Release Notes for Cisco CTI OS Release 7.0(0)

November 18, 2005

These release notes describe the new features and caveats for Cisco CTI OS release 7.0(0).

Note To view the release notes for previous versions of Cisco CTI OS, go to: http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/

Before you install Cisco CTI OS, Cisco recommends that you review the section Important Notes, page 6 for information about issues that may affect your system.

For a list of the open and resolved caveats for Cisco CTI OS Release 7.0(0), see the Resolved Caveats in the CTI OS 7.0(0) Release, page 17 and the Open Caveats in CTI OS 7.0(0) Release, page 18. 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 7.0(0) 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 6.0(0) and CTI OS 7.0(0).

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 7.0(0), 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 7.0(0), refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*, which is accessible from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

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 in somewhat more detail the new features in Release 7.0(0) of Cisco's Computer Telephony Integration Object Server product.

Support for Secure Connections (SSL)

The 7.0(0) version of CTI OS provides support for Transport Layer Security (TLS) for traffic between CTI OS Server and CTI OS Clients (COM/C++ CILs only) and between peer CTI OS Servers.

Enabling this security requires:

- Linking custom client application with new security libraries (build time).
- Setting security registry value on server (install time)
- Creating certificate requests on client and server (install time)
- Signing certificate requests by the same certificate authority (manual step)

Performance Improvements on the CTI OS Server

The following features have been included on the CTI OS Server to improve its performance:

- Maximum number of agent connections increased to 1000 (thousand) per PG pair. A Solutions Reference Network Design guide (SRND) will be forthcoming. This document will describe CTIOS sizing considerations in more detail..
- Improved statistics distribution to smooth out network traffic bursts due to statistics.
- More efficient messaging, resulting in a reduction in bandwidth usage.
- The number of CTI OS server processes is reduced from two to one.

Support for Quality of Service (QoS)

The CTI OS Release 7.0(0) supports the marking of packets with "Type of Service" (ToS). It also allows for preferential treatment of CTI signaling traffic if network is configured to support that QoS scheme.

Note The support for QoS is applicable to COM/C++ CILs only.

Setting outbound QoS on client requires:

- Enabling user ToS in Windows registry
- Setting CTIOS_TOS property of Session object
- Setting CTIOS_TOS property of SilentMonitorManager

Support for .NET Framework

Cisco CTI OS Toolkit 7.0(0) introduces support for application development targeting the Microsoft .NET Framework 1.1 (Service Pack 1 inclusive) and Microsoft Visual Studio .NET 2003. Cisco CTI OS Toolkit 7.0 provides a native .NET class library (.NET CIL) and runtime callable wrappers for COM CIL and the CTI OS ActiveX controls.

The .NET CIL and the runtime callable wrappers (RCWs) are installed in the Global Assembly Cache (GAC) by the setup program such that all the components are available to any of the samples included in the toolkit and any new application in development.

The .NET CIL provides native .NET class libraries for developing native .NET Framework applications. It is built using the same architecture as the Java CIL and the interface is also similar to C++ with some differences. As a result, a developer porting a C++ CIL application to .NET CIL should find it fairly easy to switch between the two. Along with the native .NET class libraries and RCWs, version 7.0 also provides a rich set of sample code illustrating agent, supervisor, and outbound functionality as well as monitor mode programming. Also included is a .NET version of CilTest.

Note QoS, Silent Monitor, and Security not yet supported in .NET CIL

Siebel Support of Outbound Option

For complete and current information about the Siebel versions supported by CTI OS version 7.0(0), see the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials (BOM). The ICM BOM is available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

The Cisco Siebel driver now supports Outbound Option.

Note The Siebel support for Outbound Option is now available only for IPCC and Avaya.

The Cisco Outbound Option (formerly known as Cisco Blended Agent) is supported with the Cisco Driver for Siebel 7 starting the ICM Release 7.0(0). A set of sample DEF files demonstrate how to provide access to the Outbound Option related functionality from the Siebel desktop. The Outbound Option has a special set of ECC variables to ferry requests and responses between agent desktop and the Dialer.

An Outbound Option configuration can have the following modes:

1. Progressive
2. Predictive

3. Preview
4. Direct Preview

Sample DEF files are provided for all supported modes. These DEF files incorporate the Outbound Option functionality in the form of menu options on the Siebel Communications Menu. When imported into a Siebel configuration for a chosen mode, the sample DEF file provides support for handling Outbound related requests and appropriate event handling.

Note This version of CTI OS requires the customization of the Siebel Communications Toolbar if outbound option functionality through the toolbar is desired.

Support for Hosted IPCC

CTI OS 7.0(0) provides support for Hosted IPCC. Following are the major features:

- Multiple instances of CTI OS Server can be configured on the same physical server.
- Service providers can deploy up to 10 instances of CTI OS Server on one physical box.
- Supports Security, Silent Monitor, and QoS.
- Maximum number of agents distributed across all instances of CTI OS on a duplex server will be less than on a single instance

Support for Login by Login Name, Skillgroup Name, and Agent Name

CTI OS 7.0(0) provides support for Login by Login Name. Depending on the option chosen for logging in during the installation of the CTI OS Server, the Login dialog on the Agent desktop or the Supervisor Desktop will prompt for either the Agent/Supervisor ID or the Login Name.

Agent login can now be performed in the following two ways:

- By Agent ID (numeric) – using the CTIOS_AGENTID
- By Login Name (alpha numeric) – using the CTIOS_LOGINNAME (new)

In the CTIOS Server setup application only Peripheral Types of IPCC, System IPCC, and IPCC Hosted Edition have the “Login By” group box enabled where you can choose between logging in by Agent ID or by Login Name.

The "Login By" setting determines how CTI Toolkit Agent and Supervisor desktops allow Login and Chat request (either AgentID OR LoginName). This setting does not affect other CTI applications. CTI OS Server itself can service Login requests both ways (by AgentID and by LoginName) for IPCC. All other peripheral types will login by Agent ID only, and the choice is disabled. If this is to be a multi-instance environment, select “IPCC Hosted Edition".

Note The ODBC configuration requirement for Agent name (First/Last name) support has been eliminated in the 7.0(0) Release. The First/Last name of the Agent is automatically received now.

CTI OS clients receive skillgroup name information in new event (SkillInfoEvent).

Support for Dynamic Reskilling

The CTI OS 7.0(0) release has been enhanced to provide for dynamic reskilling of IPCC agents. The following features support for re-skilling:

- No CTI OS Server restart required after re-skill.
- Real Time Status grid on the supervisor desktop updated with skillgroup changes (both skillgroup number and skillgroup name)
- Skillgroup statistics will be updated appropriately after a reskill.
- CTIOS_NUMSKILLGROUPS and Skillgroup[x] properties on Agent objects are updated appropriately after reskill

Addition of Accessibility Features to the CTIOS Agent Desktop

In version 7.0(0) of CTI OS, accessibility features have been added to the CTI OS Agent Desktop to make the desktop more navigable by keyboard as well as readable by the JAWS Screen Reader. Please see the *CTI OS Agent Desktop User Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more information.

Migration from Media Termination to IP Communicator

In release 7.0(0) of CTI OS, the IP Communicator replaces CTI Media Termination product as the supported softphone solution.

Note Media Termination customers upgrading to 7.0 must move to IP Communicator.

Important Notes

The following sections contain important information that may have been unavailable upon the initial release of documentation for Release 7.0(0).

Patch Behavior

Because of the way the patching mechanism works, CTI OS is viewed as a single product. Since patches must be removed before an installation can take place, Setup will remove patches applied to one CTI OS component when another CTI OS component is being applied.

As a particular example:

Suppose CTI Driver for Siebel 7 (CTI OS Release 7.0(0)) has had Service Release 2 installed. You now attempt to install a component of the CTI OS Client 7.0(0) Software Development Toolkit. Setup will uninstall the patches applied to CTI Driver for Siebel 7 (that is, will uninstall SR2), install the component of the Development Toolkit, and then inform you that you need to reinstall the patches.

That is, all CTI OS Software components (CTI OS Server, CTI OS Client, CTI Driver for Siebel 7, and Cisco Data Store) that are installed on the same box must have the same level of patching, even though some patches will only apply to a subset of the components.

Limitation to Where the Cisco Data Store Resides

Cisco Data Store cannot reside on the same machine as the CTI OS Server, ICM PG or any other ICM components. It also cannot reside on the same machine as the Siebel Communication server.

Note If you're looking for the *CiscoDataStore* directory in the CTI OS Installation CDs, please look for the directory *CTIOSObjectStore.* You will find the contents of the Cisco Data Store in there. If it helps, rename the directory to *CiscoDataStore*.

/LOAD 0 (Forced NotReady) vs. /LOAD 1 (Forced LogOut)

Note This setting applies to IPCC only.

"/LOAD 0", agents are taken to the not ready state, or if talking, they are set to not ready when the call ends, which helps in fail over situations. This would mean less traffic, better performance, and less chance of call context loss.

While "/LOAD 1", agent is forced logged out when a CTI component fails, the agent always attempts to initialize from a logged out state. If it is in logged in state, the PIM will attempt to log it out. It remembers agent state and will attempt to bring it back to the previous agent state after logging back in on fail over scenarios.

The default behavior for ICM version 7.0 if no parameters are set is "/LOAD 0". Also, all CTI OS versions recommends "/LOAD 0" in order for CTI OS failover to work correctly.

The behavior of the system depends on whether "/LOAD 0" or "/LOAD1" is set. The behavior of the system is as follows when "/LOAD 0" is set:

- Log in an agent using CTI OS agent desktop, and then close the CTI OS agent desktop without sending SetAgentStateRequest(Logout). The PIM will change the agent state to NotReady. The next time you log in the same agent, you will NOT receive AgentStateEvent because the agent state at the PIM is NotReady.
- Log in an agent using CTI OS agent desktop, then explicitly log the agent out by sending SetAgentStateRequest(Logout), and then close the CTI OS agent desktop The next time you log in the same agent, you will receive AgentStateEvent.

The behavior of the system is as follows when "/LOAD 1" is set:

- Log in an agent using CTI OS agent desktop, and then close the CTI OS agent desktop without sending SetAgentStateRequest(Logout). The PIM will change the agent state to Logout. The next time you log in the same agent, you will receive AgentStateEvent.
- Log in an agent using CTI OS agent desktop, then explicitly log the agent out by sending SetAgentStateRequest(Logout), and then close the CTI OS agent desktop The next time you log in the same agent, you will receive AgentStateEvent.

So with "/LOAD 0", the CTI OS agent desktop receives AgentStateEvent at login time only if the agent state at the PIM was Logout.

The custom application that is supporting "/LOAD 1" only needs to make necessary changes in order to support "/LOAD 0". The changes are broken into two phases:

1. Login phase

Since we don't receive AgentStateEvent in all cases, the custom application needs to depend on OnQueryAgentStateConf instead. At login time, the custom application will receive 2 OnQueryAgentStateConf. The first one gets generated when SetAgentMode() method gets called, and the second one gets generated when SetAgentState() gets called. Here are the steps that can be used to achieve a login:

   a. Custom application calls SetAgentMode(), (NOTE: The SetAgentMode() method generates OnSetAgentModeEvent and OnQueryAgentStateConf) and then it waits for OnSetAgentModeEvent.
   b. After receiving OnSetAgentModeEvent and OnQueryAgentStateConf, the custom application calls Login() method and it waits for OnQueryAgentStateConf (NOTE: The Login () method generates OnQueryAgentStateConf).
   c. When the custom application receives the second OnQueryAgentStateConf, then the login phase succeeds.

2. Logout phase

The custom application needs to explicitly log the agent out before disconnecting from the CTI OS Server, otherwise the agent stays in a state other than Logout. To explicitly log an agent out that is already logged in, call Logout() method, and then waits for AgentStateEvent.

Addition of ConsoleTraceMask

A new DWORD registry value called "ConsoleTraceMask" has been added. It is a bitmask that specifies the level of console tracing that are enabled. This registry value is not added to the registry at install time, and its default value is 0x3. If a customer wants to print out more information to the CTI OS Server console window, then this registry value needs to be added under the following registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<customer_instance_name>\CTIOS1\EMS\CurrentVersion\Library\Processes\ctios]

Adding a Standalone CTI OS Server to the Firewall Exception List

If the CTIOS Server is co-located with PG, then all the necessary scripts that allow to add servers to the firewall exception list are available on the system. These scripts are a part of the ICM install.

If a standalone CTI OS Server is installed on Win2003 SP1 server and Windows firewall is ON, then the customer needs to run a script to add CTI OS Server to the Windows firewall exception list. The *Security Best Practices Guide* details how to use the script which is located in the ICM CD under a directory called FirewallConfig.

Cisco Data Store on the Firewall Exception List

If Cisco Data Store is installed on Win2003 SP1 server and Windows firewall is ON, then the customer needs to run a script to add Cisco Data Store to the Windows firewall exception list. The *Security Best Practices Guide* details how to use the script which is located in the ICM CD under a directory called FirewallConfig.

CTI OS Server Behavioral Changes: MinimizeAgentStateEvents Registry

The MinimizeAgentStateEvents registry value exists under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco systems, Inc.\Ctios\<Customer-Instancename>\CTIOS1\Server\Agent

This registry value controls number of AgentStateEvent(s) that the Ctios Client receives from the Ctios Server. If this registry value is set to 1, then the CTI OS Client receives one AgentStateEvent from Ctios Server. If it is set to 0, then CTI OS Client receives all AgentStateEvent(s) that were sent from CtiSvr to CTI OS Server.

Ctios Server doesn't use the MinimizeAgentStateEvents registry value in Release 7.0 anymore, instead Ctios Server uses an internal value which turns MinimizeAgentStateEvents OFF.

System IPCC's Installation of CTI OS Server

Following are some of the restrictions with the System IPCC's Installation of the CTI OS Server:

- The System IPCC installer automatically installs CTI-OS server on the Agent Controllers. You should not run the CTI-OS server installer manually. Doing so may break your installation.
- System IPCC does not support CTI-OS QoS (QoS from CTI-OS client to CTI-OS server) as this turns off skillgroup and agent statistics.
- System IPCC does not support CTI-OS server-client security

Automatic Installation of Silent Monitor

With the 7.0(0) Release, Silent Monitor is no longer a choice to be installed separately. Instead, if you select "Agent Desktop", the agent component for Silent Monitoring (WinPCap) will be automatically installed. If you select "IPCC Supervisor Desktop", the Silent Monitor components for supervisor are also installed and an additional screen appears first. Please read this screen carefully; it contains important information about using Silent Monitor in a VLAN network.

C++ CIL: SetAgent Return Error Codes

Until the Release 6.0 of CTI OS, the C++ CIL public method SetAgent always returned CIL_OK.

In the 7.0(0) Release, the SetAgent request returns the following error codes:

- CIL_FAIL if request to authenticate the agent fails. The SetAgent request will not be sent.
- E_CTIOS_SET_AGENT_SESSION_DISCONNECT_REQUIRED if you attempt to SetAgent for a session in monitor mode. The SetAgent request won't be sent. In order to successfully execute a SetAgent, a session Disconnect is required first.
- E_CTIOS_AGENT_ALREADY_IN_SESSION if you attempt to SetAgent that is currently already set in this session. The SetAgent request will not be sent.

Note In the above cases of error, the SetAgent request won't be sent to CTIOSServer and the client application will not receive any events in return.

- CIL_OK if a SetAgent request was sent to the CTI OSServer.

Reduced number of Peer Server Support

The CTI OS Server may enter only one peer server in the registry instead of the three that have been supported in releases prior to 7.0(0). As a result, if user upgrades from an earlier version to 7.0 in an environment where there had been three peer servers configured, after running the setup, only the first peer server (in alphabetical order) will be retained. The other two peer servers will have been deleted.

Reduction in Win32 Samples

The 6.0 Win32 AllAgents and AllCalls samples have been replaced with similar samples built on top of the .NET CIL. Therefore there’s a reduction in the number of Win32 samples used in the 7.0(0) Release. Please see the CTI OS Developer’s Guide for the location of these samples.

Following were the Win32 samples used in 6.0(0) Release:

```
C++/C++Phone
COM/C++/COMPhone
COM/VB/BlendedAgentPhone
COM/VB/SimplePhone
COM/VB/VBPhone

MonitorSamples/AllAgents
MonitorSamples/AllAgentsMonitor
MonitorSamples/AllCalls
MonitorSamples/CILMonitor
```

Following are the Win32 samples that are used in the 7.0(0) Release:

```
AgentDesktop
IPCCSupervisorDesktop
OutboundOptionDesktop (BAPhone)
C++Phone
```

Cisco CTI Driver for Siebel 7.5 and up

This section contains CTI Release 7.0(0) information for the Cisco CTI Driver for Siebel 7.5 and up.

Supported Siebel Versions

For complete and current information about the Siebel versions supported by CTI OS version 7.0(0), see the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials (BOM). The ICM BOM is available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

Version Restrictions within a Peripheral Gateway

If Siebel upgrades are in progress on a given Peripheral Gateway (PG) or PG pair, it is permissible for some agents to still be running Siebel version 7.5.x while other agents are running Siebel version 7.7. However, these versions of Siebel cannot share a Siebel database between them, and any given agent cannot be configured for both versions. This cross version support is allowed only for the period of migration from one version of Siebel to the other. It is strongly recommended that all agents be upgraded to the newer version of Siebel as quickly as possible.

CTI OS/Siebel Driver Compatibility

CTI OS Release 7.0(0) supports Release 7.0(0) of the CTI Driver for Siebel 7. Customers are expected to upgrade to the Siebel Driver for Release 7.0(0) as soon as possible after the upgrade to CTI OS Release 7.0(0) is complete.

Installation Packages and Version Support

CTI Release 7.0(0) includes the installation package for the Cisco CTI Driver for Siebel 7.5 and up. This package is located in the folder named 'Siebel75plus' in the Install directory on the CTI OS CD and supports Siebel version 7.5.2 and up.

Cisco Data Store

A socket version of Cisco Data Store is provided on the CTI OS CD. If you are running Cisco Data Store with the Cisco CTI Driver for Siebel 7, you must use this socket version.

To install, configure, and use the socket version of Cisco Data Store, perform the following steps:

- Follow the instructions in the *CTI Driver for Siebel 7 Reference Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* to install Socket CDS. The installation process sets the default listen port as 42027; you can change this value by modifying the Registry.
- Add the following parameters to the Cisco CTI Driver for Siebel 7 DEF file:

  ```
  Driver:DataServerName = "CiscoDataStoreHostName"
  Driver:DataServerPort = "42027"
  ```

  See the *CTI Driver for Siebel 7 Reference Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for information about the DEF file.
- Start the Socket Cisco Data Store process (process name is ctiosdatastore) from ICM Service Control.

Siebel Release Restriction

All agents connected to a Cisco Data Store *must* be running the same release of Siebel. Cisco Data Store does *not* support configurations in which agents are running different releases of Siebel.

Cisco Data Store Capacity with Siebel 7 Driver

With the Siebel 7 driver, Cisco Data Store supports a maximum of 20,000 agents. (The Cisco Data Store capacity with the Siebel 6 driver is much lower; see the *Release Notes for Service Release 3 for Cisco CTI Software Release 4.7* for specifics.)

The *actual* number of agents your Cisco Data Store will be able to support may be less than 20,000 agents, and will depend on the following factors.

- Number of transfer calls per second.
- Amount of data transferred between agents and Cisco Data Store
- CPU processor speed
- Memory size

It is important to ensure that CPU usage does not regularly exceed 50% during normal operation of the server when fully loaded. Since performance is affected by many factors including CPU capacity, it is important to monitor your system to determine the maximum number of agents you can support without exceeding the 50% CPU usage limit.

For example, Cisco testing has determined that Cisco Data Store can support 20,000 agents in the following configuration:

- Cisco Data Store residing on a Windows 2000 system that meets the recommended hardware requirements stated in the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*, which is accessible from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm
- Simplex system (Cisco Data Store does not support fault tolerance)
- Cisco Data Store trace mask is set to 0x7
- 200 calls per second
- A call ratio of 60% standard calls and 40% transfer calls
- 600 bytes of data transferred per call
- Call duration is 100 seconds

The Cisco Data Store cannot reside on the same machine as the ICM Peripheral Gateway (PG) or any other ICM components. It also cannot reside on the same machine as the Siebel Communication Server.

Up to 50 Siebel 7 drivers can connect to a single Cisco Data Store.

See the *CTI Driver for Siebel 7 Reference Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for additional Socket CDS usage and troubleshooting information.

Cisco Data Store Data Transfer Limitation

The largest data block that Cisco Data Store can transfer in a single operationis 65,535 bytes (including a 12-byte header). The actual maximum may be less for a given transfer depending on such factors as type of data, number of data items, and number of keywords.

Siebel Driver Does Not Work with Silent Monitor

The CTI OS Silent Monitor feature does not work with the Cisco CTI Driver for Siebel.

CTI OS

This section contains CTI Release 7.0(0) information for CTI OS.

Functionality Not In Java™ CIL Release 7.0(0)

Release 7.0(0) of Java CIL does not support the following CTI OS functionalities.

- Media Termination
- Silent Monitor
- Java Bean similar to the CTI OS ActiveX Controls

Java™ 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 Intelligent Contact Management Software Release 7.0(0) Bill of Materials*, which is accessible from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

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 must also be installed on the client machine prior to using Java CIL.

Silent Monitor

Known Silent Monitor Limitations in Release 7.0(0)

The following limitations exist in the Release 7.0(0) 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 Softphone. The following Cisco IP Phones are supported for use with Silent Monitor.
  - 7910+SW
  - 7940
  - 7960
  - 7970

  The 7912 phone does not work, since it does not replicate voice packets on the second port
- Agents need to be logged on to a supported hardphone with the Agent desktop PC connected to the second port of the phone (see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*) or via Media Termination.
- 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. However, 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 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.

Silent Monitor Does Not Work With All NIC Cards

If agents use supported IP hardphones with their desktops connected to the second port of the phone *and* if the network is configured to use a VLAN for voice traffic, 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. This restriction does *not* apply if the network is not configured for 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 and the Intel 8255x-based PCI Ethernet Adapter cards. 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: Developer Information

Note This section pertains only to developers creating custom applications using Silent Monitor. The out-of-the-box CTI OS Supervisor Desktop and CTI OS Agent Desktop install applications perform all required configuration automatically.

For supervisor desktops using silent monitor, you need to install the following files:

- ccnsmt.dll - this file is the COM dll that transmits monitored audio via the sound card. It must be registered. (e.g. regsvr32 ccnsmt.dll)
- libg723.dll - this file is a dependency of ccnsmt.dll. ccnsmt will fail to register without it
- traceserver.dll - this is the tracing mechanism for ccnsmt.dll

For agent desktops using silent monitor you need to run the WinPcap install executable:

- WinPcap_3_0_nogui.exe

The CTIOS silent monitor feature requires that you modify a WinPcap registry setting after installing (or reinstalling) WinPcap. In the Windows registry go to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NPF

Change the value of the Start setting under this key from 0x00000003 to 0x00000002. Reboot the PC.

Cisco Secure Agent (CSA) Limitation

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 exist.

Citrix and Windows Terminal Services

The CTI OS Agent or Supervisor Desktops are supported in the Citrix and Windows Terminal Services environments. In addition, the CTI Desktop Toolkit allows development of custom applications built using the C++ CIL, .NET CIL, and Java CIL for the Citrix and Windows Terminal Services environments.

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 (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.

CTI OS Agents and CAD Agents Cannot Share a PG

If both a CTI OS desktop and a Cisco Agent Desktop (CAD) are used, the CTI OS agents and the CAD agents must be placed on separate PGs.

Supported ACDs

For information about the Automatic Call Distributors (ACDs) that are supported by the CTI OS Release 7.0(0) refer to the *Cisco Compatibility Matrix*.

Resolved Caveats in the CTI OS 7.0(0) 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.

Tips You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

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

Open Caveats in CTI OS 7.0(0) Release

This section contains a list of defects that are currently pending in CTI OS Release 7.0(0). 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.

Tips If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 1 Open Caveats for Cisco CTI OS Release 7.0(0)

Identifier	Component	Headline
CSCsa60345	cti.ctisim	CtiServer Simulator needs to be updated to support protocol 11 for R 7
CSCsa95104	cti.sample-code	Empty MessageBox after starting CTI Toolkit Combo Desktop .NET
CSCsb10849	cti.sample-code	All Calls Sample.NET and CtiOs Data Grid.NET Do Not Build
CSCsb12950	cti.sample-code	Windows User Names with Spaces Break Combo Desktop
CSCsb19837	cti.siebel	An attempt is made to write a record to CDS at the start of every call
CSCsa65256	ctios.server	Possible Memory Leak in CtiosServerNode
CSCsa99735	ctios.server	CTIOS Server shows exceptions in process window on start
CSCsb10071	ctios.server	CTIOS Desktop of Calling agent hangs when RONA call goes to VRU.
CSCsb15438	ctios.server	Multiple call is present in ctios grid after supervisor barge-in
CSCsb16604	ctios.server	CTIOS Server crashing after 12 hours of load at 2cps
CSCsb18111	ctios.server	BringtToFront desktop setting for .NET Sample Phone not working properly
CSCsb35744	ctios.server	Unable to complete CDN Conference call in Symposium
CSCsa94673	ctios.setup	TOS Registry Setting Removed when CTIOS Client Uninstalled
CSCsb20552	ctios.setup	SIPCC Install/CTIOS Server Install: Missing EMSTraceServer key
CSCsb11119	ctios.softphone	After PG/CG failover supervisor cannot silent monitor. Must restart app.
CSCma25978	ctios.supervisor	Supervisor Desktop memory leak on login/logout
CSCsb36857	setup	The url to Dynamic Reskilling is missing when installed with icm setup
CSCsb99693	documentation	CTIOS 7.0 Client Installer Installs 6.0 Documentation

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.

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