Release Notes for Cisco IPICS Release 4.0(1)

April, 2010

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) release 4.0(1).

For information about caveats that apply to Cisco IPICS release 4.0(1), see the "Caveats for Cisco IPICS" section on page 6.

To access the documentation suite for Cisco IPICS, refer to the following URL:

www.cisco.com/go/ipicstechdocs

You can access Cisco IPICS software upgrades on Cisco Connection Online (CCO) by going to the following URL, clicking the **Security** link in the Select a Software Product Category area, and then expanding Cisco Physical Security > Cisco Interoperability Systems:

http://www.cisco.com/public/sw-center/index.shtml

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

Contents

These release notes contain the following topics:

Introduction

This section provides an introduction to the Cisco IPICS product. It includes the following topics:

Overview

The Cisco IPICS solution provides a cost-effective and highly-efficient IP standards-based solution to enable voice interoperability among disparate systems. By interconnecting voice channels, talk groups, and virtual talk groups (VTGs), Cisco IPICS bridges communications from radio networks to the Cisco IPICS Dispatch Console (IDC) PC application, supported mobile clients, and supported models of the Cisco Unified IP Phone.

Cisco IPICS Support Team Communications

The Cisco IPICS Support Team provides an external mailing list that you can use to obtain additional support. Send your request to physec-questions@external.cisco.com.

System Requirements

The Cisco IPICS server and the IDC require specific versions of hardware and software. *Cisco IPICS Compatibility Matrix*, lists the hardware and software versions that are compatible with this release of Cisco IPICS. Make sure that you check that document for the most current versions of compatible hardware components and software versions for use with Cisco IPICS, and make sure to upgrade your RMS components and SIP and LMR gateways to the latest supported releases before you install this release of Cisco IPICS.

Also make sure to use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported

Cisco IPICS Compatibility Matrix is available at this URL:

www.cisco.com/go/ipicstechdocs

Related Documentation

For more information about Cisco IPICS, refer to the following documentation.

- *Cisco IPICS Server Administration Guide, Release 4.0(1)*—Provides information about configuring, operating, and managing the Cisco IPICS server, including how to use the Management Console user interface.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 4.0(1)*—Describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system
- *Cisco IPICS Dispatch Console User Guide, Release 4.0(1)*—Provides information about understanding, installing, operating, and performing other IDC activities

- *Cisco IPICS Mobile Client for Apple iPhone Reference Guide*—Provides detailed information about the Cisco IPICS Dispatch Console application for the Apple iPhone
- *Release Notes for Cisco IPICS Release 4.0(1)*—Provides important information about this release of Cisco IPICS Cisco IPICS and its components
- *Cisco IPICS Compatibility Matrix*—This document contains information about hardware and software that is supported for use with Cisco IPICS

To access the documentation suite for Cisco IPICS, go to the following URL:

www.cisco.com/go/ipicstechdocs

What's New in this Release

This release of Cisco IPICS includes a wide variety of new features, including the following:

- Cisco IPICS Dispatch Console (IDC)—A radio dispatching solution that is designed for critical radio communications. The IDC runs on a standard PC platform and extends push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate in an event. It provides control of radio resources and allows users to monitor and coordinate emergency response across incompatible radio systems and between multiple agencies, jurisdictions, and departments. Key features include the following:
  - An intuitive graphical user interface
  - Channel patching
  - Integrated telephony client for incoming and outgoing calls
  - Radio to telephone patching
  - Receive and transmit on-screen indicators for channel activity
  - Handset, headset, or desktop microphone operation
  - Individual channel mute/All mute
  - All talk
  - Instant recall recording per channel
  - Last call transmit

  - Alert tones
  - Channel multi-select
  - Confirmation tones for trunked systems
  - Unit ID/talker ID
  - Emergency alert/acknowledge
  - Coded/clear channels
  - Frequency select
- Cisco IPICS Mobile Client—Standalone application that runs on an Apple iPhone, provides access to an incident VTG and supporting media, and allows users to add journals, videos and pictures to an incident.
- High Availability—Cisco IPICS 4.0 supports an optional hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service.
- Loop Prevention— Cisco IPICS automatically identifies potential audio loops and resolves them before they become an issue.
- Radio Pooling—Enables grouping Cisco IPICS radio assets into logical radio pools.
- Enhanced API—A web service API enables integration of Cisco IPICS with third-party applications, such as command and control physical security information management (PSIM) and computer aided dispatch (CAD) applications.

Upgrading to Cisco IPICS 4.0(1)

To upgrade to Cisco IPICS 4.0(1) from a previous version of Cisco IPICS, make sure to follow the guidelines and instruction in C*isco IPICS Server Installation and Upgrade Guide, Release 4.0(1)*.

Caution Make sure to back up your Cisco IPICS database before performing an upgrade.

Features not Supported in this Release

The following features, which were available in Cisco IPICS 2.2, are not supported in the initial Cisco IPICS 4.0 release:

- Text-to-speech (TTS)
- Bulk notification parallel execution support
- PMC features (these features are deprecated in the IDC):
  - Direct-dial lines
  - Direct user-to-user calls
  - Automatic upgrades
  - Granular debug logs
  - Internationalization
  - Tone signals

Caveats for Cisco IPICS

Table 1 describes caveats in this release of Cisco IPICS.

Table 1 Cisco IPICS Caveats

Cisco IPICS Server Caveats	
CSCsw41409	RCS is down, need to give feedback in the SRCI, Administration Console, and IDC
CSCtd42930	White noise for policy engine dial-in coming from PSTN via multiple Cisco Unified Communications Manager hops
CSCtf17735	Cisco IPICS server failed to boot due to CSA service hang
CSCtf34087	HA GUI: should block daisy chain
CSCtf91965	Incident archiver unable to delete photo/video when HA enabled
CSCtf95202	E-mail notifications do not include the subject line

Table 1 Cisco IPICS Caveats

CSCtf95490	Alert notification status indicates success even if user is not logged in
CSCtg16303	Installation should verify at least 250 MB free in /tmp
CSCtg37140	Bulk notification may not work first time after server restart
IDC Caveats	
CSCtb61290	IDC dialer: Multiple hold/resume forces the line to be out of service
CSCtc20650	IDC requires permission to run from PC security software, such as CSA
CSCtc82243	IDC displays international characters as ?????
CSCtc96097	Incident can only be created under system ops view
CSCtd61895	IDC Policy Execution Status screen must be refreshed for latest status
CSCte54107	Dialer patch: No audio between 2 remote users when patched to same VTG
CSCte64984	IDC not sending AVT NAT keepalives
CSCte64998	IDC does not detect loss of RTCP for SIP sessions
CSCte91277	Incident association property icon is not shown on VTG and channel
CSCtf09913	IDC Wave Engine restart requires PC admin privileges
CSCtf95064	Transmit indicator stuck on patch on remote IDC after failover
CSCtf97428	Activate/Deactivate incident quickly gives “Incident VTG already exists” error
CSCtf99429	Audio buffer is not saved sometimes
CSCtg00025	IDC goes into frozen state when previewing videos for multiple incidents simultaneously
CSCtg07064	Blank pop-up message when log in as restricted system user
CSCtg07712	IDC may lock up for a few minutes if playing corrupted bwims video link
CSCtg10464	SIP IDC: Pooled channels show with gold circle

Table 1 Cisco IPICS Caveats

CSCtg18265	IDC freezes with repeated double-clicking to maximize the video window
CSCtg25636	Wave Engine sometimes fails, requiring IDC restart
CSCtg27709	Reserved indication on IDC is not updating with correct username
CSCtg31590	VTG and Incident list/details may be empty after server failover
CSCtg31730	IDC does not return to online mode if you log in in offline mode
CSCtg43029	Media Player remains in background when “Always on top” checked on IDC
CSCtg51023	IDC may not function over Cisco software VPN connections
Cisco Mobile Client for Apple iPhone Caveats	
CSCtf52210	Reload button needs to be pressed after uploading a video file to continue PTT
CSCtf52953	Poor audio quality for audio across 3G over VPN
CSCtf79041	App shuts down if Wifi is set with an invalid DNS

You can use the Bug Toolkit to find information about caveats for the this release, including a description of the problems and available workarounds. The Bug Toolkit lists both open and resolved caveats.

To access Bug Toolkit, you need the following items:

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

To use the Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

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

Step 3 To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

Step 4 To look for information if you do not know the bug ID number:

a. Choose **Security** from the Select Product Category menu.

b. Choose the desired product from the Select Product menu.

c. Choose the version number from the Software Version menu.

d. Under Advanced Options, choose **Use default settings** or **Use custom settings**. The default settings search for severity 1, 2 and 3 bugs, open and fixed bugs, and only bugs containing bug details. Use the custom settings to change the severity and status parameters, or to search for keywords within the bug headline and description.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.