Release Notes for Cisco IPICS Release 4.6(1)

Revised August 21, 2013

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) release 4.6(1).

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 upgrades 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 2
- System Requirements, page 2
- Related Documentation, page 2
- What's New in Cisco IPICS, page 3
- Important Notes, page 3
- Downgrading Cisco IPICS, page 6
- Restoring Cisco IPICS to a Specific Configuration, page 6
- Caveats, page 9
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 12

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

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.

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.

In addition, be aware of the following:

- Make sure to use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported.
- The1RU MSP server is not tested for this release. For best performance, upgrade to a supported Cisco UCS platform before you upgrade to this Cisco IPCIS release.
- Microsoft Windows 7 Professional, Ultimate, or Enterprise must be installed on the client PC on which you install the IDC.

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 4.6*—Provides information about configuring, operating, and managing the Cisco IPICS server, including how to use the Management Console user interface.
- *Cisco IPICS Installation and Upgrade Guide, Release 4.6*— Describes how to install, configure, and upgrade Cisco IPICS
- *Cisco IPICS Dispatch Console User Guide, Release 4.6*—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 Mobile Client application for the Apple iPhone
- *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:

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

What's New in Cisco IPICS

Cisco IPICS 4.6(1) includes these major new features:

- Direct radio network interoperability—This release supports Inter RF Subsystem Interface (ISSI), Console Sub-System Interface (CSSI), and TIA P25 Digital Fixed Station Interface (DFSI) standards.
- DFSI Gateway—This release includes a new P25 Conventional Gateway called DFSI gateway.
- Cisco Video Surveillance (VSM) Manager 7 support—Allows the integration of VSM videos with incidents.
- Key management—This release provides features to manage the storage and distribution of keys for IDC users in "End to End" ISSIG mode, ISSI gateways, and DFSI gateways. These keys are used to encrypt and decrypt voice traffic on P25 TalkGroups and P25 Fixed Stations
- TETRA radios—This release supports the configuration and use of TETRA radios.
- SNMP—The new SNMP tab in the Cisco IPICS Administration Console allows the configuration of SNMP V2 options for Cisco IPICS.
- Language support—Support for internationalization of the IDC, dial engine prompts, and IP-phone services is expanded to include French (Canadian), Portuguese, Russian, and Spanish.
- Cisco IP Phone high availability—The IPICS IP Phone client now supports high availability.
- Updated Cisco Unified Communications Manager support—This release supports Cisco Unified Communications Manager-9.x.
- Updated Cisco UCS support—This release is extended as a virtualized application on the Cisco Unified Computing System (UCS) E-Series.
- IP Command Touch Screen Dispatch Console—This new touch-screen dispatch capability is available through IP Trade, a Cisco SolutionsPlus partner.
- IDC features—New or updated features in the IDC include:
  - Tear away items—You can customize the appearance of the IDC by moving various items from the IDC Main window to any location on your computer screen
  - IDC Dialer updates—Addition of call transfer features allow consultative and blind call transfers
  - Address book—Lets you access and manage multiple contact lists and quickly call or send email to a contact
  - Do not disturb—Allows an incoming call to be handled in the way that the DND feature is configured in Cisco Unified Communications Manager

Important Notes

The following sections describe important issues that apply to this release

- Special Installation File for Certain Upgrades, page 4
- ISSI Gateway Unable to Register to a Remote RFSS, page 4

- Installing Certificates on an IDC Client PC, page 4
- Using Cisco IOS Release 15.1(4)M4, page 5
- Configuring Languages in Cisco IPICS, page 5
- Localized IDC May Display English Prompts in Some Situations, page 6

Special Installation File for Certain Upgrades

If you are upgrading to Cisco IPICS 4.6(1) on a 4.5(1) or 4.5(2) system that was previously upgraded from Cisco IPICS release 2.2(1) SR1, you must use the special installation file ipics-4.6.1_alternate.bin when you perform the upgrade.

To determine whether your system was previously upgraded from release 2.2(1) SR1, log in to the Cisco IPICS server as the Linux root user and enter this command:

 # ls /opt/cisco/ipics/dbspaces

If the file named ipics_log_dbspace2 appears in the output, your system was previously upgraded from release 2.2(1) SR1. In this case, obtain the ipics-4.6.1_alternate.bin installation file instead of the ipics-4.6.1.bin file when you perform the upgrade to Cisco IPICS 4.6(1) as described in *Cisco IPICS Installation and Upgrade Guide*. Using the correct installation file ensures that your upgrade completes successfully.

ISSI Gateway Unable to Register to a Remote RFSS

If the ISSI Gateway is unable to register to a remote RFSS, you may see “ERROR_UNABLE_TO_JOIN” for the P25 channel status in the IDC. Restarting the remote RFSS should resolve this issue.

Installing Certificates on an IDC Client PC

By default, IDC client PCs authenticate the Cisco IPICS server by using a self-signed certificate that is generated when the Cisco IPICS server software is installed. If you replace the self-signed certificate on the server with a certificate from an unusual CA or enterprise CA, you may need to perform the following steps on each IDC client PC that access the Cisco IPICS server. This procedure is not needed of you are using the default self-signed certificate or a certificate from a well-known CA.

Before you begin

Make sure that certificates are installed on the Cisco IPICS server as explained in the “Managing Server Certificates” section in *Cisco IPICS Server Installation and Upgrade Guide*.

Procedure

Step 1 Copy the following files from the Cisco IPICS server to the client PC:

- /opt/cisco/ipics/security/root_ca.cert.pem
- /opt/cisco/ipics/security/intermediate_ca.cert.pem
- /opt/cisco/ipics/security/signed_server.cert.pem

Step 2 On the client PC, take these actions:

a. Rename root_ca.cert.pem to root_ca.crt.

b. Rename intermediate_ca.cert.pem to intermediate_ca.crt.

c. Rename signed_server.cert.pem to *hostname*.crt, where *hostname* is the hostname of the Cisco IPICS server.

Step 3 On the client PC, take these actions for each .crt file that you renamed in the previous step:

a. Double-click the file name.

b. Click **Install Certificate** to launch the Windows Certificate Import Wizard.

c. Click **Next**.

d. Click **Place all certificates in the following trust store**.

e. Choose **Trusted Root Certification Authorities**.

f. Click **Next**.

g. Click **Finish**.

Step 4 Restart the IDC if it is running.

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 LMRG or RMS components.

Configuring Languages in Cisco IPICS

Table 1 provides a summary of the various options that you can use to configure languages in the Cisco IPICS Administration Console. For more detailed information about these options, see *Cisco IPICS Server Administration Guide*.

Table 1 Cisco IPICS Language Configuration Options

Option Name	Location in Administration Console	Description
Default language	Server tab > Configuration drawer > Ops Views > *Ops_view_name*	Designates the language in which notifications are sent and the language that is used by the dial engine for the voice prompts that are played to users who call in to Cisco IPICS
Languages	Policy Engine tab > Dial Engine drawer > Prompt Management	Select the languages that appear on language drop-down lists in other pages
Language	Policy Engine tab > Dial Engine drawer > Prompt Management > Spoken Names	Designates the language tag that is applied to recorded prompts

Table 1 Cisco IPICS Language Configuration Options (continued)

Option Name	Location in Administration Console	Description
Language	Policy Engine tab > Dial Engine drawer > TTS Management	Designates the language that is used for TTS prompts
Default Language	Policy Engine tab > Dial Engine drawer > Dial Engine Parameters	Designates the language that is used for dial out prompts

Localized IDC May Display English Prompts in Some Situations

If you installed language files to localize the IDC user interface, some messages may display in English. This situation occurs if an external server provides a message that cannot be localized.

Downgrading Cisco IPICS

If you need to downgrade Cisco IPICS 4.6 to 4.5(1) or 4.5(2), you must reinstall the operating system on each server in your deployment before you install Cisco IPICS. Make sure to back up Cisco IPICS before you reinstall the operating system.

Restoring Cisco IPICS to a Specific Configuration

When a database backup is performed for this Cisco IPICS release, a set of files are saved that you can use to manually recover Cisco IPICS to a specific configuration snapshot after you perform a database restore procedure.

The system stores all of these files in a database backup directory.

The following sections describe these files and how to use them:

- Node Manager Configuration Files, page 6
- Trust Certificates, page 7
- IDC Language Packs, page 8

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

IDC Language Packs

The system stores a snapshot of the IDC language packs installation directory (/opt/cisco/ipics/tomcat/current/webapps/ipics_server/language-packs/idc/*Cisco_IPICS_version*) as a tar file. This file contains all installed IDC language packs.

To restore the language packs, 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 language pack files, where *path* is the full path to backup directory:

 # cd *path*

 # tar xvf idc_langpks.tar

Step 2 Enter this command to replace the language packs with the files that you extracted:

 # /bin/cp -rp idc /opt/cisco/ipics/tomcat/current/webapps/ipics_server/language-packs

Step 3 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 Toolkit, page 9
- Known Caveats, page 10

Using the Bug Toolkit

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.

Known Caveats

Table 2 describes known caveats in this Cisco IPICS release.

Table 2 Known Caveats

Headline	Description
CSCua29629	IP Phone: Only one global language supported at a time
CSCuc47207	Zombie SIP connections on IDC when VM on UMS is shut down and restarted
CSCud15428	Audio replay feature on P25 native channel does not playback RX Audio
CSCud23183	Camera feed list in multipane viewer blackout when navigated
CSCud37410	Docking and undocking Policies tab causes Incidents tab to be unselectable
CSCud54687	Region deletion displays VTG in 2 regions
CSCud67713	IDC does not display private call failures
CSCud70711	IDC Tetra Sepura yellow PTT bar during PTT attempt while receiving
CSCue06595	ES CRYPTO: Deleting key from one keyset deletes key from all keysets
CSCue06599	ES ISSIG: Cannot preempt with higher priority call
CSCue08884	Multipane viewers live to record change shows delay in IPICS
CSCue19298	DND state is not persistent when shutting down and restarting IDC
CSCue25622	Tetra Sepura RCS does not clear emergency status messages
CSCue39078	Remote-IDC: Some channels did not receive audio
CSCue44363	IDC: some channels or VTG do not power-off gracefully(socket (Err -1))
CSCue51460	IDC takes extremely long to initialize 50+ channels if many panels undoc
CSCue53874	SIP provider credential configuration/update needs IPICS service restart
CSCue54169	After updating SIP provider configuration, first call always fails
CSCue58330	Tetra Sepura needs admin console disable/reenable after quick radio resets
CSCue76242	SIP IDC: Intermittent SIP reconnect of RMS channel after network drop
CSCue82417	Updating MC address of fixed station does not get updated on DFSI gateway
CSCuf47417	Pink noise after receive voice from PTT on Wireless/IP phone service
CSCuf51368	Recovering trust after a DB restore
CSCuf51368	Recovering trust after a DB restore
CSCuf91438	Unable to modify channel selector for an ISSIG channel
CSCug04027	Remote IDC frequently disconnects calls during channel connect attempts
CSCug17354	P25 channel stays in yellow ring after network connection recovered
CSCug20278	Mixing versions between the IPICS server and UMS should not be allowed
CSCug21340	Mixing versions between the IPICS server and ISSIG should not be allowed
CSCug22425	Deactivating a channel with an non-cleared emergency alert
CSCug30339	VLC 2.0.6 is not supported to play media in IDC
CSCug40890	P25 Secure lock icon tied to user input, not state of Ctrl function in GW mode
CSCug41813	IDC cannot select secure/clear mode for ISSIG channel when no keys assigned

Table 2 Known Caveats (continued)

Headline	Description
CSCug44237	Multicast IDC could not terminate audible emergency alarm
CSCug47148	Total Voice port: Rows get left behind after deleting an RMS/UMS
CSCug49546	GW and native IDC session emergency alert Acks/CLR not synced
CSCug60347	SNMP: CISCO-IPICS-MIB.my missing traps such as ISSIG FO, NTP err, DB replication
CSCug61335	Cannot install ISSIG 4.5(2) after uninstalling 4.6(1)
CSCug69468	32-bit Windows 7 IDC ISSIG channels get in invalid state in extended time test
CSCug72243	Improve keyfail experience on P25 native channel
CSCug90653	Failover from primary IPICS generates remoteNodeOutOfService notification
CSCug90772	P25 native channel continues to use key for secure transmit/receive after disassociation
CSCug93047	Fixed Station should inherit location info from DFSI gateway, hide location on Fixed Station configuration page
CSCug93208	Dialling out to multiple participants in an active VTG fails, except one
CSCug93293	IPICS server license is getting expired before the expiry date
CSCug93312	Changing strapping mode form any to CLR/SEC does not reflect on P25 end-to-end channel
CSCug96135	IDC process takes a long time to shut down
CSCuh01637	Need to toggle SEC CF to secure tx/rx after key association on native P25 channel
CSCuh01848	Fixed Station channel goes into UNDEFINED state on server failback
CSCuh01853	Ticking sound heard on Cisco IP Phone 8945 and 6945 when PTT/latch on IDC
CSCuh04150	Not receiving trap when node manager detects a service has gone OOS
CSCuh04319	Secured LDAP config fails with certificate error
CSCuh07320	IPICS Server allows second DFSI gateway with identical unit ID to be configured
CSCuh07695	With VTG loop Policy Engine dial fails to join VTG (in getImmediateChildren loop)
CSCuh12517	Reinstalling IPICS 4.6 on secondary high availability server without uninstalling first
CSCuh17209	Issues for patching VTGs and getting SIP connections
CSCuh17327	Talker ID packets drop for resources in a patch
CSCuh18225	No UMS resource allocated for IPPE joining first and same talk group after server failover
CSCuh20659	UMS CPU 50% with just 5 resource allocated, one CPU ~100% other 0%
CSCuh23179	IPPE dial-in with TTS causing server failover
CSCuh28017	No audio flow across some talk group participants in a patch
CSCuh28851	Emergencies do not persist across channel changes for P25 gateway channels
CSCuh33338	Upgrade 4.5(x) to 4.6(1): Does n0t update the NLR admin user
CSCuh36898	Cannot transmit or receive on P25 native channels set up with encryption after extended use
CSCuh47753	Issue of IDC VPN users getting logged out just after login

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.