Cisco ICM Software CTI OS Troubleshooting Guide
Cisco CTI Release 6.0(0)
May 2004

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number:
CONTENTS

About This Guide vii
  Purpose vii
    How to Use this Manual vii
    What if I can’t resolve the problem? viii
  Other Useful Resources viii
  Audience viii
  Organization ix
  Conventions ix
  Other Publications x
  Obtaining Documentation x
    Cisco.com x
    Ordering Documentation x
  Documentation Feedback xi
  Obtaining Technical Assistance xi
    Cisco TAC Website xi
    Opening a TAC Case xii
    TAC Case Priority Definitions xii
  Obtaining Additional Publications and Information xiii

CHAPTER 1 Problems and Symptoms 1-1
  CTI OS Server Problems 1-1
    CTI OS Server Cannot Connect to CtiDriver 1-1
    CtiDriver Cannot Connect to CTI Server 1-2
    Problems Using Multiple Peripherals 1-3
General Softphone/Desktop Problems 1-4
Start up Problems 1-4
Login Problems 1-4
Logout Problems 1-7
Miscellaneous Button Problems 1-8
Miscellaneous Behavior Problems 1-9
Problems Making Calls 1-10
Problems Receiving Calls 1-11
Problems While Talking on a Call 1-12
Problems After Call Ends 1-13
Statistics Problems 1-15
Problems with ECC Variables 1-16

Failover Problems 1-17
Emergency and Supervisor Assist Problems 1-19
Chat Problems 1-20

Supervisor Feature Problems (IPCC Only) 1-21
Supervisor Button Problems 1-21
Problems with Real Time Status Window 1-22

Media Termination Problems 1-23
Login Problems 1-24
Sound Problems 1-24
Silent Monitor Problems (IPCC Only) 1-26

CHAPTER 2
Resolutions to Common Problems 2-1
Incorrect or Unreachable Configuration Server 2-1
Incorrect or Unreachable CTI OS Server in Connection Profile 2-2
Incorrect Configuration of Peripheral ID or Peripheral Type During Server Install 2-4
Incorrect Configuration of the Peripheral ID in the Connection Profile 2-5
Contents

Media Termination Cannot Find Wave Files  2-6
Volume is Too Low or Too High  2-7
Media Termination Did Not Release Sound Resources  2-7

APPENDIX A  Obtaining Logs for Support  A-1
Taking CTI OS Server logs  A-2
How to Set Trace Levels  A-3
Taking CTI OS Client Logs  A-3
How to Set Trace Levels  A-4

APPENDIX B  CTI OS FAQs  B-1

INDEX
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 Cisco ICM Software CTI OS System Manager’s Guide on the CTI OS distribution media (CD) for the product description, architecture, installation, and configuration information for the CTI OS product. See 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 can’t 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 Technical Assistance” section.

Other Useful Resources

This guide presumes knowledge of the CTI OS system, and therefore cannot cover every detail of the system architecture and environment. Table 1 displays useful resource documentation for the ICM and CTI OS systems.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICM configuration</td>
<td><em>Cisco ICM Software Administration Guide</em></td>
</tr>
<tr>
<td>Configuring CTI OS</td>
<td><em>Cisco ICM Software CTI OS System Manager’s Guide</em></td>
</tr>
<tr>
<td>CTI OS System Architecture</td>
<td>Refer to Appendix B, “CTI OS FAQs”</td>
</tr>
<tr>
<td>Connection profiles</td>
<td><em>Cisco ICM Software CTI OS System Manager’s Guide</em></td>
</tr>
<tr>
<td>CTITest tool</td>
<td>Ctitest.txt file in Tools directory on CTI OS CD</td>
</tr>
<tr>
<td>Supported switches</td>
<td>Refer to Appendix B, “CTI OS FAQs”</td>
</tr>
<tr>
<td>Peripheral types</td>
<td>Refer to Appendix B, “CTI OS FAQs”</td>
</tr>
</tbody>
</table>

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.

Refer to the *Cisco ICM Software Product Description* guide for an introduction to ICM software.
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 B, “CTI OS FAQs”</td>
<td>Contains important facts about CTI OS.</td>
</tr>
</tbody>
</table>

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 Script &gt; Call Type Manager.</td>
</tr>
<tr>
<td>Italic type indicates one of the following:</td>
<td>A skill group is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td>- A newly introduced term</td>
<td>Do not use the numerical naming convention that is used in the predefined templates (for example, persvc01).</td>
</tr>
<tr>
<td>- For emphasis</td>
<td>IF (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 Cisco ICM Software Database Schema Handbook.</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 File &gt; Save.</td>
</tr>
</tbody>
</table>
Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software, see the Cisco web site listing Customer Contact Center documentation.

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:
http://www.cisco.com/univercd/home/home.htm
You can access the Cisco website at this URL:
http://www.cisco.com
International Cisco websites can be accessed from this URL:

Ordering Documentation

You can find instructions for ordering documentation at this URL:
You can order Cisco documentation in these ways:
- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
About This Guide

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

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac
Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:


Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

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

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

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


TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

### Obtaining Additional Publications and Information

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

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

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
  
  http://cisco.com/univercd/cc/td/doc/pcat/

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

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,
configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
http://www.cisco.com/go/iqmagazine

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

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
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 CtiDriver

**Symptom**  A message in the CTI OS server console window indicates a system event for the CtiDriver going offline, followed by messages indicating how long the driver has been unreachable. The message reads "[SYSTEM] SYSTEM_EVENT: SYS_CTI_SERVER_DRIVER_OFFLINE."

**Possible Cause**  This problem may be caused by a failure of the CtiDriver process. Try the following:

- Check to see if the CtiDriver process is running (there will be a console window for it). If it's not running, then it must be restarted. Start up ICM Service Control and restart CTI OS.
- If the CtiDriver process is running, then the problem might be that there is more than one CTI OS Server running on the same NT/W2K Server, creating a system resource conflict. Stop all CTI OS server processes on
the system (from ICM service control or by closing the console window(s), as appropriate). Restart the CTI OS server. Ensure that only one CTI OS Server (CTIOSServerNode and CtiDriver process pair) is running at a time on the system.

If this fails to resolve the problem, set the trace level on the CTIOSServer to 0x00000fff, and collect a log file of the CTI OS server to send to Technical Support. See Appendix A, “Obtaining Logs for Support,” for details on how to set trace levels and collect logs.

CtiDriver Cannot Connect to CTI Server

**Symptom**  Error messages in the CtiDriver 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 CTIDriver console window should display an error message with an error description. Some possible causes of this symptom are:

- CtiDriver 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:

  HKLM\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\CtiDriver\Config

- If the configuration is correct, CtiDriver 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 CtiDriver 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:
CTI OS Server Problems

HKLM\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName\\ <CTIOSServerName\\CtiDriver\Config.

If this fails to resolve the problem, set the trace mask on CtiDriver to 0x00000fff, and collect a log file of the CtiDriver to send to Technical Support. See Appendix A, “Obtaining Logs for Support,” for details on how to set trace levels and collect logs.

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 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 B, “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\<CTIOSInstanceName\\<CTIOSServerName\\Server\Peripherals. This registry entry is a table, where each entry is named by a Logical Name (e.g. 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 *Cisco ICM Software CTI OS System Manager’s Guide* for a complete explanation of configuring peripherals and connection profiles in the CTI OS Server.
Chapter 1  Problems and Symptoms

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

If you are using the Cisco Media Termination Service, see also the section “Media Termination Problems” for login problems specific to that package.

Symptom  The softphone starts correctly but when I attempt to login (i.e., 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 (i.e. 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 (i.e., 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.
Chapter 1  Problems and Symptoms

General Softphone/Desktop Problems

**Symptom**  Duplicate Login: The softphone starts correctly but when I attempt to login (i.e. 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 the following registry key should be set to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\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\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<YourConnectionProfileName>\LoginTimeout
```
General Softphone/Desktop Problems
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\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<YourConnectionProfileName>\RejectIfAlreadyLoggedln
```

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 (refer to the Cisco ICM Software Configuration Guide). This timeout cannot be disabled at this time.

- There may be another CTI OS client 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 "RejectIfAlreadyLoggedln" in the ConnectionProfile being used. For details, see Symptom D in preceding section dealing with Login problems.

- If this is an IPCC system and your agent is a member of an agent team, your supervisor may have logged you out.
If you are using the Cisco Media Termination Service, this symptom may indicate a recovery from a Media Termination failure. Login again.

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.

### 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 CTIOS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise 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
Chapter 1 Problems and Symptoms

General Softphone/Desktop Problems

- 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 explained in the table can be used to enable this functionality. (Refer to the *Cisco ICM Software CTI OS System Manager’s Guide* for information.) In brief, the registry keys listed below need to be set to 1.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ <CTIOSInstanceName>\ <CTIOSServerName>\Server\Agent\LogoutReasonRequired

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ <CTIOSInstanceName>\ <CTIOSServerName>\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 explained in the table can be used to enable this functionality for a TDM switch. (Refer to the *Cisco ICM Software CTI OS System Manager’s Guide* for information.) In brief, the registry keys listed below need to be enabled as needed.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ <CTIOSInstanceName>\ <CTIOSServerName>\Server\Agent\EnableWrapupDialog

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \ <CTIOSInstanceName>\ <CTIOSServerName>\Server\Agent\WrapupDataRequired
```
General Softphone/Desktop Problems

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 Cisco ICM Software CTI OS System Manager’s Guide 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 (e.g., the request specified an invalid AgentID).
- Message boxes display stating that arguments are missing (e.g. 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.

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 (e.g., for IPCC 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.
General Softphone/Desktop Problems

**Symptom**  On a system running a version of CallManager earlier than Version 4.0, a non-controller Conference party receives a Control Failure when it tries to make a Consult Call for a Conference.

**Possible Cause**  The Server\CallObject\IPCCConference_Supports MultipleControllers registry value must be set to 0 on systems that are running CallManager versions earlier than Version 4.0. See the *Cisco ICM Software CTI OS System Manager’s Guide* for details on this registry value.

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 in a state that allows it to receive calls (e.g., on most ACD systems, an 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. (Refer to the *Cisco ICM Software Administration Guide* for more information on how to do this.)
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. (Refer to the Cisco ICM Software Administration Guide for more information on how to configure the Ring No Answer feature.)

Problems While Talking on a Call

Symptom  : All three AgentState buttons (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 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 Calls 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 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.

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, etc., instead of 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: HKLM\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\Server/Agent/WrapupStrings.

Replace the default Wrapup strings with more meaningful ones, adding more if necessary. NOTE: You must restart CTI OS Server and the softphone to for your changes to take effect. Refer to the Cisco ICM Software CTI OS System Manager’s Guide 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 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 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.
Chapter 1      Problems and Symptoms

General Softphone/Desktop Problems

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 \<CTIOSInstanceName>\<CTIOSServerName>\Server\Agent\for agent statistics and

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS \<CTIOSInstanceName>\<CTIOSServerName>\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\CTIOS \<CTIOSInstanceName>\<CTIOSServerName>\CtiDriver\Config

You can find a list of the statistics supported for a particular protocol version (X) in the Cisco ICM Software CTI Server Message Reference Guide (Protocol X).
**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 *Cisco ICM Software CTI OS System Manager's Guide* explains this setting. If you are running version 4.7 or later, check this registry setting. If it is present it should be set 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 *Cisco ICM Software CTI OS System Manager's Guide* 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. It may be that the ECC variables are being sent with the call but are not being displayed correctly. If this is the case, you should be able to enter ECC data via the softphone call appearance grid after you make the call.

- Check that the ECC variables are registered correctly in the CTI OS server registry. ECC variable registration is described in the *Cisco ICM Software CTI OS System Manager's Guide* in Chapter 4. Remember that the ECC scalar/array key name configured in the registry is case sensitive and must be the same as that configured in the ICM without the "user." prefix. It may be that the ECC variable name does not match the names
known by ICM and the data is being discarded. If this is the case, you should not be able to enter ECC data via the softphone call appearance grid after you make the call.

**Symptom**  On a duplexed system (i.e., a system with two CTI OS Servers), some ECC variables do not always appear in the CTI OS Agent Desktop and CTI OS Supervisor Desktop for IPCC Enterprise Call Information grids.

**Possible Cause**  When you start the CTI OS Agent Desktop or CTI OS Supervisor Desktop for IPCC Enterprise on a duplexed system, it downloads Call Information grid settings from one of the two CTI OS servers (selected at random). If ECC variable configuration on the two CTI OS servers is not identical, inconsistencies in Call Information grid content will occur. Check the ECC variable configuration on both CTI OS Servers and make sure that it is identical.

### 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, or an overloaded CTI OS server. 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.

- 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 Cisco ICM Software CTI OS System Manager's Guide, 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 clients 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 similar 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 state.

- There may be a problem with the ICM configuration. This functionality requires an ICM script (refer to Cisco ICM Software CTI OS System Manager's Guide) 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 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 Cisco ICM Software CTI OS System Manager’s Guide 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 Cisco ICM Software CTI OS System Manager’s Guide.

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 in to 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.
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 Call Manager 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 \ <CTIOSInstanceName>\ <CTIOSServerName>\CtiDriver\Config. It should be 0x296 or decimal 662 - 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  Cannot see agent names in real time status window.

Possible Cause  The names displayed are the names entered in the ICM database (see ICM Configuration Manager - Agent Explorer). Some possible causes:

- The ODBC driver used to query for these names was not setup correctly during CTI OS Server setup (see the Cisco ICM Software CTI OS System Manager's Guide).
- There are no names configured in the ICM database.
The Data Source Tool used to configure the DSN entry to retrieve the names has an option to “Test Data Source” in the last dialog. It is recommended to use this tool to verify the DSN. Common problems include that the ICM database has no user configured with the right privileges or the connection method is not set properly (for example, named pipes will not work if the SQL server with the database is located on a different domain - use TCP instead).

**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.

**Media Termination Problems**

This section discusses problems related to Media Termination.
Login Problems

Symptom  After clicking the Login button, and entering the necessary information in the Login dialog (including my Media Termination instrument number), and clicking OK, the Connected to <server name> and Online messages display in the status bar, but there is no agent state or change in button enablement.

Possible Cause  This indicates that you were not able to log in, even though there is no error message. First, explore softphone login problems described in the section “General Softphone/Desktop Problems”. If these do not describe and resolve the problem, ensure that the mediaclient.exe application is running:

Open the TaskManager by right-clicking on the Windows task bar. Click the Processes tab and check if MediaTerminationProcMonitor.exe and MediaClient.exe are there. If not, exit the softphone and restart it. Check TaskManager to ensure these processes are running. If they are still not running, check your client installation to see that these processes were installed.

Sound Problems

Symptom  Cannot hear ring, busy, fastbusy, or DTMF tones.

Possible Cause  This symptom may be caused by any of the following problems:

- The Media Termination application cannot find the wave files because they are not in the directory where the application is looking for them. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)

- The volume is turned too low on your machine. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)
Chapter 1 Problems and Symptoms

Media Termination Problems

- In the course of a failover scenario, the Media Termination application did not release the sound resources on the computer resulting in no sound reception or transmission. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)

Symptom Cannot hear the other party.

Possible Cause This symptom may be caused by any of the following problems:

- Your headset may be broken. Try a new headset.
- The volume is turned too low on your machine. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)
- In the course of a failover scenario, the Media Termination application did not release the sound resources on the computer resulting in no sound reception or transmission. (See Chapter 2, “Resolutions to Common Problems,” for more information on how to resolve this problem.)
- If you are connecting to CTI OS Server via a VPN connection, special configuration is necessary. Refer to the Cisco ICM Software CTI OS System Manager's Guide for instructions.

Symptom The other party cannot hear the transmission.

Possible Cause Ensure that the microphone on your headset is working and that your sound card is working. You can do this using the Windows Sound Recorder. With your headset plugged in, press the Record button and speak into the microphone. You should see a distinct sound pattern and you should be able to hear what you just recorded when you press the Play button. If you
cannot see the pattern and hear the recorded sound, there is either a headset problem or a sound card problem. Try a different headset. If that does not fix the problem you may need a different sound card.

**Silent Monitor Problems (IPCC Only)**

**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:

<table>
<thead>
<tr>
<th>CTI Warning:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Error Code = 0x1000000C]</td>
</tr>
<tr>
<td>Silent Monitor session failed.</td>
</tr>
<tr>
<td>The workstation of the targeted agent is not receiving any voice from the IP phone.</td>
</tr>
<tr>
<td>There are two possible causes for this problem</td>
</tr>
<tr>
<td>1) The agent selected for monitoring has logged on to a IP hardphone, which is not connected to the agent desktop system.</td>
</tr>
<tr>
<td>2) The network adapter card (NIC) on the agent desktop system is not compatible with Silent Monitor in a network environment where data and voice are separated on different VLANs.</td>
</tr>
<tr>
<td>Please contact your system administrator.</td>
</tr>
</tbody>
</table>

**Possible Cause**

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

– The PC cannot capture the voice packets sent from the phone (see next symptom).

**Symptom** A Silent Monitor session failed message box appears because the PC cannot capture the voice packets sent from the phone. (See also previous symptom.)

**Possible Cause** If agents use supported IP hardphones with their desktops connected to the second port of the phone and if the network is configured to use a VLAN for voice traffic, the network card and driver in the agent desktop PC need to be capable of capturing packets on a different VLAN in order for Silent Monitor to work. This restriction does not apply if the network is not configured for VLANs.

As a first step, Cisco recommends to use a Public domain network analyzer called Ethereal to verify if voice packets can be captured.


2. Make sure WinPcap is installed on the agent’s machine via Start->Control Panel->Add remove programs. WinPcap should be on the list. If not, run WinPcap_3_0_nogui.exe from the CTIOS CD (located at ctios\Installs\CTIOSClient) to install it or download WinPcap from http://winpcap.polito.it/. Reboot to make sure WinPcap will function properly.

3. Run Ethereal: Select Capture->Start->OK

4. Make a voice call from or to the agent’s phone (there is no need to be logged on to CTIOS right now) and insure that UDP packets are captured at roughly 100 packets/second.

5. If no packets are captured, click stop, then Capture -> Start again, but this time select an different Adapter from the “Interface” drop down list (if available).

If Ethereal cannot capture packets, neither can CTI OS. Possible reasons:
Silent Monitor Problems (IPCC Only)

- The Phone is not sending the packets because the PC port is deactivated (check Network settings on the phone, note, in this case the system is off the network). 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 specific NIC card in the PC has problems accessing voice packets. Check NIC card properties and configuration. Some NIC cards require special configuration to capture packets off a different VLAN. If possible, try another NIC card (or system) to verify this is the case.

**Symptom** After just installing CTI OS Server Release 5.1 or later, CTI OS Agent Desktop, and CTI OS Supervisor Desktop for IPCC Enterprise (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 OS Supervisor Desktop for IPCC Enterprise.

**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 on to a connection profile (See section about connection profiles in the Systems manager guide) 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 (i.e., 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:

![CTI Warning]

Possible Cause

- The agent is logged on to a connection profile, which has Silent Monitor disabled (See section about connection profiles in the Systems manager guide) 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 OS client software and close the CTI OS Agent Desktop.

- On certain systems it is necessary to reboot after installing WinPCap, which is installed with Silent Monitor option on the CTI OS 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. See the following Microsoft website for more information on how to check this setting and how to disable the ICF:
  
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 in to 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. (e.g. call begins, hold, retrieve, call ends, etc.) 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 OS Supervisor Desktop for IPCC Enterprise.

To determine if this is the case, retrieve the CTI OS Client Log from the agent’s computer and open it on 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
  CCTiOsObject(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. This can be obtained from
http://winpcap.polito.it/install/default.htm. 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 0xA0f 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 0x7. If the tracing level
is set higher than the default, silent monitor audio quality may be
impacted. Reduce the desktop trace mask to 0x7 or lower.

- Check the tracing level of the media termination control. On rare
occasions, excessive logging related to this control may degrade audio
quality. The trace settings for this control are located in the Windows
registry at HKEY_CURRENT_USER\Software\Cisco
Systems\CCNMediaTerm\1.0\Tracing. To turn off all tracing for the
media termination control set the value AllComponents to '1'.

- 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.
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 CTI OSA, CTI OSB, PortA, and PortB in the registry under the key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\CTI Desktop\CTI OS.
  - 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.
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
Incorrect or Unreachable CTI OS Server in Connection Profile

button is enabled). Additionally, the status bar displays the last message received from the configuration server (i.e. Disconnected/Offline) 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 CTI OSA and CTI OSB settings under the HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\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\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<Profile name from step a>

Check the following items:
- The key shown above should exist on both configuration machines.
- The information contained within the key should be identical on both configuration machines.
- Check the values of CTI OSA, CTI OSB, 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.
- If the names (or addresses) of the connect machines are correct, the problem may be caused by a loss of network connectivity or an inability to resolve the CTI OS Server name.
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:

- From the client application machine, open a console window and attempt to ping the connect machines. If the system is configured correctly, the ping should
- If the ping succeeded then the problem may be that the CTI OS server is not running on either of the connect machines. Start the CTI OS server on those machines and restart the client application.

- If the ping fails for both connect machines and the connect machine entries in the registry are not TCP addresses, the problem may be an inability to resolve the connect machine name into an IP address.
  - Try to ping the IP addresses corresponding to the connect machine names configured in the registry.
  - 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 connect machine names in the registry with the associated IP addresses, restart the download machines, 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 connected machine is down. Your TCP/IP network administrator should be able to help resolve this issue.

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:

- From the client application machine, open a console window and attempt to ping the connect machines. If the system is configured correctly, the ping should
- If the ping succeeded then the problem may be that the CTI OS server is not running on either of the connect machines. Start the CTI OS server on those machines and restart the client application.

- If the ping fails for both connect machines and the connect machine entries in the registry are not TCP addresses, the problem may be an inability to resolve the connect machine name into an IP address.
  - Try to ping the IP addresses corresponding to the connect machine names configured in the registry.
  - 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 connect machine names in the registry with the associated IP addresses, restart the download machines, 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 connected machine is down. Your TCP/IP network administrator should be able to help resolve this issue.
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:

- 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\ <CTIOSInstanceName>\ <CTIOServerName>\ 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.
Media Termination Cannot Find Wave Files

- 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.
- 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\<CTIOSInstanceName>\<CTIOServerName>\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name\<Profile name from step a> on the server with which the client application is connected.
- Modify the value of peripheralID so that it is correct. (The Peripheral ID can be found in the ICM configuration.)
- Restart the CTI OS server.
- Restart the client application.
- Try to login again.

Media Termination Cannot Find Wave Files

If a particular wave file needed by Media Termination is not located where Media Termination thinks it should be, Media Termination will fail to play the associated sound when required.

- Look in the latest TraceFile_000n.txt file located in the IPMedia directory under the directory where the AgentDesktop was installed.
- Search this file for the following entry:
  "PlayWave::Unable to playwave. Couldn’t open file = <full path name of wave file>"
- Search the machine for the file indicated in the previous step and then move it into the directory where the application is looking for it. (This directory is indicated in the trace file entry found in the previous step).
Volume is Too Low or Too High

If the volume is set to an inappropriate level, the agent may be unable to hear Media Termination sounds or voice at the appropriate times. To check the volume level, bring up the Windows volume control (the speaker icon in the lower-right section of the task bar) and adjust the wave volume. If this is not satisfactory, you can change the following settings in the registry:

- To adjust the volume for the Wave files (i.e. Ringing, Busy, Tones, etc.), adjust the setting for HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\CTI Desktop\IPMedia\Volume\WaveFiles. The default is 30 (0x1e) and the range is from 0 (mute) to 100 (full volume).

- To adjust the volume for voice and wave files equally, adjust the setting for HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\CTI Desktop\IPMedia\Volume\Speaker. The default is 100 (full volume).

Media Termination Did Not Release Sound Resources

If Media Termination failed to release a sound resource after a failure, it will be unable to obtain the appropriate sound resources when it recovers from the failure and it will be unable to play sounds at the appropriate times. To determine whether this has occurred, look in the latest TraceFile_000n.txt file (see Section 3.5 for details on where to find this file) to see if the following entry has been logged:

"CCNSMT.dll : MicrophoneAvailable : error : could not open wavein device. waveInOpen returned 0x463521.781 : : CCNSMT.dll : ~SetTransmitSource : error : Microphone not available."

If this is the case, you must reboot your computer to restore sound function.
Media Termination Did Not Release Sound Resources
Obtaining Logs for Support

When you report a problem to Cisco, Cisco personnel will ask that you supply certain details about that 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 OS client
- 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 OS Client logs and trace levels. See the *Cisco ICM Software Administrator Guide* for information on other logs.

## Taking CTI OS Server logs

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

```
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM\<CustomerInstance>\CTIOS\EMS\CurrentVersion\Library\Processes\CTIOS\ EMSLogFileLocation
HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM\<Customer Instance>\CTIOS\EMS\CurrentVersion\Library\Processes\ctidriver\ EMSLogFileLocation
```

The default location is: `<CTI OS Server Install Directory>\logfiles`. It is recommended that the default values not be changed. 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 `<CTI OS Server Install Directory>\logfiles` directory in order to use dumplog on the CTI OS Server log files. For information on how to use dumplog, refer to the *Cisco ICM Software Administration Guide*.

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

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

⚠️ Warning The default value for the trace masks is 0x03. 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.

Taking CTI OS Client Logs

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

\HKEY_LOCAL_MACHINE\Software\Cisco Systems\CTIOS\Logging\TraceFileName

The default filename is CTIOSClientLog. Logfiles are created using the convention <TraceFileName>.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 CTI OSClientLog.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\CTIOS\Logging\TraceMask
```

⚠️ Warning: The default value for the trace masks is 0x03. 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.
CTI OS FAQs

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), which is a Windows NT or Windows 2000 system. 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 B-1):

- CTI OS Server
- CTI OS Agent Desktop
- CTI OS Supervisor Desktop for IPCC Enterprise (only on Cisco IPCC Enterprise)
The CTI OS Server connects to the CTI Server via TCP/IP. Depending on call and agent load (see product specification), CTI OS Server can reside on the same physical machine as the CTI Server, or on a separate box. The CTI OS server consists of two executables:

- CtiServerDriver.exe
- CtiosServerNode.exe

CtiServerDriver handles the connection to the CTI Server. 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). CTI OSServerNode handles CTI OS client connections (such as the connection to the Agent Desktop) over TCP/IP. CTI OSServerNode and CtiServerDriver are "nodemanaged" components (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 (e.g., agents, calls, skillgroups, ...) and exposes these objects and selected event messages to CTI OS clients. It also abstracts all switch specific behavior for clients, exposing the same interfaces to CTI OS clients for all supported switches.
The CTI OS Agent Desktop and CTI OS Supervisor Desktop for IPCC Enterprise run on desktop computers and provide a user interface to CTI OS for Agents and Supervisors. The user interface includes a softphone for agent state 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 OS Agent Desktop and CTI OS Supervisor Desktop for IPCC Enterprise are built upon the Client Interface Library (CIL). Developers can write custom applications using the published interfaces of CIL. At this time the CIL is available in C++, COM (called CTIOSClient), 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 OS client application (e.g., 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 application 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 (not recommended).

**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 B-1 shows switches and their corresponding PeripheralTypes that are supported in CTI OS Release 6.0.
**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 in to. 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\<CTIOSInstanceName>\<CTIOServerName>\EnterpriseDesktopSettings\All Desktops\Login\ConnectionProfiles\Name.

When the CTI OS Server is first installed, the Setup program creates a default Connection Profile called "Main Contact Center" 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?

---

**Table B-1  Supported Switches and Peripheral Type Values**

<table>
<thead>
<tr>
<th>Peripheral Vendor (Name)</th>
<th>Peripheral Type Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IPCC</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>
A. When the softphone starts up, the following steps are executed:

1. The softphone 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 CTI OSA and CTI OSB and are located at `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\CTI Desktop\CTI OS`.
3. The Softphone 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\<CTIOSInstanceName>\<CTIOSServerName>\EnterpriseDesktopSettings`.
5. The softphone 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.
When the client receives a QueryAgentStateConf it reads the current agent state. If the current agent state indicates that the agent is logged out, the client sends a SetAgentStateRequest to login.

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.

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\<CTIOSInstanceName>\<CTIOSServerName>\Server\Agent\PollingIntervalSec
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\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 should 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\ <CTIOSInstanceName>\<CTIOServerName>\ EnterpriseDesktopSettings\AllDesktops\Grid\AgentStatistics\ Columns\Number for agent statistics
```

and

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS\ <CTIOSInstanceName>\<CTIOServerName>\ 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 (e.g. 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 *Cisco ICM Software CTI OS System Manager's Guide*, Chapter 4. A column key can have Header and Width string values (plus other values as explained in the *Cisco ICM Software CTI OS System Manager's Guide*).

- **Header:** enter custom header; same as "Type" by default
- **Width:** 70 screen units by default (e.g. 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\<CTIOSInstanceName>\<CTIOSServerName>\Server\Agent\PollingIntervalSec

  - For Skillgroup Statistics:
    
    HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\CTIOS\<CTIOSInstanceName>\<CTIOSServerName>\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 \<CTIOSInstanceName>\<CTIOServerName>\Server\SkillGroup, the client will see skillgroup statistics refresh every 30 seconds.

For Agentstatistics, however, it is recommended to use the default behavior described in 6) below, which ignores PollingIntervalSec at HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTIOS \<CTIOSInstanceName>\<CTIOServerName>\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 OS client. The procedure to customize which fields are displayed on the client is explained in the Cisco ICM Software CTI OS System Manager’s Guide 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 \ <CTIOSInstanceName>\ <CTIOSServerName> \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 \ <CTIOSInstanceName>\ <CTIOSServerName> \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 A, “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 0x7 for both Clients and CTI OS Server is sufficient for high level issues. A TraceMask of 0xA0f is recommended for detailed troubleshooting.
INDEX

C
Chat problems 1-20
Configuration server 2-1
Connection profile 2-2, B-4
CtiDriver
  connection problems 1-2
CTI OS architecture B-1
CTI OS Client
  logs A-3
CTI OS Server 1-1
  connection problems 1-1
  logs A-2

E
Emergency assist problems 1-19

F
Failover problems 1-17

I
IPCC Supervisor problems 1-21

button 1-21
real time status window 1-22

M
Media Termination 2-6
Media Termination problems 1-23
  login 1-24
  sound 1-24
Multiple peripherals 1-3

P
PeripheralType
  list of supported B-4

S
Softphone problems
  behavior 1-9
  button 1-8
  ECC variables 1-16
  login 1-4
  logout 1-7
  making calls 1-10
Index

problems after call ends 1-13
receiving calls 1-11
startup 1-4
statistics problems 1-15
talking on a call 1-11
Supervisor assist problems 1-19

Trace levels
CTI OS Client A-4
CTI OS Server A-3