CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted

Release 8.5(3)
September 2011

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Customer Order Number:

CONTENTS

INDEX

About This Guide

Purpose

This manual provides instructions for installing, configuring, and running the Cisco CTI Object Server (CTI OS) product.

Release 8.0(1a) is an update of Release 8.0(1) that includes installation support for Windows Server 2008 R2 (when used with the release 8.5(2) or later Maintenance Release). Release 8.0(1a) supersedes and replaces the previous Release 8.0(1) install media. There are no additional capability or feature changes in Release 8.0(1a) for systems running Windows Server 2003.

Documentation for Release 8.0(1a) has been updated to include Windows Server 2008 R2 installation and configuration support. However, the documentation and application screens refer to the release as "Release 8.0(1)". The remainder of this document also refers to release 8.0(1a) as Release 8.0(1).

Audience

This manual is for system administrators and other personnel who are responsible for installing and maintaining CTI OS and its associated components. You must have administrator privileges to perform the procedures discussed in this manual.

Organization

The manual is divided into the following chapters.

Chapter	Description
Chapter 1, "Introduction"	Provides an overview of Cisco CTI Object Server (CTI OS) and lists the tasks that a CTI OS system manager must perform.
Chapter 2, "CTI OS Server Installation"	Provides procedures for installing CTI OS Server.
Chapter 3, "CTI Toolkit Desktop Client Installation"	Provides procedures for installing CTI OS Client components.
Chapter 4, "Installing and Configuring CTI OS Silent Monitor"	Discusses the process of installing the new functionality in CTI OS Release 8.0(1).
Chapter 5, "Installing, Uninstalling, and Failed Installation Recovery of CTI OS Release 8.0(1) Components"	This chapter discusses the silent installation and uninstallation of CTI OS Release 8.0(1) components. In addition, it discusses the steps necessary to recover from a failed installation of CTI OS components.
Chapter 6, "Configuring Unified CM-Based Silent Monitor"	Discusses how to configure devices and JTAPI users on Unified CM 6.0 to enable silent monitor.
Chapter 7, "CTI OS Security"	Provides information to the System Manager about configuring the CTI OS Security Certificate and the Security Compatibility.
Chapter 8, "CTI OS Configuration"	Explains how to start and stop CTI OS and its associated processes and describes how CTI OS handles failover scenarios.
Chapter 9, "Startup, Shutdown, and Failover"	Discusses how to use the Windows Registry Editor to configure CTI OS.
Chapter 10, "Peripheral-Specific Support"	Discusses levels of CTI OS support for switch-specific features.
Appendix A, "Testing an Ethernet Card for Silent Monitor"	Discusses testing an ethernet card for silent monitor, including test target preparation, preparing the packet generator host, and test execution.

Related Documentation

Documentation for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at

http://www.cisco.com/cisco/web/psa/default.html?mode=prod.

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (Unified CVP), Cisco Unified IP IVR (Unified IP IVR), Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).

- For Cisco Unified Contact Center Products documentation and for Cisco Unified Communications Manager documentation, go to http://www.cisco.com/cisco/web/psa/default.html?mode=prod.
Click **Voice and Unified Communications > Customer Contact > Cisco Unified Contact Center Products**, and choose the appropriate product/option.
- For troubleshooting tips for these Cisco Unified Contact Center Products, go to http://docwiki.cisco.com/wiki/category:Troubleshooting, then click the product/option you are interested in.
- Technical Support documentation and tools can be accessed from http://www.cisco.com/en/US/support/index.html
- The Product Alert tool can be accessed through (login required) http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice

Conventions

This manual uses the following conventions.

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Choose **Edit > Find** from the Configure menu bar.
Italic type indicates one of the following: • A newly introduced term • For emphasis • A generic syntax item that you must replace with a specific value • A title of a publication	• A *skill group* is a collection of agents who share similar skills. • *Do not* use the numerical naming convention that is used in the predefined templates (for example, **persvc01**). • IF *(condition, true-value, false-value)* • For more information, see the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted.*
An arrow (>) indicates an item from a pull-down menu.	The Save command from the File menu is referenced as **File > Save**.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending an email message to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

CHAPTER 1

Introduction

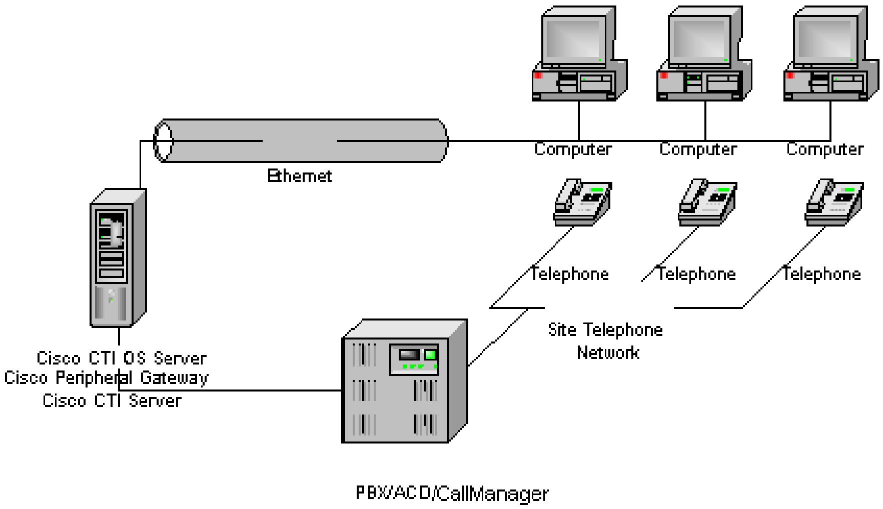
This chapter provides an overview of Cisco CTI Object Server (CTI OS) and lists the tasks that a CTI OS system manager must perform. It contains the following sections:

- "Overview of CTI OS" on page 1
- "System Manager Responsibilities" on page 3
- "System Requirements" on page 4
- "Silent Monitoring" on page 5.

Overview of CTI OS

The CTI OS is the next generation customer contact integration platform from Cisco. CTI OS combines a powerful, feature-rich server and an object-oriented software development toolkit to enable rapid development and deployment of complex CTI applications. Together, the Cisco CTI Server Interface, CTI OS Server and CTI OS Client Interface Library (CIL) create a high performance, scalable, fault-tolerant three-tiered CTI architecture, as illustrated in Figure 1-1.

Figure 1-1 CTI OS Three-Tiered Architecture Topology



The CTI OS application architecture employs three tiers:

- The CIL is the first tier, providing an application-level interface to developers.
- The CTI OS Server is the second tier, providing the bulk of the event and request processing and enabling the object services of the CTI OS system.
- The Cisco CTI Server is the third tier, providing the event source and the back-end handling of telephony requests.

Advantages of CTI OS as Interface to Unified ICME

CTI OS brings several major advances to developing custom CTI integration solutions. The CIL provides an object-oriented and event-driven Application Programming Interface (API), while the CTI OS server does the‘heavy-lifting’ of the CTI integration: updating call context information, determining which buttons to enable on softphones, providing easy access to supervisor features, and automatically recovering from failover scenarios.

For a list of supported codecs for the MTU softphone, refer to the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*. This document is available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html.

The key advantages of CTI OS include

- **Rapid integration.** Developing CTI applications with CTI OS is significantly easier and faster than any previously available Cisco CTI integration platform. The same object-oriented interface is used across programming languages, enabling rapid integrations in C++, Visual Basic, .NET, Java, or any Microsoft COM-compliant container environment.

Note The inclusion of the .NET toolkit allows for custom applications to be written in C#, VB.NET, or any other CLR-compliant language. By starting with the code for the .NET sample, the CTI Toolkit Combo Desktop developers can quickly customize the code without having to start from scratch.

CTI OS enables developers to create a screen-pop application in as little as five minutes. The only custom-development effort required is within the homegrown application to which CTI is being added.

- **Complex solutions made simple**. CTI OS enables complex server-to-server integrations and multiple agent monitoring-type applications. The CIL provides a single object-oriented interface that can be used in two modes: agent mode and monitor mode. See the *CTI OS Developer's Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for an explanation of these two modes.
- **Fault tolerant.** CTI OS is built upon the Unified ICM Node Manager fault-tolerance platform, which automatically detects process failure and restarts the process, enabling work to continue. Upon recovery from a failure, CTI OS initiates a complete, system-wide snapshot of all agents, calls, and supervisors and propagates updates to all client-side objects.

Key Benefits of CTI OS for CTI Application Developers

The CTI OS CIL provides programmers with the tools required to rapidly develop high-quality CTI-enabled applications, taking advantage of the rich features of the CTI OS server. Every feature of CTI OS was designed with ease of integration in mind, to remove the traditional barriers to entry for CTI integrations.

- **Object-oriented interactions.** CTI OS provides an object-oriented CTI interface by defining objects for all call center interactions. Programmers interact directly with Session, Agent, SkillGroup, and Call objects to perform all functions. CIL objects are thin proxies for the server-side objects, where all the ‘heavy-lifting’ is done. The Session object manages all objects within the CIL. A UniqueObjectID identifies each object. Programmers can access an object by its UniqueObjectID or by iterating through the object collections.
- **Connection and session management.** The CTI OS CIL provides out-of-the-box connection and session management with the CTI OS Server, hiding all of the details of the TCP/IP sockets connection. The CIL also provides out-of-the-box failover recovery: upon recovery from a failure, the CIL automatically reconnects to another CTI OS Server (or reconnects to the same CTI OS Server after restart), reestablishes the session, and recovers all objects for that session.
- **All parameters are key-value pairs.** The CTI OS CIL provides helper classes to treat all event and request parameters as simply a set of key-value pairs. All properties on the CTI OS objects are accessible by name via a simple Value = GetValue(“key”) mechanism. Client programmers can add values of any type to the CTI OS Arguments structure using the enumerated CTI OS keywords or their own string keywords (for example, AddItem(“DialedNumber”, “1234”)). This provides for future enhancement of the interface without requiring any changes to the method signatures.
- **Simple event subscription model.** The CTI OS CIL implements a publisher-subscriber design pattern to enable easy subscription to event interfaces. Programmers can subscribe to the event interface that suits their needs, or use the AllInOne interface to subscribe to all events. Subclassable event adapter classes enable programmers to subscribe to event interfaces and only add minimal custom code for the events they use, and no code at all for events they do not use.

System Manager Responsibilities

The remainder of this document provides step by step procedures for the tasks a system manager must perform to set up and configure CTI OS. These tasks include:

- Installing Release 8.0(1) CTI OS Server (see Chapter 2, “CTI OS Server Installation”).

- Installing Release 8.0(1) CTI Toolkit Agent Desktop, IPCC Supervisor Desktop, Tools, Documentation, Win32 SDK, Java SDK, and .NET SDK. (see Chapter 3, "CTI Toolkit Desktop Client Installation").

Note You can skip the procedures discussed in Chapters 2 and 3 if you already have CTI OS Release 7.0(0) or one of its associated service releases (SRs) installed on your system.

- Installing Release 7.1(1) and later specific components (see Chapter 4, "Installing and Configuring CTI OS Silent Monitor").
- Enabling CTI OS security (see Chapter 7, "CTI OS Security").
- Using the Windows Registry Editor (regedit.exe) to configure the required CTI OS registry keys (see Chapter 8, "CTI OS Configuration").
- Starting CTI OS and its associated processes from Unified CCE Service Control (see Chapter 9, "Startup, Shutdown, and Failover").

Note You *must* have administrator privileges to perform the procedures discussed in this manual.

System Requirements

For a list of hardware and software requirements and for information on compatibility and interoperability with related Cisco and third-party hardware and software, see the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*. This document is available at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html.

Desktop User Accounts

On Windows 2000 and Windows XP systems, a user must be defined as a Power User to have user privileges comparable to the default user privileges of an NT user. Windows 2000 and Windows XP systems users must either be members of the Power User group, or have their user privileges modified to enable them to run legacy applications and have read/write access to the Cisco registry keys that the desktop applications use. To set user privileges to enable users to run CTI OS Agent Desktop and CTI OS Supervisor Desktop for IPCC, an administrator must perform the following steps.

Step 1 On the Microsoft Windows Start Menu, select **Start > Run**.

Step 2 Type in **regedt32** and click **OK**. The Microsoft Windows Registry Editor window appears.

Step 3 Go to the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTI Desktop\Ctios
```

Step 4 Select **Security > Permissions**. A Permissions dialog box appears.

Step 5 If you are adding a new user, perform the following steps.

- Click **Add**. A Select Users dialog box appears.
- Select the user to be added from the list in the top half of the Select Users dialog box.

- Click **Add**, then click **OK**. You return to the Permissions dialog box; the user you just added is now on the list.

Step 6 Click on the user whose privileges you want to set.

Step 7 Set the Full Control permissions for this user to **Allow**.

Step 8 Click **Apply**.

Step 9 Click **OK**.

Step 10 Exit Registry Editor.

Silent Monitoring

Silent monitoring is a feature that allows a supervisor to eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Silent monitoring functionality can be provided by Cisco Unified Communications Manager (Unified CM) or CTI OS.

Each CTI OS Server can be configured for either Unified CM-based or CTI OS-based silent monitoring.

Differences Between Unified CM and CTI OS Silent Monitor

Besides the differences in implementation, CTI OS and Unified CM also differ in when they can be invoked and when they end.

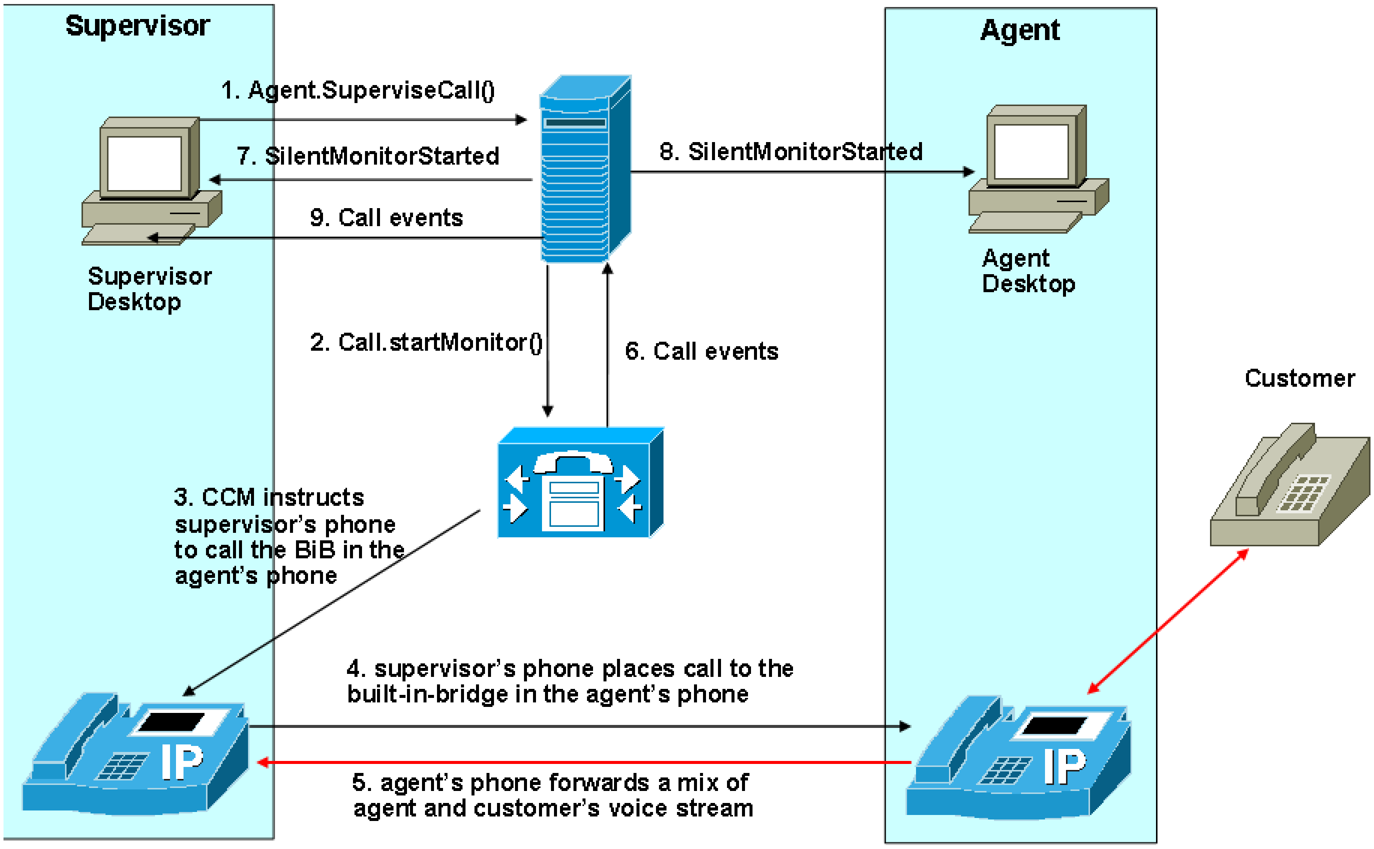
Table 1-1 Unified CM-Based and CTI OS-Based Silent Monitor Differences

Unified CM-Based Silent Monitor	CTI OS-Based Silent Monitor
The supervisor can only silent monitor an agent who is actively talking in a call.	The supervisor can silent monitor an agent in any state as long as the agent is logged in.
Supervisor cannot silent monitor an agent on hold.	Supervisor can silent monitor an agent on hold.
When agent consults, supervisor must stop silent monitoring held call and start silent monitoring conference.	When agent consults, supervisor automatically hears consult call.
Supervisor can only silent monitor in Not Ready state.	Supervisor can silent monitor in any state.
Supervisor must stop silent monitoring before barging in.	Supervisor can barge in while silent monitoring.
When the call that is being silent monitored ends, the silent monitor call ends. The supervisor must restart silent monitor after the agent answers another call.	When call ends, supervisor automatically silently monitors the next call as long as the supervisor has not stopped silent monitoring.

Unified CM-Based Silent Monitoring

Unified CM-based Silent Monitor allows a supervisor to listen in on agent calls in IPCC call centers that use Unified CM version 6.0 and later. Supervisors can send Silent Monitor requests to monitor agents without the agent being aware of any monitoring activity. When the Unified CM-based approach is adopted for silent monitoring, the agent phone is used to mix the media streams of the agent call. The mix is then sent to the supervisor phone.

Figure 1-2 Unified CM-Based Silent Monitor


Supervisor
Agent
1. Agent.SuperviseCall()
7. SilentMonitorStarted
8. SilentMonitorStarted
9. Call events
Supervisor Desktop
Agent Desktop
2. Call.startMonitor()
6. Call events
Customer
3. CCM instructs supervisor's phone to call the BiB in the agent's phone
4. supervisor's phone places call to the built-in-bridge in the agent's phone
5. agent's phone forwards a mix of agent and customer's voice stream
IP
IP

Unified CM Silent Monitor Advantages

Unified CM-based Silent Monitor provides the following advantages:

- No NIC card restrictions.
- Any 7.x version of any desktop (C++, Java, .Net, Siebel) can be silent monitored provided the agent is not a mobile agent.
- Silent monitor is implemented via a call therefore the silent monitor call is carried on the voice LAN. With CTI OS Silent Monitor, the silent monitor stream is carried on the data LAN.
- Silent monitor calls are reported as agent-to-agent calls for supervisors. With CTI OS silent monitor, the time the supervisor spends silent monitoring is not tracked.

Unified CM Silent Monitor Limitations and Restrictions

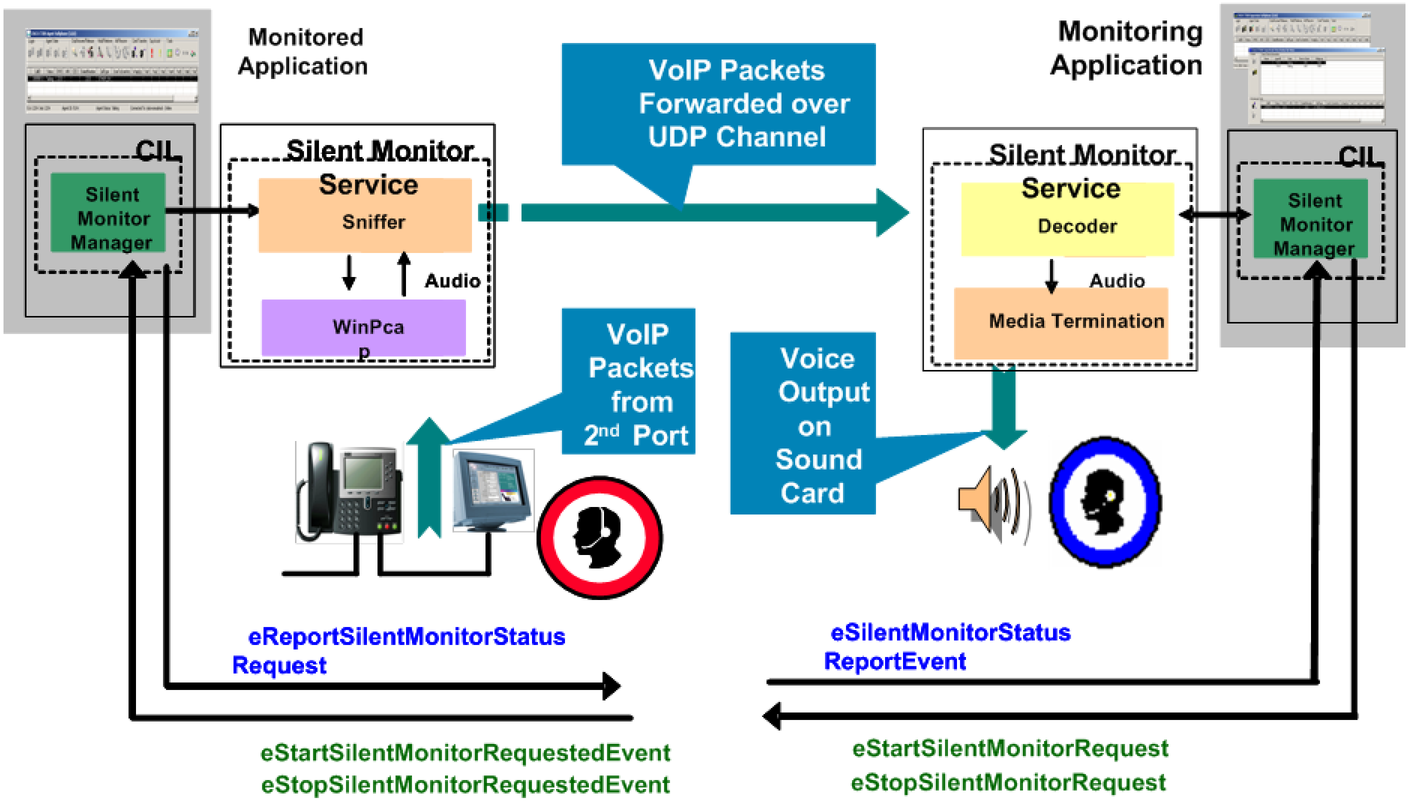
The following items prevent the use of Unified CM-based silent monitor:

- Agents using phones other than 79x1 phones (7941, 7961, or 7971)
- Agents using Cisco IP Communicator
- Supervisors using 7.1(x) or earlier desktops
- IPCC 7.1(x)
- Unified CM 5.x and earlier
- Silent monitoring SRTP streams is not supported
- Mobile agents cannot be silent monitored

CTI OS-Based Silent Monitoring

CTI OS-based Silent Monitor allows a supervisor to listen in on agent calls in IPCC call centers that use CTI OS. Supervisors can send Silent Monitor requests to agent desktops without the agent being aware of any monitoring activity. Voice packets sent to and received by the monitored agent's IP desk phone are captured from the network and sent to the supervisor silent monitor service connected to the supervisor desktop. At the supervisor silent monitor service, these voice packets are decoded and played on the supervisor system sound card.

Figure 1-3 CTI OS-Based Silent Monitor


Monitored Application
CIL
Silent Monitor Manager
Silent Monitor Service
Sniffer
Audio
WinPcap
VoIP Packets Forwarded over UDP Channel
Monitoring Application
Silent Monitor Service
Decoder
Audio
Media Termination
CIL
Silent Monitor Manager
VoIP Packets from 2nd Port
Voice Output on Sound Card
eReportSilentMonitorStatus Request
eSilentMonitorStatus ReportEvent
eStartSilentMonitorRequestedEvent
eStopSilentMonitorRequestedEvent
eStartSilentMonitorRequest
eStopSilentMonitorRequest

Note Silent Monitor does not capture and translate DTMF digits that are selected on the CTI OS Agent Desktop or on agent desk phones.

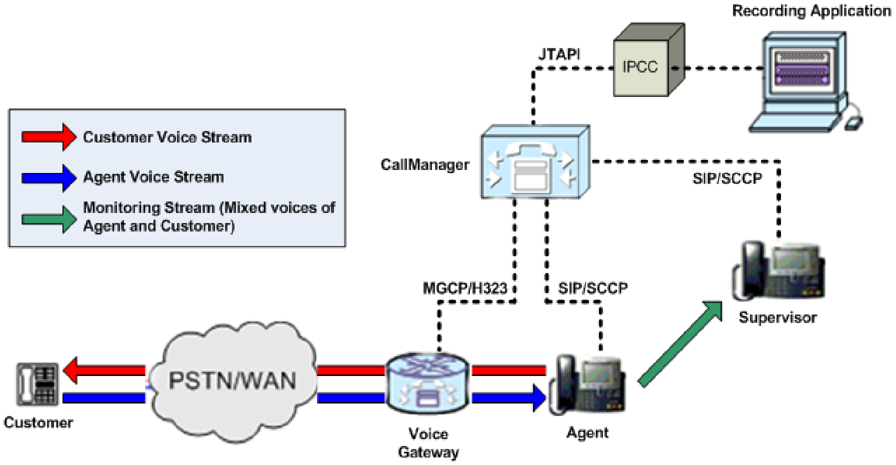
Note For the agent using the 7941, 7961, 7970, and 7971 phones, these devices must be configured on the Unified CM Administration web page with the “Span to PC Port”, “PC Voice VLAN Access” and the “PC Port” enabled. By default, the “Span to PC Port” is disabled and the “PC Voice VLAN Access” and the “PC Port” are enabled.

Network Topology for Silent Monitoring

Unified CM-Based Silent Monitoring

Figure 1-4 shows the network components and protocols involved in a Unified CM-based call monitoring session.

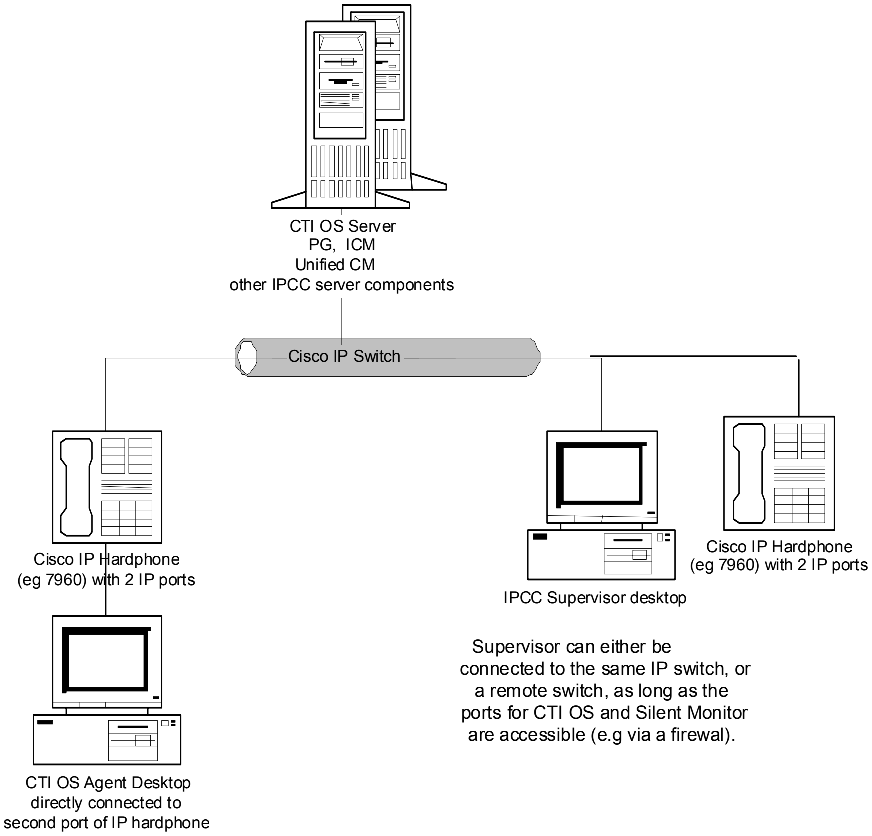
Figure 1-4 Unified CM-Based Silent Monitoring Network Topology



CTI OS-Based Silent Monitoring

The necessary network topology for non-mobile IPCC agents is shown in Figure 1-5.

Figure 1-5 CTI OS-Based Silent Monitor Network Topology


CTI OS Server
PG, ICM
Unified CM
other IPCC server components
Cisco IP Switch
Cisco IP Hardphone
(eg 7960) with 2 IP ports
CTI OS Agent Desktop
directly connected to
second port of IP hardphone
IPCC Supervisor desktop
Cisco IP Hardphone
(eg 7960) with 2 IP ports
Supervisor can either be
connected to the same IP switch, or
a remote switch, as long as the
ports for CTI OS and Silent Monitor
are accessible (e.g via a firewal).

Agents in this topology may have either an IP hardphone or IP Communicator. (The supervisor in this topology must have an IP hardphone. IP Communicator is not an option.) If the agent has an IP desk phone, it must have an agent desktop PC connected to the second IP port. If the agent has IP Communicator, it must be installed on the same machine as the agent desktop.

A CTI OS-based desktop application that implements the CTI OS Silent Monitor feature must be installed on the agent desktop and supervisor desktop PCs. In addition, the components needed for an agent to be silently monitored are now automatically installed when the Agent Desktop is installed and those needed for a supervisor to do the silent monitoring are automatically installed when the IPCC Supervisor Desktop is installed (see Chapter 3, “CTI Toolkit Desktop Client Installation”).

Silent Monitoring and System IPCC

Instead of re-running the CTI OS Server setup, System IPCC administrators can set the Silent Monitor mode in the System IPCC Web Administration tool by performing the following:

Step 1 Select **System Management > Machine Management > Machines**.

Step 2 From the Machines page, run the Machine Wizard for each machine with the role Agent/IVR Controller.

Step 3 On the IPCC Network page of the wizard, select one of the following:

- CTI OS-based
- Unified CM-based
- Disabled

Step 4 Finish the wizard for the change to take effect.

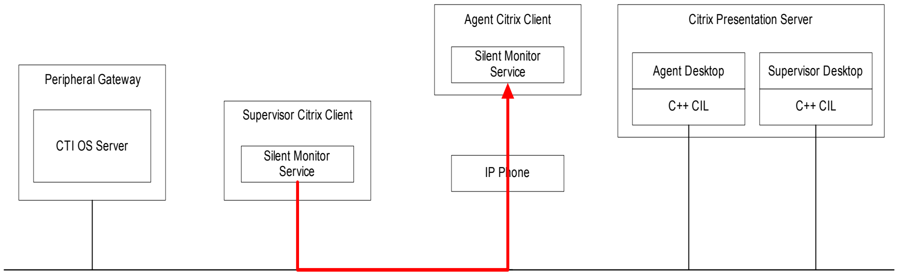
-or-

Go directly to the IPCC Network page for each Agent/IVR Controller by selecting **System Management > Machine Management > IPCC Network**, and save your silent monitor mode selection.

Silent Monitoring and Citrix

IPCC agents using Citrix clients can also be monitored. This is done by installing silent monitor services on the computers running the agent and supervisor Citrix clients. The agent Citrix client must be deployed behind the agent IP phone. The supervisor Citrix client must have a sound card. The necessary network topology is as follows.

Figure 1-6 Silent Monitoring and Citrix Topology



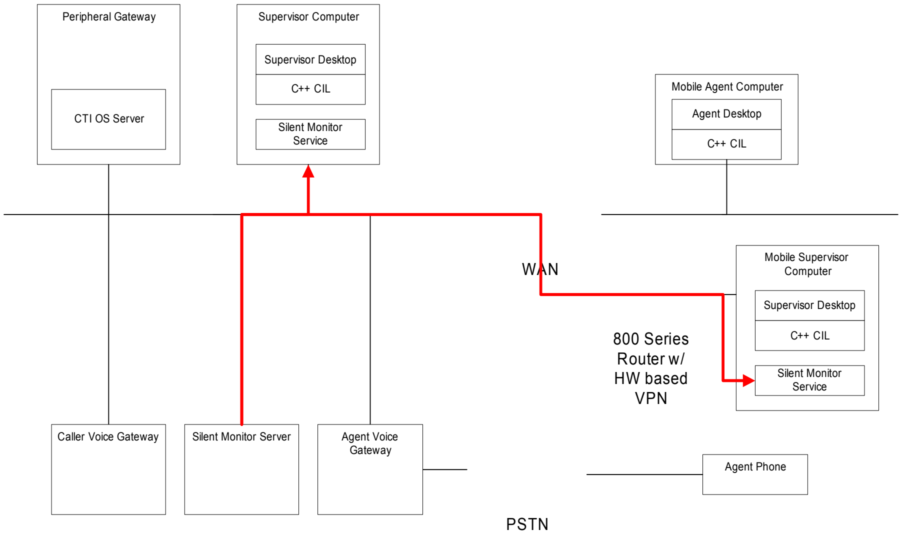
For more details on this deployment, see the section Silent Monitor Service Deployments, in Chapter 4, "Installing and Configuring CTI OS Silent Monitor."

Silent Monitoring and Mobile Agent

Mobile agents can also be silently monitored. To do this, a standalone silent monitor server must be manually deployed. This silent monitor server gains access to mobile agent voice traffic through a SPAN port that must be configured to send all traffic to and from the agent gateway to the silent monitor server. The silent monitor server then filters and forwards voice traffic for the selected agent to the supervisor silent monitor server.

The necessary network topology is as follows.

Figure 1-7 Silent Monitoring and Mobile Agent Topology



For more details on this deployment, see the section Silent Monitor Service Deployments in Chapter 4, "Installing and Configuring CTI OS Silent Monitor."

Calculating Additional Needed Bandwidth

Silent monitoring of an agent consumes almost the same network bandwidth as an additional voice call. If a single agent requires bandwidth for one voice call, then the same agent being silent monitored would require bandwidth for two concurrent voice calls.

For example, assume the following:

- You have 100 concurrent agents on your network.
- Up to 20% of the agents are monitored at any given time.

In this case, plan for network capacity for 100 + (20% of 100) concurrent calls, or 120 concurrent calls.

To calculate the total network bandwidth required for your call load, you would then multiply this number of calls by the per-call bandwidth figure for your particular codec and network protocol.

For example, the table on the Cisco Voice Over IP – Per Call Bandwidth Consumption website (http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml) lists the per-call bandwidth on the G.711 codec (for a call with the default voice payload size) over Ethernet as 87.2 Kbps. You would multiply this 87.2 Kbps by 120 calls to obtain the total required network bandwidth.

For more information on per-call bandwidths for various codecs and network protocols, see the Cisco Voice Over IP–Per Call Bandwidth Consumption website at

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

For more information on calculating bandwidth, see the Cisco Voice Codec Bandwidth Calculator website at http://tools.cisco.com/Support/VBC/jsp/Codec_Calc1.jsp.

CHAPTER 2

CTI OS Server Installation

This chapter lists some guidelines to consider when you install CTI OS Servera and provides procedures for these tasks. It contains the following sections:

- CTI OS Server Installation Guidelines
- Upgrading from a Previous Version
- Installing CTI OS Server
- Uninstalling CTI OS Server
- Determining Version Number of Installed Files

Caution Running CTI OS setup over the network is not supported. You must either run the installer from the install DVD or copy the installer directory to the target machine and then run the installer from the local machine. Various errors can occur during installation over the network. Keep in mind that 8.0(1) is a full installation and there is no way to roll the installation back to the previous release if installation or upgrade fails part way through.

CTI OS Server Installation Guidelines

Following are some guidelines to consider when you install CTI OS Server:

- CTI OS is typically installed in a duplex configuration. Two CTI OS servers installed on separate systems work in parallel to provide redundancy. Installing only one CTI OS server prevents failover recovery by client systems. See Chapter 9, "Startup, Shutdown, and Failover" for more information on CTI OS failover.
- CTI OS must be co-located on the same box as the PG/CG.
- Ensure that your CTI OS system meets the minimum hardware and software requirements as listed in the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*. This document is available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm.

Upgrading from a Previous Version

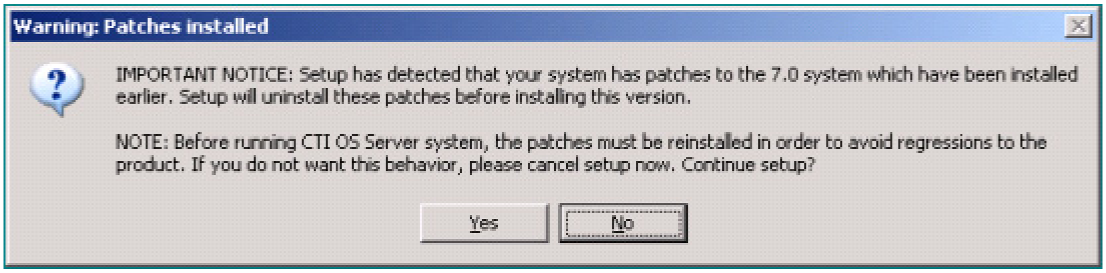
If you are upgrading from a previous 7.x(y) release of CTI OS Server (including CTI OS 7.0(x), 7.1(x), 7.2(x), or 7.5(x)); you do *not* need to uninstall CTI OS Server before you install CTI OS Server Release 8.0(1).

Note The listen ports for CTI OS Server and Silent Monitor are registered as firewall exceptions upon installation of patch 8.5(2). These firewall exceptions are removed when the patch is uninstalled.

Step 1 When you start Setup.exe, the Instance dialog is displayed. Click **Upgrade All**.

Step 2 If you have a version of CTI OS Server already installed and you are attempting to install the latest version, the following pop-up window appears:

Figure 2-1 Patch installation warning



Warning: Patches installed

IMPORTANT NOTICE: Setup has detected that your system has patches to the 7.0 system which have been installed earlier. Setup will uninstall these patches before installing this version.

NOTE: Before running CTI OS Server system, the patches must be reinstalled in order to avoid regressions to the product. If you do not want this behavior, please cancel setup now. Continue setup?

Step 3 Click **Yes**.

Several status dialogs are displayed informing you that registry entries are being copied, files are being copied, and so forth. All files that belong to the old version are deleted and the files for the 8.0 version are installed.

Installing CTI OS Server

If you are installing a new CTI OS Server, perform the following steps.

Note The CTI OS Server installation procedure described on the following pages includes some screens for mobile agents and silent monitor server.

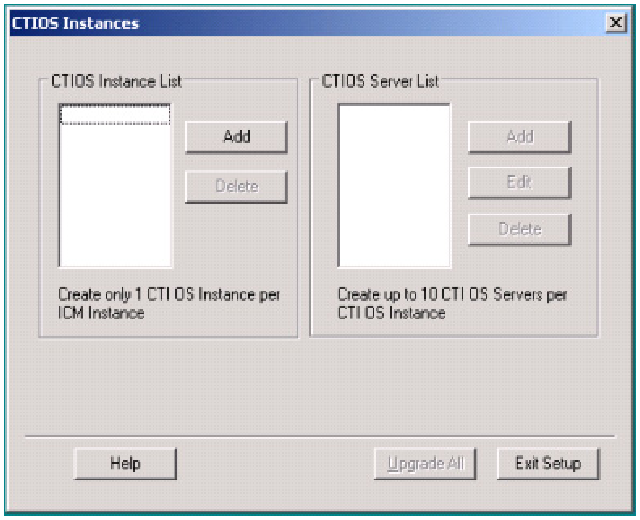
Step 1 From the Server directory on the CD, run **Setup.exe**.

Note When you run programs from a Windows Server 2008 R2 system with User Account Control enabled, Windows needs your permission to continue. Click **Allow** in the User Account Control window to run the programs.

Step 2 Click **Yes** on the Software License Agreement screen. The CTIOS Instances dialog appears.

The CTIOS Instances dialog allows you to create CTI OS Instances and add CTI OS Servers to a configured instance of CTI OS.

Figure 2-2 CTI OS Instances



The CTIOS Instance List contains an **Add** and a **Delete** button.

Add is enabled under the following conditions:

- There are no existing CTI OS instances.
- There is one CTI OS instance with no servers configured.
- A multi-instance configuration is detected (1-10 CTI OS instances with one CTI OS Server configured per instance using a Hosted IPCC peripheral type).

Delete is enabled whenever an instance is selected.

The CTIOS Server List group contains an **Add**, an **Edit**, and a **Delete** button.

Add is enabled under the following conditions:

- There is one instance of CTI OS with no CTI OS Servers.
- There is one instance of CTI OS with less than 6 CTI OS Servers configured. Each CTI OS Server is configured for any peripheral type except Hosted IPCC.

You can create up to 10 CTI OS Servers per CTI OS instance. The maximum number of CTI OS Servers per instance is configured using the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\ MaxServersPerInstance.

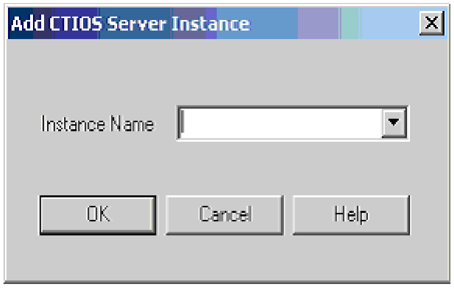
When the first CTI OS Server instance is installed, this key (of type DWORD) is added and set to 10.

Edit and **Delete** are enabled whenever a server is selected.

Step 3 You must install a Windows Server 2008 R2 compatible maintenance release (Release 8.5(2) or later) for this software to function on Windows Server 2008 R2.

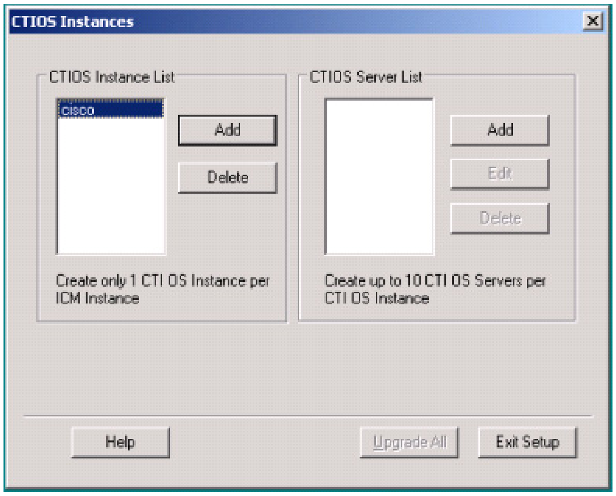
Step 4 Under the CTI OS Instance List, click **Add**. The following dialog box appears.

Figure 2-3 CTI OS Instance List



Step 5 Enter an instance name. For example, if you enter an instance called “cisco,” the following window appears:

Figure 2-4 CTI OS Instances

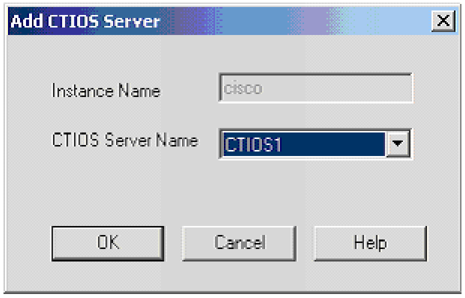


Create only 1 CTI OS Instance per ICM Instance

Create up to 10 CTI OS Servers per CTI OS Instance

Step 6 Click **Add** inside the CTI OS Server List. The Add CTIOS Server dialog appears.

Figure 2-5 CTI OS Server selection



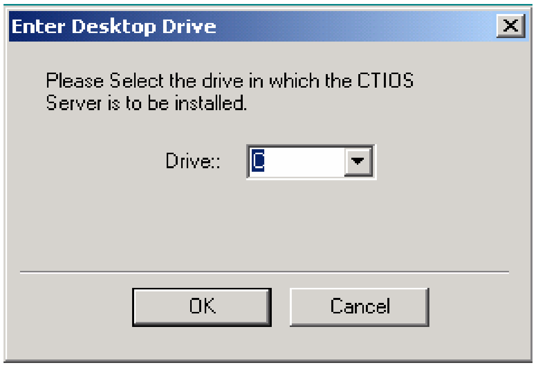
Instance Name: cisco

CTIOS Server Name: CTIOS1

The CTIOS Server Name is filled in with the string “CTIOS” followed by the next available index for a CTI OS Server. If a CTI OS Server has been deleted, the CTIOS Server Name string is filled in with the index that was deleted.

Step 7 If you are installing CTI OS Server for the first time, an Enter Desktop Drive screen appears. Accept the default installation drive or select another drive from the drop-down list.

Figure 2-6 Desktop Drive selection



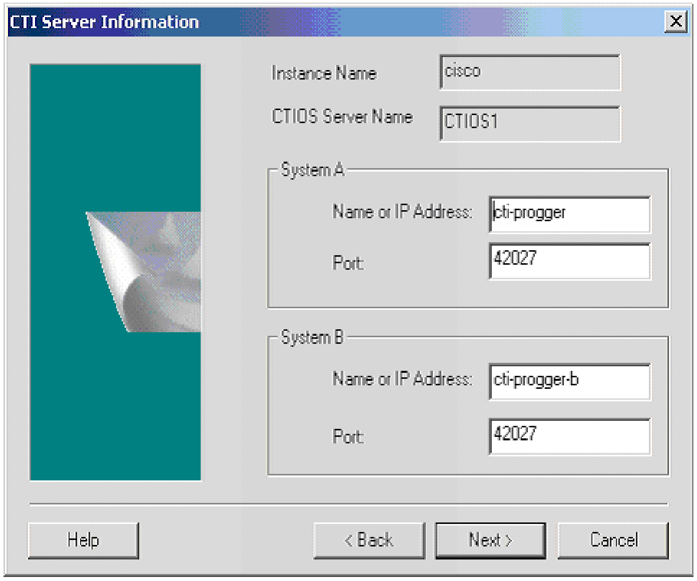
Enter Desktop Drive

Please Select the drive in which the CTIOS Server is to be installed.

Drive:: C

Step 8 Click **OK**. The CTI Server Information screen appears.

Figure 2-7 CTI OS Server Information



CTI Server Information

Instance Name: cisco

CTIOS Server Name: CTIOS1

System A

Name or IP Address: cti-progger

Port: 42027

System B

Name or IP Address: cti-progger-b

Port: 42027

Step 9 Enter the **Name** or **IP Address** and the **Port Number** for your CTI systems.

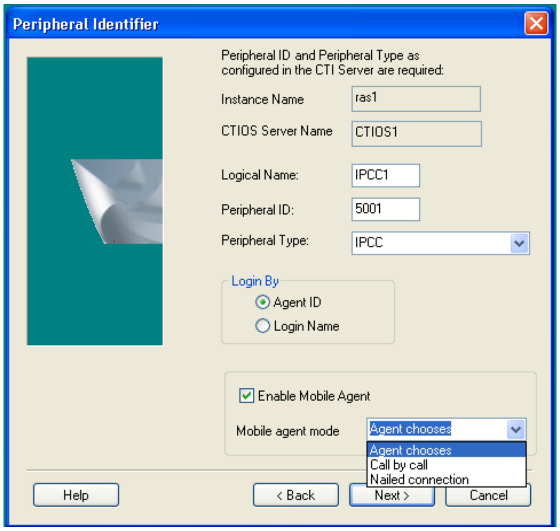
The Peripheral Type field is prepopulated with the peripheral type if the peripheral has been configured for a previous CTI OS Server.

Note When you configure multiple CTI OS servers to use a single CTI server, every CTI OS server configured in addition to the first defaults to the configuration of the first CTI OS server.

Step 10 Click **Next**. The Peripheral Identifier screen appears.

If the peripheral has been configured for a previous CTI OS server, the “Name or IP Address” field is pre-populated with the CTI Server name of that previously configured CTI OS Server.

Figure 2-8 Peripheral Identifier



Peripheral Identifier

Peripheral ID and Peripheral Type as configured in the CTI Server are required:

Instance Name: ras1

CTIOS Server Name: CTIOS1

Logical Name: IPCC1

Peripheral ID: 5001

Peripheral Type: IPCC

Login By

● Agent ID

○ Login Name

☑ Enable Mobile Agent

Mobile agent mode: Agent chooses

Because multi-instance does not support multiple servers, any server configured as part of an instance that has other servers does not list “IPCC Hosted” in the peripheral type field.

ARS and ERS peripheral types are not listed either, as they are not supported for multiple servers.

Because multiple servers cannot be supported with multiple instances, the peripheral type drop-down only contains “IPCC Hosted” when a server is added to a system with multiple instances already configured.

Step 11 If the peripheral has not been configured for a previous CTI OS server, specify the following information:

- A **Logical Name** for your peripheral. This can be any valid logical name that uniquely identifies your peripheral.

Note Only Peripheral Types of “IPCC”, “System IPCC”, and “IPCC Hosted Edition” have the “Login By” and “Enable Mobile Agent” group boxes enabled. In the “Login By” box, 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. CTIOS Server itself can service Login requests both ways (by AgentID and by LoginName) for IPCC.

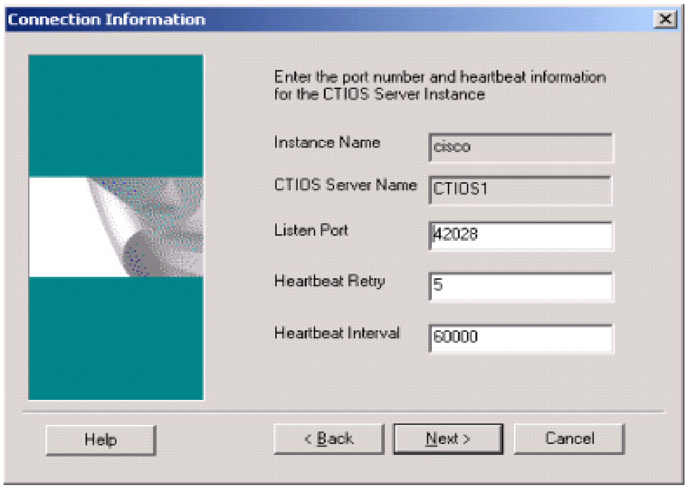
All other peripheral types login by Agent ID only, and the choice is disabled. If this is to be a multi-instance environment, select **IPCC Hosted Edition**.

- The **Peripheral ID** associated with the switch your telephone is connected to.
- The **Peripheral Type** of the switch your telephone is connected to.
- Whether to enable Mobile Agent.
- Mobile Agent mode. Specify one of the following.
  - **Agent chooses**—Agent chooses the mode.
  - **Call by call**—The agent’s remote phone is dialed for each individual call.
  - **Nailed connection**—The agent is called once upon login and remains connected.

Note You can specify information for only one peripheral during CTI OS Server setup. To configure additional peripherals, follow the procedure in the section Configuring Additional Peripherals in Chapter 8, "CTI OS Configuration."

Step 12 Click **Next**. The Connection Information screen appears.

Figure 2-9 Connection Information



Connection Information

Enter the port number and heartbeat information for the CTIOS Server Instance

Instance Name: cisco

CTIOS Server Name: CTIOS1

Listen Port: 42028

Heartbeat Retry: 5

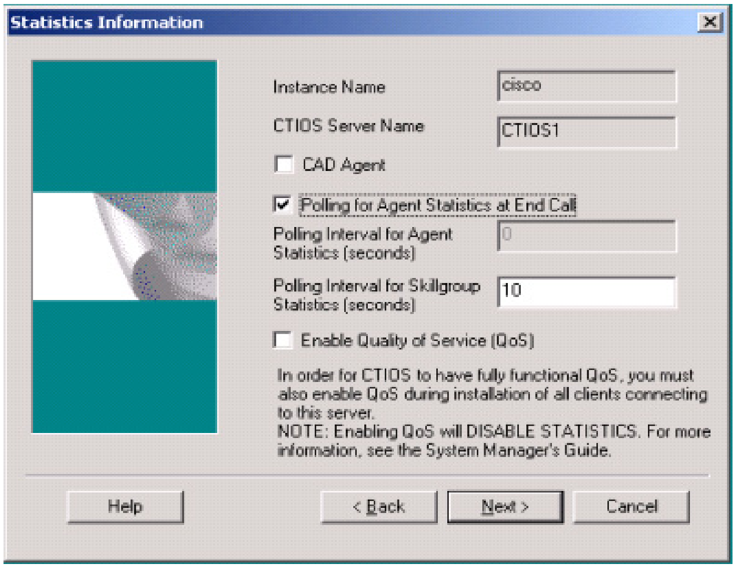
Heartbeat Interval: 60000

Enter the port number and the heartbeat information for your CTI OS server instance.

Note For all peripheral types except IPCC Hosted, accept the default Listen Port value of 42028. For the IPCC Hosted peripheral type, only the first instance can have this port. For subsequent instances, increment the port number by 1 (42029, 42030, and so forth), taking care to configure the clients that connect to them with the same port in their installs.

Step 13 Click **Next**. The Statistics Information screen appears.

Figure 2-10 Statistics Information



Statistics Information

Instance Name: cisco

CTIOS Server Name: CTIOS1

□ CAD Agent

☑ Polling for Agent Statistics at End Call

Polling Interval for Agent Statistics (seconds): 0

Polling Interval for Skillgroup Statistics (seconds): 10

□ Enable Quality of Service (QoS)

In order for CTIOS to have fully functional QoS, you must also enable QoS during installation of all clients connecting to this server.
NOTE: Enabling QoS will DISABLE STATISTICS. For more information, see the System Manager's Guide.

Note

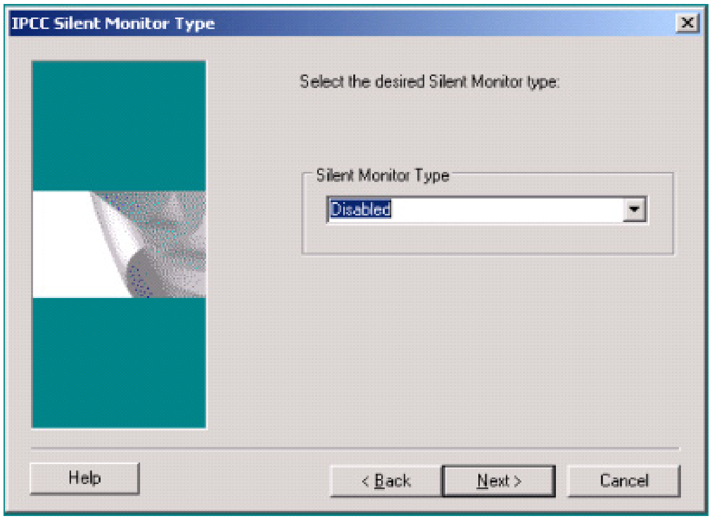
- Enabling CAD Agent disables the agent statistics polling interval from the CTI OS Server. CAD agents receive only skillgroup statistics from CTI OS Server.
- After performing an **Upgrade All**, you must rerun setup in order to access this screen and reconfigure the for appropriate statistical information.

Step 14 Enter the default polling interval for Skillgroup statistics (in seconds).

Note Since QoS enablement and statistics enablement are mutually exclusive, enabling QoS zeros and disables all of the information relating to statistics.

Step 15 Click **Next**. The IPCC Silent Monitor Type screen appears.

Figure 2-11 IPCC Silent Monitor Type



IPCC Silent Monitor Type

Select the desired Silent Monitor type:

Silent Monitor Type: Disabled

Step 16 Select the Silent Monitor type.

If **Unified CM Based** or **Disabled** is chosen, clicking **Next** takes you to the "Peer CTI OS Server" screen. Proceed to **Step 17**.

Note If **Unified CM-Based** is chosen, refer to Chapter 6, "Configuring Unified CM-Based Silent Monitor."

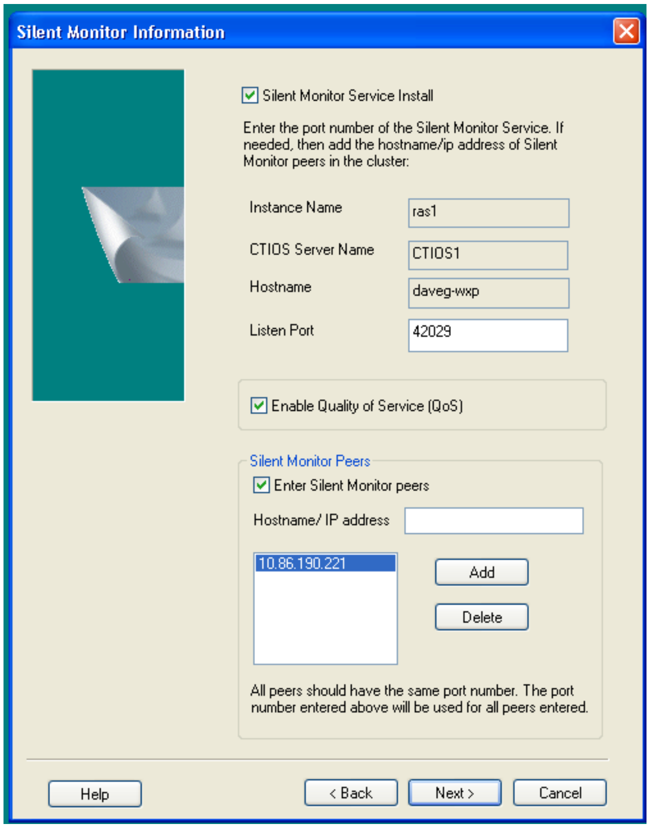
If **Disabled** is chosen, CTI OS-based silent monitor is configured, but disabled. This means the registry settings below have the following values:

.

Key	Setting
HKLM\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_<*instance*>\CTIOS1\EnterpriseDesktopSettings\All Desktops\UCCESilentMonitor\Name\Settings\CCMBasedSilentMonitor	0
HKLM\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_<*instance*>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\UCCE\ UCCESilentMonitorEnabled	0

If **CTI OS Based** silent monitor is chosen, clicking **Next** takes you to the "Silent Monitor Information" screen.

Figure 2-12 Silent Monitor Information



Silent Monitor Information

☑ Silent Monitor Service Install

Enter the port number of the Silent Monitor Service. If needed, then add the hostname/ip address of Silent Monitor peers in the cluster:

Instance Name: ras1

CTIOS Server Name: CTIOS1

Hostname: daveg-wxp

Listen Port: 42029

☑ Enable Quality of Service (QoS)

Silent Monitor Peers

☑ Enter Silent Monitor peers

Hostname/ IP address:

10.86.190.221

All peers should have the same port number. The port number entered above will be used for all peers entered.

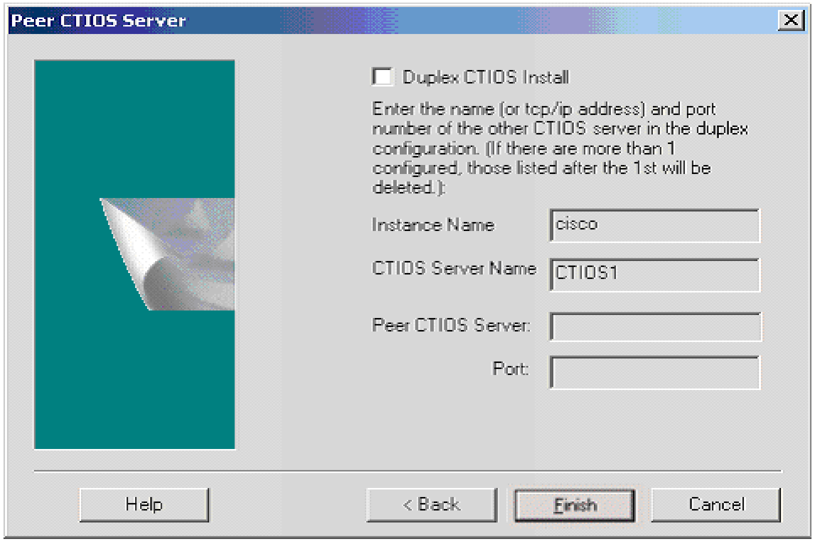
Step 17 On the Silent Monitor Information screen enter the following information:

- The port number used by the client to connect to the silent monitor service.
- Whether or not the desktop uses Quality of Service (QoS) to communicate with the silent monitor server.
- The set of silent monitor servers that the desktop connects to. The desktop randomly connects to one of the silent monitor servers specified here. If the client is configured to use secure connections, the client attempts to connect to the silent monitor server using a secure connection. If the silent monitor server is configured to use secure connections, then a secure connection is established with the silent monitor server. Otherwise, an unsecure connection is used.

  A client uses the same certificates it uses to communicate with CTI OS Server to establish a secure connection to the silent monitor server.

Step 18 Click **Next**. The Peer CTI OS Server screen appears.

Figure 2-13 CTI OS Server information



☐ Duplex CTIOS Install

Enter the name (or tcp/ip address) and port number of the other CTIOS server in the duplex configuration. (If there are more than 1 configured, those listed after the 1st will be deleted.):

Instance Name: cisco

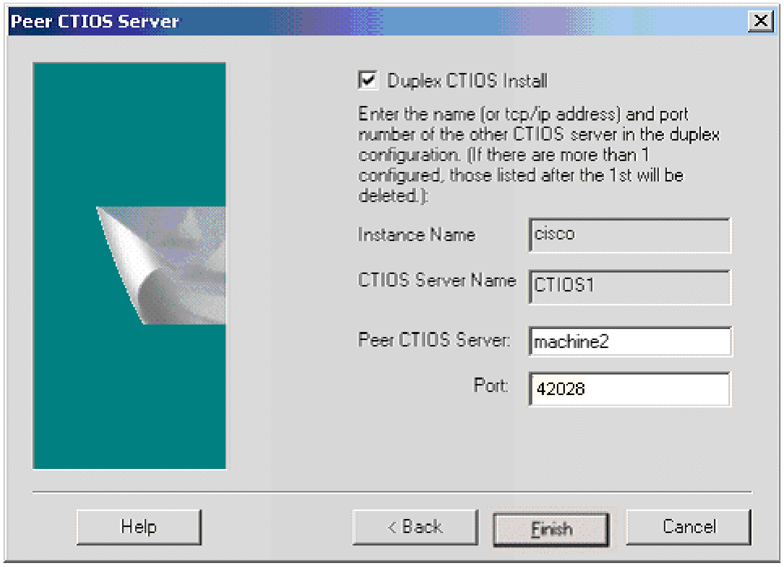
CTIOS Server Name: CTIOS1

Peer CTIOS Server:

Port:

Step 19 The Peer CTIOS Server dialog is used to configure a CTI OS Peer Server. It is also used for Chat and CTI OS Silent Monitoring. Enter the appropriate information as shown in the following figure:

Figure 2-14 Peer CTI OS Server



Peer CTIOS Server

☑ Duplex CTIOS Install

Enter the name (or tcp/ip address) and port number of the other CTIOS server in the duplex configuration. (If there are more than 1 configured, those listed after the 1st will be deleted.):

Instance Name: cisco

CTIOS Server Name: CTIOS1

Peer CTIOS Server: machine2

Port: 42028

After you click **Finish** and the files are created, the service is registered and Registry entries are made.

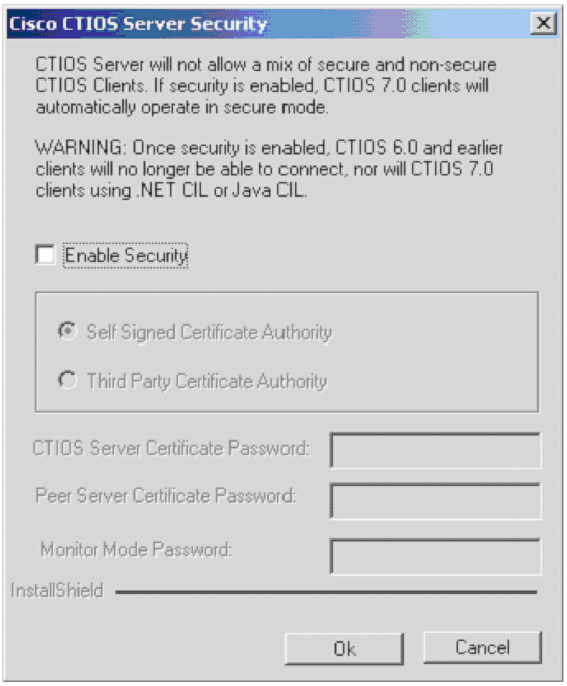
Note The chat window can be configured to beep every time a new message arrives. To make the Chat control beep every time a new message arrives, set the following registry key to a non-zero value.

```
HKEY_LOCAL_MACHINE\Cisco Systems, Inc.\CTI Desktop\CtiOs\BeepOnMsgReceived
```

If the registry key does not exist or if its value is set to zero, the Chat control does not beep.

Step 20 The Security installation is launched with the following dialog:

Figure 2-15 CTI OS Server Security



Cisco CTIOS Server Security

CTIOS Server will not allow a mix of secure and non-secure CTIOS Clients. If security is enabled, CTIOS 7.0 clients will automatically operate in secure mode.

WARNING: Once security is enabled, CTIOS 6.0 and earlier clients will no longer be able to connect, nor will CTIOS 7.0 clients using .NET CIL or Java CIL.

☐ Enable Security

● Self Signed Certificate Authority

○ Third Party Certificate Authority

CTIOS Server Certificate Password:

Peer Server Certificate Password:

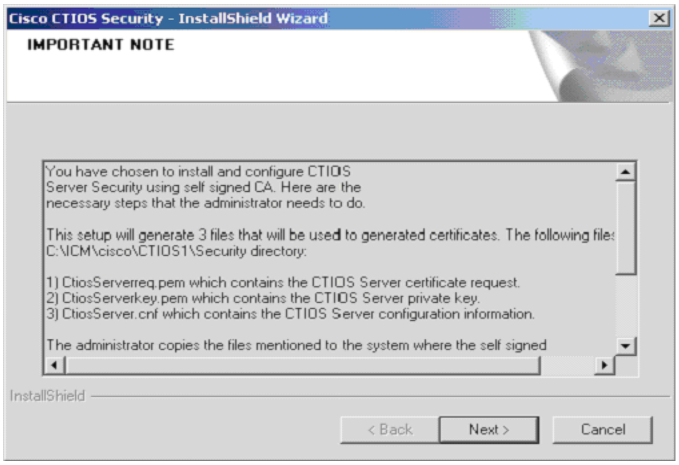
Monitor Mode Password:

If you wish to disable Security, click **OK**; otherwise, select the checkbox and enter the appropriate information, and click **OK**. For more information about CTI OS Security, see Chapter 7, "CTI OS Security".

Note In order to simplify deployments, security must be enabled for all CTI OS components (clients, CTI OS Server, and Silent Monitor Server) or disabled for all CTI OS components.

Step 21 The following window appears if you enable Security:

Figure 2-16 CTI OS Security InstallShield Wizard



You have chosen to install and configure CTIOS
Server Security using self signed CA. Here are the
necessary steps that the administrator needs to do.

This setup will generate 3 files that will be used to generated certificates. The following file
C:\ICM\cisco\CTIOS1\Security directory:

1) CtiosServerreq.pem which contains the CTIOS Server certificate request.
2) CtiosServerkey.pem which contains the CTIOS Server private key.
3) CtiosServer.cnf which contains the CTIOS Server configuration information.

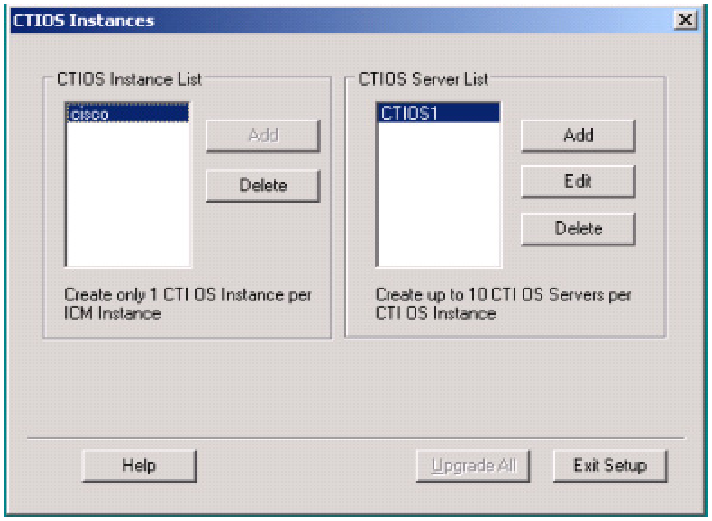
The administrator copies the files mentioned to the system where the self signed

Once the CTI OS Server Security Setup is complete, click **Finish**.

You are asked about whether you want to restart your computer now or later. If you select **Yes** your machine reboots.

Step 22 If you select **IPCC Hosted Edition** and wish to add more instances, you must then restart setup. The MR Installer launches after the 2008 R2 machine reboots. If you select **No,** you see the following:

Figure 2-17 CTI OS Instances



Create only 1 CTI OS Instance per ICM Instance

Create up to 10 CTI OS Servers per CTI OS Instance

In this core "CTIOS Instances" dialog box you can **Add** more instances and **Delete** or **Edit** the one you just installed.

Note If you have selected any peripheral type other than "IPCC Hosted Edition", the **Add** button under the Instance List is disabled so that no more instances can be added.

For “IPCC Hosted Edition”, adding an instance runs the entire progression just described above. Editing an instance displays all of the dialogs from the “CTI Server Information” dialog to the end. When adding or editing instances after the first one, only Services are registered and Registry settings are written. That is, the files are only transferred when the first instance is added because all instances share the same code base.

Note In CTI OS Releases 6.0 and later, updates to Cisco CTI OS software (Engineering Specials, Service Releases and Maintenance Releases) are installed with Patch Manager. Once installation completes you cannot move any CTI OS files from the directories in which they are installed, or Patch Manager is unable to perform CTI OS software updates correctly.

Note CTI OS Multi Instance setup does not allow two or more CTI OS Servers to connect to the same CTI Server. Also, it does not allow two or more CTI OS Servers to use the same listen port.

Note Rerun CTI OS Server setup after completing the installation.

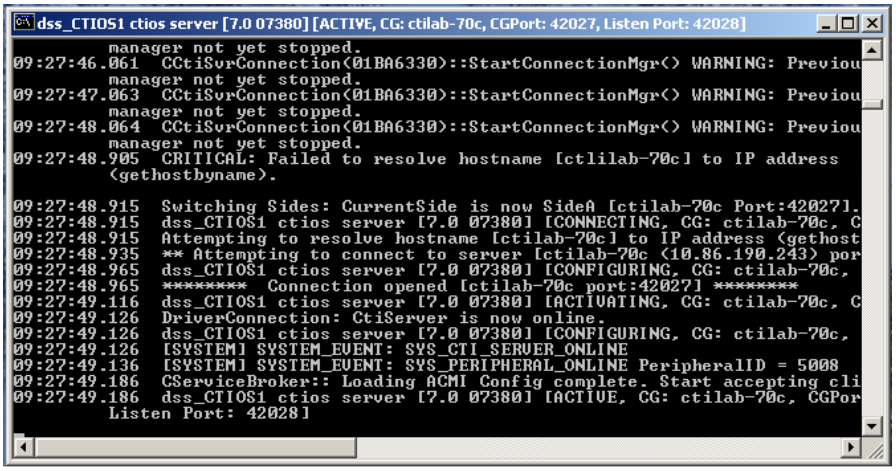
Uninstalling CTI OS Server

To uninstall CTI OS Server, rerun the Setup program for Unified ICM Release 8.0(1) and delete the Unified ICM Customer Instance that you specified during CTI OS Server Setup.

Determining Version Number of Installed Files

If CTI OS Server is currently running, the title bar of the CTIOS Server process window displays the CTI OS version number and the build number.

Figure 2-18 CTI OS Server Process



dss_CTIOS1 ctios server [7.0 07380] [ACTIVE, CG: ctilab-70c, CGPort: 42027, Listen Port: 42028]

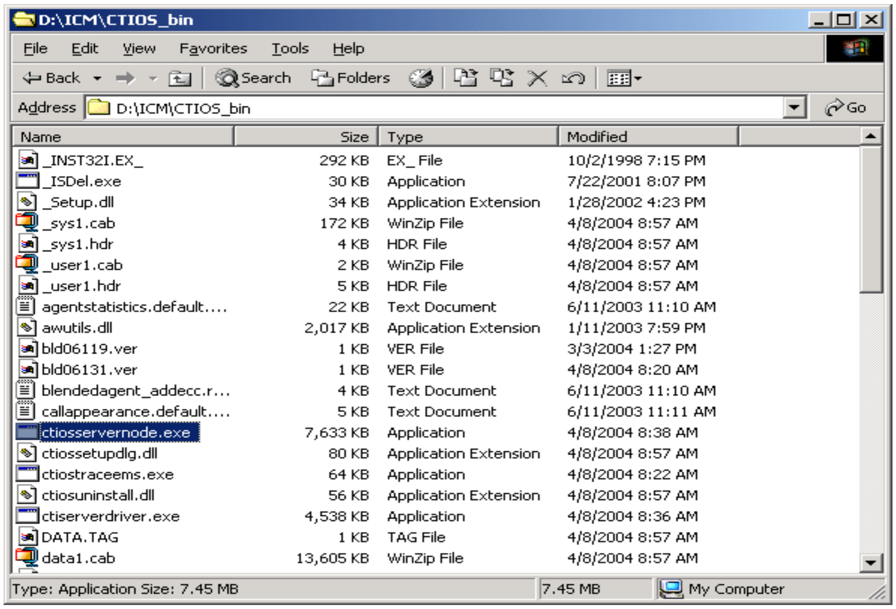
```
             manager not yet stopped.
09:27:46.061  CCtiSvrConnection(01BA6330)::StartConnectionMgr() WARNING: Previou
             manager not yet stopped.
09:27:47.063  CCtiSvrConnection(01BA6330)::StartConnectionMgr() WARNING: Previou
             manager not yet stopped.
09:27:48.064  CCtiSvrConnection(01BA6330)::StartConnectionMgr() WARNING: Previou
             manager not yet stopped.
09:27:48.905  CRITICAL: Failed to resolve hostname [ctlilab-70c] to IP address
             (gethostbyname).

09:27:48.915  Switching Sides: CurrentSide is now SideA [ctilab-70c Port:42027].
09:27:48.915  dss_CTIOS1 ctios server [7.0 07380] [CONNECTING, CG: ctilab-70c, C
09:27:48.915  Attempting to resolve hostname [ctilab-70c] to IP address (gethost
09:27:48.935  ** Attempting to connect to server [ctilab-70c (10.86.190.243) por
09:27:48.965  dss_CTIOS1 ctios server [7.0 07380] [CONFIGURING, CG: ctilab-70c,
09:27:48.965  ********  Connection opened [ctilab-70c port:42027] ********
09:27:49.116  dss_CTIOS1 ctios server [7.0 07380] [ACTIVATING, CG: ctilab-70c, C
09:27:49.126  DriverConnection: CtiServer is now online.
09:27:49.126  dss_CTIOS1 ctios server [7.0 07380] [CONFIGURING, CG: ctilab-70c,
09:27:49.126  [SYSTEM] SYSTEM_EVENT: SYS_CTI_SERVER_ONLINE
09:27:49.136  [SYSTEM] SYSTEM_EVENT: SYS_PERIPHERAL_ONLINE PeripheralID = 5008
09:27:49.186  CServiceBroker:: Loading ACMI Config complete. Start accepting cli
09:27:49.186  dss_CTIOS1 ctios server [7.0 07380] [ACTIVE, CG: ctilab-70c, CGPor
             Listen Port: 42028]
```

If CTI OS Server is *not* running, you can determine the version number of an installed CTI OS Server file by performing the following steps.

Step 1 Open a window for the ICM\CTIOS_bin subdirectory.

Step 2 Highlight the file **ctiosservernode.exe**.

Figure 2-19 CTI OS Bin folder



Name	Size	Type	Modified
INST32I.EX	292 KB	EX_ File	10/2/1998 7:15 PM
_ISDel.exe	30 KB	Application	7/22/2001 8:07 PM
_Setup.dll	34 KB	Application Extension	1/28/2002 4:23 PM
_sys1.cab	172 KB	WinZip File	4/8/2004 8:57 AM
_sys1.hdr	4 KB	HDR File	4/8/2004 8:57 AM
_user1.cab	2 KB	WinZip File	4/8/2004 8:57 AM
_user1.hdr	5 KB	HDR File	4/8/2004 8:57 AM
agentstatistics.default....	22 KB	Text Document	6/11/2003 11:10 AM
awutils.dll	2,017 KB	Application Extension	1/11/2003 7:59 PM
bld06119.ver	1 KB	VER File	3/3/2004 1:27 PM
bld06131.ver	1 KB	VER File	4/8/2004 8:20 AM
blendedagent_addecc.r...	4 KB	Text Document	6/11/2003 11:10 AM
callappearance.default....	5 KB	Text Document	6/11/2003 11:11 AM
ctiosservernode.exe	7,633 KB	Application	4/8/2004 8:38 AM
ctiossetupdlg.dll	80 KB	Application Extension	4/8/2004 8:57 AM
ctiostraceems.exe	64 KB	Application	4/8/2004 8:22 AM
ctiosuninstall.dll	56 KB	Application Extension	4/8/2004 8:57 AM
ctiserverdriver.exe	4,538 KB	Application	4/8/2004 8:36 AM
DATA.TAG	1 KB	TAG File	4/8/2004 8:57 AM
data1.cab	13,605 KB	WinZip File	4/8/2004 8:57 AM

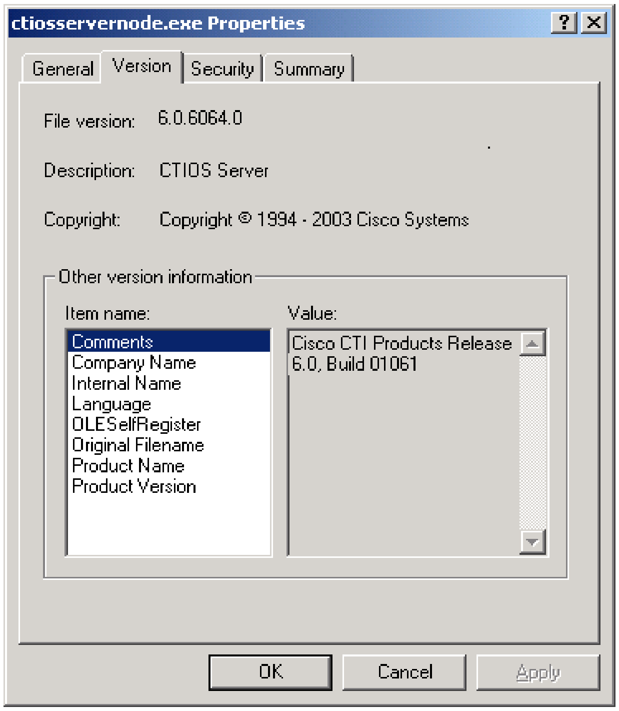
Type: Application Size: 7.45 MB 7.45 MB My Computer

Step 3 Right-click on the highlighted file.

Step 4 Select **Properties** from the drop-down menu. The Properties dialog box appears.

Step 5 Select the **Version** tab. This tab contains version information (release number and build number) for the file.

Figure 2-20   CTI OS Servernode Properties



ctiosservernode.exe Properties

File version: 6.0.6064.0

Description: CTIOS Server

Copyright: Copyright © 1994 - 2003 Cisco Systems

Other version information

Item name:
- Comments
- Company Name
- Internal Name
- Language
- OLESelfRegister
- Original Filename
- Product Name
- Product Version

Value:
Cisco CTI Products Release 6.0, Build 01061

CHAPTER 3

CTI Toolkit Desktop Client Installation

Note **IMPORTANT:** The new CTI OS functionality that is part of Release 8.0(1) is installed by the procedure discussed in Chapter 4, "Installing and Configuring CTI OS Silent Monitor". Release 8.0(1) upgrades Release 7.5(1) or later. When Release 8.0(1) is applied to a Release 7.5(1) system, it performs an upgrade. However, when Release 8.0(1) is applied to a Release 7.1 or a Release 7.2 system, it first rolls back the system to Release 7.0 and then performs the upgrade to Release 8.0(1).

This chapter provides procedures for installing the following CTI Toolkit Desktop Client components:

- CTI Toolkit Desktop applications:
  - Agent Desktop (including Silent Monitor)
  - IPCC Supervisor Desktop (including Silent Monitor)
  - Tools
- Documentation
- CTI Toolkit SDK (previously the CTI OS Developer's Toolkit, including necessary files, controls, documentation, and samples needed to write custom applications):
  - Win32
  - Java
  - .NET

It also provides procedures for enabling the Emergency Call and Supervisory Call buttons, which enable an agent to make a call to a supervisor. It contains the following sections:

Note Before you begin installation, verify that your system meets the hardware and software requirements for the components you plan to install, as listed in the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*. This document is available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm

Upgrading from a Previous Version

If you are upgrading from a previous CTI OS release, you need not uninstall the CTI Toolkit Desktop Client software before you install CTI Toolkit Desktop Client Release 8.0(1).

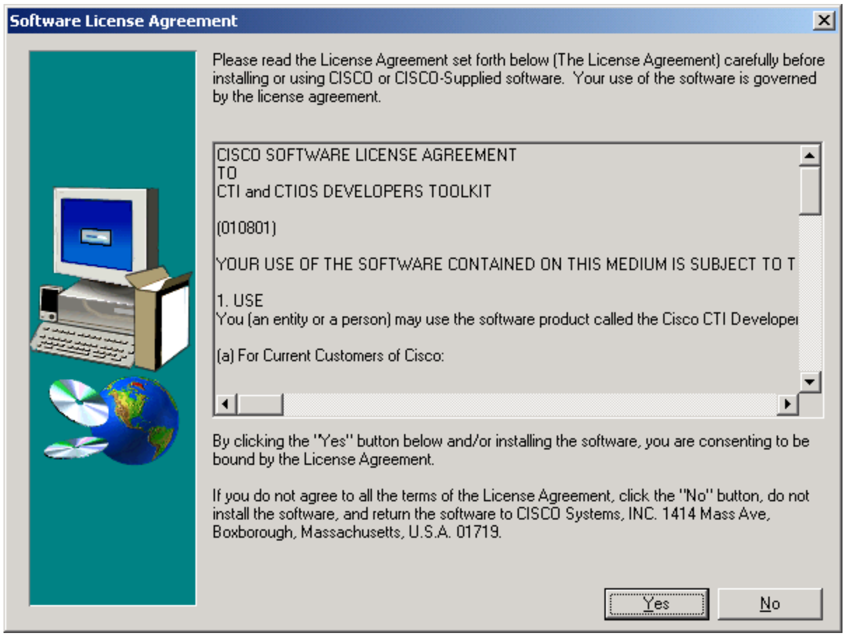
Cisco CTI Toolkit Desktop Client Component Installation

To install the CTI Toolkit Desktop Client components, perform the following steps.

Step 1 From the Installs\CTIOSClient directory on the CD, run **Setup.exe**.

Step 2 Click the **Next** button on the Welcome screen. The Software License Agreement screen appears.

Figure 3-1 CTI Toolkit Desktop Client Component Installation License Agreement



Please read the License Agreement set forth below (The License Agreement) carefully before installing or using CISCO or CISCO-Supplied software. Your use of the software is governed by the license agreement.

CISCO SOFTWARE LICENSE AGREEMENT
TO
CTI and CTIOS DEVELOPERS TOOLKIT

(010801)

YOUR USE OF THE SOFTWARE CONTAINED ON THIS MEDIUM IS SUBJECT TO T

1. USE
You (an entity or a person) may use the software product called the Cisco CTI Develope

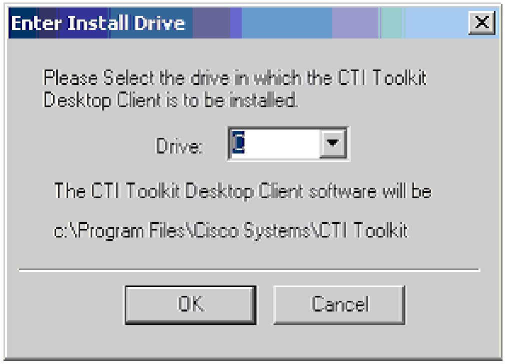
(a) For Current Customers of Cisco:

By clicking the "Yes" button below and/or installing the software, you are consenting to be bound by the License Agreement.

If you do not agree to all the terms of the License Agreement, click the "No" button, do not install the software, and return the software to CISCO Systems, INC. 1414 Mass Ave, Boxborough, Massachusetts, U.S.A. 01719.

Step 3 Click the **Yes** button. The Choose Destination Location screen appears.

Figure 3-2 Destination Drive selection



Enter Install Drive

Please Select the drive in which the CTI Toolkit Desktop Client is to be installed.

Drive: C

The CTI Toolkit Desktop Client software will be

c:\Program Files\Cisco Systems\CTI Toolkit

Step 4 Accept the default drive or click the **Browse** button and specify another drive.

Step 5 Click **Next**. The Select Components screen appears.

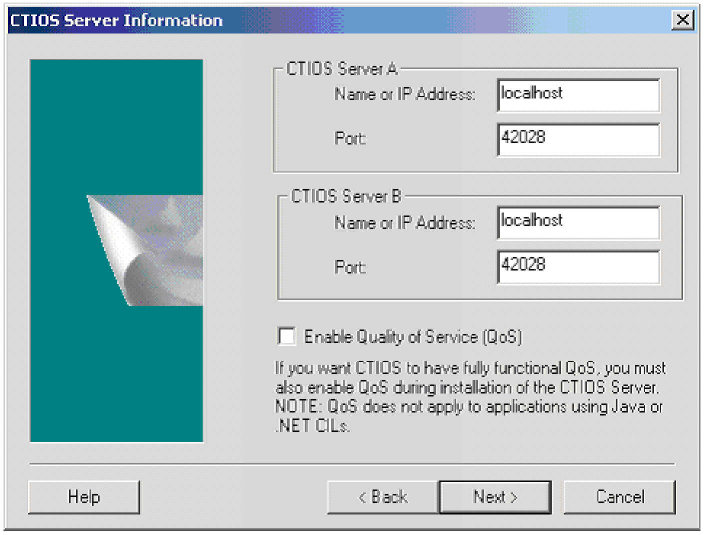
Select the CTI Toolkit Desktop Client components that you want to install.

Note If you plan to use the Release 8.0(1) Silent Monitor Service, you must select at least one of the CTI Toolkit Desktop Software components or the CTI Desktop SDK Win32 component.

Step 6 Click **Next**. If you selected CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop, the CTIOS Server Information screen appears.

Note Phones that are configured to use SRTP are not able to be silently monitored. Customers who wish to silently monitor agents must not configure the agent phones to use SRTP.

Figure 3-3 CTI OS Server Information



CTIOS Server Information

CTIOS Server A
Name or IP Address: localhost
Port: 42028

CTIOS Server B
Name or IP Address: localhost
Port: 42028

□ Enable Quality of Service (QoS)

If you want CTIOS to have fully functional QoS, you must also enable QoS during installation of the CTIOS Server. NOTE: QoS does not apply to applications using Java or .NET CILs.

Enter the Name or IP Address and the Port Number for your CTI OS systems.

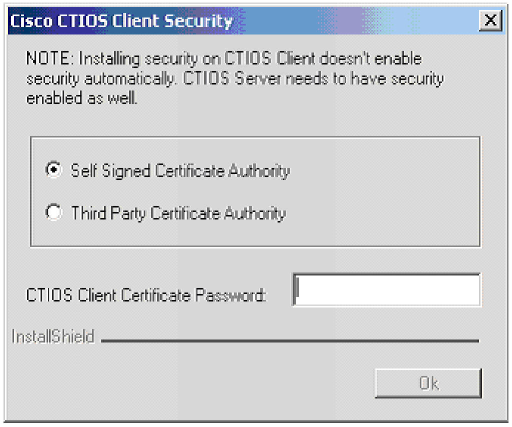
Note If you enabled the QoS checkbox during the CTI OS Server Installation, you must select the checkbox at this stage as well. If the Desktop is being installed on either Windows Vista or Windows 7, ensure that you are familiar with Quality of Service/Type of Service (QoS/ToS), page 8-34 before proceeding.

Step 7 Click the **Next** button. The Start Copying Files screen appears.

Step 8 Click the **Next** button to begin installation.

Step 9 When installation is complete, you see the following window that prompts you to install the Security feature. For more information about CTI OS Security, see Chapter 7, “CTI OS Security”.

Figure 3-4 CTI OS Client Security



Cisco CTIOS Client Security

NOTE: Installing security on CTIOS Client doesn't enable security automatically. CTIOS Server needs to have security enabled as well.

● Self Signed Certificate Authority

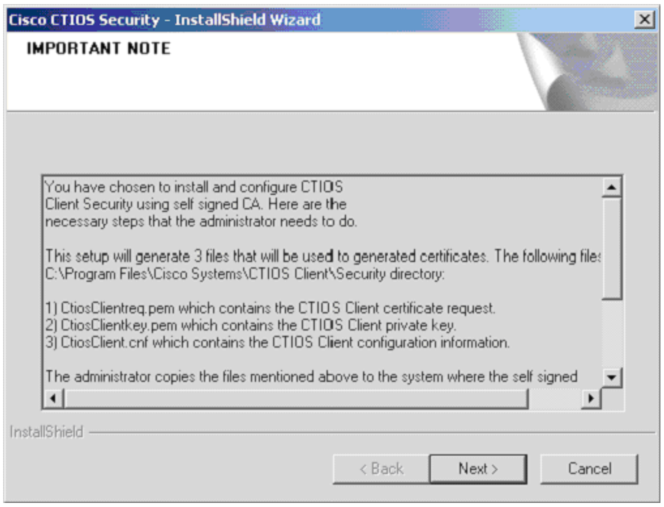
○ Third Party Certificate Authority

CTIOS Client Certificate Password:

For details about what Security Certificate option you must select, refer to Chapter 7, "CTI OS Security."

Step 10 Click **OK**. You see the following window:

Figure 3-5 CTI OS Security InstallShield Wizard



Cisco CTIOS Security - InstallShield Wizard

IMPORTANT NOTE

You have chosen to install and configure CTIOS
Client Security using self signed CA. Here are the
necessary steps that the administrator needs to do.

This setup will generate 3 files that will be used to generated certificates. The following file:
C:\Program Files\Cisco Systems\CTIOS Client\Security directory:

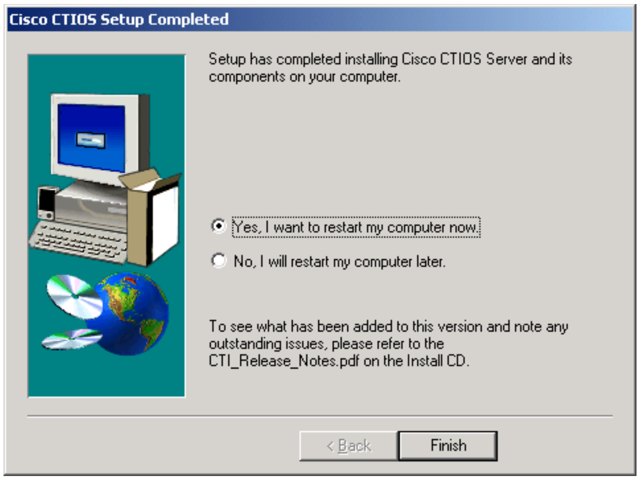
1) CtiosClientreq.pem which contains the CTIOS Client certificate request.
2) CtiosClientkey.pem which contains the CTIOS Client private key.
3) CtiosClient.cnf which contains the CTIOS Client configuration information.

The administrator copies the files mentioned above to the system where the self signed

While Security is being configured, several status messages are displayed.

Step 11 Lastly, you see a Setup Complete screen.

Figure 3-6 CTI OS Server setup completion dialog



Cisco CTIOS Setup Completed

Setup has completed installing Cisco CTIOS Server and its components on your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

To see what has been added to this version and note any outstanding issues, please refer to the CTI_Release_Notes.pdf on the Install CD.

Step 12 Specify whether or not you want to restart your computer. Click the **Finish** button to exit Setup.

Installed Files

When you install CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop, the CTI Toolkit installation process installs a number of dynamic link libraries (DLLs). The installation process registers many of these DLLs automatically, but some of these DLLs must be registered manually in order to work correctly.

Table 3-1 lists the Windows DLLs that are installed with CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop, along with the command line entry for manually registering the DLL (if needed).

Table 3-1 Windows DLLs

DLL	Command Line Entry For Manually Registering
msvcrt.dll	Registration not needed.
msvcrtd.dll	Registration not needed.
msvcp60.dll	Registration not needed.
msvcp60d.dll	Registration not needed.
mfc42.dll	Registration not needed.
mfc42d.dll	Registration not needed.
atl.dll	regsvr32 atl.dll
msvbvm60.dll	regsvr32 msvbvm60.dll

The following Softphone Controls DLLs are installed with CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop.

- CtiosStatusbar.dll
- EmergencyAssistCtl.dll
- AgentSelectCtl.dll

- GridControl.dll
- AgentStateCtl.dll
- HoldCtl.dll
- AlternateCtl.dll
- IntlResourceLoader.dll
- AnswerCtl.dll
- Arguments.dll
- BadLineCtl.dll
- ButtonControl.dll
- ChatCtl.dll
- ConferenceCtl.dll
- CtiCommonDlgs.dll
- MakeCallCtl.dll
- ReconnectCtl.dll
- CTIOSAgentStatistics.dll
- RecordCtl.dll
- CTIOSCallAppearance.dll
- SubclassForm.dll
- CTIOSClient.dll
- SupervisorOnlyCtl.dll
- CTIOSSessionResolver.dll
- TransferCtl.dll
- CTIOSSkillGroupStatistics.dll

If the CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop indicate that a given DLL is not registered, the DLL can be registered manually by the following command.

regsvr32 <DLL filename>

For example, CtiosStatusbar.dll would be registered by the following command.

regsvr32 CtiosStatusbar.dll

With interoperability, the Win32 COM controls work under the .NET framework. The installation lays down the following files and installs them into the Global Access Cache (GAC):

AxInterop.AgentSelectCtl.dll	Cisco.CTICOMMONDLGSLib.dll	Interop.AgentSelectCtl.dll
AxInterop.AgentStateCtl.dll	Cisco.CTIOSARGUMENTSLib.dll	Interop.AgentStateCtl.dll
AxInterop.AlternateCtl.dll	Cisco.CTIOSCLIENTLib.dll	Interop.AlternateCtl.dll
AxInterop.AnswerCtl.dll	Cisco.CTIOSSESSIONRESOLVERLib.dll	Interop.AnswerCtl.dll

AxInterop.BadLineCtl.dll	Cisco.INTLRESOURCELOADERLib.dll	Interop.BadLineCtl.dll
AxInterop.ButtonControl.dll		Interop.ButtonControl.dll
AxInterop.ChatCtl.dll		Interop.ChatCtl.dll
AxInterop.ConferenceCtl.dll		Interop.ConferenceCtl.dll
AxInterop.CTIOSAgentStatistics.dll		Interop.CTIOSAgentStatistics.dll
AxInterop.CTIOSCallAppearance.dll		Interop.CTIOSCallAppearance.dll
AxInterop.CTIOSSkillGroupStatistics.dll		Interop.CTIOSSkillGroupStatistics.dll
AxInterop.CTIOSStatusBar.dll		Interop.CTIOSStatusBar.dll
AxInterop.EmergencyAssistCtl.dll		Interop.EmergencyAssistCtl.dll
AxInterop.GridControl.dll		Interop.GridControl.dll
AxInterop.HoldCtl.dll		Interop.HoldCtl.dll
AxInterop.MakeCallCtl.dll		Interop.MakeCallCtl.dll
AxInterop.ReconnectCtl.dll		Interop.ReconnectCtl.dll
AxInterop.RecordCtl.dll		Interop.RecordCtl.dll
AxInterop.SilentMonitorCtl.dll		Interop.SilentMonitorCtl.dll
AxInterop.SubclassForm.dll		Interop.SubclassForm.dll
AxInterop.SupervisorOnlyCtl.dll		Interop.SupervisorOnlyCtl.dll
AxInterop.TransferCtl.dll		Interop.TransferCtl.dll

Uninstalling CTI Toolkit

To uninstall CTI Toolkit, run **Add/Remove** programs from the Windows Control Panel and select **Cisco CTI Toolkit Uninstall**.

Determining Version Number of Installed Files

If CTI Toolkit Agent Desktop or CTI Toolkit Supervisor Desktop for IPCC are currently running, the title bars of the desktop windows display the CTI Toolkit version number.

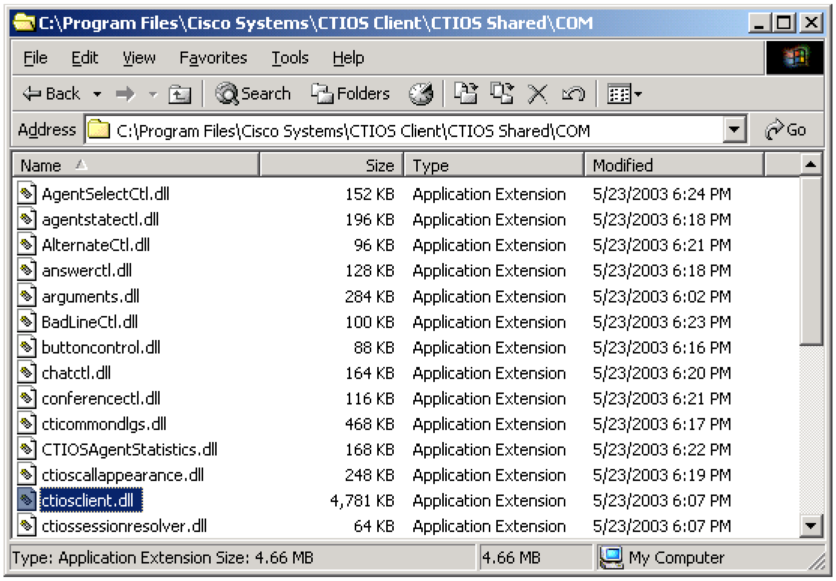
If these desktops are *not* currently running, you can determine the version number of an installed CTI Toolkit file by performing the following steps.

Step 1 Go to the directory:

```
Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\COM Servers and
Activex Controls
```

Step 2 Highlight and right-click on the file **ctiosclient.dll**.

Figure 3-7 CTI OS COM Directory



C:\Program Files\Cisco Systems\CTIOS Client\CTIOS Shared\COM

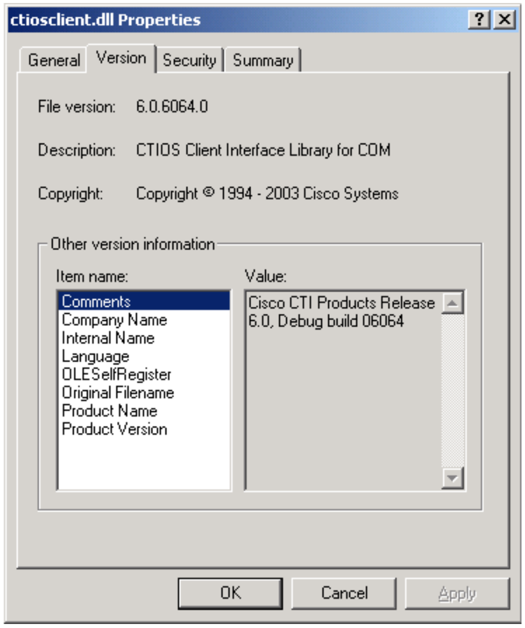
Name	Size	Type	Modified
AgentSelectCtl.dll	152 KB	Application Extension	5/23/2003 6:24 PM
agentstatectl.dll	196 KB	Application Extension	5/23/2003 6:18 PM
AlternateCtl.dll	96 KB	Application Extension	5/23/2003 6:21 PM
answerctl.dll	128 KB	Application Extension	5/23/2003 6:18 PM
arguments.dll	284 KB	Application Extension	5/23/2003 6:02 PM
BadLineCtl.dll	100 KB	Application Extension	5/23/2003 6:23 PM
buttoncontrol.dll	88 KB	Application Extension	5/23/2003 6:16 PM
chatctl.dll	164 KB	Application Extension	5/23/2003 6:20 PM
conferencectl.dll	116 KB	Application Extension	5/23/2003 6:21 PM
cticommondlgs.dll	468 KB	Application Extension	5/23/2003 6:17 PM
CTIOSAgentStatistics.dll	168 KB	Application Extension	5/23/2003 6:22 PM
ctioscallappearance.dll	248 KB	Application Extension	5/23/2003 6:19 PM
ctiosclient.dll	4,781 KB	Application Extension	5/23/2003 6:07 PM
ctiossessionresolver.dll	64 KB	Application Extension	5/23/2003 6:07 PM

Type: Application Extension Size: 4.66 MB | 4.66 MB | My Computer

Step 3 Select **Properties** from the drop-down menu. The Properties dialog box appears.

Step 4 Select the **Version** tab. This tab contains version information (release number and build number) for the file.

Figure 3-8 CTI OS Client Properties



ctiosclient.dll Properties

File version: 6.0.6064.0

Description: CTIOS Client Interface Library for COM

Copyright: Copyright © 1994 - 2003 Cisco Systems

Other version information

Item name:
Comments
Company Name
Internal Name
Language
OLESelfRegister
Original Filename
Product Name
Product Version

Value:
Cisco CTI Products Release 6.0, Debug build 06064

Unified CM Intercept Configuration Requirement

Cisco Unified CM service parameter named Drop Ad Hoc Conference must be set to "never" (the default value), otherwise during the Intercept function, all the parties in the call get dropped.

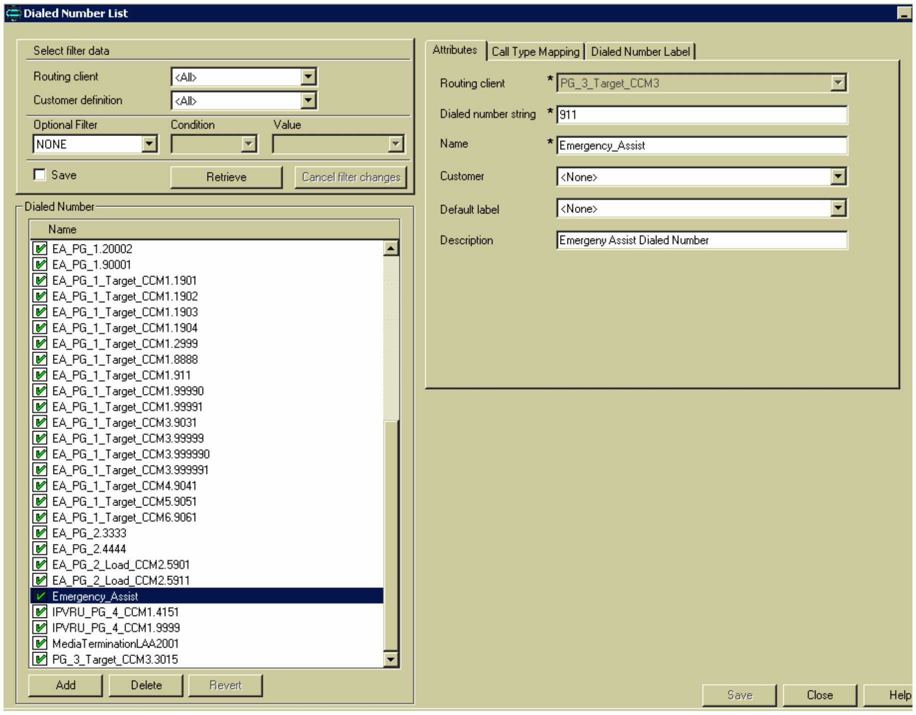
Configuring Supervisory Assistance Features

The CTI Toolkit Agent Desktop includes buttons that enable an agent to make an emergency call to a supervisor or to place a call to request assistance from a supervisor. To enable the functionality for these buttons, a *Unified ICM system administrator* must perform the following steps.

Step 1 Do the following tasks from the Unified ICM Configuration Manager (refer to the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted*).

a. On the Dialed Number List screen, create a Dialed Number for the supervisor, as shown in the following screens.

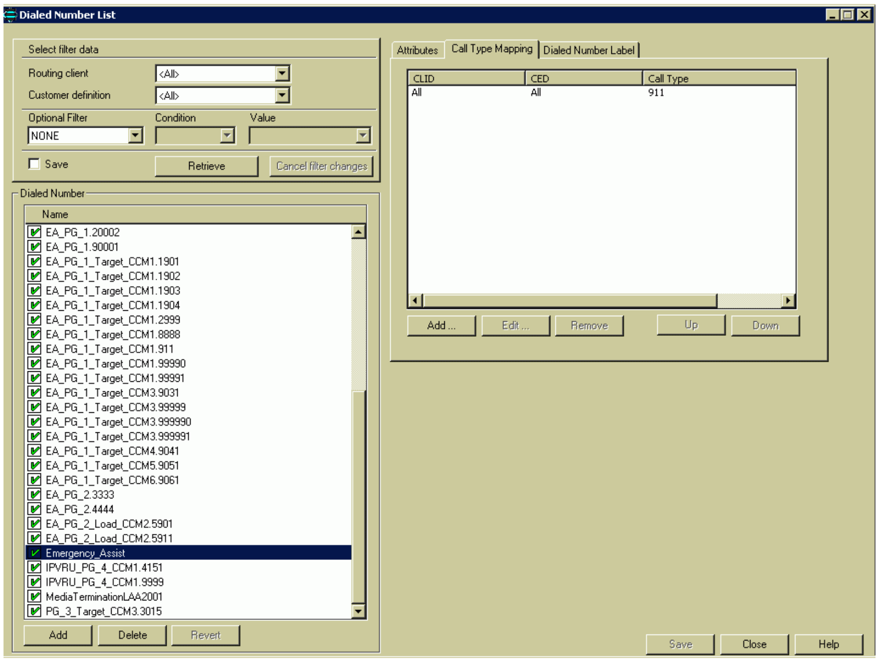
Figure 3-9 Dialed Number List



Routing client <All>
Customer definition <All>
Optional Filter NONE

- ☑ EA_PG_1.20002
- ☑ EA_PG_1.90001
- ☑ EA_PG_1_Target_CCM1.1901
- ☑ EA_PG_1_Target_CCM1.1902
- ☑ EA_PG_1_Target_CCM1.1903
- ☑ EA_PG_1_Target_CCM1.1904
- ☑ EA_PG_1_Target_CCM1.2999
- ☑ EA_PG_1_Target_CCM1.8888
- ☑ EA_PG_1_Target_CCM1.911
- ☑ EA_PG_1_Target_CCM1.99990
- ☑ EA_PG_1_Target_CCM1.99991
- ☑ EA_PG_1_Target_CCM3.9031
- ☑ EA_PG_1_Target_CCM3.99999
- ☑ EA_PG_1_Target_CCM3.999990
- ☑ EA_PG_1_Target_CCM3.999991
- ☑ EA_PG_1_Target_CCM4.9041
- ☑ EA_PG_1_Target_CCM5.9051
- ☑ EA_PG_1_Target_CCM6.9061
- ☑ EA_PG_2.3333
- ☑ EA_PG_2.4444
- ☑ EA_PG_2_Load_CCM2.5901
- ☑ EA_PG_2_Load_CCM2.5911
- ☑ Emergency_Assist
- ☑ IPVRU_PG_4_CCM1.4151
- ☑ IPVRU_PG_4_CCM1.9999
- ☑ MediaTerminationLAA2001
- ☑ PG_3_Target_CCM3.3015

Routing client * PG_3_Target_CCM3
Dialed number string * 911
Name * Emergency_Assist
Customer <None>
Default label <None>
Description Emergeny Assist Dialed Number


Dialed Number List

Select filter data
Routing client: <All>
Customer definition: <All>
Optional Filter: NONE
☐ Save

Dialed Number

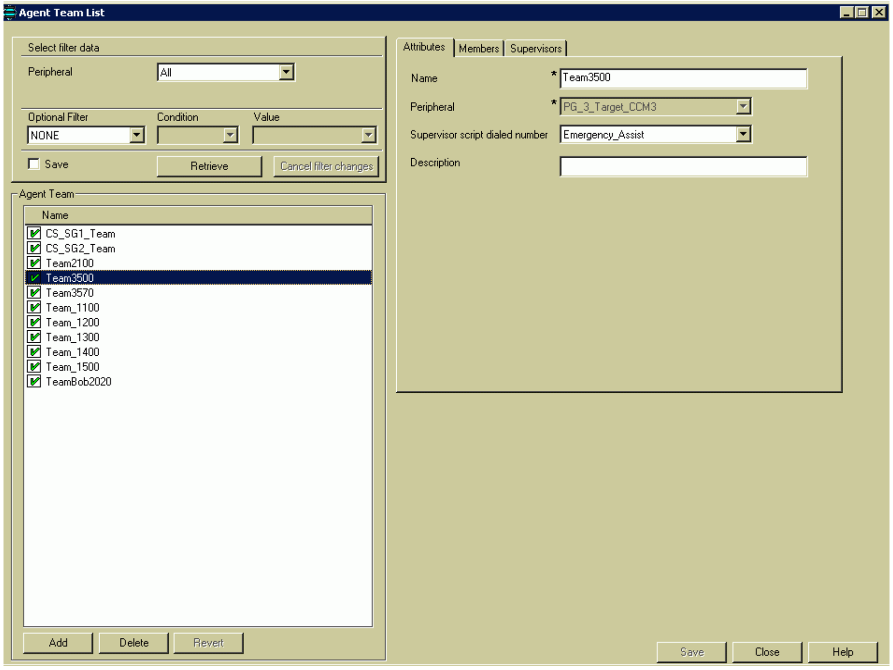
Name
☑ EA_PG_1.20002
☑ EA_PG_1.90001
☑ EA_PG_1_Target_CCM1.1901
☑ EA_PG_1_Target_CCM1.1902
☑ EA_PG_1_Target_CCM1.1903
☑ EA_PG_1_Target_CCM1.1904
☑ EA_PG_1_Target_CCM1.2999
☑ EA_PG_1_Target_CCM1.8888
☑ EA_PG_1_Target_CCM1.911
☑ EA_PG_1_Target_CCM1.99990
☑ EA_PG_1_Target_CCM1.99991
☑ EA_PG_1_Target_CCM3.9031
☑ EA_PG_1_Target_CCM3.99999
☑ EA_PG_1_Target_CCM3.999990
☑ EA_PG_1_Target_CCM3.999991
☑ EA_PG_1_Target_CCM4.9041
☑ EA_PG_1_Target_CCM5.9051
☑ EA_PG_1_Target_CCM6.9061
☑ EA_PG_2.3333
☑ EA_PG_2.4444
☑ EA_PG_2_Load_CCM2.5901
☑ EA_PG_2_Load_CCM2.5911
☑ Emergency_Assist
☑ IPVRU_PG_4_CCM1.4151
☑ IPVRU_PG_4_CCM1.9999
☑ MediaTerminationLAA2001
☑ PG_3_Target_CCM3.3015

Call Type Mapping

CLID	CED	Call Type
All	All	911

b. On the Agent Team List screen, enter the Dialed Number in the Supervisor script dialed number field, as shown.

Figure 3-10 Agent Team List


Agent Team List

Select filter data
Peripheral: All
Optional Filter: NONE
☐ Save

Agent Team

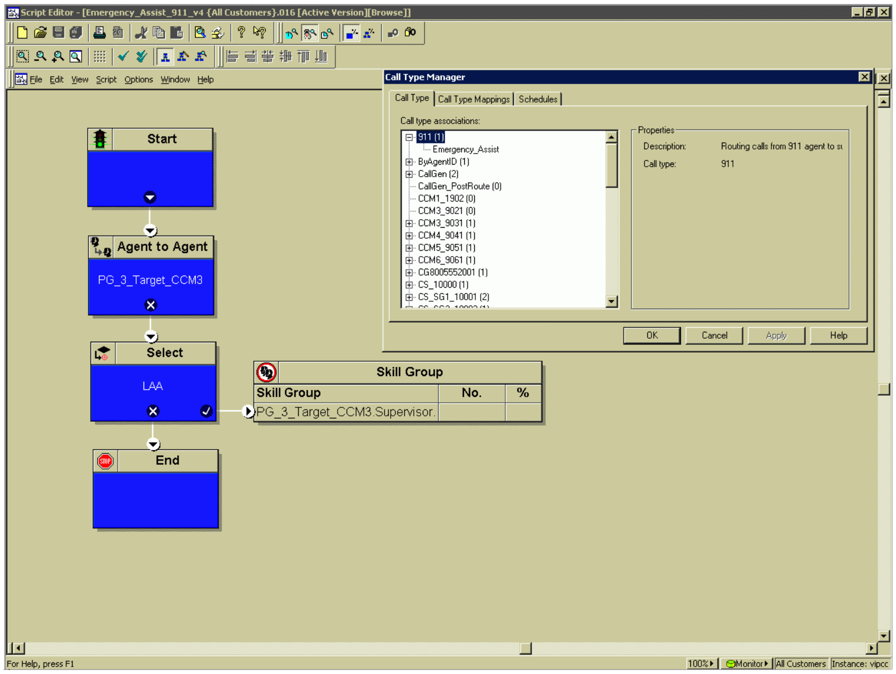
Name
☑ CS_SG1_Team
☑ CS_SG2_Team
☑ Team2100
☑ Team3500
☑ Team3570
☑ Team_1100
☑ Team_1200
☑ Team_1300
☑ Team_1400
☑ Team_1500
☑ TeamBob2020

Attributes
Name *: Team3500
Peripheral *: PG_3_Target_CCM3
Supervisor script dialed number: Emergency_Assist
Description:

Step 2 Perform the following task from the Script Editor (refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*).

a. On the Call Type Manager screen, associate the Dialed Number with your script, as shown.

Figure 3-11 Call Type Manager



Call type associations:

- 911 (1)
  - Emergency_Assist
- ByAgentID (1)
- CallGen (2)
- CallGen_PostRoute (0)
- CCM1_1902 (0)
- CCM3_9021 (0)
- CCM3_9031 (1)
- CCM4_9041 (1)
- CCM5_9051 (1)
- CCM6_9061 (1)
- CG8005552001 (1)
- CS_10000 (1)
- CS_SG1_10001 (2)

Properties

Description: Routing calls from 911 agent to su

Call type: 911

Skill Group		
Skill Group	No.	%
PG_3_Target_CCM3.Supervisor.		

Configuring Video

For information on configuring video on CTI OS or CAD desktops, refer to *Configuring Video on the Cisco CTI OS or CAD Desktops* topic in the *Configuration and Administration Guide for Cisco Unified Customer Voice Portal, Release 8.0(1)* located at:
http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp7_0/configuration/guide/cvp70cfg.pdf.

CHAPTER 4

Installing and Configuring CTI OS Silent Monitor

This chapter describes how to install CTI OS Silent Monitor.

Note You must install CTI OS before installing and configuring the Silent Monitor Service

Installing and Configuring the Silent Monitor Service

This section provides an overview of the Silent Monitor service and discusses the tasks involved in installing and configuring the Silent Monitor service.

Note The terms Silent Monitor service and Silent Monitor server are used throughout this document. Silent Monitor service refers to a silent monitoring service running on agent or supervisor's desktop computer or Citrix client. This service handles silent monitoring functionality for one agent or supervisor. Silent Monitor server refers to a Silent Monitor service providing silent monitoring functionality for a group of mobile agents. These agents share the same gateway.

Silent Monitor service Overview

The silent monitor functionality resides in a separate silent monitor service, rather than in the CIL. This is necessary to support both Citrix and Mobile Agent environments. C++ agent and supervisor desktops communicate with the silent monitor service via TCP connection. The agent desktop uses the silent monitor service to forward a voice stream to the supervisor's silent monitor service that plays the stream on the supervisor's computer speakers.

In a traditional IPCC environment, the silent monitor service runs alongside the agent and supervisor desktops on the agent’s and supervisor’s computer. However, Mobile Agent and Citrix environments do not give the CIL access to the voice packets because the agent's computer is not connected to the network through the agent’s phone. In a Citrix environment, the desktop is actually running on the Citrix Presentation Server. The agents and supervisor computers are running Citrix clients. These clients render the user interface for the desktops, but the actual desktop processes are running on the presentation server. In a Citrix deployment, the silent monitor service is deployed on the Citrix client where it has access to the agent’s voice stream or the supervisor’s speaker. In a Citrix deployment, a silent monitor service is deployed on the agent's Citrix client where it has access to the voice stream. The agent desktop uses this service to forward the agent's voice stream to the supervisor. The supervisor's Citrix client also runs a silent monitor service. This service plasy back streams from monitored agents using the speaker on the Citrix client.

In mobile agent deployments, the voice path crosses the Public Switched Telephone Network (PSTN) and two gateways. One gateway control calls from customer phones. The other gateway controls agent calls. In this deployment, the silent monitor service is deployed from a SPAN port on the same switch as the agent gateway. This provides the silent monitor service with access to voice streams passing through the gateway. In a mobile agent environment, the supervisor still uses a silent monitor service on the supervisor's desktop or Citrix client to play back the voice stream.

How Desktops Connect to Silent Monitor Services

The following is the Supervisor Desktop connection algorithm:

1. If the supervisor desktop is running under Citrix, determine the IP address of the Citrix client. Connect to the silent monitor service running at port 42228 on the Citrix client.
2. If the supervisor desktop is not running under Citrix, connect to the silent monitor service running at port 42228 on localhost.

Note While CTI OS Silent Monitor clusters use port 42228 (the default), the Silent Monitor peers utilize port 42029 for communications purposes.

The following is the Agent Desktop connection algorithm:

1. If the agent desktop's connection profile specifies a silent monitor server or set of silent monitor servers, randomly choose a silent monitor server to connect to using the port present in the connection profile. Refer to Chapter 2, "CTI OS Server Installation" for more information on how a connection profile is configured to include silent monitor services.
2. If the agent desktop is running under Citrix, determine the IP address of the Citrix client. Connect to the silent monitor service running at port 42228 on the Citrix client.
3. If the agent desktop is not running under Citrix, connect to the silent monitor service running at port 42228 on localhost.

Note A connection profile may be used to override port 42228. In this case, desktops use the preceding algorithms to determine the address of the silent monitor service. After the address is determined, desktops connect using the determined address and the port that is present in the connection profile.

Silent Monitor Service Installers

The installer places two silent monitor service installers in the following directory:

```
<Install Drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\Silent
Monitor Files
```

The following installers are available after the 7.1(1) CTI OS Client Upgrade and can be obtained from the Cisco.com:

- SilentMonitorInstall_nogui.exe – this executable silently installs the silent monitor service with the following settings:

- Installed in the directory C:\Program Files\CiscoSystems\CTIOS SilentMonitor
- Listens on port 42228
- No QoS
- No Security

This executable runs automatically when a Release 7.0(0) client is updated to Release 7.1(1) (or later). It replaces the Release 7.0(0) CIL with the Release 7.1(1) (or later) CIL, and installs and starts the silent monitor service so that the agent and supervisor desktops do not lose functionality. Running only this executable is sufficient if you do not wish to override the default settings or enable QoS or Security.

Note This executable works only on the machines that either do not have WinPCap installed or have WinPCap Release 3.0 installed.

- SMSelfExtractedInstallPackage.exe – this executable extracts the silent monitor service setup program into the following directory:

```
<Install Drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32
CIL\Silent Monitor Files\SilentMonitorServiceInstall
```

Run this executable if you wish to specify a different destination directory or port, or if you want to enable QoS and/or Security.

To run this executable silently:

Step 1 Open a command prompt window and navigate to the directory <Install Drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\Silent Monitor Files\SilentMonitorServiceInstall.

Step 2 Enter the command:

setup.exe /s

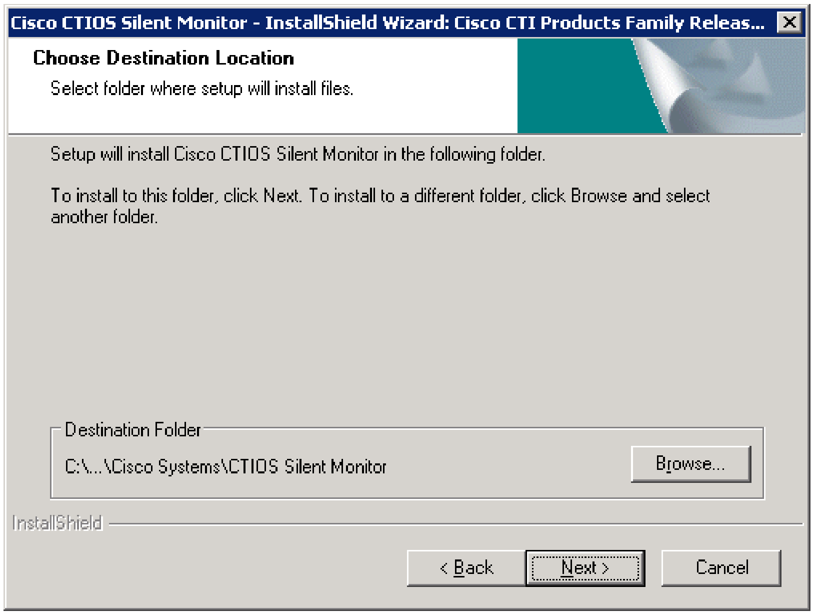
Note This runs the executable with the default values specified in the supplied answer file setup.iss. To override the default values, edit this answer file and change the values that you wish to change.

To run the full installation program for this executable, perform the following steps:

Step 1 In Windows Explorer, navigate to the <Install Drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\Silent Monitor Files\SilentMonitorServiceInstall directory.

Step 2 Double-click on **setup.exe**. The installation process begins and the following screen appears.

Figure 4-1 Silent Monitor Service InstallShiels Wizard I



Cisco CTIOS Silent Monitor - InstallShield Wizard: Cisco CTI Products Family Releas...

Choose Destination Location

Select folder where setup will install files.

Setup will install Cisco CTIOS Silent Monitor in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

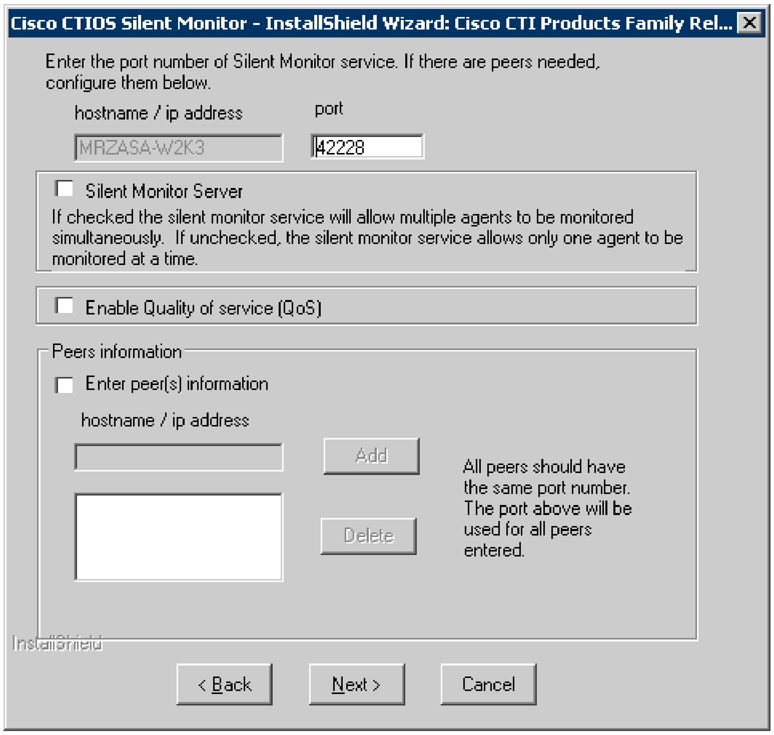
Destination Folder

C:\...\Cisco Systems\CTIOS Silent Monitor

You can either accept the default destination folder or click the **Browse** button and specify another directory.

Step 3 Click **Next**. The following screen appears.

Figure 4-2 CTI OS Silent Monitor InstallShield Wizard II



Cisco CTIOS Silent Monitor - InstallShield Wizard: Cisco CTI Products Family Rel...

Enter the port number of Silent Monitor service. If there are peers needed, configure them below.

hostname / ip address: MRZASA-W2K3

port: 42228

□ Silent Monitor Server

If checked the silent monitor service will allow multiple agents to be monitored simultaneously. If unchecked, the silent monitor service allows only one agent to be monitored at a time.

□ Enable Quality of service (QoS)

Peers information

□ Enter peer(s) information

hostname / ip address

All peers should have the same port number. The port above will be used for all peers entered.

Specify the following information on this screen.

- **Port** – Enter the number of the port on which the silent monitor service listens for incoming connections.
- **Silent Monitor Server** – Select this to allow the silent monitor service to monitor many mobile agents simultaneously.

  IMPORTANT: The silent monitor server *must* be installed on its own server; it *cannot* be coresident with CTI OS Server or a Peripheral Gateway. This server machine must meet the hardware and software requirements specified in the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*. This document is available at: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1626/ccmigration_09186a00804d7607.pdf.
- **Enable Quality of service** – Select this to enable Quality of Service (QoS).

Note If the Desktop is being installed on either Windows Vista or Windows 7, ensure that you are familiar with Quality of Service/Type of Service (QoS/ToS), page 8-34 before proceeding.

- **Enter peer(s) information** – Select this if this silent monitor service is part of a cluster of silent monitor services.
- **Hostname / IP address** – the hostname or IP address of the other silent monitor services in the cluster. All services in a cluster must be configured to listen on the same port. For example, if port is set to 42228 for the service you are currently configuring, it must be set to 42228 for all other services in the cluster. See also the section entitled Silent Monitor Service Clusters, page 4-9.

Step 4 Users must install a Windows Server 2008 R2 compatible maintenance release (MR) for this software to function on Windows Server 2008 R2.

Note If **setup.exe** is run from a *local* drive, you cannot apply the maintenance release (the Maintenance Release Installer window does not display).

Step 5 Click **Next** to finish the installation process.

Step 6 Set up security. Depending on whether you want to use a self-signed certificate authority (CA) or a third-party CA, follow the instructions in the section Signing Silent Monitor Server Certificate Request with Self-Signed CA or the section Signing Silent Monitor Service Certificate Request with Third-Party CA. For more information on CTI OS Security, see Chapter 7, "CTI OS Security."

Signing Silent Monitor Server Certificate Request with Self-Signed CA

Follow these steps to sign a Silent Monitor Server certificate request:

Step 1 If the self-signed CA does not exist, then run **CreateSelfSignedCASetupPackage.exe** and store all the files that were created by the **CreateSelfSignedCASetupPackage.exe** program in a safe place.

Step 2 Copy **CtiosServerKey.pem**, and **CtiosServerReq.pem** files from the Silent Monitor Server machine to the machine where **CtiosRoot.pem** and **CtiosRootCert.pem** reside. Both **CtiosServerKey.pem** and **CtiosServerReq.pem** files must be copied to the same directory as **CtiosRoot.pem** and **CtiosRootCert.pem**.

Step 3 Run **SignCertificateSetupPackage.exe** from the same directory where **CtiosServerKey.pem**, **CtiosServerReq.pem**, **CtiosRoot.pem** and **CtiosRootCert.pem** reside, select **CTI OS Server Certificate Request**, and enter the Ctios Certificate Authority password. This step generates **CtiosServer.pem** file if it is successful; otherwise it displays an error message.

Step 4 Copy **CtiosServer.pem** and **CtiosRootCert.pem** back to the machine where Silent Monitor Server resides and save them in the C:\Cisco Systems\CTIOS\Silent Monitor\Security directory.

Step 5 Delete **CtiosServerkey.pem** from the machine where Silent Monitor Server is installed.

Step 6 Delete **CtiosServerKey.pem**, **CtiosServerReq.pem**, and **CtiosServer.pem** from the machine where **SignCertificateSetupPackage.exe** ran.

Step 7 If the Silent Monitor Server machine has a peer server, then:

a. Copy **CtiosClientkey.pem** and **CtiosClientreq.pe**m files from the Silent Monitor Server machine to the machine where **CtiosRoot.pem** and **CtiosRootCert.pem** reside. Both **CtiosClientkey.pem** and **CtiosClientreq.pem** files must be copied to the same directory as **CtiosRoot.pem** and **CtiosRootCert.pem**.

b. Run **SignCertificateSetupPackage.exe** from the same directory where **CtiosClientkey.pem, CtiosClientreq.pem**, **CtiosRoot.pem** and **CtiosRootCert.pem** reside, select **CTI Toolkit Desktop Client Certificate Request**, and enter the Ctios Certificate Authority password. This step generates **CtiosClient.pem** file if it is successful, otherwise it displays an error message.

c. Copy **CtiosClient.pem** to the machine where Silent Monitor Server resides and save it in the C:\Cisco Systems\CTIOS\Silent Monitor\Security directory.

d. Delete **CtiosClientkey.pem** from the machine where Silent Monitor Server is installed.

e. Delete **CtiosClientkey.pem**, **CtiosClientreq.pem**, and **CtiosClient.pem** from the machine where **SignCertificateSetupPackage.exe** ran.

Signing Silent Monitor Service Certificate Request with Third-Party CA

Follow these steps to sign a Silent Monitor service certificate request:

Step 1 Copy **CtiosServerReq.pem** file from the Silent Monitor service machine to the machine where the third-party CA resides.

Step 2 Signing Silent Monitor service certificate request (CtiosServerReq.pem) with third-party CA generates a Silent Monitor service certificate. Rename it **CtiosServerCert.pem**.

Step 3 The third-party CA has its certificate public information in a file. Rename this file **CtiosRootCert.pem**.

Step 4 Copy **CtiosServerCert.pem** and **CtiosRootCert.pem** to the machine where Silent Monitor Service resides and save them in the C:\Cisco Systems\CTIOS\Silent Monitor\Security directory.

Step 5 On the Silent Monitor Service machine, copy the data in **CtiosServerCert.pem** and the data in **CtiosServerkey.pem** files into one file called **CtiosServer.pem**. The order is very important, so **CtiosServer.pem** must contain **CtiosServerCert.pem** data first and **CtiosServerkey.pem** data second.

Step 6 Delete **CtiosServerCert.pem** and **CtiosServerkey.pem** from the Silent Monitor service machine.

Step 7 If the Silent Monitor service machine has a peer server, then:

a. Copy **CtiosClientreq.pem** file from the Silent Monitor service machine to the machine where the third-party CA resides.

b. Signing CTI Toolkit Desktop Client certificate request (CtiosClientreq.pem) with third-party CA generates a CTI Toolkit Desktop Client certificate. Rename it **CtiosClientCert.pem**.

c. Copy **CtiosClientCert.pem** file to the machine where Silent Monitor service resides and save it in the C:\Cisco Systems\CTIOS\Silent Monitor\Security directory.

d. On the Silent Monitor service machine, copy the data in **CtiosClientCert.pem** and the data in the **CtiosClientkey.pem** files into one file called **CtiosClient.pem**. The order is very important, so **CtiosClient.pem** must contain **CtiosClientCert.pem** data first and **CtiosClientkey.pem** data second.

e. Delete **CtiosClientCert.pem** and **CtiosClientkey.pem** from the Silent Monitor service machine.

Additional Configuration Steps

This section discusses the Silent Monitor service configuration steps that you must perform after you install the Silent Monitor service. These steps are necessary to deliver Silent Monitor service connection information to client applications.

Rerun CTI OS Server Setup

Rerun CTI OS Server setup to perform the following tasks:

- To configure agents to use the Silent Monitor service.
- To configure security for clients, so they can connect to Silent Monitor services that have security enabled.

- To configure Mobile Agents. When you rerun setup, enable Mobile Agent and the appropriate agent mode. This modifies the connection profile information in the registry. The **ShowFieldBitMask** is modified to display the RAS fields on the login dialog and the **RasCallMode** registry key is added.
- To enable the default tracemark set it to 0x3.

See Chapter 2, "CTI OS Server Installation" for instructions on running CTI OS Server setup.

Installing and Configuring the Silent Monitor Service in a Traditional IPCC Environment

When a desktop is upgraded to CTI OS Release 7.1(1), the Silent Monitor service is silently installed on the desktop computer and set to listen for incoming connections on port 42228. The upgraded desktop then uses the Silent Monitor service to forward and play back streams.

Installing and Configuring the Silent Monitor Service in a Citrix /WTS Environment

The following considerations apply to installing and configuring the Silent Monitor service in a Citrix or Citrix/WTS environment:

- You can use the SilentMonitorInstall_nogui.exe executable to silently install the silent monitor service on both agent and supervisor Citrix clients.
- All supervisors in a Citrix environment must have the Silent Monitor service installed on the computer running the Citrix client.
- All standard IPCC agents in a Citrix environment must have the Silent Monitor service installed on the computer running the Citrix client.
- Mobile agents in a Citrix environment do not need the Silent Monitor service installed because they use the Silent Monitor service that is forwarding traffic from the agent gateway. See Chapter 2, "CTI OS Server Installation" for information on how to configure agents to use a specific Silent Monitor service.

Additional Configuration for Mobile Agent Environments

The following configuration considerations apply to environments that run Mobile Agent:

- Mobile Agent is not supported with Siebel.
- In a mobile agent environment, the silent monitor service uses a Switched Port Analyzer (SPAN) port to receive the voice traffic that passes through the agent gateway. This requires the computer running the silent monitor service to have two NIC cards: one to handle communications with clients, and one to receive all traffic spanned from the switch. For example, if the agent gateway is connected to port 1 and the NIC on the Silent Monitor server that receives SPAN traffic is connected on port 10, the following commands are used to configure the SPAN session:

  ```
  monitor session 1 source interface fastEthernet0/1
  monitor session 1 destination interface fastEthernet0/10
  ```

  Refer to your switch manual for details on configuring a span port. In general, traffic to and from the agent gateway's port must be forwarded to the port that is configured to receive span traffic on the silent monitor service.
- There must be two gateways: one gateway for agent traffic, and another for caller traffic. If one gateway is used for agent and caller traffic, the voice traffic does not leave the gateway and cannot be silently monitored.

- Voice traffic that does not leave the agent gateway or does not cross the agent gateway cannot be silent monitored. For example, agent-to-agent and consultation calls between mobile agents that share the same gateway cannot be silently monitored. In most mobile agent deployments, the only calls that can be reliably silent monitored are calls between agents and customers.
- All supervisors in a Mobile Agent environment must have the Silent Monitor service installed on their desktop or installed on the computer running the Citrix client if the supervisor is in a Citrix environment.
- Agents do not need the silent monitor service configured on their desktops. However, you must configure the agent to use one or more silent monitor servers in the CTI OS Server setup program.
- If there are agents that can be both mobile and traditional IPCC, there must be at least two profiles for such agents. One profile, used when logging in as IPCC, does not contain any Silent Monitor service information. A second profile, used when logging in as a mobile agent, contains information used to connect to a Silent Monitor server. This enables the Mobile Agent to use the Silent Monitor service on their desktop computer or Citrix client and provides that Mobile Agent with silent monitoring functionality.

Silent Monitor Service Clusters

If more than one agent gateway is present in the call center, and an agent can use either gateway to log in, Silent Monitor services must be clustered to support Silent Monitor. A separate silent monitor server must be deployed for each gateway. A SPAN port must be configured for each silent monitor server as described in the previous section. The Silent Monitor server installer must then be run to install and configure the two Silent Monitor servers as peers. After this is done, you must set up a a connection profile to instruct the agent desktops to connect to one of the peers. (See Chapter 2, "CTI OS Server Installation"for information on the CTI OS Server installer program.) To set up a connection profile, check the "Enter peer(s) information" checkbox and fill in the IP address of the other silent monitor service in the "Hostname/ip address" text box during silent monitor service installation (see Step 3 in the section "Silent Monitor Service Installers").

Installing and Configuring the Silent Monitor Service with Windows Firewall Service Enabled

Any Windows 2008 R2 computer that has Windows Firewall Service enabled must create a new port with the following parameters:

- Port Type: Silent Monitor Service Port
- Port Number: 42029

Note While CTI OS Silent Monitor clusters use port 42228 (the default), the Silent Monitor peers utilize port 42029 for communications purposes.

Silent Monitor Server Security Hardening Procedure

ICM Security Hardening script can be only run on Windows Server 2003. To apply security hardening on a Silent Monitor Server, you must perform the following manual steps:

Step 1 Run the executable **SMSelfExtractedInstallPackage.exe**, which the Release 7.1(1) installation process installs in the following directory:

```
<Install Drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\Silent
Monitor Files
```

This executable puts a batch file named CopySecurityHardeningFiles.bat and the SecurityTemplate directory in the current directory.

Step 2 Run **CopySecurityHardeningFiles.bat.** This creates the directory C:\CiscoUtils and copies the corresponding files there.

Step 3 Go to the directory C:\CiscoUtils\SecurityTemplate.

Step 4 Run the command **cscript ICMSecurityHardening.vbe HARDEN**.

Add Silent Monitor Service to Windows Firewall Exceptions

The following steps describe how to add the Silent Monitor Service as an exception if Windows Firewall is enabled on Windows Server 2003.

Step 1 From the Windows Control Panel, click on **Windows Firewall**.

Step 2 If you see a message"Your PC is not Protected: Turn on Windows Firewall," turn on Windows Firewall.

Step 3 From the Windows Firewall dialog box, click on the **Exceptions** tab.

Step 4 Select the **Silent Monitor service** and specify it as an exception. If you do not see the Silent Monitor service on the list of programs, click the **Add Program** button then click the **Browse** button. The Silent Monitor service executable SilentMonitorService.exe is located in the bin directory below the install directory.

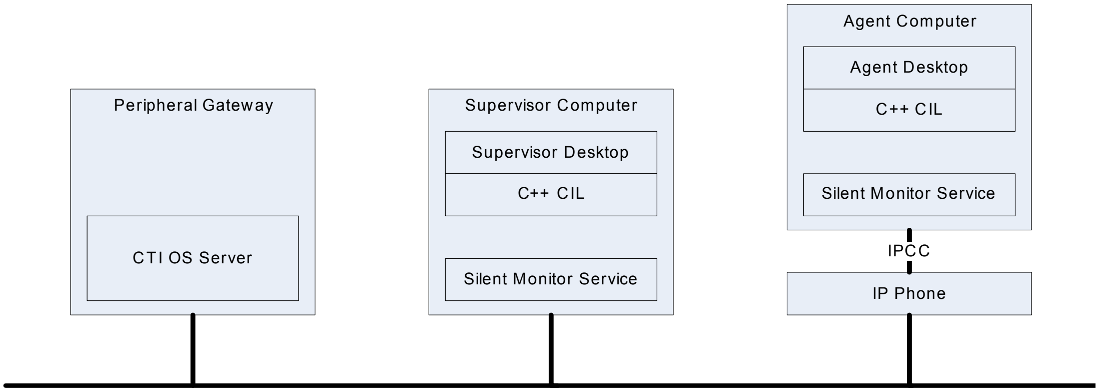
Silent Monitor Service Deployments

This section illustrates the following example silent monitor service deployments:

- IPCC
- Citrix
- Mobile Agent
- Mobile Agent with Citrix

IPCC Deployment

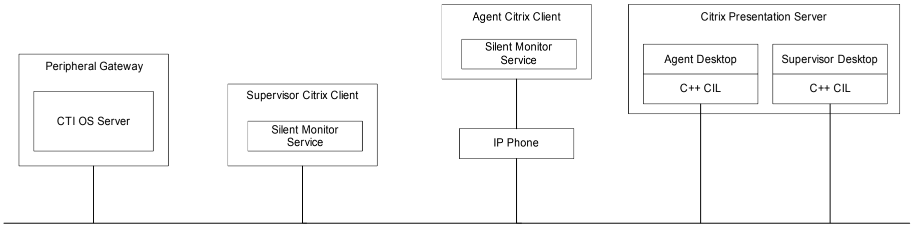
Figure 4-3 IPCC Deployment topology



- When customers upgrade from 7.0 desktops to 7.1, the Silent Monitor service is silently installed on the agent desktop computer.
- The desktop is deployed behind the agent's phone. Silent monitor functionality will be the same as before the upgrade. The only difference is that the service and not the CIL provides the silent monitor functionality.
- If the Silent Monitor service needs a different configuration than the one provided by the silent installer, SMSelfExtractedInstallPackage.exe must be used to reconfigure the service.
- A default IPCC connection profile may be used for IPCC agents if no QoS is required. Otherwise a connection profile containing QoS settings must be configured. This works because CTI OS agent desktops attempt to connect to the localhost if no silent monitor services are configured using the connection profile.
- A default IPCC connection profile may be used for IPCC supervisors if no QoS is required. Otherwise, a connection profile containing QoS settings must be configured. This works because CTI OS supervisor desktops attempt to connect to localhost if no silent monitor services are configured via the connection profile.

Citrix Deployment

Figure 4-4 Citrix Deployment topology

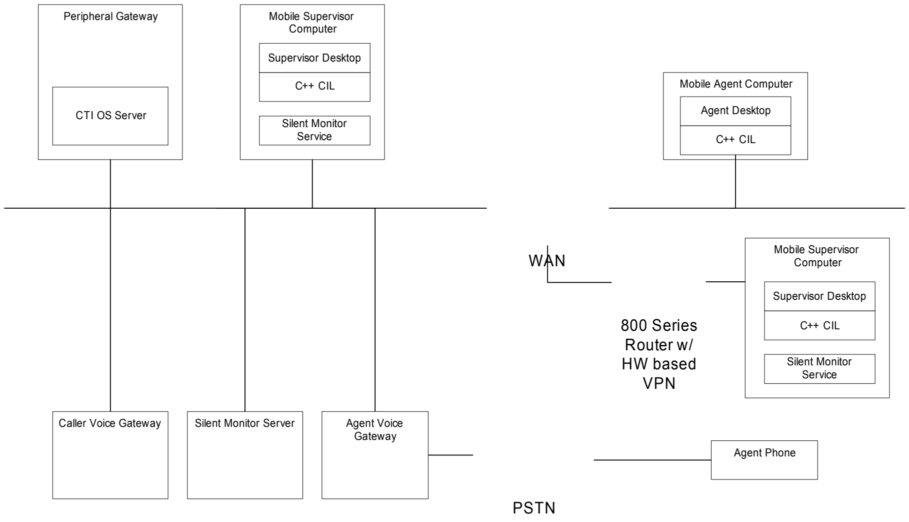


- The 7.1 desktop is installed on the Citrix server.
- If Citrix clients are required to have silent monitoring functionality, the Silent Monitor service must be deployed on the Citrix client computers.

- The silent installer can be used to install the Silent Monitor service with default settings. Otherwise, SMSelfExtractedInstallPackage.exe must be used.
- A default IPCC connection profile may be used for IPCC agents if no QoS is required. Otherwise, a connection profile containing QoS settings must be configured. This works because CTI OS agent desktops attempt to connect to the Silent Monitor service running on the Citrix client if the client detects it is running under Citrix.
- A default IPCC connection profile may be used for IPCC supervisors if no QoS is required. Otherwise, a connection profile containing QoS settings must be configured. This works because CTI OS supervisor desktops attempt to connect to the Silent Monitor service running on the Citrix client if the client detects it is running under Citrix.

Mobile Agent Using Analog/PSTN Phone

Figure 4-5 Mobile Agent Analog/PSTN Phone topology



- A Silent Monitor server is installed on a separate computer using the SMSelfExtractedInstallPackage.exe installer.
  - Make sure to check “Silent Monitor Server” when installing the silent monitor server.
  - This computer must have two NIC cards: one to receive SPAN port traffic and the other to receive control requests from clients and to forward monitored voice streams.
- Supervisors use the silent monitor service configured on supervisor’s computer.
- Connection profiles are configured to tell mobile agents how to connect to the Silent Monitor servers.
- **SPAN port is configured on the switch.** The following steps are used to configure a SPAN port:
  - Locate the port on the switch where the agent voice gateway is connnected.
  - Locate the port on the switch where the NIC card that receives SPAN traffic on the Silent Monitor server is connected.
  - Configure the switch to route SPAN traffic to the Silent Monitor server.

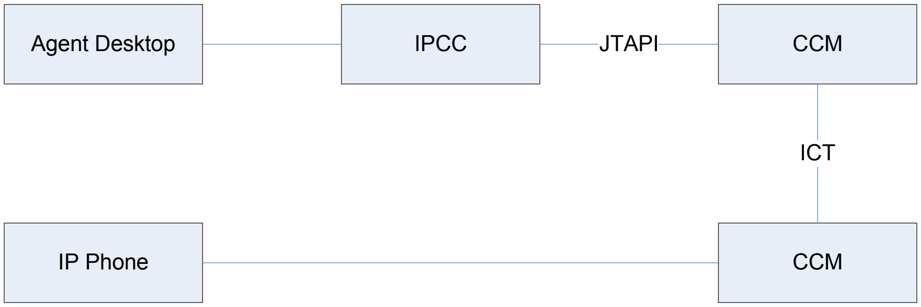
- The following commands would be issued in global configuration mode if the voice gateway was connected to port 10 on the switch and the silent monitor service was connected to port 15.

```
no monitor session 1
monitor session 1 source interface fastEthernet0/10
monitor session 1 destination interface fastEthernet0/15
```

Mobile Agents Using IP Phones

In some deployments, mobile agents use IP phones homed to a Unified CM other than the Unified CM used by IPCC. The following diagram illustrates the deployment of the agent phones.

Figure 4-6 Mobile Agents IP Phones topology



In these cases, the silent monitor deployment is the same as the equivalent IPCC Agent deployment. The only difference is the Unified CM to which the agent's phone is homed. The following sections describe how to deploy silent monitor when mobile agents use IP phones.

Mobile Agent Using IP Phone

Silent monitor is deployed as described below when mobile agents are using IP phones homed to a Unified CM other than the Unified CM used by IPCC.

- When customers upgrade 7.0 desktops to 7.1 or later, the Silent Monitor service is silently installed on the agent desktop computer. The desktop is deployed behind the agent's phone: silent monitor functionality is the same as before the upgrade. The only difference is that the service and not the CIL provides the silent monitor functionality.
- If the silent monitor service needs a different configuration than the one provided by the silent installer, SMSelfExtractedInstallPackage.exe must be used to reconfigure the service.
- A connection profile is configured to allow agents and supervisors to login as mobile agents. See the "Defining Connection Profiles" section of this document for details.

Refer to the figure in the "IPCC Deployment" section of this document for an illustration of this silent monitor deployment.

Mobile Agent Using IP Phone and Citrix

Silent monitor is deployed as described below when mobile agents using Citrix are using IP phones homed to a Unified CM other than the Unified CM used by IPCC:

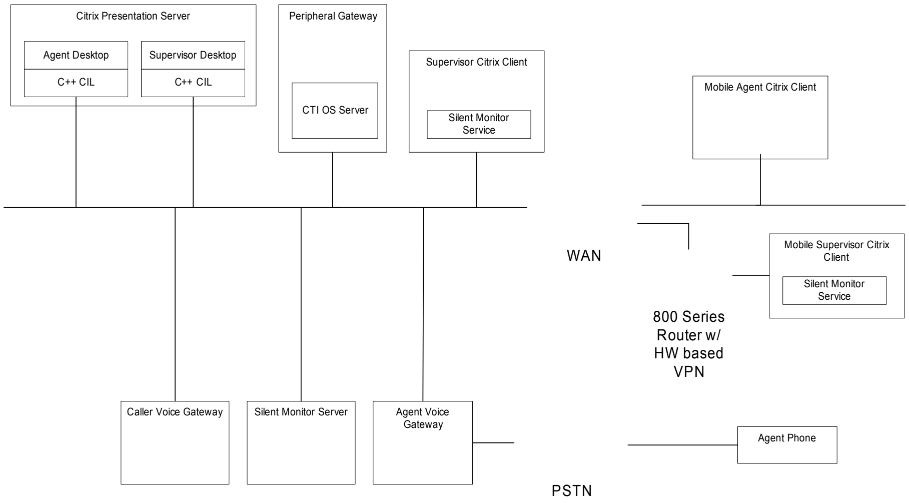
- The 7.1 or later desktop is installed on the Citrix server.

- If Citrix clients are required to have silent monitoring functionality, the Silent Monitor service must be deployed on the Citrix client computers.
- The silent installer can be used to install the Silent Monitor service with default settings. Otherwise, SMSelfExtractedInstallPackage.exe must be used.
- A connection profile must be configured to allow agents and supervisors to log in as mobile agents. See the "Defining Connection Profiles" section of this document for details.

Refer to the diagram in the "Citrix Deployment" section of this document for an illustration of this silent monitor deployment.

Mobile Agent Using Analog/PSTN Phone and Citrix

Figure 4-7 Mobile Agent Analog/PSTN and Citrix topology



For the most part, Citrix mobile agents are configured the same as non-Citrix mobile agents with the following exceptions:

- Mobile supervisors using Citrix clients need Silent Monitor services configured on their Citrix clients.
- Mobile agents using Citrix do not need Silent Monitor services configured since the clients use the Silent Monitor server configured from the SPAN port.

CHAPTER 5

Installing, Uninstalling, and Failed Installation Recovery of CTI OS Release 8.0(1) Components

This chapter contains the following sections:

- "Silent Installation of CTI OS Release 8.0(1) Components" on page 1
- "Uninstalling Release 8.0(1) Components" on page 3
- "Recovering from a Failed Installation of CTI OS Release 8.0(1)" on page 4

Silent Installation of CTI OS Release 8.0(1) Components

CTI OS Release 8.0(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 Desktops.
- CTI OS Agent and Supervisor Desktops under Citrix.
- CTI OS Server.

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 For CTI OS Release 8.0(1), silent installation of the CTI OS Agent and Supervisor desktops be aware of the following:
-.NET 2.0 must be installed prior to silent installation.
- Only CTI OS Agent and Supervisor desktops of CTI OS Client install can be silently installed; other CTI OS Client installation options cannot be installed silently.
- Only fresh silent installation is supported. You must uninstall all previous versions or patches of CTI OS Client prior to silently installing the CTI OS Client.
- Security is not installed when you install Client phones silently in Release 8.0(1). If security is needed, after the installation is complete, run **SecuritysetupPackage.exe** from the installation CD.
- You must stop the Cisco Security Agent (CSA) manually before silent installation, and restart the service after the installation procedure is completed.

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

The silent installation process involves two tasks:

- Creating a response file.
- Using the response file to run CTI OS silent install on other machines.

The following sections list the steps involved in these tasks.

Warning **Use of silent installations is discouraged, as errors encountered during the install process may go unnoticed and leave the system in an invalid state. If you choose to run installations silently, be absolutely certain that the required pre and post installation instructions are manually performed on the target systems.**

Creating a Response File

The process of creating a response file for use with CTI OS silent install installs the 7.x(y) release of all CTI OS components (CTI OS Agent Desktop, CTI OS Supervisor Desktop, CTI OS Server) that exist on the machine where the response file is recorded. To create a response file for use with CTI OS silent install, perform the following steps:

Step 1 Shut down CSA (Windows 2003 only) and any running CTI OS components (CTI OS Server, CTI OS Client, and so on).

Step 2 From a command prompt, run the CTI OS Release 7.x(y) installer with the following syntax:

```
CTIOS7[1].1(1).exe -options-record “c:\mypatfh\myresponsefile.opt”
```

where “c:\mypatfh\myresponsefile.opt” is the complete path and filename that you want to give to the response file. The -options-record flag indicates that the install runs in record mode, which triggers the output of the response file. However, in order to create a response file the installer actually runs and installs the application on the system.

Note For Release 8.0(1) on a Windows Server 2003 or Release 8.0(1a) on a 2008 R2 system, run setup from a command prompt with the following option: **setup.exe /r**. For Windows Server 2003, this outputs a file called setup.iss to the Windows directory. For Windows Server 2008 R2, this outputs a file called setup.iss to the <drive>:\icm directory. When the installer completes, examine the setup log file to verify that the installation is complete with no errors.

Step 3 When the installation is complete, examine the setup log file to verify that installation ran to completion with no errors.

Caution It is critical that you verify that the installation process ran successfully and created a valid response file. Running CTI OS silent install with an invalid response file can leave your system in an invalid state.

Step 4 Reboot your system.

Running CTI OS Silent Install on Other Machines

After you create a response file on one machine, you can use that response file to run CTI OS silent install on other machines. To do this, perform the following steps:

Step 1 Copy the response file to the machine(s) on which you wish to run CTI OS silent install.

Step 2 Shut down Cisco Security Agent (CSA) (Windows Server 2003 only) and any running CTI OS components (CTI OS Server, CTI OS Client, and so on).

Step 3 From a command prompt, run the CTI OS Release 8.0(1) installer with the following syntax:

```
CTIOS7[1].1(1).exe –options “c:\mypath\myresponsefile.opt” -silent
```

where “c”\mypath\myresponsefile.opt” is the complete path and filename for the response file. The -silent flag indicates that the installation runs in silent mode.

Note For Release 8.0(1), copy the setup.iss file created above to the same directory where setup.exe is located, and then run the setup with the following syntax: **setup.exe /s**.

Step 4 When the installation is complete, examine the setup log file to verify that installation ran to completion with no errors.

Caution It is critical that you verify that the installation process ran successfully and created a valid response file. Running CTI OS silent install with an invalid response file can leave your system in an invalid state.

Step 5 Reboot your system.

Uninstalling Release 8.0(1) Components

For Windows Server 2008 R2 systems, run setup.exe from the <drive>:\icm\CTIOS_bin directory to delete an instance.

To uninstall all CTI OS Release 7.x(y) components, run Add/Remove programs from the Windows Control Panel and select Cisco CTI OS Release 7.x(y) Uninstall.

When you uninstall CTI OS Release 7.x(y) components, your system reverts back to CTI OS Release 7.0(0). In addition, the following changes occur:

- Client registry keys—The registry key name HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc. reverts back to HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems. Also, any registry key changes from HKEY_LOCAL_MACHINE to HKEY_CURRENT_USER revert.
- Server registry keys—Any Release 7.x(y) registry keys that are associated with Remote Agent agents and peripheral type are removed.
- Server setup—If 7.1(x) or 7.2(x) has been installed over 7.0,the system reverts back to the Release 7.0(0) server setup. Selections pertaining to Remote Agent or Silent Monitor Server are no longer present. If 7.2(x) has been installed over 7.1(x), the system reverts back to the Release 7.1(x) server setup. Selections pertaining to silent monitor type (Unified CM Based, CTI OS Based, Disabled) are no longer present.

- Client setup—Removed altogether.

Recovering from a Failed Installation of CTI OS Release 8.0(1)

If an attempted CTI OS Release 8.0(1) installation fails for reasons such as power failure, disk error, or other similar circumstances, perform the following procedures to recover from the failed installation:

Step 1 Uninstall Release 8.0(1), as documented in the "Uninstalling Release 8.0(1) Components" section on page 5-3.

Step 2 Reinstall Release 8.0(1) by performing the procedures documented in the following sections:

- "Installing CTI OS Server" section on page 2-2.
- "Silent Monitor Service Installers" section on page 4-2.
- Additional Configuration Steps, page 4-7.

CHAPTER 6

Configuring Unified CM-Based Silent Monitor

This chapter contains the following sectionss

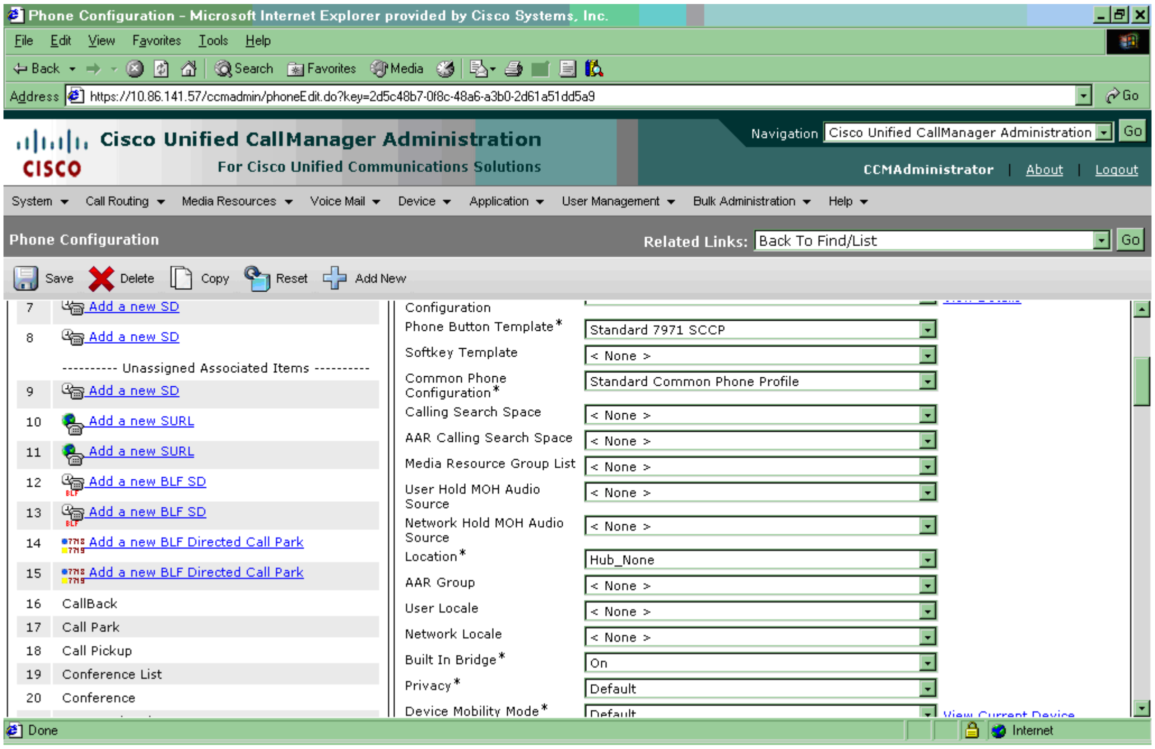
Unified CM Configuration and Administration

This section describes how to configure devices and JTAPI users on Unified CM to enable silent monitoring.

Enable "Built-in Bridge" for the Agent's Device

On the Phone Configuration page (Figure 6-1), “Built-in Bridge” must be set to **On** for the agent's device (79X1) to be silently monitored.

Figure 6-1 Phone Configuration (Built in Bridge)


Phone Configuration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CallManager Administration Go
CCMAdministrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Add New
Done
Internet

Address: https://10.86.141.57/ccmadmin/phoneEdit.do?key=2d5c48b7-0f8c-48a6-a3b0-2d61a51dd5a9

7 Add a new SD
8 Add a new SD
---------- Unassigned Associated Items ----------
9 Add a new SD
10 Add a new SURL
11 Add a new SURL
12 Add a new BLF SD
13 Add a new BLF SD
14 Add a new BLF Directed Call Park
15 Add a new BLF Directed Call Park
16 CallBack
17 Call Park
18 Call Pickup
19 Conference List
20 Conference

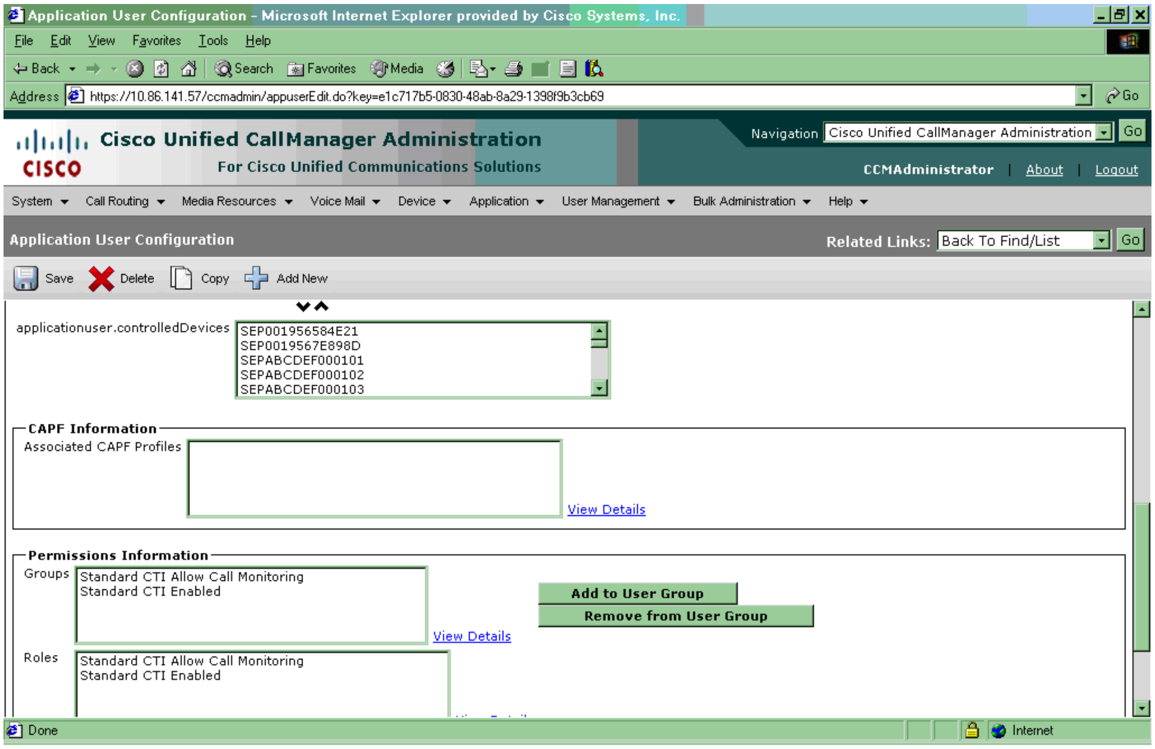
Configuration	
Phone Button Template*	Standard 7971 SCCP
Softkey Template	< None >
Common Phone Configuration*	Standard Common Phone Profile
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	On
Privacy*	Default
Device Mobility Mode*	Default

View Current Device

Add PG User to "Standard CTI Allow Call Monitor"

A new user group called "Standard CTI Allow Call Monitor" has been added in Unified CM 6.0. This group contains the set of application users that can silent monitor calls. The PG user must be added to the "Standard CTI Allow Call Monitor" user group in order to silent monitor calls. The following figure shows an example of an Application User Configuration page with an Application User added to the "Standard CTI Allow Call Monitor" user group.

Figure 6-2 Application User Configuration (CTI Allow Call Monitoring)


Application User Configuration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation
CCMAdministrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Application User Configuration
Related Links:
Save Delete Copy Add New
View Details
Add to User Group
Remove from User Group
Done
Internet

Address: https://10.86.141.57/ccmadmin/appuserEdit.do?key=e1c717b5-0830-48ab-8a29-1398f9b3cb69

Navigation: Cisco Unified CallManager Administration

Related Links: Back To Find/List

applicationuser.controlledDevices:
SEP001956584E21
SEP0019567E898D
SEPABCDEF000101
SEPABCDEF000102
SEPABCDEF000103

CAPF Information

Associated CAPF Profiles

Permissions Information

Groups:
Standard CTI Allow Call Monitoring
Standard CTI Enabled

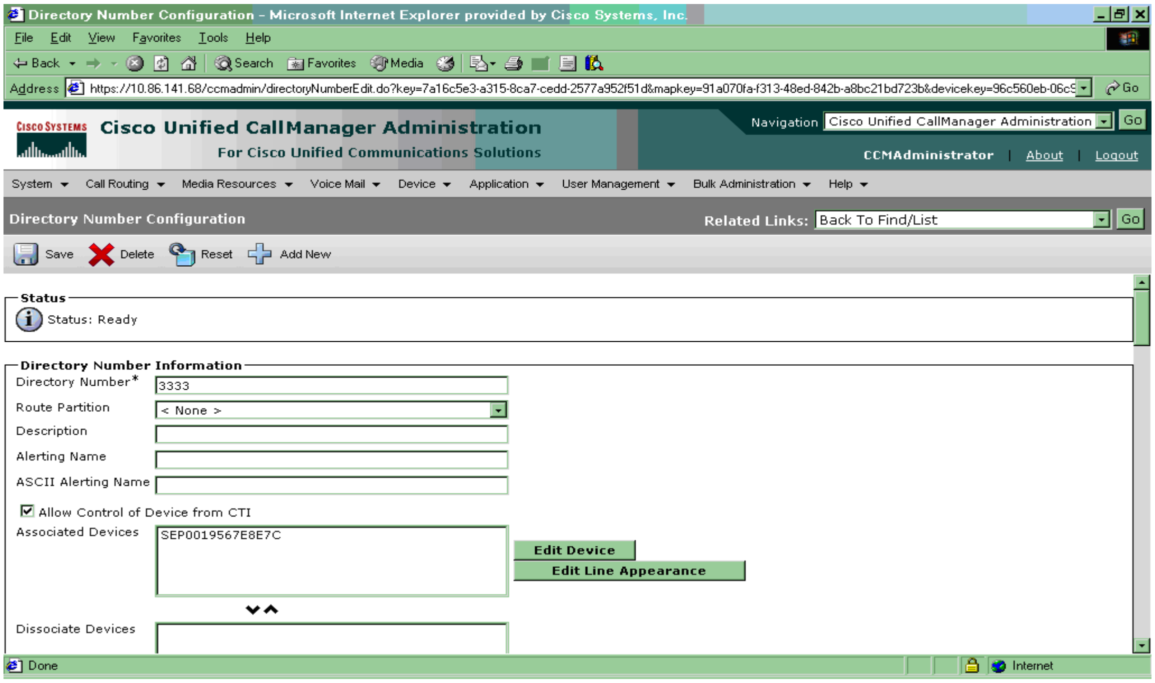
Roles:
Standard CTI Allow Call Monitoring
Standard CTI Enabled

Monitoring Calling Search Space

On the supervisor's line appearance page, there is an entry for "Monitoring Calling Search Space". The administrator enters the previously created partition for the agent that can be monitored. The Monitoring Calling Search Space on the supervisor's line appearance page must include the partition to which the agent's line belongs.

The following figure shows the Route Partition on the agent's line appearance page.

Figure 6-3 Agent Route Partition


Directory Number Configuration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.86.141.68/ccmadmin/directoryNumberEdit.do?key=7a16c5e3-a315-8ca7-cedd-2577a952f51d&mapkey=91a070fa-f313-48ed-842b-a8bc21bd723b&devicekey=96c560eb-06c9
Go
Cisco Systems
Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CallManager Administration Go
CCMAdministrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Directory Number Configuration
Related Links: Back To Find/List Go
Save Delete Reset Add New
Edit Device
Edit Line Appearance
Done
Internet

Status

Status: Ready

Directory Number Information

Directory Number* 3333

Route Partition < None >

Description

Alerting Name

ASCII Alerting Name

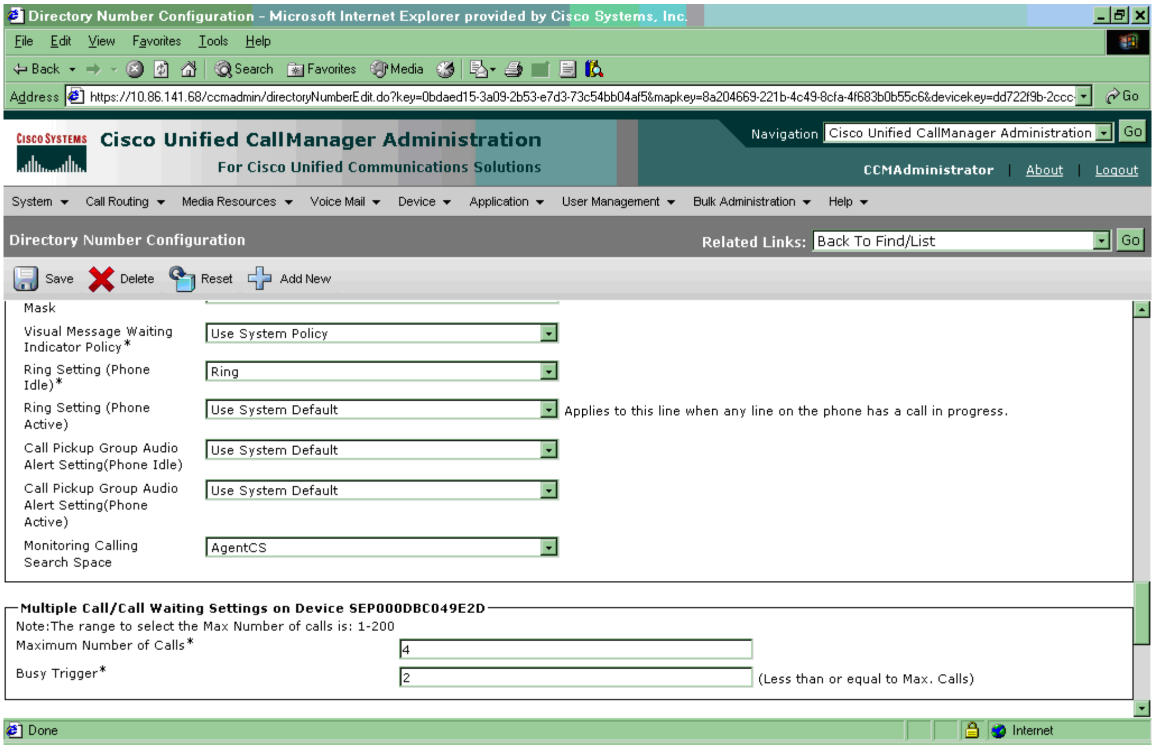
☑ Allow Control of Device from CTI

Associated Devices SEP0019567E8E7C

Dissociate Devices

The following figure shows the Monitoring Calling Search Space on the supervisor's line appearance page.

Figure 6-4 Supervisor Monitoring Calling Search Space


Directory Number Configuration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.86.141.68/ccmadmin/directoryNumberEdit.do?key=0bdaed15-3a09-2b53-e7d3-73c54bb04af5&mapkey=8a204669-221b-4c49-8cfa-4f683b0b55c6&devicekey=dd722f9b-2ccc
Go
Cisco Systems
Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CallManager Administration Go
CCMAdministrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Directory Number Configuration
Related Links: Back To Find/List Go
Save Delete Reset Add New
Done
Internet

Mask

Visual Message Waiting Indicator Policy* Use System Policy

Ring Setting (Phone Idle)* Ring

Ring Setting (Phone Active) Use System Default Applies to this line when any line on the phone has a call in progress.

Call Pickup Group Audio Alert Setting(Phone Idle) Use System Default

Call Pickup Group Audio Alert Setting(Phone Active) Use System Default

Monitoring Calling Search Space AgentCS

Multiple Call/Call Waiting Settings on Device SEP000DBC049E2D

Note:The range to select the Max Number of calls is: 1-200

Maximum Number of Calls* 4

Busy Trigger* 2 (Less than or equal to Max. Calls)

Monitoring Notification Tone

A monitoring notification tone can be configured using the Service Parameter Configuration page in Unified CM Administration. There are two entries:

- Play Monitoring Notification Tone to Observed Target

  When set to true, this option plays the tone to the monitored party (usually an agent).

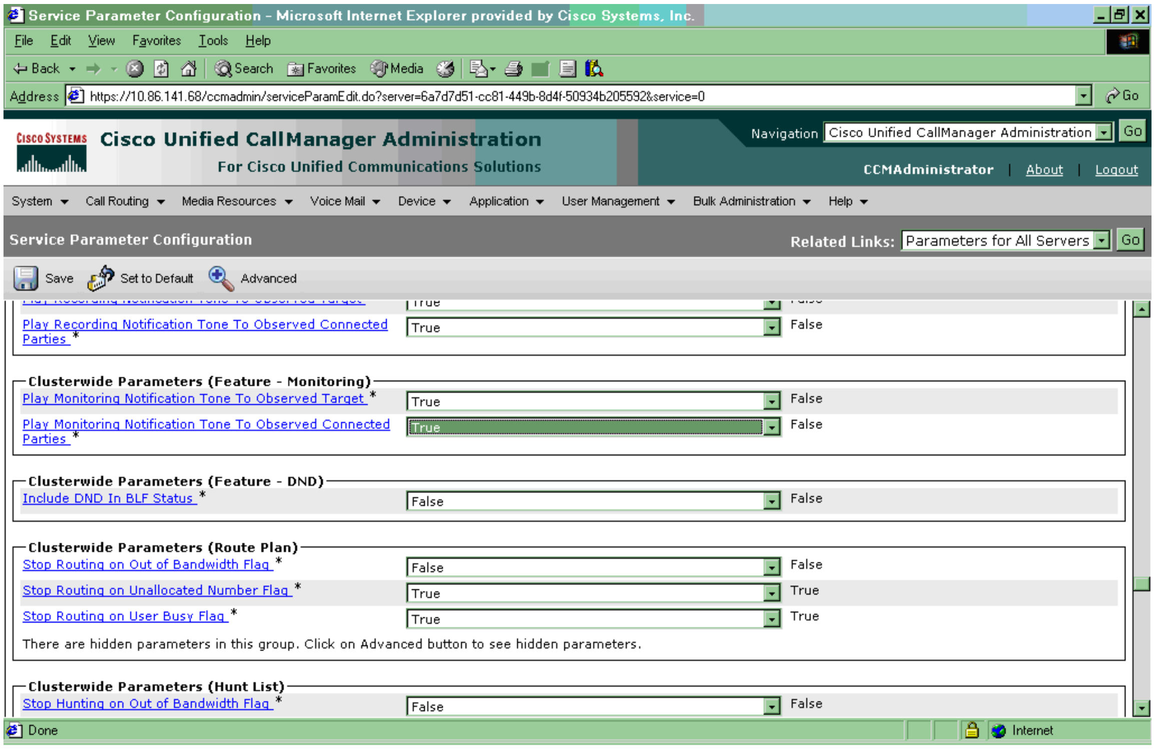
- Play Monitoring Notification Tone to Observed Connected Parties

  When set to true, this option plays the tone to the party to which the monitored party is talking (usually a customer).

A monitoring notification tone can be configured using the Service Parameter Configuration page in the Unified CM Administration Interface/ Select Server/ Select Unified CM (active) for Service.

The following figure illustrates both tones enabled.

Figure 6-5 Notification Tones


Service Parameter Configuration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.86.141.68/ccmadmin/serviceParamEdit.do?server=6a7d7d51-cc81-449b-8d4f-50934b205592&service=0
Go
Cisco Systems
Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CallManager Administration Go
CCMAdministrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Service Parameter Configuration
Related Links: Parameters for All Servers Go
Save Set to Default Advanced
Done Internet

Play Recording Notification Tone To Observed Connected Parties *	True	False

Clusterwide Parameters (Feature - Monitoring)

Play Monitoring Notification Tone To Observed Target *	True	False
Play Monitoring Notification Tone To Observed Connected Parties *	True	False

Clusterwide Parameters (Feature - DND)

Include DND In BLF Status *	False	False

Clusterwide Parameters (Route Plan)

Stop Routing on Out of Bandwidth Flag *	False	False
Stop Routing on Unallocated Number Flag *	True	True
Stop Routing on User Busy Flag *	True	True

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Clusterwide Parameters (Hunt List)

Stop Hunting on Out of Bandwidth Flag *	False	False

CTI OS

CTI OS Server can be configured to use either Unified CM-based silent monitor or CTI OS-based silent monitor. This is controlled by the following field in the CTI OS Server registry.

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\ CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\IPCCSilentMonitor\Name\Settings\CCMBasedSilentMonitor

This field is a DWORD. If this field is present and is set to 1, Unified CM-based silent monitor is used. If this field is set to 0, CTI OS-based silent monitor is used.

Run the CTI OS Server setup program to enable Unified CM-based silent monitor. If the server setup program is not run, the Unified C-BasedSilentMonitor field is not present causing CTI OS to use CTI OS-based silent monitor. The setup program can also be run to reconfigure CTI OS-based silent monitor.

Note This field is removed if CTI OS 7.2 is rolled back.

Restrictions

Phones

Unified CM-based silent monitor is only supported on 79x1 versions of Cisco IP Phones. This means that deployments without these phones or deployments with mobile agents must use CTI OS-based silent monitor.

Cisco Unified CM

Cisco Unified CM is required.

CTI OS Desktop Versions

Unified CM-based silent monitor can only be initiated by 7.2 IPCC Supervisor Desktops.

Release 7.2 Agent and Supervisor desktops can monitor and be monitored by 7.x desktops only if the desktops are using CTI OS-based silent monitor. Table 6-1 provides a matrix that shows which versions of CTI OS components can successfully silent monitor each other.

Table 6-1 CTI OS Desktop Version Matrix

Supported	Silent Monitor Type	CTI OS Server	CTI OS Agent Desktop	CTI OS Supervisor Desktop
Yes	CCM	7.2	7.2	7.2
No	CCM	7.2	7.1 and earlier	7.1 and earlier
No	CCM	7.2	7.2	7.1 and earlier
Yes	CCM	7.2	7.1 and earlier	7.2
Yes	CTI OS	7.2	7.2	7.2
Yes	CTI OS	7.2	7.1 and earlier	7.1 and earlier
Yes	CTI OS	7.2	7.2	7.1 and earlier
Yes	CTI OS	7.2	7.1 and earlier	7.2

Recording Applications

Recording applications are able to record agent conversations. Recording applications do not interfere with silent monitoring.

Transfer and Conferencing of Monitored Calls

Supervisors cannot transfer or conference silent monitor calls because these functions are not supported.

CHAPTER 7

CTI OS Security

This chapter provides information about configuring the CTI OS Security Certificate and the Security Compatibility. It contains the following sections:

Configuring CTI OS Security Certificate

The CTI OS Security Certificate comprises the following:

- CTI OS Security Setup programs.
- Signing CTI Toolkit Desktop Client Certificate Request with Self-Signed Certificate Authority (CA).
- Signing CTI OS Server Certificate Request with Self-Signed CA.
- Signing CTI Toolkit Desktop Client Certificate Request with Third-Party CA.
- Signing CTI OS Server Certificate Request with Third-Party CA.

Each of these entities is detailed in this section.

Note Both Certificate Revocation List (CRL) and certificate chain are not supported in CTI OS Security.

CTI OS Security Setup Programs

In order to configure the CTI OS, three setup programs are implemented. These setup programs are part of the Win32 CTI OS toolkit installation, and are located in the <*drive*>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security\Utilities directory.

1. The first setup program, **CreateSelfSignedCASetupPackage.exe**, creates a self-signed certificate authority (CA). This must be run once if the customer wants to use a self-signed CA instead of third party and the output of **CreateSelfSignedCASetupPackage.exe** must be saved in a secure place. This program creates CA-related files. One file, **CtiosRoot.pem,** contains the private CA information. This file must be kept in a safe place. Another file, **CtiosRootCert.pem,** contains public CA information. This setup program asks the user to enter a password for the CA (between 8 and 30 characters), which are used when signing CTI OS certificate requests.

2. The second setup program, **SecuritySetupPackage.exe,** is used to generate certificate requests for both CTI Toolkit Desktop Client and CTI OS Server. If the certificate request is for the CTI OS Server, then it generates **CtiosServerKey.pem**, and **CtiosServerReq.pem**. These files are used when signing server certificates. If the certificate request is for the CTI Toolkit Desktop Client, then it generates **CtiosClientkey.pem**, and **CtiosClientreq.pem**. These files are used when signing client certificates.
3. The third setup program, **SignCertificateSetupPackage.ex**e. is used to sign both CTI Toolkit Desktop Client and CTI OS Server certificates. This program is used only when the customer decides to sign their CTI Toolkit Desktop Client and CTI OS server certificates with self signed CA. This program must reside in the same directory as the **CtiosRootCert.pem** and **CtiosRoot.pem**. If the certificate that is going to be signed is for the client, it generates **CtiosClient.pem** file. If the certificate that is going to be signed is for the server, it generates **CtiosServer.pem** file. This program asks the user to enter the following information:
   a. Ctios Certificate Authority Password. This password is the one used to create a self-signed CA.
   b. Select either CTI Toolkit Desktop Client Certificate Request or CTI OS Server Certificate Request.

Signing CTI Toolkit Desktop Client Certificate Request with Self-Signed CA

Follow these steps to sign a CTI Toolkit Desktop Client certificate request:

Step 1 If the self-signed CA does not exist, then run **CreateSelfSignedCASetupPackage.exe** and store all the files that were created by the **CreateSelfSignedCASetupPackage.exe** program in a safe place.

Step 2 Copy **CtiosClientkey.pem**, and **CtiosClientreq.pem** files from the CTI Toolkit Desktop Client machine to the machine where **CtiosRoot.pem** and **CtiosRootCert.pem** reside. Both **CtiosClientkey.pem** and **CtiosClientreq.pem** files must be copied to the same directory as **CtiosRoot.pem** and **CtiosRootCert.pem**.

Step 3 Run **SignCertificateSetupPackage.exe** from the same directory where **CtiosClientkey.pem**, **CtiosClientreq.pem**, **CtiosRoot.pem** and **CtiosRootCert.pem** reside, select CTIOS Client Certificate Request, and enter the “Ctios Certificate Authority password.” This step generates **CtiosClient.pem** file if it is successful; otherwise it displays an error message.

Step 4 Copy both **CtiosClient.pem** and **CtiosRootCert.pem** back to the machine where CTI Toolkit Desktop Client is installed and save them in the <*drive*>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security directory.

Step 5 Delete **CtiosClientkey.pem** from the machine where CTI Toolkit Desktop Client is installed.

Step 6 Delete **CtiosClientkey.pem**, **CtiosClientreq.pem**, and **CtiosClient.pem** from the machine where **SignCertificateSetupPackage.exe** ran.

Signing CTI OS Server Certificate Request with Self-Signed CA

Follow these steps to sign a CTI OS Server certificate request:

Step 1 If the self-signed CA does not exist, then run **CreateSelfSignedCASetupPackage.exe** and store all the files that were created by the **CreateSelfSignedCASetupPackage.exe** program in a safe place.

Step 2 Copy **CtiosServerKey.pem**, and **CtiosServerReq.pem** files from the CTI OS Server machine to the machine where **CtiosRoot.pem** and **CtiosRootCert.pem** reside. Both **CtiosServerKey.pem** and **CtiosServerReq.pem** files must be copied to the same directory as **CtiosRoot.pem** and **CtiosRootCert.pem** (<*drive*>:\icm\<*Instance name*>\CTIOS1\Security).

Step 3 Run **SignCertificateSetupPackage.exe** from the same directory where **CtiosServerKey.pem**, **CtiosServerReq.pem**, **CtiosRoot.pem** and **CtiosRootCert.pem** reside, select CTIOS Server Certificate Request, and enter the "Ctios Certificate Authority password." This step generates **CtiosServer.pem** file if it is successful; otherwise it displays an error message.

Step 4 Copy both **CtiosServer.pem** and **CtiosRootCert.pem** back to the machine where CTI OS Server resides and save them in the <*drive*>:\icm\<*Instance name*>\CTIOS1\Security directory.

Step 5 Delete **CtiosServerkey.pem** from the machine where CTI OS Server is installed.

Step 6 Delete **CtiosServerKey.pem**, **CtiosServerReq.pem**, and **CtiosServer.pem** from the machine where **SignCertificateSetupPackage.exe** ran.

Step 7 If CTIOS Server has peer server, then:

a. Copy **CtiosClientkey.pem** and **CtiosClientreq.pem** files from the CTI OS Server machine to the machine where **CtiosRoot.pem** and **CtiosRootCert.pem** reside. Both **CtiosClientkey.pem** and **CtiosClientreq.pem** files must be copied to the same directory as **CtiosRoot.pem** and **CtiosRootCert.pem**.

b. Run **SignCertificateSetupPackage.exe** from the same directory where **CtiosClientkey.pem**, **CtiosClientreq.pem**, **CtiosRoot.pem** and **CtiosRootCert.pem** reside, select CTI Toolkit Desktop Client Certificate Request, and enter the "Ctios Certificate Authority password." This step generates **CtiosClient.pem** file if it is successful; otherwise it displays an error message.

c. Copy **CtiosClient**.**pem** to the machine where CTI OS Server resides and save it in <*drive*>:\icm\<*Instance name*>\CTIOS1\Security directory.

d. Delete **CtiosClientkey**.**pem** from the machine where CTI OS Server is installed.

e. Delete **CtiosClientkey**.**pem**, **CtiosClientreq**.**pem**, and **CtiosClient**.**pem** from the machine where **SignCertificateSetupPackage**.**exe** ran.

Signing CTI Toolkit Desktop Client Certificate Request with Third-Party CA

Follow these steps to sign a CTI Toolkit Desktop Client certificate request:

Step 1 Copy **CtiosClientreq.pem** file from the CTI Toolkit Desktop Client machine to the machine where the third-party CA resides.

Step 2 Signing CTI Toolkit Desktop Client certificate request (CtiosClientreq.pem) with third-party CA generates a CTI Toolkit Desktop Client certificate. Rename it **CtiosClientCert**.**pem**.

Step 3 The third-party CA has its certificate public information in a file. Rename this file **CtiosRootCert**.**pem**.

Step 4 Copy both **CtiosClientCert.pem** and **CtiosRootCert.pem** to the machine where CTI Toolkit Desktop Client resides and save them in the <drive>:\Program Files\Cisco Systems\CTIOS Client\Security directory.

Step 5 On the CTI Toolkit Desktop Client machine, copy the data in **CtiosClientCert**.**pem** and the data in **CtiosClientkey**.**pem** files into one file called CtiosClient.pem. The order is very important, so **CtiosClient**.**pem** must contain **CtiosClientCert**.**pem** data first and then **CtiosClientkey**.**pem** data second.

Step 6 Delete **CtiosClientCert**.**pem** and **CtiosClientkey**.**pem** from the CTI Toolkit Desktop Client machine.

Signing CTI OS Server Certificate Request with Third-Party CA

Follow these steps to sign a CTI OS Server certificate request:

Step 1 Copy **CtiosServerReq.pem** file from the CTI OS Server machine to the machine where the third-party CA resides.

Step 2 Signing CTI OS Server certificate request (CtiosServerReq.pem) with third-party CA generates a CTI OS Server certificate. Rename it **CtiosServerCert**.**pem**.

Step 3 The third-party CA has its certificate public information in a file. Rename this file **CtiosRootCert.pem**.

Step 4 Copy both **CtiosServerCert.pem** and **CtiosRootCert.pem** to the machine where CTI OS server resides and save them in the <*drive*>:\icm\<*Instance name*>\CTIOS1\Security directory.

Step 5 On the CTI OS Server machine, copy the data in **CtiosServerCert.pem** and the data in **CtiosServerkey.pem** files into one file called **CtiosServer.pem**. The order is very important, so **CtiosServer.pem** must contain **CtiosServerCert**.**pem** data first and then **CtiosServerkey**.**pem** data second.

Step 6 Delete **CtiosServerCert**.**pem** and **CtiosServerkey**.**pem** from the CTI OS Server machine.

Step 7 If CTIOS Server has peer server, then:

a. Copy **CtiosClientreq**.**pem** file from the CTI OS Server machine to the machine where the third party CA resides.

b. Signing CTI Toolkit Desktop Client certificate request (CtiosClientreq.pem) with third party CA generates a CTI Toolkit Desktop Client certificate. Rename it **CtiosClientCert.pem**.

c. Copy **CtiosClientCert.pem** file to the machine where CTI OS Server resides and save it in the <*drive*>:\icm\<*Instance name*>\CTIOS1\Security directory.

d. On the CTI OS Server machine, copy the data in **CtiosClientCert.pem**, and the data in **CtiosClientkey.pem** files into one file called **CtiosClient.pem**. *You must copy the files in this order*, so that **CtiosClient.pem** contain **CtiosClientCert.pem** data first and then **CtiosClientkey.pem** data second.

e. Delete **CtiosClientCert**.**pem** and **CtiosClientkey**.**pem** from the CTI OS Server machine.

CTI OS Security Passwords

CTI OS Security introduces five types of passwords:

1. CTI OS Client certificate password: The administrator or installer enters this password when installing CTI OS Client security. This password is used for the CTI OS Client certificate request private key and it can be anything and the administrator or installer need not remember it.

2. CTI OS Server certificate password: The administrator or installer enters this password when installing CTI OS Server security. This password is used for the CTI OS Server certificate request private key and it can be anything and the administrator or installer need not remember it.
3. CTI OS Peer certificate password: The administrator or installer enters this password when installing CTI OS Server security. This password is used for the CTI OS Peer Server certificate request private key and it can be anything and the administrator or installer need not remember it.
4. Monitor Mode password: The administrator or installer enters this password when installing CTI OS Server security. This password is used by the agents when connecting to secure CTI OS Server using CTI OS monitor mode applications such as AllAgents and AllCalls. This password must be the same on both CTI OS Peer Servers and the administrator or installer and whoever is using the CTI OS monitor mode applications must remember it.
5. Certificate Authority (CA) password: The administrator or installer enters this password when creating self-signed CA. The password can be anything and the administrator or installer must remember it because they will use it every time that this CA signs a certificate request.

CTI OS Security Registry Keys

The registry keys located at [HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems, Inc.\CTIOS\<*CTIOS_Instancename*>\CTIOS1\Server\Security] define the settings for CTI OS Server Security.

Table 7-1 lists the registry values for these keys.

Table 7-1 Registry Values for CTI OS Server

Registry Value Name	Value Type	Description	Default
AuthenticationEnabled	**DWORD Value**	Refer to the Authentication Mechanism section of this document.	**1**
CAType	**DWORD Value**	Is created at install time. A value of 1 means the chosen CA type is self signed, and a value of 2 means the chosen CA type is third party.	**1**

Table 7-1 Registry Values for CTI OS Server

Registry Value Name	Value Type	Description	Default
NumBytesRenegotiation	**DWORD Value**	Is used for session renegotiation, which means requesting a handshake to be performed during an already established connection. This causes CTI OS Client credentials to be reevaluated and a new session to be created. It is important to replace the session key periodically for long-lasting SSL connections, because doing so makes the connection between CTI OS Server and CTI OS Client more secure. Renegotiation happens after the CTI OS Server sends 10000000 bytes to the CTI OS Client. The minimum and the default value are 10000000.	**10000000**
SecurityEnabled	**DWORD Value**	Is created at install time. A value of 1 means CTI OS Security is enabled, and a value of 0 means CTI OS Security is disabled.	**0**

Table 7-1 Registry Values for CTI OS Server

Registry Value Name	Value Type	Description	Default
MonitorModeDisableThreshold	**DWORD Value**	Controls the number of consecutive failed attempts to access monitor mode functionality before monitor mode is disabled. **Note** For additional information, refer to the section "Monitor Mode Security."	**3 (default)**
MonitorModeDisableDuration	**DWORD Value**	Controls the length of time to disable monitor mode functionality after the configured number of consecutive failed attempts to access monitor mode functionality have occurred. **Note** For additional information, refer to the section "Monitor Mode Security."	**15 minutes (default)**

The registry keys located at [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTI OS Client\CtiOs] define the settings for CTI OS Client Security. Table 7-2 lists the registry values for these keys.

Table 7-2 Registry Values for CTI OS Client

Registry Value Name	Value Type	Description	Default
CAType	**DWORD Value**	Is created at install time. A value of 1 means the chosen CA type is self signed, and a value of 2 means the chosen CA type is third party.	**1**
HandShakeTime	**DWORD Value**	Is created at install time. This key defines how long the CTI OS client waits during the SSL/TLS handshake phase.	**5**

Monitor Mode Security

When CTI OS Server has security enabled, the server guards itself against unlawful attempts to gain access to monitor mode functionality. It does this by tracking the number of failed attempts to access monitor mode functionality. After the configured number of consecutive failed attempts to access monitor mode functionality have occurred (3 by default), CTI OS Server disables monitor mode functionality. When this happens, all attempts to access monitor mode functionality fail. This occurs until the configured period of time after the last failed attempt to access monitor mode functionality has passed. This time period is 15 minutes by default.

The *MonitorModeDisableThreshold* and the *MonitorModeDisableDuration* registry settings have been added to the *HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS<instance>\<ServerName>\Server\Security* to allow you to modify the defaults.

- *MonitorModeDisableThreshold*—This registry field is a DWORD. It controls the number of consecutive failed attempts to access monitor mode functionality before monitor mode is disabled.
- *MonitorModeDisableDuration*—This registry field is a DWORD. It controls the length of time to disable monitor mode functionality after the configured number of consecutive failed attempts to access monitor mode functionality have occurred.

Security Compatibility

Passing data over the network in a secure way is vital to both Cisco and the customer. CTI OS 6.0 and earlier releases do not support any type of security. In CTI OS 7.0, two features were implemented to deal with security:

- Wire Level Encryption - To help secure all the traffic between CTI OS Server and CTI OS Client using Transport Layer Security (TLS). This protocol provides encryption and certification at the transport layer (TCP).
- Authentication mechanism - For IPCC and System IPCC only, makes sure that an agent logs in successfully only if the agent supplies the correct password.

Note The information in this guide does not pertain to specifics of Cisco Unified System Contact Center Enterprise (Unified SCCE) deployments. The Cisco IPCC Enterprise Web Administration Tool is used for administering Unified SCCE. (Unified SCCE Release 7.5 is supported in the 8.0(1) solution.)

Wire Level Encryption

Wire Level Encryption provides an encryption mechanism between CTI OS Server 7.0 and CTI OS Client 7.0 only. By default, Wire Level Encryption is turned OFF. If the value of “SecurityEnabled” registry key is 0, then security is off. If the value of “SecurityEnabled” registry key is 1, then security is on. This key exists under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```

If the security is turned on in CTI OS Server 7.0, then the backward compatibility between earlier versions of CTI OS client with this version of CTI OS server is not maintained. Also if security is turned on in CTI OS Server, then CTI OS 7.0 Clients using .NET CIL, Java CIL, or Siebel Driver cannot connect to the CTI OS Server. If security is on in one CTI OS Server and this server has peers, then security must be turned on in the peers as well. Table 7-3 contains the list of CTI OS toolkits.

Table 7-3 Wire Level Encryption: List of CTI OS Toolkits

	C++ CIL Toolkit	COM CIL Toolkit	Java CIL Toolkit	.NET CIL Toolkit
Support Wire Level Encryption	Yes	Yes	No	No

Table 7-4 contains the compatibility information between CTI OS Server 8.0 and CTI OS Clients 8.0.

Table 7-4 Wire Level Encryption: List of CTI OS Toolkits

	CTI OS Client 8.0 using C++ CIL toolkit	CTI OS Client 8.0 using COM CIL toolkit	CTI OS Client 8.0 using Java CIL toolkit	CTI OS Client 8.0 using .NET CIL toolkit
CTI OS Server 8.0 (Security ON)	Yes	Yes	No	No
CTI OS Server 8.0 (Security OFF)	Yes	Yes	Yes	Yes

Table 7-5 contains the compatibility information between CTI OS Server 7.0 and CTI OS Clients 6.0 and earlier versions.

Table 7-5 Wire Level Encryption: CTI OS Server 7.0 with CTI OS Client 6.0 and earlier versions

	CTI OS Client 6.0 and earlier versions using C++ CIL toolkit	CTI OS Client 6.0 and earlier versions using COM CIL toolkit	CTI OS Client 6.0 using Java CIL toolkit
CTI OS Server 7.0 (Security ON)	No	No	No
CTI OS Server 7.0 (Security OFF)	Yes	Yes	Yes

Authentication Mechanism

The authentication mechanism is for IPCC only. It is on by default. If the value of "AuthenticationEnabled" registry key is 0, then authentication is off. If the value of "AuthenticationEnabled" registry key is 1, then authentication is on. This key exists under

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```

For all peripherals other than IPCC, System IPCC or HIPCC this registry key is not used.

Note The CTI OS Client (CIL) blocks events if authentication is turned on and the agent is not logged in but the agent mode is set. This can be circumvented by turning off Authentication or by actually logging in the agent. This only occurs in agent mode, not in monitor mode.

Table 7-6 contains compatibility information between CTI OS Server 8.0 and CTI OS Clients 8.0.

Table 7-6 Authentication Mechanism: CTI OS Server 8.0 with CTI OS Client 8.0

	CTI OS Client 8.0 using C++ CIL toolkit	CTI OS Client 8.0 using COM CIL toolkit	CTI OS Client 8.0 using Java CIL toolkit	CTI OS Client 8.0 using .NET CIL toolkit
CTI OS Server 8.0 (Authentication Enabled)	Yes	Yes	Yes	Yes
CTI OS Server 8.0 (Authentication Disabled)	No	No	No	No

Table 7-7 contains compatibility information between CTI OS Server 7.0 and CTI OS Clients 6.0 and earlier versions.

Table 7-7 Authentication Mechanism: CTI OS Server 7.0 with CTI OS Client 6.0 and earlier versions

	CTI OS Client 6.0 and earlier versions using C++ CIL toolkit	CTI OS Client 6.0 and earlier versions using COM CIL toolkit	CTI OS Client 6.0 using Java CIL toolkit
CTI OS Server 7.0 (Authentication Enabled)	Yes (*, **)	Yes (*, **)	Yes (*, **)
CTI OS Server 7.0 (Authentication Disabled)	Yes	Yes	Yes

* CTI OS Agent Desktop, IPCC Supervisor Desktop, and BA Phone always display the following CTI Warning: “Agent with ID <ID> is already logged in to instrument <INSTRUMENT>” even though the agent was not already logged in. This problem can be solved by setting the “WarnIfAlreadyLoggedIn” registry key to 0. This key exists under

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, 
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\
ConnectionProfiles\Name\<ConnectionProfileName>
```

** Assume the following scenario:

- If agent A is already logged in to CTIOS Server using either CTI OS Agent Desktop, IPCC Supervisor Desktop, or BA Phone

- Agent B is connected to CTIOS Server using either CTI OS Agent Desktop, IPCC Supervisor Desktop, or BA Phone
- Agnet Bis trying to log in using agent A’s ID with invalid password
- Agent B receives control failure but the desktop has all 3 Login, Logout ,and Ready buttons enabled(which agent B can use to manipulate agent A’s desktop).
- Agent B pushes the Ready button, then button enablement becomes fine. Also, agent B’s desktop always displays a CTI Warning: “Agent with ID <ID> is already logged in to instrument <INSTRUMENT>” even though the agent was not already logged in.

This problem can be solved by setting the “WarnIfAlreadyLoggedIn” registry key to 0. This key exists under

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\
ConnectionProfiles\Name\<ConnectionProfileName>
```

The desktop also displays a CTI Warning” “The request specified an invalid agent password.”

Note When one CTI OS Server is down, 6.0 and earlier clients may fail to log in if the client attempts to connect to the CTI OS Server that is down first. If this happens, the agent should attempt to log in again. If the desktop connects to the CTI OS Server that is up, the agent is logged in as long as the correct credentials were entered.

CHAPTER 8

CTI OS Configuration

CTI OS Configuration is handled through the Windows Registry Editor. Using the Editor, you can add of change registry values. This chapter provides instructions for working with the Windows Registry Editor and discusses the required values for the CTI OS registry keys.

This chapter includes the following sections:

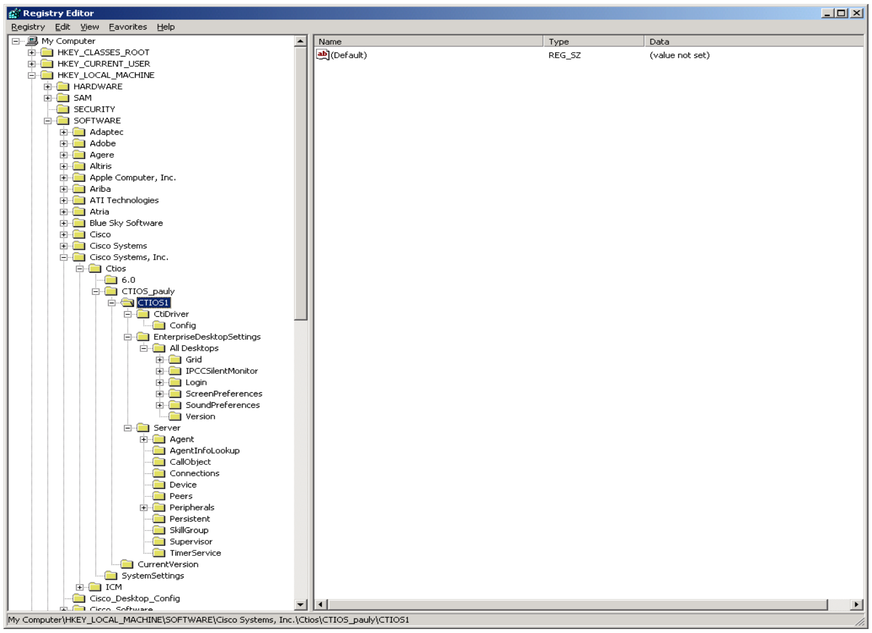
This chapter does *not* discuss configuration of CTI OS Client registry values that the CTI OS Client downloads from CTI OS Server upon client login. For a discussion of CTI OS Client logging and tracing registry values, see Appendix B of the *CTI OS Developer's Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

Note Except where otherwise indicated, the CTI OS Registry keys discussed in this chapter are local and start at the [HKEY_LOCAL_MACHINE\SOFTWARE\ Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>] path.

Using the Windows Registry Editor

CTI OS Server installation initializes a configuration that is stored in the Windows System Registry database. This configuration is accessible and editable through the Windows Registry Editor (regedit.exe). Figure 8-1 shows the Registry Editor main window.

Figure 8-1 Windows Registry Editor Main Window



```
My Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
      Adaptec
      Adobe
      Agere
      Altiris
      Apple Computer, Inc.
      Ariba
      ATI Technologies
      Atria
      Blue Sky Software
      Cisco
      Cisco Systems
      Cisco Systems, Inc.
        Ctios
          6.0
          CTIOS_pauly
            CTIOS1
              CtiDriver
                Config
              EnterpriseDesktopSettings
                All Desktops
                  Grid
                  IPCCSilentMonitor
                  Login
                  ScreenPreferences
                  SoundPreferences
                  Version
              Server
                Agent
                AgentInfoLookup
                CallObject
                Connections
                Device
                Peers
                Peripherals
                Persistent
                SkillGroup
                Supervisor
                TimerService
            CurrentVersion
          SystemSettings
        ICM
      Cisco_Desktop_Config
      Cisco_Software
```

Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_pauly\CTIOS1

To add a key or registry value under an existing key, perform the following steps:

Step 1 Highlight the existing key in the left panel.

Step 2 Position the cursor in the right panel and click. A popup menu appears.

Step 3 From the popup menu, select **Key**, **String Value**, **Binary Value**, or **DWORD** value. If you select **Key**, a placeholder for the key you want to add appears highlighted in the left panel. For other items, a placeholder for the item you want to add appears highlighted in the right panel.

Step 4 Right-click the highlighted item. A popup menu appears.

- To name the item, select **Rename** from the popup menu; then type the new name for the item.
- To set the value data for **String**, **Binary**, and **DWORD** values, select **Modify**. A dialog box appears. Enter the value data following the **Value Data** prompt.

To edit an existing key or registry value, highlight the key or value and right-click on it. Select Modify, Delete, or Rename from the popup menu and proceed.

Note After you make a change to the registry, you must restart the CTI OS processes before the new setting can take effect.

Note About Registry Directories in Previous CTI OS Releases

In CTI OS releases prior to 7.0, the [HKEY_LOCAL_MACHINE\SOFTWARE\ Cisco Systems, Inc. directory was named [HKEY_LOCAL_MACHINE\ SOFTWARE\ Cisco Systems. If you upgrade from a previous release of CTI OS Software to Release 7.0(0), the installation procedure automatically copies the contents of the old Cisco Systems directory to the new Cisco Systems Inc. directory and deletes the old directory.

Configuring the Silent Monitor Type for CTI OS

CTI OS can be configured to use either Unified CM-based silent monitor or CTI OS-based silent monitor. This is accomplished by setting the following field in the CTI OS registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\ CTIOS\<CTIOS
InstanceName>\<CTIOSServerName> \EnterpriseDesktopSettings\All Desktops\UCCESilentMonitor
\Name\Settings\CCMBasedSilentMonitor
```

This field is a DWORD and if present and set to “1”, Unified CM-based silent monitor is used.

CTI OS-based silent monitor is used if this field is not present or if it is present and set to “0”.

Note This field is not added to the registry by the patch. You must run the CTI OS setup program to enable Unified CM-based silent monitor.

The setup program can also be run to reconfigure CTI OS-based silent monitor.

If the server setup program is not run, the CCMBasedSilentMonitor field is not present. As a result, CTI OS-based silent monitor is used.

This field is removed if version 7.2 of CTI OS is rolled back.

Virtual Desktop Infrastructure (VDI)

Virtual Desktop Infrastructure (VDI) is a server-centric computing model. It is designed to help you to host and centrally manage desktop virtual machines in the data center, while providing a full PC desktop experience.

The VMware View portfolio of products (VDI) lets IT run virtual desktops in the data center while giving you a single view of all your applications and data in a familiar, personalized environment on any device at any location. VDI provides greater flexibility, reliability, efficiency and security managing desktops and applications from the datacenter.

Installing CTI OS Desktop on VDI Agent Desktops

CTI OS desktops on VDI environment is supported starting from CTI OS 7.5(6).

Prerequisites

Complete functional VDI deployment as per the VDI requirements. For more information see http://www.vmware.com/products/view/.

How to Install CTI OS Desktop on VDIAgent

Step 1 On any VDI agent desktop, run the CTI OS client installer and configure the desktop. Refer to the *CTI OS System Manager's Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted 8.0(1)* for more information on the deployment, limitations, and supported features of CTI OS desktops on VDI.

Step 2 When the installation is complete, launch the CTI OS desktop and verify basic functionality by logging in an agent, changing agent states, or making calls.

Step 3 After the testing is complete, follow the same steps on the other VDI agent desktops.

Notes and Restrictions

Silent Monitoring

CTI OS-based silent monitoring is not supported due to physical limitations. For CTI OS-based silent monitoring, the agent machine must be connected to the network via the phone hard-set. This cannot be achieved with a Virtual Machine, such as when using VDI.

ThinApp

ThinApp is not supported with the CTI OS 7.5(6) release. For more information on ThinApp see http://www.vmware.com/products/thinapp/.

CTI Driver

The CTI Driver key includes registry settings required for CTI Server connection. The CTI Driver key contains one key, the Config key. Table 8-1 describes the CtiDriver/Config key registry values.

Table 8-1 Registry values for [CtiDriver\Config]

Registry Value Name	Value Type	Description	Default
ClientID	String Value	The identifier of the CTI Client. This is displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.	CTIOSServer
ClientPassword	String Value	The password of the CTI Client. This is displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.	CTIOSServer

Table 8-1 Registry values for [CtiDriver\Config] (continued)

Registry Value Name	Value Type	Description	Default
ClientSignature	String Value	The signature of the CTI Client. This is displayed in the CTI Server log file to help identify which session the CTI OS Server is connected on.	CTIOSServer
SideAHost	String Value	The CTI Server (sideA) IP address or hostname to which the CTI OS Server connects.	Host specified during CTI Server installation.
SideAPort	DWORD Value	The CTI Server (sideA) IP port to which the CTI OS Server connects.	Port specified during CTI Server installation.
SideBHost	String Value	The CTI Server (sideB) IP address or hostname to which the CTI OS Server connects.	Host specified during CTI Server installation.
SideBPort	DWORD Value	The CTI Server (sideB) IP port to which the CTI OS Server connects.	Port specified during CTI Server installation.
Heartbeat Interval	DWORD Value	The interval (in seconds) at which HEARTBEAT_REQ messages are sent to the CTI Server.	5
ServicesMask	DWORD Value	The services requested from the CTI Server and provides the functionality that the MinimizeAgentStateEvents registry value used to provide. To suppress multiple state events add the bit: CTI_SERVICE_IGNORE_DUPLICATE_AGENT_STATES = 0x00100000 to the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_bbld1\CTIOS1\CtiDriver\Config Example Change: "ServicesMask"=dword:000c0016 to: "ServicesMask"=dword:001c0016	0x00000296 (52) (default)
CallMsgMask	DWORD Value	The unsolicited call events requested from the CTI Server.	0x00ffffff (16777215)
AgentStateMask	DWORD Value	The agent states requested from the CTI Server.	0x000003ff (1023)

Table 8-1 Registry values for [CtiDriver\Config] (continued)

Registry Value Name	Value Type	Description	Default
ProtocolVersion	DWORD Value	The highest protocol version to use when connecting to the CTI Server. The highest common denominator is used when establishing the CTI Session. **Note** This field is set to 13 (0x0D) if the CTI OS Server Setup program is run after upgrading to CTI OS 7.2(1). Protocol 13 is necessary to use Unified CM silent monitor functionality.	9
IdleTimeout	DWORD Value	The session inactivity timeout (in seconds). The CTI Server disconnects clients after this time threshold has elapsed without other socket messages.	0x7fffffff (2147483647)
MemoryPoolSize	DWORD Value	Size of the memory pool, in bytes.	0x00000064 (100)

EMS Tracing Values

The registry keys located at [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<customer_instance_name>\<CTIOSComponent Name>\EMS\CurrentVersion\Library\Processes\ ctios] define the settings for Event Management System (EMS) tracing. Table 8-2 lists the registry values for these keys.

Table 8-2 Registry values for EMS Tracing

Registry Value Name	Value Type	Description	Default
EMSDisplayToScreen	DWORD Value	If set to 1, EMS routines attempt to write formatted messages to standard output.	0
EMSAllLogFilesMax	DWORD Value	The maximum total number of bytes that the EMS library writes to all local log files.	5000000
EMSBreakOnExit	DWORD Value	If set to 1, EMS exit routines invoke the Debugger.	0
EMSBreakOnInit	DWORD Value	If set to 1, EMS initialization routines invoke the Debugger.	0
EMSDebugBreak	DWORD Value	If set to 1, EMS failure routines invoke the Debugger before exiting the process.	1
EMSLogFileCountMax	DWORD Value	The maximum number of log files that the EMS library writes.	10

Table 8-2 Registry values for EMS Tracing

EMSLogFileLocation	String Value	The directory where the EMS library creates local log files.	Default directory specified at installation.
EMSLogFileMax	DWORD Value	The maximum number of bytes that the EMS library writes to a single local log file.	500000
EMSNTEventLogLevel	DWORD Value	The minimum severity event that EMS logs in the Application Event Log.	0Xffffffff
EMSTraceMask	DWORD Value	A bitmask that specifies the levels of EMS tracing that are enabled.	3
EMSUserData	DWORD Value	Placeholder for arbitrary binary user data.	
EMSForwardLevel	DWORD Value	The minimum severity event that EMS forwards to the Unified ICM central controller.	0
ConsoleTraceMask	DWORD Value	A bitmask that specifies the level of console tracing that are enabled. The ConsoleTraceMask is not added to the registry at install time.	0x3

Server

The Server registry key contains CTI OS Server related configuration information. It contains the following subkeys:

- Agent
- CallObject
- Connections
- Device
- Peers
- Peripherals
- SkillGroup
- SilentMonitor
- Supervisor
- ThreadPoolSize
- TimerService

Agent

The Agent key contains agent related configuration information. Table 8-3 lists the registry values for the Agent key.

Table 8-3 Registry values for [Server\Agent]

Registry Value Name	Value Type	Description	Default
AgentChatLevel	string	Defines the call center personnel with whom an agent is permitted to chat. This must be set to one of the values listed in Table 8-4.	TeamSupervisors
EnableWrapupDialog	DWORD Value	When enabled (1), a Wrapup dialog box pops up at the end of the call. A value of 0 disables this feature.	1
forceLogoutOnSessionClose	DWORD Value	Set to "1" in order to turn on the feature to force logout an agent when their session is ended by the agent closing the window without properly logging out. **Note** This value must be manually entered into the registry. If the value has not been entered into the registry, the effect is the same as having it set to its default (0).	0

Table 8-3 Registry values for [Server\Agent] (continued)

Registry Value Name	Value Type	Description	Default
forceLogoutOnSessionCloseReason (Optional unless logout reason is required.)	DWORD Value	Indicates the reason code to be used by the CTI OS server when the agent is forced to log out. This need not be defined in the registry when the default value is sufficient. By setting this to a specific reason code you can easily determine when an Agent is logged out by the CTI OS server and when the Agent logs out normally. **Note** You must set this to a non-zero value if an idle reason code reason is required. Refer to "Unified ICM Agent Desk Settings" to determine if the idle reason code is required. **Note** This value must be manually entered into the registry.	0

Table 8-3 Registry values for [Server\Agent] (continued)

Registry Value Name	Value Type	Description	Default
forceNotReadyOnSessionCloseReason (Optional unless idle reason is required.)		Indicates the reason code to be used by the CTI OS server when the agent is forced to the Not Ready state before being forced to log out. This need not be defined in the registry when the default value is sufficient. By setting this to a specific reason code you can easily determine when an Agent is logged out by the CTI OS server and when the Agent logs out normally. **Note** You must set this to a non-zero value if an idle reason code reason is required. Refer to "Unified ICM Agent Desk Settings" to determine if the idle reason code is required. **Note** This value must be manually entered into the registry.	0
LogoutReasonRequired	DWORD Value	On all switches except IPCC, when enabled (1) a Logout Reason Code dialog box pops up when changing state to Logout. On all switches, a value of 0 disables this feature.	1 for Spectrum, 0 for all other switches
NotReadyReasonRequired	DWORD Value	On all switches except IPCC, when enabled (1) a Not Ready Reason Code dialog box pops up when changing state to NotReady. On all switches, a value of 0 disables this feature.	0

Table 8-3 Registry values for [Server\Agent] (continued)

Registry Value Name	Value Type	Description	Default
PollForAgentStatsAtEndCall	DWORD Value	Controls when agent statistics are sent from CTI OS Server to CTI OS clients. A value of 0 means that agent statistics are sent at a regular interval (specified in PollingIntervalSec). A value of 1 means that agent statistics are sent only when a call ends. **Note** Changing the value of PollForAgentStatsAtEndCall may degrade performance and is not recommended.	1
PollingIntervalSec	DWORD Value	The agent statistics polling interval, in seconds.	15
WrapupDataRequired	DWORD Value	When enabled (1), wrapup data is mandatory. When disabled (0), wrapup data is not required. Not applicable to IPCC agents.	0

Table 8-4 AgentChatLevel Values

Value	Meaning
Disabled	All agent chat disabled.
PrimarySupervisor	Agents can chat only with primary supervisor of their team.
TeamSupervisors	Agents can chat with the primary or secondary supervisor of their team.
Team	Agents can chat with anyone in team.
Unrestricted	Agents can chat with anyone on the same peripheral.

The Agent key also contains the following subkeys:

- ReasonCodes
- WrapupStrings

ReasonCodes

The ReasonCodes key is a site-specific key that defines the reason codes the CTI OS Agent Desktop uses. For each reason code, a string is mapped to an unsigned short value. The CTI OS Agent Desktop displays the string and sends the appropriate value to the CTI Server, which in turn passes the value along to the ACD.

The ReasonCodes key contains two subkeys:

- **Logout**. This key defines the reason codes that appear on the Select Reason: Logout screen when an agent logs out. Immediately following CTI OS Server installation, the Logout registry key contains four values that serve as placeholders for Logout reason codes (see Table 8-5).

Table 8-5 Initial Contents of [Server\Agent\ReasonCodes\Logout]

Registry Value Name	Value Type	Description
Insert logout reason code 1 here	DWORD Value	Placeholder for first Logout reason code.
Insert logout reason code 2 here	DWORD Value	Placeholder for second Logout reason code.
Insert logout reason code 3 here	DWORD Value	Placeholder for third Logout reason code.
Insert logout reason code 4 here	DWORD Value	Placeholder for fourth Logout reason code.

  To define the text that appears for each Logout reason code in the Select Reason dialog box, set the value data associated with the reason code to the text you want to appear for that reason code. You may also add additional reason code entries as needed.

- **NotReady**. This key defines the reason codes that appear in the Select Reason: NotReady dialog box when an agent goes to NotReady state. As with the Logout key, the NotReady key initially contains four placeholder DWORD values that you can edit to define the reason codes in the Select Reason: NotReady dialog box.

Note The maximum length permitted for a reason code is 42 characters.

WrapupStrings

The WrapupStrings key defines the predefined wrapup text strings that appear in the softphone Wrapup dialog box. The WrapupStrings key contains a subkey, Incoming, that defines the wrapup text for incoming calls. Immediately following CTI OS Server installation, the Incoming key contains the registry values listed in Table 8-6.

Table 8-6 Initial Contents of [Server\Agent\WrapupStrings\Incoming]

Registry Value Name	Value Type	Description
String0	String Value	Placeholder for first wrapup text string.
String1	String Value	Placeholder for second wrapup text string.
String2	String Value	Placeholder for third wrapup text string.
String3	String Value	Placeholder for fourth wrapup text string.

To define the text that appears for each wrapup text string in the WrapUp dialog box, set the value data associated with the reason code to the text you want to appear for that wrapup string. You may also add additional wrapup string entries as desired.

Note There are no CTI OS registry keys for defining text for outgoing wrapup strings. The Unified ICM does not save any wrapup data for outgoing calls, so you need not define outgoing wrapup strings. This is applicable to transfer and conference initiated calls also. (Both transfer and conference calls are treated as outgoing calls.)

CallObject

The CallObject key defines the values pertaining to call objects. Table 8-7 defines the CallObject key registry values.

Table 8-7 Registry values for [Server\CallObject]

Registry Value Name	Value Type	Description	Default
AgentPreCallEvent Timeout	DWORD Value	Length of time, in seconds, within which an AGENT_PRE_ CALL_EVENT must be followed by a BEGIN_CALL_ EVENT or the call object is deleted.	30
IPCCConference_ SupportsMultipleControllers	DWORD Value	When set to 1, allows all parties of a Conference to add new parties to the conference as supported by Unified CM. If running against an earlier version of Unified CM, this must be set to 0. If this is not set to 0 when running against an earlier version of Unified CM, and a non-controller Conference party tries to make a Consult Call for a Conference, the party receives a Control Failure.	1
MinimizeEventArgs	DWORD Value	When set to 1 (recommended setting), minimizes the amount of nonessential call object parameters sent to the client.	1
TrashCollectionInterval Sec	DWORD value	Controls how often (in seconds) the trash collector activates and removes any stale objects from memory. A value of 0 disables the trash collector.	7200

Connections

The Connections key defines the values for client connections to the CTI OS Server. Table 8-8 defines the Connections key registry values.

Table 8-8 Registry values for [Server\Connections]

Registry Value Name	Value Type	Description	Default
ClientPoolInitialSize	DWORD Value	The number of Client objects to pre-create. ⚠ **Caution** It is recommended that you leave this registry entry set to its default value.	1500
ClientPoolMinSize	DWORD Value	The minimum number of Client objects in the pool to trigger growing the pool. ⚠ **Caution** It is recommended that you leave this registry entry set to its default value.	50
ClientPoolIncrement	DWORD Value	The number of Client objects to create when the pool must be grown. ⚠ **Caution** It is recommended that you leave this registry entry set to its default value.	50
HeartbeatIntervalMs	DWORD Value	The number of milliseconds between heartbeats from the server to its clients.	60000
HeartbeatRetrys	DWORD Value	The number of missed heartbeats before a connection is closed for unresponsiveness.	5
ListenPort	DWORD Value	The TCP/IP port on which the CTI OS Server listens for incoming client connections.	Port specified during CTI OS Server setup.
MaxMonitorModeConnections	DWORD Value	This registry entry controls the number of monitor mode connections connected to a CTI OS Server. By default, this registry value does not exist in the registry so the default maximum number of monitor mode connections is two (2). CTI OS Server can detect when this registry value has been added, deleted, or updated without the need of recycling CTI OS server.	2

The heartbeating mechanism uses the HeartbeatIntervalMs and HeartbeatRetrys values together to determine when a connection is stale and must be closed. The interval serves as a timeout and the retries is the number of attempts that have timed out before closing the socket.

Example with an interval of 5 seconds and three retries:

- After 5 seconds Total time), if the server does not receive a response from the client, it sends a heartbeat request and increments the retry count to 1.
- After another 5 seconds, if the server does not receive a response from the client, it sends a heartbeat request and increments the retry count to 2.
- After another 5 seconds, if the server does not receive a response from the client, it sends a heartbeat request and increments the retry count to 3.
- After another 5 seconds, if the server does not receive a response from the client, the connection is reported failed and the socket is closed.

To disable heartbeating, set the HeartbeatIntervalMs value to 0.

A Retry value of 0 causes the connection to time out after the interval without sending any heartbeat.

Device

The Device registry key contains one value, SnapshotDelaySec. This is a reserved value that must not be changed.

Peers

The Peers registry key informs a CTI OS Server about other CTI OS servers. This allows CTI OS servers to make direct connections with one another for the purposes of routing internal messages. On startup, CTIOSServerNode reads this key and opens client connections to all peer servers.

Note You can define two CTI OS Servers as peer servers only if they are connected to the same CTI Server or CTI Server pair. You cannot define two CTI OS Servers as peer servers if they are connected to CTI Servers that reside on different PGs.

The Peers key contains the values listed in Table 8-9.

Table 8-9 Registry values for [Server\Peers]

Registry Value Name	Value Type	Description	Default
Heartbeat IntervalMs	DWORD Value	Number of milliseconds between heartbeats for client connection to peer servers.	5000
HeartbeatRetrys	DWORD Value	Number of retry attempts before a connection to a peer server is determined to be down.	3

In addition, there must be a subkey for each peer server to which the current server connects. The key name is the hostname or IP address of the peer server; for example, "HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\ Server\Peers\DallasCTIOS". Each such subkey must contain the registry value listed in Table 8-10.

Table 8-10 Registry values for [Server\Peers] Subkeys

Registry Value Name	Value Type	Description
Port	DWORD Value	The number of the TCP/IP port on which the peer server is listening for the client connection.

Peripherals

The Peripherals key stores the maps of valid PeripheralID and Peripheral Types. On CTI OS System startup, these mappings are read into a map which creates the appropriate peripheral-type objects on the server.

This information must correspond to the Unified UCCE database Peripheral table Peripheral.PeripheralID and Peripheral.ClientType. While the values in ClientType are not equal to the PeripheralTypes, there is a one-to-one relationship between ClientTypes and PeripheralTypes.

The symbol PERIPHERAL_LOGICAL_NAME can be any logical name that uniquely identifies a Peripheral, such as “Phoenix ACD 1.” This is equivalent to the Peripheral.EnterpriseName logical name in the Unified UCCE database. There must be one entry for each valid Peripheral at this site.

Table 8-11 lists the Peripherals key registry values.

Table 8-11 Registry values for [Server\Peripherals\PERIPHERAL_LOGICAL_NAME]

Registry Value Name	Value Type	Description
PeripheralID	DWORD Value	The PeripheralID configured in the Unified UCCE database for this Peripheral.
PeripheralType	DWORD Value	The PeripheralType corresponding to this PeripheralID.

Examples:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTIOS
InstanceName>\<CTIOSServerName>\Server\Peripherals\G3 ACD]
"PeripheralID"=dword:00001388
"PeripheralType"=dword:00000005

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTIOS
InstanceName>\<CTIOSServerName>\Server\Peripherals\Aspect ACD]
"PeripheralID"=dword:00001390
"PeripheralType"=dword:00000001
```

SkillGroup

The SkillGroup key defines skill group configuration values. Table 8-12 lists the SkillGroup key registry values.

Table 8-12 Registry values for [Server\SkillGroup]

Registry Value Name	Value Type	Description	Default
PollingInterval Sec	DWORD Value	The SkillGroup statistics polling interval, in seconds.	10

Supervisor

The Supervisor key contains supervisor related configuration information. Table 8-13 lists the registry values for the Supervisor key.

Table 8-13 Registry values for [Server\Supervisor]

Registry Value Name	Value Type	Description	Default
Supervisor ChatLevel	String Value	Defines the call center personnel with whom a supervisor is permitted to chat. This must be set to one of the values listed in Table 8-14.	Unrestricted

Table 8-14 SupervisorChatLevel Values

Value	Meaning
Disabled	All supervisor chat disabled.
Team	Supervisors can chat with anyone in their primary team.
Unrestricted	Supervisors can chat with anyone on the same peripheral.

ThreadPoolSize

ThreadPoolSize is the number of threads in the IO completion port pool.

The ThreadPoolSize registry value is found under the following registry key:

```
HKLM\Software\Cisco Systems.Inc.\ctios\CTIOS_<instancename>\CTIOS1\Server\ThreadPool
```

Table 8-15

Registry Value Name	Value Type	Description	Default
ThreadPoolSize	DWORD Value	If set to <= 0, then the number of threads in the pool are calculated using the following formula: number of CPU's +2. Maximum threads allowed are 32.	0 for all peripheral types except Avaya where the default value is 10.

Note Balancing threads against overall performance is not a trivial task. It is recommended that you not modify this value. If the ThreadPoolSize value is changed, follow up with overall performance monitoring to see whether CTI OS Server performance is affected.

TimerService

The TimerService key specifies configuration parameters for the CTI OS Server’s internal TimerService. Table 8-16 lists the registry values for the TimerService key.

Table 8-16 Registry values for [Server\TimerService]

Registry Value Name	Value Type	Description	Default
ResolutionSec	DWORD Value	The interval at which the TimerService services queued requests, expressed in seconds.	1

MainScreen

The MainScreen key, located at [HKEY_LOCAL_MACHINE\SOFTWARE\ Cisco Systems, Inc.\CTIOS\ <CTIOSInstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All Desktops\ ScreenPreferences\ Name\MainScreen], includes registry values that define the behavior of softphone windows and icons in response to a BeginCallEvent. Table 8-17 lists the registry values for the MainScreen key.

Table 8-17 MainScreen Registry Key Values

Registry Value Name	Value Type	Description	Default
BringToFrontOnCall	DWORD Value	When enabled (1), the softphone window is raised above all other windows when a BeginCallEvent occurs.	1
FlashOnCall	DWORD Value	When enabled (1), the softphone icon on the taskbar flashes when a BeginCallEvent occurs.	0
RecordingEnabled	DWORD Value	Controls whether the Record button is enabled on the Agent and Supervisor Softphones (0 = disabled, 1 = enabled).	0
AgentStatistics IntervalSec	DWORD Value	Controls how often (in seconds) the Agent and Supervisor Softphones update time-in-state agent statistics.	0xF

Configuring IPCC Silent Monitor

The IPCCSilentMonitor key contains silent monitor configuration information. The IPCCSilentMonitor key contains one subkey, named Settings.

The IPCCSilentMonitor configuration settings are declared in the registry of each server on the following location:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\ CTIOS\<CTIOS
InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All
Desktops\UCCESilentMonitor\Name\Settings]
```

The Settings subkey contains the parameters used by the silent monitor subsystem to establish a monitoring session between a supervisor and a monitored agent. The values are listed in Table 8-18.

Table 8-18 Settings Registry Subkey Values

Registry Value Name	Value Type	Description	Default
HeartbeatInterval	DWORD value	The time in seconds between consecutive heartbeats.	5
HeartbeatTimeout	DWORD value	The amount of time in seconds that must elapse without receiving data before a disconnect is signaled.	15
MediaTerminationPort	DWORD value	Reserved. This is the TCP/IP port that the silent monitor subsystem uses to render monitored audio.	4000
MonitoringIPPort	DWORD value	This is the TCP/IP port on the monitoring application to which the monitored application sends monitored audio.	39200
StopSMNonACDCall	DWORD value	This stops silent monitoring of Non-ACD calls. When enabled (1) in Unified CM-based silent monitoring, the supervisor's monitor button is disabled. When enabled in desktop-based silent monitoring, the supervisor's monitor button is enabled but the supervisor can only hear ACD calls. **Note** This value must be manually entered into the registry. If the value has not been entered into the registry, the effect is the same as having it set to its default (0).	00000000

Defining Connection Profiles

The ConnectionProfiles key contains an organized list of the connection information of all configured CTI OS servers present in the corporate network that can be accessed by a client application. The connection profiles are defined in the registry of each server at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\CtiOs\<CTIOS
InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\All
Desktops\Login\ConnectionProfiles\Name
```

To create a profile for a given server, you must define a subkey under ConnectionProfiles\Name with the following format:

```
[HKEY_LOCAL_MACHINE\Software\…\ConnectionProfiles\Name\CtiOsServerName]
"PeripheralID"=dword:5000
"Heartbeat"=dword:00000000
"MaxHeartbeats"=dword:00000005
"CtiOsA"="HostName_A"
"CtiOsB"="HostName_B"
"PortA"=dword:0000a42c
```

```
"PortB"=dword:0000a42c
"AutoLogin"=dword:00000001
“ShowFieldBitMask”=dword:00000023
"WarnIfAlreadyLoggedIn"=dword:00000001
"RejectIfAlreadyLoggedIn"=dword:00000000
"DisableSkillGroupStatistics"=dword:00000001
"DisableAgentStatistics"=dword:00000001
“UCCESilentMonitorEnabled”=dword:0x00000001
“WarnIfSilentMonitored”=0x00000000
```

Table 8-19 describes the required ConnectionProfiles key registry values.

Table 8-19 ConnectionProfiles Key Registry Values

SubKey/Value	Description
CtiOsServerName	The name given to the profile. This string is displayed on the Login Dialog when a user is about to login using the CTI OS Agent State Control.
PeripheralID	The numeric value of the peripheral to which the CTI OS Server connects.
Heartbeat	Time interval between heartbeat messages between the client and CTI OS Server.
MaxHeartbeats	Maximum number of heartbeats that can be missed by the CTI OS Client Session before failover occurs.
CtiOsA	DNS name of IP Address of the primary CTI OS Server to which a client application can connect.
CtiOsB	DNS name of IP Address of the secondary CTI OS Server to which a client application can connect.
PortA	TCP/IP port number assigned to the primary server.
PortB	TCP/IP port number assigned to the secondary server.
AutoLogin	Indicates if the client must automatically login an agent or supervisor after it has recovered from a system failure. For all peripherals other than IPCC this field must be set to 0x00000000. For IPCC, set this field to 0x00000001.
ShowFieldBit Mask	Indicates what fields are displayed in the CTI OS Login dialog box. Fields are displayed on the dialog box only if their corresponding bit in the mask is on. The possible fields and their corresponding masks are shown in Table 8-20. The default value at setup for ShowFieldBit Mask is 0x00000023 (AgentID, Instrument and Password displayed).
WarnIfAlready LoggedIn	Indicates whether to display a warning but still permit login if an agent who is already logged in attempts to log in again. A value of 1 (default) enables the warning; a value of 0 disables the warning. This value is relevant only if RejectIfAlreadyLoggedIn is 0.
RejectIfAlready LoggedIn	Indicates whether or not to permit an agent who is already logged in to log in again. A value of 0 (default) permits an agent to log in again. A value of 1 prohibits an agent from logging in again.

Table 8-19 ConnectionProfiles Key Registry Values (continued)

SubKey/Value	Description
DisableSkillGroup Statistics	Indicates whether skill group statistics are enabled for the agent using this connection profile. A value of 1 disables statistics. If this value is 0 (default) or not present, skill group statistics are enabled for this agent.
DisableAgent Statistics	Indicates whether agent statistics are enabled for the agent using this connection profile. A value of 1 disables statistics. If this value is 0 (default) or not present, statistics are enabled for this agent.
IPCCSilent MonitorEnabled	Indicates whether silent monitor is enabled for the clients using this connection profile. A value of 0x00000001 (default) enables silent monitor. If this value is 0x00000000 or not present, silent monitor is disabled for this client. For all peripherals other than IPCC, this field must be set to 0x00000000.
WarnIfSilent Monitored	Indicates whether to display an indicator on the agent desktop when the agent is silent monitored by the team supervisor. A value of 0x00000001 causes a message to be displayed on the agent desktop when the supervisor is silent monitoring this agent. If this value is 0x00000000 (default) or not present, no message is displayed on the agent desktop when the supervisor is silent monitoring this agent.
RasCallMode	Indicates the agent work mode options for the mobile agent login dialog box. Valid values are 0 (agent chooses), 1 (call by call), and 2 (nailed up).

Table 8-20 ShowBitFieldMask Fields

Field	Mask
Instrument	0x00000001
Password	0x00000002
Work Mode	0x00000004
Position ID	0x00000008
Skillgroup	0x00000010
AgentID	0x00000020
Login Name	0x00000040
Mobile Agent	0x00000080

The heartbeating mechanism uses the MaxHeartbeats and Heartbeat values together to determine when a client must send heartbeat requests to the server and when the client must connect to the other server.

MaxHeartbeats is the max number of missed heartbeats before failover.
(Default = 3)

Heartbeat is the time interval between consecutive heartbeats. (Default = 5)

This is how the heartbeating mechanism works on the CTI OS client:

- After 5 seconds, if the client does not receive a response from the server, it sends a heartbeat request 1.
- After 5 seconds, if the client does not receive a response from the server, it sends a heartbeat request 2.
- After another 5 seconds, if the client does not receive a response from the server, it sends a heartbeat request 3.
- After yet another 5 seconds, if the client does not receive any response from the server, it connects to an alternative server.

Note The amount of time it takes a client to reconnect to the other server depends on the type of failure that occurs.

The heartbeat parameters above are only a factor if the TCP/IP socket is not broken. For example, if you disconnect the network cable to the CTI OS server, TCP/IP does not break the socket. In this case, the client uses the heartbeating mechanism listed above to detect the failure.

In a different case, however, if the CTI OS server process crashes or the machine is turned off, the socket breaks and the client immediately knows that the connection has failed. In this case, the client directly connects to the other server without heartbeat attempts.

Note In either case, although the socket connection might get established right away, it might take a few more seconds for the agents to fully recover their previous, pre-failure state. This delay might particularly be experienced if many agents are failing over at the same time, or if the system is experiencing a heavy call load at the time of the failure.

SilentMonitorService Subkey

The ConnectionProfiles key contains a <profile_name>\SilentMonitorService subkey, which contains parameters that clients use to connect to one of a set of silent monitor services. It contains the following keywords.

Table 8-21 ConnectionProfiles\<profile_name>\SilentMonitorService Subkey Values

Registry Value Name	Value Type	Description
ListenPort	integer	Port on which the silent monitor service is listening for incoming connections.
TOS	integer	QOS setting for the connection.
HeartbeatInterval	integer	Amount of time in milliseconds between heartbeats.
HeartbeatRetries	integer	Number of missed heartbeats before the connection is abandoned.

Table 8-21 ConnectionProfiles\<profile_name>\SilentMonitorService Subkey Values (continued)

Registry Value Name	Value Type	Description
Cluster		A key that contains a list of silent monitor services to which the CIL tries to connect. The CIL randomly chooses one of the services in this list. This key contains the following subkeys. • 0—Index of the first silent monitor service • N—Index of the Nth silent monitor service Both subkeys contain the following keyword. SilentMonitorService - hostname or IP address of a silent monitor service to which to connect.

Configuring Additional Connection Profiles

Creating a Second Profile

Use the following template to create a connection profile that includes a silent monitor server.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
Desktops\Login\ConnectionProfiles\Name\<profileName>]
    "peripheralID"=dword:00001389
    "ShowFieldBitMask"=dword:000000a3
    "SwitchCapabilityBitMask"=dword:7f3f1bff
    "CtiOsA"="ctios-a"
    "PortA"=dword:0000a42c
    "UCCESilentMonitorEnabled"=dword:00000001
    "WarnIfSilentMonitored"=dword:00000000
    "CtiOsB"="ctios-b"
    "PortB"=dword:0000a42c
    "MaxHeartbeats"=dword:00000003
    "Heartbeat"=dword:00000005
    "AutoLogin"=dword:00000001
    "WarnIfAlreadyLoggedIn"=dword:00000000
    "RejectIfAlreadyLoggedIn"=dword:00000000
    "TOS"=dword:00000000
```

```
          "RasCallMode"=dword:00000000


     [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
     Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
     Desktops\Login\ConnectionProfiles\Name\<profileName>\SilentMonitorService]

          "HeartbeatInterval"=dword:00001388

          "HeartbeatRetries"=dword:00000005

          "ListenPort"=dword:0000a42d

          "TOS"=dword:00000000


     [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
     Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
     Desktops\Login\ConnectionProfiles\Name\<profileName>\SilentMonitorService\Cluster]


     [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
     Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
     Desktops\Login\ConnectionProfiles\Name\<profileName>\SilentMonitorService\Cluster\0]

          "SilentMonitorService"="sms-host-or-ip"
```

Note The SilentMonitorService key is not always present.

When the SilentMonitorService key is present, the agent desktop attempts to connect to the silent monitor service running on the host specified in the key.

When the SilentMonitorService key is not present, the agent desktop determines if it is running under Citrix. If it is, the desktop attempts to connect to a silent monitor service running on the Citrix Client computer. Otherwise, the desktop connects to a silent monitor service running locally (on the same computer as the agent desktop).

Two Profiles for a Server- and Desktop-Based Silent Monitor Scenario

If no silent monitor key exists in the connection profile, the profile defaults to desktop silent monitoring. The following template illustrates two connection profiles—one for desktop-based silent monitor, and one for server-based silent monitor.

```
     [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
     Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
     Desktops\Login\ConnectionProfiles\Name\UCCE]

          "peripheralID"=dword:00001388

          "ShowFieldBitMask"=dword:00000023

          "SwitchCapabilityBitMask"=dword:7f3f1bff

          "CtiOsA"="ctios-a"

          "PortA"=dword:0000a42c

          "UCCESilentMonitorEnabled"=dword:00000001
```

```
    "WarnIfSilentMonitored"=dword:00000001
    "CtiOsB"="ctios-b"
    "PortB"=dword:0000a42c
    "MaxHeartbeats"=dword:00000003
    "Heartbeat"=dword:00000005
    "AutoLogin"=dword:00000001
    "WarnIfAlreadyLoggedIn"=dword:00000000
    "RejectIfAlreadyLoggedIn"=dword:00000000
    "TOS"=dword:00000000
    "SaveShowField"=dword:00000043

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
Desktops\Login\ConnectionProfiles\Name\Mobile Agent]
    "peripheralID"=dword:00001388
    "ShowFieldBitMask"=dword:000000a3
    "SwitchCapabilityBitMask"=dword:7f3f1bff
    "CtiOsA"="ctios-a"
    "PortA"=dword:0000a42c
    "UCCESilentMonitorEnabled"=dword:00000001
    "WarnIfSilentMonitored"=dword:00000000
    "CtiOsB"="ctios-b"
    "PortB"=dword:0000a42c
    "MaxHeartbeats"=dword:00000003
    "Heartbeat"=dword:00000005
    "AutoLogin"=dword:00000001
    "WarnIfAlreadyLoggedIn"=dword:00000000
    "RejectIfAlreadyLoggedIn"=dword:00000000
    "TOS"=dword:00000000
    "RasCallMode"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All
Desktops\Login\ConnectionProfiles\Name\Mobile Agent\SilentMonitorService]
    "HeartbeatInterval"=dword:00001388
    "HeartbeatRetries"=dword:00000005
    "ListenPort"=dword:0000a42d
    "TOS"=dword:00000000
```

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\Mobile Agent\SilentMonitorService\Cluster]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS_<instance>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\Mobile Agent\SilentMonitorService\Cluster\0]

"SilentMonitorService"="sms-host-or-ip"

Configuring the Call Appearance Grid

The CallAppearance key contains a list of all the columns that are displayed on the softphone Call Appearance grid.

The columns are declared in the registry of each server on the following location:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\
<CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\
All Desktops\Grid\CallAppearance\Columns\Number\Position]
```

Position represents the actual location in the grid where the column appears. For example for the first column Position is “1” and for the fifth column it is “5”.

Table 8-22 lists the attributes that a column declaration can contain.

Table 8-22 Column Declaration Attributes

Attribute	Type	Description
Type	String Value	Assigns a column to display the Call information identified by the value of this attribute. Table 8-23 lists the possible values.
Header	String Value	Contains the text string to be displayed on the header of the column. If not specified, the Type is displayed instead.
Width	DWORD value	Column width expressed in pixels. If the Auto Resize Columns property is set on the Call Appearance Grid, this attribute has no effect. The column is automatically sized to match the column header or column cell content, whichever is longer. If the Auto Resize Columns property is *not* set, one of the following occurs: • If Width is specified, the column sizes to match it. • If Width is *not* specified, the column sizes to a default length.
MaxChars	String Value	Maximum number of characters that can appear in the column.

Table 8-22 Column Declaration Attributes (continued)

Attribute	Type	Description
Name	String Value	Used only when the Type is ECC; contains the name of a given ECC variable. The name in this attribute must be entered without the prefix "**user.**" For the standard Outbound Option ECC variables, use the prefix **BA** without any dots following it; for example, **BAResponse**.
Alignment	String Value	Defines the alignment of the information on the columns. Possible values are "left", "right" or "centered."
NumericOnly	String Value	If "true" the column accepts only numeric values for display. If "false" alphanumeric values may be displayed.
editable	String Value	Indicates if the user can modify the cells on the column at runtime.

Table 8-23 lists the Type Values.

Table 8-23 Type Values

Type	Description
CallID	Associates the column with the unique call ID.
CallStatus or Status	Associates the column with Call Status.
DNIS	Associates the column with DNIS.
ANI	Associates the column with ANI.
CED	Associates the column with the caller entered digits.
DialedNumber or DN	Associates the column with the dialed number.
UserToUserInfo or UserToUser	Associates the column with user to user information.
WrapUp	Associates the column with the call wrap up data.
Var1, Var2, …, Var10	Associates the column with a call variable.
NAMEDVARIABLE, ECCVariable, ECCVar, ECC, or ECCNAME	Associates the column with an scalar ECC Variable.
NAMEDARRAY or ECCARRAY	Associates the column with a Named Array ECC variable.

Table 8-23 Type Values (continued)

Type	Description
CampaignID	Campaign ID for value appears in the Agent Real Time table. Set to zero if not used. *Applicable to Outbound Option systems only.*
QueryRuleID	Query rule ID for value appears in the Agent Real Time table. Set to zero if not used. *Applicable to Outbound Option systems only.*

The following are examples of column declarations:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\
<CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\
All Desktops\Grid\CallAppearance\Columns\Number\1]
"Type"="CallID"
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\
<CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\
All Desktops\Grid\CallAppearance\Columns\Number\10]
"Type"="Var2"
"editable"="true"
```

The following is an example of associating a column with an ECC variable:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\
<CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\
All Desktops\Grid\CallAppearance\Columns\Number\19]
"Type"="ECC"
"Name"="bobc"
"Header"="ECC Bobc"
"Maxchars"="8"
"editable"="true"
```

The following is an example of associating a column with an ECC array variable. Note that the “Name” key must contain both the array name and the subscript/index:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CtiOs\
<CTIOS InstanceName>\<CTIOSServerName>\ EnterpriseDesktopSettings\
All Desktops\Grid\CallAppearance\Columns\Number\19]
"Type"="ECCARRAY"
"Name"="bobc[0]"
"Header"="ECCARRAY Bobc"
"Maxchars"="8"
"editable"="true"
```

Automatic Call Appearance Grid Configuration

The CTIOSServer directory contains a file, callappearance.default.reg.txt, that provides the following default definition for Call Appearance grid columns 1 to 18:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\ Number\1]
“Type”=”CallID”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\ Number\10]
“Type”=”Var2”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\ Number\11]
“Type”=”Var3”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\12]
“Type”=”Var4”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\ Number\13]
“Type”=”Var5”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\14]
“Type”=”Var6”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\15]
“Type”=”Var7”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\16]
“Type”=”Var8”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\17]
“Type”=”Var9”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\18]
“Type”=”Var10”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\2]
“Type”=”CallStatus”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\3]
“Type”=”DNIS”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\4]
“Type”=”ANI”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\5]
“Type”=”CED”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\6]
“Type”=”DialedNumber”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\7]
“Type”=”UserToUserInfo”
“maxchars”=”129”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\8]
“Type”=”WrapUp”
“maxchars”=”40”
“editable”=”true”

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\9]
“Type”=”Var1”
“maxchars”=”40”
“editable”=”true”
```

To import this default definition into your registry, perform the following steps:

Step 1 Choose **Start** > **Run** dialog box.

Step 2 Rename the **callappearance.default.reg.txt** file to **callappearance.default.reg**.

Step 3 Enter

```
regedit filename
```

where *filename* is the *full pathname* of the callappearance.default.reg file.

Step 4 Cycle your CTI OS Server process (see the section entitled Unified CCE Service Control in Chapter 9, "Startup, Shutdown, and Failover" for instructions).

Automatic Agent Statistics Grid Configuration

The CTIOSServer directory contains a file, agentstatistics.default.reg.txt, that contains the default definition for the Agent Statistics grid. The following is an example agentstatistics.default.reg.txt file that defines Agent Statistic grid columns 1 and 2.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\AgentStatistics]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\AgentStatistics\Columns]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\AgentStatistics\ Columns\Number]
"DisableStatsMinimization"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\AgentStatistics\ Columns\Number\1]
"Type"="CallsHandledToday"
"Header"="CallsHandledToday"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\AgentStatistics\Columns\Number\2]
"Type"="TimeLoggedInToday"
"Header"="TimeLoggedInToday"
```

The DisableStatsMinimization registry value controls the quantity of agent statistics that are sent from the CTI OS Server to CTI OS clients. Possible values are 0 (only those agent statistics that are configured to be displayed on the agent statistics grid are sent to the client) and 1 (all agent statistics are sent to the client); default is 0.

To customize the Agent Statistics grid, perform the following steps.

Step 1 Make a copy of the agentstatistics.default.reg.txt file.

Step 2 Rename the copied agentstatistics.default.reg.txt file to agentstatistics.default.reg.

Step 3 Add, remove, and renumber column definitions *in the copied file* as desired.

Step 4 Choose **Start** > **Run** dialog box.

Step 5 Enter

```
regedit filename
```

where *filename* is the *full pathname* of the *edited copy* of the agentstatistics.default.reg file.

Step 6 Cycle your CTI OS Server process (see the section entitled Unified CCE Service Control in Chapter 9, “Startup, Shutdown, and Failover” for instructions).

Automatic Skill Group Statistics Grid Configuration

The CTIOSServer directory contains a file, skillgroupstatistics.default.reg.txt, that contains the default definition for the Skill Group Statistics grid. The following is an example skillgroupstatistics.default.reg.txt file that defines columns 1 through 4.

Note The first column of the Skill Group Statistics window should be **SkillGroupNumber**.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ Columns\Number]
“DisableStatsMinimization”=dword:00000000
“DisableMonitorModeStatsMinimization”=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns\Number\1]
"Type"="SkillGroupNumber"
"header"="SkillGroupNumber"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\Columns\Number\2]
"Type"="AgentsAvail"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ Columns\Number\3]
"Type"="AgentsNotReady"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
<CTIOS InstanceName>\<CTIOSServerName>\
EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ Columns\Number\4]
"Type"="AgentsReady"
```

The DisableStatsMinimization registry value controls the quantity of skill group statistics that are sent from the CTI OS server to CTI OS agent mode clients. Possible values are 0 (only those skill group statistics that are configured to be displayed on the skill group statistics grid are sent to the client) and 1 (all skill group statistics are sent to the client); default is 0.

The DisableMonitorModeStatsMinimization registry value controls the quantity of skill group statistics that are sent from the CTI OS server to CTI OS monitor mode clients. Possible values are 0 (only those skill group statistics that are configured to be displayed on the skill group statistics grid are sent to the client) and 1 (all skill group statistics are sent to the client); default is 0.

Note At all the new installs, when viewing CTIOS with the Supervisors, the default skill group shows up on the CTIOS Agent Skill Group stats. This default skill group gets added by default when you create a peripheral, or upgrade to 5.0 or later. IPCC uses the new default skill group added for support of media routing. All voice calls not routed by a Unified UCCE script are reported in this new default skill group.

Note While you can customize columns in the **Skill Group Statistics** grid, you should retain the following registry settings:

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS

<CTIOS InstanceName>\<CTIOSServerName>

EnterpriseDesktopSettings\All

Desktops\Grid\SkillGroupStatistics\Columns\Number\1]

"Type"="SkillGroupNumber"

"header"="SkillGroupNumber".

The header can vary depending on the language you use. To customize the Skill Group Statistics grid, perform the following steps”

Step 1 Make a copy of the skillgroupstatistics.default.reg.txt file.

Step 2 Rename the copied skillgroupstatistics.default.reg.txt file to skillgroupstatistics.default.reg.

Step 3 Add, remove, and renumber column definitions *in the copied file* as desired.

Step 4 Open the Windows **Start** > **Run** dialog box.

Step 5 Enter

```
regedit filename
```

where *filename* is the *full pathname* of the *edited copy* of the skillgroupstatistics.default.reg file.

Step 6 Cycle your CTI OS Server process (see the section entitled Unified CCE Service Control in Chapter 9, “Startup, Shutdown, and Failover” for instructions).

Configuring Additional Peripherals

The Peripheral Identifier screen in CTI OS Server setup lets you supply peripheral information for a single peripheral only. To configure additional peripherals, perform the following steps:

Step 1 Define a registry key for the peripheral in [Server\Peripherals\ PERIPHERAL_LOGICAL_NAME]. See the section entitled Peripherals for instructions.

Step 2 Create a connection profile for the peripheral, following the directions in the section entitled Defining Connection Profiles.

Note The value that you specify for Peripheral ID in the Peripherals registry key definition *must* match the value that you specify for Peripheral ID in the connection profile definition.

Quality of Service/Type of Service (QoS/ToS)

CTI OS supports QoS markings (ToS / DSCP). However, QoS is not supported for Siebel communications. For more information on QoS and the meaning of ToS/DSCP, please see http://www.cisco.com/en/US/docs/voice_ip_comm/bts/4.1/command/reference/93PktCbl.pdf.

Note ToS is not supported in CTI OS Releases 6.0 and earlier.

The following connections/components support Qos/ToS:

- (1) CTI OS Server to CTI OS Client.
- (2) CTI OS Client (C++ CIL only) to CTI OS Server.
- (3) CTI OS Silent Monitoring. If the PCs network connection is via the desk phone and Silent Monitoring is used, then the switch in the phone overrides the ToS marking to 0 and it affects both silent monitor and client to server traffic. It does not affect the server to client traffic.

Note CTI OS Client installations (including Silent Monitor Service) on Windows Vista or Windows 7 will not mark packets for QoS. Due to the number of clients in a typical installation, it is recommended that Active Directory (or equivalent group administered approach) be used to set QoS Policies on Client installations. This approach will drive consistency across the client installations. If a group administered approach is undesirable, the Group Policy Editor (gpedit.msc) may be used to implement QoS policies locally.

For more information, see http://technet.microsoft.com/en-us/library/cc771283.aspx.

CTI OS supports the marking of TCP/IP packets with ToS. This allows for preferential treatment (for example, class AF31 for assured forwarding) of CTI signaling traffic if the network is configured to support this QoS scheme.

By default, CTI OS does not mark packets, which means that the traffic is sent with "best effort" (ToS = 0).

In order to turn on the ToS markings, you must configure certain registrykeys. In general, ToS effects only outgoing packets. For example, the CTI OS server can send packets with ToS markings for assured forwarding to CTI OS clients. However, that does not imply that CTI OS clients must also send their network traffic with the same ToS value to the CTI OS server. CTI OS clients could in fact send their traffic on a best-effort basis, which would mean that ToS is only active one way. Most likely, though, ToS is configured the same for both directions.

Basic Configuration

In order to turn on ToS with AF31 for bidirectional communications, add/modify some registry keys for CTI OS server.

1. The following key turns on marking of packets CTI OS server sends to CTI OS clients:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\<customer-instance>\CTIOS1\Server\Connections
"TOS"=dword:00000068
```

Note The dword value above is listed in hexadecimal format (decimal 104).

2. This registry key turns on markings of packets sent from the client to the server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\<customer-instance>\CTIOS1\EnterpriseDesktopSettings\All
Desktops\Login\ConnectionProfiles\Name\UCCE<or other profile name>
"TOS"=dword:00000068
```

3. This key turns on TOS marking for Silent Monitor packets. Note, for a silent monitor stream a different class (real-time/voice) with a different TOS value (Hex B8) is suggested:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\<customer-instance>\CTIOS1\EnterpriseDesktopSettings\ All
Desktops\UCCESilentMonitor\Name\Settings
"TOS"=dword:000000B8
```

Important Additional Configuration Information

This type of ToS marking requires the setting of a special system registry key in Windows 2000, Windows 2003 as well as Windows XP as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters
"DisableUserTOSSetting"=dword:00000000
```

Disable **UserTOSSetting** defaults to 1 (and is not present by default) and therefore TOS markings are disabled without setting this key. After this registry key is set, the system must be restarted for this change to become effective.

For additional information see:

http://support.microsoft.com/default.aspx?scid=kb;en-us;258978

http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/deployguide/en-us/242666.asp

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx

Caveats

- In order for the ToS to become effective, the network (specifically the routers) must be configured to treat packets with ToS markings preferentially.
- The traffic between CTIOS server and CTIOS clients may include types of data that do not qualify for AF31 type of service. AF31 is suggested for signaling traffic. For example, a calldelivered event sent from CTIOS server is time critical as is a potential Answer request sent from the client in response in order to answer an alerting call. However, CTIOS server can also send statistics to clients and this type of data is not suggested for AF31. However, because CTIOS sends all traffic on the same connection, either all packets are marked or none. Therefore, CTIOS Skillgroupstatistics must be turned off with TOS enabled.
- When hardphones are used with Silent Monitoring, the switch in the phone overrides the TOS marking to 0. This affects both Silent Monitor and CTI OS client to CTI OS server traffic. (It does not affect CTI OS server to CTI OS client traffic.) To correct this problem, write ACL to classify traffic based on TCP/UDP port number from the endpoint.

CHAPTER 9

Startup, Shutdown, and Failover

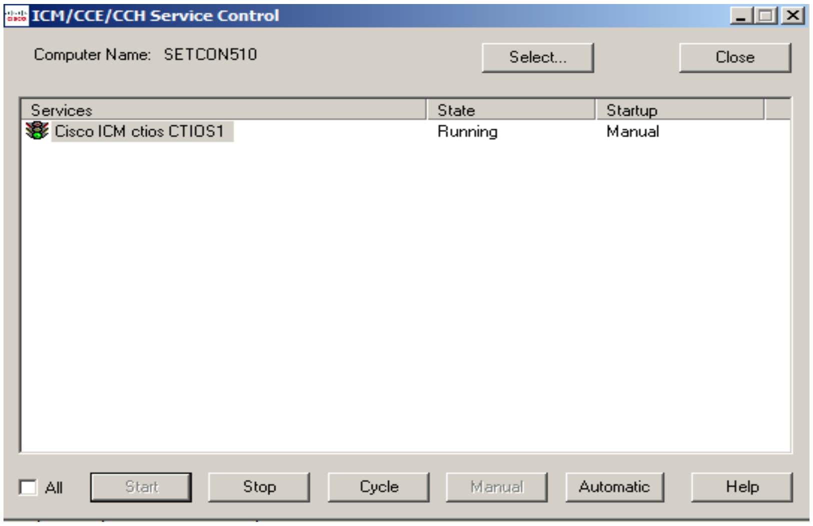
This chapter explains how to start and stop the CTI OS System and describes how CTI OS handles failover scenarios. It contains the following sections”

- Unified CCE Service Control, page 9-1
- CTI OS Failover, page 9-2

Unified CCE Service Control

The CTI OS Server runs as a Windows 2000 service on the host computer. The Unified CCE Service Control application is an interface into the Windows platform’s service control manager, which starts and stops services. See Figure 9-1.

Figure 9-1 Unified CCE Service Control



ICM/CCE/CCH Service Control

Computer Name: SETCON510

Services	State	Startup
Cisco ICM ctios CTIOS1	Running	Manual

To start, stop, or cycle the processes in the CTI OS Server, use the appropriate tabs from the Unified CCE Service Control window. To set CTI OS to start automatically on Windows startup (the recommended method), select the service name and click the Automatic button.

When the CTI OS service starts, it launches processes listed in Table 9-1. Some of these processes open and run in console windows. These windows can be minimized, but cannot be closed. Closing the console window in which a process is running forces a restart of that process.

Table 9-1 CTI OS System Processes

Process Name	Process Description	Runs In Console Window
CtiosServerNode	The main CTI OS Server process. This process manages all CTI OS objects and listens for and manages client connections.	Yes
CTIOSTrace	The CTI OS tracing utility. This process uses the Unified ICM Event Management System (EMS) to trace server messages to local log files in EMS format.	No
NM	The Unified ICM NodeManager (fault tolerance manager). Each Unified ICM service is started by NodeManager, and NodeManager restarts any abnormally terminated processes.	No
NMM	The Unified ICM NodeManagerManager (system fault tolerance). Each Unified ICM Node (e.g. CTI OS) starts up a NMM process to handle system-level faults. In the event of a unrecoverable system fault, NMM restarts the host computer.	No

CTI OS Failover

The server processes are managed by a fault tolerance/recovery platform called NodeManager. NodeManager creates and monitors each process running as part of the CTI OS service, and automatically restarts abnormally terminated processes.

Setting the /LOAD Configuration Parameter

In order for CTI OS failover to work correctly, the settings for the peripheral in the PG Explorer must be configured correctly. Perform the following steps to verify that the parameters are correct:

Step 1 Run the PG explorer.

Step 2 Click the "+" to open the branch for the correct PG.

Step 3 Select the peripheral.

Step 4 Select the PERIPHERAL tab on the right.

Step 5 In the edit field for the Configuration Parameters, enter "/LOAD 0" (without the quotes), if it is not already datafilled.

Step 6 Cycle the PG.

"/LOAD 0" causes agents to be set to NotReady during a failover. By setting the agents to NotReady, calls are not routed to them and the failover is quicker and cleaner.

Note The default for ICM versions 4.6.1.x and earlier was "/LOAD 0". It was changed in Versions 4.6.2, 5.0, and 6.0 to "/LOAD 1". In version 7.0, the default was changed back to "/LOAD 0". If you upgraded from 4.6.1.x to 4.6.2, 5.0, or 6.0, you must go into the PG explorer and manually set the parameter to "/LOAD 0" if you are using CTI OS. The default remains “/LOAD 0” in release 8.0(1).

CTI OS 7.0 does not support "/LOAD 1". Therefore, if RejectIfAlreadyLoggedIn is set to 1, then the behavior of the system is as follows:

1. If RejectIfAlreadyLoggedIn flag is on, then no two agents are able to log in using the same agentID.
2. The agent desktop crashes while the agent is successfully logged in to CTI OS Server and does not have calls. In this case, the supervisor must log out the agent first, and then the agent must re-launch the agent desktop, supply the correct password, and log in manually.
3. The agent desktop crashes while the agent is logged in to CTI OS Server and has calls. In this case, the supervisor must log out the agent first, and then the agent must re-launch the agent desktop, supply the correct password, and log in manually.

Failover of CTI OS Related Components

CTI OS handles failover of related components as described in the following sections.

IP Phones

If an IP phone goes out of service, CTI OS sends an event to all soft phones associated with the IP phone that their IP phone is out of service. In addition, the affected softphones display the message “Offline.” When the IP phone is back in service, agents must log in again manually.

Switches

If a switch goes out of service, CTI OS sends an event to all softphones associated with the switch that the switch is offline. In addition, the affected softphones display the message “Offline.” When the switch is back in service, agents must sign in again manually.

Peripheral Gateway

Because the Peripheral Gateway (PG) is a fault-tolerant process pair, CTI OS is not affected if the PG merely switches active sides. If the PG goes offline, CTI OS sends an “Offline” message to each softphone client.

CTI Server

On a CTI Server failure, CTI OS Server usually reconnects almost immediately to the redundant CTI Server. If reconnection to the redundant CTI Server is not possible, CTI OS Server sends a failure response to any requests made to the CTI Server.

In addition, CTI OS sends an event message to all softphone clients. On receipt of this message, the softphone clients display an “Offline” message.

When the CTI Server comes back online, CTI OS performs a snapshot of all agents, devices, and calls to reestablish state information.

CTI OS Server

On a CTI OS Server failure, CTI OS disconnects all softphones from the failed CTI OS Server. These softphones attempt to reconnect automatically to another CTI OS Server; if reconnection is not possible, CTI OS sends an event message to all softphone clients. On receipt of this message, the softphone clients display an “Offline” message.

NodeManager restarts the CTI OS Server. When the CTI OS Server process comes back online, CTI OS performs a snapshot of all agents, devices, and calls to reestablish state information.

CHAPTER 10

Peripheral-Specific Support

This chapter provides information on the Time Division Multiplexing (TDM) peripherals supported by CTI OS. It contains the following sections:

- General Unified ICM Support, page 10-1
- CTI OS Support, page 10-3

Different peripheral manufacturers provide varying levels of support for CTI specific features. These differences must be taken into account when writing a CTI OS client application. As far as possible, the CTI OS Server and Agent Desktop simulate the hardphone behavior of the peripheral in question. The CTI OS Supervisor Desktop for IPCC Enterprise is specific to IPCC Enterprise and is currently not supported on the TDM switches because they do not, in general, provide the Supervisory features that IPCC provides.

Note The peripherals mentioned in this chapter are the ones that CTI OS supports. For a complete list of all peripherals supported by the Cisco CTI Server please see the *Cisco Unified ICM CTI Programmer's Guide*. Please contact Cisco CTI Product Management if you are interested in CTI OS support for a peripheral not mentioned here.

This chapter provides the following information:

- Peripheral-specific equivalents for some common Unified ICM terms
- A list of Unified ICM features that some peripherals do not support
- A table of CTI call event types that are unavailable for different peripheral types
- A table of CTI OS client control requests that are unsupported by different peripheral types
- Differences and limitations in the level of CTI support provided by various peripherals—including a list of CTI Server agent states and the corresponding terminology/functionality associated with the various peripherals

General Unified ICM Support

This section describes differences in how various peripherals implement Unified ICM functionality.

Peripheral-Specific Terminology

Different peripheral manufacturers use different terminology for Unified ICM terms such as agents, skill groups, and services. For example, other manufacturers might call a service an application, a split, or a gate. Table 10-1 lists several Unified ICM terms and provides peripheral-specific equivalents.

Table 10-1 Unified ICM and Peripheral-Specific Terminology

Unified ICM Term	Peripheral-Specific Equivalent
Agent	Agent
Peripheral target	**Alcatel 400**: DNIS **IPCC**: Device Target **Others**: Trunk group and DNIS[1]
Service	**Alcatel 400**: Pilot **Aspect Contact Server**: Application **Avaya DEFINITY ECS**: Vector Directory Number (VDN) **Nortel Symposium**: Application **Rockwell Spectrum**: Application
Skill group	**Alcatel 400**: Agent PG **Aspect Contact Server**: Agent group **Avaya DEFINITY ECS**: Skill group or hunt group[2] **Nortel Symposium**: Skill Set **Others**: Skill group
Trunk	**Alcatel 400**: None **Aspect Contact Server**: Instrument[3] **Nortel Symposium**: None **Others**: Trunk
Trunk group	**Alcatel 400**: None **Nortel Symposium**: Route **Others**: Trunk group

[1] The Aspect Contact Server maps a trunk group and DNIS to a Call Control Table (CCT). The DEFINITY ECS uses the trunk group and DNIS for incoming calls.

[2] If an ECS is running in Expert Agent Selection (EAS) mode, a skill group maps to an ECS skill group; otherwise, it maps to a hunt group.

[3] A CallCenter instrument can be a trunk, a teleset, or a workstation.

In some cases, the Unified ICM concept is very close to the corresponding ACD feature. For example, the Unified ICM concept of a service is very similar to the Aspect concept of an application. In other cases, the ACD does not have a feature that maps exactly to the Unified ICM feature. In these cases, you might choose a different mapping than shown in Table 10-1. For example, although it might make sense to associate each VDN on a DEFINITY ECS with an Unified ICM service, you could also map each hunt group to a service.

On an Avaya DEFINITY ECS running in EAS mode, each skill group may have multiple subgroups depending on the switch configuration. Unified ICM emulates this by automatically creating additional skill groups for these peripheral types.

Unified ICM Feature Limitations

Some ACDs have limitations that prevent them from making full use of specific features of Unified ICM. Table 10-2 summarizes these limitations for those ACDs.

Table 10-2 Unified ICM Features Not Supported for Specific Peripherals

Peripheral Type	Restrictions
Aspect Contact Server	Only one skill group assignment per agent
Avaya DEFINITY ECS	none
IPCC	Does not support Trunks or Trunk Groups
Nortel Symposium	No Peripheral Service Level reporting No Trunk Group Real Time or Trunk Group Half Hour data elements
Rockwell Spectrum	No real-time trunk group monitoring Duplexed PG operation supported only for TCP/IP Transaction Link configurations

CTI OS Support

This section describes how different peripheral types implement and support CTI OS functionality. It includes the following information:

- A table of call event types that are unavailable for different peripheral types
- A table of client control requests that are unsupported by different peripheral types
- A list of other peripheral-specific differences and limitations
- A table of agent states

Call Events

Table 10-3 lists the call events that are *not* available from different peripheral types.

- The entry “none” indicates that the event is available from all supported peripherals.
- A single asterisk (*) indicates that the event is available from the starred peripheral, subject to the restrictions/limitations listed in the “Peripheral-Specific Limitations and Differences” section on page 10-5.
- A double asterisk (**) indicates that the event is available from Aspect when the PG is configured to use the Aspect Event Link.

Table 10-3 Call Events Not Available to Specific Peripherals

Unavailable Event	Peripherals
AGENT_PRE_CALL	Alcatel, Aspect, DEFINITY, Nortel Symposium, Rockwell Spectrum, IVR
AGENT_PRE_CALL_ ABORT	Alcatel, Aspect, DEFINITY, Nortel Symposium, Rockwell Spectrum, IVR
AGENT_STATE	none
BEGIN_CALL	none
CALL_ CLEARED	Aspect*
CALL_CONFERENCED	Aspect**, Rockwell Spectrum, IVR
CALL_CONNECTION_ CLEARED	none
CALL_DATA_UPDATE	none
CALL_DELIVERED	Aspect*, Rockwell Spectrum*
CALL_DEQUEUED	Alcatel, DEFINITY, Nortel Symposium, IPCC, IVR
CALL_DIVERTED	Aspect, IPCC, Nortel Symposium
CALL_ESTABLISHED	IVR
CALL_FAILED	Aspect, Nortel Symposium, Rockwell Spectrum, IVR
CALL_HELD	Aspect**, IVR, Rockwell Spectrum*
CALL_ORIGINATED	Aspect, DEFINITY*, Nortel Symposium, Rockwell Spectrum
CALL_QUEUED	IPCC, IVR
CALL_REACHED_ NETWORK	Aspect, Nortel Symposium, Rockwell Spectrum, IVR
CALL_RETRIEVED	Aspect**, IVR, Rockwell Spectrum*
CALL_ SERVICE_ INITIATED	Aspect**, DEFINITY*, IVR
CALL_TRANSFERRED	IVR
CALL_TRANSLATION_ ROUTE	IPCC
END_CALL	none
RTP_STARTED_EVENT	Alcatel, Aspect, Nortel Symposium, Rockwell Spectrum, IVR
RTP_STOPPED_EVENT	Alcatel, Aspect, Nortel Symposium, Rockwell Spectrum, IVR
SYSTEM	none

Client Control Requests

Table 10-4 lists the client control requests that are *not* supported by the different peripheral types.

Table 10-4 Client Control Requests NOT Available to Specific Peripherals

Unavailable Request	Peripherals
ALTERNATE_CALL	Nortel Symposium
ANSWER_CALL	IVR
CLEAR_CALL	Alcatel, IVR
CLEAR_CONNECTION	IVR
CONFERENCE_CALL	IVR
CONSULTATION_CALL	IVR
DEFLECT_CALL	Aspect, Nortel Symposium, Rockwell Spectrum, IVR
HOLD_CALL	IVR
MAKE_CALL	IVR
MAKE_PREDICTIVE_CALL	Alcatel, IVR
QUERY_AGENT_STATE	IVR
QUERY_DEVICE_INFO	IVR
RECONNECT_CALL	IVR
RETRIEVE_CALL	IVR
SEND_DTMF_SIGNAL	Aspect, Nortel Symposium, Rockwell Spectrum, IVR
SET_AGENT_STATE	IVR
SNAPSHOT_CALL	IVR
SNAPSHOT_DEVICE	IVR
TRANSFER_CALL	IVR

Peripheral-Specific Limitations and Differences

This section lists CTI OS-related restrictions and implementation differences for various peripherals.

Note

- MAKE_CALL is only supported when the agent is in the NotReady state for an IPCC peripheral.
- MAKE_CALL is not supported for the remaining peripherals supported by CTI OS.
- The call continues to be active even after a party is released from the conference.

Alcatel

- Conference calls can have a maximum of three parties.

- Single-step/blind transfer or conference is not supported. Transfer and conference calls must be consultative.
- When an agent (for example, 3550) logs into a phone/device (for example, 3300), the device becomes the agent. So to reach the agent, one would dial 3550.
- Alcatel requires a position ID as part of the Login information. Position ID is the same as instrument (an indication of the physical device).
- When an agent logs in, a skill group must be specified. Failure to specify a skil lgroup or specifying an incorrect skill group results in a login failure.
- An inside call cannot be put on Hold.
- Alcatel does not support a second line. When a call is active, the Inside and Outside controls must be unavailable. A second call can only be made as a Consult call in the context of an existing call (via Transfer or Conference).

Aspect Contact Server

- AgentExtension and AgentInstrument are defined as the port number that the teleset is connected to.
- Events marked by an asterisk (*) are available when the PG is configured to use the Aspect EventLink.
- Call Alerting (Call Delivered, LocalConnectionState = LCS_ALERTING) is available when the EventLink is used.
- Outbound calls on some trunk types do not always provide Call Cleared events. Interflow calls that are accepted, but handled by the originating site, also sometimes do not provide Call Cleared events.
- Outbound calls require that the CallPlacementType be specified in an outbound request.
- Conference calls can have a maximum of three parties.
- In a single-step/blind transfer of a call, the initial call must come in over a trunk (be a CCT call) and the dialed number must go to a CCT.
- In a regular call transfer, the consult call can be either a CCT call or an agent_inside call.
- Alternate call operations require that the initial call be a CCT call. The second call (consult call) can be either a CCT call or an agent_inside call.
- In the MAKE_PREDICTIVE_CALL_REQ message, the AnswerDetectControl1 field must contain the binary value of the Application Bridge AD_PARAM setting, and the AnswerDetectControl2 field must contain the binary value of the Application Bridge ANS_MAP setting.
- Transfer and Conference behavior is modeled after hardphone behavior. To initiate a Transfer or a Conference, you must first use the MakeCall control (Transfer Init and Conference Init buttons are unavailable at this point) to make a second (consult) call. After you make this call, the Transfer Complete and Conference Complete buttons become available to complete the desired action.

Avaya DEFINITY ECS

- AgentExtension and AgentInstrument are defined as the station extension.
- DEFINITY ECS events are the same with or without EAS (Expert Agent Selection).
- Both EAS and non-EAS versions maintain a list of preconfigured agent groups. When you log in with EAS, the agent is automatically logged in to all preconfigured Agent groups. When you log in without EAS, the agent is logged in to only those groups that you specify in the login request.

- The Cisco Peripheral Interface Module (PIM)—the Cisco proprietary interface between a peripheral and the Peripheral Gateway (PG)—does support call events on inside calls only when the agent's station is monitored by Unified ICM (that is, appears in the Unified ICM Peripheral Monitor Table), when the call goes through a monitored VDN, or when the call is originated by a CTI MakeCallReq. Inside calls are calls originated by an agent on the switch; this includes consult calls prior to a transfer or conference. After the transfer or conference is completed, you can see call events for the merged ACD call.
- Auto Answer agents must have the phone off the hook or you canno log in to the agent. Manual Answer agents must leave the phone on the hook.
- Applications must wait a time interval of three times the refresh rate (defined in the Avaya Call Management System) between login or logout attempts. Failure to do so may cause the PIM to miss the login event and result in a failed call request.
- CTI OS clients that access a DEFINITY ECS switch are returned an ASAI cause value if a third-party action fails. If you have a copy of the *DEFINITY Technical Reference Manual*, you can determine the actual cause of the failure by performing the following steps:

- Refer to Table 10-5 to obtain the *DEFINITY* ECS value that corresponds to the returned ASAI cause value.
- Refer to Table 10-6 to find the chapter of the *DEFINITY Technical Reference Manual* that discusses the third-party action that you attempted:
- Refer to the chapter specified in Table 10-6 for an explanation of the DEFINITY ECS cause value.

Table 10-5 DEFINITY Cause Values

ASAI Value	*DEFINITY* ECS Value	Cause Value	Description
-MAX_LONG	none	*C_NUSE_LONG	No value was returned by the ECS.
0	CS0/28	*C_INVLDNUM	Invalid origination or destination address.
1	CS0/111	*C_PROTERR	Capability sequence has been violated or underlying protocol error has been detected; an unrecognized value was returned by the ECS.
2	CS3/40	*C_RESUNAVL	Resources to fulfill service are not available.
3	CS0/50	*C_FACUNSUB	Capability is implemented but not subscribed to by requester.
4	CS3/79	*C_SER_UNIMP	Incompatible options selected.
5	CS0/96	*C_MAND_INFO	One of the required parameters is missing.
6	CS0/100	*C_INVLDIE	Value specified in parameter is not allowed or defined.
7	CS3/63	*C_SERV_UNAVIL	Domain or call is being monitored by another adjunct.
8	CS3/86	*C_CALLID_TERM	Call is no longer in active state.
9	CS0/98	*C_INCOM_ST	Message not compatible with call state.
10	CS0/81	*C_INVALID_CRV	Invalid call identifier (sao_id also known as cluster_id) used or call does not exist.

Table 10-5 DEFINITY Cause Values (continued)

ASAI Value	*DEFINITY* ECS Value	Cause Value	Description
11	CS3/80	*C_INCOM_OPT	Incompatible options used to establish the call.
12	CS0/102	*C_REC_TIMER	Timer expired.
13	CS3/15	*C_NOLOGIN	Agent not logged in to split.
14	CS3/11	*C_NOSPLIT_MEM	Agent not member of specified split or split number specified incorrectly.
15	CS0/17	*C_USER_BUSY	Domain or call is being monitored by another adjunct.
16	CS0/18	*C_NOUSE_RESP	Originating address does not respond to service.
17	CS3/43	*C_PERM_DENIED	Permission checks for service have failed.
18	CS3/87	*C_CLUST_TERM	Association terminated because service is not active.
19	CS3/27	*C_OUT_OF_SERV	Domain has been removed by administration.
20	CS3/12	*C_INCS_AGT_ST	Agent not in compatible state.
21	CS3/13	*C_MAXLOGIN	Agent logged in to maximum number of splits.
22	CS3/14	*C_INC_PASWD	Invalid login password.
23	CS3/16	*C_AGT_STATE	Request to put agent in the state that the agent is already in.
24	CS3/41	*C_BAD_ADMIN	ACD not provisioned or optioned.
25	CS0/16	*C_NORMAL	Normal termination; call routed successfully.
26	CS0/42	*C_NETCONJ	Association terminated because of network congestion.
27	CS0/99	*C_BAD_IE	Unknown information element detected.

Table 10-5 DEFINITY Cause Values (continued)

ASAI Value	*DEFINITY* ECS Value	Cause Value	Description
28	CS3/22	*C_QUEFULL	Queue is full.
29	CS3/42	C_REORDER_ DENIAL	Reorder/Denial.
30	CS3/46	C_ADMIN_ PROGRESS	Administration is in progress; request cannot be serviced.
31	CS3/53	C_FEATURE_ REJECTED	The ECS has rejected a request from the adjunct.
32	CS0/1	C_UNASSIGNED_ NUM	Unassigned number.
33	CS0/21	C_CALL_ REJECTED	Call rejected.
34	CS0/22	C_NUM_ CHANGED	Number changed.
35	CS0/31	C_NORMAL_ UNSPECIF	Normal, unspecified.
36	CS0/34	C_NO_CIRCUIT	No circuit or channel available.
37	CS0/41	C_TEMP_FAILURE	Temporary Failure.
38	CS0/58	C_BEARER_CAP_ UNAVAIL	Bearer capability not presently available.
39	CS0/88	C_INCOMPAT_ DESTINATION	Incompatible destination.
40	CS0/95	C_INVALID_ MESSAGE	Invalid message, unspecified (backward compatibility).
41	CS0/97	C_NON_EXIST_ MESSAGE	Message nonexistent/ not implemented.
42	CS0/127	C_UNSPECIFIED	Unspecified.
43	CS3/19	C_NO_ANSWER	No answer.
44	CS3/20	C_NO_TRUNKS	Trunks not available.
45	CS3/21	C_NO_ CLASSIFIERS	Classifiers not available.
46	CS3/30	C_REDIRECT	Redirected.
47	CS3/38	C_NETWORK_ OUT_OF_ORDER	Network out of order.
48	Undefined	*C_CAUSE_ UNKNOWN	Undefined value returned from the ECS.
49	CS0/52	*C_OUT_CALL_ BARRED	Outgoing call has been barred.

Table 10-5 DEFINITY Cause Values (continued)

ASAI Value	DEFINITY ECS Value	Cause Value	Description
50	CS3/23	C_REMAINS_IN_Q	Call remains in queue.
51	CS0/65	C_BEARER_SVC_ NOT_IMPL	Bearer service not implemented.
52	CS3/17	C_TIMED_ ANSWER	Assumed answer based on internal timer.
53	CS3/18	C_VOICE_ ENERGY_ANSWER	Voice energy detected by the ECS.
54	CS0/82	C_NO_TONE_ CHANNEL	Channel or tone do not exist (no tone connected to the specified call).
55	CS3/24	C_ANSWERING_ MACHINE	Answering machine detected.
56	CS0/29	C_FACILITY_ REJECTED	Facility rejected.
57	CS3/25	C_FORWARD_ BUSY	Redirection cause.
58	CS3/26	C_COVER_BUSY	Redirection cause.
59	CS3/28	C_COV_DONT_ ANS	Redirection cause.
60	CS3/31	C_FORWARD_ALL	Redirection cause.
61	CS3/8	C_LISTEN_ONLY	Single-Step Conference listen only.
62	CS3/9	C_LISTEN_TALK	Single-Step Conference listen-talk.

For example, an ASAI value of 15 corresponds to the DEFINITY ECS value of CSO/17 (C_USER_BUSY).

Table 10-6 Third-party Request/Section in DEFINITY Manual

Third-party Action or Request	Chapter in Manual
Third-party actions via Call Control: Auto Dial (3PAD), Clear (3PCC), Deflect (Redirect) (3PREDIR), Drop (Selective Drop) (3PSD), Listen-Disconnect, Listen-Reconnect, Selective Hold (3PSH), Make Call (3PMC) (or Predictive Call), Relinquish Control (3PRC), Reconnect (Retrieve) (3PR), Send DTMF (3PSDS), Take Control (3PTC)	Chapter 4: ASAI and Call Control

Table 10-6 Third-party Request/Section in DEFINITY Manual

Third-Party actions via Domain Control: Auto Dial (3PAD), Domain Control (3PDC), Answer (3PANS), Merge (Transfer/Conference) (3PM)	Chapter 5: ASAI and Domain Control
Call Routing (RT_REQ, RT_SEL, RT_END)	Chapter 7: ASAI and Call Routing
Agent State change: Login, Logout, Change Workmode: NotReady (AUX), Ready (AVAIL), WorkReady (ACW), and so forth.) Activating/Canceling Call Forwarding Activating/Canceling Send All Calls	Chapter 8: ASAI and Request Feature Capabilities
Value Queries	Chapter 9: ASAI and Value Query Capabilities
Set Value: Message Waiting Indicator (MWI) Set Billing Type	Chapter 10: ASAI and Set Value Capabilities

For example, third-party login requests are discussed in Chapter 8, “ASAI and Request Feature Capabilities.”

IPCC

- MAKE_CALL is only supported when the agent is in the NotReady state. It is not possible for an agent to make new calls when in wrapup mode.
- Consult and blind transfers are supported. However, placing a call on hold, making a new call and then completing the transfer is not supported.
- The consult call must be in the Talking state before the Transfer/Conference can be completed. Therefore, if an Alternate is done in the middle of a Transfer/Conference, the operation can only be completed after a second Alternate is done to restore status quo.
- Completing a conference or a transfer to a consulted agent on hold is not supported.
- Transferring conferences to an unobserved party is not supported.
- Overlapping transfer and conference consult operations on the same parties are not supported. For example, Agent A calls Agent B. During the conversation, Agent A must conference consult Agent C. Agent B feels that Agent D has more information, so Agent B then transfer consults to Agent D. To end the call, Agent A completes the conference and Agent B completes the transfer. This would fail.
- Only the conference initiator can add parties to the conference.
- Calls do not get queued at the Unified CM but instead at some queue point. Because of this, skill group queue statistics are not available via the QUERY_SKILL_GROUP_STATISTICS_REQ. Service controlled IVRs can be monitored via CTI to get queued and dequeued events, as well as established events.
- RTP_STARTED_EVENT and RTP_STOPPED_EVENT are particular to IPCC to support recording vendors.

- AGENT_PRECALL_EVENT and AGENT_PRECALL_ABORT_EVENT are particular to IPCC. They provide call context data before the routed call arrives.
- A CALL_CONNECTION_CLEARED_EVENT may be received with a cause of CEC_REDIRECTED for the following cases:
  - Agent calls a CTI Route Point and call is directed to another resource
  - Agent calls an IVR and the IVR redirects the call
  - Agent calls a number with a forwarding option turned on
- Only devices that have agents logged in can be monitored via CTI OS. The Unified ICM Peripheral Monitor Table is not supported for the IPCC PG.
- For updated information on the Unified CM Multiline feature, refer to the *Cisco Unified Communication Manager System Guide*.
- The Unified CM Shared line feature (agents share the same extension) is not supported.
- Agent Desk Settings control some agent behaviors. These are configured in Unified ICM and downloaded by the Agent Desktop upon startup. WrapupInMode is the wrapup mode variable for incoming calls and WrapupOutMode is the wrapup mode variable for outgoing calls. The valid values for these parameters are:
  - REQUIRED

    For either incoming or outgoing calls, the agent has no option but to go to the Wrapup state when a call ends. While the agent is on the call, all agent state buttons are disabled. While the agent is in the wrapup state, the Ready and NotReady buttons must be enabled.

    Clicking either the Ready or NotReady buttons must dismiss the Wrapup dialog box and put the agent in the state that was chosen. However, if the wrapup timer has been enabled in the PG configuration and timeout occurs before an agent state is chosen, the agent state automatically changes as follows:

    - If the timeout occured at the end of an incoming call, the agent state changes to Ready.
    - If the timeout occured at the end of an outgoing call, the agent state changes to NotReady.
  - REQUIRED_WITH_DATA

    The same as REQUIRED, but the agent must input some data into the Wrapup dialog box before exiting the dialog box and going to a Ready or NotReady state. This applies only to WrapupInMode.
  - OPTIONAL

    For either incoming or outgoing calls, the agent is able to enter any after call state—Wrapup, Ready or NotReady—by clicking the appropriate button.
  - NOT_ALLOWED

    For either incoming or outgoing calls, the agent is only able to enter the Ready or NotReady states. The wrapup button is disabled.

Points of note for API users:

- If the wrapup mode is REQUIRED_WITH_DATA, SetAgentState for returning to ready or not ready fails with an error code of CF_WRAPUP_DATA_REQUIRED (280) if there is no wrapup data entered into a call.
- If Logout Reason or NotReady Reasons are required, an error of CF_REASON_CODE_REQUIRED (281) isreceived if the reasons are not assigned in set agent state request. You must also create Logout Reason and NotReady Reason dialog boxes in the Reason Code if these properties are required.

For more information about reason code and wrapup modes, see the *Administration Guide for Cisco Unified Contact Center Enterprise and Hosted*.

- The PG also uses the Supervisor Interface periodically to interrogate the switch in order to examine agent configuration change. The period interval is controlled by the Windows Registry entry "MonitorGroupTimerQuery". If there is an agent skill group assignment change, the PG knows only when it next interrogates the switch.

IPCC Error Codes

The following table provides a brief description of the error message and what they indicate

Table 10-7 .Error Code Indicator

Error	Indicates
PERERR_TELDRIVE	The telephony driver layer generated the error.
PERERR_JTCLIENT	The JTAPI client generated the error.
PERERR_JTAPPLAY	The JTAPI application layer generated the error.
PERERR_GW_E	The JTAPI gateway generated the error.
PERERR_CM	Cisco Unified Communications Manager generated the error.

The following table lists error codes and their descriptions:

Note Some of these values are displayed over two lines due to space limitations.

Table 10-8 Error Code Description

Return Value/ Code	Error Message	Description
-1 PERERR_UNKNOWN	Unknown Peripheral Error.	The Peripheral error specified does not exist.
10001 PERERR_TELDRIVE_L OCKTPSERVICES	A logic error occurred prior to Locking TP Services.	The TP Services cannot be locked by the thread because they are already locked. This is a serious logic condition and should be reported/resolved.
10002 PERERR_TELDRIVE_L OCKINSTANCE	A logic error occurred prior to Locking the Client Instance.	The Client Instance cannot be locked by the thread because it is already locked. This is a serious logic condition and should be reported/resolved.
10003 PERERR_TELDRIVE_L OCKTELDRIVELAYER	A logic error occurred prior to Locking the Telephony Driver Layer.	The Telephony Driver Layer cannot be locked by the thread because it is already locked. This is a serious logic condition and should be reported/resolved.

Return Value/ Code	Error Message	Description
10004 PERERR_TELDRIVE_NOINSTRUMENTFOREXTENSION	The extension number specified is not associated with any known instrument.	An instrument with the number specified cannot be found for any instrument. Perhaps an invalid extension was specified.
10101 PERERR_TELDRIVE_AGENTALREADYLOGGEDOUT	The agent is already LOGGED out.	An attempt was made to log out an agent that is already logged out. This attempt failed.
10102 PERERR_TELDRIVE_AGENTALREADYSIGNEDON	The agent is already LOGGED ON.	An attempt was made to log in an agent that is already logged in. This attempt failed.
10103 PERERR_TELDRIVE_AGENTAVAILORWORK	The requested function cannot be performed since the agent is AVAILABLE or in a CALL WORK State.	This can occur when an agent tries to make a call from an AVAILABLE, or WORK state.
10104 PERERR_TELDRIVE_AGENTCANTGOUNVAILABLE	The Agent cannot go UNAVAILABLE due to possible calls.	When this error occurs, the ROUTER did not approve the agent going unavailable. Typically retrying this makes it succeed.
10105 PERERR_TELDRIVE_AGENTNOTINATEAM	Agent is not a TEAM member - cannot make supervisor call.	The agent is trying to make a supervisor assist call but is not a member of a team.
10106 PERERR_TELDRIVE_AGENTRESERVED	Agent is RESERVED - cannot make call.	This error occurs when the agent is trying to make a call or consult call but is currently RESERVED for an incoming call.
10107 PERERR_TELDRIVE_AGENTTEAMNOTFOUND	Internal Logic Error - Agent Team not found.	The agent team specified in the agent object cannot be found. This indicates an internal error that should be reported and resolved.
10108 PERERR_TELDRIVE_BADSTATETRANSITION	The state transition is invalid from the current state.	The routine ValidateAgentPrevalentStateTransition determined that the desired transition was illegal from the current state.
10109 PERERR_TELDRIVE_CALLTYPENOTVALIDFORDIALPLAN	The agent is attempting to make a call that is not valid for their defined call plan.	The call type that the call was classified into is not allowed for the dialed Number Plan used.

Return Value/ Code	Error Message	Description
10111 PERERR_TELDRIVE_CANTGOREADYFROMCURRENTSTATE	Cannot transition to READY from current state.	Based upon transition rules, the agent cannot go READY. Examples: You cannot go READY from TALKING.
10112 PERERR_TELDRIVE_CANTLOGOUTFROMCURRENTSTATE	The agent cannot log out from the current state.	The agent must be NOT READY in order to log out.
13042 PERERR_GW_E_THREADCLEARCALL_DROP_EXCEPTION	JTAPI Gateway - Error on CLEAR CALL operation - Exception.	The routine run in object ThreadClearCall got an exception (not of type CiscoJTapiException) on a call to 'drop'.
13044 PERERR_GW_E_THREADCLEARCONNECTION_UNKNOWN_CONNECTION	JTAPI Gateway - Error on CLEARCONNECTION operation - Unknown connection ID.	
13045 PERERR_GW_E_THREADCONFERENCECALL_ACTIVE_CONN_NOT_TALKING	JTAPI Gateway - Error on CONFERENCE operation - ACTIVE connection not in proper state.	The connection specified in the active connection is not in the TALKING state.
13046 PERERR_GW_E_THREADCONFERENCECALL_BAD_ACTIVE_CONNECTION	JTAPI Gateway - Error on CONFERENCE operation - ACTIVE connection not found.	
13047 PERERR_GW_E_THREADCONFERENCECALL_BAD_HELD_CONNECTION	JTAPI Gateway - Error on CONFERENCE operation - HELD connection not found.	
13048 PERERR_GW_E_THREADCONFERENCECALL_CREATECALL_NULL_CALL	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got a null call returned from 'createcall’.
13049 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_ADDPARTY	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'addparty'.

Return Value/ Code	Error Message	Description
13050 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_CONFERENCE_NEW	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'conference' for the NEW call.
13051 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_CONFERENCE_HELD	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'conference' for the HELD call.
13052 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_CONSULT	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'consult'.
13053 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_CREATECALL	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'consult.
13054 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_SETCONFERENCEENABLE	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'setconferenceenable’.
13055 PERERR_GW_E_THREADCONFERENCECALL_EXCEPTION_SETTRANSFERCONTROLLER	JTAPI Gateway - Error on CONFERENCE operation.	The routine run in object ThreadConferenceCall got an exception (not of type CiscoJTapiException) on a call to 'settransfercontroller'.
13056 PERERR_GW_E_THREADCONFERENCECALL_HELD_CONN_NOT_HELD	JTAPI Gateway - Error on CONFERENCE operation - HELD connection not HELD	The connection passed for the held connection is not in the HELD state.
13057 PERERR_GW_E_THREADCONFERENCECALL_NULL_DIALED_NUMBER	JTAPI Gateway - Error on CONFERENCE operation - Invalid Dialed Number.	A NULL dialed number was specified for the consultation number.
13058 PERERR_GW_E_THREADCONSULTATIONCALL_CREATECALL_NULL_CALL	JTAPI Gateway - Operation error on CONSULT operation.	The routine run in object ThreadConsultationCall got a null call returned from 'createcall.'

Return Value/ Code	Error Message	Description
13059 PERERR_GW_E_THREADCONSULTATIONCALL_EXCEPTION_CONSULT	JTAPI Gateway - Error on CONSULT operation.	The routine run in object ThreadConsultationCall got an exception on a call to 'settransfercontroller'.
13060 PERERR_GW_E_THREADCONSULTATIONCALL_EXCEPTION_CREATECALL	JTAPI Gateway - Error on CONSULT operation.	The routine run in object ThreadConsultationCall got an exception on a call to 'createCal.
13061 PERERR_GW_E_THREADCONSULTATIONCALL_EXCEPTION_SETCONFERENCEENABLE	JTAPI Gateway - Error on CONSULT operation.	The routine run in object ThreadConsultationCall got an exception on a call to 'setConferenceEnable'.
13062 PERERR_GW_E_THREADCONSULTATIONCALL_INVALID_CONSULT_TYPE	JTAPI Gateway - Error on CONSULT operation - Invalid Consult type.	The type specified is not TRANSFER or CONFERENCE.
13063 PERERR_GW_E_THREADCONSULTATIONCALL_NO_ACTIVE_CONNECTION	JTAPI Gateway - Error on CONSULT operation - No Active Connection.	The ACTIVE connection specified in the request does not exist.
13064 PERERR_GW_E_THREADESCAPESERVICE_CREATECALL_NULL_CALL1	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got a NULL call returned from 'createCall' (method ‘CreateNewCall' in class ThreadEscapeService).
13065 PERERR_GW_E_THREADESCAPESERVICE_CREATECALL_NULL_CALL2	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got a NULL call returned from 'createCall' (method 'CreateConsultCall' in class ThreadEscapeService).
13066 PERERR_GW_E_THREADESCAPESERVICE_CREATECALL_NULL_CALL3	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got a NULL call returned from 'createCall' (method ‘CreateBlindConferenceCall' in class ThreadEscapeService)'.
13067 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CONFERENCE	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'conference' (method ‘CreateBlindConferenceCall' in class ThreadEscapeService)'.

Return Value/ Code	Error Message	Description
13068 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CONNECT	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'connect' (method 'CreateNewCall' in class ThreadEscapeService)’.
13069 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CONSULT1	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'consult' (method 'CreateConsultCall' in class ThreadEscapeService)’.
13070 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CONSULT2	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'consult' (method 'CreateBlindConferenceCall' in class ThreadEscapeService)'.
13071 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CREATECALL1	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'createCall' (method 'CreateNewCall' in class ThreadEscapeService).
13072 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CREATECALL2	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'createCall' (method 'CreateConsultCall' in class ThreadEscapeService).
13073 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_CREATECALL3	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'createCall' (method 'CreateBlindConferenceCall' n class ThreadEscapeService).
13074 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_GETADDRESS	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'getAddress' (method 'CreateNewCall' in class ThreadEscapeService).
13075 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_GETTERMINALS	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got an exception on a call to 'getTerminals' (method 'CreateNewCall' in class ThreadEscapeService).
13076 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_SETCONFERENCEENABLE1	JTAPI Gateway - Error on SUPERVISOR (escape) operation	Got an exception on a call to 'setConferenceEnable' (method 'CreateConsultCall' in class ThreadEscapeService.
13077 PERERR_GW_E_THREADESCAPESERVICE_EXCEPTION_SETCONFERENCEENABLE2	JTAPI Gateway - Error on SUPERVISOR (escape) operation	Got an exception on a call to 'setConferenceEnable' (method 'CreateBlindConference' in class ThreadEscapeService).

Return Value/ Code	Error Message	Description
13078 PERERR_GW_E_THREADESCAPESERVICE_INVALID_EMERGENCY_ALERT_TYPE	JTAPI Gateway - Error on SUPERVISOR (escape) operation - Invalid Alert Type.	The Alert type specified was not CONSULT or BLIND_CONFERENCE.
13079 PERERR_GW_E_THREADESCAPESERVICE_INVALID_SUPERVISOR_ASSIST_TYPE	JTAPI Gateway - Error on SUPERVISOR (escape) operation - Invalid Alert Type.	The Alert type specified was not CONSULT or BLIND_CONFERENCE.
13080 PERERR_GW_E_THREADESCAPESERVICE_NO_TERMINAL_LIST	JTAPI Gateway - Error on SUPERVISOR (escape) operation.	Got a NULL terminal list from 'getTerminals' (method 'CreateNewCall' in class ThreadEscapeService).
13081 PERERR_GW_E_THREADHOLDCALL_CALL_NOT_CONTROLLED	JTAPI Gateway - Error on HOLD operation - Uncontrolled Call.	The call specified is not a controlled call.
13082 PERERR_GW_E_THREADHOLDCALL_EXCEPTION_HOLD	JTAPI Gateway - Error on HOLD operation - Exception.	Got an exception on a call to 'hold' (method 'run' in class ThreadHoldCall).
13083 PERERR_GW_E_THREADMAKECALL_CREATECALL_NULL_CALL	JTAPI Gateway - Error on MAKE CALL operation - Can't create call.	Got a NULL call returned from 'createCall' (method 'run' in class ThreadMakeCall).
13084 PERERR_GW_E_THREADMAKECALL_CREATE_CALL_FAILURE	JTAPI Gateway - Error on MAKE CALL operation - Can't create call.	Got an exception on a call to 'createCall' (method 'run' in class ThreadMakeCall).
13085 PERERR_GW_E_THREADMAKECALL_GENERIC_CM_ERROR	JTAPI Gateway - Error on MAKE CALL operation - Exception.	Got an exception on a call to 'connect' (method 'run' in class ThreadMakeCall).
13086 PERERR_GW_E_THREADMAKECALL_NULL_TERMINAL_LIST	JTAPI Gateway - Error on MAKE CALL operation.	Got a NULL terminal list returned from 'getTerminals' (method 'run' in class ThreadMakeCall).
13087 PERERR_GW_E_THREADMAKECALL_PROVIDER_GETADDRESS	JTAPI Gateway - Error on MAKE CALL operation.	Got an exception on a call to 'getAddress' (method 'run' in class ThreadMakeCall).
13088 PERERR_GW_E_THREADMAKECALL_PROVIDER_GETTERMINAL	JTAPI Gateway - Error on MAKE CALL operation.	Got an exception on a call to 'getTerminals' (method 'run' in class ThreadMakeCall).

Return Value/ Code	Error Message	Description
13089 PERERR_GW_E_THREADREDIRECTCALL_EXCEPTION_REDIRECT	JTAPI Gateway - Error on REDIRECT operation - Exception.	Got an exception on a call to 'redirect' (method 'run' in class ThreadRedirectCall).
13090 PERERR_GW_E_THREADRETRIEVECALL_CALL_NOT_CONTROLLED	JTAPI Gateway - Error on RETRIEVE operation - Uncontrolled Call.	The call specified is not a controlled call.
13091 PERERR_GW_E_THREADRETRIEVECALL_EXCEPTION_UNHOLD	JTAPI Gateway - Error on RETRIEVE operation - Exception.	Got an exception on a call to 'unhold' (method 'run' in class ThreadRetrieveCall).
13092 PERERR_GW_E_THREADSENDDTMF_EXCEPTION_GENERATEDTMF	JTAPI Gateway - Error on SEND DTMF operation - Exception.	Got an exception on a call to 'generateDTMF' (method 'run' in class ThreadSendDTMF).
13093 PERERR_GW_E_THREADSENDDTMF_INVALID_CONNECTION	JTAPI Gateway - Error on SEND DTMF operation - Invalid Connection ID.	The method 'run' in class ThreadSendDTMF got a null connection from a call to 'findTerminalConnection'.
13094 PERERR_GW_E_THREADSENDDTMF_NOT_MEDIATERMINALCONNECTION	JTAPI Gateway - Error on SEND DTMF operation - No Media.	
13095 PERERR_GW_E_THREADSUPERVISECALL_ACTIVE_CONN_NOT_TALKING	JTAPI Gateway - Error on SUPERVISE operation - ACTIVE connection not in proper state.	The connection specified in the active connection is not in the TALKING state.
13096 PERERR_GW_E_THREADSUPERVISECALL_ALREADY_BARGED_IN	JTAPI Gateway - Error on SUPERVISE operation - Cannot Barge in, already barged into.	The call specified on the barge in request has already been barged into.
13097 PERERR_GW_E_THREADSUPERVISECALL_CREATECALL_NULL_CALL	JTAPI Gateway - Error on SUPERVISE operation - Can't create call.	The routine run in object ThreadSuperviseCall got a null call returned from 'createcall'.
13098 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_ANSWER1	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'answer' (method 'DirectSupervisorBargeIn' in class ThreadSuperviseCall).

Return Value/ Code	Error Message	Description
13099 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_ANSWER2	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'answer' (method 'BargeInBlindConferenceCall' in class ThreadSuperviseCall).
13100 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_CONFERENCE1	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'conference' (method 'SupervisorBargeInCall' in class ThreadSuperviseCall).
13101 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_CONFERENCE2	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'conference' (method 'DirectSupervisorBargeIn' in class ThreadSuperviseCall).
13102 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_CONSULT	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'conference' (method 'DirectSupervisorBargeIn' in class ThreadSuperviseCall).
13103 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_CREATECALL	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'createCall' (method 'DirectSupervisorBargeIn' in class ThreadSuperviseCall).
13104 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_DISCONNECT1	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'disconnect' (method 'DropSupervisorCall' in class ThreadSuperviseCall).
13105 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_DISCONNECT2	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'disconnect' (method 'InterceptCall' in class ThreadSuperviseCall).
13106 PERERR_GW_E_THREADSUPERVISECALL_EXCEPTION_SETCONFERENCEENABLE	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'disconnect' (method 'DirectSupervisorBargeIn' in class ThreadSuperviseCall).
13107 PERERR_GW_E_THREADSUPERVISECALL_HELD_CONN_NOT_HELD1	JTAPI Gateway - Error on SUPERVISE operation - HELD connection is not HELD.	The connection specified for the HELD call is not in the held state (method 'BargInCall' class ThreadSuperviseCall).
13108 PERERR_GW_E_THREADSUPERVISECALL_HELD_CONN_NOT_HELD2	JTAPI Gateway - Error on SUPERVISE operation - HELD connection is not HELD.	The connection specified for the HELD call is not in the held state (method 'DirectSupervisorBargeIn' class ThreadSuperviseCall).

Return Value/ Code	Error Message	Description
13109 PERERR_GW_E_THREADSUPERVISECALL_INVALID_ACTION	JTAPI Gateway - Error on SUPERVISE operation - Invalid action. The action specified was not CLEAR, BARGE_IN or INTERCEPT.	
13110 PERERR_GW_E_THREADSUPERVISECALL_INVALID_ACTIVE_CONNECTION	JTAPI Gateway - Error on SUPERVISE operation - No ACTIVE connection.	The connection specified in the active connection does not exist.
13111 PERERR_GW_E_THREADSUPERVISECALL_INVALID_AGENT_CALLID1	JTAPI Gateway - Error on SUPERVISE operation - Bad Call ID.	The call ID in the agent object is invalid (method 'BargeInCall' class ThreadSuperviseCall).
13112 PERERR_GW_E_THREADSUPERVISECALL_INVALID_AGENT_CALLID2	JTAPI Gateway - Error on SUPERVISE operation - Bad Call ID.	The call ID in the agent object is invalid (method 'DirectSupervisorBargeIn' class ThreadSuperviseCall).
13113 PERERR_GW_E_THREADSUPERVISECALL_INVALID_AGENT_CONNECTION1	JTAPI Gateway - Error on SUPERVISE operation - Bad Connection ID.	The connection ID in the agent object is invalid (method 'BargeInCall' class ThreadSuperviseCall).
13114 PERERR_GW_E_THREADSUPERVISECALL_INVALID_AGENT_CONNECTION2	JTAPI Gateway - Error on SUPERVISE operation - Bad Connection ID.	The connection ID in the agent object is invalid (method 'InterceptCall' class ThreadSuperviseCall).
13115 PERERR_GW_E_THREADSUPERVISECALL_INVALID_HELD_CONNECTION	JTAPI Gateway - Error on SUPERVISE operation - Invalid HELD connection.	The connection ID in the agent object is invalid (method 'BargeInCall' class ThreadSuperviseCall).
13116 PERERR_GW_E_THREADSUPERVISECALL_INVALID_SUPERVISOR_CONNECTION1	JTAPI Gateway - Error on SUPERVISE operation - Invalid Supervisor connection.	The connection ID in the agent object is invalid (method 'DropSupervisorCall' class ThreadSuperviseCall).
13117 PERERR_GW_E_THREADSUPERVISECALL_INVALID_SUPERVISOR_CONNECTION2	JTAPI Gateway - Error on SUPERVISE operation - Invalid Supervisor connection.	The connection ID in the agent object is invalid (method 'BargeInCall' class ThreadSuperviseCall).

Return Value/ Code	Error Message	Description
13118 PERERR_GW_E_THREADSUPERVISECALL_INVALID_SUPERVISOR_CONNECTION3	JTAPI Gateway - Error on SUPERVISE operation - Invalid Supervisor connection.	The connection ID in the agent object is invalid (method 'DirectSupervisorBargeIn' class ThreadSuperviseCall).
13119 PERERR_GW_E_THREADSUPERVISECALL_INVALID_SUPERVISOR_CONNECTION4	JTAPI Gateway - Error on SUPERVISE operation - Invalid Supervisor connection.	The connection ID in the agent object is invalid (method 'BargeInBlindTransferCall' class ThreadSuperviseCall).
13120 PERERR_GW_E_THREADSUPERVISECALL_SUPERVISOR_NOT_TALKING	JTAPI Gateway - Error on SUPERVISE operation - Supervisor Connection not TALKING.	The supervisor's connection is not in the talking state (method 'DirectSupervisorBargeIn' class ThreadSuperviseCall).
13121 PERERR_GW_E_THREADTRANSFERCALL_ACTIVE_CONN_NOT_TALKING	JTAPI Gateway - Error on SUPERVISE operation - Connection not TALKING.	The connection is not in the talking state (method 'BargeInCall' class ThreadSuperviseCall).
13122 PERERR_GW_E_THREADTRANSFERCALL_EXCEPTION_SETTRANSFERCONTROLLER	JTAPI Gateway - Error on SUPERVISE operation - Exception.	method 'run' in class ThreadTransferCall Got an exception on a call to 'setTransferController'.
13123 PERERR_GW_E_THREADTRANSFERCALL_EXCEPTION_TRANSFER1	JTAPI Gateway - Error on SUPERVISE operation - Exception.	method 'run' in class ThreadTransferCall Got an exception on a call to 'transfer' with the HELD call specified.
13124 PERERR_GW_E_THREADTRANSFERCALL_EXCEPTION_TRANSFER2	JTAPI Gateway - Error on SUPERVISE operation - Exception.	Got an exception on a call to 'transfer' with the ACTIVE call specified. (method 'run' in class ThreadTransferCall)
13125 PERERR_GW_E_THREADTRANSFERCALL_HELD_CONN_NOT_HELD	JTAPI Gateway - Error on TRANSFER operation HELD connection not HELD.	The connection passed for the held connection is not in the HELD state.
13126 PERERR_GW_E_THREADTRANSFERCALL_INVALID_ACTIVE_CONNECTION	JTAPI Gateway - Error on TRANSFER operation - No ACTIVE.	The connection specified in the active connection does not exist.

Return Value/ Code	Error Message	Description
13127 PERERR_GW_E_THREADTRANSFERCALL_INVALID_HELD_CONNECTION	JTAPI Gateway - Error on TRANSFER operation Invalid HELD connection.	The connection id in the agent object is invalid.
20000 PERERR_CM_UNSPECIFIED	An unspecifiedCall Manager - error occurred on the operation.	
20001 PERERR_CM_TIMEOUT	A time-out CallManager - occurred on the operation.	An operation exceeded the time limit that was configured/allocated for that operation.
20002 PERERR_CM_NO_ACTIVE_DEVICE_FOR_THIRDPARTY	CallManager - Undescribed Error.	
20003 PERERR_CM_EXISTING_FIRSTPARTY	CallManager - Line was specified that was not found.	
20004 PERERR_CM_ILLEGAL_HANDLE	CallManager - Handle is unknown to the system.	
20005 PERERR_CM_UNDEFINED_LINE	CallManager - Undescribed Error.	
20006 PERERR_CM_ILLEGAL_CALLINGPARTY	CallManager - Attempt to originate call using a calling party that is not on the device.	
20007 PERERR_CM_CALL_ALREADY_EXISTS	CallManager - Another call already exists on the line.	
20008 PERERR_CM_LINECONTROL_FAILURE	CallManager - Line control refuses to let a new call because of it's state (probably bug).	
20009 PERERR_CM_ILLEGAL_CALLSTATE	CallManager - Line is not in a legal state to invoke the command.	
20010 PERERR_CM_CALLHANDLE_NOTINCOMINGCALL - CallManager	Attempt to answer a call that either does not exist or is not in the correct state.	

Return Value/ Code	Error Message	Description
20011 PERERR_CM_TRANSFERFAILED_DESTINATION_UNALLOCATED	CallManager - Attempt to transfer to a directory number that is not registered.	
20013 PERERR_CM_TRANSFERFAILED_DESTINATION_BUSY	CallManager - Attempt to transfer to a busy destination.	
20014 PERERR_CM_TRANSFERFAILED	CallManager - Transfer failed.	Probable cause is one of the call legs was hung up or disconnected from the far end.
20015 PERERR_CM_HOLDFAILED	CallManager - Hold was rejected by line control or call control.	
20017 PERERR_CM_RETRIEVEFAILED	CallManager - Retrieve was rejected by line control or call control.	
20018 PERERR_CM_DB_NO_MORE_DEVICES	CallManager - Error No longer used.	
20020 PERERR_CM_DB_ILLEGAL_DEVICE_TYPE	CallManager - Error No longer used.	
20021 PERERR_CM_DB_ERROR	CallManager - Device query contained an illegal device type.	
20022 PERERR_CM_CANNOT_TERMINATE_MEDIA_ON_PHONE	CallManager - Media cannot be terminated by an application when the device has a physical phone (the phone always terminates the media).	
20025 PERERR_CM_UNKNOWN_GLOBAL_CALL_HANDLE	CallManager - Error no longer used.	
20026 PERERR_CM_DEVICE_NOT_OPEN	CallManager - Command issued on a line that must be open.	
20027 PERERR_CM_ASSOCIATED_LINE_NOT_OPEN	CallManager - Undescribed Error.	
20028 PERERR_CM_SSAPI_NOT_REGISTERED	CallManager - Redirect command was issued when the internal supporting interface was not initialized.	

Return Value/ Code	Error Message	Description
20029 PERERR_CM_REDIRECT_CALL_DOES_NOT_EXIST	CallManager - Attempt to redirect a call that does not exist or is no longer active.	
20048 PERERR_CM_REDIRECT_CALLINFO_ERR	CallManager - Internal error returned from call control.	
20049 PERERR_CM_REDIRECT_ERR	CallManager - Internal error returned from call control.	
20050 PERERR_CM_REDIRECT_CALL_CALL_TABLE_FULL	CallManager - Internal error returned from call control.	
20051 PERERR_CM_REDIRECT_CALL_PROTOCOL_ERROR	CallManager - Internal error returned from call control.	
20052 PERERR_CM_REDIRECT_CALL_UNKNOWN_DESTINATION	CallManager - Attempt to redirect to an unknown destination.	
20053 PERERR_CM_REDIRECT_CALL_DIGIT_ANALYSIS_TIMEOUT	CallManager - Internal error returned from call control	
20054 PERERR_CM_REDIRECT_CALL_MEDIA_CONNECTION_FAILED	CallManager - Internal error returned from call control.	
20055 PERERR_CM_REDIRECT_CALL_PARTY_TABLE_FULL	CallManager - Internal error returned from call control.	
20056 PERERR_CM_REDIRECT_CALL_ORIGINATOR_ABANDONED	CallManager - Far end hung up on the call being redirected.	
20057 PERERR_CM_REDIRECT_CALL_UNKNOWN_PARTY	CallManager - Internal error returned from call control.	
20058 PERERR_CM_REDIRECT_CALL_INCOMPATIBLE_STATE	CallManager - Internal error returned from call control.	

Return Value/ Code	Error Message	Description
20059 PERERR_CM_REDIRECT_CALL_PENDING_REDIRECT_TRANSACTION	CallManager - Internal error returned from call control.	
20060 PERERR_CM_REDIRECT_CALL_UNKNOWN_ERROR	CallManager - Internal error returned from call control.	
20061 PERERR_CM_REDIRECT_CALL_NORMAL_CLEARING	CallManager - Internal error returned from call control.	
20062 PERERR_CM_REDIRECT_CALL_UNRECOGNIZED_MANAGER	CallManager - Internal error returned from call control.	
20063 PERERR_CM_REDIRECT_CALL_DESTINATION_BUSY	CallManager - Redirect destination is busy.	
20064 PERERR_CM_REDIRECT_CALL_DESTINATION_OUT_OF_ORDER	CallManager - Redirect destination is out of order.	
20065 PERERR_CM_CANNOT_OPEN_DEVICE	CallManager - Device open failed because the associated device is shutting down (unregistering).	
20066 PERERR_CM_TRANSFERFAILED_OUTSTANDING_TRANSFER	CallManager - Existing transfer still in progress.	
20067 PERERR_CM_TRANSFERFAILED_CALLCONTROL_TIMEOUT	CallManager - Expected response from call control not received during a transfer.	
20068 PERERR_CM_CALLHANDLE_UNKNOWN_TO_LINECONTROL	CallManager - Attempt to redirect call that was unknown to line control.	
20069 PERERR_CM_OPERATION_NOT_AVAILABLE_IN_CURRENT_STATE	CallManager - Undescribed Error.	

Return Value/ Code	Error Message	Description
20070 PERERR_CM_CONFERENCE_FULL	CallManager - Undescribed Error.	
20071 PERERR_CM_MAX_NUMBER_OF_CTI_CONNECTIONS_REACHED	CallManager - Undescribed Error.	
20080 PERERR_CM_INCOMPATIBLE_PROTOCOL_VERSION	CallManager - Undescribed Error.	
20081 PERERR_CM_UNRECOGNIZABLE_PDU	CallManager - QBE protocol error (bug).	
20082 PERERR_CM_ILLEGAL_MESSAGE_FORMAT	CallManager - QBE protocol error (bug).	
20094 PERERR_CM_DIRECTORY_TEMPORARY_UNAVAILABLE	CallManager - Undescribed Error.	
20095 PERERR_CM_DIRECTORY_LOGIN_NOT_ALLOWED	CallManager - Undescribed Error.	
20096 PERERR_CM_DIRECTORY_LOGIN_FAILED	CallManager - Login to the directory server failed when opening the provider.	
20097 PERERR_CM_PROVIDER_NOT_OPEN	CallManager - Attempt to issue a CTI command before the provider was open.	
20098 PERERR_CM_PROVIDER_ALREADY_OPEN	CallManager - Attempt to reopen a provider.	
20099 PERERR_CM_NOT_INITIALIZED	CallManager - Attempt to open a provider before CTI initialization completes.	
20100 PERERR_CM_CLUSTER_LINK_FAILURE	CallManager - Link failed to one of the call managers in the cluster (network error).	
20101 PERERR_CM_LINE_INFO_DOES_NOT_EXIST	CallManager - Undescribed Error.	

Return Value/ Code	Error Message	Description
20102 PERERR_CM_DIGIT_GENERATION_ALREADY_IN_PROGRESS	CallManager - Undescribed Error.	
20103 PERERR_CM_DIGIT_GENERATION_WRONG_CALL_HANDLE	CallManager - Undescribed Error.	
20104 PERERR_CM_DIGIT_GENERATION_WRONG_CALL_STATE	CallManager - Undescribed Error.	
20105 PERERR_CM_DIGIT_GENERATION_CALLSTATE_CHANGED	CallManager - Undescribed Error.	
20112 PERERR_CM_RETRIEVEFAILED_ACTIVE_CALL_ON_LINE	CallManager - Undescribed Error.	
20113 PERERR_CM_INVALID_LINE_HANDLE	CallManager - Undescribed Error.	
20114 PERERR_CM_LINE_NOT_PRIMARY	CallManager - Undescribed Error.	
20115 PERERR_CM_CFWDALL_ALREADY_SET	CallManager - Undescribed Error.	
20116 PERERR_CM_CFWDALL_DESTN_INVALID	CallManager - Undescribed Error.	
20117 PERERR_CM_CFWDALL_ALREADY_OFF	CallManager - Undescribed Error.	
20119 PERERR_CM_DEVICE_OUT_OF_SERVICE	CallManager - Undescribed Error.	
20120 PERERR_CM_MSGWAITING_DESTN_INVALID	CallManager - Undescribed Error.	
20121 PERERR_CM_DARES_INVALID_REQ_TYPE	CallManager - Undescribed Error.	

Return Value/ Code	Error Message	Description
20122 PERERR_CM_CONFERENCE_FAILED	CallManager - Undescribed Error.	
20123 PERERR_CM_CONFERENCE_INVALID_PARTICIPANT	CallManager - Undescribed Error.	
20124 PERERR_CM_CONFERENCE_ALREADY_PRESENT	CallManager - Undescribed Error.	
20125 PERERR_CM_CONFERENCE_INACTIVE	CallManager - Undescribed Error.	
20126 PERERR_CM_TRANSFER_INACTIVE	CallManager - Undescribed Error.	
20153 PERERR_CM_COMMAND_NOT_IMPLEMENTED_ON_DEVICE	CallManager - Device does not support the command.	Undescribed Error.
20512 PERERR_CM_PROVIDER_CLOSED	CallManager - Undescribed Error.	
20513 PERERR_CM_PROTOCOL_TIMEOUT	CallManager - Undescribed Error.	
24095 PERERR_CM_GENERAL	CallManager - Unknown CallManager Failure on Operation.	An error response was received for a request issued to the call manager, but no error code could be extracted. This is always the case in the Encore Release. Please refer to the JTAPI log for more information.

Nortel Symposium

- The Peripheral Gateway (and thus CTI OS clients) do not receive a CallEstablished Event for an off-switch call. As a result of this limitation, the feature *conference operation on off-switch* is not supported. The soft phone receives no notification that the call has been connected off-switch, and thus the application requires manual intervention from the agent (who heard a dial-tone, a ring, or an answer, and so forth) before completing the conference or transfer operation.
- The Transfer button is not enabled after an off-switch consult.
- Single-step conference is not supported.
- Consultative Transfer to a Supervisor is not supported.

- Users are unable to transfer to an AgentID.
- Users are unable to put a conference or consultative call on hold, therefore the button is disabled.
- There is a delay when switching from the NotReady state to the Ready state.
- There is no equivalent to the Symposium state WalkAway. The ACD gives a NOT_READY state to Unified ICM, but the switch rejects a request to set WalkAway to Not_Ready.
- Third-party call control and agent control requests issued through the CTI Server interface sometimes return a Peripheral error code in the failure indication message if the request fails. For the Nortel Symposium, this Peripheral error code is either a Status value or a Cause value. Generally, Status values are returned for call requests such as MakeCall and Cause values are returned for agent control requests such as SetAgentState. The Nortel Symposium Status and Cause values are defined in Table 10-9 and Table 10-10.
- The ALTERNATE_CALL request is supported with the Nortel Symposium with "NortelSwapPatchInstalled" registry set to 1 in the PG registry "KEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\InstancenameXX\PGXX\PG\CurrentVersion\PIMS\pimXX\SymposiumData\Config" (see Table 10-3).

Table 10-9 Nortel Status Values

Status Value (hex/dec)	Description
Invalid Parameters	
0A00 / 2560	Invalid calling TN
0A01 / 2561	Invalid calling DN; wrong DN specified
0A02 / 2562	Incomplete calling DN
0A03 / 2563	Invalid called DN
0A04 / 2564	Incomplete called DN
0A05 / 2565	Invalid called TN
0A06 / 2566	Invalid origination manner
0A07 / 2567	Invalid destination manner
0A08 / 2568	Invalid origination user type
0A09 / 2569	Invalid customer number
0A0A / 2570	System or data base error
Unsuccessful Call Origination	
0B00 / 2816	Origination party busy
0B01 / 2817	Origination resource blocking
0B02 / 2818	Origination set is maintenance busy
0B03 / 2819	500/2500 set is onhook
0B04 / 2820	Origination DN busy
0B05 / 2821	Origination is ringing
0B06 / 2822	Unable to disconnect origination (that is, already disconnected)
0B07 / 2823	Origination access restriction blocking

Table 10-9 Nortel Status Values (continued)

Status Value (hex/dec)	Description
0B08 / 2824	Origination call on permanent hold
0B0A / 2826	System or data base error
0B0B / 2827	Origination receiving end to end signaling
0B0C / 2828	The call is currently in an ACD queue
0B0E / 2830	Origination set invoked hold
0B14 / 2836	Transfer key not configured
0B15 / 2837	Transfer key not idle
0B16 / 2838	Set active in conference call
0B17 / 2839	Transfer or MPO/TSA class of service not configured
0B18 / 2840	Cannot put call on hold
0B1D / 2845	No active call exists on set
0B1E / 2846	No held call exists on set
Unsuccessful Call Termination	
0C00 / 3072	Terminating party is busy
0C01 / 3073	Destination resource blocking
0C02 / 3074	Destination in invalid state
0C07 / 3079	Destination access restriction blocking
0D0A / 3338	System or database error
Network Interceptions	
0C08 / 3080	Unassigned number
0C09 / 3081	No route to destination
0C0A / 3082	No user responding
0C0B / 3083	Number changed
0C0C / 3084	Destination out of service
0C0D / 3085	Invalid number format
0C0E / 3086	No circuit available
0C0F / 3087	Network out of order
0C10 / 3088	Temporary failure
0C11 / 3089	Equipment congestion
Network Interceptions with In-Band Information	
0C19 / 3097	Terminating party is busy
0C1A / 3098	Unassigned number
0C1B / 3099	No route to destination
0C1C / 3100	No user responding
0C1D / 3101	Number changed

Table 10-9 Nortel Status Values (continued)

Status Value (hex/dec)	Description
0C1E / 3102	Destination out of service
0C1F / 3103	Invalid number format
0C20 / 3104	No circuit available
0C21 / 3105	Network out of order
0C22 / 3106	Temporary failure
0C23 / 3107	Equipment congestion
0C24 / 3108	Interworking, unspecified
0CFE / 3326	Other cause
Unsuccessful Conference or Transfer Operation	
0D00 / 3328	Cannot complete conference
0D01 / 3329	Cannot initiate transfer
0D02 / 3330	Cannot complete transfer
0D03 / 3331	Cannot retrieve original call
0D04 / 3332	Fast Transfer initiation failed
0D05 / 3333	Fast Transfer completion failed
0D0B / 3339	Hold Request failed

Table 10-10 Nortel Cause Values

Cause Value (hex/dec)	Description
1002 / 4098	Access restricted
1003 / 4099	Resource unavailable
1004 / 4100	Invalid customer number
1005 / 4101	Invalid origination address
1006 / 4102	Invalid destination address
1007 / 4103	Invalid manner
1008 / 4104	Unsuccessful retrieve original
1009 / 4105	Unsuccessful transfer
100A / 4106	Unsuccessful conference
100B / 4107	Unsuccessful answer request
100C / 4108	Unsuccessful release request
1070 / 4208	Refer to Connection Status IE
2004 / 8196	The target DN is invalid
2005 / 8197	The target DN is not AST
2006 / 8198	The Customer Number is invalid
2007 / 8199	The feature could not be invoked

Table 10-10 Nortel Cause Values (continued)

Cause Value (hex/dec)	Description
2008 / 8200	The feature is not configured on the set
2009 / 8201	The requested feature is out of valid range
200A / 8202	The target set is not ACD agent
200B / 8203	The target set is a Virtual Agent
200C / 8204	The set is maintenance busy
200D / 8205	Set is in wrong state for invocation
200E / 8206	Set is in target state
200F / 8207	No NRDY/RDY while ACD set is logged out
2010 / 8208	Package C customer cannot use NRDY with IDN call
2011 / 8209	Feature IE is missing or invalid
2012 / 8210	DN IE is missing or invalid
2013 / 8211	Agent ID IE is missing or invalid
2014 / 8212	Agent ID is invalid
2015 / 8213	CFW DN IE is invalid
2016 / 8214	The Call Forward DN is too long
2017 / 8215	The Call Forward DN is invalid
2018 / 8216	User is invoking Call Forward
2019 / 8217	MSB/MSI not supported for 500/2500 sets
201A / 8218	500/2500 ACD agent already changed status
201B / 8219	500/2500 ACD agent set is being rung
201C / 8220	User is manually logging in 500 /2500 ACD set

Swap Feature in Symposium ACD

The Swap feature enables the agents to swap or alternate between customer calls and consult calls, both from hardphones as well as softphones.

The Swap feature deploys a CTI toolbar with Unified ICM, offering most of the phone set functionalities. One of the most important functionalities is that it allows the agent to swap or alternate between primary and consult calls during a Consultation Call.

The agent performing the transfer must carry out a swap, or alternate between the primary key (ACD or DN) and the secondary key of transfer. On the phone set, a swap can be performed by using the transfer or primary key of the used line (ACD or DN).

Note The Swap feature is supported from the following ICM versions: 05.0(00) SR13(00), 07.0(00) SR02(00), 06.0(00) SR05(00). The Swap feature is not supported when CTI OS is used with the Symposium.

Dependencies and patches for the Swap feature support in SoftPhones and HardPhones

The following patches are required for Swap feature support.

Symposium SCCS 5.0

- SU 05
- SUS0501/02/03
- NN_SCCS_5.0_DP_050302_S [mandatory]
- NN_SCCS_5.0_DP_050301_S [optional]

NCCM 6.0

- SU03
- SUS0301
- PEP_030130_RU

Nortel CS1000 Succession 4.0 or 4.5

- MPLR20429
- MPLR21764

Enabling Swap Feature on Unified ICM

The Swap feature can be enabled with the help of Config REGISTRY Key called NortelSwapPatchInstalled. This key is created when the patch is installed. Set the value of this registry key to 1 before starting the PG.

If there are multiple instances of symposium PG in the same box, the registry NortelSwapPatchInstalled must be set to 1 for all the PG instances. This allows the CTI OS server to enable the alternate button on the client desktop.

Rockwell Spectrum

- The dialed number is used for AgentID, AgentExtension, and AgentInstrument, except during agent login.
- In order to perform an agent login, the SET_AGENT_STATE_REQ message must contain the actual agent ID value in the AgentID field instead of the dialed number, and the logical workstation number must be provided in the PositionID field.
- For the Login request, the user is required to enter the AgentID, AgentInstrument and the PositionID. PositionId in this case is an indication of the physical device (phone). Due to the peculiarity of the communication between the switch and the PIM, the Agent softphone freezes if an INVALID AgentInstrument is provided with a VALID AgentID and VALID PositionID. To fix this issue, a Spectrum-specific registry key has been added that provides a timeout interval for the Login request. This is set to 60 seconds by default. If your particular configuration calls for a different value (network response time must be taken into account), change the following registry key to the appropriate value:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\
  <CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\
  AllDesktops\Login\ConnectionProfiles\Name\Spectrum\LoginTimeout
  ```

- Call Alerting (CallDelivered, LocalConnectionState = LCS_ALERTING) is not available.

- When a call is Conferenced, both the original call and the consult call continue to exist as independent calls. Therefore, both calls appear on the Controller's Call Appearance grid. The Controller can control each call individually. If the Controller wants to drop out of the Conference, he must perform a Transfer between the other two parties so they can continue talking.
- Held and Retrieved events are only reported on client controlled calls unless you are using Spectrum Release 7.1a or later.
- The AgentInstrument field in the ANSWER_CALL_REQ message is required.
- The logical workstation number of the agent answering a call, if known, is placed in the LastRedirectDeviceID field in the CALL_ESTABLISHED_EVENT.
- Blind Conference is not supported.
- There is no CTI support for answering a specific call. An agent can be made to go Available when a call is alerting so it can be auto-answered.
- Spectrum requires the AgentID field to contain the AgentInstrument (also known as AgentExtension) for all agent control requests except for the login. For the login request, it requires the actual AgentID (assuming that AgentID is distinct from AgentInstrument and AgentExtension).
- Agent is required to be in the NotReady state to either make a call or to log out.
- A logout request needs a Reason code.
- Transfer and Conference behavior is modeled after hardphone behavior. To initiate a Transfer or a Conference, you must first use the MakeCall control (Transfer Init and Conference Init buttons are unavailable at this point) to make a second (consult) call. After you make this call, the Transfer Complete and Conference Complete buttons become available to complete the desired action.

Agent States

This section presents the agent-state terminology and functionality used by CTI OS Server and how it corresponds to the terminology and functionality of various call center peripherals.

Table 10-11 Agent State Functionality and Call Center Terminology

State	Peripheral-Specific Equivalent
Available The agent is ready to accept a call.	*Alcatel*: **Idle** *Aspect Contact Server*: **Avail** *Avaya DEFINITY ECS*: **AVAIL** *Nortel Symposium*: **Idle**
BusyOther The agent is busy performing a task associated with another active Skill Group.	*Alcatel*: **no equivalent** (only one Skill Group) *Aspect Contact Server*: **MSG** (if Aspect Event Link is not being used) *Avaya DEFINITY ECS*: **OTHER** *Nortel Symposium*: **no equivalent** *Rockwell Spectrum*: **Busy** (on either an internal call or a call for an agent group other than the agent's primary group)

Table 10-11 Agent State Functionality and Call Center Terminology (continued)

State	Peripheral-Specific Equivalent
Hold The agent currently has all calls on hold.	*Alcatel*: **Busy** *Aspect Contact Server*: **HOLD** *Avaya DEFINITY ECS*: **no equivalent** *Nortel Symposium*: **On Hold**, **On Hold Walkaway** *Rockwell Spectrum*: **no equivalent**
Login The agent has logged in to the ACD. It does not necessarily indicate that the agent is ready to accept calls.	Although viewed as a state by CTI Server, this is really more an event than a state, and is not treated as a state by the switches.
Logout The agent has logged out of the ACD and cannot accept any additional calls.	*Alcatel*: **Null/logged off** *Aspect Contact Server*: **Signed Off** *Avaya DEFINITY ECS*: **no equivalent** *Nortel Symposium*: **Logout** *Rockwell Spectrum*: **Signed Off**
NotReady The agent is logged in but is unavailable for any call work.	*Alcatel*: **Pause/Withdrawn/No agent group after login** (preassigned state) *Aspect Contact Server*: **Idle** *Avaya DEFINITY ECS*: **AUX** *Nortel Symposium*: **Not Ready Walkaway** (however, this requires the agent to click Hold and physically unplug the headset – because a physical act is involved, a software request to set the agent state to NotReady fails), **Emergency** *Rockwell Spectrum*: Any state in which the Available console lamp is not lit
Reserved The agent is reserved for a call that arrives at the ACD shortly.	*Alcatel*: **no equivalent** *Aspect Contact Server*: **RSVD** *Avaya DEFINITY ECS*: **no equivalent** *Nortel Symposium*: **Call Presented** *Rockwell Spectrum*: **no equivalent**

Table 10-11 Agent State Functionality and Call Center Terminology (continued)

State	Peripheral-Specific Equivalent
Talking The agent is currently talking on a call (inbound, outbound, or inside).	*Alcatel*: **Busy** *Aspect Contact Server*: **Talking ACD1**, **Talking ACD2**, **Talking ACT1**, **Talking ACT2**, **Talking Out1**, **Talking Out2**, **Talking Inside**, **Supervisor Line**, **MSG**, **HELP** (MSG and HELP correspond to Talking only if Aspect Event Link is being used) *Avaya DEFINITY ECS*: **AUX-IN**, **AUX-OUT**, **ACD-IN**, **ACD-OUT**, **ACW-IN**, **ACW-OUT**, **DACD** *Nortel Symposium*: **Active**, **Consultation** *Rockwell Spectrum*: **Busy** (other than cases listed under BusyOther)
Unknown The agent state is currently unknown.	*Alcatel*: **no equivalent** *Aspect Contact Server*: **no equivalent** *Avaya DEFINITY ECS*: **UNKNOWN** *Nortel Symposium*: **no equivalent** *Rockwell Spectrum*: **no equivalent**
WorkNotReady The agent is performing after-call work and is not ready to receive a call after the work is complete..	*Alcatel*: **no equivalent** *Aspect Contact Server*: **no equivalent** *Avaya DEFINITY ECS*: **no equivalent** *Nortel Symposium*: **no equivalent** *Rockwell Spectrum*: **Call work** (with Available console lamp not lit)
WorkReady The agent is performing after-call work and is ready to receive a call after the work is complete..	*Alcatel*: **Working After Call/Wrapup** (may be manually invoked) *Aspect Contact Server*: **Wrap-up** *Avaya DEFINITY ECS*: **ACW**, **DACW** *Nortel Symposium*: **Not Ready**, **Break**, **Busy** *Rockwell Spectrum*: **Call work** (with Available console lamp lit)

APPENDIX A

Testing an Ethernet Card for Silent Monitor

On a site where IP telephony is or will be deployed, the Unified CM and the IP Phones are normally configured to use a Virtual Local Area Network (VLAN) such that voice is logically separated from data. Although both traffic types are carried on the same physical channel they are transmitted on different VLANs, one for voice and other for data. This configuration allows voice to be transmitted with higher priority than data.

In a call center that will use silent monitor it is required that the agent desktop system be connected to the PC port on the back of the IP phone, such that voice packets reaching the phone can be collected by the silent monitor subsystem to then forward to the supervisor workstation. The agent desktop system will then be using one single physical channel to interact with two different VLANs.

The agent desktop system accesses the physical channel via an Ethernet Network Interface Controller (NIC). The NIC monitors the channel and collects Ethernet frames addressed to the agent's computer. The NIC then runs a preprocessing step to extract IP packets from the Ethernet frames and deliver them to the TCP/IP stack on the operating system.

During internal testing Cisco identified that some Ethernet NIC card drivers available in the market are not capable of pre-processing Ethernet frames that have an IP packet encapsulated in a VLAN frame; that is the NIC card driver will discard the Ethernet frame altogether if the IP packet is encapsulated in an 802.1Q frame. Some vendors can provide a configuration setting that allows their NIC card driver to forward VLAN traffic to the TCP/IP stack.

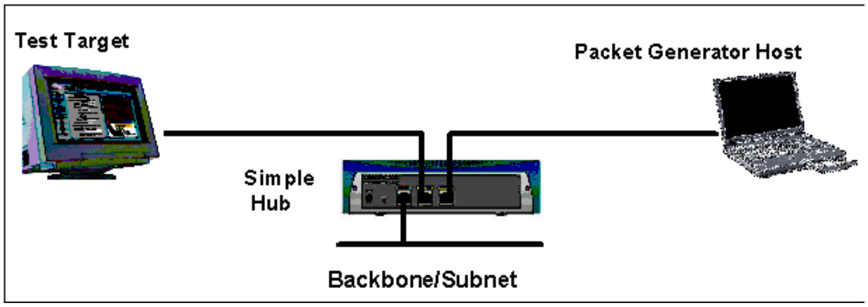
If an agent desktop's NIC card driver discards VLAN traffic, then the silent monitor subsystem on that desktop will not be able to collect and forward voice packets to the supervisor workstation and silent monitor will not function properly. Cisco has developed a procedure to determine if a particular Ethernet NIC card driver will work with CTI OS Silent Monitor. The procedure is described in the following sections.

Test Procedure

The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packets are not discarded by the pre-processing step but are passed onto the TCP/IP stack on the operating system at the computer hosting the NIC card.

The test requires a configuration as shown in the following diagram.

Figure A-1 Silent Monitor Ethernet Card test configuration



The *Test Target NIC* is connected to one port of a simple Hub. The Hub is connected to the network backbone or subnet. You also need a *Packet Generator Host* capable of generating Ethernet traffic. The *Packet Generator Host* will be connected to another port on the Hub.

The *Packet Generator Host* equipment can be either a dedicated packet analyzer or a computer with a software-based packet analyzer with capabilities to generate Ethernet traffic.

There are several software packet analyzers available that can be used for this purpose. For a comprehensive list of reliable analyzers visit the *Cooperative Association for Internet Data Analysis* website at http://www.caida.org/tools/taxonomy/workload.xml.

The following sections demonstrate the use of Sniffer Pro.

After the environment is set up as described above you will must load the software tools on the *Test Target* and *Packet Generator Host* as follows:

Preparing Test Target

Perform the following steps to prepare the test target.

Step 1 Install the *WinPcap* utility. The WinPcap installation program is located at the root directory on the Cisco Computer Telephony Integration CTI Object Server CD.

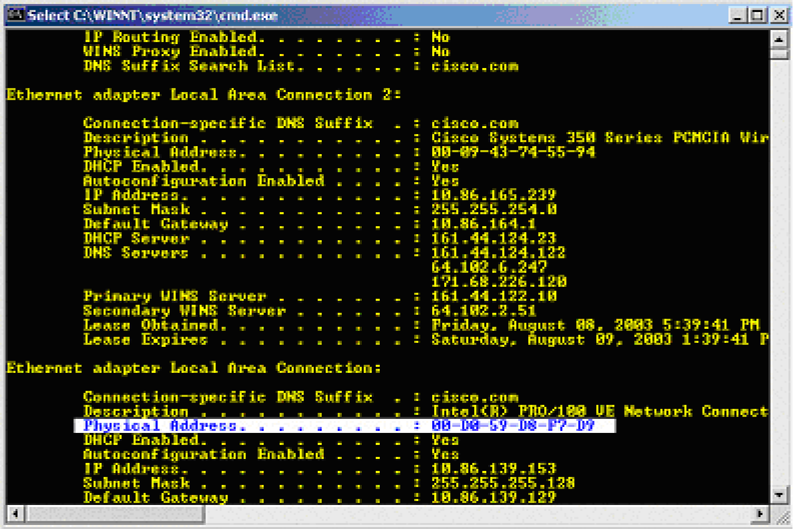
Step 2 Create a directory on the *Test Target* computer named “VLANTest”.

Step 3 From the Cisco Computer Telephony Integration CTI Object Server CD, copy *WinDump.exe* and place it in the directory you created in Step 2. (*WinDump is located on the CD under CtiOS\Tools\VLANTest\WinDump*.)

Step 4 Open a console window. Go to the directory where you copied WinDump.exe.

Step 5 Determine the MAC address of the *Test Target NIC* by executing ***ipconfig /all*** at the command prompt. Write down the number that appears for the Physical Address. For example, the “Intel Pro/100” NIC card has a MAC address of **00D059d8f7d9**.

Figure A-2 Determining the Test Target NIC Mac address



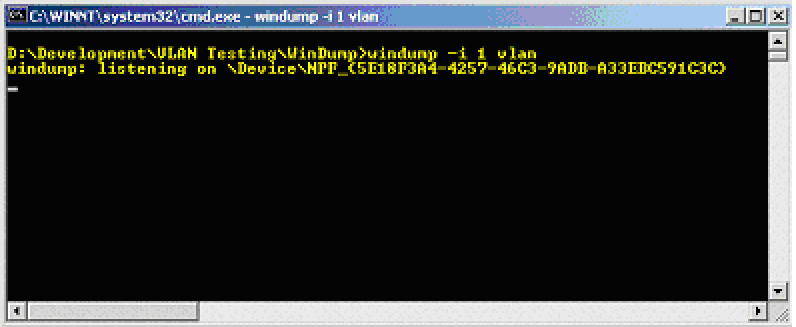
```
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : cisco.com

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : cisco.com
        Description . . . . . . . . . . . : Cisco Systems 350 Series PCMCIA Wir
        Physical Address. . . . . . . . . : 00-09-43-74-55-94
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.86.165.239
        Subnet Mask . . . . . . . . . . . : 255.255.254.0
        Default Gateway . . . . . . . . . : 10.86.164.1
        DHCP Server . . . . . . . . . . . : 161.44.124.23
        DNS Servers . . . . . . . . . . . : 161.44.124.122
                                            64.102.6.247
                                            171.68.226.120
        Primary WINS Server . . . . . . . : 161.44.122.10
        Secondary WINS Server . . . . . . : 64.102.2.51
        Lease Obtained. . . . . . . . . . : Friday, August 08, 2003 5:39:41 PM
        Lease Expires . . . . . . . . . . : Saturday, August 09, 2003 1:39:41 P

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : cisco.com
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connect
        Physical Address. . . . . . . . . : 00-D0-59-D8-F7-D9
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.86.139.153
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 10.86.139.129
```

Step 6 Determine the device interface number of the *Test Target NIC*. Execute ***windump –D*** and write down the number of the NIC you want to test. In this example, you would choose interface number 1, which corresponds to the “Intel Pro/100” NIC card.

Note If you are not sure which number to pick, repeat the test for each card until the test succeeds for one (sufficient to pass) or this fails for all cards.

Step 7 Start WinDump to monitor the *Test Target NIC* for incoming VLAN packets. To do this execute ***windump –i <device_number> vlan***. In the following example the *device_number* is 1.

Figure A-3 Monitoring the Test Target NIC for incoming VLAN packets



```
D:\Development\VLAN Testing\WinDump>windump -i 1 vlan
windump: listening on \Device\NPF_{5E18F3A4-4257-46C3-9ADD-A33EDC591C3C}
_
```

Preparing Packet Generator Host

Perform the following steps to prepare the packet generator host.

Step 1 Load the packet analyzer software onto your *Packet Generator Host*.

Step 2 Load the sample capture file provided in the Cisco Computer Telephony Integration CTI Object Server CD (Ctios\Tools\VLANTest\VLANCapture\VLANSamplePackets.cap). The capture file was generated in a format that is used by most dedicated and software packet analyzers.

Step 3 Select the Decode view from the tab at the bottom of the screen.

Executing Test

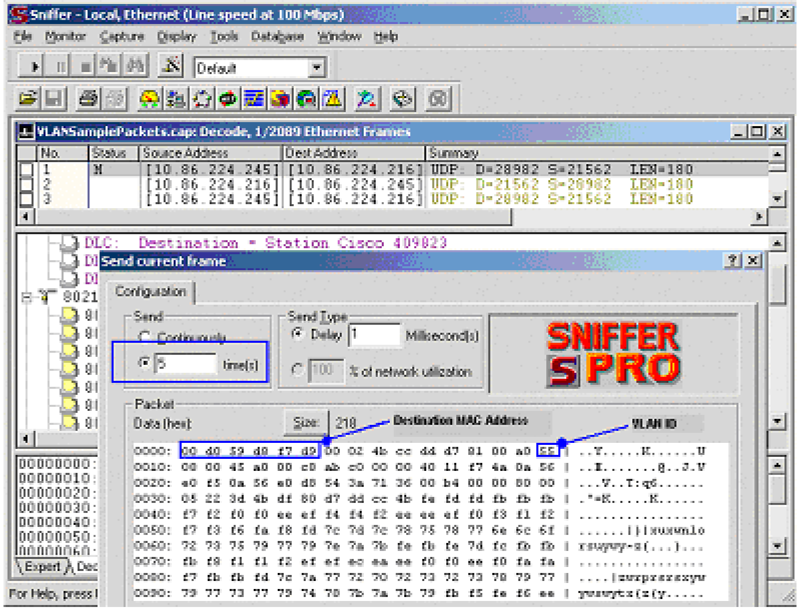
The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packet is not discarded by the pre-processing step but is passed onto the TCP/IP stack on the computer hosting the NIC card.

The test case to determine whether or not the *Test Target NIC* is qualified to work with CTI OS Silent monitor is as follows. (In the test case nomenclature, PA stands for Packet Analyzer and WD stands for WinDump.)

SMNIC- 1 Send Sample VLAN Packets to Test Target NIC Card

Objective	Verify that the Test Target NIC is able to pre-process VLAN packets and forward them to the TCP/IP stack on the Test Target Host.	
Steps	**Party**	**Action**
1	PA	Select one of the loaded sample VLAN Packets.
2	PA	Select or right-click “Send Current Frame”.
3	PA	Modify the destination MAC address to use the MAC address of the Test target NIC. See Figure A-4.
4	PA	Send five times the new frame to the Test Target NIC.
5	WD	Verify that there is activity reported on the *Test Target NIC*.
Expected Result	At the *Test Target* computer *windump* will display five packets for VLAN ID = 85 as shown in Figure A-5. If the test fails, no packets are displayed.	

Figure A-4 Modifying the Destination MAC address


Sniffer - Local, Ethernet (Line speed at 100 Mbps)
File Monitor Capture Display Tools Database Window Help
Default
VLANSamplePackets.cap: Decode, 1/2089 Ethernet Frames
Send current frame
Configuration
SNIFFER
S PRO
Destination MAC Address
VLAN ID
Expert Dec
For Help, press

No.	Status	Source Address	Dest Address	Summary
1	M	[10.86.224.245]	[10.86.224.216]	UDP: D=28982 S=21562 LEN=180
2		[10.86.224.216]	[10.86.224.245]	UDP: D=21562 S=28982 LEN=180
3		[10.86.224.245]	[10.86.224.216]	UDP: D=28982 S=21562 LEN=180

DLC: Destination = Station Cisco 409823

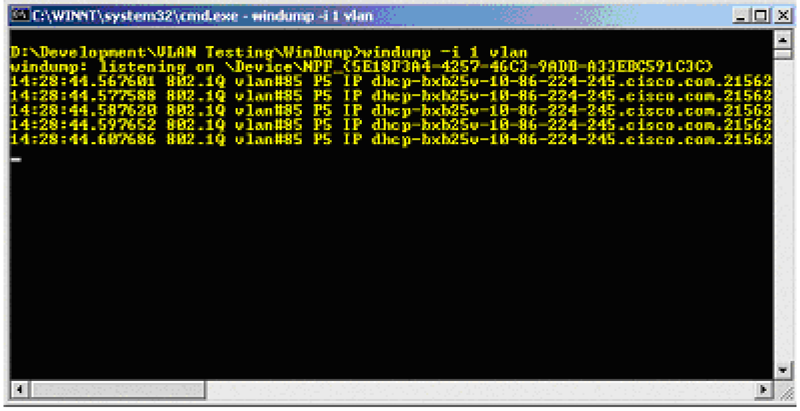
Send: ○ Continuously ● 5 time(s)

Send Type: ● Delay 1 Millisecond(s) ○ 100 % of network utilization

Packet Data (hex): Size: 218

```
0000: 00 d0 59 d8 f7 d9 00 02 4b cc dd d7 81 00 a0 55 | ..Y.....K......U
0010: 00 00 45 a0 00 c0 ab c0 00 00 40 11 f7 4a 0a 56 | ..E.......@..J.V
0020: a0 f5 0a 56 a0 d8 54 3a 71 36 00 b4 00 00 80 00 | ...V..T:q6......
0030: 05 22 3d 4b df 80 d7 dd cc 4b fe fd fd fb fb fb | ."=K.....K......
0040: f7 f2 f0 f0 ee ef f4 f4 f2 ee ee ef f0 f3 f1 f2 | ................
0050: f7 f3 f6 fa f8 fd 7c 7d 7c 78 75 78 77 6e 6c 6f | ......|}|xuxwnlo
0060: 72 73 75 79 77 79 7e 7a 7b fe fb fe 7d fc fb fb | rsuywy~z{...}...
0070: fb f8 f1 f1 f2 ef ef ec ea ee f0 f0 ee f0 fa fa | ................
0080: f7 fb fb fd 7c 7a 77 72 70 72 73 72 73 78 79 77 | ....|zwrprsrsxyw
0090: 79 77 73 77 79 74 78 7b 7a 7b 79 fb f5 fe f6 ee | ywswytx{z{y.....
```

Figure A-5 Sample Output Showing Successful Packet Capture



```
D:\Development\VLAN Testing\WinDump>windump -i 1 vlan
windump: listening on \Device\NPF_{5E18F3A4-4257-46C3-9ADD-A33EDC591C3C}
14:28:44.567601 802.1Q vlan#85 P5 IP dhcp-bxb25v-10-86-224-245.cisco.com.21562
14:28:44.577588 802.1Q vlan#85 P5 IP dhcp-bxb25v-10-86-224-245.cisco.com.21562
14:28:44.587620 802.1Q vlan#85 P5 IP dhcp-bxb25v-10-86-224-245.cisco.com.21562
14:28:44.597652 802.1Q vlan#85 P5 IP dhcp-bxb25v-10-86-224-245.cisco.com.21562
14:28:44.607686 802.1Q vlan#85 P5 IP dhcp-bxb25v-10-86-224-245.cisco.com.21562
_
```

If the outcome of this test is successful, then your *Test Target NIC* will work with CTI OS Silent Monitor. Otherwise, contact your NIC card provider and ask what settings are necessary to allow your NIC card driver to forward all packets including VLAN packets to the TCP/IP stack on the computer so that your packet analyzer tool can capture and display them. Then apply the appropriate adjustments and rerun this test procedure.

INDEX