CTI OS System Manager's Guide for Cisco
ICM/IPCC Enterprise & Hosted Editions

Cisco CTI OS Release 7.2(1)
May 2007
Contents

About This Guide ix
  Purpose ix
  Audience ix
  Conventions ix
  Organization x
  Other Publications x
  Obtaining Documentation xi
    Cisco.com xi
    Product Documentation DVD xi
    Ordering Documentation xi
  Documentation Feedback xii
  Field Alerts and Field Notices xii
  Cisco Product Security Overview xii
    Reporting Security Problems in Cisco Products xiii
  Obtaining Technical Assistance xiii
    Cisco Technical Support & Documentation Website xiii
    Submitting a Service Request xiv
    Definitions of Service Request Severity xiv
  Obtaining Additional Publications and Information xv

Chapter 1 1-1

Introduction 1-1
  Overview of CTI OS 1-1
    Advantages of CTI OS as Interface to ICM 1-2
    Key Benefits of CTI OS for CTI Application Developers 1-2
  System Manager Responsibilities 1-3
  System Requirements 1-4
    Desktop User Accounts 1-4
  Silent Monitoring 1-4
    Differences Between CCM and CTI OS Silent Monitor 1-5
    CCM Based Silent Monitoring 1-5
      CCM Silent Monitor Advantages 1-6
      CCM Silent Monitor Limitations/Restrictions 1-6
    CTI OS Based Silent Monitoring 1-7
Network Topology for Silent Monitoring 1-8
CCM Based Silent Monitoring 1-8
CTI OS Based Silent Monitoring 1-8
Silent Monitoring and System IPCC 1-9
Silent Monitoring and Citrix 1-10
Silent Monitoring and Mobile Agent 1-10
Calculating Additional Needed Bandwidth 1-11

CHAPTER 2
Release 7.0(0) CTI OS Server Installation 2-1
CTI OS Server Installation Guidelines 2-1
Upgrading from a Previous Version 2-2
Installing CTI OS Server 2-3
Uninstalling CTI OS Server 2-15
Determining Version Number of Installed Files 2-15

CHAPTER 3
Release 7.0(0) CTI Toolkit Desktop Client Installation 3-1
Upgrading from a Previous Version 3-2
Cisco CTI Toolkit Desktop Client Component Installation 3-2
Installed Files 3-5
Uninstalling CTI Toolkit 3-8
Determining Version Number of Installed Files 3-8
CallManager Intercept Configuration Requirement 3-9
Configuring Supervisory Assistance Features 3-9

CHAPTER 4
Installing & Configuring CTI OS Silent Monitor 4-1
Installing CTI OS Release 7.1(1) (or later) 4-1
Installing and Configuring the Silent Monitor Service 4-1
Silent Monitor Service Overview 4-2
How Desktops Connect to Silent Monitor Services 4-2
Silent Monitor Service Installers 4-3
Signing Silent Monitor Server Certificate Request with Self Signed CA 4-5
Signing Silent Monitor Service Certificate Request with Third Party CA 4-6
Additional Configuration Steps 4-7
Rerun CTI OS Server Setup 4-7
Installing and Configuring the Silent Monitor Service in a Traditional IPCC Environment 4-7
Installing and Configuring the Silent Monitor Service in a Citrix /WTS Environment 4-7
Additional Configuration for Mobile Agent Environments 4-7
Silent Monitor Service Clusters 4-8
Installing and Configuring the Silent Monitor Service with Windows Firewall Service Enabled 4-8
Silent Monitor Server Security Hardening Procedure 4-9
Silent Monitor Service Deployments 4-9
  IPCC Deployment 4-10
  Citrix Deployment 4-10
  Mobile Agent 4-11
  Mobile Agent with Citrix 4-12

CHAPTER 5
Installing, Uninstalling, and Failed Installation Recovery of CTI OS Release 7.x(x) Components 5-1
  Silent Installation of CTI OS Release 7.x(x) Components 5-1
    Creating a Response File 5-2
    Running CTI OS Silent Install on Other Machines 5-2
  Uninstalling Release 7.x(x) Components 5-3
  Recovering from a Failed Installation of CTI OS Release 7.x(x) 5-3

CHAPTER 6
Configuring CCM Based Silent Monitor 6-1
  CCM Configuration and Administration 6-1
    Enable “Built in Bridge” for the Agent’s Device 6-1
    Add PG User to “Standard CTI Allow Call Monitor” 6-2
    Monitoring Calling Search Space 6-2
    Monitoring Notification Tone 6-4
  CTI OS 6-5
    Restrictions 6-6
      Phones 6-6
      Cisco CallManager 6-6
      CTI OS Desktop Versions 6-6
      Remote Agents 6-6
      Recording Applications 6-7
      Transfer and Conferencing Monitored Calls 6-7

CHAPTER 7
CTI OS Security 7-1
  Configuring CTI OS Security Certificate 7-1
  CTI OS Security Setup Programs 7-1
  Signing CTI Toolkit Desktop Client Certificate Request with Self Signed CA 7-2
  Signing CTI Toolkit Desktop Client Certificate Request with Third Party CA 7-3
  Signing CTI OS Server Certificate Request with Self Signed CA 7-2
  Signing CTI OS Server Certificate Request with Third Party CA 7-3
CONTENTS

CTI OS Security Passwords 7-4
CTI OS Security Registry Keys 7-5
Security Compatibility 7-6
  Wire Level Encryption 7-6
  Authentication Mechanism 7-8

CHAPTER 8
CTI OS Configuration 8-1
  Using the Windows Registry Editor 8-2
    Note About Registry Directories in Previous CTI OS Releases 8-3
    Configuring the Silent Monitor Type for CTI OS 8-3
  CTI Driver 8-3
  EMS Tracing Values 8-5
  Server 8-6
    Agent 8-7
      ReasonCodes 8-8
      WrapupStrings 8-9
      CallObject 8-9
    Connections 8-11
    Device 8-11
    Peers 8-12
    Peripherals 8-12
    SkillGroup 8-13
    Supervisor 8-14
    TimerService 8-14
  MainScreen 8-15
  Configuring IPCC Silent Monitor 8-15
  Defining Connection Profiles 8-16
    SilentMonitorService Subkey 8-19
  Declaring ECC Variables 8-20
  Configuring the Call Appearance Grid 8-20
    Automatic Call Appearance Grid Configuration 8-23
  Automatic Agent Statistics Grid Configuration 8-25
  Automatic Skill Group Statistics Grid Configuration 8-26
  Configuring Additional Peripherals 8-28
  Quality of Service/Type of Service (QoS/ToS) 8-28
    Basic Configuration 8-29
    Important Additional Configuration 8-29
    Caveats 8-30
About This Guide

Purpose

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

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.

Conventions

This manual uses the following conventions.

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

The manual is divided into the following chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introduction”</td>
<td>Provides an overview of Cisco CTI Object Server (CTI OS) and lists the tasks that a CTI OS system manager must perform.</td>
</tr>
<tr>
<td>Chapter 2, “Release 7.0(0) CTI OS Server Installation”</td>
<td>Provides procedures for installing CTI OS Server.</td>
</tr>
<tr>
<td>Chapter 3, “Release 7.0(0) CTI Toolkit Desktop Client Installation”</td>
<td>Provides procedures for installing CTI OS Client components.</td>
</tr>
<tr>
<td>Chapter 4, “Installing &amp; Configuring CTI OS Silent Monitor”</td>
<td>Discusses the process of installing the new functionality in CTI OS Release 7.1(1) (or later).</td>
</tr>
<tr>
<td>Chapter 5, “Installing, Uninstalling, and Failed Installation Recovery of CTI OS Release 7.x(x) Components”</td>
<td>This chapter discusses the silent installation and uninstallation of CTI OS Release 7.x(x) components. In addition, it discusses the steps necessary to recover from a failed installation of CTI OS components.</td>
</tr>
<tr>
<td>Chapter 6, “Configuring CCM Based Silent Monitor”</td>
<td>Discusses how to configure devices and JTAPI users on CCM 6.0 to enable silent monitor.</td>
</tr>
<tr>
<td>Chapter 8, “CTI OS Configuration”</td>
<td>Explains how to start and stop CTI OS and its associated processes and describes how CTI OS handles failover scenarios.</td>
</tr>
<tr>
<td>Chapter 9, “Startup, Shutdown, and Failover”</td>
<td>Discusses how to use the Windows Registry Editor to configure CTI OS.</td>
</tr>
<tr>
<td>Chapter 10, “Peripheral-Specific Support”</td>
<td>Discusses levels of CTI OS support for switch-specific features.</td>
</tr>
<tr>
<td>Appendix A, “Testing an Ethernet Card for Silent Monitor”</td>
<td>Discusses testing an ethernet card for silent monitor, including test target preparation, preparing the packet generator host, and test execution.</td>
</tr>
</tbody>
</table>

Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software and Cisco Computer Telephony Integration (CTI) products, see the Cisco web site listing ICM and CTI documentation.
Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport

You can access the Cisco website at this URL:
http://www.cisco.com

You can access international Cisco websites at this URL:

Product Documentation DVD

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

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

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

Cisco Ordering tool:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

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

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:
• Instructions for ordering documentation using the Ordering tool are at this URL:
• Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Field Alerts and Field Notices

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

Cisco Product Security Overview

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

From this site, you can perform these tasks:
• Report security vulnerabilities in Cisco products.
• Obtain assistance with security incidents that involve Cisco products.
• Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:
http://www.cisco.com/go/psirt

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

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

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

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

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

Tip

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

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


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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

### Submitting a Service Request

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


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

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

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

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


### Definitions of Service Request Severity

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

- **Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- **Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- **Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- **Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.
Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
  http://www.cisco.com/go/marketplace/

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

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

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
  http://www.cisco.com/go/iqmagazine
  or view the digital edition at this URL:
  http://ciscoiq.texterity.com/ciscoiq/sample/

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

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

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

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

Overview of CTI OS

The Computer Telephony Integration Object Server (CTI OS) is Cisco’s next generation customer contact integration platform. 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 with 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.

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 ICM**

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 all 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.

- **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.

  \[\text{Note}\] 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 it 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 Cisco ICM Software CTI OS Developer’s Guide for an explanation of these two modes.

- **Fault tolerant.** CTI OS is built upon the ICM NodeManager 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 Client Interface Library (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 interface 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 reconnect to the same CTI OS Server after restart), reestablish the session, and recover 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 appropriate event interface that suits their needs, or use the IAllInOne interface to subscribe for 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 7.0(0) CTI OS Server (see Chapter 2, “Release 7.0(0) CTI OS Server Installation”).
* Installing Release 7.0(0) CTI Toolkit Agent Desktop, IPCC Supervisor Desktop, Tools, Documentation, Win32 SDK, Java SDK, and .NET SDK. (see Chapter 3, “Release 7.0(0) 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) specific components (see Chapter 4, “Installing & Configuring CTI OS Silent Monitor”).
* Installing Release 7.2(x) specific components (see Chapter 6, “Configuring CCM Based 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 ICM 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 appropriate Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials). This document is available at: http://www.cisco.com/en/US/products/sw/customsw/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 Enterprise, 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 in 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 CallManager (CCM) or CTI OS.

Each CTI OS Server can be configured for either CCM based or CTI OS based silent monitoring.
Differences Between CCM and CTI OS Silent Monitor

Besides the differences in implementation CTI OS and CCM silent monitor also differ in when they can be invoked and when they end.

Table 1-1  CCM Based and CTI OS Based Silent Monitor Differences

<table>
<thead>
<tr>
<th>CCM Based Silent Monitor</th>
<th>CTI OS Based Silent Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>The supervisor can only silent monitor an agent who is actively talking in a call.</td>
<td>The supervisor can silent monitor an agent in any state as long as the agent is logged in.</td>
</tr>
<tr>
<td>Cannot silent monitor an agent on hold.</td>
<td>Can silent monitor an agent on hold.</td>
</tr>
<tr>
<td>When agent consults, supervisor must stop silent monitoring held call and start silent monitoring conference.</td>
<td>When agent consults, supervisor automatically hears consult call.</td>
</tr>
<tr>
<td>Supervisor can only silent monitor in not ready state.</td>
<td>Supervisor can silent monitor in any state.</td>
</tr>
<tr>
<td>Supervisor must stop silent monitoring before barging in.</td>
<td>Supervisor can barge-in while silent monitoring.</td>
</tr>
<tr>
<td>When the call that is being silent monitored ends, the silent monitor call ends. The supervisor must re-start silent monitor once the agent answers another call.</td>
<td>When call ends, supervisor will automatically silent monitor the next call as long as the supervisor has not stopped silent monitoring.</td>
</tr>
</tbody>
</table>

CCM Based Silent Monitoring

CCM based Silent Monitor provides a supervisor with a means to listen in on agent calls in IPCC call centers that use Cisco CallManager version 6.0 and higher. Supervisors can send Silent Monitor requests to monitor agents without the agent being aware of any monitoring activity. When the CCM based approach is adopted for silent monitoring, the agent's phone is used to mix the media streams of the agent's call. The mix is then sent to the supervisor's phone.
**CCM Silent Monitor Advantages**

CCM 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 was carried on the data LAN.
- Silent monitor calls are reported as agent-to-agent calls for supervisors. With CTI OS silent monitor, supervisor’s time spent silent monitoring is not tracked.

**CCM Silent Monitor Limitations/Restrictions**

The following items prevent the use of CCM based silent monitor:

- Agents using phones other than 79x1 phones (7941, 7961, or 7971)
- Agents using IP communicator
- Supervisors using 7.1(x) or earlier desktops
- IPCC 7.1(x)
- CCM 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 provides a supervisor with a means 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 hardphone are captured from the network and sent to the supervisor’s silent monitor service connected to the supervisor’s desktop. At the supervisor’s silent monitor service, these voice packets are decoded and played on the supervisor’s system sound card.

![Figure 1-3 CTI OS Based Silent Monitor](image)

**Note**
Silent Monitor does not capture and translate DTMF digits that are pressed on either the CTI OS Agent Desktop or on an agent's hardphone.

**Note**
For the agent using the 7941, 7961, 7970, and 7971 phones, these devices need to be configured on the Call Manager CCM Admin 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

CCM Based Silent Monitoring

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

Figure 1-4  CCM 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**

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 hardphone, 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 “silent-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, “Release 7.0(0) 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
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's Citrix clients. The agent Citrix client must be deployed behind the agent's IP phone. The supervisor Citrix client must have a sound card. The necessary network topology is as follows.

For more details on this deployment, see the section Silent Monitor Service Deployments, in Chapter 4, “Installing & 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's silent monitor server.
The necessary network topology is as follows.

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

**Calculating Additional Needed Bandwidth**

Silent Monitoring of an agent consumes roughly 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/warp/public/788/pkt-voice-general/bwidth_consume.html#topic1) 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/warp/public/788/pkt-voice-general/bwidth_consume.html

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.
Release 7.0(0) CTI OS Server Installation

IMPORTANT NOTE: The new CTI OS functionality that is part of Release 7.2(1) is discussed in Chapter 1, “Silent Monitoring”. However, in order to install Release 7.2(1), CTI OS Server Release 7.0(0) must be installed on your system. If you have CTI OS Server Release 7.0(0) installed, proceed to Chapter 6, “Configuring CCM Based Silent Monitor”. If you do not have CTI OS Server Release 7.0(0) installed, follow the procedures in this chapter to install CTI OS Server from the CTI OS CD before you install Release 7.2(1).

This chapter lists some guidelines to consider when you install CTI OS Server and provides procedures for the following tasks.

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

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 would prevent 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 Cisco ICM/IPCC Enterprise & Hosted Editions, Hardware and System Software Specifications (Bill of Materials). 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 release of CTI OS Server, you do not need to uninstall CTI OS Server before you install CTI OS Server Release 7.0(0).

**Step 1**
If you have a version of CTI OS Server already installed, and are attempting to install the latest version, you will get a pop-up window as follows:

---

**Note**
Upgrading directly from the CTI OS Server from version 4.x to 7.0 is not supported. You must either uninstall first, and reinstall version 7.0; or, upgrade first from version 4.x to 5.1, and then perform an upgrade procedure to the CTI OS Server Release 7.0(0).

However, note that the CTI OS Client may be upgraded directly from 4.x to 7.0.

If you click “Yes”, several status dialogs are displayed, informing you that registry entries are being copied, files are being copied, and so forth. When this is done, the Instance dialog will be displayed. Click on “Upgrade All”.

All files that belong to the old version are deleted and the files for the 7.0 version are installed.

You will be asked about whether you want to restart your computer now or later. If you select “Yes” your machine will reboot. If you select “No”, it will return you to the Instance dialog, and you will be able to Edit or Delete the configuration of the server instance.

---

**Note**
- Some important changes from earlier versions of CTI OS Server to 7.0:
  - The CTI OS Server is now only 1 process: “CTIOSServerNode.exe”.
  - There is no more CTIServerDriver.exe.
  - In previous versions, an instance of CTIOS Server could have up to three peer CTIOS Servers configured for chat and Silent Monitoring, and so forth. As of 7.0, because of scalability enhancements making this unnecessary, only one peer CTIOS Server may be configured. Therefore, when upgrading to 7.0, if there are multiple keys under the HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_apple\CTIOS1\Server\Peers

  key, setup will delete all but the 1st key (that is, first alphabetically).
Installing CTI OS Server

If you are performing a new install of the CTI OS Server altogether, 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. These screens are only available after upgrading a CTI OS 7.0 Server.

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

**Step 2** Click **Yes** on the Software License Agreement screen.

**Step 3** Under the CTI OS Instance List, click **Add**. You get the following window.
**Step 4** Enter an instance name. For example, if you have entered an instance called “cisco”, the following window appears:

![CTI OS Server List](image.png)

**Step 5** Now click on **Add** inside the CTI OS Server List. The following window appears.

![Add CTI OS Server](image.png)

**Step 6** 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 pulldown list.

![Enter Desktop Drive](image.png)
**Step 7**  Click OK. The CTI Server Information screen appears.

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

**Step 8**  Click Next. The Peripheral Identifier screen appears.

Specify the following information.
- **A Logical Name** for your peripheral. This can be any valid logical name that uniquely identifies your peripheral.
Installing CTI OS Server

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 will 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 9
Click Next. The Connection Information screen appears.

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 will connect to them with the same port in their installs.
Step 10  Click Next. The Statistics Information screen appears.

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

Note  Since QoS enablement and statistics enablement are mutually exclusive, enabling QoS will zero and disable all of the information relating to statistics.
Step 11  Click Next. The IPCC Silent Monitor Type screen appears.

![IPCC Silent Monitor Type](image)

Step 12  Select the Silent Monitor type.

If **CCM Based** or **Disabled** is chosen, clicking **Next** takes you to the "Peer CTI OS Server" screen. Proceed to **Step 14**.

**Note**  If **CCM Based** is chosen, refer to Chapter 6, “Configuring CCM Based Silent Monitor.”

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

<table>
<thead>
<tr>
<th>Key</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLMSOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_&lt;instance&gt;\CTIOS1\EnterpriseDesktopSettings\AllDesktops\IPCCSilentMonitor\Name\Settings\CCMBasedSilentMonitor</td>
<td>0</td>
</tr>
<tr>
<td>HKLMSOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_&lt;instance&gt;\CTIOS1\EnterpriseDesktopSettings\AllDesktops\Login\ConnectionProfiles\Name\IPCC\IPCCSilentMonitorEnabled</td>
<td>0</td>
</tr>
</tbody>
</table>

If **CTI OS Based** silent monitor is chosen, clicking **Next** takes you to the "Silent Monitor Information" screen. Proceed to **Step 13**.
Step 13  Click Next. The Silent Monitor Information screen appears.

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 may connect to. The desktop will randomly connect to one of the silent monitor servers specified here. If the client is configured to use secure connections, the client will attempt 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 will be established with the silent monitor server. Otherwise, an unsecure connection will be 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 14** Click the Next button. The Peer CTI OS Server screen appears.
Step 15  Alternatively, if you wish to configure a Peer Server for Chat and Silent Monitoring, enter the appropriate information as follows:

![Peer CTIOS Server window]

After you click Add Server, and the files are laid down, 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 will not beep.
**Step 16** Now, the Security installation is launched with the following dialog:

![Security Installation Dialog](image)

If you wish to disable Security, just click **OK**, otherwise, check 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 17  The following window appears if you enable Security:

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

You will be asked about whether you want to restart your computer now or later. If you select Yes your machine will reboot.

Step 18  If you had selected IPCC Hosted Edition and wish to add more instances, you must then restart setup. If, instead, you select No you will see the following:

In this core “CTIOS Instances” dialog, you can then Add more instances, Delete the one you just installed, or you can Edit that one as well.

Note  If you had selected any peripheral type other than “IPCC Hosted Edition”, the “Add” button under the Instance List would be disabled so no more instances can be added.

For “IPCC Hosted Edition” adding an instance will run the entire progression just described above. Editing an instance will display all of the dialogs from the “CTI Server Information” dialog to the end. For either adding or editing instances after the first one, only Services will be registered and Registry settings will be written. That is, the files will only be transferred at the time the first instance is added, since 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 will be 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.
Uninstalling CTI OS Server

To uninstall CTI OS Server, rerun the Setup program for ICM Release 7.0(0) and delete the ICM Customer Instance that you specified during CTI OS Server Setup.

Note

If Release 7.0(0) Service Releases (SRs) or Engineering Specials (ESs) for any CTI OS components are installed on your machine, you must uninstall these before you uninstall the base Release 7.0(0) CTI OS Server software.

Determining Version Number of Installed Files

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

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.

Step 3  Right click on the highlighted file.

Step 4  Select Properties from the dropdown menu. A properties dialog box appears.
**Step 5** Select the **Version** tab. This tab contains version information (release number and build number) for the file.
Release 7.0(0) CTI Toolkit Desktop Client Installation

**IMPORTANT NOTE:** The new CTI OS functionality that is part of Release 7.1(1) is installed by the procedure discussed in Chapter 4, “Installing & Configuring CTI OS Silent Monitor”. However, in order to install Release 7.1(1), CTI Toolkit Desktop Client Release 7.0(0) must first be installed on your system. If you have CTI Toolkit Desktop Client Release 7.0(0) installed, skip this chapter and proceed to Chapter 4, “Installing & Configuring CTI OS Silent Monitor”. If you do not have CTI Toolkit Desktop Client Release 7.0(0) installed, follow the procedures in this chapter to install CTI Toolkit Desktop Client before you install Release 7.1(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.

**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 *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1) Hardware and System Software Specifications (Bill of Materials)*. This document is available at: [http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm](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 do not need to uninstall the CTI Toolkit Desktop Client software before you install CTI Toolkit Desktop Client Release 7.0(0).

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.

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

**Step 4**  Accept the default drive or click the Browse button and specify another drive.
Step 5  Click the Next button. 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 7.1(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 the Next button. If you selected CTI Toolkit Agent Desktop or CTI Toolkit IPCC Supervisor Desktop, the CTIOS Server Information screen appears.

Note  With the 7.0(0) Release, Silent Monitor is no longer a choice to be installed separately. Instead, if you select "Agent Desktop", the agent component for Silent Monitoring (WinPCap) will be automatically installed.

If you select "IPCC Supervisor Desktop", the Silent Monitor components for supervisor are also installed and an additional screen appears first.

Please read this screen carefully; it contains important information about using Silent Monitor in a VLAN network.
Note
Phones configured to use SRTP will not be able to be silent monitored. Customers who wish to Silent Monitor agents must not configure the agent's phone to use SRTP.

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 enable the checkbox at this stage as well.

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 will 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.”

For details about what Security Certificate option you need to select, refer to Chapter 7, “CTI OS Security.”
Step 10  Click OK. You will see the following window:

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

Step 11  You will finally see a Setup Complete screen.

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>
<thead>
<tr>
<th>DLL</th>
<th>Command Line Entry For Manually Registering</th>
</tr>
</thead>
<tbody>
<tr>
<td>msvcrtd.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>msvcp60.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>msvcp60d.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>mfc42.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>mfc42d.dll</td>
<td>Registration not needed.</td>
</tr>
<tr>
<td>atl.dll</td>
<td>regsvr32 atl.dll</td>
</tr>
<tr>
<td>msvbvm60.dll</td>
<td>regsvr32 msvbvm60.dll</td>
</tr>
<tr>
<td>msvbvm60d.dll</td>
<td>regsvr32 msvbvm60d.dll</td>
</tr>
</tbody>
</table>

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

- CtosStatusBar.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 will lay down the following files and install them into the Global Access Cache (GAC):

| AxInterop.AgentSelectCtl.dll | Cisco.CTICOMMONDLMGL.dll | Interop.AgentSelectCtl.dll |
| AxInterop.AgentStateCtl.dll | Cisco.CTIOSSARGUMENTSL.dll | Interop.AgentStateCtl.dll |
| AxInterop.AlternateCtl.dll | Cisco.CTIOSSCLIENT.dll | Interop.AlternateCtl.dll |
| AxInterop.AnswerCtl.dll | Cisco.CTIOSESSIONRESOLVER.dll | Interop.AnswerCtl.dll |
| AxInterop.BadLineCtl.dll | Cisco.INTLRESOURCESLOAD.dll | Interop.BadLineCtl.dll |
| AxInterop.ButtonControl.dll | | Interop.ButtonControl.dll |
| AxInterop.ChatCtl.dll | | Interop.ChatCtl.dll |
| AxInterop.ConferenceCtl.dll | | Interop.ConferenceCtl.dll |
| AxInterop.CTIOSSAgentStatistics.dll | | Interop.CTIOSSAgentStatistics.dll |
| AxInterop.CTIOSCALLAppearance.dll | | Interop.CTIOSCALLAppearance.dll |
| AxInterop.CTIOSSkillGroupStatistics.dll | | Interop.CTIOSSkillGroupStatistics.dll |
| AxInterop.CTIOSSStatusBar.dll | | Interop.CTIOSSStatusBar.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 |
Uninstalling CTI Toolkit

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

Note
If Release 7.0(0) Service Releases (SRs) or Engineering Specials (ESs) for any CTI OS components are installed on your machine, you must uninstall these before you uninstall the base Release 7.0(0) CTI OS Server software.

Determining Version Number of Installed Files

If CTI Toolkit Agent Desktop or CTI Toolkit Supervisor Desktop for IPCC Enterprise 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.

Step 3  Select Properties from the dropdown menu. A properties dialog box appears.

<table>
<thead>
<tr>
<th>AxInterop.SupervisorOnlyCtl.dll</th>
<th>Interop.SupervisorOnlyCtl.dll</th>
</tr>
</thead>
<tbody>
<tr>
<td>AxInterop.TransferCtl.dll</td>
<td>Interop.TransferCtl.dll</td>
</tr>
</tbody>
</table>
Step 4  Select the Version tab. This tab contains version information (release number and build number) for the file.

![ctiosclient.dll Properties](image)

**CallManager Intercept Configuration Requirement**

Cisco CallManager 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, an *ICM system administrator* must perform the following steps.

**Step 1**  Do the following tasks from the ICM Configuration Manager (refer to the *ICM Configuration Guide for ICM Enterprise Edition*).
a. On the Dialed Number List screen, create a Dialed Number for the supervisor, as shown in the following screens.
b. On the Agent Team List screen, enter the Dialed Number in the Supervisor script dialed number field, as shown.

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

a. On the Call Type Manager screen, associate the Dialed Number with your script, as shown.
Installing & Configuring CTI OS Silent Monitor

The process of installing the new functionality in CTI OS Release 7.1(1), or later, involves two steps:

- Downloading and installing the CTI OS Release from the CTI OS Cisco Connection Online (CCO) public download area
- Installing and configuring the CTI OS Silent Monitor Service

This chapter discusses these steps. This chapter also discusses CTI OS silent install of Release 7.1(1), or later, as well as uninstalling the CTI OS Release, and recovery from an unsuccessful Release installation.

Installing CTI OS Release 7.1(1) (or later)

The new CTI OS software functionality that is included in Release 7.x(x) is posted on the Cisco CCO public download area. This area contains updates to the following CTI OS components.

- CTI OS Server
- CTI Toolkit Desktop Applications, including Silent Monitor
- CTI Toolkit

Note

This area does not include an update to the CTI Driver for Siebel 7, as this component is unchanged from Release 7.0(0).

Note

In order to upgrade to Release 7.x(x), Release 7.0(0) or one of its associated service releases of the CTI OS Server and CTI Toolkit Desktop Client must be installed on your system.

To install Release 7.x(x), go to the CTI OS Cisco Connection Online (CCO) public download area at http://www.cisco.com/kobayashi/sw-center/contact_center/ctios/
and follow the posted instructions to download and install the Release 7.x(x) software.

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.
Chapter 4 Installing & Configuring CTI OS Silent Monitor

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 monitor service running on agent or supervisor's desktop computer or Citrix client. This service handles silent monitor functionality for one agent or supervisor. Silent monitor server refers to a silent monitor service providing silent monitor functionality for a group of mobile agents. These agents share the same gateway.

Silent Monitor Service Overview

In CTI OS Release 7.1(1) (or later), 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 a TCP connection. The agent desktop will use the silent monitor service to forward a voice stream to the supervisor's silent monitor service that will play the stream on the supervisor's computer's speaker.

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 and its sniffer 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 is used to play 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 controls calls from customer phones. The other gateway controls agent calls. In this deployment, the silent monitor service is deployed off of 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 playback 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.

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 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 will use the preceding algorithms to determine the address of the silent monitor service. Once determined, desktops will connect using the determined address and the port present in the connection profile.

**Silent Monitor Service Installers**

The Release 7.1(1) (or later) 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 Connection Online (CCO) public download area:

- SilentMonitorInstall_nogui.exe – this executable silently installs the silent monitor service with the following settings:
  - Installed in the directory C:\Program Files\Cisco Systems\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 will work only on 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, 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. Enter the command:

**setup.exe /s**

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.

Either accept the default destination folder or click the **Browse** button and specify another directory.

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

Specify the following information on this screen.
• **Port** – the number of the port on which the silent monitor service listens for incoming connections.

• **Silent Monitor Server** – check this box 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 *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(1) Hardware and System Software Specifications (Bill of Materials)*. This document is available at:


• **Enable Quality of service** – check this box to enable Quality of Service (QoS).

• **Enter peer(s) information** – check this box 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 4-8*.

**Step 4** Click *Next* to finish the installation process.

**Step 5** 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

Following are the necessary 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 will display an error message.

**Step 4** Copy both `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.
Installing and Configuring the Silent Monitor Service

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


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 will display 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

Following are the necessary 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 both 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 then 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 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.

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.

See Chapter 2, “Release 7.0(0) 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 playback 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 will use the silent monitor service that is forwarding traffic from the agent gateway. Please see Chapter 2, “Release 7.0(0) 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 will run Mobile Agent.

- 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 will receive SPAN traffic is connected on port 10, the following commands are used to configure the SPAN session.

```bash
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 silent 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 will need to be at least two profiles for such agents. One profile, used when logging in as IPCC, will 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 monitor 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 login, silent monitor services must be clustered to support silent monitor. A separate silent monitor server must be deployed for each gateway. A SPAN port will need to be configured for each silent monitor server as described in the first bullet. The silent monitor server installer must then be run to install and configure the two silent monitor servers as peers. Once this is done, a connection profile will need to be setup to instruct the agent desktops to connect to one of the peers. (See Chapter 2 for information on the CTI OS Server installer program.) To do this, 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 2003 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
Silent Monitor Server Security Hardening Procedure

ICM Security Hardening can be run only on a Windows 2003 Server. To apply security hardening on a Silent Monitor Server, 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 will create the directory C:\CiscoUtils and copy the corresponding files there.

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

### Step 4
Run the command "cscript ICMSecurityHardening.vbe HARDEN".

If you are using Windows Firewall, you will need to perform the following additional steps to add the Silent Monitor Service as an exception.

### Step 5
From the Windows Control Panel, click on Windows Firewall.

### Step 6
If you see a message "Your PC is not Protected: Turn on Windows Firewall.", turn on Windows Firewall.

### Step 7
From the Windows Firewall dialog box, click on the Exceptions tab.

### Step 8
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**

- When customers upgrade 7.0 desktops to 7.1, the silent monitor service is silently installed on the agent desktop computer.
- Given the desktop is deployed behind the agent’s phone. Silent monitor functionality will be the same as before the upgrade. The only difference being the service and not the CIL is providing 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 localhost if no silent monitor services are configured via 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**

- The 7.1 desktop is installed on the Citrix server.
- If Citrix clients are required to have silent monitor functionality, the silent monitor service will need to 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

- Silent monitor server is installed on a separate computer using the SM SelbstExtractedInstallPackage.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. 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 configured to tell mobile agents how to connect to the silent monitor server(s).
- **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 connected.
  - Locate the port on the switch where the NIC card that will receive SPAN traffic on the silent monitor server is connected.
  - Configure the switch to 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.

```bash
no monitor session 1
monitor session 1 source interface fastEthernet0/10
monitor session 1 destination interface fastEthernet0/15
```
Mobile Agent with Citrix

- 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 will need silent monitor services configured on their Citrix clients.
  - Mobile agents using Citrix will not need silent monitor services configured since the clients will use the silent monitor server configured off of the SPAN port.
Installing, Uninstalling, and Failed Installation Recovery of CTI OS Release 7.x(x) Components

Silent Installation of CTI OS Release 7.x(x) Components

CTI OS Release 7.x(x) 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

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

This 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 all of 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 will install the 7.x(x) release of all CTI OS components (CTI OS Agent Desktop, CTI OS Supervisor Desktop, CTI OS Server) which 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 Cisco Security Agent (CSA) 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(x) installer with the following syntax.

```
CTIOS7[1].1(1).exe -options-record "c:\mypath\myresponsefile.opt"
```

where “c:\mypath\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.

### Step 3
When the installer completes, 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

Once you have created 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) 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 7.x(x) 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.

### Step 4
When the installer completes, 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.
Uninstalling Release 7.x(x) Components

To uninstall all CTI OS Release 7.x(x) components, run Add/Remove programs from the Windows Control Panel and select Cisco CTI OS Release 7.x(x) Uninstall. When you uninstall CTI OS Release 7.x(x) 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. is reverted back to HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems. Also, any registry key changes from HKEY_LOCAL_MACHINE to HKEY_CURRENT_USER are reverted.
- Server registry keys -- any Release 7.x(x) 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, 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), reverts back to the Release 7.1(x) server setup. Selections pertaining to silent monitor type (CCM Based, CTI OS Based, Disabled) are no longer present.
- Client setup -- removed altogether.

Recovering from a Failed Installation of CTI OS Release 7.x(x)

If an attempted CTI OS Release 7.x(x) 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 7.x(x), as documented in the “Uninstalling Release 7.x(x) Components” section on page 5-3.

Step 2  Reinstall Release 7.x(x) by performing the procedures documented in the following sections.

- “Installing CTI OS Release 7.1(1) (or later)” section on page 4-1.
- “Silent Monitor Service Installers” section on page 4-3.
- Additional Configuration Steps, page 4-7.
Recovering from a Failed Installation of CTI OS Release 7.x(x)
CHAPTER 6

Configuring CCM Based Silent Monitor

CCM Configuration and Administration

This section describes how to configure devices and JTAPI users on CCM 6.0 to enable silent monitor.

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)
Add PG User to “Standard CTI Allow Call Monitor”

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

![Application User Configuration (CTI Allow Call Monitoring)](image)

Monitoring Calling Search Space

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

The following screen shot is captured to show the Route Partition on the agent's line appearance page.
Figure 6-3  **Agent Route Partition**

The following screen shot is captured to show the Monitoring Calling Search Space on the supervisor's line appearance page.
Figure 6-4  Supervisor Monitoring Calling Search Space

Monitoring Notification Tone

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

- Play Monitoring Notification Tone to Observed Target
  - When set to true, this option will play the tone to the monitored target (usually an agent).
- Play Monitoring Notification Tone to Observed Connected Target
  - When set to true, this option will play 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 CCM Administration Interface/Select Server/Select Cisco CallManager (active) for Service.

The following screenshot illustrates both tones enabled.
CTI OS

CTI OS Server can be configured to use either CCM 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>\<CTIOS ServerName>\EnterpriseDesktopSettings\All Desktops\IPCCSilentMonitor\Name\Settings\CCMBasedSilentMonitor

This field is a DWORD. If this field is present and is set to 1, CCM 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 CCM based silent monitor. If the server setup program is not run, the CCMBasedSilentMonitor 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

CCM 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 CallManager

Cisco CallManager 6.0 or higher is required.

CTI OS Desktop Versions

CCM 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.

Remote Agents

CCM based silent monitor is only supported for agents who are connected to IPCC on the LAN. CCM based silent monitor is not supported for agents who are connected to IPCC across a WAN.
Recording Applications

Recording applications are able to record agent’s conversations. Recording applications will not interfere with agent desktops while these agents are on calls, including while the agents are being silently monitored.

Transfer and Conferencing Monitored Calls

Supervisors cannot transfer and/or conference silent monitor calls as transfering and/or conferencing silent monitor calls is not supported.
CTI OS Security

This chapter provides information to the System Manager about configuring the CTI OS Security Certificate and the Security Compatibility.

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 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 have been detailed in the following sections.

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 install, and are located in: <drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Toolkit\Win32 CIL\Security directory.

1. The first setup program is called CreateSelfSignedCASetupPackage.exe which creates a self signed certificate authority (CA). This needs to 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 of the files is called CtiosRoot.pem which contains the private CA information. This file must be kept in a safe place. Another file is called CtiosRootCert.pem which contains public CA information. This setup program asks the user to enter a password for the CA (between 8 and 30 characters) which will be used when signing CTI OS certificate requests.

2. The second setup program is called SecuritySetupPackage.exe which is used to generate certificates requests for both CTI Toolkit Desktop Client and CTI OS Server. If the certificate request is for the CTI OS Server, then it will generate CtiosServerKey.pem, and CtiosServerReq.pem. These files will
be used when signing server certificate. If the certificate request is for the CTI Toolkit Desktop Client, then it will generate CtiosClientkey.pem, and CtiosClientreq.pem. These files will be used when signing client certificate.

3. The third setup program is called SignCertificateSetupPackage.exe which 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 where CtiosRootCert.pem, and CtiosRoot.pem are. If the certificate that is going to be signed is for the client, then it will generate CtiosClient.pem file. If the certificate that is going to be signed is for the server, then it will generate CtiosServer.pem file. This program asks the user to enter the following information:

   a. Ctios Certificate Authority Password. This password is the one that was used to create a self signed CA.


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

Following are the necessary steps to sign a CTI Toolkit Desktop Client certificate request:

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

2. **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.

3. **Step 3** 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 will display an error message.

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

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

6. **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**

Following are the necessary steps to sign a CTI OS Server certificate request:

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

2. **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.
Chapter 7 CTI OS Security

Configuring CTI OS Security Certificate

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 will display 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\CTIOS_INSTANCE\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 will display an error message.
   c. Copy CtiosClient.pem to the machine where CTI OS Server resides and save it in <drive>:\ICM\CTIOS_INSTANCE\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

Following are the necessary 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 <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

Following are the necessary steps to sign a CTI OS Server certificate request:
Configuring CTI OS Security Certificate

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 <drive>:\ICM\CTIOS_INSTANCE\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 <drive>:\ICM\CTIOS_INSTANCE\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 5 types of passwords:

1. CTI OS Client certificate password: The administrator/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, also the administrator/installer doesn't need to remember it.

2. CTI OS Server certificate password: The administrator/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, also the administrator/installer doesn't need to remember it.

3. CTI OS Peer certificate password: The administrator/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, also the administrator/installer doesn't need to remember it.

4. Monitor Mode password: The administrator/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 needs to be the same on both CTI OS Peer Servers, also the administrator/installer and whoever is using the CTI OS monitor mode applications needs to remember it.

5. Certificate Authority (CA) password: This password is entered when creating self signed CA. This password can be anything and it needs to be remembered by the administrator/installer because it will be used every time a certificate request is signed by this CA.
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

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthenticationEnabled</td>
<td>DWORD Value</td>
<td>Refer to the Authentication Mechanism section of this document.</td>
<td>1</td>
</tr>
<tr>
<td>CAType</td>
<td>DWORD Value</td>
<td>It 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.</td>
<td>1</td>
</tr>
<tr>
<td>NumBytesRenegotiation</td>
<td>DWORD Value</td>
<td>It 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 it 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.</td>
<td>10000000</td>
</tr>
<tr>
<td>SecurityEnabled</td>
<td>DWORD Value</td>
<td>It 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.</td>
<td>0</td>
</tr>
</tbody>
</table>
The registry keys located at [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTI Desktop\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

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAType</td>
<td>DWORD</td>
<td>It 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.</td>
<td>1</td>
</tr>
<tr>
<td>HandShakeTime</td>
<td>DWORD</td>
<td>It is created at install time. This key defines how long the CTI OS client waits during the SSL/TLS handshake phase.</td>
<td>5</td>
</tr>
</tbody>
</table>

### 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 doesn’t 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, which makes sure that agent, logs in successfully if and only if supplied the correct password.

### Wire Level Encryption

It provides an encryption mechanism between CTI OS Server 7.0 and CTI OS Client 7.0 only. By default, the 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 neither CTI OS 7.0 Clients using .NET CIL nor CTI OS 7.0 Clients using Java CIL nor Siebel Driver can 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

<table>
<thead>
<tr>
<th>Support Wire Level Encryption</th>
<th>C++ CIL Toolkit</th>
<th>COM CIL Toolkit</th>
<th>Java CIL Toolkit</th>
<th>.NET CIL Toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 7-4 contains the compatibility information between CTI OS Server 7.0 and CTI OS Clients 7.0.

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

<table>
<thead>
<tr>
<th>CTI OS Server 7.0 (Security ON)</th>
<th>CTI OS Client 7.0 using C++ CIL toolkit</th>
<th>CTI OS Client 7.0 using COM CIL toolkit</th>
<th>CTI OS Client 7.0 using Java CIL toolkit</th>
<th>CTI OS Client 7.0 using .NET CIL toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CTI OS Client 6.0 and earlier versions using C++ CIL toolkit</th>
<th>CTI OS Client 6.0 and earlier versions using COM CIL toolkit</th>
<th>CTI OS Client 6.0 using Java CIL toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI OS Server 7.0 (Security ON)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CTI OS Server 7.0 (Security OFF)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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.

Table 7-6 contains compatibility information between CTI OS Server 7.0 and CTI OS Clients 7.0.

<table>
<thead>
<tr>
<th>CTI OS Client 7.0 using C++ CIL toolkit</th>
<th>CTI OS Client 7.0 using COM CIL toolkit</th>
<th>CTI OS Client 7.0 using Java CIL toolkit</th>
<th>CTI OS Client 7.0 using .NET CIL toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI OS Server 7.0 (Authentication Enabled)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CTI OS Server 7.0 (Authentication Disabled)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CTI OS Client 6.0 and earlier versions using C++ CIL toolkit</th>
<th>CTI OS Client 6.0 and earlier versions using COM CIL toolkit</th>
<th>CTI OS Client 6.0 using Java CIL toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI OS Server 7.0 (Authentication Enabled)</td>
<td>Yes (*, **)</td>
<td>Yes (*, **)</td>
</tr>
<tr>
<td>CTI OS Server 7.0 (Authentication Disabled)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* CTI OS Agent Desktop, IPCC Supervisor Desktop, and BA Phone always display a CTI Warning containing the following text “Agent with ID <ID> is already logged in to instrument <INSTRUMENT>, even though the agent was not already logged in. This 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>
** If agent A is already logged in to CTIOS Server using either CTI OS Agent Desktop, IPCC Supervisor Desktop, or BA Phone, and agent B is connected to CTIOS Server using either CTI OS Agent Desktop, IPCC Supervisor Desktop, or BA Phone, and trying to log in using agent A’s ID with invalid password, then agent B would receive control failure but the desktop would have All 3 Login, Logout and ready buttons enabled which agent B can use to manipulate agent A’s desktop. If agent B pushes the Ready button, then the button enablement becomes fine. Also, agent B’s desktop always display a CTI Warning containing the following text “Agent with ID <ID> is already logged in to instrument <INSTRUMENT>, even though the agent was not already logged in. This 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>

It also displays a CTI Warning containing the following text “The request specified an invalid agent password”.

CTI OS Configuration

CTI OS Configuration is handled through the Windows Registry Editor. Using the Editor, you can add or 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 topics:

- Using the Windows Registry Editor
- CTI Driver keys
- EMS Tracing keys
- Server keys
- Mainscreen keys
- Connection Profile keys
- Call Appearance keys
- ECC Variable keys
- Peripheral keys

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 ICM/IPCC Enterprise and Hosted Editions*.

---

**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

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 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 CCM 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>\<CTIOServerName> \EnterpriseDesktopSettings\All
Desktops\IPCCSilentMonitor \Name\Settings\CCMBasedSilentMonitor
```

This field is a DWORD and if present and set to “1”, CCM based silent monitor is used. CTI OS based silent monitor is used if this field is not present or 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 CCM 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.

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

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>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientID</td>
<td>String Value</td>
<td>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.</td>
<td>CTIOSServer</td>
</tr>
<tr>
<td>ClientPassword</td>
<td>String Value</td>
<td>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.</td>
<td>CTIOSServer</td>
</tr>
</tbody>
</table>
### Table 8-1 Registry values for [CtiDriver\Config] (continued)

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientSignature</td>
<td>String Value</td>
<td>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.</td>
<td>CTIOSServer</td>
</tr>
<tr>
<td>SideAHost</td>
<td>String Value</td>
<td>The CTI Server (sideA) IP address or hostname to which the CTI OS Server connects.</td>
<td>Host specified during CTI Server installation.</td>
</tr>
<tr>
<td>SideAPort</td>
<td>DWORD Value</td>
<td>The CTI Server (sideA) IP port to which the CTI OS Server connects.</td>
<td>Port specified during CTI Server installation.</td>
</tr>
<tr>
<td>SideBHost</td>
<td>String Value</td>
<td>The CTI Server (sideB) IP address or hostname to which the CTI OS Server connects.</td>
<td>Host specified during CTI Server installation.</td>
</tr>
<tr>
<td>SideBPort</td>
<td>DWORD Value</td>
<td>The CTI Server (sideB) IP port to which the CTI OS Server connects.</td>
<td>Port specified during CTI Server installation.</td>
</tr>
<tr>
<td>Heartbeat Interval</td>
<td>DWORD Value</td>
<td>The interval (in seconds) at which HEARTBEAT_REQ messages are sent to the CTI Server.</td>
<td>5</td>
</tr>
<tr>
<td>ServicesMask</td>
<td>DWORD Value</td>
<td>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_bld1\CTIOS1\CtiDriver\Config</td>
<td>0x00000296 (52) (default)</td>
</tr>
<tr>
<td>CallMsgMask</td>
<td>DWORD Value</td>
<td>The unsolicited call events requested from the CTI Server.</td>
<td>0x00ffffff (16777215)</td>
</tr>
<tr>
<td>AgentStateMask</td>
<td>DWORD Value</td>
<td>The agent states requested from the CTI Server.</td>
<td>0x0000003ff (1023)</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSDisplayToScreen</td>
<td>DWORD Value</td>
<td>If set to 1, EMS routines attempt to write formatted messages to standard output.</td>
<td>0</td>
</tr>
<tr>
<td>EMSAllLogFileMax</td>
<td>DWORD Value</td>
<td>The maximum total number of bytes that the EMS library writes to all local log files.</td>
<td>5000000</td>
</tr>
<tr>
<td>EMSBreakOnExit</td>
<td>DWORD Value</td>
<td>If set to 1, EMS exit routines invoke the Debugger.</td>
<td>0</td>
</tr>
<tr>
<td>EMSBreakOnInit</td>
<td>DWORD Value</td>
<td>If set to 1, EMS initialization routines invoke the Debugger.</td>
<td>0</td>
</tr>
<tr>
<td>EMSDebugBreak</td>
<td>DWORD Value</td>
<td>If set to 1, EMS failure routines invoke the Debugger before exiting the process.</td>
<td>1</td>
</tr>
<tr>
<td>EMSLogFileCountMax</td>
<td>DWORD Value</td>
<td>The maximum number of log files that the EMS library writes.</td>
<td>10</td>
</tr>
</tbody>
</table>
Table 8-2  
Registry values for EMS Tracing

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Type</th>
<th>Description</th>
<th>Default/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSLogFileLocation</td>
<td>String</td>
<td>The directory where the EMS library creates local log files.</td>
<td>Default directory specified at installation.</td>
</tr>
<tr>
<td>EMSLogFileMax</td>
<td>DWORD</td>
<td>The maximum number of bytes that the EMS library writes to a single local log file.</td>
<td>500000</td>
</tr>
<tr>
<td>EMSNTEventLogLevel</td>
<td>DWORD</td>
<td>The minimum severity event that EMS logs in the Application Event Log.</td>
<td>0xffffffff</td>
</tr>
<tr>
<td>EMSTraceMask</td>
<td>DWORD</td>
<td>A bitmask that specifies the levels of EMS tracing that are enabled.</td>
<td>3</td>
</tr>
<tr>
<td>EMSUserData</td>
<td>DWORD</td>
<td>Placeholder for arbitrary binary user data.</td>
<td></td>
</tr>
<tr>
<td>EMSForwardLevel</td>
<td>DWORD</td>
<td>The minimum severity event that EMS forwards to the ICM central controller.</td>
<td>0</td>
</tr>
<tr>
<td>ConsoleTraceMask</td>
<td>DWORD</td>
<td>A bitmask that specifies the level of console tracing that are enabled.</td>
<td>0x3</td>
</tr>
</tbody>
</table>

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
- 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]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentChatLevel</td>
<td>string</td>
<td>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.</td>
<td>TeamSupervisors</td>
</tr>
<tr>
<td>EnableWrapupDialog</td>
<td>DWORD Value</td>
<td>When enabled (1), a Wrapup dialog box pops up at the end of the call. A value of 0 disables this feature.</td>
<td>1</td>
</tr>
<tr>
<td>LogoutReasonRequired</td>
<td>DWORD Value</td>
<td>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.</td>
<td>1 for Spectrum, 0 for all other switches</td>
</tr>
<tr>
<td>NotReadyReasonRequired</td>
<td>DWORD Value</td>
<td>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.</td>
<td>0</td>
</tr>
<tr>
<td>PollForAgentStatsAtEndCall</td>
<td>DWORD Value</td>
<td>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.</td>
<td>1</td>
</tr>
<tr>
<td>PollingIntervalSec</td>
<td>DWORD Value</td>
<td>The agent statistics polling interval, in seconds.</td>
<td>15</td>
</tr>
<tr>
<td>WrapupDataRequired</td>
<td>DWORD Value</td>
<td>When enabled (1), wrapup data is mandatory. When disabled (0), wrapup data is not required. Not applicable to IPCC agents.</td>
<td>0</td>
</tr>
</tbody>
</table>
Changing the value of PollForAgentStatsAtEndCall may degrade performance and is not recommended.

<table>
<thead>
<tr>
<th>Table 8-4</th>
<th>AgentChatLevel Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td><strong>Meaning</strong></td>
</tr>
<tr>
<td>Disabled</td>
<td>All agent chat disabled.</td>
</tr>
<tr>
<td>PrimarySupervisor</td>
<td>Agents can chat only with primary supervisor of their team.</td>
</tr>
<tr>
<td>TeamSupervisors</td>
<td>Agents can chat with the primary or secondary supervisor of their team.</td>
</tr>
<tr>
<td>Team</td>
<td>Agents can chat with anyone in team.</td>
</tr>
<tr>
<td>Unrestricted</td>
<td>Agents can chat with anyone on the same peripheral.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Table 8-5</th>
<th>Initial Contents of [Server\Agent\ReasonCodes\Logout]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Value Name</td>
<td>Value Type</td>
</tr>
<tr>
<td>Insert logout reason code 1 here</td>
<td>DWORD Value</td>
</tr>
<tr>
<td>Insert logout reason code 2 here</td>
<td>DWORD Value</td>
</tr>
<tr>
<td>Insert logout reason code 3 here</td>
<td>DWORD Value</td>
</tr>
<tr>
<td>Insert logout reason code 4 here</td>
<td>DWORD Value</td>
</tr>
</tbody>
</table>

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.
Chapter 8      CTI OS Configuration

- **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>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String0</td>
<td>String Value</td>
<td>Placeholder for first wrapup text string.</td>
</tr>
<tr>
<td>String1</td>
<td>String Value</td>
<td>Placeholder for second wrapup text string.</td>
</tr>
<tr>
<td>String2</td>
<td>String Value</td>
<td>Placeholder for third wrapup text string.</td>
</tr>
<tr>
<td>String3</td>
<td>String Value</td>
<td>Placeholder for fourth wrapup text string.</td>
</tr>
</tbody>
</table>

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 ICM does not save any wrapup data for outgoing calls, therefore you do not need to define outgoing wrapup strings.

**CallObject**

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

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgentPreCallEvent Timeout</td>
<td>DWORD Value</td>
<td>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.</td>
<td>30</td>
</tr>
</tbody>
</table>
### Table 8-7 Registry values for [Server\CallObject] (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Data Type</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCCConference_SupportsMultipleControllers</td>
<td>DWORD</td>
<td>When set to 1, allows all parties of a Conference to add new parties to the conference as supported by CallManager Versions 4.0 and later. If running against an earlier version of CallManager, this must be set to 0. If this is not set to 0 when running against an earlier version of Call Manager, and a non-controller Conference party tries to make a Consult Call for a Conference, the party receives a Control Failure.</td>
<td>1</td>
</tr>
<tr>
<td>MinimizeEventArgs</td>
<td>DWORD</td>
<td>When set to 1 (recommended setting), minimizes the amount of nonessential call object parameters sent to the client.</td>
<td>1</td>
</tr>
<tr>
<td>TrashCollectionInterval Sec</td>
<td>DWORD</td>
<td>Controls how often (in seconds) the trash collector activates and removes any stale objects from memory. A value of 0 disables the trash collector.</td>
<td>7200</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeartbeatIntervalMs</td>
<td>DWORD Value</td>
<td>The number of milliseconds between heartbeats from the server to its clients.</td>
<td>60000</td>
</tr>
<tr>
<td>HeartbeatRetrys</td>
<td>DWORD Value</td>
<td>The number of missed heartbeats before a connection is closed for unresponsiveness.</td>
<td>5</td>
</tr>
<tr>
<td>ListenPort</td>
<td>DWORD Value</td>
<td>The TCP/IP port on which the CTI OS Server listens for incoming client connections.</td>
<td>Port specified during CTI OS Server setup.</td>
</tr>
<tr>
<td>MaxMonitorModeConnections</td>
<td>DWORD Value</td>
<td>This registry entry controls the number of monitor mode connections connected to a CTI OS Server. By default, this registry value doesn't 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.</td>
<td>2</td>
</tr>
</tbody>
</table>

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 5000ms and 3 retries:
- After 5000ms (five seconds Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 1.
- After another 5000ms (10 seconds Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 2.
- After another 5000ms (15 seconds Total time), if the server has not heard from the client it sends a heartbeat request and increments the retry count to 3.
- After another 5000ms (20 seconds Total time), if the server still has not heard 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 timeout 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]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartbeat IntervalMs</td>
<td>DWORD Value</td>
<td>Number of milliseconds between heartbeats for client connection to peer servers.</td>
<td>5000</td>
</tr>
<tr>
<td>HeartbeatRetrys</td>
<td>DWORD Value</td>
<td>Number of retry attempts before a connection to a peer server is determined to be down.</td>
<td>3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>DWORD Value</td>
<td>The number of the TCP/IP port on which the peer server is listening for the client connection.</td>
</tr>
</tbody>
</table>

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 ICM 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 EnterprisesName logical name in the ICM 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]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeripheralID</td>
<td>DWORD Value</td>
<td>The PeripheralID configured in the ICM database for this Peripheral.</td>
</tr>
<tr>
<td>PeripheralType</td>
<td>DWORD Value</td>
<td>The PeripheralType corresponding to this PeripheralID.</td>
</tr>
</tbody>
</table>

Examples:

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

- [HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<CTIOS InstanceName>\<CTIOServerName>\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]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>PollingInterval Sec</td>
<td>DWORD Value</td>
<td>The SkillGroup statistics polling interval, in seconds.</td>
<td>10</td>
</tr>
</tbody>
</table>
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]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor ChatLevel</td>
<td>String Value</td>
<td>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.</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>

**Table 8-14** SupervisorChatLevel Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>All supervisor chat disabled.</td>
</tr>
<tr>
<td>Team</td>
<td>Supervisors can chat with anyone in their primary team.</td>
</tr>
<tr>
<td>Unrestricted</td>
<td>Supervisors can chat with anyone on the same peripheral.</td>
</tr>
</tbody>
</table>

TimerService

The TimerService key specifies configuration parameters for the CTI OS Server’s internal TimerService. Table 8-15 lists the registry values for the TimerService key.

**Table 8-15** Registry values for [Server\TimerService]

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResolutionSec</td>
<td>DWORD Value</td>
<td>The interval at which the TimerService services queued requests, expressed in seconds.</td>
<td>1</td>
</tr>
</tbody>
</table>
MainScreen

The MainScreen key, located at \[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\AllDesktops\ScreenPreferences\Name\MainScreen\], includes registry values that define the behavior of softphone windows and icons in response to a BeginCallEvent. Table 8-16 lists the registry values for the MainScreen key.

Table 8-16  MainScreen Registry Key Values

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

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:

\[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\AllDesktops\IPCCSilentMonitor\Name\Settings\]

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 8-17.

Table 8-17  Settings Registry Subkey Values

<table>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeartbeatInterval</td>
<td>DWORD value</td>
<td>The time in seconds between consecutive heartbeats.</td>
<td>5</td>
</tr>
<tr>
<td>HeartbeatTimeout</td>
<td>DWORD value</td>
<td>The amount of time in seconds that must elapse without receiving data before a disconnect is signaled.</td>
<td>15</td>
</tr>
</tbody>
</table>
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>\<CTIOServerName>\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:00000005
"MaxHeartbeats"=dword:00000001
"CtiOsA"="HostName_A"
"CtiOsB"="HostName_B"
"PortA"=dword:0000a42c
"PortB"=dword:0000a42c
"AutoLogin"=dword:00000001
"ShowFieldBitMask"=dword:00000023
"WarnIfAlreadyLoggedin"=dword:00000001
"DisableSkillGroupStatistics"=dword:00000000
"DisableAgentStatistics"=dword:00000000
"IPCCSilentMonitorEnabled"=dword:0x00000001
"WarnIfSilentMonitored"=0x00000000
```

Table 8-17 describes the required ConnectionProfiles key registry values.

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>DWORD value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediaTerminationPort</td>
<td>DWORD value</td>
<td>Reserved. This is the TCP/IP port that the silent monitor subsystem uses to render monitored audio.</td>
</tr>
<tr>
<td>MonitoringIPPort</td>
<td>DWORD value</td>
<td>This is the TCP/IP port on the monitoring application to which the monitored application sends monitored audio.</td>
</tr>
</tbody>
</table>

Table 8-17  Settings Registry Subkey Values

Table 8-18 describes the required ConnectionProfiles key registry values.

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiOsServerName</td>
<td>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.</td>
</tr>
<tr>
<td>PeripheralID</td>
<td>The numeric value of the peripheral to which the CTI OS Server connects.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>Time interval between heartbeat messages between the client and CTI OS Server.</td>
</tr>
<tr>
<td>MaxHeartbeats</td>
<td>Maximum number of heartbeats that can be missed by the CTI OS Client Session before failover occurs.</td>
</tr>
</tbody>
</table>
Table 8-18  ConnectionProfiles Key Registry Values (continued)

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiOsA</td>
<td>DNS name of IP Address of the primary CTI OS Server to which a client application can connect.</td>
</tr>
<tr>
<td>CtiOsB</td>
<td>DNS name of IP Address of the secondary CTI OS Server to which a client application can connect.</td>
</tr>
<tr>
<td>PortA</td>
<td>TCP/IP port number assigned to the primary server.</td>
</tr>
<tr>
<td>PortB</td>
<td>TCP/IP port number assigned to the secondary server.</td>
</tr>
<tr>
<td>AutoLogin</td>
<td>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.</td>
</tr>
<tr>
<td>ShowFieldBitMask</td>
<td>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 8-19. The default value at setup for ShowFieldBitMask is 0x00000023 (AgentID, Instrument and Password displayed).</td>
</tr>
<tr>
<td>WarnIfAlreadyLoggedIn</td>
<td>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.</td>
</tr>
<tr>
<td>RejectIfAlreadyLoggedIn</td>
<td>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.</td>
</tr>
<tr>
<td>DisableSkillGroupStatistics</td>
<td>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.</td>
</tr>
<tr>
<td>DisableAgentStatistics</td>
<td>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.</td>
</tr>
<tr>
<td>IPCCSilentMonitorEnabled</td>
<td>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.</td>
</tr>
</tbody>
</table>
Defining Connection Profiles

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

### Table 8-18 ConnectionProfiles Key Registry Values (continued)

<table>
<thead>
<tr>
<th>SubKey/Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WarnIfSilent Monitored</td>
<td>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.</td>
</tr>
<tr>
<td>RasCallMode</td>
<td>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).</td>
</tr>
</tbody>
</table>

### Table 8-19 ShowBitFieldMask Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instrument</td>
<td>0x00000001</td>
</tr>
<tr>
<td>Password</td>
<td>0x00000002</td>
</tr>
<tr>
<td>Work Mode</td>
<td>0x00000004</td>
</tr>
<tr>
<td>Position ID</td>
<td>0x00000008</td>
</tr>
<tr>
<td>Skillgroup</td>
<td>0x00000010</td>
</tr>
<tr>
<td>AgentID</td>
<td>0x00000020</td>
</tr>
<tr>
<td>Login Name</td>
<td>0x00000040</td>
</tr>
<tr>
<td>Mobile Agent</td>
<td>0x00000080</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Registry Value Name</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListenPort</td>
<td>integer</td>
<td>Port on which the silent monitor service is listening for incoming connections.</td>
</tr>
<tr>
<td>TOS</td>
<td>integer</td>
<td>QOS setting for the connection.</td>
</tr>
<tr>
<td>HeartbeatInterval</td>
<td>integer</td>
<td>Amount of time in milliseconds between heartbeats.</td>
</tr>
<tr>
<td>HeartbeatRetries</td>
<td>integer</td>
<td>Number of missed heartbeats before the connection is abandoned.</td>
</tr>
<tr>
<td>Cluster</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 - index of the first silent monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- N - index of the Nth silent monitor service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Both subkeys contain the following keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SilentMonitorService - host name or IP address of a silent monitor service to which to connect.</td>
</tr>
</tbody>
</table>
Declaring ECC Variables

The ECC key contains a list of the expanded call context variables that are used on a client application with calls. The variables declared on this key must exist in the ICM database.

The ECC variables 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\ECC\Name\VariableName]

To declare a given ECC variable either named array or scalar, you must define a subkey under \ECC\Name\ without the prefix user. However, when creating ECC variables using the ICM Expanded Call Variable List tool, the ECC name must start with the prefix "user.". The subkey name is case sensitive.

For example, to declare the scalar variables user.CustomerID and user.CustomerType in CTI OS you must enter

[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerID]
"Data"="ECC" (Note: enter this line without the quotes)
[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerType]
"Data"="ECC" (Note: enter this line without the quotes)

To declare a named array user.CustomerAccount with 27 elements, you must enter

[HKEY_LOCAL_MACHINE\SOFTWARE\...\ECC\Name\CustomerAccount]
"Data"="ECCARRAY[27]" (Note: enter this line without the quotes)

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 8-21 lists the attributes that a column declaration can contain.

### Table 8-21  **Column Declaration Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>String Value</td>
<td>Assigns a column to display the Call information identified by the value of this attribute. Table 8-22 lists the possible values.</td>
</tr>
<tr>
<td>Header</td>
<td>String Value</td>
<td>Contains the text string to be displayed on the header of the column. If not specified, the Type is displayed instead.</td>
</tr>
</tbody>
</table>
| 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 of characters that can appear in the column. |
| 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 8-22 lists the Type Values.

**Table 8-22  Type Values**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallID</td>
<td>Associates the column with the unique call ID.</td>
</tr>
<tr>
<td>CallStatus or Status</td>
<td>Associates the column with Call Status.</td>
</tr>
<tr>
<td>DNIS</td>
<td>Associates the column with DNIS.</td>
</tr>
<tr>
<td>ANI</td>
<td>Associates the column with ANI.</td>
</tr>
<tr>
<td>CED</td>
<td>Associates the column with the caller entered digits.</td>
</tr>
<tr>
<td>DialedNumber or DN</td>
<td>Associates the column with the dialed number.</td>
</tr>
<tr>
<td>UserToUserInfo or UserToUser</td>
<td>Associates the column with user to user information.</td>
</tr>
<tr>
<td>WrapUp</td>
<td>Associates the column with the call wrap up data.</td>
</tr>
<tr>
<td>Var1, Var2, …, Var10</td>
<td>Associates the column with a call variable.</td>
</tr>
<tr>
<td>NAMEDVARIABLE, ECCVariable, ECCVar, ECC, or ECCNAME</td>
<td>Associates the column with an scalar ECC Variable.</td>
</tr>
<tr>
<td>NAMEDARRAY or ECCARRAY</td>
<td>Associates the column with a Named Array ECC variable.</td>
</tr>
<tr>
<td>CampaignID</td>
<td>Campaign ID for value appears in the Agent Real Time table. Set to zero if not used. Applicable to Outbound Option systems only.</td>
</tr>
<tr>
<td>QueryRuleID</td>
<td>Query rule ID for value appears in the Agent Real Time table. Set to zero if not used. Applicable to Outbound Option systems only.</td>
</tr>
</tbody>
</table>

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"

**Note**
If you wish to declare a column for an ECC variable you must first declare the ECC variable itself in the registry, as explained in the previous section, *Declaring ECC Variables*. You must also first define columns 1-18, as discussed in the next section.

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.

```plaintext
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\CTIOServerName>\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 CTIOServer directory contains a file, callappearance.default.reg.txt, that provides the following default definition for Call Appearance grid columns 1-18.

REGEDIT4

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

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

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

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\CTIOServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\10]
"Type"="Var2"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\CTIOServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\11]
"Type"="Var3"
"maxchars"="39"
"editable"="true"
```
Configuring the Call Appearance Grid

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\12]
"Type"="Var4"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\13]
"Type"="Var5"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\14]
"Type"="Var6"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\15]
"Type"="Var7"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\16]
"Type"="Var8"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\17]
"Type"="Var9"
"maxchars"="39"
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\Columns\Number\18]
"Type"="Var10"
"maxchars"="39"
"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"
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\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"="39"  
"editable"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid\CallAppearance\ Columns\Number\9]  "Type"="Var1"  
"maxchars"="39"  
"editable"="true"
```

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

**Step 1** Bring up the Windows 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 ICM 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.

REGEDIT4

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

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** Bring up the Windows **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 **ICM 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.

REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Grid]
Automatic Skill Group Statistics Grid Configuration

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

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

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

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

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

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

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\<CTIOS InstanceName>\<CTIOSServerName>\EnterprisesDesktopSettings\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 above. IPCC uses the new default skill group added for support of media routing. All voice calls not routed by an ICM script are reported in this new default skill group.

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 Bring up the Windows Start > Run dialog box.
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 "Type of Service" ToS in release 7.0. However, ToS is not supported for Siebel communications in 7.0.

---

**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. You need to know that if the PCs network connection is via the hardphone 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, but it does not affect the server to client traffic.

For CTI OS 7.0, TOS tagging is NOT be implemented in the Java or .NET (C#) CILs. As stated above, a system using these could support one way tagging from server to client, but traffic from the client to the server would be sent best effort.

CTI OS supports the marking of TCP/IP packets with ToS. This allows for preferential treatment (eg 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 need to configure certain registry keys. 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 also have to send their network traffic with the same ToS value to the CTI OS server. CTI OS clients could in fact send their traffic best efforts, 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:

   ```plaintext
   HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<customer-instance>\CTIOS1\Server\Connections
   "TOS"=dword:00000068
   ``

   **Note**

   The dword value above is listed in hex format (decimal 104)

2. This registry key turns on markings of packets sent from the client to the server

   ```plaintext
   HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<customer-instance>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\IPCC<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

   ```plaintext
   HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\<customer-instance>\CTIOS1\EnterpriseDesktopSettings\All Desktops\IPCCSilentMonitor\Name\Settings
   "TOS"=dword:00000BB8
   ```

**Important Additional Configuration**

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:

```plaintext
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters
"DisableUserTOSSetting"=dword:00000000
```

DisableUserTOSSetting 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 needs to be restarted for this change to become effective.

For additional information see:

- [http://support.microsoft.com/default.aspx?scid=kb;en-us;258978](http://support.microsoft.com/default.aspx?scid=kb;en-us;258978)
Caveats

- In order for the ToS to become effective, the network (specifically the routers) needs to be configured to treat packets with ToS markings preferentially.

- The traffic between CTIOS server and CTIOS clients may include type of data, which does not qualify for AF31 type of service. AF31 is suggested for signaling traffic. For example, a call delivered 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, since CTIOS sends all traffic on the same connection, either all packets are marked or none. Therefore, CTIOS Skillgroupstatistics need to 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.
Startup, Shutdown, and Failover

This section explains how to start and stop the CTI OS System, and how CTI OS handles failover scenarios.

ICM Service Control

The CTI OS Server runs as a Windows 2000 service on the host computer. The ICM Service Control application is an interface into the Windows platform’s service control manager, which start and stops services. See Figure 9-1.

To start, stop, or cycle the processes in the CTI OS Server, use the appropriate tabs from the ICM 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

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Process Description</th>
<th>Runs In Console Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiosServerNode</td>
<td>The main CTI OS Server process. This process manages all CTI OS objects and listens for and manages client connections.</td>
<td>Yes</td>
</tr>
<tr>
<td>CTIOSTrace</td>
<td>The CTI OS tracing utility. This process uses the ICM Event Management System (EMS) to trace server messages to local log files in EMS format.</td>
<td>No</td>
</tr>
<tr>
<td>NM</td>
<td>The ICM NodeManager (fault tolerance manager). Each ICM service is started by NodeManager, and NodeManager restarts any abnormally terminated processes.</td>
<td>No</td>
</tr>
<tr>
<td>NMM</td>
<td>The ICM NodeManagerManager (system fault tolerance). Each ICM Node (e.g. CTI OS) starts up a NMM process to handle system-level faults. In the event of an unrecoverable system fault, NMM will restart the host computer.</td>
<td>No</td>
</tr>
</tbody>
</table>

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 need to be configured correctly. Perform the following steps to verify that the parameters are correct:

Step 1  Run the PG explorer.
Step 2  Click on 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 so already.
Step 6  Cycle the PG.

"/LOAD 0" causes agents to be set to NotReady during a failover. By setting the agents to NotReady, calls will not be routed to them and the failover will be 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.

CTI OS 7.0 doesn't 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 will be 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 doesn't have call(s). In this case, the supervisor has to logout the agent first, and then the agent must re-launch the agent desktop, supplies the correct password and log in manually.

3. The agent desktop crashes while the agent is logged in to CTI OS Server, and has call(s). In this case, the supervisor has to logout the agent first, and then the agent must re-launch the agent desktop, supplies 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 softphones 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 will need to 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 will need to log in again manually.

Peripheral Gateway

As 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.
Peripheral-Specific Support

This chapter provides information on the Time Division Multiplexing (TDM) peripherals supported by CTI OS. Different peripheral manufacturers provide varying levels of support for CTI specific features. These differences need to 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 since they do not, in general, provide the Supervisory features that IPCC provides.

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 ICM Software 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 ICM terms
- A list of 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 ICM Software Support

This section describes differences in how various peripherals implement ICM software functionality.
Peripheral-Specific Terminology

Different peripheral manufacturers use different terminology for ICM software 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 ICM software terms and provides peripheral-specific equivalents.

<table>
<thead>
<tr>
<th>ICM Term</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Agent</td>
</tr>
<tr>
<td>Peripheral target</td>
<td><strong>Alcatel 400</strong>: DNIS</td>
</tr>
<tr>
<td></td>
<td><strong>IPCC</strong>: Device Target</td>
</tr>
<tr>
<td></td>
<td><strong>Siemens Hicom</strong>: Destination ACD</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk group and DNIS</td>
</tr>
<tr>
<td>Service</td>
<td><strong>Alcatel 400</strong>: Pilot</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Avaya DEFINITY ECS</strong>: Vector Directory Number (VDN)</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: ACD Directory Number (ACD DN) or ACD Controlled Directory Number (ACD CDN)³</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Rockwell Spectrum</strong>: Application</td>
</tr>
<tr>
<td></td>
<td><strong>Siemens Hicom</strong>: ACD Routing Table (ART)</td>
</tr>
<tr>
<td>Skill group</td>
<td><strong>Alcatel 400</strong>: Agent PG</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Agent group</td>
</tr>
<tr>
<td></td>
<td><strong>Avaya DEFINITY ECS</strong>: Skill group or hunt group¹</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: ACD DN</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Skill Set</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Skill group</td>
</tr>
<tr>
<td>Trunk</td>
<td><strong>Alcatel 400</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Aspect Contact Server</strong>: Instrument⁵</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: Member of route</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk</td>
</tr>
<tr>
<td>Trunk group</td>
<td><strong>Alcatel 400</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel DMS-100, DMS-500, SL-100</strong>: None</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Meridian</strong>: Route</td>
</tr>
<tr>
<td></td>
<td><strong>Nortel Symposium</strong>: Route</td>
</tr>
<tr>
<td></td>
<td><strong>Others</strong>: Trunk group</td>
</tr>
</tbody>
</table>
1. CTI OS currently supports only the North American version of the Siemens Hicom switch. The European version (Siemens Hicom 300 E) is not supported.

2. 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.

3. Without Customer Controlled Routing (CCR), one or more services map to an ACD DN. With CCR, one or more services map to an ACD CDN.

4. 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.

5. A CallCenter instrument can be a trunk, a teleset, or a workstation.

In some cases, the ICM concept is very close to the corresponding ACD feature. For example, the 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 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 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. ICM software emulates this by automatically creating additional skill groups for these peripheral types.

ICM Feature Limitations

Some ACDs have limitations that prevent them from making full use of specific features of ICM software. Table 10-2 summarizes these limitations for those ACDs.

<table>
<thead>
<tr>
<th>Peripheral Type</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcatel 4400</td>
<td>No trunk group monitoring</td>
</tr>
<tr>
<td>Aspect Contact Server</td>
<td>Only one skill group assignment per agent</td>
</tr>
<tr>
<td>Avaya DEFINITY ECS</td>
<td>none</td>
</tr>
<tr>
<td>IPCC</td>
<td>Does not support Trunks or Trunk Groups</td>
</tr>
<tr>
<td>Nortel Meridian</td>
<td>Limited trunk group monitoring</td>
</tr>
<tr>
<td></td>
<td>Ring time for a call is included in either queue time or delay time</td>
</tr>
</tbody>
</table>
| 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 |
| Siemens Hicom         | No real-time trunk group monitoring
|                       | Limited conference call monitoring                |
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 10-6.
- A double asterisk (**) indicates that the event is available from Aspect when the PG is configured to use the Aspect Event Link.

<table>
<thead>
<tr>
<th>Unavailable Event</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENT_PRE_CALL</td>
<td>Alcatel, Aspect, DEFINITY, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>AGENT_PRE_CALL_ABORT</td>
<td>Alcatel, Aspect, DEFINITY, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>AGENT_STATE</td>
<td>none</td>
</tr>
<tr>
<td>BEGIN_CALL</td>
<td>none</td>
</tr>
<tr>
<td>CALL_CLEARED</td>
<td>Aspect*</td>
</tr>
<tr>
<td>CALL_CONFERENCED</td>
<td>Aspect**, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_CONNECTION_CLEARED</td>
<td>none</td>
</tr>
<tr>
<td>CALL_DATA_UPDATE</td>
<td>none</td>
</tr>
<tr>
<td>CALL_DELIVERED</td>
<td>Aspect*, Rockwell Spectrum*</td>
</tr>
<tr>
<td>CALL_DEQUEUED</td>
<td>Alcatel, DEFINITY, Nortel Meridian, Nortel Symposium, Siemens Hicom</td>
</tr>
<tr>
<td>CALL_DIVERTED</td>
<td>Aspect, IPCC, Nortel Meridian, Nortel Symposium</td>
</tr>
<tr>
<td>CALL_ESTABLISHED</td>
<td>IVR</td>
</tr>
</tbody>
</table>
Table 10-3  Call Events NOT Available to Specific Peripherals (continued)

<table>
<thead>
<tr>
<th>Unavailable Event</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALL_FAILED</td>
<td>Aspect, Nortel Meridian, Nortel Symposium,</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_HELD</td>
<td>Aspect**, IVR, Rockwell Spectrum*</td>
</tr>
<tr>
<td>CALL_ORIGINATED</td>
<td>Aspect, DEFINITY*, Nortel Meridian, Nortel</td>
</tr>
<tr>
<td></td>
<td>Symposium, Rockwell Spectrum, Siemens Hicom</td>
</tr>
<tr>
<td>CALL_QUUEUED</td>
<td>IPCC, IVR</td>
</tr>
<tr>
<td>CALL_REACHED_NETWORK</td>
<td>Aspect, Nortel Meridian, Nortel Symposium,</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_RETRIEVED</td>
<td>Aspect**, IVR, Rockwell Spectrum*</td>
</tr>
<tr>
<td>CALL_SERVICE_INITIATED</td>
<td>Aspect**, DEFINITY*, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CALL_TRANSFERRED</td>
<td>IVR</td>
</tr>
<tr>
<td>CALL_TRANSITION_ROUTE</td>
<td>IPCC</td>
</tr>
<tr>
<td>END_CALL</td>
<td>none</td>
</tr>
<tr>
<td>RTP_STARTED_EVENT</td>
<td>Alcatel, Aspect, Nortel Meridian, Nortel</td>
</tr>
<tr>
<td></td>
<td>Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>RTP_STOPPED_EVENT</td>
<td>Alcatel, Aspect, Nortel Meridian, Nortel</td>
</tr>
<tr>
<td></td>
<td>Symposium, Rockwell Spectrum, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>none</td>
</tr>
</tbody>
</table>

Client Control Requests

Table 10-4 lists the client control requests that are not supported by the different peripheral types.

- 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 10-6.

Table 10-4  Client Control Requests NOT Available to Specific Peripherals

<table>
<thead>
<tr>
<th>Unavailable Request</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTERNATE_CALL</td>
<td>Meridian, Nortel Symposium</td>
</tr>
<tr>
<td>ANSWER_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>CLEAR_CALL</td>
<td>Alcatel, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>CLEAR_CONNECTION</td>
<td>IVR</td>
</tr>
<tr>
<td>CONFERENCE_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>CONSULTATION_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>DEFLECT_CALL</td>
<td>Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, IVR</td>
</tr>
</tbody>
</table>
Peripheral-Specific Limitations and Differences

This section lists CTI OS-related restrictions and implementation differences for various peripherals.

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 (say 3550) logs into a phone/device (say 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 has to be specified. Failure to specify a skillgroup, 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.

### Table 10-4 Client Control Requests NOT Available to Specific Peripherals (continued)

<table>
<thead>
<tr>
<th>Unavailable Request</th>
<th>Peripherals</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOLD_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>MAKE_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>MAKE_PREDICTIVE_CALL</td>
<td>Alcatel, Siemens Hicom, IVR</td>
</tr>
<tr>
<td>QUERY_AGENT_STATE</td>
<td>IVR</td>
</tr>
<tr>
<td>QUERYDEVICE_INFO</td>
<td>IVR</td>
</tr>
<tr>
<td>RECONNECT_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>RETRIEVE_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>SEND_DTMF_SIGNAL</td>
<td>Aspect, Nortel Meridian, Nortel Symposium, Rockwell Spectrum, IVR</td>
</tr>
<tr>
<td>SET_AGENT_STATE</td>
<td>IVR</td>
</tr>
<tr>
<td>SNAPSHOT_CALL</td>
<td>IVR</td>
</tr>
<tr>
<td>SNAPSHOT_DEVICE</td>
<td>IVR</td>
</tr>
<tr>
<td>TRANSFER_CALL</td>
<td>IVR</td>
</tr>
</tbody>
</table>
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. Once 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 into all preconfigured Agent groups. When you log in without EAS, the agent is logged into 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 ICM software (that is, appears in the 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. Once 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 will be unable to log into 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:

<table>
<thead>
<tr>
<th>ASAI Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-MAX_LONG</td>
<td>none</td>
<td>*C_NUSE_LONG</td>
<td>No value was returned by the ECS.</td>
</tr>
<tr>
<td>0</td>
<td>CS0/28</td>
<td>*C_INVLDNUM</td>
<td>Invalid origination or destination address.</td>
</tr>
<tr>
<td>1</td>
<td>CS0/111</td>
<td>*C_PROTERR</td>
<td>Capability sequence has been violated or underlying protocol error has been detected; an unrecognized value was returned by the ECS.</td>
</tr>
<tr>
<td>2</td>
<td>CS3/40</td>
<td>*C_RESUNAVL</td>
<td>Resources to fulfill service are not available.</td>
</tr>
<tr>
<td>3</td>
<td>CS0/50</td>
<td>*C_FACUNSUB</td>
<td>Capability is implemented but not subscribed to by requester.</td>
</tr>
<tr>
<td>4</td>
<td>CS3/79</td>
<td>*C_SER_UNIMP</td>
<td>Incompatible options selected.</td>
</tr>
<tr>
<td>5</td>
<td>CS0/96</td>
<td>*C_MAND_INFO</td>
<td>One of the required parameters is missing.</td>
</tr>
<tr>
<td>6</td>
<td>CS0/100</td>
<td>*C_INVLDIE</td>
<td>Value specified in parameter is not allowed or defined.</td>
</tr>
<tr>
<td>7</td>
<td>CS3/63</td>
<td>*C_SER_UNAVIL</td>
<td>Domain or call is being monitored by another adjunct.</td>
</tr>
<tr>
<td>8</td>
<td>CS3/86</td>
<td>*C_CALLID_TERM</td>
<td>Call is no longer in active state.</td>
</tr>
<tr>
<td>9</td>
<td>CS0/98</td>
<td>*C_INCOM_ST</td>
<td>Message not compatible with call state.</td>
</tr>
<tr>
<td>10</td>
<td>CS0/81</td>
<td>*C_INVALID_CRV</td>
<td>Invalid call identifier (sao_id also known as cluster_id) used or call does not exist.</td>
</tr>
<tr>
<td>11</td>
<td>CS3/80</td>
<td>*C_INCOM_OPT</td>
<td>Incompatible options used to establish the call.</td>
</tr>
<tr>
<td>12</td>
<td>CS0/102</td>
<td>*C_REC_TIMER</td>
<td>Timer expired.</td>
</tr>
</tbody>
</table>
### Table 10-5  DEFINITY Cause Values (continued)

<table>
<thead>
<tr>
<th>ASA1 Value</th>
<th>DEFINITY ECS Value</th>
<th>Cause Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>CS3/15</td>
<td>*C_NOLOGIN</td>
<td>Agent not logged into split.</td>
</tr>
<tr>
<td>14</td>
<td>CS3/11</td>
<td>*C_NOSPLIT_MEM</td>
<td>Agent not member of specified split or split number specified incorrectly.</td>
</tr>
<tr>
<td>15</td>
<td>CS0/17</td>
<td>*C_USER_BUSY</td>
<td>Domain or call is being monitored by another adjunct.</td>
</tr>
<tr>
<td>16</td>
<td>CS0/18</td>
<td>*C_NOUSE_RESP</td>
<td>Originating address does not respond to service.</td>
</tr>
<tr>
<td>17</td>
<td>CS3/43</td>
<td>*C_PERM_DENIED</td>
<td>Permission checks for service have failed.</td>
</tr>
<tr>
<td>18</td>
<td>CS3/87</td>
<td>*C_CLUST_TERM</td>
<td>Association terminated because service is not active.</td>
</tr>
<tr>
<td>19</td>
<td>CS3/27</td>
<td>*C_OUT_OF_SERV</td>
<td>Domain has been removed by administration.</td>
</tr>
<tr>
<td>20</td>
<td>CS3/12</td>
<td>*C_INCS_AGST_ST</td>
<td>Agent not in compatible state.</td>
</tr>
<tr>
<td>21</td>
<td>CS3/13</td>
<td>*C_MAXLOGIN</td>
<td>Agent logged into maximum number of splits.</td>
</tr>
<tr>
<td>22</td>
<td>CS3/14</td>
<td>*C_INC_PASWD</td>
<td>Invalid login password.</td>
</tr>
<tr>
<td>23</td>
<td>CS3/16</td>
<td>*C_AGST_STATE</td>
<td>Request to put agent in the state that the agent is already in.</td>
</tr>
<tr>
<td>24</td>
<td>CS3/41</td>
<td>*C_BAD_ADMIN</td>
<td>ACD not provisioned or optioned.</td>
</tr>
<tr>
<td>25</td>
<td>CS0/16</td>
<td>*C_NORMAL</td>
<td>Normal termination; call routed successfully.</td>
</tr>
<tr>
<td>26</td>
<td>CS0/42</td>
<td>*C_NETCONJ</td>
<td>Association terminated because of network congestion.</td>
</tr>
<tr>
<td>27</td>
<td>CS0/99</td>
<td>*C_BAD_IE</td>
<td>Unknown information element detected.</td>
</tr>
<tr>
<td>28</td>
<td>CS3/22</td>
<td>*C_QUFULL</td>
<td>Queue is full.</td>
</tr>
<tr>
<td>ASAI Value</td>
<td>DEFINITY ECS Value</td>
<td>Cause Value Description</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>CS3/46</td>
<td>Administration is in progress; request cannot be serviced.</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>CS3/53</td>
<td>The ECS has rejected a request from the adjunct.</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>CS0/1</td>
<td>Unassigned number.</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>CS0/21</td>
<td>Call rejected.</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>CS0/22</td>
<td>Number changed.</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>CS0/31</td>
<td>Normal, unspecified.</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>CS0/34</td>
<td>No circuit or channel available.</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>CS0/41</td>
<td>Temporary Failure.</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>CS0/58</td>
<td>Bearer capability not presently available.</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>CS0/88</td>
<td>Incompatible destination.</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>CS0/95</td>
<td>Invalid message, unspecified (backward compatibility).</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>CS0/97</td>
<td>Message nonexistent/not implemented.</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>CS0/127</td>
<td>Unspecified.</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>CS3/19</td>
<td>No answer.</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>CS3/20</td>
<td>Trunks not available.</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>CS3/21</td>
<td>Classifiers not available.</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>CS3/30</td>
<td>Redirected.</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>CS3/38</td>
<td>Network out of order.</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Undefined</td>
<td>Undefined value returned from the ECS.</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>CS0/52</td>
<td>Outgoing call has been barred.</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>CS3/23</td>
<td>Call remains in queue.</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>CS0/65</td>
<td>Bearer service not implemented.</td>
<td></td>
</tr>
</tbody>
</table>
For example, an ASAI value of 15 corresponds to the DEFINITY ECS value of CS0/17 (C_USER_BUSY).

Refer to Table 10-6 to find the chapter of the DEFINITY Technical Reference Manual that discusses the third-party action that you attempted:

<table>
<thead>
<tr>
<th>Third-party Action or Request</th>
<th>Chapter in Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td>Chapter 4: ASAI and Call Control</td>
</tr>
</tbody>
</table>
For example, third-party login requests are discussed in Chapter 8, “ASAI and Request Feature Capabilities.”
- Refer to the chapter specified in Table 10-6 for an explanation of the DEFINITY ECS cause value.

### Table 10-6 Third-party Request/Section in DEFINITY Manual

<table>
<thead>
<tr>
<th>Third-Party actions via Domain Control: Auto Dial (3PAD), Domain Control (3PDC), Answer (3PANS), Merge (Transfer/Conference) (3PM)</th>
<th>Chapter 5: ASAI and Domain Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Routing (RT_REQ, RT_SEL, RT_END)</td>
<td>Chapter 7: ASAI and Call Routing</td>
</tr>
<tr>
<td>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</td>
<td>Chapter 8: ASAI and Request Feature Capabilities</td>
</tr>
<tr>
<td>Value Queries</td>
<td>Chapter 9: ASAI and Value Query Capabilities</td>
</tr>
<tr>
<td>Set Value: Message Waiting Indicator (MWI) Set Billing Type</td>
<td>Chapter 10: ASAI and Set Value Capabilities</td>
</tr>
</tbody>
</table>

**IPCC**

- **MAKE_CALL** is only supported when the agent is in the NotReady state.
- 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 has to 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 needs to 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 Cisco CallManager 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 ICM Peripheral Monitor Table is not supported for the IPCC PG.

• For updated information on the Cisco CallManager Multi-line feature, refer to the *Cisco CallManager System Guide*.

• The Cisco CallManager Shared line feature (agents share the same extension) is not supported.

• Agent Desk Settings will control some agent behaviors. These are configured in 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 on the call, all agent state buttons are disabled. While 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 which was clicked. 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 occurred at the end of an incoming call, the agent state changes to Ready.
    - If the timeout occurred 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 will fail with an error code of **CF_WRAPUP_DATA_REQUIRED** (280) if there is no wrap up data entered into a call.

• If Logout Reason or NotReady Reasons are required, an error of **CF_REASON_CODE_REQUIRED** (281) will be received if the reasons are not assigned in set agent state request. One must also create Logout Reason and NotReady Reason dialog boxes in the Reason Code if these properties are required.
For more information regarding reason code and wrapup modes, see the *Cisco ICM Software IPCC Administrator Guide*.

- 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 will know about it only when it next interrogates the switch.

**Nortel Meridian**

- AgentExtension and AgentInstrument are defined as the PositionID.

Meridian can operate in either of two basic modes:

- Agent ID Mode
- Position ID Mode

In Agent ID mode, the agent must enter an Agent ID to login. These Agent IDs are not actually configured anywhere (and they have no associated passwords). The administrator simply defines the minimum and maximum allowable ID values (for example, 1001-9999). As long as an agent specifies an ID that is not already in use by another agent, the login will be allowed.

In Position ID mode, there is no Agent ID. An agent simply presses the InCalls key and is immediately logged in. For the purposes of CTI OS, use the Position ID for the Agent ID.

The AgentPassword can be set to anything. The switch does not have the concept of an agent password. The AgentSkillGroup is ignored by the switch on login. Meridian Link does not allow an agent to specify a queue at login. The agent is logged in to whatever queue (skill group) the physical telephone is configured to be a member of.

- Table 10-3 and Table 10-4 show the capabilities in the “Enhanced CTI” mode (described in the PIM setup for Meridian) of PG operation.
- Alternate call operations are not supported.
- NotReady is not supported; use WorkReady instead.
- On a consultation call request for Meridian, the request must specify the type of consultation, that is, whether it is conference or transfer.
- The Meridian Multiple Queue Assignment (MQA) feature enables a Meridian agent to log into multiple ACD DN(s) (skill groups) by explicitly keying in the DN numbers on the physical teleset. However, the Meridian Link protocol provided by Nortel does not currently allow you to specify, via CTI OS, the ACD DN(s) into which you are logging when you send a login message. The Meridian Link protocol only allows an agent to log into the default ACD DN for which the teleset is configured.

If an agent must log into multiple ACD DN(s), or a single ACD DN that is different from the default ACD DN for the teleset, then the workaround is to have the agent log in at the physical teleset—and specify the ACD DN(s) through the teleset. After login, you can still receive calls for all of the groups and receive CTI OS notifications for the calls that will include the relevant skill group (ACD DN) information.

- 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 Meridian, 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 following tables summarize the Status and Cause values.

**Table 10-7  Meridian Status Values**

<table>
<thead>
<tr>
<th>Status Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Invalid Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>0A00 / 2560</td>
<td>Invalid calling TN</td>
</tr>
<tr>
<td>0A01 / 2561</td>
<td>Invalid calling DN; wrong DN specified</td>
</tr>
<tr>
<td>0A02 / 2562</td>
<td>Incomplete calling DN</td>
</tr>
<tr>
<td>0A03 / 2563</td>
<td>Invalid called DN</td>
</tr>
<tr>
<td>0A04 / 2564</td>
<td>Incomplete called DN</td>
</tr>
<tr>
<td>0A05 / 2565</td>
<td>Invalid called TN</td>
</tr>
<tr>
<td>0A06 / 2566</td>
<td>Invalid origination manner</td>
</tr>
<tr>
<td>0A07 / 2567</td>
<td>Invalid destination manner</td>
</tr>
<tr>
<td>0A08 / 2568</td>
<td>Invalid origination user type</td>
</tr>
<tr>
<td>0A09 / 2569</td>
<td>Invalid customer number</td>
</tr>
<tr>
<td>0A0A / 2570</td>
<td>System or data base error</td>
</tr>
<tr>
<td><strong>Unsuccessful Call Origination</strong></td>
<td></td>
</tr>
<tr>
<td>0B00 / 2816</td>
<td>Origination party busy</td>
</tr>
<tr>
<td>0B01 / 2817</td>
<td>Origination resource blocking</td>
</tr>
<tr>
<td>0B02 / 2818</td>
<td>Origination set is maintenance busy</td>
</tr>
<tr>
<td>0B03 / 2819</td>
<td>500/2500 set is onhook</td>
</tr>
<tr>
<td>0B04 / 2820</td>
<td>Origination DN busy</td>
</tr>
<tr>
<td>0B05 / 2821</td>
<td>Origination is ringing</td>
</tr>
<tr>
<td>0B06 / 2822</td>
<td>Unable to disconnect origination (that is, already disconnected)</td>
</tr>
<tr>
<td>0B07 / 2823</td>
<td>Origination access restriction blocking</td>
</tr>
<tr>
<td>0B08 / 2824</td>
<td>Origination call on permanent hold</td>
</tr>
<tr>
<td>0B0A / 2826</td>
<td>System or data base error</td>
</tr>
<tr>
<td>0B0B / 2827</td>
<td>Origination receiving end to end signaling</td>
</tr>
<tr>
<td>0B0C / 2828</td>
<td>The call is currently in an ACD queue</td>
</tr>
<tr>
<td>0B0E / 2830</td>
<td>Origination set invoked hold</td>
</tr>
<tr>
<td>0B14 / 2836</td>
<td>Transfer key not configured</td>
</tr>
<tr>
<td>0B15 / 2837</td>
<td>Transfer key not idle</td>
</tr>
<tr>
<td>0B16 / 2838</td>
<td>Set active in conference call</td>
</tr>
<tr>
<td>0B17 / 2839</td>
<td>Transfer or MPO/TSA class of service not configured</td>
</tr>
<tr>
<td>0B18 / 2840</td>
<td>Cannot put call on hold</td>
</tr>
<tr>
<td>0B1D / 2845</td>
<td>No active call exists on set</td>
</tr>
<tr>
<td>0B1E / 2846</td>
<td>No held call exists on set</td>
</tr>
<tr>
<td>Status Value (hex/dec)</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>Unsuccessful Call Termination</strong></td>
<td></td>
</tr>
<tr>
<td>0C00 / 3072</td>
<td>Terminating party is busy</td>
</tr>
<tr>
<td>0C01 / 3073</td>
<td>Destination resource blocking</td>
</tr>
<tr>
<td>0C02 / 3074</td>
<td>Destination in invalid state</td>
</tr>
<tr>
<td>0C07 / 3079</td>
<td>Destination access restriction blocking</td>
</tr>
<tr>
<td>0D0A / 3338</td>
<td>System or database error</td>
</tr>
<tr>
<td><strong>Network Interceptions</strong></td>
<td></td>
</tr>
<tr>
<td>0C08 / 3080</td>
<td>Unassigned number</td>
</tr>
<tr>
<td>0C09 / 3081</td>
<td>No route to destination</td>
</tr>
<tr>
<td>0C0A / 3082</td>
<td>No user responding</td>
</tr>
<tr>
<td>0C0B / 3083</td>
<td>Number changed</td>
</tr>
<tr>
<td>0C0C / 3084</td>
<td>Destination out of service</td>
</tr>
<tr>
<td>0C0D / 3085</td>
<td>Invalid number format</td>
</tr>
<tr>
<td>0C0E / 3086</td>
<td>No circuit available</td>
</tr>
<tr>
<td>0C0F / 3087</td>
<td>Network out of order</td>
</tr>
<tr>
<td>0C10 / 3088</td>
<td>Temporary failure</td>
</tr>
<tr>
<td>0C11 / 3089</td>
<td>Equipment congestion</td>
</tr>
<tr>
<td><strong>Network Interceptions with In-Band Information</strong></td>
<td></td>
</tr>
<tr>
<td>0C19 / 3097</td>
<td>Terminating party is busy</td>
</tr>
<tr>
<td>0C1A / 3098</td>
<td>Unassigned number</td>
</tr>
<tr>
<td>0C1B / 3099</td>
<td>No route to destination</td>
</tr>
<tr>
<td>0C1C / 3100</td>
<td>No user responding</td>
</tr>
<tr>
<td>0C1D / 3101</td>
<td>Number changed</td>
</tr>
<tr>
<td>0C1E / 3102</td>
<td>Destination out of service</td>
</tr>
<tr>
<td>0C1F / 3103</td>
<td>Invalid number format</td>
</tr>
<tr>
<td>0C20 / 3104</td>
<td>No circuit available</td>
</tr>
<tr>
<td>0C21 / 3105</td>
<td>Network out of order</td>
</tr>
<tr>
<td>0C22 / 3106</td>
<td>Temporary failure</td>
</tr>
<tr>
<td>0C23 / 3107</td>
<td>Equipment congestion</td>
</tr>
<tr>
<td>0C24 / 3108</td>
<td>Interworking, unspecified</td>
</tr>
<tr>
<td>0CFE / 3326</td>
<td>Other cause</td>
</tr>
<tr>
<td><strong>Unsuccessful Conference or Transfer Operation</strong></td>
<td></td>
</tr>
<tr>
<td>0D00 / 3328</td>
<td>Cannot complete conference</td>
</tr>
<tr>
<td>0D01 / 3329</td>
<td>Cannot initiate transfer</td>
</tr>
<tr>
<td>0D02 / 3330</td>
<td>Cannot complete transfer</td>
</tr>
</tbody>
</table>
### Table 10-7  Meridian Status Values (continued)

<table>
<thead>
<tr>
<th>Status Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0D03 / 3331</td>
<td>Cannot retrieve original call</td>
</tr>
<tr>
<td>0D04 / 3332</td>
<td>Fast Transfer initiation failed</td>
</tr>
<tr>
<td>0D05 / 3333</td>
<td>Fast Transfer completion failed</td>
</tr>
<tr>
<td>0D0B / 3339</td>
<td>Hold Request failed</td>
</tr>
</tbody>
</table>

### Table 10-8  Meridian Cause Values

<table>
<thead>
<tr>
<th>Cause Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1002 / 4098</td>
<td>Access restricted</td>
</tr>
<tr>
<td>1003 / 4099</td>
<td>Resource unavailable</td>
</tr>
<tr>
<td>1004 / 4100</td>
<td>Invalid customer number</td>
</tr>
<tr>
<td>1005 / 4101</td>
<td>Invalid origination address</td>
</tr>
<tr>
<td>1006 / 4102</td>
<td>Invalid destination address</td>
</tr>
<tr>
<td>1007 / 4103</td>
<td>Invalid manner</td>
</tr>
<tr>
<td>1008 / 4104</td>
<td>Unsuccessful retrieve original</td>
</tr>
<tr>
<td>1009 / 4105</td>
<td>Unsuccessful transfer</td>
</tr>
<tr>
<td>100A / 4106</td>
<td>Unsuccessful conference</td>
</tr>
<tr>
<td>100B / 4107</td>
<td>Unsuccessful answer request</td>
</tr>
<tr>
<td>100C / 4108</td>
<td>Unsuccessful release request</td>
</tr>
<tr>
<td>1070 / 4208</td>
<td>Refer to Connection Status IE</td>
</tr>
<tr>
<td>2004 / 8196</td>
<td>The target DN is invalid</td>
</tr>
<tr>
<td>2005 / 8197</td>
<td>The target DN is not AST</td>
</tr>
<tr>
<td>2006 / 8198</td>
<td>The Customer Number is invalid</td>
</tr>
<tr>
<td>2007 / 8199</td>
<td>The feature could not be invoked</td>
</tr>
<tr>
<td>2008 / 8200</td>
<td>The feature is not configured on the set</td>
</tr>
<tr>
<td>2009 / 8201</td>
<td>The requested feature is out of valid range</td>
</tr>
<tr>
<td>200A / 8202</td>
<td>The target set is not ACD agent</td>
</tr>
<tr>
<td>200B / 8203</td>
<td>The target set is a Virtual Agent</td>
</tr>
<tr>
<td>200C / 8204</td>
<td>The set is maintenance busy</td>
</tr>
<tr>
<td>200D / 8205</td>
<td>Set is in wrong state for invocation</td>
</tr>
<tr>
<td>200E / 8206</td>
<td>Set is in target state</td>
</tr>
<tr>
<td>200F / 8207</td>
<td>No NRDY/RDY while ACD set is logged out</td>
</tr>
<tr>
<td>2010 / 8208</td>
<td>Package C customer cannot use NRDY with IDN call</td>
</tr>
<tr>
<td>2011 / 8209</td>
<td>Feature IE is missing or invalid</td>
</tr>
<tr>
<td>2012 / 8210</td>
<td>DN IE is missing or invalid</td>
</tr>
<tr>
<td>2013 / 8211</td>
<td>Agent ID IE is missing or invalid</td>
</tr>
</tbody>
</table>
The Peripheral Gateway (and thus CTI OS clients) will not receive a CallEstablished Event for an off-switch call. As a result of this limitation, some features—such as blind conference or transfer operation off-switch—are not supported. The soft phone has no way to know that the call has been connected off-switch, and thus the application requires manual intervention from the agent (who will either hear 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/blind transfer or conference is not supported. Transfer and conference calls must be consultative.

Consultative Transfer to a Supervisor is not supported.

One is unable to transfer to an AgentID.

One is unable to put a conference or consultative call on hold, therefore the button is disabled.

There is a delay in 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 ICM software, but the switch will reject 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 the same as the Nortel Meridian Status and Cause values (See Table 10-7 and Table 10-8).

### Nortel Symposium

- The Peripheral Gateway (and thus CTI OS clients) will not receive a CallEstablished Event for an off-switch call. As a result of this limitation, some features—such as blind conference or transfer operation off-switch—are not supported. The soft phone has no way to know that the call has been connected off-switch, and thus the application requires manual intervention from the agent (who will either hear 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/blind transfer or conference is not supported. Transfer and conference calls must be consultative.
- Consultative Transfer to a Supervisor is not supported.
- One is unable to transfer to an AgentID.
- One is unable to put a conference or consultative call on hold, therefore the button is disabled.
- There is a delay in 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 ICM software, but the switch will reject 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 the same as the Nortel Meridian Status and Cause values (See Table 10-7 and Table 10-8).

### Rockwell Spectrum

- The dialed number is used for AgentID, AgentExtension, and AgentInstrument, except during agent login.

<table>
<thead>
<tr>
<th>Cause Value (hex/dec)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014 / 8212</td>
<td>Agent ID is invalid</td>
</tr>
<tr>
<td>2015 / 8213</td>
<td>CFW DN IE is invalid</td>
</tr>
<tr>
<td>2016 / 8214</td>
<td>The Call Forward DN is too long</td>
</tr>
<tr>
<td>2017 / 8215</td>
<td>The Call Forward DN is invalid</td>
</tr>
<tr>
<td>2018 / 8216</td>
<td>User is invoking Call Forward</td>
</tr>
<tr>
<td>2019 / 8217</td>
<td>MSB/MSI not supported for 500/2500 sets</td>
</tr>
<tr>
<td>201A / 8218</td>
<td>500/2500 ACD agent already changed status</td>
</tr>
<tr>
<td>201B / 8219</td>
<td>500/2500 ACD agent set is being rung</td>
</tr>
<tr>
<td>201C / 8220</td>
<td>User is manually logging in 500 /2500 ACD set</td>
</tr>
<tr>
<td>201D / 8221</td>
<td>Meridian Link Server Option 209 is not equipped</td>
</tr>
</tbody>
</table>
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 time out 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 needs to 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 individually control each call. 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 greater.

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 Logout.

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. Once you make this call, the Transfer Complete and Conference Complete buttons become available to complete the desired action.

Siemens Hicom (North American Version)

---

**Note**

CTI OS currently supports only the North American version of the Siemens Hicom switch. The European version (Siemens Hicom 300 E) is *not* supported.
• The Release, Hold and Retrieve buttons are enabled when there is only one call on the device. The Release button is enabled when that call’s state is Initiating, Talking, Failed, or OnHold. The Hold button is enabled when that call’s state is Talking, and the Retrieve button is enabled when the call’s state is OnHold.

• When there are two calls at the device, one of which is a consult call, either call may only be hung up via the Reconnect button. Holding and retrieving the calls is accomplished via the Alternate button. To hang up the held call, it is necessary to Alternate first before Reconnecting.

• If there are two calls at the device, and the other party on the Talking call hangs up, the Held call may only be retrieved via the Reconnect button.

• Neither Single Step Transfer nor Single Step Conference are supported. However, Blind Transfer (completing the transfer before the consulted agent answers) is supported.

• SendDTMFSignal Request is valid only for trunk calls; it will fail if called via an inside call.

• If an agent has put another agent on hold, the second agent may not initiate a transfer or a conference until the first agent retrieves the call. For example:
  – Agent1 is talking to Agent2 and Agent1 clicks Hold
  – Agent2’s Transfer_Init and Conference_Init buttons are disabled until Agent1 clicks Retrieve. (Agent1 will also see the same disablement because these actions are not allowed for a held call.) When Agent1 clicks Retrieve, the Transfer_Init and Conference_Init buttons will reenable on both agent’s softphones.
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 10-9  Agent State Functionality and Call Center Terminology

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Alcatel: Idle</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: Avail</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: AVAIL</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: WAIT, DNIHOLD&lt;ACD Ready&gt;, DNOHOLD&lt;ACD Ready&gt; (these last two states occur only if ACAA is set for the ACD DN in LD 23)</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: Idle</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: Available</td>
</tr>
<tr>
<td>BusyOther</td>
<td>Alcatel: no equivalent (only one Skill Group)</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: MSG (if Aspect Event Link is not being used)</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: OTHER</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: NOT AVAIL</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: Busy (on either an internal call or a call for an agent group other than the agent’s primary group)</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: no equivalent (login to multiple Skill Groups not allowed)</td>
</tr>
<tr>
<td>Hold</td>
<td>Alcatel: Busy</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: HOLD</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: On Hold, On Hold Walkaway</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: no equivalent</td>
</tr>
<tr>
<td>Login</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 10-9  Agent State Functionality and Call Center Terminology (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logout</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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 Meridian: SPARE  
Nortel Symposium: Logout  
Rockwell Spectrum: Signed Off  
Siemens Hicom: Logged Off |
| **NotReady** |                                |
| The agent is logged in but is unavailable for any call work. | Alcatel: Pause/Withdrawn/No agent group after login (pre-assigned state)  
Aspect Contact Server: Idle  
Avaya DEFINITY ECS: AUX  
Nortel Meridian: WALKAWAY (however, this requires the agent to click Hold and physically unplug the headset – since a physical act is involved, a software request to set the agent state to NotReady will fail)  
Nortel Symposium: Not Ready Walkaway (however, this requires the agent to click Hold and physically unplug the headset – since a physical act is involved, a software request to set the agent state to NotReady will fail), Emergency  
Rockwell Spectrum: any state in which the Available console lamp is not lit  
Siemens Hicom: Unavailable |
| **Reserved** |                                |
| The agent is reserved for a call that will arrive at the ACD shortly. | Alcatel: no equivalent  
Aspect Contact Server: RSVD  
Avaya DEFINITY ECS: no equivalent  
Nortel Meridian: RESERVED (for network ACD calls)  
Nortel Symposium: Call Presented  
Rockwell Spectrum: no equivalent  
Siemens Hicom: Reserved |
### Table 10-9  Agent State Functionality and Call Center Terminology (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Peripheral-Specific Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Talking</strong></td>
<td><strong>Alcatel:</strong> Busy</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: Talking ACD1, Talking ACD2,</td>
</tr>
<tr>
<td></td>
<td>Talking ACT1, Talking ACT2, Talking Out1, Talking Out2, Talking</td>
</tr>
<tr>
<td></td>
<td>Inside, Supervisor Line, MSG, HELP</td>
</tr>
<tr>
<td></td>
<td>(MSG and HELP correspond to Talking only if Aspect Event Link is</td>
</tr>
<tr>
<td></td>
<td>being used)</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: AUX-IN, AUX-OUT, ACD-IN, ACD-OUT, ACW-IN,</td>
</tr>
<tr>
<td></td>
<td>ACW-OUT, DACD</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: ACD, ACDH, ACDHOLD, DNIN, DNIOUT, DNIHOLD, DNIOUT,</td>
</tr>
<tr>
<td></td>
<td>NRDY</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: Active, Consultation</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: Busy (other than cases listed under BusyOther)</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: Ready</td>
</tr>
<tr>
<td><strong>Unknown</strong></td>
<td><strong>Alcatel:</strong> no equivalent</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: UNKNOWN</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: no equivalent</td>
</tr>
<tr>
<td><strong>WorkNotReady</strong></td>
<td><strong>Alcatel:</strong> no equivalent</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: no equivalent</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: Call work (with Available console lamp not lit)</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: no equivalent</td>
</tr>
<tr>
<td><strong>WorkReady</strong></td>
<td><strong>Alcatel:</strong> Working After Call/Wrapup (may be manually invoked)</td>
</tr>
<tr>
<td></td>
<td>Aspect Contact Server: Wrap-up</td>
</tr>
<tr>
<td></td>
<td>Avaya DEFINITY ECS: ACW, DACW</td>
</tr>
<tr>
<td></td>
<td>Nortel Meridian: NOT READY</td>
</tr>
<tr>
<td></td>
<td>Nortel Symposium: Not Ready, Break, Busy</td>
</tr>
<tr>
<td></td>
<td>Rockwell Spectrum: Call work (with Available console lamp lit)</td>
</tr>
<tr>
<td></td>
<td>Siemens Hicom: Work Not Ready</td>
</tr>
</tbody>
</table>
Testing an Ethernet Card for Silent Monitor

On a site where IP telephony is or will be deployed, the Cisco Call Manager 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 VLAN, 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. Considering all the facts stated thus far, 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 watches the channel and collects Ethernet frames addressed to the agent’s computer. The NIC then runs a pre-processing 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, i.e. 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.

![Diagram showing test setup](image)

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 a good number of 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](http://www.caida.org/tools/taxonomy/workload.xml). The following sections demonstrate the use of Sniffer Pro.

Once the environment is setup as described above you will have to 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, consider the “Intel Pro/100” NIC card whose MAC address is 00D059d8f7d9.

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 our example we are interested on the interface number 1 that 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.
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

<table>
<thead>
<tr>
<th>Objective</th>
<th>Verify that the Test Target NIC is able to pre-process VLAN packets and able to forward them to the TCP/IP stack on the Test Target Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps</td>
<td>Party</td>
</tr>
<tr>
<td>1</td>
<td>PA</td>
</tr>
<tr>
<td>2</td>
<td>PA</td>
</tr>
<tr>
<td>3</td>
<td>PA</td>
</tr>
<tr>
<td>4</td>
<td>PA</td>
</tr>
<tr>
<td>5</td>
<td>WD</td>
</tr>
<tr>
<td>Expected Result</td>
<td>At the Test Target computer windump will display five packets for VLAN ID = 85 as shown on Figure A-2. If the test failed, no packets will be displayed at all</td>
</tr>
</tbody>
</table>
Appendix A  Testing an Ethernet Card for Silent Monitor

Test Procedure

Figure A-1  Modifying the Destination MAC address

If the outcome of this test is successful then your Test Target NIC will work with CTI OS Silent Monitor. Otherwise please 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 such that your packet analyzer tool can capture and display them. Then apply the appropriate adjustments and re-run this test procedure.
Appendix A  Testing an Ethernet Card for Silent Monitor

Test Procedure
**INDEX**

**A**

ACD CDN 10-2  
ACD DN 10-2  
ACP1000 10-2, 10-3, 10-4, 10-21  
Agent Desktop installation 3-1, 7-1  
Agent group (Aspect CallCenter) 10-2  
Agent registry key 8-7  
Agents, peripheral terminology 10-2  
Agent states 10-21  
Agent Statistics grid 8-25  
Alcatel 10-2, 10-3, 10-4, 10-6, 10-21  
Application, Rockwell Spectrum 10-2  
Aspect 10-2, 10-3, 10-4, 10-6, 10-21  
Available state 10-21  
Avaya 10-2, 10-3, 10-4, 10-7, 10-21  

**B**

BusyOther state 10-21  

**C**

CallAppearance registry key 8-20  
CallCenter 10-2, 10-3, 10-4, 10-6, 10-21  
Call events 10-4  
Call Object registry key 8-9  
ConnectionProfiles registry key 8-16  
Connections registry key 8-11  
CTI Driver registry key 8-3  
CTI OS  
advantages 1-2  
application architecture 1-1  

**D**

DEFINITY 10-2, 10-3, 10-4, 10-7, 10-21  
DMS-100 10-2, 10-3, 10-4, 10-21  

**E**

ECC registry key 8-20  
EMS registry key 8-5  
Enterprise Agent 10-12  
Ericsson 10-2, 10-3, 10-4, 10-21  
Events  
call 10-4  

**G**

Galaxy 10-2, 10-3, 10-4  

**H**

Hicom 10-2, 10-3, 10-4, 10-21  
Hold state 10-21  
Hunt group (Avaya DEFINITY) 10-2  

**I**

ICM Service Control 9-1  
installation  

**CTI OS**

advantages 1-2  
application architecture 1-1  
benefits 1-2  
CTI OS Server installation 2-3  
CTI OS system processes 9-2  
CTI support by peripherals 10-4
Index

CTI Client component 3-1
CTI OS Server 2-3
Instrument (Aspect CallCenter) 10-2
IPCC 10-12

L

Limitations of peripherals
CTI 10-6
ICM 10-3
Login state 10-21
Logout registry key 8-8
Logout state 10-22

M

Meridian 10-2, 10-3, 10-4, 10-14, 10-21

N

NEC NEAX 10-2, 10-3, 10-4, 10-21
Nortel 10-2, 10-3, 10-4, 10-14, 10-21
Nortel Sypmosium 10-18
NotReady registry key 8-9
NotReady state 10-22

P

Peers registry key 8-12
Peripherals
CTI support 10-4
limitations 10-3
Peripheral-specific
limitations, CTI 10-6
support 10-1
terminology 10-2
Peripherals registry key 8-12
Peripheral targets, peripheral terminology 10-2

R

ReasonCodes registry key 8-8
registry keys
Agent 8-7
CallAppearance 8-20
Call Object 8-9
ConnectionProfiles 8-16
Connections 8-11
CTI Driver 8-3
ECC 8-20
EMS 8-5
Logout 8-8
NotReady 8-9
Peers 8-12
Peripherals 8-12
ReasonCodes 8-8
Server 8-6
SkillGroup 8-13
Supervisor 8-14
TimerService 8-14
WrapupStrings 8-9
Reserved state 10-22
Rockwell 10-2, 10-3, 10-4, 10-18, 10-21
Rolm 10-2, 10-3, 10-4
Routes, Nortel Meridian 10-2

S

Server registry key 8-6
Services, peripheral terminology 10-2
Siemens 10-2, 10-3, 10-4, 10-21
SkillGroup registry key 8-13
Skill groups
base 10-3
DEFINITY ECS 10-2
peripheral terminology 10-2
primary 10-3
secondary 10-3
Skill Group Statistics grid 8-26
Spectrum 10-2, 10-3, 10-4, 10-18, 10-21
starting CTI OS 9-1
States, agent 10-21
stopping CTI OS 9-1
Supervisor registry key 8-14
Support, peripheral-specific 10-1

T
Talking state 10-23
Terminology, peripheral-specific 10-2
TimerService registry key 8-14
Trunk groups, peripheral terminology 10-2
Trunks, peripheral terminology 10-2

U
Unknown state 10-23

V
VDN 10-2
Vector Directory Number (VDN) 10-2

W
Windows Registry Editor 8-2
WorkNotReady state 10-23
WorkReady state 10-23
WrapupStrings registry key 8-9