# Cisco CAD Troubleshooting Guide

Cisco Unified Contact Center Enterprise and Hosted Release 8.0
revised March 2011

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

*Cisco CAD Troubleshooting Guide*

# Contents

# Contents

# Contents

# Contents

# Introduction

# 1

## CAD Documentation

The following documents contain additional information about CAD 8.0.

- *Cisco Agent Desktop User Guide*
- *Cisco Agent Desktop—Browser Edition User Guide*
- *Cisco Supervisor Desktop User Guide*
- *Cisco IP Phone Agent User Guide*
- *Cisco Desktop Administrator User Guide*
- *Cisco CAD Installation Guide*
- *Configuring and Troubleshooting VoIP Monitoring*
- *Mobile Agent Guide for Cisco Unified CC Enterprise*
- *Integrating CAD with Thin Client Environments*
- *Cisco CAD Error Code Dictionary*

## CAD 8.0 Applications

CAD 8.0 includes the following components:

### User Applications

- Cisco Desktop Administrator (Desktop Administrator)
- Cisco Supervisor Desktop (Supervisor Desktop)
- Cisco Agent Desktop (Agent Desktop)
- Cisco Agent Desktop—Browser Edition (CAD-BE)
- Cisco IP Phone Agent (IP Phone Agent)
- Cisco Desktop Monitoring Console

### Services

- Cisco Chat Service (Chat service)
- Directory Services
- Cisco Enterprise Service (Enterprise service)
- Cisco Browser and IP Phone Agent Service (BIPPA service)
- Cisco LDAP Monitor Service (LDAP Monitor service)
- Cisco Licensing and Resource Manager Service (LRM service)
- Cisco Recording & Playback Service (Recording & Playback service)
- Cisco Recording and Statistics Service (Recording and Statistics service)
- Cisco Sync Service (Sync service)
- Cisco VoIP Monitor Service (VoIP Monitor service)

For more information about CAD Enterprise user applications and services, see the *Cisco CAD Installation Guide*.

## Version Information

All CAD applications include version information. This can be obtained by:

- Checking the About dialog box (choosing Help > About on desktop application menu bars or the Help button on the toolbar)
- Right-clicking the application executable and selecting Properties from the resulting menu
- Opening *.jar and *.war files with WinZip and locating the Manifest.mf file, which contains version information

Version information is a series of four numbers separated by periods (for example, 8.0.1.10). From left to right, these represent:

- The major feature version number
- The minor feature version number
- The service level (maintenance) number
- The build number

# Capacity and Performance Guidelines

# 2

## Service Autorecovery

### Fault Tolerance

CAD 8.0 uses the “warm standby” approach to fault tolerance and autorecovery. No manual intervention is required to recover a failed service.

Data and features might be lost at the time of the failure. For instance:

- Active monitoring and recording is stopped. They can be restarted manually after the failover.
- Enterprise data for the call in progress is lost at the time of the failure.

All CAD features are fault-tolerant to a single point of failure with several exceptions. They are:

- Playback. Recordings are tied to a specific service, and thus are not replicated.
- SPAN-based monitoring and recording. If fault tolerance is required, desktop monitoring can be used for agents who use Agent Desktop only. Desktop monitoring is not supported for agents who use IP Phone Agent or CAD-BE.

CAD uses LDAP replication to provide fault tolerance for configuration information, such as work flows, agent hot seat settings, and so on. It uses SQL Server merge replication to provide fault tolerance for Recording and Statistics service-related data, such as call logs, agent state logs, recording logs, and so on.

> **NOTE:** CAD uses flat files by default to store Recording and Statistics service-related data. Use of SQL Server is optional. Flat files do provide replication, but it might not be complete. For reliable replication of this information, SQL Server must be used.

A subset of the base services fail over together. These services will either all be active or all be inactive on the same box:

- BIPPA service
- Chat service
- Enterprise service
- LRM service
- Recording and Statistics service

The LRM service controls the failover logic for this subset. Two failures of the same service within five minutes causes failover of the subset. One LRM failure causes failover of the subset.

## Agent Desktop, Supervisor Desktop, and CAD-BE

The service autorecovery feature enables Agent Desktop, Supervisor Desktop, and CAD-BE to automatically recover their connections to the CAD services in the case of a service restart or a network outage.

When Agent Desktop, Supervisor Desktop, or CAD-BE detects that it is unable to communicate with a service (generally within one minute of the service failure), the application status bar displays “Partial Service” or “No Service” to indicate some or all of the services have failed.

When Agent Desktop, Supervisor Desktop, or CAD-BE detects that the service is again available (usually within one minute of service recovery), the status bar displays “In Service” to indicate the services have recovered.

To learn more about what is affected by the service failure, double-click the status message on the status bar. The application displays a popup box that lists the application features and indicates if that feature is available or not due to the service outage.

## CAD-BE

CAD-BE displays a dialog box when a service goes down or comes back up. If the BIPPA service is down, all ACD, call control, task, and workflow capabilities are disabled. CAD-BE attempts to reconnect to the service. If it is unable to do so and there is a redundant BIPPA service, it automatically attempts to connect to the redundant BIPPA service.

If CAD-BE is unable to connect to the BIPPA service specified by the URL during the initial login attempt, it does not attempt to reconnect or failover to the redundant BIPPA service. The agent must use the URL that points to the redundant BIPPA service.

If the CTI service is down, ACD and call control capabilities are disabled.

## BIPPA Service

The BIPPA service pushes an error screen to all of the agents logged into IP Phone Agent when it detects a failover in Unified Intelligent Contact Management (Unified ICM). During the time the BIPPA service is unable to communicate with Unified ICM, any attempt to change agent state or perform other IP Phone Agent functionality returns the service error screen.

If the BIPPA service goes down and there is a redundant BIPPA service, agents must select the redundant service on the IP phone list of services.

## VoIP Monitor Service

**NOTE:** The VoIP Monitor service is not used with Unified CM-based monitoring.

VoIP Monitor service recovery is a special case, since more than one VoIP Monitor service can be installed in a single logical contact center. Supervisor Desktop is notified when one VoIP Monitor service in a multiple VoIP Monitor service configuration goes down. However, agent monitoring is not disabled because some agents may still be monitored by one of the VoIP Monitor services. The only indication a supervisor receives that a particular agent is assigned to the downed VoIP Monitor service is an error message when attempting to monitor that agent.

**NOTE:** This does not apply to desktops with desktop monitoring enabled.

# Technical Package Information

# 3

## Port Utilization

Consult the *Cisco Contact Center Product Port Utilization Guide* for a complete listing of ports and connection types used in CAD 8.0.

## Registry Entries

The following tables list the configurable registry entries used by CAD services.

**CAUTION:** Do not modify the values of any registry entries that are not listed in the tables in this chapter. Changing the values of undocumented registry entries might cause data loss and negatively impact product functionality.

### Site Setup

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Site Setup\

**Table 1. Site setup registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Site Setup | APP VERSION | string | Used by installation scripts to identify the version of the service software. The service itself does not use this entry. |
| | CALLCENTERLANG | string | The language selected during installation |
| | INSTALL DIRECTORY | string | Base install directory for Cisco software. |
| | INSTALLDIR | string | Only for use by install program. Customer should never change. |
| | IOR HOSTNAME | string | Hostname or IP address of the computer's public NIC. Value present only on the CAD services computer. |
| | LDAP Bind DN | string | User ID used to log into the LDAP service. Default = cn=Client, ou=People, o=Spanlink Communications. |
| | LDAP Connection Timeout | dword | Maximum time, in seconds, before a connection attempt times out. Default = 15. |
| | LDAP Heartbeat Enabled | dword | Is heartbeat enabled? 1 = yes, 0 = no. Default = 1. |
| | LDAP Heartbeat Retry Time | dword | Heartbeat time, in milliseconds. Default = 10000. |

Table 1. Site setup registry entries (cont'd)

| Key | Value | Type | Description |
|---|---|---|---|
| Site Setup (cont'd) | LDAP Host 1 | string | LDAP service hostname/IP address. There can be multiple LDAP hosts. |
| | LDAP LCC | string | Default logical contact center. Default = Call Center 1. |
| | LDAP Port 1 | dword | LDAP service port. There can be multiple LDAP ports. Default = 38983. |
| | LDAP Pwd | string | Encrypted user password. |
| | LDAP Recovery Retry Time | dword | Recovery retry time, in milliseconds. Default = 3000. |
| | LDAP Request Timeout | dword | Maximum time, in seconds, before an LDAP request times out. Default = 15. |
| | LDAP Root | string | Root of the LDAP data. Default = o=Spanlink Communications. |
| | MONITOR DEVICE | string | Network card on which to sniff packets. |
| | ProductCode_Admin | string | Only for use by install program. Customer should never change. |
| | ProductCode_Server | string | Only for use by install program. Customer should never change. |
| | ProductCode_Supervisor | string | Only for use by install program. Customer should never change. |
| | Serial Number | dword | Counter to indicate changes to Site Setup values. Default = 0. |
| | WorkflowEngineClassPath | string | Cannot find any information about this key. DE believes it is deprecated. |

## BIPPA Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\IPPA\

Table 2. BIPPA registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| Config | TOMCAT HOME | string | Location of the Tomcat webserver files. Default = C:\Program Files\Cisco\Desktop\Tomcat\. |

## Recording & Playback Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Recording & Playback Client\

Table 3. Recording & Playback registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| setup | From Client Port | dword | The port on the supervisor's desktop that is used to receive the "From Agent" audio stream for playback sessions. |
| | Jitter Buffer | dword | The amount of voice data to buffer before playing. Default value = 700 ms. On a typical internal network, this value can be set as low as 50 ms. The default is set higher so that the sound quality is good even on a congested network. |
| | Port Range End | dword | |
| | Port Range Start | dword | |
| | Sound Buffers | dword | Number of buffers used to hold audio data sent to the sound card. Default is 30. If sound quality is bad, increasing this number may improve the quality. |
| | To Client Port | dword | The port on the supervisor's desktop that is used to receive the "To Agent" audio stream for playback sessions. |
| | VPN Port | dword | The port used by the Recording & Playback service for its VPN address service that client applications used to determine their visible IP address used by other clients and services. Do not change this entry unless you change the corresponding entry for the Recording & Playback service. |

## Recording & Playback Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Recording and Playback Server\

**Table 4. Recording & Playback service registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| config | Audio Directory | string | The full path to the directory that will hold the audio files of recorded calls. Change this value only if the default directory cannot be used. |
| setup | IOR HostName | string | The client-visible IP address of this machine, used by the service to construct its connection string that is used by the clients. |
| | Maximum Playbacks | dword | Maximum number of simultaneous outstanding playback requests. |
| | Maximum Recordings | dword | Maximum number of simultaneous outstanding recording requests. |
| | OmniOrbUsePort | dword | The CORBA port on which the Recording & Playback service listens for client requests. |
| | VPN Port | dword | The port on which the Recording & Playback service listens for requests from clients for their visible IP address. If you change this entry, you must also change the corresponding entry for all of the client applications. |

## Recording and Statistics Service

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\RASCAL Server\

Table 5. Recording and Statistics service registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| config | DB Admin Account | string | Account that the SQL Server CADSQL instance runs under. |
| | DB Admin Created | dword | A value that indicates if the installation created the DB Admin Account. |
| | DB Admin Group | string | The group that the DB Admin Account belongs to. |
| | DB SCRIPT MESSAGE | string | Error message used by technical support for troubleshooting. |
| | DB SCRIPT RESULT | string | Error message used by technical support for troubleshooting. |
| | RASCAL Service Account | string | The account that the Recording and Statistics service runs under. |
| | Replication Enabled | dword | A value indicating whether replication has been established. |
| | Replication Publisher | string | The name of one of the computers participating in replication. |
| | Replication Script Message | string | Error message used by technical support for troubleshooting. |
| | Replication Script Result | string | Error message used by technical support for troubleshooting. |
| | Replication Subscriber | string | The name of one of the computers participating in replication. |

## VoIP Monitor Client

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\VoIP Monitor Client\

Table 6. VoIP Monitor client registry entries

| Key | Value | Type | Description |
|---|---|---|---|
| config | FROM AGENT PORT | dword | IP port for RTP stream being sent from IP agent. Default value = 59012. Port must be an even number. The next port is reserved for RTCP stream. |
| | JITTER BUFFER | dword | The amount of voice data to buffer before playing. Default value = 400 ms. On a typical internal network this value can be set as low as 50 ms. The default is set higher so the sound quality is good even on a congested network. |
| | SERVER HOST | string | Hostname of the VoIP Monitor service. |
| | SOUND BUFFERS | dword | Number of sound card buffers. Default = 30; minimum is 3. If the monitor sound quality is choppy, stuttering, or like a motorboat you may be able to make it sound better by adjusting this value higher. Setting the value higher increases the sound lag, and may cause a slight stutter at the beginning of a monitor session. |
| | TO AGENT PORT | dword | IP port for RTP stream being sent to agent IP Phone. Default value = 59010. The port must be an even number. The next port is reserved for RTCP stream. |

## VoIP Monitor Client (Optional)

These registry entries should not be needed because the VoIP Monitor recording API has built-in defaults. They can be used to override the defaults.

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\VoIP Monitor Client

**Table 7. VOIP Monitor client registry entries**

| Key | Value | Type | Description |
|---|---|---|---|
| Setup | Recording Jitter Buffer | dword | The number of milliseconds that a packet expires for recording. |
| | Recording Port Range Start | dword | The starting port number for receiving UDP packets for recording. |
| | Recording Port Range End | dword | The end port number for receiving UDP packets for recording. |

# Configuration Files, Logs, and Debugging

# 4

## Introduction

CAD events and errors are recorded in log files. CAD services and desktop applications can be configured by modifying the appropriate configuration file.

This chapter contains information about the following topics.

## Event, Error, and Chat Logs

Logs are listings of CAD events, errors, and chat messages. Event, error, and chat message logging is always enabled.

Events may represent the following:

- Actions taken by a Desktop application
- Implications of user-defined configuration settings
- Limitations of the hardware

Error codes are brief descriptions of system events.

The CAD Chat client logs all agent-to-agent, agent-to-supervisor and agent-to-SME chat messages. One file is created for each day of the week. Logs are saved in the folder C:\Program Files\Cisco\Desktop\log\transcripts on the client computer for one week. To view a log, you must log onto the client computer.

Event and error log files are limited to a default of 3 MB. (You can change the limit in the application's configuration file. When a log file reaches that size, it is closed and a new file is started. Event and error log files are numbered, up to the total number of files set in the configuration file (the default number is 2). For example:

- agent0001.log
- agent0002.log

When agent0001.log reaches its size limit, it is closed and agent0002.log is created. When the total number of log files have been created, the first log file is overwritten.

Table 8 lists the event, error, and chat message logs generated by CAD.

**Table 8. CAD event, error, and chat message logs**

| Service/Application | Log Name |
|---|---|
| Agent Desktop | agent.log |
| Backup and Restore utility | CDBRTool.log |
| BIPPA service | IPPASvr.log |
| BIPPA service JSP client | IPPAClient.log |
| CAD Configuration Setup | PostInstall.log |
| CAD uninstall process | fcuninstall.log |
| CAD-BE | CadBE.log |

Table 8. CAD event, error, and chat message logs (cont'd)

| Service/Application | Log Name |
|---|---|
| Chat client | monday.txt, tuesday.txt, wednesday.txt, thursday.txt, friday.txt, saturday.txt, sunday.txt |
| Chat service | FCCServer.log |
| Desktop Administrator: Desktop Configuration | administrator.log |
| Desktop Administrator: Enterprise Data Configuration | TSSPAdm.log |
| Desktop Administrator: framework | Splkview.log |
| Desktop Administrator: Unified CCE Configuration | IPCCAdm.log |
| Desktop Administrator: Personnel Configuration | personnel.log |
| Desktop Monitoring Console | SMC.log, SMCGetServerList.log |
| Directory Services | slapd.log |
| Directory Services Replication | slurpd.log |
| Enterprise service | CTIStorageServer.log, WorkflowEngine.log |
| LDAP Monitor service | LDAPMonSvr.log |
| License Administrator | LicensingAdmin.log |
| LRM service | LRMServer.log |
| Recording & Playback service | RPServer.log |

Table 8. CAD event, error, and chat message logs (cont'd)

| Service/Application | Log Name |
|---|---|
| Recording and Statistics service | • FCRasSvr.log<br>• db.cra_repl_ads.pub.sql.log<br>• db.cra_repl_ads.sql.log<br>• db.cra_repl_ads.sub.sql.log<br>• db.cra_repl_base.fcrassvr.pub.sql.log<br>• db.cra_repl_base.fcrassvr.sql.log<br>• db.cra_repl_base.fcrassvr.sub.sql.log<br>• db.cra_utils_base.fcrassvr.pub.sql.log<br>• db.cra_utils_base.fcrassvr.sql.log<br>• db.cra_utils_base.fcrassvr.sub.sql.log<br>• db.instrasdb.fcrassvr.pub.sql.log<br>• db.instrasdb.fcrassvr.sql.log<br>• db.instrasdb.fcrassvr.sub.sql.log<br>• db.repl_base.pub.sql.log<br>• db.repl_base.sql.log<br>• db.repl_base.sub.sql.log<br>• db.sp_make_ publisher.fcrassvr.pub.sql.log<br>• db.sp_make_ publisher.fcrassvr.sub.sql.log<br>• db.sp_splk_drop_ publisher.fcrassvr.pub.sql.log<br>• db.sp_splk_drop_ publisher.fcrassvr.sub.sql.log<br>• db.sql.log<br>• db.truncate.fcrassvr.pub.sql.log<br>• db.truncate.fcrassvr.sub.sql.log<br><br>**NOTE:** The db.*.log files exist only in systems that use SQL Server. |
| Supervisor Desktop, Supervisor Record Viewer | supervisor.log |
| Supervisor Workflow Administrator | SWFAdmin.log |
| Sync service | DirAccessSynSvr.log |
| VoIP Monitor service | FCVoIPMonSvr.log |

## Configuration Files

Table 9 lists the configuration files used by CAD services and applications. For instructions about how to modify one of these configuration files to enable debugging, see "Debugging Logs" on page 31.

**Table 9. CAD configuration files**

| Application/Service | Configuration File |
|---|---|
| Agent Desktop | agent.cfg |
| Backup and Restore utility | CDBRTool.cfg |
| BIPPA service | IPPASvr.cfg |
| CAD Configuration Setup | PostInstall.cfg |
| CAD-BE | CadBE.properties |
| Chat service | FCCServer.cfg |
| Desktop Administrator<br>• Framework<br>• Enterprise Data Configuration<br>• Unified SCC Configuration<br>• Personnel Configuration | admin.cfg<br>• SplkView.cfg<br>• TSSPAdm.cfg<br>• IPCCAdm.cfg<br>• personnel.cfg |
| Desktop Monitoring Console | smc.cfg |
| Desktop Presence Administrator | WebAdmin.properties, WebAdminLib.cfg |
| Directory Services | slapd.cfg |
| Directory Services Replication | slurpd.cfg |
| Enterprise service | CTIStorageServer.cfg |
| IP Phone Agent client | IPPAClient.properties |
| LDAP Monitor service | LDAPMonSvr.cfg |
| Licensing Administrator | LicensingAdmin.cfg |
| LRM service | LRMServer.cfg |
| Recording & Playback service | RPServer.cfg |
| Recording and Statistics service | FCRasSvr.cfg |
| Supervisor Desktop | supervisor.cfg |
| Supervisor Record Viewer | supervisorlogviewer.cfg |

Table 9. CAD configuration files (cont'd)

| Application/Service | Configuration File |
|---|---|
| Supervisor Workflow Administrator | SWFAdmin.cfg |
| Sync service | DirAccessSynSvr.cfg |
| VoIP Monitor service | FCVoIPMonSvr.cfg |

## Configuring the Recording and Statistics Service

You can choose to include or exclude outbound calls in call totals that are displayed in agent call logs and statistics reports. The default behavior is for outbound calls to be excluded from the total number of calls presented and handled. You can change this behavior so that outbound calls are included in the total number of calls presented and handled. Table 10 summarizes the default and configured behavior settings.

Table 10. Outbound call statistic handling

| Total | Outbound Calls | |
|---|---|---|
| | Default behavior | Configured behavior |
| Calls Presented | Not counted | Counted |
| Calls Handled | Not counted | Counted if answered |

***To include outbound calls in totals:***

1. On the server that hosts the Recording and Statistics service, navigate to C:\Program Files\Cisco\Desktop\config.
2. Open FCRasSvr.cfg.
3. Add the following lines to the configuration file:

   ```
   [ReportParameters]
   CallReportIncludesOutbound=1
   ```

4. Save the configuration file with the new setting. The new setting will go into effect when you restart the Recording and Statistics service.

   **NOTE:** In a High Availability configuration, perform this procedure on both servers.

# Debugging Logs

CAD can create debugging logs, although by default this capability is disabled. If you want debugging turned on, you must edit the appropriate configuration file.

Debugging information is written to the various debug files, all of which have a *.dbg suffix. These files are located in the ...\Cisco\Desktop\log directory.

> **NOTE:** If you want to read a debugging log generated by CAD-BE on a computer running Linux, and you are using a computer running Windows, open the debugging log with Microsoft Wordpad.

The debug files are numbered, up to the total number of files set in the configuration file (the default number is 2). For example:

- agent0001.dbg
- agent0002.dbg

When agent0001.dbg reaches its size limit, it is closed and agent0002.dbg is created. When the total number of debug files have been created, the first debug file is overwritten.

## Turning on Debugging

To enable debugging for CAD-BE, you must download and edit the configuration file on the computer on which CAD-BE will be run. For instructions, see the following sections.

- Downloading the CadBE.properties File (page 32)
- Enabling Debugging for Java Applications (page 33)

To enable debugging for all other CAD services and applications, you must edit the appropriate configuration file on the computer on which the CAD services are installed. For instructions, see the section that corresponds to the service or application that you are configuring.

- For IP Phone Agent, see "Enabling Debugging for Java Applications" on page 33.
- For Desktop Monitoring Console, see "Enabling Debugging for Desktop Monitoring Console" on page 34.
- For Desktop Administrator, you must edit two configuration files. For WebAdmin.properties, see "Enabling Debugging for Java Applications" on page 33. For WebAdminLib.cfg, see "Enabling Debugging for non-Java Applications" on page 34.
- For all other CAD services and applications, see "Enabling Debugging for non-Java Applications" on page 34.

For a complete list of services/applications and their corresponding configuration files, see Table 9 on page 29.

## Downloading the CadBE.properties File

***To download the CadBE.properties file:***

1. Open your web browser and access the following URL, where <CAD server> is the IP address of the server on which the CAD services are installed. The Agent Desktop/Supervisor Desktop/CAD-BE Installation web page appears.

   http://<CAD server>:8088/TUP/CAD/Install.htm

2. Right-click the hyperlink labeled CAD-BE logging and debugging file and save it to your computer. Table 11 gives the location in which the CadBE.properties file should be saved and any additional actions that need to be completed, depending on the operating system and browser you are using.

**Table 11. Properties file location and additional actions**

| Operating System | Browser | Location of properties file/additional actions |
|---|---|---|
| Windows Vista | Internet Explorer | Save the properties file to the desktop. In addition, add the CAD-BE server hostname or IP address to the Internet Explorer list of trusted sites. |
| Windows Vista | Mozilla Firefox | Save the properties file to the desktop. In addition, change the Mozilla Firefox “Start In” directory to the desktop. |
| Windows XP | Internet Explorer | Save the properties file to the desktop. |
| Windows XP | Mozilla Firefox | Save the properties file to the folder in which Mozilla Firefox is installed. The default is C:\Program Files\Mozilla Firefox. |
| Linux | Mozilla Firefox | Save the properties file to your home directory. |

### Debugging Thresholds

When setting the debugging threshold, keep in mind that the more detail the threshold provides, the slower the performance of your PC and increases the size of the debug file. Table 12 lists the debugging thresholds that are available for all services except Desktop Monitoring Console.

**Table 12. Debugging Thresholds**

| Threshold | Events Recorded |
|---|---|
| Debug | • Minor and frequently-occurring normal events. This level is usually sufficient for debugging a problem, and will not affect the computer's performance. |
| Call | • Minor and frequently-occurring normal events<br>• Entering and exiting functions |
| Trace | • Minor and frequently-occurring normal events<br>• Entering and exiting functions<br>• Detail debugging (for instance, loops) |
| Dump | • Minor and frequently-occurring normal events<br>• Entering and exiting functions<br>• Detail debugging (for instance, loops)<br>• Byte dumps |
| Off | Turns off debugging. This is the default setting. |

### Enabling Debugging for Java Applications

***To enable debugging for Java applications:***

1. Navigate to the appropriate folder.
   - For CAD-BE, navigate to the folder specified in Table 11 on page 32.
   - For all other Java applications, on the server on which the CAD services are installed, navigate to C:\Program Files\Cisco\Desktop\tomcat\conf.
2. Open the properties file. The configuration file contains one or more of the following debugging statements at the beginning of the file.

```
#log4j.rootLogger=INFO,LOG,DBG
log4j.rootLogger=DEBUG,LOG,DBG
#log4j.rootLogger=CALL#com.spanlink.util.log.SplkLevel,LOG,DBG
#log4j.rootLogger=TRACE,LOG,DBG
#log4j.rootLogger=DUMP#com.spanlink.util.log.SplkLevel,LOG,DBG
```

3. Add the '#' character to the beginning of the existing debugging threshold statement. Then either add a new debugging threshold statement or remove the '#' character at the beginning of the desired debugging threshold statement if it already exists.

   For example, to select the Call debugging threshold, add '#' to the existing debugging threshold statement. Then either add the third statement or remove '#' from the beginning of the third statement if it already exists.

   ```
   #log4j.rootLogger=INFO,LOG,DBG
   #log4j.rootLogger=DEBUG,LOG,DBG
   log4j.rootLogger=CALL#com.spanlink.util.log.SplkLevel,LOG,DBG
   #log4j.rootLogger=TRACE,LOG,DBG
   #log4j.rootLogger=DUMP#com.spanlink.util.log.SplkLevel,LOG,DBG
   ```

4. Save the configuration file with the new setting. You must restart the application to make the new setting take effect.

### Enabling Debugging for non-Java Applications

***To enable debugging for non-Java applications:***

1. On the server on which the CAD services are installed, navigate to C:\Program Files\Cisco\Desktop\config.
2. Open the appropriate configuration file.
3. Under the section headed [Debug Log], set the debugging threshold to an appropriate value. For more information, see "Debugging Thresholds" on page 33. For example:

   ```
   Threshold=DEBUG
   ```

4. Save the configuration file with the new setting. You must restart the application to make the new setting take effect.

### Enabling Debugging for Desktop Monitoring Console

***To enable debugging for Desktop Monitoring Console:***

1. On the server on which the CAD services are installed, navigate to C:\Program Files\Cisco\Desktop\Tomcat\conf.
2. Open smc.cfg.
3. Locate the following line, where <threshold> is one of the debugging levels listed in the following table.

   ```
   log4j.rootLogger=<threshold> …
   ```

| Option | Messages Recorded |
|---|---|
| DEBUG | Debug messages. |

| Option | Messages Recorded |
|---|---|
| INFO | Debug and informational messages |
| WARN | Debug, informational, and warning messages. |
| ERROR | Debug, informational, warning, and error messages |
| FATAL | Debug, informational, warning, error, and fatal messages |
| ALL | All messages. |
| OFF | Debugging is turned off. |

4. Replace <threshold> with one of the debugging levels listed below.
5. Save the configuration file with the new setting. You must restart the application to make the new setting take effect.

# Troubleshooting

# 5

## Services

### Restarting Services

If you have to stop the services, you can restart them in any order.

### Service Names/Executables

If you need to check if a service is running, use the following table to match what is shown in the Services window (accessed through the Windows Control Panel) with a particular executable.

Table 13. Service names and executables

| Service Name | Executable |
|---|---|
| Cisco Browser and IP Phone Agent Service | IPPASvr.exe |
| Cisco Chat Service | FCCServer.exe |
| Cisco Enterprise Service | CTIStorageServer.exe |
| Cisco LDAP Monitor Service | LDAPmonSvr.exe, slapd.exe, slurpd.exe |
| Cisco Licensing and Resource Manager Service | LRMServer.exe |
| Cisco Recording & Playback service | RPServer.exe |
| Cisco Recording and Statistics Service | FCRasSvr.exe |
| Cisco Sync Service | DirAccessSynSvr.exe |
| Cisco VoIP Monitor Service | FCVoIPMonSvr.exe |
| Cisco Tomcat Service | tomcat5.exe |

# Converting Recordings From *.raw to *.wav Format

Recordings made by supervisors are archived as raw voice data packets; they can only be reviewed using the Supervisor Record Viewer. However, if you wish to permanently save selected recordings as .wav files, you can use either of two methods:

- Using the "Play and Save" button in Supervisor Record Viewer and saving the recording to a selected folder
- Using the raw2wav.exe command line utility

See the *Cisco Supervisor Desktop User Guide* for information on saving recordings as .wav files through Supervisor Record Viewer.

## Using the raw2wav Utility

This utility is located in the C:\Program Files\Cisco\Desktop\bin folder. It must be run from this location in a command window on the computer that hosts the Recording & Playback service (RPServer.exe).

Each *.raw format recording is comprised of two files:

- <name>.to.raw, containing data sent to the agent phone
- <name>.from.raw, containing data sent from the agent phone

You need use only one of the file pair when running the utility. The utility finds the other file and combines the two files into one .wav file named <name>.wav.

The naming convention used for <name> is as follows:

<YYYYMMDD>_<HHMMSS>_<counter>_<extension>_<agent ID>

where:

| | |
|---|---|
| <YYYYMMDD> | Date the file was recorded |
| <HHMMSS> | Time the file was recorded |
| <counter> | Counter that is reset every time the agent logs in. It is incremented sequentially starting from 00000 every time a recording of that agent is made during that session. |
| <extension> | The extension of the agent recorded |
| <agent ID> | The ID of the agent recorded |

The utility finds the location of the *.raw files from the registry. If the registry does not have this information, the utility assumes that the location is the folder C:\Program Files\Cisco\Desktop_Audio. The utility writes the converted *.wav files to a folder it creates located at C:\Program Files\Cisco\Desktop_wav.

The utility syntax is:

raw2wav.exe <filename>

where <filename> is either the <name>.to.raw or <name>.from.raw file.

## Running raw2wav in a Batch File

You can use the raw2wav utility from a batch file that iterates through a wildcard-specified set of source files.

If the utility finds a *.wav file with a name identical to one that is about to be created, the conversion is not executed.

**NOTE:** If the utility is halted prematurely, the *.wav file being written at that time might be corrupted.

A batch file is a text file with a *.bat extension. You can put DOS commands into this file and then run the file as if it were an executable.

For example, the following series of DOS commands can be put into a batch file called convert.bat:

```
c:\
cd c:\program files\cisco\desktop\bin
for %%c in (..\..\desktop_audio\*.raw) do raw2wav "%%~nc%%~xc"
```

These DOS commands cause all the *.raw files in the folder C:\Program Files\Cisco\Desktop_audio to be converted to *.wav format and placed in the folder C:\Program Files\Cisco\Desktop_wav, leaving the original *.raw files in the Desktop_audio folder.

Additional lines can be added to the batch file to copy the files to another folder or file server.

**NOTE:** The utility has a feature that prevents it from reconverting files that are already present in the Desktop_wav directory, so the batch file does not have to explicitly check to see if the files have already been converted.

If you want the batch file to run automatically on specific days at a specific time, the Windows “at” command can be used.

For example, if you want convert.bat to run automatically every 13th and 23rd day of the month at 1:46 pm, do the following:

1. Put convert.bat in the C:\Program Files\Cisco\Desktop\bin folder.
2. Open a command window and enter the following DOS command:

```
at 1:46p /every:13,23 cmd /c "c:\program
files\cisco\desktop\bin\convert.bat" ^> c:\splkconvert.txt
```

## ShowLicenseUsage Utility

**NOTE:** This utility has not been tested thoroughly; it is provided on an as-is basis only

The ShowLicenseUsage utility can be run to view the IP addresses of clients that are consuming desktop seats or are running Cisco Desktop Administrator or Cisco Workflow Administrator.

For IP Phone Agent and CAD–BE seats, the IP address is the IP address of the active Browser and IP Phone Agent (BIPPA) service. For web-based Cisco Desktop Administrator, the IP address is the IP address of the CAD server.

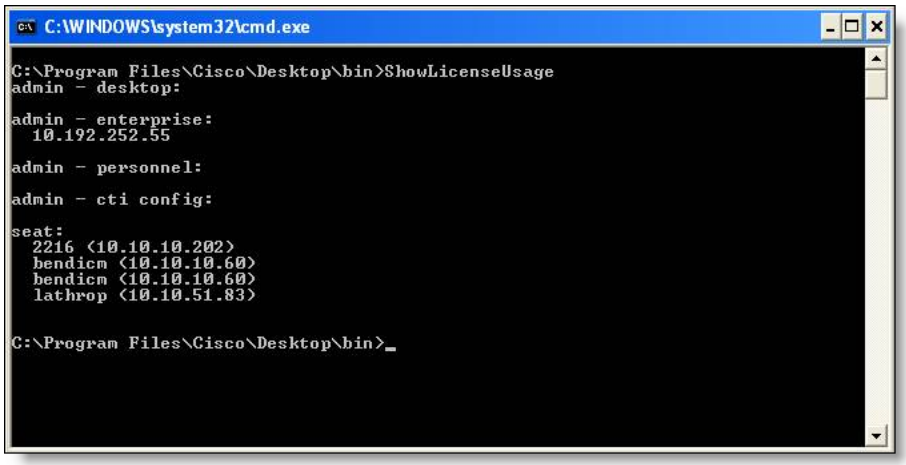
**NOTE:** An IP address that listed twice reflects a user who is running both Supervisor Desktop and Agent Desktop. In terms of concurrent licensing, this user counts for only one session.

ShowLicenseUsage.exe is run from the C:\Program Files\Cisco\Desktop\bin folder on the CAD server.

***To use the ShowLicenseUsage utility:***

1. On the server hosting the CAD services, navigate to the C:\Program Files\Cisco\Desktop\bin folder.
2. Double-click ShowLicenseUsage.exe to run the utility. A command window opens and displays the results (Figure 1).

**Figure 1. ShowLicenseUsage utility results**



Entries in the command window are described in Table 14.

**Table 14. ShowLicenseUsage result headings**

| Result Heading | Description |
|---|---|
| admin - desktop | Not used in this version. |
| admin - enterprise | Lists users of Cisco Work Flow Administrator and Cisco Desktop Administrator. |
| admin - personnel | Not used in this version. |
| admin - cti config | Not used in this version. |
| seat | Lists users of Cisco Agent Desktop, Cisco Agent Desktop—Browser Edition, Cisco IP Phone Agent, and Cisco Supervisor Desktop. |

# Recovering the Directory Services Database

## Corrupted Directory Services Database

If the Directory Services database becomes corrupted, complete the following steps.

***To recover the Directory Services database (Method 1):***

1. On the PC hosting the database, stop the LDAP Monitor service.
2. Open a command window and change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
3. Type the following command and press Enter.

   ```
   db_recover -h ../database -v
   ```

4. Type **exit** and press Enter to close the DOS window.
5. Restart the LDAP Monitor service.

If this procedure does not work, complete the following steps.

***To recover the Directory Services database (Method 2):***

1. On the PC hosting the database, stop the LDAP Monitor service.
2. Open a command window and change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
3. Type the following command and press Enter.

   ```
   slapcat -f slapd.conf -l backup.ldif -c
   ```

4. Rename ...Cisco\Desktop\database to ...Cisco\Desktop\old_database.
5. Create a new folder called ...Cisco\Desktop\database.
6. Copy DB_CONFIG and all files with a *.dat extension from the old_database folder to the new database folder.
7. In the database folder, create an empty file called rep.log.
8. Open a command window and change directories to ...Cisco\Desktop\bin (the drive and exact location of this directory depends on where the services were installed).
9. Type the following command and press Enter.

   ```
   slapadd -f slapd.conf -l backup.ldif -c
   ```

10. Type **exit** and press Enter to close the DOS window.
11. Restart the LDAP Monitor service.

## Out of Sync Directory Services Databases

The secondary Directory Services database can become out of sync with the primary Directory Services database. A possible reason for this to occur is that the secondary database was reinstalled.

Follow these steps to sync up the two databases:

1. On the PC hosting the primary database, stop the LDAP Monitor service.
2. Remove all contents from the files repl.log and repl.log.lock from the ...\Cisco\Desktop\database directory.
3. Delete all files in the ...\Cisco\Desktop\logs\replica directory.
4. Open a command window on the primary database computer.
5. Change directories to ...Cisco\Desktop\bin (the drive and exact location of this folder depends on where the service was installed).
6. Type the following command and press Enter. A file called backup.ldif is generated.

   ```
   slapcat -f slapd.conf -l backup.ldif -c
   ```

7. Copy the backup.ldif file to the computer on which the secondary LDAP service is installed, into the ...Cisco\Desktop\bin folder.
8. On the PC hosting the secondary database, stop the LDAP Monitor service.
9. Rename the existing folder ...Cisco\Desktop\database to ...Cisco\Desktop\old_database.
10. Create a new folder called ...Cisco\Desktop\database.
11. Copy DB_CONFIG and all files with a *.dat extension from the old_database folder to the database folder.
12. In the database folder, create an empty file called rep.log.
13. Open a command window on the secondary database computer and change directories to ...Cisco\Desktop\bin (the drive and exact location of this folder depends on where the service was installed).
14. Type the following command and press Enter.

    ```
    slapadd -f slapd.conf -l backup.ldif -c
    ```

15. Type **exit** and press Enter to close the DOS window.
16. Type **exit** and press Enter to close the DOS window.
17. Restart the LDAP Monitor service on the secondary computer.
18. Restart the LDAP Monitor service on the primary computer.

# Diagnostic Procedures

## Basic Checks

When CAD has problems, check that:

- The computers that host CAD services, Unified CM, Unified ICM, and other system components are running.
- The registry is correct (see "Registry Check" on page 45).
- The network is set up correctly (see "Network Check" on page 45).
- The CAD services are running and active (see "Active Service Check" on page 45).
- The CAD Configuration Setup utility has run correctly. See the *Cisco CAD Installation Guide* for more information.

## Active Service Check

This applies only to the following services: LRM, Chat, Enterprise, Recording and Statistics, BIPPA, and Sync.

### For Nonredundant Systems

- Check the service's log file for a statement that the service is active.

### For Redundant Systems

- Check the service's log file for a statement that the service is active.
- Only one instance of each service should be active at the same time. The other instance should be in standby mode.

## Registry Check

Using Windows Regedit:

- Verify that HKEY_LOCAL_MACHINE\Software\Spanlink\CAD\Site Setup exists and contains the entries specified in "Site Setup" on page 16.
- Verify that the registry entries used by specific services exist and are valid. See "Registry Entries" on page 16.

## Network Check

- On the CAD services computer, verify that the IP address in the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\CAD\Site Setup\IOR HOSTNAME is the correct IP address of the public NIC.

- To view information about the NICs on the computer, open a command window and type **ipconfig /all**.
- Verify that the hostname and IP address are as expected.
- Verify that the subnet mask is correct. It is probably 255.255.255.0.
- If there are multiple NICs enabled, verify that the public NIC comes before the private NIC:
  a. In the Control Panel, double-click Network and Dial-up Connections.
  b. From the menu bar, choose Advanced > Advanced Settings.
  c. On the Adapters and Bindings tab, verify that the NICs are in the correct order in the Connections pane.
- Check the network connectivity by pinging from the CAD services computer to others in the configuration, for example, the Unified CM computer. Then reverse it by pinging from the other computers to the CAD services computer. Do this using both hostnames and IP addresses and ensure that the ping results match.
- If hostnames are used, verify that the DNS, WINS, and hosts files are correct.
- If there is a problem connecting to a particular service, try typing **telnet <IP address/hostname> <port>** in a command window, where <IP address/hostname> is the IP address or hostname of the computer where the service is running and <port> is the port used by the service.
- Use a network protocol analyzer like Ethereal to analyze network communications.
- If security or firewall software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports.

## Memory Check

- Ensure that the amount of memory on the computer is at least the minimum required for CAD and other installed software. If the amount of memory is below the recommended level, it could be the source of the problem.
- Use Microsoft Perfmon (perfmon.exe) to perform most memory checking.
  — Add the following counters for _Total and process of interest:
    - Private Bytes
    - Virtual Bytes
    - Handle Count
    - Thread Count

    If the values for those counters keep growing without leveling or decreasing, it is likely the process has a memory leak.

If the values for those counters for a process are a significant part of the total memory used, it may be of concern. Note that certain processes will normally use more memory than others.

- Try rebooting the computer and see if it fixes the problem. Check how much and how fast processes increase their memory usage.

## CPU Check

- Ensure that the computer's processor is at least the minimum required for CAD and other installed software. If the processor is below the recommended level, it could be the cause of the problem.
- Use Task Manager to sort processes/applications by CPU usage. Check which process seems to be using the CPU most of the time.
- Use Windows Perfmon (perfmon.exe) for additional CPU checking.
  - Add the %Processor Time counter for Processor > _Total and each CPU as well as Process >_Total and process of interest.
  - Check which process seems to be using the CPU most of the time.
  - If the counter values for a process are a significant part of the total CPU use, it may be of concern. Short spikes are acceptable but a significant time with high CPU usage is of concern.
- Try rebooting the computer to see if it fixes the problem.

## Blocked Ports Check

To check whether a port is blocked:

- Using telnet:
  1. Ensure that the service is running and active.
  2. From the command line, type the following command and press Enter, where <hostname/IP address> is the hostname or IP address of the service computer and <port> is the port the service is listening on.

     ```
     telnet <hostname/IP address> <port>
     ```

     - If the telnet operation is successful, the command window will clear.
     - If the telnet operation fails, a connection failure message will appear.
- Check firewall settings on the client and server computers.
- Check firewall logs.
- If security software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports.

## Agent Desktop Problems

**Problem** An agent logs into Agent Desktop and can receive direct calls and change agent state, but cannot receive ACD calls.

**Solution** The agent's extension is configured in Unified CM, but is not in the Unified ICM Device Target list. Configure the extension's device target and label for full functionality.

**Problem** An agent receives an ACD call, but the route point does not show up in the call history.

**Solution** Unified ICM Configuration Manager must be configured to enable route points to appear in call history.

In Unified ICM Configuration Manager, choose Tools > List Tools > Dialed Number/Script Selector List, and on the Dialed Numbers tab, check the Permit application routing check box.

**Problem** An agent receives the error message, "Request Operation Failed." However, the agent has made no call control requests.

**Solution** This message is displayed when a supervisor is attempting to barge in or intercept an agent's call, and the attempt fails. The barge-in or intercept action is actually made on the agent's desktop, and so the agent receives the resulting error message.

The agent can ignore the error message, close the message dialog box, and continue as before.

**Problem** The CPU usage on an agent's PC has gone to 99%, and the PC has locked up.

**Solution** This can happen when you disable the sniffing adapter through the Windows Network and Dialup Connections window while Agent Desktop is running and is being monitored and/or recorded by the supervisor or

recorded by the agent, using desktop monitoring. Re-enabling the sniffer adapter while Agent Desktop is running will not solve the problem. You must stop Agent Desktop, re-enable the sniffer adapter, and then restart Agent Desktop to restore normal functionality.

**Problem** An agent using Windows XP is able to start Agent Desktop, but cannot enter an active state.

**Solution** Windows XP can be configured so that the Internet Connection Firewall (ICF) is active. ICF acts by keeping track of all traffic to and from the computer; it will only allow information through that has originated from that particular computer. If a message originates from outside the computer, it will be discarded.

To solve this problem, either turn off ICF (requires someone with administrator rights to the computer) or override the defaults to include known “good” connections like the CAD servers.

**Problem** Every time an agent hangs up the telephone, Agent Desktop disappears.

**Solution** In Normal mode, Agent Desktop automatically minimizes when there are no active calls. This behavior is configured in Desktop Administrator. To prevent the Agent Desktop window from minimizing, click the Preferences button on the toolbar and choose Always Open or Always on Top.

**Problem** The administrator has made changes in Desktop Administrator, but they are not showing up in Agent Desktop.

**Solution** Agent Desktop must be restarted in order for the changes to take effect.

**Problem** Sometimes during a conference call, a conference member shows up as <Unavailable>.

**Solution** <Unavailable> represents a party outside the switch. The switch sends the trunk number of the external party to the desktop, where it has no meaning. The trunk number is displayed in Agent Desktop as <Unavailable>.

**Problem** An agent can't view any skills statistics in Agent Desktop.

**Solution** If an agent is not assigned to a skill group, no skills statistics are available.

**Problem** Sometimes after placing a call on hold, an agent is unable to retrieve the call. Once the call is hung up, the agent state still reflects On Hold. Exiting and restarting Agent Desktop doesn't help.

**Solution** A task in Unified CM administration is associating devices with RmCm users. The peripheral gateway RmCm user should be associated with agent telephones. The IP IVR JTAPI user should be associated with the CTI ports corresponding to the virtual ports on the IP IVR.

Each of these device categories is distinct. A device cannot belong to more than one category. Failure to assign a device to exactly one category can cause problems.

**Problem** The agent can make and receive internal calls but gets errors when trying to make an external call.

**Solution** The dial string properties must be configured properly for outgoing calls. Some switches are set up to automatically dial an 8 or 9 to get an outside line, while others require you to dial an 8 or 9. The dial string must take into account how the switch is set up.

**Problem** The agent's call control action does not work properly.

**Solution** Try performing the same action manually using the dial pad. Telephone numbers are formatted the same way when used in call control actions as they are when making calls manually. Make sure that the dial string is configured properly for outgoing calls.

**Problem** When Agent Desktop attempts to launch an external application, the following error message appears: "Error Launching Application... The system cannot find the file specified."

**Solution** When creating a launch external application action, you must include the extension of the application you wish to launch. For example, to launch Windows Notepad, C:\Windows\Notepad.exe is correct, while C:\Windows\Notepad is incorrect.

If the path to the executable or an argument contains spaces, it must be enclosed in quotes, for instance, "C:\Program Files\MyFile.doc."

**Problem** The administrator configured a task button to start Microsoft Notepad, and changed the hint to Run Notepad (Ctrl+R). The shortcut keys do not work.

**Solution** For any task button, you may only change the hint text. You cannot change the shortcut key.

**Problem** An agent using Agent Desktop with Terminal Services logs out, closes, and then later attempts to log back in. The agent receives the message, "Cisco Agent Desktop is already running for Terminal Service user "<agent's user name>." Only one instance per user is allowed."

**Solution** The OS variable SESSIONNAME was not updated when the agent logged out. If this variable is set to RDP-<session number> or ICA-<session number>, the system looks at the HOMESHARE variable for the agent's home directory, where that agent's logs and configuration files are stored. If the SESSIONNAME variable is not cleared, then Terminal Services sees the agent as logged in. This can happen if the agent does not log off of Terminal Services cleanly after

logging out of CAD. To log out cleanly, the agent must select Log Out from the Terminal Services dialog box drop-down list and then click OK.

**Problem** An agent logs into Agent Desktop as a mobile agent on one computer and closes Agent Desktop while on a call, and then attempts to log into another instance of Agent Desktop on another computer using the same agent ID but a different extension. A forced login does not work.

**Solution** The agent must log out of the first instance of Agent Desktop that was started. If this does not work, reset the phone through Unified CM and the CAD services reset.

**Problem** When agents start Agent Desktop, they see the following error: "A licensing error has occurred. Please try again in five minutes. If the problem persists, please see your log file or the System Administrator for details."

Conditions: Telnet tests from the agent PC to the LRM service on the CAD server (port 65432) fail. The LRM service is running and agents are able to connect some of the time. Cisco Security Agent (CSA) is installed and running on the CAD server.

CSA log reports the following: "Event: Possible SYN Flood detected. Source addresses include 10.X.X.X. TCP ports, including port 59004, SYN Flood protection has been enabled."

Cause: CSA is in SYN Flood detection mode. Agent PCs have the firewall enabled and are blocking packets, and CSA thinks the PC is non-responsive.

**Solution** Short-term solution: Restart CSA on the CAD servers.

Long term solution options include:

- Option 1: Leave the systems as is. Risk: SYN Flood detection mode might become enabled, which can prevent agents from logging in. If not discovered immediately, the problem can persist until SYN Flood turns off by itself (approximately 2 hours).
- Option 2: Turn off SYN Flood detection mode. Risk: Leaves the server open to SYN Flood.
- Option 3: Turn off Agent PC firewall. Risk: Could leave agent PCs vulnerable to viruses.

Recommendation: Option 2. SYN Flood is generally not effective against modern networks.

**Problem** When trying to view agent state or call logs, no data is presented.

**Solution** The agent may not have received a call, or logged in for that particular day. The agent's or supervisor's PC's clock may not be in the correct time zone.

**NOTE:** All state and call times are based on server time.

**Problem** When an agent receives a transferred call, the enterprise data is not correct.

**Solution** Call waiting is not supported in CAD. If call waiting is enabled, enterprise data might not be correct in certain circumstances. For example, if an agent is on a call and a new call is routed to that agent, and that agent transfers the original call to another agent, the second agent's desktop might display enterprise data for the new call, rather than the original call.

**Problem** The enterprise data portion of the Contact Management pane in CAD-BE is completely blank and does not display any information about the current call.

**Solution** This error might occur if an Agent Desktop agent edits the layout name during a call and enters the name of a layout that does not exist, and then transfers the call to a CAD-BE agent. In this situation, the enterprise data portion of the Contact Management pane in CAD-BE will be empty.

## Agent State Problems

**Problem** Sometimes while talking on a call, the agent is unable to change the agent state to Not Ready. As a result the agent keeps receiving calls from the ACD, even after closing the application.

**Solution** A task in Unified CM administration is associating devices with RmCm users. The peripheral gateway RmCm user should be associated with agent telephones. The IP IVR JTAPI user should be associated with the CTI ports corresponding to the virtual ports on the IP IVR.

Each of these device categories is distinct. A device cannot belong to more than one category. Failure to assign a device to exactly one category can cause problems.

**Problem** An agent is on a call and presses the Not Ready button, but when the call ended, the agent is placed in a Work Not Ready state.

**Solution** If the Work Mode defined in the Unified ICM database is set to Required or Required with Data, transitions to Ready or Not Ready while you are on a call will actually transition to Work Ready or Work Not Ready respectively once the call ends.

**Problem** An agent is on a call and presses the Work Ready button, but Agent Desktop keeps displaying the message, “Unable to change agent state.”

**Solution** If the Work Mode defined in the Unified ICM database is set to Not Allowed, transitions to Work Ready and Work Not Ready will fail.

## CAD-BE Problems

**Problem** The browser returns HTTP Status 404 after entering the CAD-BE URL.

**Solution** An incorrect URL for CAD-BE was used. Make sure the correct URL is used. The URL is case-sensitive. The correct URL is the following, where <CAD server> is the IP address for the server on which the CAD base services are installed:

http://<CAD server>:8088/cadbe/CAD-BE.jsp

**Problem** The browser returns the error “The page cannot be displayed”.

**Solution** The browser cannot communicate with the Tomcat service.

- Make sure the IP address or hostname is for a valid CAD server.
- Make sure the port is 8088. The port to use is specified in <Parameter name=”port” value=”8088”/>, under the section <!-- Normal HTTP --> in C:\Program Files\Cisco\Desktop\Tomcat\conf\server.xml.
- Check the Services control panel to make sure the Tomcat service is running.
- Make sure port 8088 is not blocked from the client or server computer.

**Problem** A pop-up message indicates that CAD-BE is unable to connect to the BIPPA service. The CAD-BE log also shows “CADBE1002: Could not connect to BIPPA Service.”

**Solution** The BIPPA service may be down or is not active.

- If this is a redundant system, the URL used may be pointing to the standby BIPPA service. Use the active BIPPA service.
- Start the BIPPA service if it is down.
- Check the CAD Configuration Setup utility on the CAD base services server to see if the externally visible names or IP addresses specified for the CAD-BE servers are correct. They must be the

same as the ones used in the CAD-BE URL. If changes are made to the settings in CAD Configuration Setup, the BIPPA service(s) must be restarted for the changes to take effect.

- Make sure port 59012 is not blocked from the client or server computer.
- On a nonredundant system, if the LRM service is down, then the BIPPA service will become standby. Restart the LRM service.
- The BIPPA service will not become active until CAD Configuration Setup has run successfully. Complete all windows in CAD Configuration Setup.
- Desktop Administrator, Agent Desktop, or Supervisor Desktop was installed on the same computer as the CAD services. They clear a registry key (IOR Hostname under Site Setup) required by the BIPPA service. Set the registry to the public IP address of the CAD services computer.
- CAD-BE was running when CAD server computer was upgraded such that the CAD-BE that is running is of a different version than the BIPPA service to which it is attempting to connect. Check BIPPA server computer to make sure its CPU is not too high. Check that network latency between the desktop and BIPPA server computers is not too high.
- CAD-BE timed out while attempting to reach BIPPA service. Verify that CPU usage on the CAD server hosting the BIPPA service is not too high. Verify that network latency between the desktop and CAD server hosting the BIPPA service is not too high.

**Problem** When starting CAD-BE, the Java Runtime Environment installation begins.

**Solution** The agent is running CAD-BE on a computer where the Java Runtime Environment is not installed. Once JRE is installed, this will not happen again. Allow the JRE installation to complete, after which CAD-BE will start normally.

**Problem** When starting CAD-BE, the browser displays the following message: “This site might require the following ActiveX control 'J2SE Runtime Environment 5.0 Update 11' from 'Sun Microsystems, Inc.'. Click here to

install if you do not have the required Java Runtime Environment version installed."

**Solution** The agent is running CAD-BE on a computer where the Java Runtime Environment is not installed. The browser's security settings prevent the browser from automatically installing the Java Runtime Environment. See the *Cisco CAD Installation Guide* for the correct Internet Explorer settings. After you correct the settings, restart CAD-BE.

---

**Problem** When starting CAD-BE, the browser displays the following message: "Your security settings do not allow Web sites to use ActiveX controls installed on your computer. This page may not display correctly. Click here for options if you have Java or ActiveX controls disabled in your browser."

**Solution** The agent is running CAD-BE on a computer on which the security settings prevent the browser from running ActiveX components. This will prevent the Java Runtime Environment from running. The Java Runtime Environment is required to run CAD-BE. See the *Cisco CAD Installation Guide* for the correct Internet Explorer and Firefox settings. After you correct the settings, restart CAD-BE.

---

**Problem** When starting CAD-BE, the browser displays the following message: "Javascript is disabled in your browser. CAD-BE requires JavaScript to function properly. Configure your browser so that JavaScript is enabled, or contact your administrator for assistance."

**Solution** Javascript is not enabled in the browser. See the *Cisco CAD Installation Guide* for the correct browser settings. After you correct the settings, restart CAD-BE.

---

**Problem** When starting CAD-BE, the browser displays the following message: "Your browser does not understand the object tag. CAD-BE will not run."

**Solution** This message appears in the following circumstances:

- You are using an unsupported browser. Internet Explorer 6 and 7 and Mozilla Firefox 1.5 and above are the only supported browsers for this release.

- You do not have the required Java Runtime Environment version installed. You can install the Java Runtime Environment from the CAD Installation webpage.
- You have ActiveX controls disabled in your browser. See the *Cisco CAD Installation Guide* for the correct browser settings. After you correct the settings, restart CAD-BE.
- You do not have Java enabled. See the *Cisco CAD Installation Guide* for the correct browser settings. After you correct the settings, restart CAD-BE.

**Problem** When starting CAD-BE, the browser displays a message that pop-ups are blocked.

**Solution** Pop-ups are blocked in the browser. Refer to the *Cisco CAD Installation Guide* for the correct browser settings. Disable any third-party popup blockers. If CAD-BE is still being blocked by pop-up blockers, hold down the Ctrl key when selecting the CAD-BE URL to temporary unblock it.

**Problem** When starting CAD-BE, the CAD-BE window is closed. Another CAD-BE window is displayed, and no login dialog is displayed.

**Solution** CAD-BE is already running on the desktop, and the agent tried to start another instance of CAD-BE. Only one instance of CAD-BE can run on a desktop. Do not start more than one instance.

**Problem** When starting CAD-BE, an empty browser window is left behind the CAD-BE window.

**Solution** Scripts are unable to close windows. This window is safe to close. Refer to the *Cisco CAD Installation Guide* for the correct browser settings to prevent the empty window from appearing.

**Problem** The agent logged into CAD-BE and was logged out after a short while.

**Solution** The agent is a mobile agent with voice mail on the mobile phone. When the agent did not answer in time, the call from Unified ICM rolled over

into the mobile phone's voice mail. When voice mail did not detect any voice in the call from Unified ICM, it dropped the call, causing Unified ICM to log the agent out.

- Answer the call quickly.
- Turn off voice mail or any similar features that could cause the call from Unified ICM to be redirected.

**Problem** The agent receives calls in CAD-BE but has no calls on the mobile phone when logged into CAD-BE as a mobile agent.

**Solution** The agent is a mobile agent with voice mail on the mobile phone. Calls from Unified ICM may be rolling over into the mobile phone's voice mail. Turn off voice mail or any similar features that could cause the call from Unified ICM to be redirected.

**Problem** The agent is logged in and in a ready state, and the computer's screen saver or power saver feature has activated. CAD-BE is frozen or disconnected from the server.

**Solution** This is caused by a Java bug involving memory leaks. To avoid the problem, disable the screen saver/power saver features.

**Problem** A CAD-BE agent cannot be monitored or recorded.

**Solution** The CAD-BE agent's phone is not set up for SPAN port monitoring.

**Problem** The Firefox browser freezes when an agent attempts to make a call using the make call button.

**Solution** The agent is running CAD-BE on a computer that has an unsupported version of Java Runtime Environment (JRE) installed. Check if the version of JRE installed is compatible with CAD-BE.

**Problem** Partial call history or partial data appears in the Enterprise Data fields for calls right after a failover.

**Symptom.** When an agent receives a call, the Enterprise Data pane and/or the Enterprise Call History pane does not display complete data for calls that began prior to or occurred during a failover.

**Cause**. The system might have active calls during failover. The Enterprise service tries to get call information for such calls by making a snapshot of the call. The snapshot does not provide complete call history, thus the missing data.

**Solution** This is expected behavior. A call that occurs when the Enterprise service is up and running after a failover will have complete data.

**Problem** The administrator has made changes in Desktop Administrator, but they are not showing up in CAD-BE.

**Solution** CAD-BE agent must log out and restart the browser in order for the changes to take effect.

**Problem** Partial Service or No Service message displays in the CAD-BE status bar.

**Symptom**. The agent sees a message in the CAD-BE status bar: Partial Service or No Service.

**Cause**. CAD-BE has detected that it is unable to communicate with a service (generally within three minutes of the service failure), and displays the “Partial Service” or “No Service” message to indicate some or all of the services have failed.

**Solution** Double-click on the message in the status bar to display the Server Status pop-up window. This window lists CAD-BE features and indicates which features are affected by the service failure. When CAD-BE detects that the failed service is again available (usually within one minute of the service recovery) the status bar displays “In Service” to indicate that the service has recovered.

**Problem** Sometimes during a conference call, a conference member shows up as <Unavailable>.

**Solution** Solution <Unavailable> represents a party outside the switch. The switch sends the trunk number of the external party to the desktop, where it has no meaning. CAD-BE replaces the trunk number with <Unavailable>.

**Problem** No data appears in the Enterprise Data fields.

Symptom. When an agent receives a call, the Enterprise Data pane does not display the expected data.

Cause. The Unified ICM server is not correctly passing enterprise data from the Enterprise service to BIPPA service. This situation can be a result of incorrect step configuration in the script or in the Enterprise Data Configuration section of Desktop Administrator. This situation can also be a result of an out-of-sync condition between the Enterprise Data subsystem and the Enterprise service.

**Solution** Complete the following steps:

1. Verify the step configuration in the script and in the Enterprise Data.
2. Configuration section in Desktop Administrator.
3. Stop and restart the Enterprise service.
4. If the problem persists, stop and restart the Unified ICM.

**Problem** The agent sent the supervisor an emergency chat message but the supervisor never received it.

**Solution** Supervisors receive emergency chat messages only if they are monitoring the team to which the agent who sent the message belongs.

**Problem** The agent is using CAD-BE with an IP soft phone (for instance, IP Communicator) on a computer with multiple network adapter cards. When the agent switches from using one NIC to the other to connect to the network, the agent cannot log in. (An example of this situation is

running CAD-BE with an IP soft phone on a laptop that can connect to the network using either an Ethernet or wireless connection.)

**Solution** Solution Each NIC has its own MAC address. Unified CM must be able to associate a MAC address with an extension in order for CAD-BE to function correctly. If the Unified CM knows about only one of the multiple NICs, only that one will work. If an agent is going to use a computer with multiple NICs, Unified CM must be configured to recognize each NIC MAC address.

---

**Problem** When the agent starts CAD-BE, a call appearance is displayed showing that the agent is on a call, even though there is no active call on the agent's phone.

**Solution** On startup, CAD-BE asks the CTI service for a snapshot of any existing phone calls to display to the user. Occasionally the CTI service returns invalid data. To dismiss the invalid data, the agent must click Drop. If the call appearance persists, the agent might have to logout and close CAD-BE browser, pick up the phone receiver to get a dial tone, hang up, and then restart CAD-BE.

---

**Problem** Sometimes after placing a call on hold, the agent is unable to retrieve the call. Once the call is hung up, the agent state still reflects On Hold. Logging out and restarting CAD-BE doesn't help.

**Solution** A task in Unified CM administration is associating devices with JTAPI users. The peripheral gateway JTAPI user should be associated with agent telephones. The IP IVR JTAPI user should be associated with the CTI ports corresponding to the virtual ports on the IP IVR. Each of these device categories is distinct. A device cannot belong to more than one category. Failure to assign a device to exactly one category can cause problems.

---

**Problem** The agent is logged out unexpectedly.

**Solution** Possible reasons are:

- Another agent with the same ID or extension has logged in, causing the first agent to be logged out.
- A supervisor has logged the agent out.

- The telephony service has failed.
- The network has failed.

**Problem** The agent is participating in a blind conference call, but cannot see all parties on the call.

**Solution** A blind conference is defined as adding an alerting party to a conference. All parties on a blind conference call might not show up in either Supervisor Desktop, Agent Desktop or CAD-BE. This is a limitation of the CTI service software.

**Problem** The agent logs into CAD-BE and can receive direct calls and change agent state, but cannot receive ACD calls.

**Solution** The agent's extension is configured in Unified CM, but is not in the Unified ICM Device Target list. Configure the extension's device target and label for full functionality.

**Problem** An agent is on a call and presses the Work Ready button, but CAD-BE keeps displaying the message, "Unable to change agent state."

**Solution** If the Work Mode defined in the Unified ICM database is set to Not Allowed, transitions to Work Ready and Work Not Ready will fail.

**Problem** An agent is on a call and presses the Not Ready button, but when the call ended, the agent is placed in a Work Not Ready state.

**Solution** If the Work Mode defined in the Unified ICM database is set to Required or Required with Data, transitions to Ready or Not Ready while you are on a call will actually transition to Work Ready or Work Not Ready respectively once the call ends.

**Problem** The agent receives an ACD call, but the route point did not show up in the call history.

**Solution** Unified ICM Configuration Manager must be configured to enable route points to appear in call history. In Unified ICM Configuration Manager, choose Tools > List Tools > Dialed Number/Script Selector List, and on the Dialed Numbers tab, check the Permit application routing check box.

**Problem** When starting CAD-BE, the browser displays the message “The version of JRE installed on your PC is higher than the maximum version supported by CAD-BE. Uninstall all instances of JRE that have a version higher than the maximum version supported by CAD-BE, then install the version of JRE that is supplied with CAD-BE.”

**Solution** If using Firefox, uninstall any JRE higher than 1.6 or switch to using Internet Explorer. Make sure a supported JRE 1.6 is installed.

## CAD Service Problems

**Problem** How can I tell if a CAD service is running?

**Solution** To view the status of all the services in the CAD system, access the Desktop Monitoring Console browser, where <CAD server> is the IP address of the server on which the CAD base services are installed: from this URL in your server.

http://<CAD server>:8088/smc/monitor.jsp

You can also view the status of CAD services in Cisco Unified System Contact Center Enterprise (Unified SCCE) Web Administration. Log into Unified SCCE Web Administration using the following URL, where <Admin workstation> is the IP address of the server on which Unified SCCE is installed:

http://<Admin workstation>/uiroot/uicommander?svcDomain=default&req=ipccAdmin.login

Choose System Management > Machine Management > Service Management. From the Service Management page you can select a specific server for which you want to view service status. On the Services for <server name> page, you can use these options: Refresh, Cancel, Start, Stop, Cycle, Manual, and Automatic.

**Problem** How can I check if the CTI Unified ICM service is running?

**Solution** On the Unified ICM computer, check if the status of all processes in the Unified ICM Server Control are running.

**Problem** How can I tell if the Tomcat webserver is installed correctly?

**Solution** Perform the following tests:

- On the PC where the BIPPA service is installed, open the Services control panel to see if the Tomcat service and the BIPPA service are running.

- Verify you can see Tomcat's html index page. In your web browser, enter the URL http://<Tomcat server IP address>:8088/.
- Attempt to display the following page in your web browser without an error: http://<Tomcat server IP address>: 8088/ipphone/jsp/sciphonexml/IPAgentInitial.jsp

If these tests fail, check the following:

- JRE is installed on the server.
- The file that maps URLs with JSP pages to the correct java servlets, web.xml, must be in the ...\Tomcat\webapps\ipphone\ web-inf directory.
- Find this entry in the registry:

  HKEY_LOCAL_MACHINE\SOFTWARE \Spanlink\CAD\IPPA\Config\TOMCAT HOME

  and set its value to C:\Program Files\Cisco\Desktop\Tomcat\

**Problem** If the Microsoft SQL Server CADSQL Instance is uninstalled and the ICM Logger or ICM Admin Workstation is restarted, the ICM Logger or ICM AW fails to start and displays an error message. The error occurs because certain registry keys that are required by these services are removed during the uninstall.

**Solution** Complete the following steps using the SQL Server Client Network Utility.

1. Launch cliconfg from either a command window or the Start > Run prompt.
2. Enable the Named Pipes and TCP/IP protocols.
3. Ensure that Named Pipes appears before TCP/IP in the list of enabled protocols.
4. Check Enable Shared Memory Protocol.
5. Apply the changes and exit by clicking OK.

# Chat Problems

**Problem** The agent sent the supervisor an emergency chat message but the supervisor never received it.

**Solution** Supervisors receive emergency chat messages only if they are monitoring the team to which the agent who sent the message belongs.

## Desktop Administrator Problems

**Problem** The administrator cannot create a new work flow group.

**Solution** The work flow group name is already used for another group, and/or the work flow group name is not a valid Windows directory name.

**Problem** After upgrading from CAD 6.0 to CAD 8.0 and restoring the 6.0 data, the Skill data field does not appear as expected in the User Interface > Show Data Fields tab in Desktop Administrator.

**Solution** If you restore your data using the Restore Backup Data window in CAD Configuration Setup after installing CAD 8.0, the Skill data field will not appear on the Show Data Fields tab. To ensure that this data field is available for your use, restore your 6.0 data using the CDBRTool utility. See the *Cisco CAD Installation Guide* for information on using this utility.

**Problem** When Desktop Administrator starts, it does not get automatically updated.

**Solution** Automated updates are disabled for Windows Vista. Other options are:

- Manual “over-the-top” installation
- Push installation

## Desktop Monitoring Console Problems

**Problem** The Desktop Monitoring Console displays "...snmp TimeoutError" in the Status field in the right pane's Summary Status Information.

**Solution** Make sure that the SNMP service is installed and correctly configured. See the section "Cisco Desktop Monitoring Console" in the *Cisco CAD Installation Guide* for more information.

**Problem** The Desktop Monitoring Console displays "Remote LDAP Status" in the Host field and "Failed to connect to server.host:..." in the Status field in the right pane's Summary Status Information.

**Solution** Click Refresh Server List on the bottom left of the window. If the error message persists, make sure that the LDAP Monitor service and Directory Services are running without problems.

**Problem** The Desktop Monitoring Console does not display the correct service list in the left pane.

**Solution** Click Refresh Server List on the bottom left of the window to update the service list.

**Problem** The Desktop Monitoring Console displays a black screen, the information is hard to read, or the browser window automatically closes when trying to access the Desktop Monitoring Console.

**Solution** Make sure that your display settings are set for at least 256 colors.

## Desktop Presence Administrator Problems

**Problem** No names are found when searching for subject matter experts from the Contact List page.

**Solution** This error occurs when the Unified Presence cluster login credentials are not configured correctly. The user specified on the Cisco Unified Presence Cluster Settings page must be able to perform SOAP queries and must be associated with the same profile in LDAP that agents are associated with.

**Solution** To verify the credentials, complete the following steps.

1. Choose Cisco Unified Presence Settings > Cisco Unified Presence Cluster Settings.
2. Verify that the correct login is entered in the AXL Login ID field.
3. Type the correct AXL password in the Password field.
4. Click Verify to test the credentials you just entered. A message should appear, stating that the transaction was successful.
5. Click Save.

**Problem** A subject matter expert cannot log into Cisco Unified Personal Communicator.

**Solution** When a subject matter expert attempts to log into Unified Personal Communicator, the error message "401 (Unauthorized)" appears.

This error occurs when the incoming Access Control List (ACL) in Unified Presence is not configured correctly. The ACL allows you to configure patterns that control which hosts and domains can access Unified Presence. To enable SMEs to access Unified Presence from Unified Personal Communicator, you must add an entry for "all" to the incoming ACL.

To add the "all" entry as an incoming ACL, complete the following steps.

1. Log into Unified Presence Administration.
2. Choose System > Security > Incoming ACL. The Find and List Allowed Incoming Hosts page appears.

3. Click Add New. The Incoming Access Control List Configuration page appears.
4. If desired, type a description of the address pattern in the Description field.
5. Type "all" in the Address Pattern field, then click Save.

**Problem** A subject matter expert using a soft IP phone is not shown as busy when viewed by an agent running Agent Desktop.

**Solution** The Unified CM Session Initiation Protocol (SIP) publish trunk is not configured correctly.

To verify that the Unified CM SIP publish trunk is configured correctly, complete the following steps.

1. Log into Unified Presence Administration.
2. Choose Presence > Settings. The Cisco Unified Presence Settings page appears.
3. Verify that the correct trunk is selected in the CUCM SIP Publish Trunk drop-down list.

**NOTE:** You must select the Enable SIP Publish on CUCM check box to enable the CUCM SIP Publish Trunk parameter.

For more information about SIP trunks in Unified CM, see the Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager.

**Problem** A subject matter expert using a soft IP phone is not shown as busy when viewed by another subject matter expert running Unified Personal Communicator.

**Solution** The Unified CM Session Initiation Protocol (SIP) publish trunk is not configured correctly.

To verify that the Unified CM SIP publish trunk is configured correctly, complete the following steps.

1. Log into Unified Presence Administration.

2. Choose Presence > Settings. The Cisco Unified Presences Settings page appears.
3. Verify that the correct trunk is selected in the CUCM SIP Publish Trunk drop-down list.

**NOTE:** You must select the Enable SIP Publish on CUCM check box to enable the CUCM SIP Publish Trunk parameter.

For more information about SIP trunks in Unified CM, see the Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager.

**Problem** Agents cannot see SMEs.

**Solution** Perform the following checks.

- Verify that agent can log into Unified Personal Communicator and see SMEs.
- Verify that the correct IP address for the Unified Presence server is entered in Desktop Presence Administrator.
- Verify that the agent does not have a user administered in Active Directory on the Unified Presence server.
- Verify that at least one contact list containing one or more SMEs has been assigned to the work flow group to which the agent belongs.
- Verify that the SMEs are available.
- Verify that the agent is running Agent Desktop and is logged into Unified Presence. To log in, click Chat, then choose File > Log In.

**Problem** SMEs cannot see an agent or the agent's state is unknown.

**Solution** Perform the following checks.

- Verify that the agent is in the SME's contact or buddy list.
- Verify that the work flow group is configured to publish the agent's state.

**Problem** After an agent or supervisor logs into Agent Desktop or Supervisor Desktop, an error message appears, stating that the login that was entered is not valid for Unified Presence.

**Solution** Agent Desktop and Supervisor Desktop automatically try to use the same credentials to log into Unified Presence that were used to log into the desktop application. If the Unified Presence credentials are different, the agent or supervisor will have to enter the credentials manually. An alternate solution is to use the same credentials for the Unified Presence server as the credentials for the CAD desktop application.

**Problem** An agent cannot initiate a call to an SME in the Contact Selection window because the call control options in the Actions menu are inactive.

**Solution** Agent Desktop cannot retrieve the SME's phone number from the Unified Presence server. Verify that a phone number is configured for the SME in Unified Presence.

**Problem** An SME's presence status is displayed as Available in the Contact Selection window, even when the SME is already on a call.

**Solution** Unified Presence is not configured to monitor the SME's phone status.

To configure Unified Presence to monitor phone status, complete the following steps.

1. Log into Unified CM Administration.
2. Choose Device > Trunk. The Find and List Trunks page appears.
3. Verify that there is a trunk of type SIP Trunk and that the destination address of the trunk is the IP address of your Unified Presence server.
4. Choose Device > Phone. The Find and List Phones page appears.
5. Find and click the hyperlink for the device that corresponds to the SME's Unified Personal Communicator. The Phone Configuration page appears.

6. Click the hyperlink for the directory number that is configured for the SME's device. The Directory Number Configuration page appears.
7. In the Users Associated with Line section, click Associate End Users. The Find and List Users page appears.
8. Select the user you want to associate with the directory number that is configured for the SME's device, then click Add Selected. The Directory Number Configuration page reappears and displays the user you just associated with this directory number.
9. Click Save to save your changes.
10. Log into Unified Presence Administration.
11. Choose Presence > Settings. The Cisco Unified Presence Settings page appears.
12. Verify that the CUCM SIP Publish Trunk is the same SIP trunk that is configured in Unified CM (step 3 above).

**Problem** An agent is not receiving chat messages.

**Solution** This error occurs when an agent is logged into Unified Presence through two applications. An agent cannot be logged into Unified Presence through Unified Personal Communicator and through Agent Desktop/Supervisor Desktop at the same time, even if the usernames are different.

**Problem** When an agent receives a transferred call, the enterprise data is not correct.

**Solution** Call waiting is not supported in CAD. If call waiting is enabled, enterprise data might not be correct in certain circumstances. For example, if an agent is on a call and a new call is routed to that agent, if that agent transfers the original call to another agent, the second agent's desktop might display enterprise data for the new call, rather than the original call.

**Problem** The enterprise data portion of the Contact Management pane in Agent Desktop is completely blank and does not display any information about the current call.

**Solution** This error can occur if one agent edits the layout name during a call and enters the name of a layout that does not exist, and then transfers the call to another agent. In this situation, the enterprise data portion of the Contact Management pane in the second agent's desktop will be empty.

## Enterprise Data Problems

**Problem** The DNIS shown in the agent's enterprise data is incorrect for an Outbound Option call.

**Solution** The dialer port has not been set up as a monitored device. The administrator must add the dialer port to the list of monitored devices in the Enterprise Configuration dialog box in Desktop Administrator.

**Problem** Enterprise data displays data after a call has been dismissed.

**Solution** Enterprise data displays data from the last call until a new call is received. This allows agents to use the enterprise data for after-call work.

## Enterprise Service Problems

**Problem** When the user attempts to start Enterprise service, the following error displays:

"Could not start the Cisco Enterprise service on \\<computer>
Error 2140: An internal Windows NT error occurred."

**Solution** Look at the Windows NT event log to see why the service failed to start.

1. Choose Start > Programs > Administrative Tools > Event Viewer.
2. On the Log menu, choose Application.
3. Choose a message that displays Enterprise Server as the source. This should provide more information on the cause of the failure.

## Install and Upgrade Problems

**Problem** The client application installations do not download when the links on the installation web page are clicked. When the install program link is clicked, a "HTTP 404—File Not Found" error is displayed.

**Solution** CAD Configuration Setup was not completed successfully on the CAD base services server. Launch CAD Configuration Setup. (On the CAD base services server, in Windows Explorer, navigate to the folder C:\Program Files\Cisco\Desktop\bin and run PostInstall.exe).

If Configuration Setup starts in initial mode, it was not completed correctly. Go through each window and make sure that all required data is entered, and then choose File > Save.

If Configuration Setup starts in update mode, choose File > Reset Client Installs. This places the client install files in the default location, and reconfigures them to use the default setting for the IP address of the LDAP server.

Try to install the client applications from the installation web page again. If the problem persists, contact technical support.

**Problem** When upgrading from a previous version to a Unified System Contact Center (Unified SCC) version, Login by Name does not work although that is the only login method used in a Unified SCC installation. The option for choosing login method in Desktop Administrator is disabled.

**Solution** Launch CAD Configuration Setup. (On the CAD Base services server, in Windows Explorer, navigate to C:\Program Files\Cisco\Desktop\bin and run PostInstall.exe).

If CAD Configuration Setup starts in initial mode, complete the following steps.

1. A dialog box appears, asking if this is a Unified SCC installation. Click No, and then click Apply. Exit CAD Configuration Setup.
2. Launch CAD Configuration Setup again.
3. A dialog box appears, asking if this is a Unified SCC installation. Click Yes, and then click Apply. Exit CAD Configuration Setup.

4. Restart the Sync service and the VoIP Monitor service.

If CAD Configuration Setup starts in upgrade mode, complete the following steps.

1. Choose the ICM Admin Workstation Distributor window. In the Unified SCC Environment section, select Yes, and then click Apply. Exit CAD Configuration Setup.
2. Restart the Sync service and the VoIP Monitor service.

---

**Problem** When upgrading from 7.1 to 7.2, wrap-up data and reason codes are not restored.

**Solution** Complete the following steps.

1. Edit every backup file by changing the version number from 2.1.0 to 2.2.0. The version number appears at the beginning of the file. For example:
   [Version]
   V=2.1.0

   **CAUTION:** Use a clean text editor. Do not use Notepad or Wordpad to edit the backup files. Both of these editors add a double byte code at the beginning of the file that renders the file unreadable by the backup and restore utility.
2. Restore the wrap-up data and reason codes manually from the command line using CDBRTool.

---

**Problem** When upgrading a replicated system running a CAD version before 8.0, replication is re-established after upgrading only one of the servers.

**Solution** Replication should not be re-established until after both servers have been upgraded. If replication is inadvertently re-established after upgrading only one of the servers, however, recover from this error by completing the following steps.

1. Shut down replication.
2. Upgrade the server that has not yet been upgraded.
3. Restore the backup data.
4. Re-establish replication.

**Problem** When backing up and restoring CAD, the CDBRTool fails during the restore process.

**Solution** Supervisor work flows that use an audio file bigger than 50Kb in size for audible alert actions can cause the restore process to fail. Make sure that any audio files are no larger than 50Kb.

## IP Phone Agent Problems

**Problem** Agents do not see the IP Phone Agent service on their IP phones.

**Solution** The following are some reasons why the service does not appear when the services menu is accessed:

- The IP Phone Agent service has not been configured in Unified CM.
- The phone is not subscribed to the IP Phone Agent service.
- The service URL in Unified CM has a hostname and the phone cannot resolve it. Use the IP address instead.
- The phone has not been rebooted after changes were made in Unified CM. If a soft reboot does not work, try a hard reboot (unplug the phone's power cord and then plug it back in).

**Problem** Agents see an HTTP error when selecting the IP Phone Agent service on their phone.

**Solution** Some solutions:

- The IP Phone Agent service URL in Unified CM has a hostname and the phone cannot resolve it. Use the IP address instead.
- The IP Phone Agent service URL in Unified CM has an incorrect hostname, IP address, or port. The port is specified in <Parameter name="port" value="8088"/> under the section <!-- Normal HTTP --> in the file C:\Program Files\Cisco\Desktop\Tomcat\conf\server.xml.
- The IP Phone Agent service URL is case sensitive. Enter it exactly as specified in the *Cisco CAD Installation Guide*.
- The Tomcat service is not running on the CAD server.
- The BIPPA service is not running on the CAD server.
- The agent's phone was not rebooted after changes were made in Unified CM. If a soft reboot does not work, try a hard reboot (unplug the power cord and plug it back in).
- The ippa.war file is not extracted correctly. Perform the following steps on the CAD base services server:
  a. Stop Tomcat.

b. Delete the C:\Program Files\Cisco\Desktop\Tomcat\webapps\ipphone folder.

c. Restart Tomcat.

**Problem** The agent sees an error message that the BIPPA service is not active.

**Solution** Some solutions:

- The system is set up with redundant CAD services and the agent has selected the standby IP Phone Agent service instead of the active service. For redundant CAD services, there should be two IP Phone Agent services set up in Unified CM, pointing to IP Phone Agent services on different servers, and all IPPA agent phones must be subscribed to both services.
- On a nonredundant system, if the LRM service is down, then the BIPPA service will become standby. Restart the LRM service.
- The BIPPA service will not become active until CAD Configuration Setup is completed successfully. Complete all windows in CAD Configuration Setup.
- Desktop Administrator, Agent Desktop, or Supervisor Desktop was installed on the same computer as the CAD services. They clear a registry key (IOR Hostname under Site Setup) required by the BIPPA service. Set the registry to the IP address of the CAD services computer.

**Problem** The agent gets the Force Login screen when trying to log in, but attempting to force the login does not work.

**Solution** The agent is using an agent ID that is already logged in on another extension, or using an extension that is already logged in with a different agent ID. Forced logins work only for the same ID/extension pair. Use a different agent ID or extension, or find the other user and have them log out.

**Problem** The agent does not see the Enterprise Data screen when receiving/answering a call, receiving Skill Statistics screen updates, or seeing the Wrap-up screen.

**Solution** Some solutions:

- The authentication URL in Unified CM has a hostname and the phone could not resolve it. Use the IP address instead.
- If using the Unified CM authentication URL (the URL that points to authenticate.jsp), make sure that the correct BIPPA user and password (as specified in CAD Configuration Setup) exists in Unified CM and that the phone is associated with this user.
- The agent's phone was not rebooted after changes were made in Unified CM. If a soft reboot does not work, try a hard reboot (unplug the power cord and plug it back in).
- Verify that the agent is logged into the phone.
- Verify that if the agent logs into CAD using the same phone and user ID, enterprise data does pop correctly.

**Problem** The agent sees nonsense characters in enterprise data, reason codes, or wrap-up data.

**Solution** The reason codes configured in Unified ICM or wrap-up data configured in Desktop Administrator contain characters not supported by the phone. Examples are multibyte Chinese or Kanji characters. Make sure that no unsupported characters are used when configuring reason codes and wrap-up data.

**Problem** A supervisor cannot record or monitor an IP Phone Agent agent.

**Solution** Possible reasons for this problem include the following:

- The phone is not set up for SPAN port monitoring.
- Unified CM-based monitoring is being used and the IP phone that the agent is using does not support that feature.

## LDAP Monitor Problems

**Problem** Slapd.exe is not running even though the LDAP Monitor service is running.

**Solution** Do the following:

- Check slapd.conf to ensure it is correct.
- Make sure no other instances of slapd.exe are running.
- Make sure the C:\Program Files\Cisco\Desktop\database folder contains 7 files with a *.dat extension and DB_CONFIG. If these are missing, copy them from another system or reinstall the CAD services.
- Make sure the C:\Program Files\Cisco\Desktop\database folder contains log.*, __db.* and eight files with a *.bdb extension. If not, follow the procedure in "Out of Sync Directory Services Databases" on page 44, copying from the one that works to the one that does not. Otherwise, you will need to reinstall the CAD services.
- Get more information about why slapd.exe cannot start:
  a. Stop the LDAP Monitor service.
  b. Open a DOS command window and navigate to the folder C:\Program Files\Cisco\Desktop\bin.
  c. Type **slapd.exe -f slapd.conf** and press Enter.
  d. If it aborts, use the resulting error messages to diagnose the problem.
  e. If it runs successfully, press Ctrl+C to end it.
- Check the LDAP Monitor service configuration file to make sure it is starting slapd.exe correctly.

**Problem** Clients are unable to connect to the LDAP service.

**Solution** Some solutions:

- The wrong IP addresses are set for LDAP Host 1 and/or LDAP Host 2 in the registry.
- The LDAP Monitor service is not running. Start it.

- Check if slapd.exe is running. If it is not running, follow the troubleshooting steps for this problem.
- The LDAP database is corrupted. Follow the steps outlined in "Corrupted Directory Services Database" on page 43.

**Problem** Clients do not find the same information from LDAP after failing over from one LDAP to the other.

**Solution** Some solutions:

- Ensure replication is set up correctly in the CAD Configuration Setup utility. For more information, see the *Cisco CAD Installation Guide*.
- Check that registry entries for LDAP Host 1 and 2 on both CAD services computers are the same and contain the right information.
- Check that slapd.conf on both CAD services computers are correct and reference each other.
- If all else fails, follow the steps outlined in "Out of Sync Directory Services Databases" on page 44.

**Problem** The database directory contains many log files that are consuming a large amount of disk space. The rate of accumulation depends on the number of updates made to LDAP. For example, 10,000 updates consume approximately 25 MB. Log file names have the format log.0000001.

**Solution** Restarting LDAP Monitor service on a regular basis will remove log files.

**Problem** After shutting down Directory Services replication, the LDAP Host registry entries on the clients are not automatically updated.

**Solution** Update the LDAP Host 1 registry entry on each client to reflect the correct server location. Clear the other LDAP Host registry entries.

**Problem** After shutting down Directory Services replication, the Secondary Location field on the CAD-BE Servers window in CAD Configuration Setup remains populated.

**Solution** Run CAD Configuration Setup to access the CAD-BE Servers window. Ensure that the correct location is entered in the Primary Location field. Clear the Secondary Location field.

**Problem** SQL Server replication is not functioning.

**Solution** It is possible that, during Unified CCE installation, Cisco Security Agent shut down the SQL Server Browser service and the SQL Server Agent service in the process of hardening the system. This results in the SQL databases in a high availability system not being able to find each other so replication can occur. To resolve the problem, use the Windows Services utility to start the SQL Server Browser service and the SQL Server Agent service.

## Login and Logout Problems

**Problem** The agent is logged out unexpectedly.

**Solution** Possible reasons are:

- Another agent with the same ID or extension has logged in, causing the first agent to be logged out.
- A supervisor has logged the agent out.
- The telephony service has failed.
- The network has failed.
- The phone has restarted.

**Problem** The agent cannot log back into Agent Desktop after failover. The agent's PC is connected to the agent's IP phone, which is connected to the LAN. The PC and the phone are on the same subnet.

**Solution** Due to this specific configuration, Agent Desktop is missing queryagentstateconf and agentstateevent after failover. An attempt to log back into Agent Desktop by clicking the Login button will fail. The agent must restart Agent Desktop and then log in.

**Problem** Agents can't log into Agent Desktop.

**Solution** During Unified ICM installation, an "Agent Login Required for Client Events" check box is displayed. By default this check box is unchecked. It must remain unchecked for agents to be able to log in. If the check box was checked during Unified ICM installation, you must reinstall Unified ICM and make sure the check box remains unchecked.

**Problem** Users cannot log into a CAD application. The error message, "Could not connect to the Cisco CTI OS server" is displayed. Some other possible

error messages are: “The Cisco IPCC Enterprise CTI Server is offline.” and “Cannot connect to BIPPA Service.”

**Conditions**: The Unified ICM server’s firewall is enabled.

**Solution** Exceptions must be made in the Unified ICM server’s firewall in order for the CAD applications to connect. This can be done through the use of a utility called ICMfwConfig, which is located on the Unified ICM installation CD. This utility allows all traffic from Unified ICM/IPCC applications through the firewall by adding the appropriate ports and applications to the firewall exception list. Use of this utility is documented in the *Security Best Practices Guide for ICM and IPCC Enterprise*.

---

**Problem** The agent is unable to log in. The agent sees an error message after clicking OK on the Login dialog that indicates the likely cause of login failure. CAD-BE log also shows “CADBE3003: Unable to login agent. Cause <error code:error description >.”

**Solution** For invalid agent ID/name and/or password:

- Wrong agent ID/name and/or password was entered. Try again and enter the correct information. You may want to reenter the agent password in Unified ICM to be sure you have the right password.
- The agent was configured correctly in Unified ICM but the Sync service has not synchronized CAD's LDAP database to Unified ICM. Make sure the Sync service is running. In Desktop Administrator, manually synchronized Directory Services. Then check whether the agent exists in Desktop Administrator under the Personnel node.

For invalid phone configuration (regular agent):

- Wrong phone extension was entered. Try again and enter the correct information.
- Make sure the phone is associated with the PG user on Unified CM if is logging in as non-mobile agent.
- Phone is not pointing to right Unified CM.
- Non-mobile agent is using CTI port instead of extension.

For invalid phone configuration (mobile agent):

- Make sure the extension is a valid CTI port configured in Unified CM and Unified ICM that is not currently used by someone else.

- The mobile phone number may need to include access codes, area codes, and accounting codes depending on how the dial plan on Unified ICM and/or Unified CM is configured.

For mobile agent mode that does not match agent desk settings:

- Agent is not set up in Unified ICM as a mobile agent. Change agent desk setting in Unified ICM to appropriate mobile agent setting.
- Agent desk settings in Unified ICM may not match call mode selected in CAD-BE. Select the same call mode as specified in Unified ICM agent desk setting.

For no team found for agent:

- Agent does not belong to a team in Unified ICM. Associate the agent with a team in Unified ICM.
- The agent was configured correctly in Unified ICM but the Sync service has not synchronized CAD's LDAP database to Unified ICM. Make sure the Sync service is running. In Desktop Administrator, manually synchronize Directory services, then check if the agent exists and belongs to the correct team in Desktop Administrator under the Personnel node.

For CTI service that is offline:

- Make sure the CTI service is running and active again.
- The CTI service hostname/IP address specified in CAD Configuration Setup is incorrect. Enter the correct values in CAD Configuration Setup, save your changes, then restart the BIPPA service.

For invalid state change:

- The agent is attempting to log in using a phone that is on a call. Finish the call and log in when there is no call on the phone.

For CTI request timeout:

- The BIPPA service, CTI service, or Unified CM may be slow. Check their CPU usage.
- The network may be slow.

For LRM service that is down:

- Start the LRM service if it is down.
- The LRM service will not become active until CAD Configuration Setup runs successfully. Complete CAD Configuration Setup.

- Desktop Administrator, Agent Desktop, or Supervisor Desktop was installed on the same computer as the CAD services. They clear a registry key (IOR Hostname under Site Setup) required by the BIPPA service. Set the registry to the IP address of the CAD services computer.

For no more licenses:

- Wait a few minutes and retry.
- CAD-BE agents may have exited their browsers without logging out first. Those sessions will continue to use up licenses for one minute after the browser exited.
- Agents logged out of extension mobility without logging out from Agent Desktop, CAD-BE, or IP Phone Agent. These agents are still logged in but in a Not Ready state. Agent Desktop will continue to use the license until the application exits. IP Phone Agent will continue to use the license until the BIPPA service is restarted or the agents log in again and log out properly. CAD-BE will continue to use the license until CAD-BE logs out or one minute after the CAD-BE browser is closed.

For a forced login that does not work:

- The agent is using an agent ID that is already logged in on another extension, or using an extension that is already logged in with a different agent ID. Forced logins work only for the same ID/extension pair. Use a different agent ID or extension, or find the other user and have that user log out.

## Macro Problems

**Problem** While running Agent Desktop, the error message, “Macro file failed to open,” keeps appearing.

**Solution** Turn off any virus scanning applications on the desktop. Virus scanning applications attempt to intercept calls to open a file to do their own processing first. This can cause the file to be opened in such a way that restricts other applications from opening the file.

**Problem** There are four actions assigned to an event, but only the first two run.

**Solution** When executing a set of actions, execution is halted if any of the actions fail. This is because some actions may depend on previous actions executing correctly. Find out why the third action is failing and correct it.

**Problem** The keystroke macros do not play back correctly on dropped events.

**Solution** If Agent Desktop is running in normal mode (maximized when a call is received, and minimized when there are no call appearances), keystroke macros may play back to the wrong window. When Agent Desktop minimizes after a call is dropped, it steals focus from the target keystroke macro window. To fix this, place a [Delay]<milliseconds> command at the beginning of the keystroke macro. This allows time for Agent Desktop to minimize before playing back the keystroke macro. For example:

[DELAY] 1000
[APPLICATION:NOTEPAD=UNTITLED - NOTEPAD]

**Problem** Macros are not playing back correctly.

**Solution** When playing keystrokes to a window, Agent Desktop must first find the window. When recording the macro, Agent Desktop saves the window’s

title and class name (an internal Windows variable associated with a window). On playback, Agent Desktop searches in this order:

1. Find a window with the saved title and class name.
2. Find a window with the saved class name.
3. Find a window with the saved title.

If Agent Desktop does not find a window matching one or more of these criteria, it displays an error message.

If there are two windows with the same name and class, Agent Desktop may play back the macro to the incorrect window.

If there are several windows with the same class name, and the title of the target window has changed, Agent Desktop may play back the macro to the incorrect window.

Some compilers/class libraries use the same class name for all windows. If you have developed an in-house application, you may need to change the class name in your application.

**Problem** A keystroke macro will not play back even though the target application is running.

**Solution** Agent Desktop uses the application's class name and title to find the target application. Some applications change title and class name when changing screens. If this happens, Agent Desktop may not be able to locate the target application. Try using just the window title or class name to find the target application.

**Example 1**: Find both the title (NOTEPAD) and class (UNTITLED - NOTEPAD).
[APPLICATION:NOTEPAD=UNTITLED - NOTEPAD]
[SHIFT] D
et cetera.

**Example 2**: Find just the class (NOTEPAD):
[APPLICATION:NOTEPAD=]
[SHIFT] D
et cetera.

**Example 3**: Find just the title (UNTITLED - NOTEPAD):
[APPLICATION:=UNTITLED - NOTEPAD]
[SHIFT] D
et cetera.

**Problem** The administrator created a macro and put in some delays. Now the PC appears to lock up while the macro runs.

**Solution** When a macro runs, the operating system takes over the PC and locks out all user input. This is a characteristic of the operating system. Try to minimize the length of time your macro runs.

**Problem** A keystroke macro plays the wrong keys to the wrong window.

**Solution** Make sure macro playback starts from the same place every time it runs. Have the macro start from the same starting window with the cursor in the same starting position as when the macro was recorded.

**Problem** After a macro runs, focus remains on the application to which it played. How can the macro be written to make it change focus to Agent Desktop (or some other application)?

**Solution** To change focus to Agent Desktop, edit the macro and insert this line at the end:

[APPLICATION:AGENT_DESKTOP=AGENT_DESKTOP]

You can also change focus to an application other than Agent Desktop. To determine the line to insert, create a dummy macro and play a few keystrokes to the application. When you finish recording, cut and paste the application's text identifier from the dummy macro to the macro you wish to edit.

**Problem** Sometimes when a macro is running, the PC appears to lock up for short periods of time.

**Solution** A [DELAY] statement in a macro causes the system user-input hook to keep control of the system. The PC runs but rejects all user input until the macro finishes playing. To limit this problem, use the shortest delays possible.

**Problem** The agent pressed Ctrl+Alt+Del while a macro was running, and now the Agent Desktop window is locked up.

**Solution** You cannot click Start or press Ctrl+Break, Ctrl+Esc, or Ctrl+Alt+Del when running a macro. The Windows operating system unhooks the system keyboard hook when Start is pressed.

**Problem** The administrator cannot get a rule to work based on an internal extension number.

**Solution** When Agent Desktop compares the telephone numbers, if the dial string number format includes a leading x, then the telephone numbers in the list must also include a leading x.

**Problem** An action that launches an external application is not working correctly.

**Solution** Sometimes the operating system can be confused by spaces in directories and file names. If you have an application such as C:\Program Files\Acme\Search Database.exe /t/x. you may need to add quotes around the directory and executable. For example, the above would be “C:\Program Files\Acme\Search Database.exe” /t/x

## Phone Book Problems

**Problem** The only phone book appearing on the dial pad dialog box is the recent call list.

**Solution** The administrator disabled the phone books.

**Problem** Global phone books appear but there is no personal phone book.

**Solution** The administrator disabled personal phone books.

**Problem** When editing a phone book, the agent can't add an entry after editing the first name, last name, or notes.

**Solution** The agent must enter a phone number before the Add button is enabled.

**Problem** The agent can edit the personal phone book, but not other phone books.

**Solution** The personal phone book is not shared by other agents. The other phone books are shared, and can be edited only by the administrator.

# Recording, Monitoring, and Playback Problems

**Problem** Desktop monitoring fails for agents who use Agent Desktop on their local LAN and also need to connect to another LAN via VPN.

**Solution** Desktop monitoring fails if a VPN connection is active. CAD assumes that, if the VPN connection is active, then Agent Desktop is using it. As a result, CAD looks for RTP packets from the VPN connection rather than from the IP phone.

To resolve this issue, use SPAN-based monitoring for agents who must use VPN in addition to Agent Desktop.

**Problem** The Recording & Playback service is not recording the audio file.

**Solution** Check the following:

- If SPAN-based monitoring/recording is being used, make sure that a SPAN port has been created on the switch for the PC's network port where the VoIP Monitor service is connected.
- Make sure that the Recording & Playback service has permission to write to the AudioFiles directory.
- If the audio files are saved on a drive using the FAT32 file system, there is a limitation of 21,844 objects in the folder. If the folder has reached this limit, delete unused audio files, or convert the drive to the NTSF file system.

To check the user of the service, open the Services control panel. Double-click Administrative Tools and then Services. Search for the service named Recording & Playback service and click Startup. Account should be selected and a domain account given along with the password.

**Problem** When monitoring an agent's customer contact, nothing can be heard, and after 15 seconds, an error message is received that no packets are being received. Attempting to record an agent's customer contact

results in an empty recording. The agent's desktop is monitored using desktop monitoring.

**Solution** The following device settings are required for desktop monitoring to function correctly with CAD.

**NOTE**: Not all devices or Unified CM versions use all these settings. Configure those that do appear for your device and Unified CM version.

In Unified CM Administration, in the Product Specific Configuration section of the Device Configuration screen, configure these settings:

- PC Port—Enabled. If the PC Port is not enabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.
- PC Voice VLAN Access—Enabled. If the PC Voice VLAN Access is not enabled, no voice streams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.
- Span to PC Port—Enabled. If the Span to PC Port is not enabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

In the Device Information section of the Device Configuration screen, configure this setting as follows:

- Device Security Mode—Non-Secure or Authenticated. If the Device Security Mode is set to Encrypted, the voice streams can be seen but will not be converted correctly, causing the speech to be garbled.

You must also configure the agent phones to use the G.711 or G.729 codecs. Other codecs, such as G.722, are not supported for silent monitoring and recording.

---

**Problem** The CPU usage on the VoIP Monitor service PC has gone to 99%, and the PC has locked up.

**Solution** This can happen when you disable the sniffing adapter through the Windows Network and Dialup Connections window while the VoIP Monitor service is running. Re-enabling the sniffer adapter while the VoIP Monitor service is running will not solve the problem. You must stop the VoIP Monitor service, re-enable the sniffer adapter, and then restart the VoIP Monitor service to restore normal functionality.

**Problem** The message, "At least one or more errors occurred during synchronization" appeared when the administrator performed synchronization in Desktop Administrator.

**Solution** Check the Sync service log file. If the logged error points to Unified ICM database ODBC connection failure, then make sure that:

- The user account that the Sync service is running has privileges to open a Name Pipe connection (if Named Pipes are being used).
- If the logged error was "...could not prepare SQL statement" then verify that the following LDAP key for Unified ICM has a value: LCC; Servers; SvrType = Switch CTI Server; appName = Setup; sectName = Server Parameters; keyName = PeriphID.
- If the logged error points to LDAP connection failure, then make sure that the LDAP service is running and that the LDAP_HOSTA registry setting in HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\Site Setup has the correct value.

**Problem** Voice traffic generated by Desktop Monitoring, the VoIP Monitor service, and the Recording & Playback service is not tagged for QoS (quality of service).

**Solution** Winsock QoS is disabled for Windows XP and Server 2003 by default, and must be enabled through the Windows registry.

Follow these steps to enable the QoS Setting for the VoIP Monitor service on Windows XP or Windows Server 2003:

If you are running Windows XP or Windows Server 2003:

1. In the Registry Editor, access the key

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

1. On the Edit menu, point to New, and then choose DWORD Value.
2. Type **DisableUserTOSSetting** as the entry name, then press Enter.

   When you add this entry, the value is set to 0 (zero). Do not change the value.
3. Quit Registry Editor, and then restart the computer.

**Problem** The VoIP Monitor service fails with the following exception when using server-based monitoring:

FATAL FCVMS112 splk_pcap_open_live() failed. errorBuf = Error opening adapter: Access is denied.

Conditions: A second NIC is installed/enabled on the server. CAD Configuration Setup (PostInstall) is run to detect the second NIC and then the VoIP Monitor service is restarted.

**Solution** The splkpcap driver must be reinitialized. To do this, unload and reload the driver. Open a command window on the computer where the new NIC was installed and type the following commands:

```
net stop spcd
net start spcd
```

Close the command window and start CAD Configuration Setup. In the VoIP Monitor Service window, select the IP address of the new NIC and save the changes.

**Problem** The supervisor starts recording an agent's conversation, but after a short time the recording stops by itself.

**Solution** Check to make sure that no other supervisors are currently viewing the same team of agents. Any supervisor using Supervisor Desktop can see all conversations being recorded, and can stop a recording of an agent conversation even if that supervisor did not initiate the recording.

For additional troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP*.

**Problem** When the supervisor clicks on an agent (or an agent call) to start monitoring, Supervisor Desktop displays the speaker icon next to the agent but there is no sound.

**Solution** If your system is using CAD-based monitoring, check these things:

- Move the volume slider all the way to the right.
- Verify that the sound card in the PC is working properly.

- Check to see if another application is using the sound card. Some combinations of operating system, sound card, and drivers do not support multiple users.
- Verify that the agent is on a call, and is talking.

If your system is using CAD-based monitoring with SPAN port (server-based) monitoring:

- Verify that the SPAN port on the switch has been configured correctly. If the monitor service has been moved, or new agent IP phones have been added, then you may need to reconfigure the SPAN port.
- Check the Windows NT/2000 application log on the VoIP Monitor service for errors.

If your system is using CAD-based monitoring with desktop (agent-based) monitoring:

- Verify that the PC is connected to the phone in the 10/100 SW port.
- Verify that the agent's PC is connected to the same IP phone that the agent is logged into.
- Verify that the agent's PC uses a NIC that is fully NDIS-compliant (for a procedure to test if a NIC is NDIS-compliant, see http://www.cisco.com/en/US/customer/products/sw/custcosw/ps427/prod_tech_notes_list.html).
- Desktop monitoring does not function with some NICs. The Intel PRO/100 and PRO/1000 NIC series are unable to detect both voice packets and data packets in a multiple VLAN environment, which prevents desktop monitoring from functioning properly. These NICs do not fully support NDIS Promiscuous Mode settings.

If your system is using CAD-based monitoring or Unified CM-based monitoring, a workaround solution is available from the Intel Technical Support website (Solution ID: CS-005897). Other solutions include:

- Using another type of NIC that is fully NDIS-compliant.
- Monitoring agents via a VoIP Monitor service.

The workaround described in CS-005897 may not work for some of the newer Intel PRO/100 and Intel PRO/1000 cards and drivers.

For example, with the Intel PRO/1000 MT network adapter with driver version 8.8.1.0 dated 12/13/2006, the workaround described in CS-005897 does not apply. Instead, each agent desktop must add the VLAN ID of the IP phone that the PC is directly connected to. This is

done in the VLANs tab of the Intel PRO/1000 MT network connection properties page.

The VLAN ID of the IP phone can typically be obtained from the Network Configuration screen on the phone. See the documentation specific to your version of Unified CM and model of IP phone, or your network administrator for more information.

**Problem** The supervisor clicks a recording in Supervisor Log Viewer, but it does not play.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*

**Problem** The system is configured to use Unified CM-based monitoring. The supervisor selects an agent's call, but the Start Voice Monitor button is disabled.

**Solution** Check the following:

- The supervisor is logged into Agent Desktop.
- The supervisor's agent state is Not Ready.
- The call to be monitored is not on hold.
- The agent being monitored is not a mobile agent.
- The Chat service is running.
- The supervisor is not monitoring another call.
- The supervisor is selecting a call to monitor, not an agent. If the Start Voice Monitor button is enabled when the supervisor selects an agent, CAD-based monitoring is being used.
- The supervisor is not already on a call.

For additional troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** The system is configured to use Unified CM-based monitoring. The supervisor clicks the Start Voice Monitor button, but the monitoring call fails to establish. An error message appears in Supervisor Desktop and

an Operation Failure message appears in the supervisor's Agent Desktop.

**Solution** Causes of the problem may be one or more of the following:

- The build-in-bridge on the agent's device is not enabled. The build-in-bridge can be turned on from Unified CM.
- The Monitoring Call Search Space does not include the partition to which the agent's line belongs. The Monitoring Call Search Space can be turned on from Unified CM.
- The monitored device doesn't support Unified CM-based silent monitoring. The supported models are: 7906G, 7911G, 7931G, 7941G, 7941G-GE, 7961G, 7961G-GE, 7970G, and 7971G-GE. IP Communicator is not supported.
- The call is being monitored by another supervisor, or the supervisor is already monitoring another call. A supervisor cannot monitor multiple calls. In this situation, the error message may be "The agent's device doesn't support silent monitoring.", even if the agent's device does support Unified CM-based monitoring.
- The monitored agent's device has security enabled. In this case, Unified CM rejects the monitoring request.
- The PG user is not in the "Standard CTI Allow Call Monitor" user group.

---

**Problem** The system is configured to use Unified CM-based monitoring. The supervisor is monitoring an agent's call. The supervisor starts a conference call by pressing the Confrn button on the IP phone and calling a second supervisor. The second supervisor answers the call, and the first supervisor presses the Confirm button to complete the conference operation.

The first supervisor's IP phone displays the message "To Conference", but the first supervisor's Agent Desktop shows the monitoring call as still in a Connected state. The first supervisor drops the conference call. The first supervisor tries to start monitoring the same call again, and gets the error message "Supervisor has failed to start voice monitor. CTI OS exception on start monitor. PG code 13144."

The first supervisor cannot monitor the same agent call until the second supervisor drops the call.

**Problem** While a recording is in progress, the reported duration of the recording is incorrect.

**Solution** While a recording is in progress, the reported duration is calculated by taking the difference between the current time, which is determined by the server, and the start time, which is specified by the client. If the clocks on the client computer and the server computer are not synchronized, the reported duration will be incorrect. The difference between the reported duration and the correct duration can be significant if the agent is in a different time zone from the server.

When the recording is complete, the start time and end time are both specified by the client, and the reported duration will be correct.

## Supervisor Desktop Problems

**Problem** The ASA (average speed of answer) statistic is not being updated in the real-time displays in Supervisor Desktop.

**Solution** The data for this statistics comes from the ICM Admin Workstation HDS database. If any entries on the following windows in the Agent Desktop Configuration Setup tool were changed, Supervisor Desktop will not be able to retrieve current statistics:

- ICM Admin Workstation Distributor window
- ICM Admin Workstation Database window

If these windows were updated, you must stop and restart each Recording and Statistics service in the system in order for the new information to register properly in Directory services.

**Problem** A supervisor using Windows XP was able to start Supervisor Desktop, but was not able to load a team or display any agent information.

**Solution** Windows XP can be configured so that the Internet Connection Firewall (ICF) is active. ICF acts by keeping track of all traffic to and from the computer; it will only allow information through that has originated from that particular computer. If a message originates from outside the computer, it will be discarded.

To solve this problem, either turn off ICF (requires someone with administrator rights to the computer) or override the defaults to include known “good” connections like the CAD servers.

Open the System control panel. In the System Properties dialog, select the Advanced tab. Click the Environment Variable button and then Add to add OMNIORB_USEHOSTNAME and the IP address to the System Variable list.

**Problem** When the supervisor selects an agent to begin CAD-based monitoring (or an agent phone call to begin Unified CM monitoring), Supervisor Desktop displays the speaker icon next to the call but there is no sound.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** The supervisor cannot log into the VoIP Monitor service, and receives the error “Could not access sound card”.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** The sound quality is poor, and sounds choppy like a motorboat.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** The sound is lagged. There is a noticeable delay between when the agent speaks and when the supervisor hears the sound on the PC sound card.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** The supervisor scrolled the Data View (or Message View) pane sideways to view more information, and the toolbar icons disabled.

**Solution** Click anywhere in the Team View pane to enable the toolbar again.

**Problem** The supervisor clicked the Record button to record an agent conversation and nothing happened.

**Solution** There is no visible message displayed if a recording fails. If nothing happens, assume that the request failed. You will know that a recording succeeds if the icon next to the agent's conversation in the Team View pane changes to the recording icon.

For additional troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP*.

**Problem** The supervisor tried to change an agent's state and nothing happened.

**Solution** There is no visible message displayed if an agent state change request fails. If nothing happens, assume that the request failed. You will know that an agent state change succeeds if the icon next to the agent's name in the Team View pane changes to the current agent state icon.

**Problem** Supervisor Desktop is no longer displaying any skills statistics.

**Solution** The supervisor is also an agent logged into the ACD. If the supervisor is inactive (in the Not Ready state) long enough he or she is logged out of the ACD (the length of Not Ready time before logout is set up in the Agent Desk Settings in Unified ICM.)

The supervisor should log back in to see skills statistics again. A workaround to the logout situation is to create a skill group that has only supervisors in it and that does not receive ACD calls. The supervisors can then place themselves in the Ready state and remain logged in as long as necessary.

**Problem** Supervisor Desktop does not display skills statistics, and Agent Desktop does not display any enterprise data.

**Solution** The hostname or IP address of the Unified ICM CTI Server must be entered identically in Unified ICM and in CAD Configuration Setup. If a hostname is entered in Unified ICM, a hostname must be entered in Configuration Setup. If a hostname is used in one place and an IP

address in the other, then enterprise data and skills statistics are not communicated to CAD.

To correct the problem, find out how the CTI Server is entered in Unified ICM and change how the CTI Server is entered in Configuration Setup.

**Problem** The supervisor clicks a recording, but it does not play.

**Solution** For troubleshooting information about VoIP monitoring and recording, see *Configuring and Troubleshooting VoIP Monitoring*.

**Problem** After completing a conference call, Chat and Supervisor Desktop show an extra party on the call.

**Solution** Occasionally, each agent receives different data from the CTI server. For example, a customer (555-5555) calls Agent A. The CTI server reports 555-5555 as the calling number to Agent A. Agent A then conferences in Agent B. However, in this case the CTI server reports <Unavailable> as the customer number to Agent B. When the time comes to merge the data from the two agents (Agent A, Agent B, customer number, and <Unavailable>) an extra party is added because the customer number and <Unavailable> cannot be distinguished.

**Problem** If the supervisor's hook state changes during a Chat service failure and recovery, the Barge-In and Intercept buttons get out of sync in Supervisor Desktop.

**Solution** Once the supervisor takes another call after the Chat service recovers, the Barge-In and Intercept buttons will display correctly. The problem can also be corrected by restarting Supervisor Desktop.

**Problem** Supervisors are getting randomly logged out of the Chat service.

**Solution** If a supervisor attempts to log into the Chat service with the same ID as another supervisor, the Chat service logs the first supervisor out. To avoid this problem, make sure that each supervisor has a unique ID.

The ID is the extension stored in Phonedev.ini (located in the config folder). Phonedev.ini is populated with the extension field from the Login dialog box when Agent Desktop is started.

**Problem** The supervisor is viewing a blind conference call, but cannot see all parties on the call.

**Solution** In Agent Desktop and CAD-BE, a blind conference is defined as adding an alerting party to a conference. All parties on a blind conference call may not show up in either Supervisor Desktop, CAD-BE, or Agent Desktop. This is a limitation of the CTI server software.

**Problem** When Supervisor Desktop starts, it does not get automatically updated.

**Solution** Automated updates are disabled for Windows Vista. Other options are:

- Manual “over-the-top” installation
- Push installation

**Problem** A supervisor is monitoring an agent’s call and the call ends. The agent’s state continues to appear as talking in the agent title bar.

**Solution** After the agent changes state, the state in the title bar will be updated correctly.

**Problem** The system is configured to use Unified CM-based monitoring. The supervisor selects an agent’s call, but the Barge-in and Intercept buttons are disabled.

**Solution** The supervisor must stop monitoring before doing a barge-in or intercept.

**Problem** The system is configured to use Unified CM-based monitoring. The supervisor is monitoring a call. The Transfer and Conference buttons are disabled in the supervisor's Agent Desktop.

**Solution** Transfer and conference operations are not allowed on a monitoring call.

**Problem** The Agent ACD State Log Display lists two contradictory agent states, such as Talking and Hold, at the same second and in the wrong order.

**Solution** This situation can arise when two events occur in the same second. This is a known issue. No workaround is available.