CTI OS Troubleshooting Guide
for Cisco ICM/Contact Center Enterprise & Hosted
Release 7.5(1)
July 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
CONTENTS

About This Guide  v

Purpose  v
How to Use this Manual  v
What if I cannot resolve the problem?  v

Audience  v

Organization  vi

Related Documentation  2-vi

Conventions  vii

Obtaining Documentation and Submitting a Service Request  2-vii

Documentation Feedback  2-vii

CHAPTER 1

Problems and Symptoms  1-1

CTI OS Server Problems  1-1
CTI OS Server Cannot Connect to CTI Server  1-1
Problems Using Multiple Peripherals  1-2

General Softphone/Desktop Problems  1-3
Startup Problems  1-3
Login Problems  1-3
Logout Problems  1-6
Miscellaneous Button Problems  1-7
Miscellaneous Behavior Problems  1-7
Problems Making Calls  1-9
Problems Receiving Calls  1-9
Problems While Talking on a Call  1-11
Problems After Call Ends  1-11
Statistics Problems  1-12
Problems with ECC Variables  1-13

Failover Problems  1-14
Emergency and Supervisor Assist Problems  1-15
Chat Problems  1-16
CTI Server Connection-Loss Problems  1-16

Supervisor Feature Problems (IPCC Only)  1-17
Supervisor Button Problems  1-17
Problems with Real Time Status Window  1-17
About This Guide

Purpose

This manual provides information about troubleshooting the CTI OS product. It presumes that the ICM software, CTI Server, and CTI OS products have already been installed.

Refer to the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for the product description, architecture, installation, and configuration information for the CTI OS product. See [http://www.cisco.com](http://www.cisco.com) for the complete set of ICM manuals.

How to Use this Manual

This manual is organized by symptom and diagnosis. To diagnose a problem, search the table of contents for the problem description that best fits your symptoms. The document groups related symptoms into sections. Many symptom descriptions are similar, so it will be helpful to read all of the symptoms/solutions within the sections related to what you are seeing. Reviewing the troubleshooting steps for each of these problems will help ensure that your system is correctly installed and configured.

For each problem, the following information is provided:

- Problem/symptom description
- Possible causes
- Steps to diagnose and resolve

What if I cannot resolve the problem?

If the problem you are experiencing is not described in this guide, or the steps to resolve the problem have not worked for you, there is help available. For information on how to get technical assistance, see the “Obtaining Documentation and Submitting a Service Request” section.

Audience

This manual is intended for both non-programmers and programmers who want to learn about CTI in general, and Cisco CTI in particular. The reader of this manual need not have knowledge of Intelligent Contact Management (ICM) software; however, a knowledge of ICM software is necessary for implementing Cisco CTI.
Organization

The following table describes the information contained in each chapter of this guide.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Problems and Symptoms”</td>
<td>Contains troubleshooting steps to diagnose and resolve problems.</td>
</tr>
<tr>
<td>Chapter 2, “Resolutions to Common Problems”</td>
<td>Describes common CTI OS problems, their possible symptoms, and a procedure to correct the problem.</td>
</tr>
<tr>
<td>Appendix A, “Troubleshooting Checklist”</td>
<td>Provides a checklist for troubleshooting CTI OS Installation.</td>
</tr>
<tr>
<td>Appendix C, “CTI OS FAQs”</td>
<td>Contains important facts about CTI OS.</td>
</tr>
</tbody>
</table>

Related Documentation

Documentation for Cisco Unified ICM/Unified Contact Center (IPCC) Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at http://www.cisco.com/web/psa/products/index.html.


  For documentation for these Cisco Unified Contact Center Products, go to http://www.cisco.com/web/psa/products/index.html click on Voice and Unified Communications, then click on Cisco Unified Contact Center Products or Cisco Unified Voice Self-Service Products, then click on the product/option you are interested in.

- Also related is the documentation for Cisco Unified Communications Manager, which can also be accessed from http://www.cisco.com/web/psa/products/index.html


- The Product Alert tool can be accessed through (login required) http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice
Conventions

This manual uses the following conventions.

<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>• A <strong>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>(condition, true-value, false-value)</td>
</tr>
<tr>
<td>• A generic syntax item that you must replace with a specific value</td>
<td>• For more information, see the <strong>Cisco ICM Software Database Schema Handbook</strong>.</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>

Obtaining Documentation and Submitting a Service Request

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


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

Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.
Problems and Symptoms

This section is organized by problem descriptions, and contains troubleshooting steps to diagnose and resolve each problem.

CTI OS Server Problems

This section discusses some common CTI OS Server problems.

CTI OS Server Cannot Connect to CTI Server

Symptom  Error messages in the CTI OS Server console window indicate that it is unable to establish a connection to the CTI Server.

Possible Cause  There are several possible causes, the most common of which are related to TCP/IP networking problems. The CTI OS Server console window should display an error message with an error description. Some possible causes of this symptom are:

- CTI OS Server may not be configured with the proper information as to the location of CTI Server. Check the configured CTI Server hosts (SideAHost and SideBHost) and ports (SideAPort and SideBPort) in the registry at the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\CtiDriver\Config
```

- If the configuration is correct, CTI OS Server may not be able to identify the host and/or make a TCP/IP connection to the CTI Server. Your TCP/IP network administrator should be able to help resolve any TCP/IP hostname/routing issues.

- If the TCP/IP "target machine refused connection" error displays in the CTI OS Server console window, then you should ensure that the CTI Server is running as expected. Look for its console window on the target system, and note the IP port that it is listening on. Check that this is indeed the port number configured in the registry for CTI OS, under the key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\CtiDriver\Config
```
CTI OS Server Problems

Chapter 1  Problems and Symptoms

Problems Using Multiple Peripherals

Symptom  CTI OS Server does not allow login to a specific peripheral in a multiple peripheral environment (for example, multiple CallManagers in the same cluster).

Possible Cause  The current versions of the product (CTI OS Server version 4.6.1 and up) can connect to a single CTI Server only, which in turn communicates to a single PG (Peripheral Gateway). The CTI OS Server will be able to communicate to any and all peripherals configured on this same PG. For example, on IPCC Enterprise there can be multiple PIMs (peripheral interfaces) running on one PG at the same time. In this case, CTI OS will be able to access all of these co-located PIMs via one CTI Server.

To be able to login a CTI OS softphone to a peripheral, the CTI OS Server must be configured with the PeripheralID (from ICM configuration) and PeripheralType (see Appendix C, “CTI OS FAQs,” for a list of supported Peripheral Types) of each Peripheral on the PG. This information is stored in the registry on the CTI OS Server computer under HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>_\ctios1\Server\Peripherals. This registry entry is a table, where each entry is named by a Logical Name (for example, IPCC ACD1). Each entry contains the PeripheralID and PeripheralType for the peripheral specified by the Logical Name.

If you are using the out-of-box softphone or controls, you also need a valid connection profile for each peripheral.

Refer to the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for a complete explanation of configuring peripherals and connection profiles in the CTI OS Server.

Symptom  Secure CTI OS server cannot connect to a peer CTI OS server

Possible Cause  This symptom may have multiple causes:

- Make sure that security is enabled in the peer CTI OS server. If security is On, then SecurityEnabled registry value is 1, otherwise it is 0. This registry value exists under HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<customer-instance>_\CTIOS1\server\security

- Make sure that the certificates on both servers are configured correctly and are signed by the same certificate authority (CA). Refer to the CTI OS system manager guide for CTI OS Security configuration.

Symptom  CTI Toolkit monitor mode application cannot connect to Secure CTI OS server.

Possible Cause  This symptom may have multiple causes:

- Make sure that either CTI toolkit C++ or COM monitor mode applications are running. Both Java CIL and .NET CIL do not support security.
- Make sure that the certificates on both CTI OS server and CTI Toolkit are configured correctly and are signed by the same certificate authority (CA). Refer to the CTI OS System Manager Guide for CTI OS Security configuration.
- Make sure that you are using the right monitor mode password. CTI OS server asks for monitor mode password during CTI OS security configuration. If the CTI OS server has a peer server, then this password needs to be the same in both servers.

**Symptom**  
CTI Toolkit cannot connect to Secure CTI OS server.

**Possible Cause**  
This symptom may have multiple causes:
- Make sure that either CTI toolkit C++ or COM applications are running. Both Java CIL and .NET CIL do not support security.
- Make sure that the certificates on both CTI OS server and CTI Toolkit are configured correctly and are signed by the same certificate authority (CA). Refer to the CTI OS system manager guide for CTI OS Security configuration.

**General Softphone/Desktop Problems**

This section discusses softphone and desktop related problems.

**Startup Problems**

**Symptom**  
There are no buttons enabled when the softphone starts and the status bar indicates Disconnected.

**Possible Cause**  
This symptom indicates that the softphone is unable to connect to a CTI OS Server to get configuration information. This may be due to an incorrectly configured or unreachable configuration server. See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.

**Login Problems**

**Symptom**  
The softphone starts correctly but when I attempt to login (that is, click the Login button, enter login information, and click OK), nothing happens. None of the buttons are enabled. In the status bar, the Extension, Instrument, Agent ID, and Agent Status fields are blank and the rightmost fields display Disconnected and Offline.

**Note**  
NOTE: This behavior may be sporadic between system restarts.
**Possible Cause** This symptom is caused by the softphone's inability to connect to the CTI OS Server(s) specified in the connection profile chosen from the Connect to drop-down list in the login dialog. This is due to an incorrectly configured or unreachable CTI OS server in the connection profile. See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.

**Symptom** The softphone starts correctly but when I attempt to login (that is, click the Login button, enter login information, and press OK), none of the buttons are enabled. In the status bar, the Extension, Instrument, Agent ID, and Agent Status fields are filled in correctly, the rightmost field says Online, and the field next to it displays the server with which the softphone is connected.

**Note** This problem may be sporadic between system restarts.

**Possible Cause** This symptom is most likely caused by an incorrect configuration of the Peripheral ID or Peripheral Type during server install. See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.

**Symptom** The softphone starts correctly but when I attempt to login (that is, click the Login button, enter login information, and press OK), the softphone displays a message box that says: *System is offline. Login will be queued until system is back online.* When I look on the PG and on the CTI OS server, I can see that everything in the system is online.

**Note** This problem may be sporadic between system restarts.

**Possible Cause** This symptom is most likely caused by an incorrect configuration of the Peripheral ID in the connection profile that the client is using to login. See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.

**Symptom** Duplicate Login: The softphone starts correctly but when I attempt to login (that is, click the Login button, enter login information, and press OK), the softphone displays a message box that says: *Agent with ID <xx> is already logged in. To use Agent ID <xx> please logout first or contact an Administrator for help.*

**Possible Cause** This error message indicates that the Agent with this ID is already logged into a session and the CTI OS system has been configured to prevent duplicate logins to the same AgentID. The other active session must logout this agent first. If you do not want this preventive mechanism, then set the following registry key to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS
 \CTIOS_<InstanceName>\ctios1
 EnterpriseDesktopSettings\All Desktops\ Login \ConnectionProfiles
 \Name<YourConnectionProfileName>\RejectIfAlreadyLoggedIn
```

**Note** In the default Installation, this key is disabled and therefore will not prevent duplicate logins.
Symptom (Spectrum specific): When attempting a login (that is, click the Login button, enter login information, and click OK), the phone appears to freeze. All buttons are disabled and no error message displays indicating failure.

Possible Cause On Spectrum, Login parameters required from the user are AgentID, AgentInstrument (which corresponds to the extension that the Agent can be reached at) and the PositionID (indication of the physical device). If the AgentID and PositionID entered are correct, but the AgentInstrument entered is invalid it causes the phone to freeze. Restart the softphone and re-enter the Login information correctly and try again. A message displays indicating that the agent is already logged in (this is expected) but otherwise, the Login will have completed normally.

The registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\EnterpriseDesktopSettings\All Desksop\Login\ConnectionProfiles\Name\<YourConnectionProfileName>\LoginTimeout

can be set to a timeout interval appropriate for your Spectrum configuration and this will pop up an error dialog that will allow you to retry the login after the specified interval. This way you can avoid restarting the softphone. Make sure that the following registry key is disabled (set to 0) at the same time:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\EnterpriseDesktopSettings\All Desksop\Login\ConnectionProfiles\Name\<YourConnectionProfileName>\RejectIfAlreadyLoggedIn

Symptom When logging in via the CTI OS Agent or Supervisor Desktop, the Login request fails with the "Invalid AgentID" or "Invalid Login Name" error (for IPCC only).

Possible Cause If this is not user error or a typo, you may be trying to Login with AgentID when your desktop has been configured to login by LoginName or vice-versa (depending on the error message). Check the Login dialog and make sure you are entering the appropriate argument in the first edit field. As of CTI OS 7.x, support for Login by Login Name (instead of AgentID) is available only for IPCC Enterprise. While installing CTI OS 7.x (or upgrading to it) there is an option on screen where the peripheral type is selected where the user can pick the Login style for the CTI OS Agent/Supervisor desktop. The default preserves the "old" way of logging in by AgentID. This setting does not limit a custom application which can send a login request with either option.
Logout Problems

Symptom  Logout button is not enabled.

Possible Cause  Agent may not be in the appropriate state required for logout. This varies from switch to switch. For example, with IPCC the agent has to be in a Not Ready state to be able to logout.

Symptom  (IPCC specific): Agent gets logged out unexpectedly (did not intend to log out).

Possible Cause  There are several possible causes of this symptom:

- There is a timeout called "Logout Non-activity time" that will logout an agent after a certain period of time (maximum 7200 seconds or 2 hours). It is part of the AgentDeskSettings and can be configured using the ICM Configuration Manager. This timeout cannot be disabled at this time.

- There may be another CTI Toolkit using the same agent and instrument from another location. If that client logs out, your softphone will be logged out as well. To prevent duplicate logins to the same agentID/instrument, use the registry key "RejectIfAlreadyLoggedIn" in the ConnectionProfile being used. For details, see Symptom “Duplicate Login” in preceding section dealing with Login problems.

- If your agent is a member of an agent team, your supervisor may have logged you out.

- Check the status bar. A status of Offline means that some element in the system has failed or gone offline. The system will automatically recover from this situation. Wait for the status bar to indicate Online and login again.

Symptom  (under all ACDs) Agents are getting intermittently logged out of their CTI applications

Possible Cause  When the PIM is set to /LOAD 1, and two CTI OS Servers are connected to the same CTI Server, the following situation may occur:

- Agent mode connection for agent A established to CTI OS A
- Agent mode connection for agent A established to CTI OS B
- Disconnect agent mode connection from CTI OS A

At this point, the agent using the application with the connection established to CTI OS B is logged out.

Note  Under such conditions, to ensure that the agents are not logged out, configure the PIM for /LOAD 0.
**Miscellaneous Button Problems**

**Symptom** When clicking any enabled button nothing happens (no visible change in softphone appearance and no error message).

**Possible Cause** This symptom usually indicates that the system has gone offline and is recovering from some sort of failure. Check the status bar. A status of Offline means that some element in the system has failed or gone offline. The system will automatically recover from this situation. Wait for the status bar to indicate Online and try again.

**Symptom** When clicking an enabled button an error message displays.

**Possible Cause** Check the specifics of the error message to pinpoint the problem. Consult with your ACD/PBX switch resource person to evaluate any third-party problems.

**Symptom** On Windows XP systems that have installed the Oracle 32 bit client, some icons on the CTI OS Agent Desktop or CTI Toolkit IPCC Supervisor Desktop appear as black squares.

**Possible Cause** Oracle install has registered old COM components. It may be possible to correct this problem by performing the following steps:

- Shut down all applications, including the desktop
- Open a command prompt window
- CD to c:\windows\system32
- Run regsvr32 oleaut32.dll
- When a “DllRegisterServer succeeded” message box appears, click OK
- Restart the desktop

**Miscellaneous Behavior Problems**

**Symptom** The CTI OS Desktop does not prompt for Logout and/or NotReady reason codes on TDM (non-IPCC) switches.

**Possible Cause** The LogoutReasonRequired and NotReadyReasonRequired registry values must be used to enable this functionality. (Refer to the CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for information.) In brief, the registry keys listed below need to be set to 1.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\LogoutReasonRequired`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\NotReadyReasonRequired`
Symptom: The CTI OS Desktop does not prompt for Wrapup Data when agents go into Wrapup state and the call is in a cleared state on TDM (non IPCC) switches.

Possible Cause: The EnableWrapupDialog and WrapupDataRequired registry values must be used to enable this functionality for a TDM switch. (Refer to the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for information.) In brief, the registry keys listed below need to be enabled as needed.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ CTIOS_<InstanceName>\ctios1\Server\Agent\ EnableWrapupDialog
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ CTIOS_<InstanceName>\ctios1\Server\Agent\ WrapupDataRequired
```

Symptom: How do I disable the WrapupData dialog for the CTI OS Desktop with IPCC and still have my Agents go into Wrapup state after a call?

Possible Cause: If the EnableWrapupDialog registry value is set to 0, the dialog will be disabled on the CTI OS desktops. This will, however, not be the case if the Agent's Desk Settings for Incoming Wrapup are set to RequiredWithData in the ICM Configuration utility. (Refer to the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for information.)

Symptom: The softphone starts correctly and the login request is successful. However, thereafter one (or more) of the following behaviors is observed:

- Message boxes display stating that parameters are incorrect (for example, the request specified an invalid AgentID).
- Message boxes display stating that arguments are missing (for example, SetAgentState: Missing required argument PositionID. Discarding request).
- Incorrect buttons are enabled.

Note: This problem may be sporadic between logins.

Possible Cause: This symptom is most likely caused by an incorrect configuration of the Peripheral Type during server install. See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.
Symptom After a CTI Toolkit Install, you have started the Agent Desktop, and you receive the following error box:

Possible Cause You have not rebooted after a CTI Toolkit Install

Note Always reboot the machine if the CTI OS Server, or the Client Desktop Install, requests it.

Problems Making Calls

Symptom When attempting to make a call, the dial pad displays but there is no Make Call button visible.

Possible Cause This symptom may occur if you are in an agent state that does not allow you to make a call (for example, for IPCC Enterprise your agent state must be NotReady in order to make a call. You may not make a call if your agent state is Available). Change to the appropriate state and try again.

Problems Receiving Calls

Symptom Agent cannot receive any calls including calls dialed directly to the extension.

Possible Cause Check the following:
- Check that your agent is logged in. An agent must be logged in to receive calls.
- Check the status bar. A status of Offline means that some element in the system has failed or gone offline. The system will automatically recover from this situation. Wait for the status bar to indicate Online and try again.

**Symptom**  Agent cannot receive any customer calls but can receive calls to the extension.

**Possible Cause**  If an agent is having trouble receiving customer calls, try the following steps:

- Ensure that your agent is properly logged into the system and is in a state that allows it to receive calls (for example, on most ACD systems, your agent must be in the Available state in order to receive customer calls; an agent can receive agent-to-agent calls in both Available and Not Ready states).
- Check your ICM software configuration and ensure that your agent belongs to a queue that gets calls routed to it by the ICM.

**Symptom**  Agent receives calls, but loses them after a few seconds before they can be answered.

**Possible Cause**  The Ring No Answer feature is probably set on your ICM system. Open the ICM Configuration Manager and increase that value or disable it all together.
Problems While Talking on a Call

Symptom: All three AgentState buttons (Available/Ready, NotReady and Wrapup) are enabled while I am talking.

Possible Cause: Wrapup mode (configured in the ICM Configuration Manager's Agent Desk Settings) for this call is set to OPTIONAL. Therefore, clicking any of these three buttons will determine what state you will go to after you hang up the call. If you click Wrapup, you will see the Wrapup dialog pop up after you hang up, but you are not required to enter data.

Symptom: IPCC Only: None of the AgentState buttons are enabled while I am talking.

Possible Cause: Wrapup mode (configured in the ICM Configuration Manager's Agent Desk Settings) for this call is set to either REQUIRED or REQUIRED_WITH_DATA. Therefore, you have no choice as to what state you will go to after you hang up this call - you will automatically go to Wrapup state.

Symptom: IPCC Only: Only the Available/Ready & NotReady buttons are enabled while I am talking, the Wrapup button is disabled.

Possible Cause: Wrapup mode (configured in the ICM Configuration Manager's Agent Desk Settings) for this call is NOT_ALLOWED. This means that you are not allowed to go to the Wrapup state; therefore, it will never be enabled.

Problems After Call Ends

Symptom: Call remains on the softphone call appearance grid after call end.

Possible Cause: Usually this is indicative of having not yet received or missing an end call event. Possible things to check for:

- Check if your agent is in Wrapup state. If it is, then enter wrapup data (if desired) and click the Available/Ready or Not Ready button to get out of this state and the call should disappear from the grid.

- Check the status bar. A status of Offline means that some element in the system has failed or gone offline. The system will automatically recover from this situation. Wait for the status bar to indicate Online and the call should disappear from the grid.

- If the call is indeed gone from the phone (that is, no voice), and you still cannot get rid of the call entry in the grid, you can logout, and log back in and that should clear it. If however the call reappears again after the login, then it must still be in a Wrapup state somewhere in the system, so you or another party that was on the call must end it by changing the agent state to Available or Not Ready.

Note: In CTI OS Release 7.0 onwards, an ENABLE_CLEARCALL bit mask indicates when it is appropriate to clear all call connections.
**Symptom**  IPCC Only: When the Wrapup dialog pops up, the strings in the combo box are set to *Insert incoming wrapup string 0 here, Insert incoming wrapup string 1 here, ....*, instead of to meaningful phrases.

**Possible Cause**  The CTI OS Server has not had its Wrapup strings configured correctly. The Wrapup codes and corresponding strings are located in the Registry of the CTI OS Server machine at: 

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\WrapupStrings\Incoming.
```

Replace the default Wrapup strings with more meaningful ones, adding more if necessary. NOTE: You must restart CTI OS Server and the softphone too for your changes to take effect. Refer to the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for details on how to configure Wrapup strings.

**Symptom**  IPCC Only: After either selecting a string from the listbox or entering a string into the edit box of the Wrapup dialog and clicking OK, an error message pops up stating: "SYSTEM ERROR: Unable to enter data because call [call.xx.yy.zz] has ended."

**Possible Cause**  The call ends too quickly so that data cannot be entered into it. Check the ICM Configuration Manager's Agent Desk Settings for this agent to ensure that the Wrapup Time is adequately long - recommended length is 120 (seconds).

**Symptom**  IPCC Only: While in Wrapup state, neither the Available/Ready nor the NotReady buttons are enabled to allow transition from the Wrapup state.

**Possible Cause**  This could happen if the application is waiting for Wrapup data before letting you leave the Wrapup state as will be the case if your Wrapup mode for this call is REQUIRED_WITH_DATA. Enter data via the Wrapup dialog, which should pop up after you hang up the call. If that is not available, you will have to wait until the configured "Wrapup Time" (set in the ICM Configuration Manager's Agent Desk Settings) has passed, after which you will automatically go to the Available/Ready or NotReady state.

**Symptom**  IPCC Only: The Wrapup dialog cannot be dismissed because the OK button is disabled.

**Possible Cause**  The OK button is disabled because your Wrapup mode (configured in the ICM's Agent Desk Settings) for this call is REQUIRED_WITH_DATA. Therefore you must either select one of the lines in the dialog, or enter your own data in the edit box before the OK button will enable.

**Statistics Problems**

**Symptom**  The values do not change in my agent statistics grid or skill group statistics grid.

**Possible Cause**  This symptom may have multiple causes:

- Check the status bar. A status of Offline means that some element in the system has failed or gone offline. The system will automatically recover from this situation. Wait for the status bar to indicate Online and statistics should continue to update.
The frequency at which statistics are updated is governed by registry entries on the CTI OS server. The period (in seconds) between updates of statistics is stored in PollingIntervalSec in the following registry keys:

**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\**

for agent statistics and

**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\SkillGroup**

for skill group statistics.

Check these values. If they are very high, statistics will not change for a very long period of time.

- Check that the statistics you have configured for your call appearance grid are valid for the CTI Server protocol version you are running. Unsupported statistics will never update. You can find the CTI Server protocol version in the registry. It is stored in ProtocolVersion in the following registry key:

**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\CtiDriver\Config**

You can find a list of the statistics supported for a particular protocol version (13) in the *Cisco ICM Software CTI Server Message Reference Guide (Protocol Version 13)*

---

**Problems with ECC Variables**

**Symptom**  Monitor mode application still receives all skill group statistics even though it is only configured for a small subset of skill group statistics in the CTI OS settings.

**Possible Cause**  Skill group statistics are not minimized in CTI OS versions before Release 4.7. This problem is fixed in Release 4.7 and later. A new optional registry setting, DisableMonitorModeStatsMinimization, may be added to disable statistics minimization for monitor mode applications. The *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* explains this setting. If you are running version 4.7 or later, check this registry setting. If it is present, set it to zero to enable statistics minimization.

---

**Problems with ECC Variables**

**Symptom**  When entering ECC data from the Make Call or Transfer/Conference dialog, the data does not make it into the call (that is, no data displays in the softphone call appearance grid).

**Possible Cause**  This symptom may have multiple causes:

- Check that the softphone call appearance grid is configured correctly in the CTI OS server registry. Call appearance grid configuration is described in the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* in Chapter 4. Remember that the ECC scalar/array name (“Name”) configured in the registry under the column number key is case-sensitive and must be the same as that configured in the ICM without the "user." prefix.
Failover Problems

This section discusses failover related problems.

Symptom  Agents do not fail over to alternate CTI OS.

Possible Cause  Ensure that the alternate host and port number are properly configured in the connection profile and that the host is reachable over the network. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)

Symptom  Desktop applications are “ping-ponging” (failing over periodically) between sides A and B of the CTI OS Server when there is no apparent failure in the system.

Possible Cause  This symptom occurs when the client application loses contact with the CTI OS server. This may be caused by a loss of network connectivity, extremely high network utilization, an overloaded CTI OS server, or because of security configuration. Check the following:

- Ensure that there is network connectivity between the client and the CTI OS server. From the client try to ping the IP address corresponding to the CTI OS server. If this fails, you have a network connectivity problem and your TCP/IP network administrator should be able to help resolve the issue.
- If security is turned ON on CTI OS server, then make sure that security is configured on both CTI OS server and CTI Toolkit. Refer to CTI OS System Manager’s Guide for CTI OS Security Configuration.
For certain system configurations, real-time statistics reporting can significantly load down a network. The default configurations for the desktop agent statistics grid and the desktop skill group statistics grid require large amounts of data to be sent from the server to the client for each statistics update. Factors that affect the network load imposed by real-time statistics include:

- **Statistics update interval** - The more frequently that statistics are updated, the higher the network load. The FAQ in Appendix B explains how to configure the update interval.
- **Skill groups per agent** - The more skill groups to which an agent belongs, the more data is sent to that agent's desktop for skill group statistics and the greater the load on the network.
- **Number of configured statistics grid columns** - The CTI OS server only sends those statistics that will be displayed on the statistics grids. The default is to send ALL statistics. You can configure your system to only display the statistics you really need. This would greatly reduce the amount of network traffic. The *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, Chapter 4, explains how to configure statistics.

**Symptom** The CTI OS server is "ping-ponging" (failing over periodically) between CTI Server sides A and B when no clients are connected.

**Possible Cause** In duplexed CTI server versions 4.6.2 and above, the CTI Server will periodically switch active sides if only CTI OS servers are connected to CTI Server and no clients are connected to any CTI OS server. This behavior was implemented to detect network outages that occur when no clients are connected. This will cause CTI OS to "ping-pong" as it follows the active CTI Server. This is normal behavior.

### Emergency and Supervisor Assist Problems

**Symptom** Clicking the "Emergency" and/or "Supervisor Assist" buttons on the Agent desktop causes an error message.

**Possible Cause** There are three possible reasons for this symptom:

- The agent may be in an inappropriate state. The "Emergency" and "Supervisor Assist" buttons operate similarly to the "Make Call" button in that they make a call to the supervisor. In order for these buttons to function correctly the agent must be in a state that allows it to make a call (for example, with IPCC, the agent must be in Not Ready state).
- The supervisor may be in an inappropriate state. The supervisor must be in Available/Ready state.
- There may be a problem with the ICM configuration. This functionality requires an ICM script (refer to *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*) for routing these calls as well as Supervisor and Agent Team configuration. A good test is to try this functionality with CTITest (emergency and assist commands). Also, a supervisor needs to be in the Available/Ready state to accept these types of calls.
Chat Problems

Symptom Chat does not seem to work.

Possible Cause This symptom may have several causes:
- Chat permission levels are configured in the CTI OS Server. The default chat level on install only allows agents to chat with supervisors. Refer to the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for details about the various chat levels and how to configure them.
- If you have more than one CTI OS server, ensure that the chat levels are set to the same values on all peer servers.
- If you have more than one CTI OS server, ensure that each server has the other server(s) configured as a peer server. This is required for routing chat messages between servers. If each client is connected to a different server and the peer is not configured correctly, those agents will not be able to chat with one another.

Symptom Agent A can send a message to agent B, but agent B cannot send a message to agent A on a system with multiple CTI OS servers.

Possible Cause It is possible that the agents are connected to different servers and the chat permission levels on those servers are not set the same. Ensure that the AgentChatLevel and SupervisorChatLevel settings are the same on all peer servers. For information on how to configure chat levels, refer to the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

Symptom When sending a chat message to an agent, an error message displays.

Possible Cause There is no way to tell beforehand if an agent is logged into CTI OS server. If you send a chat message to an agent that is not logged in, either of the following might occur:
- If the server is currently aware of the agent and the agent is in logout state, it will return a message indicating that the agent is not logged in.
- If the server has no current knowledge of the agent, it may return a message indicating that it cannot locate the chat target/recipient.

CTI Server Connection-Loss Problems

Symptom Connection to the CTI Server is lost owing to some state issues.

Possible Cause When the CTI OS server connects to CTI Server, it needs to download all configurations before accepting client connections. Therefore, owing to some state issues or config issues, when CTI OS loses the connection to CTI Server and must reconnect, it restarts so that all
client connections are dropped until the server rebuilds its state and configuration. The result of this will likely be that failover will take longer because clients lose their connections and have to reconnect.

### Supervisor Feature Problems (IPCC Only)

This section discusses problems related to the IPCC Supervisor feature.

#### Supervisor Button Problems

**Symptom**  Barge In button is not enabled.

**Possible Cause** A supervisor needs to be in Not Ready state to barge in. Furthermore, a supervisor can only barge into a call that is in Talking state.

**Symptom**  Barge In does not work - causes error message.

**Possible Cause** The Barge In feature uses conference functionality. From the CallManager configuration, check that the conference bridge is configured correctly and that it has been started. Also try to make a regular conference call. If Hardphones are available, try to make a conference call from the IP hardphone (will indicate if the conference bridge is not available).

**Symptom**  Intercept Button is not enabled.

**Possible Cause** A supervisor can only intercept a call to which he/she has barged-in. In CTI OS Releases 4.7 and later, a supervisor can also intercept a conference call.

**Symptom**  The Agent's "Supervisor Assist" and "Emergency" buttons do not work.

**Possible Cause** The assist and emergency buttons are implemented via an ICM routing script. This script needs to be configured and the agent team (see ICM Configuration Manager for Agent Team configuration) needs to be associated with this specific script. The best way to diagnose this problem is to look at the script in "Monitor Mode" and tune the configuration, until the script handles these calls.

#### Problems with Real Time Status Window

**Symptom**  After login, supervisor does not see his team members listed in the agent select grid.

**Possible Cause** Check the following items:

- Ensure that the team is configured correctly in the ICM configuration.
- Ensure that your supervisor has supervisor privileges in ICM configuration.
- Check the ServicesMask for CTI OS Server in the registry at
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS \CTIOS_<InstanceName>\ctios\CtiDriver\Config. It must be 0x1c0296 or decimal 1835670 - these values include supervisor services.

Symptom: Supervisor tried to log out an agent who has an active call and nothing happened.

Possible Cause: The IPCC PIM queues the request. The agent is logged out once the call has ended. To accomplish this, a supervisor can first barge-in and then intercept the call after clicking the agent Logout button. The supervisor should see a message displayed in a dialog box.

Symptom: In the supervisor desktop's real time status grid, some agents' skill groups are listed as NA when they actually do belong to at least one skill group.

Possible Cause: When a supervisor logs in, he/she sees all skill groups of agents currently logged in. Since CTI OS only learns about skill groups when agents are logged in, logged out agents might display NA (not available) in the Agent Real Time status window until these agents log in.

Symptom: A secondary supervisor is [is not] listed in the real time status window.

Possible Cause: Starting with CTI OS 4.7, secondary supervisors are only listed in the team status window if they are also configured as team members (See ICM Configuration Manager for the Agent Team configuration). Primary supervisors are never listed in the real time status window.
Silent Monitor Problems (IPCC Only)

Troubleshooting CTI OS Based Silent Monitor Problems

Symptom A supervisor has clicked the silent monitor start button, the session seems active (monitored indicator in the agent real-time status window for voice), but after a while the following message box appears:

Possible Cause

- The agent’s desktop PC is not plugged into the second port of the hardphone.
- The agent is logged into a device other than the hard phone to which his/her PC is connected.
- The Phone is not sending the packets because the PC port is deactivated.

Note

If the system is off the network, you may want to check the Network settings on the phone. Also, future CallManager versions might support a setting on the phone configuration page to enable/disable voice packets on the PC port of the phone.

- The PC cannot capture the voice packets sent from the phone. See “Determining if a PC can capture audio packets sent from an IP phone”
Symptom After just installing CTI OS Server Release 5.1 or later, CTI Toolkit Agent Desktop, and CTI Toolkit IPCC Supervisor Desktop (both with the Silent Monitor option), Silent Monitor does not work.

Possible Cause Make sure that the agent that is being monitored has the agent desktop system plugged into the back of the hardphone. In a duplex CTI OS environment, make sure that the CTI OS servers are configured as peers during the CTI OS server install. In a lab environment try temporarily shutting down one CTI OS server and try again. If it still does not work, please read the other symptom discussions in this section.

Symptom The Silent Monitor Button is not enabled on the CTI Toolkit IPCC Supervisor Desktop.

Possible Cause Possible reasons:
- When the Client was installed, the Silent Monitor option was not checked. Please reinstall and check the Silent Monitor option
- The supervisor is logged onto a connection profile (see the section about connection profiles in the CTI OS System Manager’s Guide) that has the registry key “IPCCSilentMonitorEnabled” set to 0 (1 means enabled and is the default) – either change this key or use a different connection profile
- The agent currently selected in the Real-Time grid is not logged on
- The CTI OS Server this client is currently connected to does not support Silent Monitor (that is, it is a release prior to Release 5.1)
- The supervisor is not logged on

Symptom A supervisor has clicked the silent monitor start button and after a while a message box appears indicating the session has timed out:

Possible Cause
- The agent is logged onto a connection profile, which has Silent Monitor disabled (see the section about connection profiles in the CTI OS System Manager’s Guide), that is, has the registry key “IPCCSilentMonitorEnabled” set to 0 (1 means enabled and is the default). Either change this key or use a different connection profile.
- The client selected for monitoring does not have Silent Monitor installed or does not support Silent Monitor (legacy client).
- The client is not available on the network. The client might have chosen to abort the CTI Toolkit software and close the CTI Toolkit Agent Desktop.
On certain systems it is necessary to reboot after installing WinPCap, which is installed with Silent Monitor option on the CTI Toolkit Agent Desktop. Please reboot and try again.

The agent or supervisor is not running CTI OS Release 5.1 or later.

On a Windows XP system, the Internet Connection Firewall (ICF) must be disabled in order for the agent PC to receive heartbeat packets. Check to ensure that the ICF on the agent PC is disabled. The ports for CTI OS and Silent Monitor should be accessible via a firewall if supervisors and/or agents are connected to a remote switch.

See the following Microsoft website for more information on how to check this setting and how to disable the ICF:


For details about backward compatibility refer to the Cisco Compatibility Matrix.

**Symptom** A supervisor has clicked the silent monitor start button, the session seems active (monitored indicator in the agent real-time status window for voice) but there is no monitored audio. The message box shown in the previous symptom does not appear. Other agents may be monitored successfully.

**Possible Cause** On rare occasions, if an agent logs into a desktop associated with a phone that already has an active call, the desktop may not be able to capture packets from that phone. This is due to the fact that the desktop does not know the IP address of the phone. The desktop automatically detects the address of the hardphone any time audio starts or stops on the phone (for example, call begins, hold, retrieve, call ends, and so forth). If the agent logs in after the call has already started, auto-detection does not take place. The desktop will assume that the phone is located at its last known address. If that address is incorrect, the desktop will be unable to capture packets. This problem will correct itself on the next call handled by the agent or when the agent performs an action that causes audio to start or stop.

It may also be possible that WinPcap 3.0 cannot enumerate the network devices on the system. This causes CTI OS Agent Softphone to not initiate the silent monitor session and not forward voice to the CTI Toolkit IPCC Supervisor Desktop.

To determine if this is the case, retrieve the CTI Toolkit Log from the agent’s computer and open it in a text editor. See if the following entries appear in the log file:

```
07/29/03 12:41:06.961   1800   CTIOSSoftphone
CSilentMonitorManager::StartSMMonitoredMode, (MonitoredDeviceID:2032
HeartBeatInterval:1 HeartbeatTimeout:3 MonitoringIPPort:8500)
07/29/03 12:41:06.961   1800   CTIOSSoftphone  CSMSniffer::Initialize : Pcap not
available on system or Pcap found no network device :
07/29/03 12:41:06.961   1800   CTIOSSoftphone  CIIOSObject(01CB27C8)::ReportError{
Code(-127) )
07/29/03 12:41:06.961   1800   CTIOSSoftphone  CSilentMonitorManager::m_pSMSniffer{
01CCA7B0 ): Error(268435458): Failed to initialize Sniffer
```

If these entries are present, you need to install the newest version of WinPcap available. See Installing WinPcap in Chapter 2 of this document for details on how to install WinPcap. Note that Before you install the new WinPcap version, you need to uninstall WinPcap 3.0, restart the agent’s system, and then install the newer version.

If these entries are not present, increase the tracing mask on the agent’s computer to 0xf0f and try to silent monitor the agent again.
Symptom  The monitored audio on the supervisor desktop is not clear (frequent drop-outs or audio distortions)

Possible Cause  The supervisor softphone requires some CPU power to decode monitored audio packets in real time. If the CPU is used heavily by other applications on the supervisor's PC, the audio decoder may not have access to the CPU power required to keep up with incoming audio. Here are some steps you can take to improve audio quality:

- Stop any unnecessary applications that are running on the supervisor's desktop machine.
- Open Windows Task Manager on the supervisor's machine and check for other applications that may be utilizing a large percentage of the machine's CPU.
- Check the tracing level on the Supervisor Desktop. Silent Monitoring is tuned to work well at the default tracing mask of 0x40000307. If the tracing level is set higher than the default, silent monitor audio quality may be impacted. Reduce the desktop trace mask to 0x40000307 or lower.
- An overloaded network may cause audio packets to be delayed or lost as they are sent from the agent to the supervisor. If a large number of audio packets are lost or do not arrive at the supervisor in a timely manner, monitored audio may be degraded. Check with your system administrator to determine whether you are having network bandwidth issues and fix any network problem.

Symptom  Silent Monitoring experiences 1 way audio across VPN. As soon as agents go home and connect into the network via Remote Cisco 831 to HQ located Cisco 3845 (acting as VPN Concentrator), the Silent Monitoring function only works one way. This issue only occurs when a call goes across the VPN tunnel which activates the Checkpoint software.

Possible Cause  Disable the Checkpoint firewall and two way audio can be heard when silent monitoring. This works fine on the LAN, both sides of conversation can be monitored.
Troubleshooting Cisco CallManager Based Silent Monitor Problems

Figure 1-1 illustrates the call flow of a request and event sequence that takes place when a silent monitor call is initiated. It is helpful to keep this call flow in mind when looking at log files.

Figure 1-1   Request and Event Sequence when Cisco CallManager Based Silent Monitor Call Initiated
Trace Levels

In most cases, default trace levels are enough to track down silent monitor problems. The following sections contain log file snippets with default tracing enabled:

- Desktop default trace level – 0x40000307
- CTI OS Server default trace level – 0x03
- CTI Server default trace level – 0xF0
- JTAPI Gateway default trace level – 0x00

In some cases, it may be necessary to increase the following trace masks:

- CTI OS Server – 0x20403
- CTI Server – 0xF8

Troubleshooting - Initiating Silent Monitor

Supervisor Desktop Log

The following trace statement is logged to the supervisor’s desktop log when the supervisor initiates silent monitor.

```
04/19/07 22:04:24.390  3040  SupervisorSoftphone  Thd(3536)
[agent.5000.101]::SuperviseCall: Action = 1, Agent = agent.5000.102, Call =
    call.5000.16786462.30002
04/19/07 22:04:24.390  3040  SupervisorSoftphone  Thd(3536)
[agent.5000.101]::MakeRequest( eSuperviseCallRequest )
04/19/07 22:04:24.390  3040  SupervisorSoftphone  Thd(3536)
[agent.5000.101]::MakeRequest: (SupervisoryAction:1
    UniqueObjectID:agent.5000.101 ClassIdentifier:1 AgentReference:agent.5000.102
    AgentCallReference:call.5000.16786462.30002)
04/19/07 22:04:24.390  3040  SupervisorSoftphone  Thd(3536)
CCtiOsSession::MakeRequest(eSuperviseCallRequest)
04/19/07 22:04:24.390  3040  SupervisorSoftphone  Thd(3536)  CCtiOsSession::MakeRequest:
    (SupervisoryAction:1 UniqueObjectID:agent.5000.101
    ClassIdentifier:1 AgentReference:agent.5000.102
    AgentCallReference:call.5000.16786462.30002)
```

CTI Server Log

Initiating Silent Monitor – CTI Server Log

The following trace statement is logged to the CTI Server log when the supervisor initiates silent monitor.

```
09:47:55 cg1A-ctisvr Trace: ProcessSuperviseCallRequest - sessionID 2
09:47:55 cg1A-ctisvr Trace: CSTASuperviseCall- ProcessSuperviseCallRequest
InvokeID=0x2600b8ae
    AgentCall(CallID=16786464 Device=30002 Type=Static) SupervisorCall(CallID=-1
    Device=30001 Type=Static Action=1)
09:47:55 cg1A-ctisvr Trace: PRIVATE_DATA - AgentExtension=30002 AgentID=102
    AgentInstrument=30002 SupervisorInstrument=30001
```

JTAPI Log

The following trace statement is logged to the JTAPI Gateway log when the supervisor initiates silent monitor.
Troubleshooting – Silent Monitor Established

**JTAPI Log**

The following trace statements are logged to the JTAPI Gateway log once the silent monitor call has been established. The following trace illustrates the message sent from Cisco CallManager when silent monitor starts.

```
09:47:55 pg1A-jgw1 Trace: CiscoTermConnMonitoringStartEv Monitored CID: 16786464 Addr: 30002 Term: SEP0019E8035BA6 MonitorType: 1
09:47:55 pg1A-jgw1 Trace: ------- CallChangedEvent called with 1 events.
09:47:55 pg1A-jgw1 Trace: NEW META EVENT Cause: NORMAL MetaCode: META_CALL_PROGRESS

09:47:55 pg1A-jgw1 Trace: CiscoTermConnMonitorInitiatorInfoEv Monitored CID: 16786464 Addr: 30002 Term: SEP0019E8035BA6 Monitor Initiator Addr: 30001 Monitor Initiator Term: SEP0015FAB8F3EB Monitoring CID: 16786465 Cause: NORMAL
09:47:55 pg1A-jgw1 Trace: handleCiscoTermConnMonitorInitiatorInfoEvent: address: 30001 Address Type: INTERNAL
09:47:55 pg1A-jgw1 Trace: handleCiscoTermConnMonitorInitiatorInfoEvent: address: 30002 Address Type: MONITORING_TARGET
09:47:55 pg1A-jgw1 Trace: handleCiscoTermConnMonitorInitiatorInfoEvent Found target connection: 30002 for monitoring call116786465
09:47:55 pg1A-jgw1 Trace: MyConnection() address:30002 type:MONITORING_TARGET
09:47:55 pg1A-jgw1 Trace: findInstrumentByAddressString() since the address: 30002 and type:MONITORING_TARGET
09:47:55 pg1A-jgw1 Trace: findInstrumentByAddressString(): find the instrument for address: 30002 and its type:MONITORING_TARGET
09:47:55 pg1A-jgw1 Trace: handleConnCreated::Created new MyConn: GenID: 10 ConnIDVal: 21683064 ConnDev: 30001/0 DevExt: 30001 DevTgDevStr: ConnAddr: 30001 State: ALERTING CCState: ESTABLISHED prevCCState: ESTABLISHED loggedIn: Y
```

```
CTI Server Log

The following trace statements are logged to the CTI Server log once the silent monitor call has been established. Please note that the call events that result from a silent monitor request are the same as any other call. The only differences are the call and line types.

09:47:55 cg1A-ctisvr Trace: CALL_CREATED: CallID=16786465.30001(s) Dest= Periph=5000 Type=21 (SUPERVISOR_MONITOR) ECCsize=0 Disposition=0(INVALID)

09:47:55 cg1A-ctisvr Trace: CSTA_ESTABLISHED - callID=16786465.30002(s) answeringDev=30002 callingDev=(DEV)30001 calledDev=(DEV)30002 localConnectionInfo(3)=CS_CONNECT cause=46

Silent Monitor Problems (IPCC Only)

Agent Desktop Log

The following trace statement is logged to the Agent Desktop log when the silent monitor call is established. Note the SilentMonitorStarted event. This event is added to the flow by CTI OS to notify the app that silent monitor has started.

04/20/07 09:53:50.500 3136 CTIOSSoftphone Thd(3880) CCTiOsSession::OnEvent(eSilentMonitorStartedEvent), EnablementMask = fffffff

09:47:55 cg1A-ctisvr Trace: CSTASuperviseCallConfEvent - InvokeID=0x2600b8ae

Supervisor Desktop Log

The following trace statement is logged to the Supervisor Desktop log when the silent monitor call is established. Note the SilentMonitorStarted event. This event is added to the flow by CTI OS to notify the application that silent monitor has started. Also notice that call events are not sent to the agent desktop.

04/19/07 22:04:25.343 3040 SupervisorSoftphone Thd(3072) CCTiOsSession::OnEvent(eSupervisorButtonChange), EnablementMask:0xffffffc1

Agent Desktop Log

The following trace statement is logged to the Agent Desktop log when the silent monitor call is established. Note the SilentMonitorStarted event. This event is added to the flow by CTI OS to notify the application that silent monitor has started. Also notice that call events are not sent to the agent desktop.

09:47:55 cg1A-ctisvr Trace: CSTA_ESTABLISHED - callID=16786465.30002(s) answeringDev=30002 callingDev=(DEV)30001 calledDev=(DEV)30002 localConnectionInfo(3)=CS_CONNECT cause=46

Silent Monitor Problems (IPCC Only)

Agent Desktop Log

The following trace statement is logged to the Agent Desktop log when the silent monitor call is established. Note the SilentMonitorStarted event. This event is added to the flow by CTI OS to notify the application that silent monitor has started. Also notice that call events are not sent to the agent desktop.

04/20/07 09:53:50.500 3136 CTIOSSoftphone Thd(3880) CCTiOsSession::OnEvent(eSilentMonitorStartedEvent), EnablementMask = ffffff

04/19/07 22:04:25.343 3040 SupervisorSoftphone Thd(3072) CCTiOsSession::OnEvent(eSupervisorButtonChange), EnablementMask:0xffffffc1

Agent Desktop Log

The following trace statement is logged to the Agent Desktop log when the silent monitor call is established. Note the SilentMonitorStarted event. This event is added to the flow by CTI OS to notify the application that silent monitor has started. Also notice that call events are not sent to the agent desktop.

09:47:55 cg1A-ctisvr Trace: CSTA_ESTABLISHED - callID=16786465.30002(s) answeringDev=30002 callingDev=(DEV)30001 calledDev=(DEV)30002 localConnectionInfo(3)=CS_CONNECT cause=46

Silent Monitor Problems (IPCC Only)
SilentMonitorInitiatingDeviceID:30001 SilentMonitorTargetDeviceID:30002
SilentMonitorCallUID:call.5000.16786465.30002)

Troubleshooting – Stopping Silent Monitor

Supervisor Desktop Log

The following trace statements are logged to the supervisor’s desktop log when the supervisor stops silent monitor. Note that the silent monitor call is torn down the same as an agent to agent call.

04/20/07 11:36:54.750  3040  SupervisorSoftphone  Thd(3536)  CCtiOsSession::MakeRequest:
(SupervisoryAction:0 UniqueObjectID:agent.5000.101
ClassIdentifier:1 AgentReference:agent.5000.102
AgentCallReference:call.5000.16786465.30001)
04/20/07 11:36:54.828  3040  SupervisorSoftphone  Thd(3072)  CCtiOsSession::OnEvent(eCallConnectionClearedEvent ), EnablementMask = 68bf0006
...
04/20/07 11:36:54.875  3040  SupervisorSoftphone  Thd(3072)  CCtiOsSession::OnEvent,
(AgentID:101 UniqueObjectID:agent.5000.101
MessageID:eSilentMonitorStopRequestedEvent
SilentMonitorInitiatingAgentUID:agent.5000.101
SilentMonitorTargetAgentUID:agent.5000.102
SilentMonitorInitiatingDeviceID:30001 SilentMonitorTargetDeviceID:30002
SilentMonitorCallUID:call.5000.16786465.30001 SilentMonitorCallDisposition:0)
04/20/07 11:36:54.906  3040  SupervisorSoftphone  Thd(3072)  CCtiOsSession::OnEvent,
(CallType:21 DeviceID:3001
UniqueObjectID:call.5000.16786465.30001 CallStatus:0 MessageID:eCallEndEvent
DeviceUniqueObjectID:device.5000.30001)

Agent Desktop Log

The following trace statements are logged to the agent’s desktop log when the supervisor stops silent monitor. Note that the agent desktop only receives the SilentMonitorStopRequestedEvent.

04/20/07 11:37:57.468  3136  CTIOSSoftphone  Thd(3880)  CCtiOsSession::OnEvent(eSilentMonitorStopRequestedEvent ), EnablementMask = ffffffffff
04/20/07 11:37:57.468  3136  CTIOSSoftphone  Thd(3880)  CCtiOsSession::OnEvent,
(AgentID:102 UniqueObjectID:agent.5000.102
MessageID:eSilentMonitorStopRequestedEvent
SilentMonitorInitiatingAgentUID:agent.5000.101
SilentMonitorTargetAgentUID:agent.5000.102
SilentMonitorInitiatingDeviceID:30001 SilentMonitorTargetDeviceID:30002
SilentMonitorCallUID:call.5000.16786465.30002 SilentMonitorCallDisposition:0)

CTI Server Log

The following trace statements are logged to the CTI Server log when the supervisor stops silent monitor.

11:32:00 cg1A-ctisvr Trace: CSTASuperviseCall– ProcessSuperviseCallRequest
InvokeID=0x2600c827
AgentCall(CallID=-1 Device=30002 Type=Static)     SupervisorCall(CallID=16786465
Device=30001 Type=Static Action=0)
11:32:00 cg1A-ctisvr Trace: PRIVATE_DATA - AgentExtension=30002 AgentID=102
AgentInstrument=30002 SupervisorInstrument=30001
11:32:00 cg1A-ctisvr Trace:

11:32:00 cg1A-ctisvr Trace: CSTA_CONNECTION_CLEARED - callID=16786465.30002(s)
releasingDev=30002 localConnectionInfo(-1)=CS_NONE cause=-1
11:32:00 cg1A-ctisvr Trace: callAction=must clear
11:32:00 cg1A-ctisvr Trace:
Silent Monitor Problems (IPCC Only)

JTAPI Log

The following trace statement is logged to the JTAPI Gateway log when the supervisor stops silent monitor.

```
11:32:00 pg1A-jgw1 Trace:   MsgSuperviseCall:   SupervisorAction: 0 AgentCID: -1
AgentConnDevID: 30002/0 SupervisorCID: 16786465 SupervisorConnDevID: 30001/0 SubjectDevID: 30001/0 InvID: 107825430

11:32:00 pg1A-jgw1 Trace:   ConnDisconnectedEv CID: 16786465 Addr: 30002
11:32:00 pg1A-jgw1 Trace:   CallCtlConnDisconnectedEv CID: 16786465 Addr: 30002 Calling: 30000 Called 30002 LastRed: 30002 CiscoCause: CAUSE_NORMALCALLCLEARING Cause: NORMAL State: DISCONNECTED CCState: DISCONNECTED

11:32:00 pg1A-jgw1 Trace:   MsgConnectionCleared: CID: 16786465 ConnDevID: 30002/0 RelDevID: 30000/0 LocConnInfo: -1 Cause: -1 DevTgDevStr: 30002

11:32:00 pg1A-jgw1 Trace: TermConnDroppedEv CID: 16786465 Addr: 30001 Term: SEP0015FAB8F3EB
11:32:00 pg1A-jgw1 Trace:   CallCtlTermConnDroppedEv CID: 16786465 Addr: 30001 Term: SEP0015FAB8F3EB Calling: 30000 Called 30002 LastRed: 30002 CiscoCause: CAUSE_NORMALCALLCLEARING Cause: NORMAL

11:32:00 pg1A-jgw1 Trace: CiscoTermConnMonitoringEndEv CID: 16786464 Addr: 30002 Term: SEP0019E8035BA6 MonitorType: 1
```

```
11:32:00 pg1A-jgw1 Trace:   MsgSuperviseCallConf: InvID: 107825430
```
Troubleshooting – PG Error Codes

The following errors are sent from the PG when silent monitor fails. These error codes are delivered in control failure events the (log files are displayed in the following sections).

<table>
<thead>
<tr>
<th>Table 1-1 Silent Monitor PG Error Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Code</strong></td>
</tr>
<tr>
<td>13138</td>
</tr>
<tr>
<td>13139</td>
</tr>
<tr>
<td>13140</td>
</tr>
<tr>
<td>13141</td>
</tr>
<tr>
<td>13142</td>
</tr>
<tr>
<td>13143</td>
</tr>
<tr>
<td>13144</td>
</tr>
<tr>
<td>13145</td>
</tr>
<tr>
<td>13146</td>
</tr>
<tr>
<td>13147</td>
</tr>
<tr>
<td>13148</td>
</tr>
</tbody>
</table>
Silent Monitor Problems (IPCC Only)

Supervisor Desktop

When silent monitor fails for any of the reasons described in the previous table, the supervisor desktop displays the error number as well as text describing the error. The following dialog occurs when a supervisor attempts to silent monitor an agent that is using a phone that does not support silent monitor.

**Figure 1-2 Superviser Desktop Error 13144**

Supervisor Desktop Log

The error is also logged in the supervisor desktop log.

<table>
<thead>
<tr>
<th>Time</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/20/07 20:58:11.734</td>
<td>2560 SupervisorSoftphone Thd(3740) CCTiOsSession::OnEvent(</td>
</tr>
<tr>
<td></td>
<td>ErrorNumber:13144</td>
</tr>
<tr>
<td></td>
<td>AgentID:101</td>
</tr>
<tr>
<td></td>
<td>UniqueObjectID:agent.5000.101</td>
</tr>
<tr>
<td></td>
<td>PeripheralID:5000</td>
</tr>
<tr>
<td></td>
<td>FailureCode:1</td>
</tr>
<tr>
<td></td>
<td>PeripheralErrorCode:13144</td>
</tr>
<tr>
<td></td>
<td>AgentID:101</td>
</tr>
<tr>
<td></td>
<td>UniqueObjectID:agent.5000.101</td>
</tr>
<tr>
<td></td>
<td>MessageID:CONTROL_FAILURE_CONF</td>
</tr>
<tr>
<td></td>
<td>MessageType:esuperviseCallRequest</td>
</tr>
<tr>
<td></td>
<td>ErrorMessage:IPCC Error [13144] Monitoring request has encountered error, please make sure that Built-In-Bridge is turned on and the phone has the monitoring capability</td>
</tr>
<tr>
<td></td>
<td>FilterTarget:agent.5000.101</td>
</tr>
<tr>
<td></td>
<td>TargetCILClientID:VM3AGENT1-2560-3740</td>
</tr>
</tbody>
</table>

CTI Server Log

The error is also logged in the CTI Server log.

<table>
<thead>
<tr>
<th>Time</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>20:53:23</td>
<td>Trace: CSTADUniversalFailureConfEvent</td>
</tr>
<tr>
<td></td>
<td>InvokeID=0x27000110</td>
</tr>
<tr>
<td></td>
<td>Error=GENERIC_OPERATION</td>
</tr>
<tr>
<td></td>
<td>PRIVATE_DATA - PeripheralErrorCode=0x3358(13144)</td>
</tr>
</tbody>
</table>

JTAPI Log

The JTAPI Gateway logs the error as well. When JTAPI logs the error, it only logs the last 3 digits. For example 13144 is logged as 144.

<table>
<thead>
<tr>
<th>Time</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>20:53:22</td>
<td>Trace: ThreadSuperviseCall::SilentMonitorCall: Call to call[] encountered exception.</td>
</tr>
<tr>
<td></td>
<td>com.cisco.jtapi.PlatformExceptionImpl: Monitor req</td>
</tr>
<tr>
<td></td>
<td>InvID: 197149365 Status: 144</td>
</tr>
</tbody>
</table>
Troubleshooting – Legacy Supervisor

If a 7.1(x) or earlier supervisor desktop initiates silent monitor when connected to a 7.2(1) CTI OS Server, the supervisor desktop receives the following error (Figure 1-3).

Figure 1-3  Supervisor Desktop Error 0x00000015

CTI Warning:

[Error Code – 0x00000015]:
Silent Monitor session failed.
Please contact your system administrator

The supervisor desktop also logs the error as well.

04/20/07 21:24:41.706  5972  SupervisorSoftphone Thd(5112)
CSilentMonitorManager::OnSilentMonitorStatusReportEvent,
(UniqueObjectID:SilentMonitorManagerObject
  MessageID:eSilentMonitorStatusReportEvent
  MonitoredUniqueObjectID:agent.5000.102 StatusCode:21 SMSessionKey:101
  TargetCILClientID:bmadison-5972-5112)

Silent Monitor: Developer Information

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

For supervisor desktops using silent monitor, you need to install the following files:
- ccnsmt.dll - this file is the COM dll that transmits monitored audio via the sound card. It must be registered. (for example, regsvr32 ccnsmt.dll)
- libg723.dll - this file is a dependency of ccnsmt.dll; ccnsmt will fail to register without it
- traceserver.dll - this is the tracing mechanism for ccnsmt.dll

For agent desktops using silent monitor you need to run the WinPcap install executable:
- WinPcap_3_0_nogui.exe

The CTI OS silent monitor feature requires that you modify a WinPcap registry setting after installing (or reinstalling) WinPcap. In the Windows registry go to the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NPF
Change the value of the Start setting under this key from 0x00000003 to 0x00000002. Reboot the PC.
ToS/QoS Problems

Symptom  TCP packets going from CTI OS server to CTI Toolkit do not have ToS/QoS (Type of Service/Quality of Service) tagged.

Possible Cause  Ensure that the ToS/QoS is properly configured on the system where CTI OS Server resides. Make sure that the following registry has ToS value set to 0x68:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Connection

Also make sure that the following system registry value “DisableUserTOSSetting” is set to 0. It can be found under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters.

Note  The system needs to be restarted if the “DisableUserTOSSetting” registry value has been changed.

Symptom  TCP packets going from CTI Toolkit to CTI OS server do not have ToS/QoS tagged.

Possible Cause  This symptom may have multiple causes:

– ToS tagging is NOT implemented in the Java or .NET (C#) CILs. 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.

– Ensure that the ToS/QoS is properly configured on the system where CTI OS Server resides. If changes are made to the registry, then both CTI OS server and CTI Toolkit need to be re-started. Make sure that the following registry has ToS value set to 0x68

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_<customer-instance>\CTIOS1\EnterpriseDesktopSettings\AllDesktops\Login\ConnectionProfiles\Name\IPCC<or other profile name>

– Make sure that the following registry has ToS value set to 0xB8:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_<customer-instance>\CTIOS1\EnterpriseDesktopSettings\AllDesktops\IPCCSilentMonitor\Name\Settings
Resolutions to Common Problems

This section describes common CTI OS problems, their possible symptoms, and a procedure to correct the problem.

Incorrect or Unreachable Configuration Server

When the client application starts, it looks in the Windows registry for the location of the server from which it will obtain its configuration information. (For clarity, we will call these servers "configuration machines"). If this information is incorrect or if the specified servers are not reachable, the client application will not connect to a configuration machine. Since the client application gets all information about button enablement from the CTI OS server, button enablement will remain in the same state it was in upon start-up. Perform the following checks to determine where the problem lies:

- First check that you properly configured the client application to find its CTI OS Server(s) when you installed the softphone.
  - Check the values of CtiosA, CtiosB, PortA, and PortB in the registry under the key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTI Desktop\CTIOS.
  - If the CTI OS Server names (or addresses) are incorrect, enter the correct server names and restart the client application.

- If the server names (or addresses) of the configuration machines are correct, the problem may be caused by a loss of network connectivity or an inability to resolve the download machine name.
  - From the client application machine, open a console window.
  - Attempt to ping the configuration machines entered in the registry key listed above. If the system is configured correctly, the ping should succeed for at least one of the configuration machines listed in the registry.
  - If the ping succeeded then the problem may be that the CTI OS server is not running on either of the configuration machines in the client application's registry or the CTI OS server is listening on a port different than the client application registry, or the CTI OS server is not active. Make sure that all configurations are correct, and then start the CTI OS server on those machines and re-start the client application.

- If the ping fails for both configuration machines and the configuration machine entries in the registry are not TCP addresses, the problem might be an inability to resolve the CTI OS server name into an IP address.
  - Try to ping the IP addresses corresponding to the configuration machine names entered in the registry.
Incorrect or Unreachable CTI OS Server in Connection Profile

When a client attempts to login, he/she chooses a connection profile from a list of available connection profiles on the login dialog. The client application receives the list of connection profiles from the configuration server. The connection profile provides the location of the CTI OS servers with which to connect. If this information is incorrect or if the specified servers are not reachable, the client application will not connect to a CTI OS machine. Since the client application gets all information about button enablement from the CTI OS server, this error will cause the client application's buttons to remain in the state they were in after the application connected to the configuration machine (that is, only the login button is enabled). Additionally, the status bar displays the last message received from the configuration server (that is, Configuring/Disconnected/Offline).

- If the ping succeeds, your DNS server may be down or the "hosts" file on the client machine may map the hostname to an incorrect address. Replace the configuration machine names in the registry with the associated IP addresses and restart the client application.
- If pinging the IP address fails then either the IP address is incorrect or the network connection between the client application and the configuration machine is down. Your TCP/IP network administrator should be able to help resolve this issue.

Incorrect or Unreachable CTI OS Server in Connection Profile

The CTI OS Server will not allow any client to connect while it is still configuring.

Since the client application randomly selects a configuration server each time the client application starts, symptoms of this problem may be sporadic if connection profile information is not consistent between configuration servers. Perform the following checks to determine where the problem lies:

- Note the connection profile (step a) you are using when you login from the client application. The connection profile is specified in the login dialog box using the "Connect to" dropdown list.
- On the client application machine, note the CTI OS Servers (step b) from which the application downloads its connection profile information (configuration machines). You can find this information in the CtiosA and CtiosB settings under the HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTI Desktop\CTI OS registry key.
- On each of the configuration machines determined in step b, check that you have properly configured the connection profile from step a. The connection profile information is located in the registry under the key

\[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<Profile name from step a>\]

Check the following items:
- The key shown above exists on both configuration machines.
- The information contained within the key is identical on both configuration machines.
- Check the values of CtiosA, CtiosB, PortA, and PortB. (For clarity, we will call these machines the "connect machines".) Are these CTI OS Server names (or addresses) and port numbers correct? If they are incorrect, enter the correct server names, restart the configuration machines, restart the client application, and try again.
Incorrect Configuration of Peripheral ID or Peripheral Type During Server Install

When installing the CTI OS server, the system administrator must enter a Peripheral ID and Peripheral Type corresponding to the target peripheral. The server uses this information to determine which switch behavior to emulate. If the wrong Peripheral ID or Peripheral Type is entered during install, CTI OS may attempt to emulate the incorrect switch type or may emulate a generic switch type. This will result in incorrect button enablement on the client application. Since the client application randomly selects a configuration server each time the client application starts, symptoms of this problem may be sporadic if connection profile information is not consistent between configuration servers. Perform the following checks to determine where the problem lies:

- Note the name of the server with which the client application connected. This information is contained in the OnConnection event and is displayed on the status bar control.
- Go to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Peripherals on the server with which the client application is connected.
- Under this key there are subkeys. Each subkey represents a peripheral with which CTI OS is configured to communicate. Find the peripheral to which you are attempting to login.
- Open the corresponding subkey and modify the values of peripheralID and peripheralType so that they are correct. The Peripheral ID can be found in the ICM configuration; a list of supported Peripheral Types appears in Appendix B.
- Restart the CTI OS server.
- Restart the client application.
- Try to login again.
Incorrect Configuration of the Peripheral ID in the Connection Profile

When the client attempts to login using a specific connection profile, the client application associates itself with the Peripheral ID contained in the connection profile. The client application then waits for CTI OS server to signal that the peripheral associated with that Peripheral ID is online before it attempts to login to that peripheral. If the connection profile contains the incorrect Peripheral ID, the client application may receive this notification prematurely or not at all. In the former case the login will fail with no indication to the user. In the latter case, the user will be informed that the system is offline and that the login attempt will be queued until the system comes online. Since the client application randomly selects a configuration server each time the client application starts, symptoms of this problem may be sporadic if connection profile information is not consistent between configuration servers. To modify the Peripheral ID in the connection profile:

1. Note the connection profile you are using when you login (step a). The connection profile is specified in the client application's login dialog box using the "Connect to" dropdown list.
2. Note the name of the server with which the client application connected. This information is contained in the OnConnection event and is displayed on the status bar control.
3. Go to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\CTIOS_<InstanceName>\ctios1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<Profile name from step a> on the server with which the client application is connected.
4. Modify the value of peripheralID so that it is correct. (The Peripheral ID can be found in the ICM configuration.)
5. Restart the CTI OS server.
6. Restart the client application.
7. Try to login again.

Determining if a PC can Capture Audio Packets sent from an IP Phone

To determine if an agent PC is unable to capture packets sent from the IP phone, Cisco recommends you use a public domain packet sniffer called Wireshark. (This is because Wireshark uses WinPCap, which is the same packet capture technology that is used by CTI OS Silent Monitor.):

1. Download Wireshark from [http://www.wireshark.org/download.html](http://www.wireshark.org/download.html) and install it on the agent’s machine.
2. Verify that WinPcap is installed on the agent’s machine via Start->Control Panel->Add remove programs. WinPcap should be on the list. If not, install WinPcap as described in the Installing WinPcap section of this document.
3. Run Wireshark: Select Capture > Start > OK
4. Make a voice call from or to the agent’s phone (there is no need to be logged onto CTI OS right now) and ensure that UDP packets are captured at roughly 100 packets/second.
5. If no packets are captured, click stop, then Capture -> Start again. However, make sure that you select a different Adapter from the drop down list, go to step 3., and repeat the test. If there are no adapters listed in the Interface drop down list and you are not an Administrator on the PC, there may be a WinPcap user permissions issue. To fix this issue, check the value of the Start setting at the following Windows registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NPF

Change the value of the Start setting to 0x00000002, reboot the PC, and try to monitor the agent again.

If you are unable to capture packets on any of the adapters listed in the drop down list, and your PC is on a VLAN, your PC’s network interface card may not be able to capture packets from a different VLAN. Some interface cards require special configuration to capture packets off a different VLAN.

Refer to Appendix A of the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for details on how to qualify your network interface card for silent monitor.

**Installing WinPcap**

To install WinPcap you may either run WinPcap_3_0_nogui.exe from the CTI OS CD (located at ctios\Installs\CTIOSClient) to install it or download WinPcap from [http://www.winpcap.org/](http://www.winpcap.org/). The CTI OS silent monitor feature requires that you modify a WinPcap registry setting after installing (or reinstalling) WinPcap. In the Windows registry go to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NPF

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

Note
Troubleshooting in a CTI OS installation can be simple if you follow the correct procedure, and very difficult if done arbitrarily. Do not forget that you are dealing with a multi-component distributed system and that the source of the problem may not be the component where the symptoms are seen.

Following are the steps that you need for troubleshooting a CTI OS Installation:

Note
Steps 3 to 7 are the “Problem Isolation” procedure used to discard any malfunction of the components in Cisco ICM.

1. Write down all the steps that reproduce the problem.
2. Write down the call flow clearly and concisely.
3. Bump the trace mask up to 0x00020A0f as minimum on CTI OS Server.
4. Bump the trace mask up to 0x00000A0f for the CTI OS Clients. (Use 0x00003E0F if you are troubleshooting Silent Monitor problems)
5. Use the hard phone and verify whether the problem repeats. If the problem no longer occurs using the hard phone, rule out the CallManager/ACD as the source of the problem.
6. Use CTITest and verify whether the problem repeats. If the problem no longer occurs using CTITest, rule out the CTI Server, PIM and OPC as the sources of the problem.
7. Use CILTest and verify whether the problem repeats. If the problem no longer occurs using the CILTest, rule out the CTI OS Server as the source of the problem.
8. Use CTI OS Desktop and verify whether the problem repeats. Using CTI OS Desktops will help isolate the problem to the phone if the problem is reproducible there.
9. Examine the CTI OS configuration registry.
10. If the problem cannot be fixed onsite, collect all logs and version numbers, and submit them to TAC. Remember to include call flow and logs for OPC, PIM, CTI Server, CTI OS Server Node, CTI Driver, CTI Client and JTAPI Gateway (if working with IPCC). Also include all comments about the troubleshooting efforts you made.
Obtaining Logs for Support

When you report a problem to Cisco, Cisco personnel will ask that you supply certain details about the problem. You should be prepared to provide Cisco with the following details about your problem when you call.

- At exactly what time did the problem happen?
- What was the agent ID of affected agent?
- What was the device ID of affected device?
- What was the call ID of affected call?
- What was the affected agent doing prior to the failure?
- What buttons if any were pressed, and what buttons were enabled?
- Was a call in the grid at the time, and was the call on the hard phone?
- What was the call flow?

In addition, Cisco will usually require logs in order to troubleshoot a problem. It is best to collect all of the following logs for the timeframe when the problem occurred.

- CTI Toolkit
- CTI OS server
- CTI server
- PIM
- OPC
- JTAPI Gateway (only if using IPCC)

Include logs for all of the relevant servers, including both sides of a duplexed system.

The following sections discuss CTI OS Server and CTI Toolkit logs and trace levels. See the ICM Administration Guide for Cisco ICM Enterprise Edition for information on other logs.

Taking CTI OS Server Logs

The trace log location for the server processes can be found under the following directory:

<drive>:\ICM\<customer_instance>\CTIOS1\logfiles
Files are named using the convention `<process name>_ymmd_hhmmss.ems`. The date/time stamp part of the file name indicates when the file was created. The information in these files is stored in a binary format and must be read using the dumplog utility. You will need to open a DOS Command Prompt window and change to the `<drive>:\ICM<customer_instance>\CTIOS\logfiles` directory in order to use dumplog on the CTI OS Server log files. For information on how to use dumplog, refer to the ICM Administration Guide for Cisco ICM Enterprise Edition.

When reporting a problem, it is generally very helpful to provide the logs for the timeframe in which the problem occurred. This is Cisco’s “window” into the activity that is taking place at the time of the problem. Try to provide all files that cover the needed timeframe. Do this by looking at the timestamp in the filename to find out when they were created and by looking at the modification timestamp in Windows Explorer to see the last time a given file was written to.

### How to Set Trace Levels

Trace levels for the server processes can be found in the registry under:

```
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc\ICM\<Customer Instance>\CTIOS\EMS\CurrentVersion\Library\Processes\CTIOS\EMSTraceMask
```

**Warning**

The default value for the trace masks is 0x20003. Changing this value can have a serious impact on server performance. It should only be modified by experienced field personnel or at the request of Cisco support personnel.

Trace masks can be combined in order to uniquely log the messages you are interested in. For example:

- **TRACE_MASK_CONNECTION | TRACE_MASK_METHOD_LOW**
  - logs low important method messages of the connection layer
- **TRACE_MASK_EVENTFILTER | TRACE_MASK_METHOD_HIGH**
  - logs high important method messages of the EventFilter component

### Setting CTI OS Server Trace Levels

The default trace mask is 0x3 in all releases except in release 7.0(0) where it is set to 0x20003.

Setting the trace mask high (for example: 0xf or higher) has a big impact on both the CTI OS server performance and the call completion rate. As a result, only set the trace mask high when debugging a problem. When the required logs have been collected, turn the trace mask back to its default value.

During load testing, ensure the default trace mask is set across all the PG components, and not just the CTI OS server.

**Note**

The PG and CTI OS server are co-resident.

For troubleshooting purposes, set the CTI OS Server trace mask to:

- 0x0A0F for Release 6.0 and earlier
- 0x20A0F for Release 7.0, and 7.1(1)
- 0x60A0F for Release 7.1(2) and later
Setting CTI OS Client Trace Levels

The default trace mask is:
- 0x7 for Release 6.0 and earlier
- 0x40000307 in release 7.x.x

Setting the trace mask to 0x40000307 is OK when running one, two or three agent desktops on the systems, but it impacts the system if a load test is running and CILTest is used to simulate CTI OS agents. When running load testing using CILTest, setting a low trace mask value (0x3 for example) is more appropriate.

Set the trace mask higher than 0x40000307 only when debugging a problem. When the required logs are collected, set the trace mask back to its default value.

For troubleshooting purposes, set the CTI OS Client trace mask to 0xFFF.

Setting Point-to-Point Silent Monitor Trace Levels (Client only)

For troubleshooting purposes, and to get all events as described before for the client plus Silent Monitor Sniffer, Decoder events/requests, and communication of forwarded VoIP (send/receive of encapsulated VoIP in UPD stream); set the trace mask to 0x20003E0F.

Note: All CTI OS component trace settings are essentially the same. For trace masks specific to .NET CIL, refer to the CTI OS Developer’s Guide.

<table>
<thead>
<tr>
<th>Trace Mask Name</th>
<th>Trace Mask Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_MASK_ALWAYS</td>
<td>0x00</td>
<td>Used across all CTI OS components. Only the necessary messages need to use this trace mask. Examples: initialization phases, important error messages, ... The message is always printed, regardless of the trace mask setting.</td>
</tr>
<tr>
<td>TRACE_MASK_CRITICAL</td>
<td>0x01</td>
<td>Used across all CTI OS components. Only the necessary messages need to use this trace mask. Examples: critical error messages, ... The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_WARNING</td>
<td>0x02</td>
<td>Used across all CTI OS components. This trace mask bit is used for warning messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>Trace Mask Name</td>
<td>Trace Mask Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_HIGH</td>
<td>0x04</td>
<td>Used across all CTI OS components. This trace mask bit is used to display high important events, confs, and requests names without their parameters. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_HIGH_PARM</td>
<td>0x08</td>
<td>The same as TRACE_MASK_EVT_REQ_HIGH, but the messages include events, confs, and requests parameters.</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_AVG</td>
<td>0x10</td>
<td>Used across all CTI OS components. This trace mask bit is used to display average important events, confs, and requests names without their parameters. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_AVG_PARM</td>
<td>0x20</td>
<td>The same as TRACE_MASK_EVT_REQ_AVG, but the messages include events, confs, and requests parameters.</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_LOW</td>
<td>0x40</td>
<td>Used across all CTI OS components. This trace mask bit is used to display low important events, confs, and requests names without their parameters. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_EVT_REQ_LOW_PARM</td>
<td>0x80</td>
<td>The same as TRACE_MASK_EVT_REQ_LOW, but the messages include events, confs, and requests parameters.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_HIGH</td>
<td>0x0100</td>
<td>Used across all CTI OS components. This trace mask bit is used to display high visibility method entry/exit messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_HIGH_LOGIC</td>
<td>0x0200</td>
<td>Used across all CTI OS components. This trace mask bit is used to display high visibility method logic messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_AVG</td>
<td>0x0400</td>
<td>Used across all CTI OS components. This trace mask bit is used to display average visibility method entry/exit messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_AVG_LOGIC</td>
<td>0x0800</td>
<td>Used across all CTI OS components. This trace mask bit is used to display average visibility method logic messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>Trace Mask Name</td>
<td>Trace Mask Number</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_LOW</td>
<td>0x1000</td>
<td>Used across all CTI OS components. This trace mask bit is used to display low visibility method entry/exit messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_LOW_LOGIC</td>
<td>0x2000</td>
<td>Used across all CTI OS components. This trace mask bit is used to display low visibility method logic messages. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_METHOD_MAP</td>
<td>0x4000</td>
<td>It is used in CTI OS server for the following components: 1. ServiceBroker component 2. ObjectMap component 3. CtiServerDriverLib component This trace mask bit is used to display map information. These maps hold objects such as call, agent, skillgroup, arguments, and supervisor. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_CONTROLS</td>
<td>0x8000</td>
<td>Not used.</td>
</tr>
<tr>
<td>TRACE_MASK_EVENTFILTER</td>
<td>0x010000</td>
<td>It is used in CTI OS server for the EventFilter component. This trace mask bit is used to display messages in the EventFilter component. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_MESSAGEPASSING</td>
<td>0x020000</td>
<td>Used in CTI OS server for the IOCPConnectionMgr component (this component accepts CTI OS client connections). For Release 7.1(2) and later, this trace mask bit is used to display all the messages coming and going between CTI OS server and CTI OS client. For Releases 7.0, 7.0 SRx, 7.0 SRx ESx, and 7.1(1) this trace mask bit is used to display all the messages coming and going between CtiServer and CTI OS Server. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK.CG_MESSAGEPASSING</td>
<td>0x040000</td>
<td>It is used in CTI OS server for the Driver piece of the ServiceBroker component. Valid only for Release 7.1(2) and later. This trace mask bit is used to display all the messages coming and going between CtiServer and CTI OS server (for example: events, requests and confs). The message is printed only if the trace mask bit is set.</td>
</tr>
</tbody>
</table>
### Trace Mask Name | Trace Mask Number | Description
--- | --- | ---
TRACE_MASK_MESSAGEQUEUE | 0x080000 | Used in CTI OS server for the MultiThread algorithm in the ServiceBroker component. It is valid only in release 7.1(2) and later. This trace mask bit is used to display messages in the ServiceBroker component for the MultiThread algorithm. The message is printed only if the trace mask bit is set.

TRACE_MASK_SECURITY | 0x100000 | Used in the security and the connection libraries that are used in CTI OS server and CTI OS client. Valid only for Release 7.0(0) and later. This trace mask bit is used to display messages related to security in the security and the connection libraries. The message is printed only if the trace mask bit is set.

TRACE_MASK_ARGREFCOUNTING | 0x400000 | Used in the arguments library that is used in CTI OS server and CTI OS client. This trace mask bit is used to display messages related to the arguments reference count (Addref and Release) in the arguments library. The message is printed only if the trace mask bit is set.

TRACE_MASK_REFcounting | 0x800000 | Used for all objects that are used in CTI OS server and CTI OS client (for example: call, agent, skillgroup, supervisor objects). This trace mask bit is used to display messages related to the object reference count (Addref and Release) in the CTI OS server and CTI OS client. The message is printed only if the trace mask bit is set.

TRACE_MASK_ARGS_METHODS | 0x0100000 | Used in the arguments library used in CTI OS server and CTI OS client. This trace mask bit is used to display the name of the class::method of the arguments library. The message is printed only if the trace mask bit is set.

TRACE_MASK_ARGS_LOGIC | 0x0200000 | Used in the arguments library used in CTI OS server and CTI OS client. This trace mask bit is used to display the logic of the methods of the arguments library. The message is printed only if the trace mask bit is set.

TRACE_MASK_PACKETS_METHODS | 0x0400000 | Used in the connection library used for the peer CTI OS server connection and for CTI OS client connection. This trace mask bit is used to display the name of the class::method of the connection library. The message is printed only if the trace mask bit is set.
<table>
<thead>
<tr>
<th>Trace Mask Name</th>
<th>Trace Mask Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_MASK_PACKETS_LOGIC</td>
<td>0x08000000 0</td>
<td>Used in the connection library used for the peer CTI OS server connection and for CTI OS client connection. This trace mask bit is used to display the logic of the methods of the connection library. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_SERIALIZE_DUMMP</td>
<td>0x10000000 0</td>
<td>Not used.</td>
</tr>
<tr>
<td>TRACE_MASK_SOCKETS_DUMMP</td>
<td>0x20000000 0</td>
<td>Used in the connection library used for the connection between: 1. peer CTI OS servers 2. CTI OS client and CTI OS Server 3. CtiServer and CTI OS Server This trace mask bit is used to display the packets coming from the network. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_THREADING</td>
<td>0x40000000 0</td>
<td>Used in the: 1. CilTest 2. CtiServerDriverLib used in CTI OS server 3. Util library used by the CTI OS server and CTI OS client This trace mask bit is used to display thread information (for example: thread name, thread status, ...). The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_MASK_CONNECTION</td>
<td>0x80000000 0</td>
<td>Used in all the connection layers used by CTI OS server and CTI OS client. This trace mask bit is used to display logic information of the connection layers. The message is printed only if the trace mask bit is set.</td>
</tr>
<tr>
<td>TRACE_LEVEL_MAJOR</td>
<td>0x000000ff</td>
<td>Not used.</td>
</tr>
<tr>
<td>TRACE_LEVEL_EVENT_REQ</td>
<td>0x0000ff00</td>
<td>Not used.</td>
</tr>
<tr>
<td>TRACE_LEVEL_METHOD</td>
<td>0x00ff0000</td>
<td>Not used.</td>
</tr>
<tr>
<td>TRACE_LEVEL_MEMORY</td>
<td>0xff000000</td>
<td>Not used.</td>
</tr>
</tbody>
</table>
Taking CTI Toolkit Logs

The trace log name and location for client processes can be found under the following registry keys:

\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\Logging\TraceFileName

The default filename is CTIOSClientLog. Logfiles are created using the convention
<TraceFileName>.<username>.mmdd.hhmmss.log. The files will be created in the current directory of
the executing program, such as the directory into which the AgentDesktop is installed. You can provide
a fully qualified path for the TraceFileName if you wish to store the files in a different location. For
example, setting the value to "C:\Temp\CTIOSClientLog" would put the logfiles in the directory
"C:\Temp" using the naming convention CTIOSClientLog.<username>.mmdd.hhmmss.log. Client trace
files are simple ASCII text and can be opened with a conventional text editor such as Notepad.

How to Set Trace Levels

Trace levels for client processes, such as the AgentDesktop phone, can be found in the registry under:

\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\Logging\TraceMask

Warning: The default value for the trace masks is 0x40000307. Changing this value can have a serious impact
on client performance. It should only be modified by experienced field personnel or at the request of
Cisco support personnel.
This appendix provides answers to some frequently asked questions about CTI OS.

**Q.** What is the basic CTI OS architecture?

**A.** CTI OS provides end-user CTI functionality in an ICM system. On the ICM side it connects to the CTI Server. CTI Server typically runs on a PG (Peripheral Gateway). On the end-user side CTI OS provides an agent desktop application, a supervisor desktop application, and a programming interface to develop CTI custom applications.

The CTI OS system consists of three major components (see Figure C-1):

- CTI OS Server
- CTI Toolkit Agent Desktop
- CTI Toolkit IPCC Supervisor Desktop (only on Cisco IPCC Enterprise)

![Figure C-1 CTI OS Basic Architecture](image)

The CTI OS Server connects to the CTI Server via TCP/IP. Depending on call and agent load (see product specification), CTI OS Server resides on the same physical machine as the CTI Server. The CTI OS server consists of the following executable:

- CtiosServerNode.exe
In CTI Server terms, the CTI OS Server establishes an "All Events" or "Bridge" Mode connection to the CTI Server (as opposed to a "Client" Mode connection). CtiosServerNode handles CTI Toolkit connections (such as the connection to the Agent Desktop) over TCP/IP. CtiosServerNode is a "nodemanaged" component (see ICM documentation) and can therefore be started and stopped via the ICM Service Control Panel.

The main task of the CTI OS server is to do the heavy lifting of CTI messaging. It creates CTI objects (agents, calls, skillgroups, ...) and exposes these objects and selected event messages to CTI Toolkits. It also abstracts all switch specific behavior for clients, exposing the same interfaces to CTI Toolkits for all supported switches.

The CTI Toolkit Agent Desktop and CTI Toolkit IPCC Supervisor Desktop run on desktop computers and provide a user interface to CTI OS for Agents and Supervisors. The user interface includes a softphone for agentstate control, call control, handling of call context data and a chat interface. The supervisor functionality for IPCC includes monitoring and controlling agent states of monitored agents (logout, make ready), as well as barge-in and intercept functions.

The CTI Toolkit Agent Desktop and CTI Toolkit IPCC Supervisor Desktop are built upon the Client Interface Library (CIL). Developers can write custom applications using the published interfaces of CIL. The CIL is available in C++, COM (called CTIOSClient), .NET and Java, and as Active-X controls.

CTI OS supports a centralized configuration mechanism. Most parameters can be configured via the system registry on CTI OS server machine. The configuration settings will be downloaded by the CTI Toolkit application (for example, the Agent Desktop), when it connects to CTI OS server and requests them.

CTI OS will typically be installed in a duplex mode, with two CTI OS servers running in parallel. CTI OS desktop applications will randomly connect to either server and automatically fail over to the other server if the connection to their original CTI OS server fails. CTI OS can also run in a simplex mode with all clients connecting to one server (although the duplex mode is preferred because it supports fault tolerance).

Q. Which switches are supported by CTI OS? What are PeripheralTypes?

A. CTI OS provides a switch-independent user interface via its softphone application. To accomplish this, some parts of the CTI OS Server must be specialized to support each switch (also referred to as Peripherals or ACDs).

To support a switch, the CTI OS system must be configured with the PeripheralID and PeripheralType of each switch. PeripheralIDs are deployment-specific, and can be found in the ICM configuration.
Table C-1 shows switches and their corresponding PeripheralTypes that are supported in CTI OS Release 7.0(0).

<table>
<thead>
<tr>
<th>Peripheral Vendor (Name)</th>
<th>Peripheral Type Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IPCC System</td>
<td>23</td>
</tr>
<tr>
<td>Cisco IPCC</td>
<td>17</td>
</tr>
<tr>
<td>Cisco IPCC Hosted Edition</td>
<td>17</td>
</tr>
<tr>
<td>Lucent/Avaya Definity ECS</td>
<td>5</td>
</tr>
<tr>
<td>Aspect Call Center ACD</td>
<td>1</td>
</tr>
<tr>
<td>Alcatel 4400 ACD</td>
<td>13</td>
</tr>
<tr>
<td>Nortel Meridian ACD</td>
<td>2</td>
</tr>
<tr>
<td>Nortel Symposium</td>
<td>16</td>
</tr>
<tr>
<td>Rockwell Spectrum ACD</td>
<td>7</td>
</tr>
<tr>
<td>Siemens Hicom (North American version only)</td>
<td>11</td>
</tr>
</tbody>
</table>

Q. What is a Connection Profile?
A. A Connection Profile stores all of the information needed for a CTI OS Softphone to select a peripheral (switch) to log into. The information includes the Logical Name of the phone switch, the logical hostname or IP address of a CTI OS server (or pair of CTI OS Servers) that provide the service to that peripheral, and the ICM's PeripheralID that is used to track that Peripheral.

The Connection profiles are stored in the registry on the CTI OS server under:
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>_ctios1\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name.

When the CTI OS Server is first installed, the Setup program creates a default Connection Profile called "Peripheral type name" (for example, IPCC) with information collected from the Setup prompts. You can rename the default profile to any name you like and change its properties in the registry editor (REGEDIT), and add more Connection Profiles by re-running Setup to create a new default profile. Alternatively, you can export the registry tree for your Connection Profiles to a flat (.reg) file, and edit the profiles using Notepad. Then, double-click on the .reg file to reload it into your registry.

Q. What happens at softphone startup and login?
A. When the softphone starts up, the following steps are executed:
   1. The CTI toolkit agent desktop or CTI toolkit supervisor desktop looks at the System registry of the local client desktop machine and reads the HostName or IP address of the Configuration machine.
   2. The relevant configuration values include CTIOSA and CTIOSB and are located at HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTI Desktop\CTIOS.
   3. The CTI toolkit agent desktop or CTI toolkit supervisor desktop randomly connects to one of the two Configuration machines and downloads the CTI OS connection profiles and all other configuration settings.
4. These configuration settings are located in the registry of the Configuration machine under the following key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\EnterpriseDesktopSettings.

5. The CTI toolkit agent desktop or CTI toolkit supervisor desktop is now ready to accept login requests and the Login button is enabled.

When the user clicks login, the following steps are executed:

1. The login dialog is presented and the user can select one of the previously downloaded connection profiles and may enter additional required data.

2. When the user clicks OK, the softphone randomly attempts to connect with one of the two CTI OS servers defined in the user selected connection profile.

3. Upon successful connection, the client sends a SetSessionMode request to CTI OS server. This request sets a message filter for the agent ID.

4. When the CTI OS server receives a SetSessionMode request it does two things.
   - It determines the current state of the system including the relevant peripheral and sends SetAgentModeEvent, including the status, to the client.
   - It sends a QueryAgentStateRequest to CTI Server on behalf of the client to determine the current agent state on the switch.

5. When the Client receives SetAgentModeEvent it updates its own system status. This allows the client to inform the user if the system is offline and the login request is postponed.

6. When the client receives a QueryAgentStateConf, the client then sends a SetAgentStateRequest to login.

7. When CTI OS Server receives a login request, it snapshots the agent, logs in the agent if it is not already logged in, snapshots the agent's device, and snapshots any calls on the device. This builds the complete state of the agent.

8. Using the information obtained from the snapshots the softphone is updated to reflect the agent state and any calls. At this point the agent is fully logged in.

Q. Why is TimeInState on the Agent Real Time Status window sometimes black and sometimes red?

A. If an agent remains in a certain state for longer than 10 minutes, the TimeInState column will turn red to bring this agent to the supervisor's attention. If an agent changes state, the TimeInState column will be reset to 0 and turn black again.

Q. How can I change the update interval of SkillgroupStatistics and AgentStatistics?

A. The update interval for SkillgroupStatistics and AgentStatistics is set to 10 seconds by default. This means that every 10 seconds, the CTI OS server will request statistics from the CTI Server and send them to any connected Agent and Supervisor Desktops, where they will be displayed. The update interval can be changed in the system registry on the system where the CTI OS Server is installed by modifying the following keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\PollingIntervalSec
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\SkillGroup\PollingIntervalSec
```

Setting the update interval to zero (0) will disable statistics entirely. This is only supported for version 4.6.2 and later.
Besides the update interval of CTI OS, the ICM configuration has its own separate update interval to compute and store statistics (see ICM documentation). To prevent unnecessary network traffic, the CTI OS interval must not be smaller than the ICM interval.

Q. How can one customize which columns are displayed in the callappearance, agentstatistics and skillgroupstatistics grids?

A. The procedure for how to customize the columns in the grids is explained in the Cisco ICM Software CTI OS System Manager’s Guide, Chapter 4.

Q. How can I disable statistics minimization?

A. Release 4.6.2 and later: If you are not using the default statistics columns and are instead customizing your columns (as described in the Cisco ICM Software CTI OS System Manager’s Guide, Chapter 5), the CTI OS server will only send updates for the statistics that you have configured. This is done to reduce network traffic. If you would like to disable this feature and receive ALL statistics for every update, set DisableStatsMinimization = 1 in the registry at the following keys:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\          
   CTIOS_<InstanceName>\ctios\                                 
   EnterpriseDesktopSettings\AllDesktops\Grid\AgentStatistics\ 
   Columns\Number for agent statistics
```

and

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\          
   CTIOS_<InstanceName>\ctios\                                 
   EnterpriseDesktopSettings\All Desktops\Grid\SkillGroupStatistics\ 
   Columns\Number for skill group statistics
```

The desktop softphone will still only display the configured columns, but it will receive ALL statistics.

Note

A defect in CTI OS versions earlier than 4.7 prevents skill group statistics from being minimized on monitor mode applications. This problem was fixed in Releases 4.7 and later. An optional DisableMonitorModeStatsMinimization setting in the SkillGroupStatistics key shown above can be used to disable minimization of skill group statistics for monitor mode applications using version 4.7 and higher.

Q. Why does the column definition of the callappearance, agentstatistics or skillgroupstatistics grid not change after updating the registry?

A. The changes only become active when the CTI OS server and the client application (for example, softphone, Supervisor desktop) are shutdown and restarted.

Q. How do I change the header and column width of a displayed column?

A. The procedure for how to customize the columns in the registry is explained in the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, Chapter 4. A column key can have Header and Width string values (plus other values as explained in the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*).

Header: enter custom header; same as "Type" by default

Width: 70 screen units by default (for example, 140 will double the standard width)
Q. Why does CallsQNow on IPCC not display the current number of calls in the queue?
A. To look at the number of calls in queue on an IPCC switch, look at RouterCallsQNow. CallsQNow is supported only on legacy ACD switches.

Q. How can one change column 1 in skillgroupstatistics?
A. Column 1 of the skillgroupstatistics grid always displays the skillgroupnumber and cannot be changed. The column header can be edited.

Q. How can the network traffic caused by CTI OS statistics be reduced?
A. There are several ways to reduce the amount of traffic caused by the CTI OS Agent and Skillgroup Statistics messages.

• Turning off skill group or agent statistics for all agents
  This can be done separately for agent and skillgroup statistics via a registry setting for each on the machine that hosts the CTI OS server. Setting the PollingIntervalSec to 0 in the registry keys listed below will disable that particular set of statistics:
  For Agent Statistics:
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\PollingIntervalSec
  For Skillgroup Statistics:
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\SkillGroup\PollingIntervalSec

• Expanding the update interval between statistics
  The same registry keys indicated above, specify the update interval between statistics on the client in seconds if set to a value different from 0.
  For example, if PollingIntervalSec is set to 30 (default is 10) at
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\SkillGroup\, the client will see skillgroup statistics refresh every 30 seconds.
  For Agentstatistics, however, for reasons that the agent statistics is likely to change after the call, it is suggested that you continue to use the default behavior (see below), which ignores PollingIntervalSec at HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\CTIOS_<InstanceName>\ctios1\Server\Agent\PollingIntervalSec.

• Reducing the number of skillgroups overall and the number of skillgroups per agent
  This can be accomplished via the Agent Explorer or Skillgroup Explorer config tool, which is part of the ICM Configuration Manager.

• Reducing the number of specific statistics fields being sent to the client desktop
  By default, the CTI OS server only sends the statistics required for display on the CTI Toolkit. The procedure to customize which fields are displayed on the client is explained in the CTI OS System Manager’s Guide for Cisco ICM/IPCC Enterprise & Hosted Editions Chapter 4.

• Turning off statistics for some agents while leaving them on for others
In CTI OS 4.7 a new registry key was introduced to allow disabling of statistics on a per agent basis. This is done by creating a connection profile (see section on connection profiles in the CTI OS systems manager guide) for which statistics are disabled and direct some agents to use this connection profile, while others use a different connection profile with statistics enabled.

The relevant keys are:
- DisableAgentStatistics
- DisableSkillgroupStatistics

A value of 1 indicates that the statistics are disabled for this connection profile, while a value of 0 indicates they are enabled (default).

The keys are located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ CTIOS_<InstanceName>\ctios1\ EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\ Name\<ConnectionProfileName>
```

- Poll for Agent statistics only at end of call.

If the registry key "PollForAgentStatsAtEndCall" located at

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ CTIOS_<InstanceName>\ctios1\Server\Agent\ 
```

is set to 1, PollingIntervalSec described above will be ignored and agent statistics will only be sent when a call ends. This is the recommended method (and the default behavior), since most statistics fields are only updated when a call ends. Some statistics, like TimeLoggedinToday, TimeNotReadyToday and TimeReadyToday are updated on the client independently until a new message arrives from CTI server. If PollForAgentStatsAtEndCall is set to 0, PollingIntervalSec will become effective and determine the update interval as described.

Q. Which logs are required to diagnose a Silent Monitor issue, and what is the recommended TraceMask?

A. Silent Monitor is largely a client based feature and uses CTI OS server to signal the start and stop of Silent Monitor sessions as well as reporting status. See Appendix B, “Obtaining Logs for Support” for details of how to retrieve logs.

The following logs are required to diagnose a problem:
- Client log from Supervisor Desktop (CtiosClientlog)
- Client log from Agent Desktop (CtiosClientLog)
- Ctios Server log (from both CTI OS servers in a duplexed environment, retrieved with dumplog)

The default TraceMask of 0x40000307 for CTI Toolkits and 0x20003 for CTI OS Server are sufficient for high level issues. A TraceMask of 0xF0F is recommended for CTI Toolkit detailed troubleshooting and a TraceMask of 0xA0F is recommended for CTI OS server detailed troubleshooting.

Q. What Version of CTI OS Supports Security?

A. The versions of CTI OS that support Security are:
- CTI OS Server 7.0
- C++ CIL and COM CIL of CTI Toolkit 7.0
If old CTI Toolkit tries to connect to CTI OS Server 7.0 with security ON, then the connection will fail.

If Java CIL or .NET CIL client try to connect to CTI OS Server 7.0 with security ON, then the connection will fail.

Q. How do you know if Security is ON/OFF on CTI OS Server?
A. 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 “SecurityEnabled” registry value exists under the following registry key:

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

Note: 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.

Q. How do you configure security on the CTI OS server and CTI Toolkit?
A. All the necessary information is in *CTI OS System Manager Guide*.

Q. What files are used by Security, and where are they located?
A. The CTI OS files that are used by Security can be classified as CTI OS Server Security files and CTI Toolkit Security files.

**CTI OS Server Security Files:** If the CTI OS Server is installed under “<drive>\ICM\<instance name>\<CTIOS Component name>” directory, then the following security files will be copied to “<drive>\ICM\<instance name>\<CTIOS Component name>\Security” directory.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiosClient.pem (if CTI OS Server has a peer)</td>
<td>This file contains the CTI Toolkit certificate, and its private key.</td>
</tr>
<tr>
<td>CtiosClientPWD.dat (if CTI OS Server has a peer)</td>
<td>This file contains the password which is used to encrypt the CTI Toolkit private key. This password is saved in cipher text.</td>
</tr>
<tr>
<td>PrivateClientKey.pem (if CTI OS Server has a peer)</td>
<td>This file contains RSA private key which is used to decrypt/encrypt the password that is saved in CtiosClientPWD.dat.</td>
</tr>
<tr>
<td>CtiosServer.pem</td>
<td>This file contains CTI OS Server certificate, and its private key.</td>
</tr>
<tr>
<td>CtiosServerPWD.dat</td>
<td>This file contains the password which is used to encrypt the CTI OS Server private key. This password is saved in cipher text.</td>
</tr>
<tr>
<td>File Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>PrivateServerKey.pem</td>
<td>This file contains RSA private key which is used to decrypt/encrypt the password that is saved in CtiosServerPWD.dat.</td>
</tr>
<tr>
<td>MonitorPWD.dat</td>
<td>This file contains the monitor mode password in cipher text.</td>
</tr>
<tr>
<td>PrivateMonitorKey.pem</td>
<td>This file contains RSA private key which is used to decrypt/encrypt the password that is saved in MonitorPWD.dat.</td>
</tr>
<tr>
<td>CtiosDH1024.pem</td>
<td>This file contains Diffie-Hellman-Parameters (1024 bit).</td>
</tr>
<tr>
<td>CtiosRootCert.pem</td>
<td>This file contains CA certificate.</td>
</tr>
<tr>
<td>openssl.exe</td>
<td>This is the OpenSSL command line tool which is used when troubleshooting is necessary.</td>
</tr>
<tr>
<td>dbghelp.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>atl71.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>mfc71.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>mfc71d.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>msvcp71.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>msvcp71d.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>msvcr71.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
<tr>
<td>msvcr71d.dll</td>
<td>This system DLL is needed to run openssl.exe</td>
</tr>
</tbody>
</table>

**CTI Toolkit Security Files:** If the CTI Toolkit is installed under “<drive>\Program Files\Cisco Systems, Inc\CTIOS Client” directory, then the following security files will be copied to “<drive>\Program Files\Cisco Systems, Inc\CTIOS Client\Security” directory.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CtiosClient.pem</td>
<td>This file contains the CTI Toolkit certificate, and its private key.</td>
</tr>
<tr>
<td>CtiosClientPWD.dat</td>
<td>This file contains the password which is used to encrypt the CTI Toolkit private key. This password is saved in cipher text.</td>
</tr>
<tr>
<td>CtiosRootCert.pem</td>
<td>This file contains CA certificate.</td>
</tr>
</tbody>
</table>
Q. What Type of Certificate Authority (CA) was used to sign both CTI OS Server and Client Certificate Requests?

A. If the value of “CAType” registry key is 1, then the self signed CA is used.
   If the value of “CAType” registry key is 2, then the third party CA is used.

In CTI OS Server, this registry value exists under the following registry key:

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

In CTI Toolkit, this registry value exists under the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTI Desktop\CtiOs
```

Both CTI OS Server and CTI Toolkit certificate requests need to be signed by the same CA. There are two types of CA.

- A self signed CA which is created by running “CreateSelfSignedSetupPackage.exe” program
- A third party CA.

So, if the CTI OS Server certificate request is signed by a self signed CA, then all CTI Toolkit certificate requests must be signed by a self signed CA.

Q. How do we display information about a Certificate?

A. Following are the various options for Display Information About a Certificate:

- Display the contents of a certificate:
  ```
  openssl x509 -in CtiosClient.pem -noout -text
  ```
Appendix C: CTI OS FAQs

- Display the certificate serial number:
  openssl x509 -in CtiosClient.pem -noout -serial
- Display the certificate subject name:
  openssl x509 -in CtiosClient.pem -noout -subject
- Display the start and expiry dates:
  openssl x509 -in CtiosClient.pem -noout -dates

Q. What type of Peripheral does Multi-Tenancy/Multi-Instance CTI OS support?
A. “IPCC Hosted Edition” only.

Q. Can I install Multi-Tenancy/Multi-Instance CTI OS on a regular IPCC?
A. No. Multi-Tenancy/Multi-Instance CTI OS supports “IPCC Hosted Edition” only.

Q. Can C++ CIL, COM CIL, Java CIL, and .NET CIL Clients connect to Multi-Tenancy/Multi-Instance CTI OS Servers?
A. Yes.

Q. Does Multi-Tenancy/Multi-Instance CTI OS support Siebel?
A. No. It does not support Siebel.

Q. Does Multi-Tenancy/Multi-Instance CTI OS support Security?
A. Yes it does. Turning security ON in one of the CTI OS servers does not affect the other servers that are running on the same machine.

**Note**
If old CTI Toolkit tries to connect to CTI OS Server 7.0 with security ON, then the connection will fail.
If Java CIL or .NET CIL client try to connect to CTI OS Server 7.0 with security ON, then the connection will fail.

Q. Do all CTI OS Servers (in a Multi-Instance environment) running on the same machine use the same “ListenPort”?
A. No. Each CTI OS Server must have a unique listen port. The “ListenPort” value of a specific CTI OS server can be found under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\connections

Q. How many CTI OS Servers (in a Multi-Instance environment) can I have installed on one machine?
A. Up to 10 CTI OS Servers can be installed on one machine.

**Note**
Multi-Instance CTI OS supports up to 10 instances, and each instance listens on a unique TCP port. Hence, all 10 ports should be accessible via a firewall.

Q. Can I control one CTI OS Server (in a Multi-Instance environment) without affecting the others?
A. Yes. You can manage CTI OS Servers independently. You can stop, start, and recycle one CTI OS server without affecting the others.

Q. Does each CTI OS Server (in a Multi-Instance environment) have its own log files?
A. Yes it does. The log files can be located in “<drive>:\ICM<instancename>\CTIOS1\logfiles” directory.

Q. Can I change the trace mask of one CTI OS Server (in a Multi-Instance environment) without affecting the others?
A. Yes, there is a trace mask for every CTI OS Server. You can change the trace mask through the registry. The “EMSTraceMask” trace mask value of a specific CTI OS server can be found under:

`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\CTIOS_<InstanceName>\CTIOS1\EMS\CurrentVersion\LibraryProcesses\ctios`

Q. Can two or more CTI OS Servers (in a Multi-Instance environment) that reside on the same machine be connected to the same CtiServer?
A. No. The relation between CTI OS Server and CtiServer is one to one. So, one CTI OS Server can be connected to only one CtiServer.
INDEX

C
Chat problems 1-16
Configuration server 2-1
Connection profile 2-2, C-3
CtiDriver
  connection problems 1-1
CTI OS architecture C-1
CTI OS Server 1-1
  logs B-1
CTI Toolkit
  logs B-8

E
Emergency assist problems 1-15

F
Failover problems 1-14

I
IPCC Supervisor problems 1-17
  button 1-17
  real time status window 1-17

M
Multiple peripherals 1-2

P
PeripheralType
  list of supported C-3

S
Softphone problems
  behavior 1-7
  button 1-7
  ECC variables 1-13
  login 1-3
  logout 1-6
  making calls 1-9
  problems after call ends 1-11
  receiving calls 1-9
  startup 1-3
  statistics problems 1-12
  talking on a call 1-9
  Supervisor assist problems 1-15

T
Trace levels
  CTI OS Client B-8
  CTI OS Server B-2