Release Notes for Cisco CTI OS Release 7.1(1)

September 1, 2006

These release notes describe the new features and caveats for Cisco CTI OS Release 7.1(1).

> **Note** To view the release notes for previous versions of Cisco CTI OS, go to:
> http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html

For a list of the open and resolved caveats for Cisco CTI OS Release 7.1(1), see the section Caveats, page 11. Updates for these release notes occur with every maintenance release and major release.

Contents

These release notes discuss the following topics:

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

Introduction

The CTI OS software Release 7.1(1) supports:

- IP Contact Center Enterprise Edition
- ICM Enterprise Edition
- IP Contact Center Hosted Edition
- ICM Hosted Edition

This document covers the differences between CTI OS 7.0(0) and CTI OS 7.1(1).

Additional information on new features, and on many of the product changes, is available in the relevant end-user documentation.

Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.1(1), Cisco Agent Desktop, Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender) are available separately and are not included as part of these Release Notes.

Note For the most up-to-date version of these release notes, as well as all other CTI OS, ICM/ IP Contact Center documentation, go to the Cisco Web page: http://www.cisco.com

System Requirements

For hardware and third-party software specifications for Release 7.1(1), refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(1) Hardware and System Software Specifications (Bill of Materials)*. This document is available at:
http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1626/ccmigration_09186a00804d7607.pdf.

Related Documentation

Documentation for Cisco CTI Object Server (CTI OS), as well as most related documentation, is accessible from

http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm

Related documentation includes the documentation sets for IPCC/ICM Enterprise & Hosted Editions, Cisco Agent Desktop (CAD), Cisco E-mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).

Also related is the documentation for Cisco CallManager.

New and Changed Information

This section discusses the new features in Release 7.1(1) of Cisco's Computer Telephony Integration Object Server product.

- Citrix MetaFrame Presentation Server 4.0 Support, page 3
- Mobile Agent Support, page 3
- Slient Install, page 3
- Silent Monitoring Architecture Changes, page 4

Citrix MetaFrame Presentation Server 4.0 Support

CTI OS now supports the running of CTI OS Desktop applications within a Citrix MetaFrame Presentation Server 4.0 or a Microsoft Terminal Services (MTS) environment. In addition, the CTI OS Silent Monitor feature is enhanced in Release 7.1(1) to operate in a Citrix environment.

Note Cisco Secure Agent (CSA) does not work in a Citrix MetaFrame Presentation Server 4.0 environment.

This feature is fully supported in CTI OS Release 7.1(1), and supported in Release 7.0(0) with the limitations and caveats documented in the manual *Integrating Cisco CTI OS Into a Citrix MetaFrame Presentation Server Environment*.

Mobile Agent Support

CTI OS Release 7.1(1) supports the Mobile Agent feature. A Mobile Agent is an Agent that is located in a home or remote location and who is using a standard PSTN phone instead of the typical IPCC Agent's IP phone. This feature extends IPCC Enterprise to support agents on non-IP phones.

For information on the installation and configuration steps needed to enable CTI OS support of Mobile Agent, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Editions*.

For information on logging into the CTI OS Agent and Supervisor Desktops as a Mobile Agent, see the *CTI OS Agent Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted* and the *CTI OS Supervisor Desktop User Guide for Cisco Unified Contact Center Enterprise (CCE)*. CTI OS Desktop users in Mobile Agent deployments also need to read the sections "Using Unified Mobile Agent (for Agents)" and "Using Unified Mobile Agent (for Supervisors)" in the *Mobile Agent Guide for Cisco Unified CC Enterprise* for Mobile Agent specific considerations and caveats.

Slient Install

CTI OS Release 7.1(1) supports installation of some CTI OS components in unattended silent install mode. Silent install is supported for the following components.

- CTI OS Agent and Supervisor stand-alone installations
- CTI OS Agent and Supervisor Installation under Citrix
- CTI OS Server Install

Silent install is *not* supported for the following components.

- CTI Driver for Siebel
- Cisco Data Store
- New Silent Monitor Installer introduced in Release 7.1(1)

Note Silent uninstall is *not* supported in Release 7.1(1) for any CTI OS components.

For instructions and syntax for running silent install, and a list of steps that must be performed prior to and immediately following silent install, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.*

Silent Monitoring Architecture Changes

CTI OS Release 7.1(1) introduces a change to the software architecture for Silent Monitoring. A new component is introduced in this release, the Silent Monitor Service (SMS), that uses the same basic method for sniffing packets, but is no longer limited to running on the agent desktop and sniffing packets directly from the agent's IP phone. The supervisor also uses the silent monitor service. This allows the supervisor to hear a forwarded stream when the supervisor desktop is not running on the supervisor's computer such as in Citrix. This software architecture change enables CTI OS based Silent Monitoring in configurations, such as the following, that could not support CTI OS based Silent Monitoring in releases prior to Release 7.1(1):

- Configurations where the agent PC is not connected to the IP phone, including the new Mobile Agent feature
- Configurations where CTI OS Desktop is not running on the agent PC, such as Citrix environments
- Configurations where limited bandwidth is a consideration, such as small remote locations with remote supervisors

This new service acts in a fashion similar to the CIL-integrated Silent Monitor functionality, providing packet sniff-and-forward capability, but its primary benefit is the ability to relocate the SMS anywhere within the network. This allows the SMS to monitor calls at any point where the VoIP is present, for example at an egress Voice Gateway or switch Switched Port Analyzer (SPAN) port. All Agent Desktops are configured with the location of their primary Silent Monitor Service, and will communicate with it in order to initiate a Silent Monitor session.

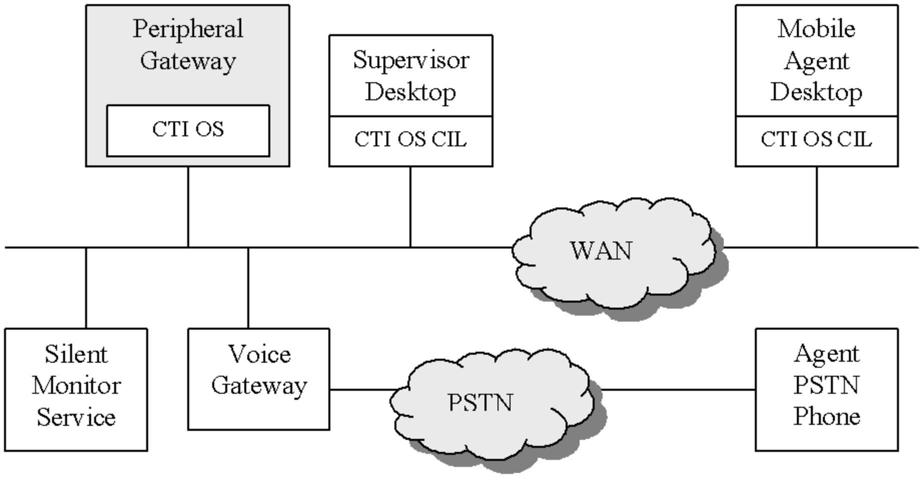
The new control sequence for monitoring an Agent is as follows. As before, a Supervisor that wishes to monitor an Agent within their team would click the Silent Monitor button on the Supervisor Desktop to initiate the session. This sends a request to the supervisor's silent monitor service to setup to receive and playback the agent's voice stream. When the supervisor desktop receives confirmation that the silent monitor service is setup, it sends a request to the CTI Object Server (CTI OS) which locates the Agent and forwards the request to the Agent Desktop CTI OS CIL, same as before. Now however, the Agent Desktop CTI OS CIL will locate the Agent's SMS and forward the request to it to begin the packet sniffing process. The RTP voice packets as seen by the SMS are forwarded directly back to the Supervisor desktop's silent monitor service, where the packets are then played out through the local PC audio card.

For complex deployments with significant numbers of Agents or with one or more remote sites, multiple sniffing points may be required. In this case, additional Silent Monitor Services may be deployed in order to provide complete coverage for Agent monitoring. The group of Silent Monitor Services can then be configured as a cluster to work cooperatively with one another to locate the Agent RTP voice stream regardless of which egress voice gateway is used for the outbound PSTN call. The presence of a cluster of Silent Monitor Services and the process of locating and forwarding the RTP voice stream from within the cluster is completely transparent to the Agent and Supervisor Desktop applications. Release 7.1(1) supports a maximum of two silent monitor services per cluster.

The new SMS is capable of providing Silent Monitoring to the following deployment models that previously could not support Silent Monitoring.

Mobile Agent

The new Silent Monitor Service is of particular interest to the newly introduced Cisco Unified Mobile Agent in release 7.1(1). A Mobile Agent is an Agent that is located in a home or remote location and who is using a standard PSTN phone instead of the typical IPCC Agent's IP phone. The use of a PSTN phone precludes the pre-Release 7.1(1) Silent Monitor feature from working as it does today. RTP voice packets are not sent to the Mobile Agent's phone, and the Mobile Agent's Desktop is no longer located on the network in a location where it has access to the voice stream. The following figure depicts a typical Mobile Agent deployment with the new SMS service.



The Mobile Agent desktop continues to utilize the CTI OS CIL as before. However, the desktop is now located in a remote location across the WAN. Furthermore, the Agent's phone is now receiving analog voice instead of VoIP. As a result of this topology, the Agent Desktop application is no longer able to provide the packet sniff capability necessary for Silent Monitoring. However, the SMS can sniff and forward packets from the IP LAN before the egress gateway.

Citrix or Microsoft Terminal Services Desktops

The SMS also solves the problems presented by a Citrix or Microsoft Terminal Services (MTS) environment. In these environments, the Agent Desktop application is hosted by a central server which may or may not have access to the voice packet stream. The Agent PC, which is the Citrix/MTS client, is still deployed in a fashion similar to the following figure, where it is located behind the Agent IP phone. A supervisor desktop running on a Citrix server can use an SMS deployed on the computer running the supervisor's Citrix client to play back monitored agent conversations.Thus, with the ability to run the SMS locally on the Agent PC, while the Agent Desktop application executes on the central Citrix/MTS server, Silent Monitoring is supported.

Note that this requires the Agent PC to be a regular Windows machine and the SMS service to run as a local service on the PC. This rules out, for example, Citrix ICA appliance devices on the agent desktop.

Java and .NET CIL Based Agent Desktops

Silent Monitoring is not supported with Java or .NET CIL based desktops.

Third Party Applications

CTI Server third party applications that use the CTI Server Message protocol for recording or monitoring are unaffected by the changes discussed in this section.

CTI OS third party applications built on the CTI OS CIL can transparently leverage the Silent Monitor Services that are deployed for Mobile Agents and Citrix/MTS. The custom third party CTI OS Application can simply use the SilentMonitorManager object with the C++ or COM CIL as described in the *CTI OS Developer's Guide* to initiate and respond to silent monitor requests and events. Third Party Applications developed on top of the CTI OS Client Interface Library will reduce deployment complexity and can best leverage the existing Silent Monitor infrastructure.

Important Notes

This section contains important notes for the Cisco CTI Driver for Siebel 7.5 and up and for CTI OS.

Cisco CTI Driver for Siebel 7

The Cisco CTI Driver for Siebel 7 component was not updated for CTI OS Release 7.1(1). There are no installers for the Cisco CTI Driver for Siebel 7 on the CTI OS Release 7.1(1) CD. Use of Release 7.0(0) and earlier versions of the Cisco CTI Driver for Siebel 7 with CTI OS Release 7.1(1) has not been tested and thus is not supported.

For information on the most recent version (Release 7.0(0)) of the Cisco CTI Driver for Siebel 7, please refer back to the *Release Notes for Cisco CTI OS Release 7.0(0)*.

CTI OS

This section contains CTI Release 7.1(1) information for CTI OS.

CTI OS Agent Capacity Information

For specifics on CTI OS agent capacity in this release and conditions under which support of the maximum number of agents is possible, see the *CIsco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specifications (Bill of Materials)* for this release. This document is available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html.

Functionality Not In .NET CIL Release 7.1(1)

Release 7.1(1) of .NET CIL does not support the following CTI OS functionalities.

- Silent Monitor
- Quality of Service (QoS)
- Security

Functionality Not In Java^{TM} CIL Release 7.1(1)

Release 7.1(1) of Java CIL does not support the following CTI OS functionalities.

- Silent Monitor
- Java Bean similar to the CTI OS ActiveX Controls
- Quality of Service (QoS)

Java^{TM} CIL Installation

On Windows systems, use the CTI OS Client installation program to copy the Java CIL files to your system. Be sure to specify CTI OS Developer’s Toolkit on the Select Components screen. Refer to the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for installation instructions.

Note If you install the Java CIL with the CTI OS Client installation program, it will not modify your CLASSPATH environment variable. You will need to modify this environment variable yourself.

On Linux systems, copy the contents of the following directory and all its associated subdirectories from the CTI OS CD to your system:

```
Installs\CTIOSClient\CTIOS_JavaCIL
```

Note For the correct version of RedHat Linux that Java CIL requires on Linux systems, refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(1) Hardware and System Software Specifications (Bill of Materials)*. This document is available at: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1626/ccmigration_09186a00804d7607.pdf.

The CTIOSJavaCIL directory contains three subdirectories.

- **Javadoc**. This directory contains the Java CIL Javadoc files (see the next section).
- **Samples**. This directory contains AllAgents and JavaPhone sample Java CIL programs.
- **Tools**. This directory contains CILTest and TestPhone Java CIL test tools.

Note Java 2SE SDK and Java 2RE SDK Version 1.4.2_10 must also be installed on the client machine prior to using Java CIL.

Silent Monitor

Known Silent Monitor Limitations in Release 7.1(1)

The following limitations exist in the Release 7.1(1) version of the Silent Monitor feature.

- Silent Monitor is supported for use on Cisco IPCC Enterprise *only*. It is *not* supported for use on other ACDs.
- An agent can be monitored only by one supervisor at a time.
- A supervisor can monitor only a single agent at a time.
- A supervisor needs to log on to a hardphone when silent monitoring via the IPCC Supervisor Desktop.
- The following Cisco IP Phones are supported for use with Silent Monitor.
  - 7910+SW
  - 7940/7941

  - 7960/7961
  - 7970

  The 7912 phone does not work, since it does not replicate voice packets on the second port

- Every active Silent Monitor session causes the same amount of network traffic as an additional voice call on the network. The network needs to be provisioned accordingly; see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for guidelines.
- There is no hard limit for concurrent Silent Monitor sessions when monitoring IPCC agents. When using a silent monitor server, the maximum number of concurrent silent monitor sessions is listed in the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(1) Hardware and System Software Specifications (Bill of Materials)*. In addition, the maximum number of concurrent Silent Monitor sessions may be limited by the number of agents and supervisors, as well as the network's ability to handle the additional network traffic (see previous item).
- If agents are using IP hardphones, they need to be left in the default configuration, where voice traffic is replicated on the second port.
- The only supported audio codecs for Silent Monitoring are G.711 and G.729.
- If you unplug a USB digital headset from the USB port during a silent monitoring session and then plug the headset back in, the CTI OS Desktop for IPCC Enterprise application may freeze. Use an analog headset if your environment may require unplugging the headset while monitoring an agent on a call.
- On both Agent and Supervisor XP systems, the Internet Connection Firewall (ICF) needs to be disabled.
- The Silent Monitor feature does not work with the Cisco CTI Driver for Siebel 7.
- Silent monitor servers that supply silent monitor functionality for mobile agents require the silent monitor server, egress gateways, and ingress gateways to all be connected to a switch that supports SPAN. The use of SPAN ports enables the new Silent Monitor Service to monitor agents on any device.

Silent Monitor Does Not Work With All NIC Cards

If the silent monitor service is installed on the agent desktop to silent monitor from a supported IP phone *and* the following conditions are true, the network card and driver in the agent desktop PC need to be capable of capturing packets on a different VLAN in order for Silent Monitor to work.

- If agents use supported IP hardphones with their desktops connected to the second port of the phone
- If the network is configured to use a VLAN for voice traffic

This restriction does *not* apply if the network is not configured to use VLANs.

Cisco testing has determined that several NIC cards manufactured by Intel are not capable of capturing packets from a different VLAN. No workaround exists for the Intel 8255x-based PCI Ethernet Adapter card. A workaround is available for the Intel Pro/1000 and Intel Pro/100 NIC cards; see the following Intel website for information:

http://support.intel.com/support/network/sb/cs-005897-prd38.htm

For NIC cards from other manufacturers, there are procedures you can run to determine if your NIC card can capture packets on a different VLAN.

- If you have Cisco CallManager installed, perform the procedure listed in the *CTI OS Troubleshooting Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, Chapter 1, section “Silent Monitor Problems”, symptom “A Silent Monitor session failed message box appears because the PC cannot capture the voice packets sent from the phone.”. Ensure that the PC is connected to the second port of the hard phone when you perform this procedure.

Cisco CTI OS Does Not Work With All Network Address Translation (NAT) Configurations

If Cisco CTI OS is to be deployed on a network environment where more than one disjoint network is interconnected using NAT, then Cisco Call Manager, the Physical IP Phone, Cisco CTI OS Server, Cisco CTI OS Agent Desktop and the Cisco CTIOS IPCC Supervisor Desktop must be on the same network.

Silent Monitor Service Installer Restriction

The SilentMonitorInstall_nogui.exe installer executable, which silently installs the silent monitor service with default settings, will work only on machines that either do not have WinPCap installed or have WinPCap Release 3.0 installed. For more information on SilentMonitorInstall_nogui.exe, see the *CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise and Hosted Edition*.

Silent Monitor Server Security Hardening Procedure

ICM Security Hardening can be run only on a Windows 2003 Server. To apply security hardening on a Silent Monitor Server, perform the procedure documented in Chapter 4 of the *Release 7.1(1) CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise and Hosted Editions*.

Cisco Secure Agent (CSA) Limitations

You cannot run Cisco Secure Agent (CSA) on a machine that contains CTI OS Client libraries. CSA can run only on machines where CTI OS Servers or standalong silent monitor servers exist.

Also, CSA does not work in a Citrix MetaFrame Presentation Server 4.0 environment.

Supervisor Controls and Agent Not Ready

Making a monitored agent Not Ready is not supported by the supervisor controls. This may be somewhat confusing to the user since the option is not grayed out like other unsupported features.

Important Notes about Server to Server Integration

If you are planning to use CTI OS to do a server to server integration in Agent mode, please note the following design considerations.

- Server integrations will need to use a separate AgentMode session per agent. This means that there are resource considerations for the machine since each session has four threads and one socket. Depending on the capabilities of the system in areas such as RAM and processing power, the limit for the number of agents that is practical will vary.

- If Skillgroup statistics are desired, a separate MonitorMode session should be used to receive them. You must then open a MonitorMode session and set a special filter "filtertarget=skillgroupstats". Then, use the EnableSkillGroupStatistics method on the Session object (do *not* use the one on the Agent object). Call it once for each SkillGroup you want to receive statistics for. Each time you will provide the SkillGroup Number and Peripheral ID. See the section “Filtering Skillgroup Statistics” in the *CTI OS Developer's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.
- After a failover you need to reenable the SkillGroup statistics because the CIL will not automatically do this for the MonitorMode session. If you receive an OnConnectionFailed the CIL will go into failover. If this happens, wait for an OnConnection event before calling the EnableSkillGroupStatistics method.

Connecting CTI OS Agents and CAD Agents to the Same PG

CTI OS desktops and a Cisco Agent Desktops (CAD) can be concurrently connected to the same PG. When this configuration is deployed, be aware that the CAD Agents will work only with the Cisco Supervisor Desktop and CTI OS Agents will work only with the IPCC CTI OS Supervisor Desktop. Supervisors cannot manage mixed Agent types. Also, other functions such as chat and silent monitoring will only work for teams using the same desktop type.

Supported ACDs

For information about the Automatic Call Distributors (ACDs) that are supported by the CTI OS Release 7.1(1), refer to the document *Cisco ICM Software Supported Switches* document located at

http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/acddoc/index.htm

Supervisor Desktop Barge In on Consult Call Not Supported

Due to a Cisco CallManager limitation, the Barge In operation on the IPCC Supervisor Desktop is not supported when an agent is on a consult call. An attempt to perform such an operation results in the following message.

```
"IPCC Error[20999] CallManager - Unknown Call Manager Failure on Operation".
```

Installation Notes

See the *CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for CTI OS Release 7.1(1) installation information.

Caveats

This section contains information on resolved and open caveats in CTI OS Release 7.1(1) and gives instructions for using Bug Toolkit.

Resolved Caveats in the CTI OS 7.1(1) Release

Resolved caveats are no longer listed in these Release Notes. Instead, you can find the latest resolved caveat information through Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs. For a keyword search of the CTI OS defects using the Bug Toolkit, select the product Cisco Computer Telephony Integration Option. For instructions on using Bug Toolkit, see the section "Bug Toolkit"

Open Caveats in CTI OS 7.1(1) Release

This section contains a list of defects that are currently pending in CTI OS Release 7.1(1). Defects are listed by component and then by identifier. For a keyword search of the CTI OS defects using the Bug Toolkit, select the product Cisco Computer Telephony Integration Option.

Table 1 Open Caveats for Cisco CTI OS Release 7.1(1)

Identifier	Component	Headline
CSCsd74550	ctios.ctidriver	OPC failover, Agent not ready after completing failed over call
CSCsa60345	cti.ctisim	CtiServer Simulator needs to be updated to support protocol 11 for R 7
CSCsb50684	ctios.ctiosclient	Conference controller unable to retrieve the call after PG failover
CSCsd84306	ctios.ctiosclient	Agent desk setting for screen not picked up with toolkit phone
CSCsd75899	ctios.javatestphone	JAVA CIL tracing does not expand %HOMEDRIVE% and %HOMEPATH%
CSCsa65256	ctios.server	Possible Memory Leak in CtiosServerNode
CSCsb57001	ctios.server	Ringing call not displayed in CTIOS Softphone after PG failover on G3
CSCsa70119	ctios.server	CTIOS Agent Desktop hangs after second Single Step Transfer
CSCsb59495	ctios.server	Service Observer softphone hangs after PG failover
CSCsb73210	ctios.server	After PG failover on G3, 'Not Ready' agent Desktop hangs
CSCsb11119	ctios.softphone	After PG/CG failover supervisor cannot silent monitor. Must restart app.
CSCsb44233	ctios.softphone	Call status shows "Cleared" after releasing a conference call.
CSCsb69958	ctios.softphone	ctios agent desktop only takes max 39 charaters for call variables
CSCsc13769	ctios.softphone	Unable to retrieve a consulted call-after the consulted agent drops call
CSCsc38998	ctios.softphone	Agent softphone hangs when CTIOS server is cycled during conference
CSCsd67233	ctios.softphone	Logging out of CTIOS desktop is slow due to SilentMonitorEnabled=1
CSCsd72703	ctios.softphone	MakeCall Control missing the Enable Post Route option
CSCsc20162	ctios.supervisor	Supervisor desktop hangs on emergency and supervisor assist.
CSCse13150	ctios.setup	Uninstalling the CTIOS 7.1(1) patch does not uninstall SMS

Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser

- Cisco.com user ID and password

Procedure

Tips To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Step 1 Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco ICM/IPCC Enterprise and Hosted Editions, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Computer Telephony Integration Option** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Computer Telephony Integration Option**.

Step 4 Click **Next**. The Cisco Computer Telephony Integration Option search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Select the Cisco Computer Telephony Integration Option version:

- Choose the major version for the major releases.

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information.

  A revision release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

b. Choose the Features or Components to query; make your selection from the "Available" list and click **Add** to place your selection in the "Limit search to" list.

To query for all caveats for a specified release, choose "All Features" in the left window pane.

Note The default value specifies "All Features" and includes all of the items in the left window pane.

c. Enter keywords to search for a caveat title and description, if desired.

Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

d. Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the Fixed check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

Step 6 Bug Toolkit returns the list of caveats on the basis of your query. You can modify your results by submitting another query and using different criteria.

Documentation Updates

The following CTI OS documents have been revised for CTI OS Release 7.1(1).

- *CTI OS Developer's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
- *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
- *CTI OS Supervisor Desktop User Guide for Cisco Unified Contact Center Enterprise and Hosted*
- *CTI OS Agent Desktop User Guide for Cisco Unified Contact Center Enterprise and Hosted*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html