Release Notes for Cisco IPICS Release 4.0(2)

December, 2011

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (Cisco IPICS) release 4.0(2).

For information about caveats that apply to Cisco IPICS release 4.0(2), see the "Caveats" section on page 9.

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 > Interoperability Systems > Cisco IP Interoperability and Collaboration System**, then clicking the link for your Cisco IPICS release:

http://www.cisco.com/cisco/web/download/index.html

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

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.

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 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 4.0(2)*—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(2)*—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(2)*—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:

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

What's New in Cisco IPICS

The following sections provide information about new features and functions in Cisco IPICS 4.0(x):

What's New in Cisco IPICS 4.0(2)

New features and functions in Cisco IPICS 4.0(2) include the following:

- ISR G2 LMR gateway
- Text-to-speech in the policy engine
- Direct dial
- Ops view functionality—Incidents can now be associated with the ops view that the incident creator is associated with
- IPICS Dispatch Console enhancements:
  - Microsoft Windows 7 support
  - Increased number of regions
  - Increased channel name length
  - Configurable video clip size

What's New in Cisco IPICS 4.0(1)

New features and functions in Cisco IPICS 4.0(1) include 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.

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 third-part party certificate, 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.

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.

Changing the Password for a Trusted Certificate

This section describes how to change the default keystore password for trusted certificates.

Before you begin

Make a backup copy of the truststore or keystore that you will modify.

Procedure

Step 1 On the Cisco IPICS server, enter these commands to stop all Cisco IPICS services:

a. [root]# **ssh root@*ipics-server***, where *ipics-server* is the host name or IP address of the Cisco IPICS server.

b. [root]# **cd /opt/cisco/ipics/security/security.properties**

c. [root]# **service ipics stop-all**

Step 2 Use the following command to change the password:

[root]# **cp server.keystore.p12 server.keystore.p12.bkup**

[root]# **keytool -storepasswd -keystore server.keystore.p12**

Enter keystore password: *Old password*

New keystore password: *New password*

Re-enter new keystore password: *New password*

Step 3 Update the security.properties file with the password that you changed.

For example, if you edited the keystore, you might update this file as follows:

```
#
# Cisco IPICS - Advanced Security Configuration
#
# You may customize the x500 settings, passwords, and/or key
```

```
# strength, and re-run './security-manager' to regenerate your
# local self-signed certificates. Be aware that the keystore
# password must match the private key password!
#Note: If you change the keystore and/or truststore passwords, be
# sure to also fix server.xml in tomcat/conf otherwise tomcat
# cannot start-up.
#
#Wed Aug 04 00:41:34 GMT 2010
certValidity=1095
x500OrginizationName=Cisco Systems, Inc.
providerName=
x500OrginizationalUnit=PSBU
providerClass=
keyAlgorithm=RSA
protectedFlag=false
truststorePassword=changeit
x500LocalityName=San Jose
x500Country=US
sigAlgorithm=
privateKeyPassword=changeit
sshPort=22
x500Email=admin@ipics.cisco.com
javaOption=
keystoreType=PKCS12
enableSynchronizeTrust=false
keystorePassword=changeit
truststoreType=JKS
providerArg=
x500StateName=California
keySize=2048
```

Step 4 Take these actions to update the server.xml file with the password that you changed.

a. Enter this command:

[root]# **cd /opt/cisco/ipics/tomcat/current/conf**

Step 5 Update the line with the truststore or keystore you changed. For example, if you edited the truststore, you might update this file as follows:

```
<Connector port="8443"
maxHttpHeaderSize="4096"
ciphers="SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_RC4_128_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA,
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
```

```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_KRB5_WITH_3DES_EDE_CBC_MD5, TLS_KRB5_WITH_3DES_EDE_CBC_SHA,
TLS_KRB5_WITH_RC4_128_MD5, TLS_KRB5_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA"
maxThreads="500" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="/opt/cisco/ipics/security/server.keystore.p12"
keystoreType="PKCS12"
keystorePass="changeit"
truststoreFile="/opt/cisco/ipics/security/server.truststore.jks"
truststoreType="JKS"
truststorePass="changeit"
connectionTimeout="60000" />
```

Step 6 On the Cisco IPICS server, enter this command to start all Cisco IPICS services:

[root]# **service ipics start-all**

Using Cisco IOS Release 15.0(1)M4

In your Cisco IPICS deployment, use Cisco IOS release 15.0(1)M4 on routers that function as LMRG and RMS components. This release addresses the following issues:

- Allows the “Go Ahead” tone to be heard when making a transmission on a secure digital channel
- Eliminates audio clipping that occurred when multiple channel or talk group resources were included in a VTG
- Enables DTMF key transmission from IDC remote users to relay properly from the RMS to all other participants in the same or associated talk groups.

Caveats

Table 1 describes caveats in this release of Cisco IPICS.

Table 1 Cisco IPICS Caveats

Cisco IPICS Server Caveats	
CSCsy21874	Exceptions while parsing channel activity logs
CSCsy30829	Re-executing dial out policy from Execution Status page does not work
CSCth62808	No HTTPS support for CAP XML notification
CSCth62991	TTS server still connected even after TTS Enabled flag is unchecked
CSCth82859	HA config times out due to no or bad DNS entry
CSCth91770	Not all the idle session time out taken effects and active users removed
CSCti43668	When TTS link lost, the policy engine takes long time to determine connection lost
CSCtj22292	NPE in IppeUmsCommunicator.endCall() after failover causes second failover
CSCtj37561	IPICS running older version of Apache Tomcat
CSCtj78063	Unable to add more ports on secondary server even if it is active
CSCtj79071	RMS—"Ghost" DS0s in use with heavy RMS load
CSCtk55736	IPICS 4.0 VMware LM issue on MAC
IDC Caveats	
CSCtd44783	Sometimes yellow triangle on channels when login multicast and remote
CSCte13365	New alert tones are not updated on IDC
CSCtf99429	Audio buffer is not saved sometimes
CSCtf99601	Sometimes incident enable but has yellow triangle
CSCtg07712	IDC locks for 15–20 minutes if played corrupted video link
CSCtg42610	Media TX/RX failed after disabling/enabling network connection
CSCtg46059	Invalid Session ID error on IDC post server fail over
CSCth32666	IDC4.0(2):Alert tone UI issue if the user is set as "listen only"

Table 1 Cisco IPICS Caveats

CSCth34557	Radios list not visible from IDC when in a non-SYSTEM opsview
CSCth44278	Direct dial: IDC does not send CANCEL message call is in ringing state
CSCti06570	Channels remain in yellow triangle upon unplugging the headset.
CSCti28690	Auto reconnect occurs for invalid Session ID on IDC
CSCti38072	IDC4.0(2):Audio can be heard in the groups w/o audio device selections
CSCti49132	DC4.0(2):Cannot upload video if max video size 2048 mb set on server
CSCti92251	IDC4.0(2) remote: Patch VTG flickers while unpatching
CSCti92344	IDC is shutting down when the pagination edited from IDC
CSCtj02371	IDC4.0(2):Issues with disabling a channel while it is latched
CSCtj02583	RX Indicator is not showing up on Remote IDC
CSCtj19307	IDC4.0(2):Unable to view video/photo when maximized the IDC
CSCtj19607	Direct-dial hang up the call on IP phone during direct dial PTT causes next DD fail
CSCtj20060	Abnormal termination while exiting the IDC application
CSCtj34515	Disable remote user with blue theme does not work
CSCtj90622	Muted channel receives audio after powering then down and back up
CSCtj91362	IDC cannot access VLC player download site
CSCtk06929	Voice replay does not play any audio if audio devices are changed quickly
CSCtk84355	IDC4.0(2): VSM 6.3.1 AxClient client version 6.3.309.0 or higher version—upgrade does not work on Windows XP
CSCtk96611	IDC4.0(2):Centerpane stuck in move mode if patch is moved while unpatch

Table 1 Cisco IPICS Caveats

CSCtk97057	Direct dial does not show up in summary tab if its created after IDC is up
CSCtl03185	On a machine, the IDC locked up on media related controls, requiring an IDC restart
CSCtl04590	IDC4.0(2): IDC comes with yellow triangle on talk groups at first login
CSCtl07256	IDC shuts down when assigning keys to non system Opsview dispatcher
CSCtl09530	No channels are displayed in main region when logged in offline mode
CSCtl09568	IDC remote login offline: Direct dial channels remain in yellow triangle
CSCtl09625	Sometimes cannot hear audio from headsets
IP Phone Caveats	
CSCth35283	IPAD client: Saved videos cannot be uploaded to an incident
CSCtj24574	IPhone with 4.0 IOS PTT does not work if RMS is added back after removing
CSCtj24586	IPhone with 4.0 IOS gets stuck on a black screen while changing screen
CSCtj51880	IPhone 4.0 IOS app PTT gets latched when watching video
Radio Caveats	
CSCth48834	Incorrect signal frequencies used for signals in channel
CSCth59065	A defined signal with tone and DTMF does not play the DTMF portion
CSCti55888	Post failover, serial radio is “Socket_Failure” on new active server
CSCtj14046	All Radio Details page shows CS and CF
CSCtj34444	EFJ loses CF status with CF change
CSCtj62644	Win7 MC IDC: Could not PTT EFJ due to exception
CSCtl06684	Radio Talk Permit Tone should only be heard at the local IDC

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.