Release Notes for Cisco IPICS Release 4.7(1)

Revised November 27, 2013

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) release 4.7(1). This release features support for the new Cisco Instant Connect for Android Devices and Cisco Instant Connect MIDlet.

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

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

You can access Cisco IPICS software on Cisco Connection Online (CCO) by going to the following URL and, under "Make a selection to continue," clicking **Products > Cisco IP Interoperability and Collaboration System**, then clicking the link for your Cisco IPICS release:

http://www.cisco.com/cisco/software/navigator.html?mdfid=280723930&flowid=7120

Contents

These release notes contain the following topics:

- Overview, page 1
- What's New in Cisco IPICS, page 2
- System Requirements, page 2
- Related Documentation, page 3
- Important Notes, page 3
- Caveats, page 5
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 8

Overview

The Cisco IPICS solution streamlines radio dispatch operations and improves response to incidents, emergencies, and facility events. Cisco IPICS dissolves communication barriers between land mobile radio systems and devices including mobile phones, landline phones, IP phones, and PC users, helping

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

enable communications among users of all devices, wherever they are located. When time is critical, Cisco IPICS delivers information into the hands of the right people, at the right time and in the right format. By providing flexible, scalable communication interoperability, Cisco IPICS enhances the value of existing and new radio, telephony, and IP communications networks.

What's New in Cisco IPICS

Cisco IPICS 4.7(1) includes these major new features:

- Cisco Instant Connect, which includes:
  - New Android mobile client—A full-featured mobile client for Android devices that provides users with instant push-to-talk group (PTT) communications.
  - Cisco wireless Wireless IP Phone MIDlet—Application that runs on supported Cisco Wireless IP Phone models and provides group and individual PTT capabilities.
  - Superior user experience—PTT users log in to the system, pick channels, and then push a button to transmit. In addition to visual indications, users hear a go-ahead tone when PTT audio is transmitted.
  - Flexible control of groups—Designated individuals can control and manage channels and user groups directly from the Cisco IPICS Administration Console.
  - Wide area communications—Wired and wireless networks and public networks can be used to extend Cisco Instant Connect services to mobile environments that are beyond enterprise WiFi network coverage areas.
  - Virtualized solution—The Cisco Instant Connect solution back end is delivered as a virtualized application on supported servers, allowing savings in network and infrastructure costs.
- IP Command Touch Screen Dispatch Consoles:
  - IP Trade, a Cisco SolutionsPlus partner, offers solutions that can be used with Cisco Instant Connect to provide incident response with IP Command Touch Screen Dispatch Consoles
  - Allows dispatchers to talk and listen to many Cisco Instant Connect groups at the same time
  - Supports advanced telephony features that are integrated with Cisco Unified Communications Manager, such as call queuing, call priority queuing, multiple line appearances, hold and transfer capabilities
  - When combined with Cisco Unified Communications Manager features, allows dispatchers to prioritize their work and achieve higher productivity

System Requirements

The Cisco IPICS server requires 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,

In addition, 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 the following URL:

http://www.cisco.com/en/US/products/ps7026/products_device_support_tables_list.html

Related Documentation

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

- *Cisco IPICS Server Administration Guide, Release 4.7*—Provides information about configuring, operating, and managing the Cisco IPICS server, including how to use the Management Console user interface.
- *Cisco IPICS Installation Guide, Release 4.7*— Describes how to instal Cisco IPICS and perform related tasks
- *Cisco Instant Connect for Android Devices User Guide, Cisco IPICS release 4.7*—Provides detailed information about Cisco Instant Connect for Android devices
- *Cisco Instant Connect MIDlet Reference Guide, Cisco IPICS release 4.7*—Describes how to configure and use the Cisco Instant Connect MIDlet
- *Cisco IPICS Compatibility Matrix*—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:

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Important Notes

The following sections describe important issues that apply to this release:

- Cisco IPICS Features Not Supported in Release 4.7, page 3
- Using Cisco IOS Release 15.1(4)M4, page 3

Cisco IPICS Features Not Supported in Release 4.7

This release of Cisco IPICS does not support the following features. However, these features appear in the Administration Console user interface and are discussed in the product documentation:

- IDC
- RMS
- UMS high availability
- ISSI gateway
- DFSI gateway
- P25 radios
- Channels using the G.729 codec
- Talker ID
- Serial radio control

Using Cisco IOS Release 15.1(4)M4

In your Cisco IPICS deployment, use Cisco IOS release 15.1(4)M4 on routers that function as an LMRG component.

Node Manager Configuration Files

The system stores these node manager configuration files:

- nodemanager.pri.*ip_address*.tar—Tape-archive format (tar) file that contains a snapshot of the node manager installation directory (/opt/cisco/nodemanager) from the primary Cisco IPICS server. In this file name, *ip_address* is the IP address of the primary Cisco IPICS server.
- nodemanager.sec.*ip_address*.tar—Applies to a high availability deployment only. Tar file that contains a snapshot of the node manager installation directory (/opt/cisco/nodemanager) from the the secondary Cisco IPICS server. In this file name, *ip_address* is the IP address of the secondary Cisco IPICS server.

Situations in which you might need to manually restore these files include the following:

- An error or unexpected interruption occurs during the configuration of the high availability server causes the server no longer allows log in Cisco IPICS Administration Console
- The /opt/cisco/nodemanager directory on the currently active server is corrupted or deleted

To restore the node manager configuration files, follow these steps:

Procedure

Step 1 Use an SSH client to access the server on which the Cisco IPICS backup is located, log in as the root user, and enter these commands to extract the node manager backup file to a /tmp directory:

a. # **cd /tmp**

b. To extract the file for the primary Cisco IPICS server, enter this command, where *path* is the full backup directory path and *ip_address* is the IP address of the primary Cisco IPICS server:

# **tar xvf *path*/nodemanager.pri.*ip_address*.tar nodemanager/conf/ipicsNode.properties**

To extract the file for the secondary Cisco IPICS server, (in a high availability deployment only), where *path* is the full backup directory path and *ip_address* is the IP address of the secondary Cisco IPICS server:

# **tar xvf *path*/nodemanager.sec.*ip_address*.tar nodemanager.sec.*ip_address* .informix/conf/ipicsNode.properties**

Step 2 Log in as the root user to the Cisco IPICS server on which the node manager property file is to be manually restored and enter these commands to back up the current node manager properties file:

# **cd /opt/cisco/nodemanager/conf**

# **/bin/cp -p ipicsNode.properties ipicsNode.properties.save**

Step 3 Enter this command to replace the current node manager configuration file with the file that you extracted in Step 1:

# **/bin/cp -p /tmp/ipicsNode.properties**

Step 4 Enter these commands to restart Cisco IPICS:

# **service ipics stop-all**

# **service ipics start-all**

Trust Certificates

The system stores these trust certificate files:

- security.pri.*ip_address*.tar—Tar file that contains a snapshot of the Cisco IPICS security directory (/opt/cisco/ipics/security) from the primary Cisco IPICS server. This directory contains all self-signed certificates and third-party certificates for Cisco IPICS. In this file name, *ip_address* is the IP address of the primary Cisco IPICS server.
- nodemanager.sec.*ip_address*.tar—Applies to a high availability deployment only. Tar file that contains a snapshot of the Cisco IPICS security directory (/opt/cisco/ipics/security) from the secondary Cisco IPICS server. This directory contains all self-signed certificates and third-party certificates for Cisco IPICS. In this file name, *ip_address* is the IP address of the secondary Cisco IPICS server.

Situations in which you might need to manually restore these files include the following:

- The /opt/cisco/ipics/security directory on the active Cisco IPICS server is corrupted or deleted
- The server trust setup is accidentally reinitialized

To restore the certificate files, follow these steps:

Procedure

Step 1 Use an SSH client to access the server on which the Cisco IPICS backup is located, log in as the root user, and enter these commands to extract the security tar file to a /tmp directory:

a. # **cd /tmp**

b. To extract the files for the primary Cisco IPICS server, where *path* is the full backup directory path and *ip_address* is the IP address of the primary Cisco IPICS server:

# **tar xvf *path*/security.pri.*ip_address*.tar**

To extract the files for the secondary Cisco IPICS server, (in a high availability deployment only), where *path* is the full backup directory path and *ip_address* is the IP address of the primary Cisco IPICS server:

# **tar xvf *path*/security.sec.*ip_address*.tar**

Step 2 Log in as the root user to the Cisco IPICS server on which the security directory is to be manually restored and enter these commands to back up the current security directory:

# **cd /opt/cisco/ipics**

# **tar cvf security.tar.save security**

Step 3 Enter this command to replace the trust certificate files with the files that you extracted in Step 1:

# **/bin/cp -rp /tmp/security/* /opt/cisco/security**

Step 4 Enter this command to restart Cisco IPICS:

# **service ipics restart**

Caveats

The following sections provide information about caveats in this Cisco IPICS release:

- Using the Bug Search Tool, page 6
- Known Caveats, page 6

Using the Bug Search Tool

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

Note Bug Search Tool is the successor to the Bug Toolkit.

To use the Bug Search Tool, follow these steps:

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

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 field, then press **Enter**.

Step 4 To look for information if you do not know the bug ID number, enter keywords which search for text matches in the following sections of a bug:

- headline/title
- release note text
- product
- known affected releases/ known fixed releases

For more information about the Bug Search Tool, click Help on the main Bug Search Tool page:

https://tools.cisco.com/bugsearch/

Known Caveats

Table 1 describes known caveats in this Cisco IPICS release.

Table 1 Known Caveats

Headline	Description
Cisco IPICS Server	
CSCul23253	MIDlet releases the currently used license after IPICS failover
CSCuj31843	Installation failure due to the disc space almost full on / directory
CSCul56536	IPICS server throws misleading error when no IP Phone licences available
UMS	
CSCui49032	Stale port on UMS once SIP client gets logged out due to session timeout
CSCui66393	UMS stuck in Out Of Service when eth1 enabled
CSCuj45942	Active parent VTG with common channel after IPICS failover causes audio loop
CSCuj18555	UMS restart cause SIP call end but resource allocation still exists
CSCul11779	Red TX and Green RX flickering when PTT and no one to talk to
CSCul14493	Deactivating parent VTG of nested VTG breaks the restream of child VTG
CSCul25953	Three VTGs with common channel have one way audio
Cisco Instant Connect for Android Devices	
CSCui86486	Android app: Stale SIP connection due to no SIP session refresh
CSCuj23605	Android app: Status update does not happen when users are disassociated
CSCuj75427	Android app: Persistent talk group is not keeping context with server/user
CSCuj81753	Android app: If no Mobile license, app gives invalid user/password error
CSCul13801	Instant Connect shortcut in the Ongoing app list does not work
CSCul14355	Android app: Receiving Audio feeble on Rugby in internal speaker mode
CSCul25911	Android app: Rx indicator flickers between green and white
CSCul35821	Android app: App stuck in logging out screen intermittently; needs force stop
CSCul36781	Android app: Intermittent logged out message seen on Rugby/ S3 devices
Cisco Instant Connect MIDlet	
CSCug88202	No indication for out of Wifi service area
CSCui05267	MIDlet: Ringback tone did not stop when the call was “ignored” by remote
CSCui07161	P2P PTT call autoconnects when callee busy in CUCM call outside MIDlet
CSCui10730	MIDlet: Multiple services on handset gives “Error, contact administrator”
CSCui18061	MIDlet: MIDlet unresponsive when it can talk to active server
CSCui26011	MIDlet: Cannot receive audio on losing and resuming network coverage in 2 minutes
CSCui31013	End Call softkey exists on Wifi MIDlet phone after CUCM call release
CSCuj17586	MIDlet: Volume settings do not stick
CSCuj59015	MIDlet: Transmit audio interrupted by new tone playback during concurrent point-2-point calls
CSCuj60929	MIDlet: Battery drains less than hours as a result of 15s client poll to server

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.