follows:

- Documents labeled as 7.1(1) include information that is new and specific to Release 7.1(1)
- Documents labeled as 7.0(0) include no new information specific to Release 7.1(1) and apply equally to both 7.0(0) and 7.1(1) releases.
- In instances where a 7.1(1) document has superseded its 7.0(0) predecessor, the 7.1(1) version is provided.

# Additional Documentation

This section contains new documentation that may not be available in the documentation set at the time of release.


- Enabling Mobile Agent in System IPCC, page 22
- Outbound Option: Disabling Ringback During Transfer to Agent, page 22
- ICM ID Finder Tool, page 23


## Enabling Mobile Agent in System IPCC

The online help page for configuring mobile agent in System IPCC mentions the need to check the 'Enable Cisco Unified Mobile Agent' check box in the 'Edit Desk Setting' page and choose the 'Mobile agent mode' from the drop down box.

However, it does not mention that you then need to re-run the CTI OS Server setup.

If CTI OS Server setup is not re-run at the end of the procedure currently described in the online help, Mobile Agent will not be enabled.

For a discussion of CTI OS Server setup and Mobile Agent, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Edition, Release 7.2(1).*

## Outbound Option: Disabling Ringback During Transfer to Agent

In order that customers not hear a ringback tone while a call is being transferred to an agent, configure as follows:

**Step 1** Log into the CallManager Administration window

**Step 2** Access Service Parameters for CallManager

**Step 3** Change "Send H225 User Info Message* " = "Use ANN for Ringback"

**Step 4** Click **Update**

**Step 5** Access Service Parameters for Cisco IP Voice Media Streaming Application

**Step 6** Change, under "Annunciator (ANN) Parameters", "Run Flag" = "False"

**Step 7** Click **Update**

## ICM ID Finder Tool

Release 7.1(1) introduces additional support for the ICM ID Finder Tool.

### About the ICM ID Finder Tool

The ICM ID Finder is a tool that allows configuration managers and administrators to find the various configuration IDs of the following ICM components:

- Agent
- Label
- NIC
- Peripheral
- PG
- Physical Interface Controller
- Routing Client
- Service
- Service array
- Skill group
- Skill targets
- Translation route
- Application Path

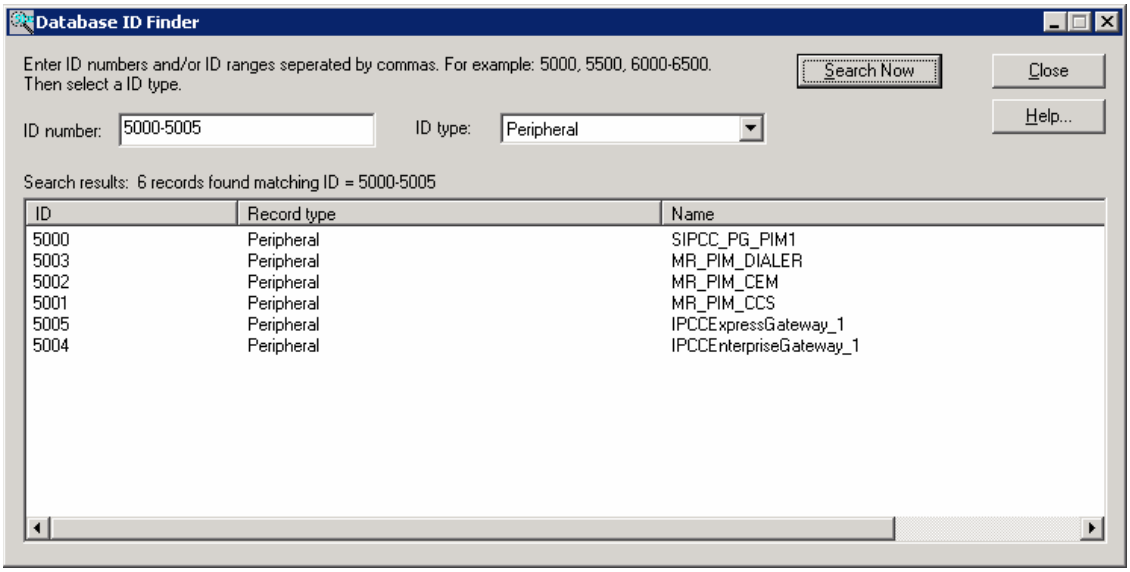
The ICM ID Finder tool helps you easily search for the IDs for particular ICM components. You can identify the component ID, record type and the name of the component from the search results by entering an ID or range of IDs.

Most of the ICM configuration tools do not show component IDs in the user interface; you need to look for the component IDs while setup or during configuration.

For System IPCC also, the ID Finder tool can be used for identifying the component IDs.

The user interface of this tool is shown in the following figure.

*Figure 1 The ICM ID Finder Tool*




## Usage of the ICM ID Finder

The ICM ID Finder tool is used mainly in the following three cases:

- During ICM setup, the peripheral ID is required to setup a PG. The ICM ID Finder tool enables you to access the peripheral IDs.
- The ICM logs usually list the component IDs. During troubleshooting, the ICM ID Finder tool can be used to look for the object names by component IDs.
- In System IPCC, you do not see the component IDs. The ICM ID Finder tool helps you to get the component IDs whenever necessary.

## How to Access the ICM ID Finder Tool

The ICM ID Finder tool is available as an executable file, idfinder.exe, starting in ICM version 4.6.2.

You can access this tool from all ICM Admin Workstations from the following path *icm\bin\idfinder.exe*.

In Release 7.1(1), the ICM ID Finder tool is enhanced to provide the ICM application path of the component ID.

## How to Use the ICM ID Finder Tool

To use the ICM ID Finder tool, perform the following steps:

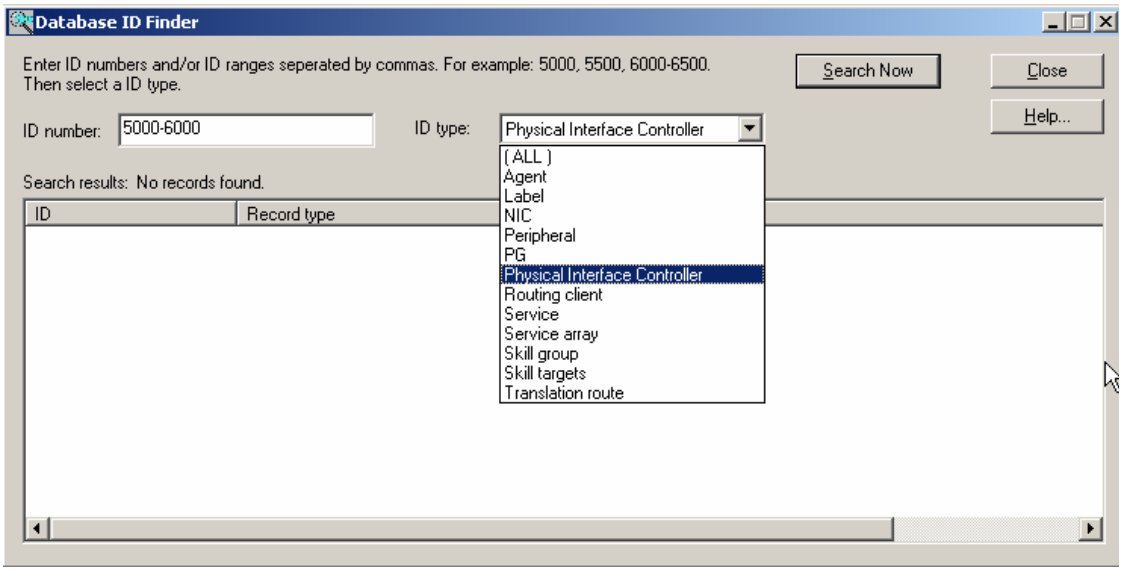
**Step 1** Go to ICM > Bin.

**Step 2** Double-click on the file idfinder.exe. The ID Finder screen opens up.

**Step 3** Enter the ID range (such as 5000-6000) in the ID Number.

**Step 4** Select the ID Type (such as Agent, Label) from the list, as shown in the figure below:

*Figure 2 ICM ID Finder Tool: ID Types*




**Step 5** Click **Search Now** to get the results.

**Note** You can double click the column headers to sort the list.

**Step 6** Click Close to close the ID Finder window.

# 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

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 active 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 any 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 e-mail 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 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)—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