Release Notes for Cisco IPICS Release 4.8(2)

First published October 24, 2014

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) release 4.8(2).

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

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 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 4.8(2) includes these major new features:

- Improved security—The latest IPICS Linux kernel in the Unified Media Service (UMS) and Cisco IPICS server software now protects against the Shellshock software bug. Shellshock is a vulnerability that can lead to denial of service attacks in Linux and Unix software platforms.
- Trust management—The Trust Management window in the Cisco IPICS Administration Console provides options for viewing and managing trust relationships between servers in a Cisco IPICS deployment.
- Cisco Instant Connect Android Software Developers Kit (SDK)—Allows developers to embed Cisco push to talk technology in any Android application. You can download the Cisco Instant Connect Android SDK from the Cisco Devnet site:

  https://developer.cisco.com/site/networking/interoperability-services/cisco-instant-connect/
- Improved UMS audio quality—Improved audio streams buffers for each smart phone device eliminating unwanted noise during situations with loud or quiet backgrounds.
- Improved P25 supplemental services—This release has been tested with P25 supplemental services, P25 group calls, and P25 individual calls.
- Polish language support—Support for internationalization of the IDC, dial engine prompts, and IP-phone services is expanded to include Polish.
- Microsoft Windows 8 support: Cisco IPICS now supports the Windows 8 operating system for the Cisco IPICS Dispatch Console (IDC).
- New Cisco router code support—Cisco IPICS now supports the new iOS version RMS-15.4.2(T)
- Cisco Unified Communications Manager 10.0 and 10.5.1 support—Cisco IPICS was tested with the Cisco Unified Communications Manager 10.0 and 10.5.1.
- HP server support—Cisco IPICS has been tested in a VM Ware environment on c7000 Series HP Servers.

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

Upgrading to Cisco IPICS 4.8(2)

If you have a Cisco Software Application Support contract, you can upgrade to Cisco IPICS 4.8(2) from Cisco IPICS 4.6(1) or 4.8(1) by going to the following URL:

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

For complete upgrade instructions, see Cisco IPICS Installation and Upgrade Guide, Release 4.8(1), which is available at the following URL:

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

Related Documentation

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:

- Node Manager Configuration Files, page 3
- Trust Certificates, page 4
- Cisco Instant Connect MIDlet Upgrade Consideration, page 5

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 (such as /idspri/backup/cron/IDSB_2014-10-20_23-59-03/) 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

- The Cisco IPICS server suffered a catastrophic failure, which requires the Cisco IPICS software to be reinstalled followed and the Cisco IPICS database to be restored

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

Cisco Instant Connect MIDlet Upgrade Consideration

Cisco Instant Connect MIDlet users should log out of Cisco IPICS before you upgrade the Cisco Instant Connect MIDlet by unsubscribing and subscribing to the service from Cisco Unified Communications Manager. If any users are not logged out, you must manually log them out from Cisco IPICS before they can log in to the new Cisco IPICS version. To manually log out Cisco Instant Connect MIDlet users, go to the Administration > Active Users window in the Cisco IPICS Administration Console.

Feature Notes

- The call assurance functionality for Cisco Instant Connect for Android Devices release 4.8 is supported with the UMS only.
- To simplify deployment and avoid audio loop scenarios, the nested VTG feature has been deprecated. The IDC prevents including VTGs and incidents in a patch.
- Channel attenuation on the IDC dialer is not supported in the 4.8 release. For channel attenuation options that use third-party audio hardware, contact your Cisco representative.

Caveats

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

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

ID	Description
CSCug67526	Need to click End button twice to end calls if IDC Dial Pad and Channel Patch panel is open

Table 1 Known Caveats (continued)

ID	Description
CSCun64223	On clients such as IDC or CIC, the receive audio (RX) indicator sometimes blinks even when there is no audio heard when listening to a VTG whose participants are hosted on multiple UMS or RMS components
CSCun77570	Android: Cannot get new SIP connection after IPICS failover
CSCup67946	UMS sends comfort noise and Remote ID displays Rx once channel is powered on
CSCup78511	IP address of Cisco Unified IP Phone 9971/9951 shown on P25 channel in Gateway P25 mode
CSCup78913	ERROR: /home/ipicsadmin/.ssh/known_hosts should have mode 600, not 640
CSCup83697	LIDC_MediaServiceFailure intermittently post headset disconnect
CSCup95113	No error for P25 channel when limit exceeds 50 channels
CSCuq12668	IDC active P25 Advanced Encryption Standard secure PTT gets interrupted after a keyset shangeover
CSCuq14293	Bad VQ scores when PTT from Android to Android with 4.4.2 OS version
CSCuq44038	Cannot build the trust due to bad ipicsadmin user ID or password over retry limit
CSCuq68639	The trust is still valid between server and UMS even though certificate is expired
CSCuq70536	IDC—Direct Dial audio replay buffer records only the first 60 seconds
CSCuq79890	IPICS server node manager stopped and did not come up until Node Manager restart
CSCuq82245	DFSIG listed as a Radio on both IDC VTG Details Page and Incident Details page
CSCuq82295	IPICS—Deleting language package does not remove the package completely
CSCuq93443	Certs install fails with “... certificate for null” due to wrong certificates
CSCuq99078	Users wont be able to power on Native channels due to cluttered hosts file
CSCuq99310	IDC_2nd Dialer call drops post IDC start
CSCuq99368	Remote IDC stops working intermittently when End Dialer call/shutdown during Dialer call
CSCur13005	Cisco IP Phone 7906 and 7911—Not receive audio if Stop Latch before going on-hook
CSCur18157	IP Phone Service_HTTP Error 500 post IPICS failover/fallback on Cisco IP Phone 8961, 9951, 9971
CSCur24523	The checksec output should display 4 certificates instead of 2 after installing 4 certificates
CSCur26059	Multicast to unicast randomly broken on a channel
CSCur26252	VTG Tx in Secure mode on a strapped selectable ISSI channel inheriting form GW Mode
CSCur28525	Refresh of the Trust Management page required for any trust update
CSCur34133	RIDC—Direct Dial fails longevity tests longer than 48 hours
CSCur40150	IDC version on Administration Console does not change to recommended post upgrade

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