Cisco CAD Troubleshooting Guide

CAD 8.5 for Cisco Unified Contact Center Express Release 8.5
Cisco Unified Communications Manager Edition

First Published: December 2010
Last Modified: April 25, 2013

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

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

Cisco CAD Troubleshooting Guide

Contents

Contents

Contents

Introduction

1

CAD Documentation

The following documents contain additional information about CAD 8.5:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Documentation Feedback

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

ccbu_docfeedback@cisco.com

We appreciate your comments.

CAD 8.5 Applications

CAD 8.5 includes the following applications:

User Applications

- Cisco Desktop Administrator (Desktop Administrator)
- Cisco Agent Desktop (Agent Desktop)
- Cisco Agent Desktop—Browser Edition (CAD-BE)
- Cisco Supervisor Desktop (Supervisor Desktop)
- Cisco IP Phone Agent (IP Phone Agent, IPPA)

Services

- Cisco Desktop Browser and IP Phone Agent Service (BIPPA service)
- Cisco Desktop Agent E-Mail Service (Agent E-Mail service)
- Cisco Desktop Call/Chat Service (Call/Chat service)
- Cisco Desktop Enterprise Service (Enterprise service)
- Cisco Desktop LDAP Monitor Service (LDAP Monitor service)
- Cisco Desktop Licensing and Resource Manager Service (LRM service)
- Cisco Desktop Recording and Statistics Service (Recording and Statistics service)
- Cisco Desktop Recording Service (Recording service)
- Cisco Desktop Sync Service (Sync service)
- Cisco Desktop VoIP Monitor Service (VoIP Monitor service)
- Directory Services

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)
- Right-clicking the application executable and selecting Properties from the resulting menu

Version information is a series of four numbers separated by periods (for example, 8.5.1.56). From left to right, these represent:

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

CAD Services on Unified Communications Operating System

2

Guidelines for Sizing Deployments

Service capacities vary based on the total number of agents in a contact center and whether or not silent monitoring and recording are required.

For up-to-date component sizing information, capacity and configuration limits, see the Cisco Unified CCX Data Sheet available at the following URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_data_sheets_list.html

CAD Services Autorecovery

Fault Tolerance

CAD 8.5 uses the “warm standby” approach to fault tolerance and autorecovery. No manual intervention is required to recover a failed service.

See "CAD Desktop Applications Autorecovery" on page 37 for more information on how CAD desktop applications reconnect to CAD services during service failure.

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

- Active monitoring is stopped. It 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 IPPA or CAD-BE.

  NOTE: If any (but not all) VoIP monitor service nodes are down, agents and supervisors will see partial service for monitoring and recording. This is because, for SPAN-based recording, all VoIP services are active and are solely responsible for the devices that have been assigned to them in Cisco Desktop Administrator and in the SPAN port configuration on the Catalyst switch. If a VoIP Monitor service is unavailable, then monitoring and recording will be unavailable for those agents in a SPAN-based deployment. Supervisor and agent desktop will reflect this by showing partial service for those features.

CAD uses LDAP replication to provide fault tolerance for configuration information, such as work flows and agent hot seat settings. It uses IBM Informix Database (IDS) for Unified CCX 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.

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

- Agent E-Mail service
- Call/Chat service
- Enterprise service
- LRM service
- Sync service
- Recording and Statistics service
- BIPPA service

BIPPA Service

The BIPPA service pushes an error screen to all agents logged into IP Phone Agent when it detects a failover in Unified CCX. During the time it is unable to communicate with Unified CCX, any attempt to change agent state or perform another IP Phone Agent function returns the service error screen.

Once the BIPPA service is able to reconnect to Unified CCX, it pushes one of the following screens to the agent's phone:

- The Login screen, if the agent in not logged into Unified CCX
- The Skill Statistics screen, if the agent is still logged into Unified CCX

VoIP Monitor Service

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 it is not possible to tell which agents are monitored by which VoIP Monitor service. 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.

Agent E-Mail

Agent E-Mail connects to one Microsoft Exchange server. If the MS Exchange server goes down, then Agent E-Mail will not function. If the MS Exchange server to which Agent E-Mail connects is part of a Database Availability Group (DAG) and any of these servers go down, then Agent E-Mail functionality might be compromised. For more information, see *Understanding Database Availability Groups* at:

http://technet.microsoft.com/en-us/library/dd979799%28v=exchg.141%29.aspx

Command Line Interface Tool and Commands

The Command Line Interface (CLI) tool is used to execute CLI commands on the Unified Communications Operating System. These tools help diagnose and troubleshoot problems with the CAD services.

For detailed information on CLI, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release* 8.5, available at:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Executing CLI Commands

The CLI tool framework automatically loads when the user logs into the Unified Communications Operating System as an administrator.

To execute CLI commands:

1. Log into the Unified Communications Operating System as an administrator. CLI starts.
2. At the admin prompt, type the desired CLI command.

CLI Command Syntax

Table 1 lists CLI command syntax.

NOTE: Pathkey, Key, and Value are mandatory fields and case sensitive. Refer to Table 2 on page 22 for a list of CAD service and application pathkeys.

NOTE: If a key or value contains spaces, enclose the string with double quotes. For example:

set uccx cad prefs SiteSetup "LDAP Host 5" "cal lab.lab.com"

NOTE: All commands are case sensitive.

Table 1. CLI Commands

Command	Example / Description
show uccx cad license usage	Displays the available and used license information.

Table 1. CLI Commands — *Continued*

Command	Example / Description
`help` <command>	Displays the description of the command. Example: help utils service list
utils service list	Displays the status of all services running on the Unified Communications Operating System.
utils uccx dump packets <Capturefile.cap> <Time interval>	Copies active span-based monitoring packets into the specified file. • <Capturefile.cap>: Name of the file into which the packets must be copied. The file must have a CAP extension. • <Time interval>: Captures the packets for the specified time. The value for time interval must be in seconds. **NOTE:** Make sure the time interval specified is less than 180 seconds. If the time interval is longer than 180 seconds, the process continues without stopping, leading to more memory and space usage. Example: utils uccx dump packets capturefile.cap 5
Preferences	
show uccx cad prefs <pathkey>	Displays key value pairs for the specified preferences file. Example: show uccx cad prefs SiteSetup
set uccx cad prefs <pathkey> <key> <value>	Sets the key value pairs with a new value. • Pathkey: Name of the CAD service’s preferences. • Key: The name of the key that you want to set with a new value. • Value: Specify a new value. Example: set uccx cad prefs SiteSetup "LDAP Host 5" 0
Configuration files	

Table 1. CLI Commands — *Continued*

Command	Example / Description
show uccx cad config <pathkey>	Displays configuration file values for the specified CAD service's configuration file. Example: show uccx cad config CTIStorageServer
set uccx cad config <pathkey> <key> <value>	Sets the configuration file value with a new value for the specified CAD service's configuration file. • Pathkey: Name of the CAD service's preferences. • Key: The name of the key that you want to set with a new value. • Value: Specify a new value. Example: set uccx cad config RascalService CallReportIncludesOutbound 1
Debugging log threshold, number, size, and alert preferences	
show uccx cad log <pathkey>	Displays the specified CAD service's log configuration details. Example: show uccx cad log slapd

Table 1. CLI Commands — *Continued*

Command	Example / Description
set uccx cad log <pathkey> <type> <key> <value>	Sets debugging log threshold, number size, and alerts for debug or log files for the specified CAD application. • Pathkey: Name of the CAD service's configuration file. • Type: The type of logging you want to set with the specified key value pairs. The types are debug or log. The additional type xslt can be set only for Bars CLI. • Key: The name of the key you want to set for the log threshold. The keys are Threshold, Size, and Files. **NOTE:** The Threshold key is used only with the debug type. You cannot set the Threshold key for Bars CLI. • Value: The values for Threshold can be one of the following: OFF, DEBUG, CALL, TRACE, and DUMP. The value for Size and Files must be an integer. The value for Alarm must be either Enable or Disable. Examples: Threshold: set uccx cad log LRMService debug Threshold CALL Size: set uccx cad log LRMService log Size 10 File: set uccx cad log LRMService debug Files 25 Alarm: set uccx cad log EEMServerJava log Alarm Enable
Restart, start, and stop CAD services	
utils service restart <CAD service>	Restarts the specified CAD service. Example: utils service restart Cisco Desktop LDAP Monitor Service
utils service start <CAD service>	Starts the specified CAD service. Example: utils service start Cisco Desktop Sync Service

Table 1. CLI Commands — *Continued*

Command	Example / Description
utils service stop <CAD service>	Stops the specified CAD service. Example: utils service stop Cisco Desktop LDAP Monitor Service
Recordings	
show uccx recordings allowed	Displays the maximum amount of disk size allowed for recordings.
show uccx recordings space	Displays the total size of all the recording files.
utils uccx recordings purge <size in MB> <cutoff date>	Deletes the specified size of recording files on or before the cutoff date. No recordings newer than the cutoff date will be purged. • Size in MB: Value must be a positive real number. • Cutoff date: Value can be any recognizable date as specified by the Unix system date command. Examples: utils uccx recordings purge 4.005 10/28/2011 20:56:33 utils uccx recordings purge 50 2 weeks ago
E-mail	
utils uccx eemtables cleanup uid <uid>	Purges e-mail records from the database that contain the specified e-mail UID (UID Mode). <uid>: The unique ID for an e-mail message, corresponding to the emailUIDOnMailServer field in the e-mail tables. These IDs can be obtained by running SELECT queries on the appropriate tables. Example: utils uccx eemtables cleanup uid 206785259 1208664064 -1111623128

Table 1. CLI Commands — *Continued*

Command	Example / Description
utils uccx eemtables cleanup normal <CSQ ID> <cutoff date> <e-mail state>	Purges e-mail records from the database (Normal Mode). All e-mail records meeting the parameters you enter are removed from the database. • <CSQ ID>: All records containing this CSQ ID are purged if other criteria are met. This must be an integer. • <cutoff date>: Any recognizable date as specified by the Informix Date command. All e-mail records are purged up to, but not including, the cutoff date. • <e-mail state>: Optional. If this parameter is not given, the command behaves as if the parameter ALL is used. The options are as follows: queued: use for e-mail statuses In Queue Waiting, Transferred, Requeued, and PeerReview. Assigned: Use for e-mail statuses In process at agent and In draft at agent Resolved: Use for e-mail statuses Pending Delete, Sent, and Deleted All: Use to select all e-mail statuses. Example: utils uccx eemtables cleanup normal 15 9/16/2010 all
LDAP utilities	
utils uccx ldap recover	Recovers the LDAP database from an inconsistent state.
utils uccx ldap archive	Displays the path of LDAP transaction log files that are currently not used.
utils uccx ldap stat	Displays the statistics of the LDAP database.
utils uccx ldap checkpoint	Inspects and clears all LDAP database transaction logs and exits.
utils uccx ldap index	Regenerates the LDAP service indices based on the current LDAP database. Stop the LDAP service in the Unified CCX Serviceability page before executing this command.

Table 1. CLI Commands — *Continued*

Command	Example / Description
utils uccx ldap search <base DN value> [filter] [attribute]	Displays information from the specified directory name in LDAP. • Base DN value: The directory name. • Filter and attribute: Optional. Filters the specified directory name by these criteria. Example: utils uccx ldap search "ou=Agents,lcc=Call Center 1,ou=Company,o=Calabrio Communications" "empID=dactuser1"
utils uccx ldap add <ldifFile>	Adds, modifies, or deletes entries in the LDAP database according to the format in the specified LDIF file. • <LDIF File>: The LDIF file name. Stop the LDAP Monitor service in the Cisco Unified CCX Serviceability page before executing these commands. Examples: utils uccx ldap add adp_add.ldif utils uccx ldap modify ldp_mod.ldif utils uccx ldap delete cdp_del.ldif
utils uccx ldap modify <ldifFile>	
utils uccx ldap delete <ldifFile	
utils uccx ldap cat <ldifFile>	Copies all LDAP contents into the specified LDIF file. • <LDIF File>: The LDIF file name. Stop the LDAP Monitor service in the Unified CCX Serviceability page before executing this command. Example: utils uccx ldap cat ldp_list.ldif

Table 1. CLI Commands — *Continued*

Command	Example / Description
utils uccx ldap modrdn [add] [file <ldifFile>] | [DN RDN]	Modifies the specified relative directory name in the LDAP database. • add: Optional. Adds a new relative directory name in LDAP. If this option is not specified, it replaces the existing directory name with the new one. • file <ldifFile>: The LDIF file name. The LDIF file must contain two lines, where: The first line contains the existing directory name The second line contains the new relative directory name Or DN RDN: DN is the existing directory name and RDN is the new relative directory name. You must provide parameters to either the [file <ldif file>] or DN RDN fields. Example: utils uccx ldap modrdn file /tmp/ldap_add.ldif

Preferences and Configuration Files

Table 2 lists the pathkeys used by CAD services to view and edit debugging log thresholds, setup preferences, and configuration files. See "Preferences" on page 24 for information on the list of key value pairs for the particular preferences.

Table 2. Preferences files

CAD services/applications	Pathkey
Debugging log threshold, number, and size preferences, and Configuration files	
Bars CLI	BarsCLI
Cisco Desktop Browser and IP Phone Agent Service	BIPPAService
Cisco Desktop Call/Chat Service	ChatService
Cisco Desktop Enterprise Service	CTIStorageService
Cisco Desktop Sync Service	DirAccessSyncService
Cisco Desktop Agent E-Mail Service	EEMService, EEMServerJava

Table 2. Preferences files

CAD services/applications	Pathkey
Cisco Desktop IP Phone Agent Service	IPPAClientServlet
Cisco Desktop LDAP Monitor Service	LdapMonitorService
Cisco Desktop License and Resource Manager Service	LRMService
Cisco Desktop Recording and Playback Service	RecordingPlaybackService
Cisco Desktop Recording and Statistics Service	RascalService
Cisco Desktop LDAP Service	slapd
Cisco Desktop VoIP Monitor Service	VoIPMonitorService
Cisco Desktop Administrator	WebAdmin, WebAdminLib
Preferences	
SiteSetup	SiteSetup
Cisco Desktop Browser and IP Phone Agent Service	BIPPAConfig
Cisco Desktop Enterprise Service	EnterpriseServiceSetup EnterpriseServiceConfig
Cisco Desktop Recording and Playback Service	RecordingPlaybackClientSetup RecordingPlaybackServiceConfig
Cisco Desktop Recording and Statistics Service	RecordingPlaybackServiceSetup
Cisco Desktop VoIP Monitor Service	VoIPMonitorClientSetup VoIPMonitorClientConfig VoIPMonitorServiceConfig

Technical Package Information

Service Connection Types and Port Numbers

Consult the *Cisco Unified CCX (IP IVR and IPCC Express) Port Utilization Guide* for a complete listing of ports and connection types used in CAD 8.5.

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Preferences

Preferences are CAD-specific settings that are put in place when the CAD services are installed on the Unified Communications Operating System. Preferences files contain key value pairs, where <key>=<value>. An example of a key value pair is IOR HOSTNAME=10.19.25.50.

You can view and modify key value pairs by connecting to the Unified Communications Operating System using the CLI tool and executing the appropriate CLI commands. CLI commands listed in this section are only to view key value pairs of preferences files. See "Command Line Interface Tool and Commands" on page 15 for more information on CLI commands to view and modify key value pairs.

SiteSetup

```
show uccx cad prefs SiteSetup
```

Table 3. SiteSetup key values

Pathkey	Key	Description
SiteSetup	APP VERSION	Used by installation scripts to identify the version of the service software.
	CALLCENTERLANG	Language selected during installation.
	DEPLOYTYPE	Defines the Unified CM type.
	INSTALL DIRECTORY	Base install directory for Cisco software.
	INSTALLDIR	Parent directory of base install directory for Cisco software.
	IOR HOSTNAME	Hostname or IP address of the computer’s NIC. Its value is only present on the CAD services computer.
	LDAP Heartbeat Enabled	Is heartbeat enabled? 1=yes, 0=no. Default = 1.

Table 3. SiteSetup key values — *Continued*

Pathkey	Key	Description
SiteSet up	LDAP Bind DN	User ID used to log in to the LDAP service. Default = cn=Client, ou=People, o=Calabrio Communications.
	LDAP Connection Timeout	Maximum time, in seconds, before a connection attempt times out. Default = 15.
	LDAP Heartbeat Retry Time	Heartbeat time, in milliseconds.ƒn Default = 10000.
	LDAP Host 1	LDAP service hostname/IP address. There can be multiple LDAP hosts.
	LDAP LCC	Default logical contact center
	LDAP Port 1	LDAP service port. There can be multiple LDAP ports. Default = 38983.
	LDAP Pwd	Encrypted user password
	LDAP Recovery Retry Time	Recovery retry time, in milliseconds. Default = 3000.
	LDAP Request Timeout	Maximum time, in seconds, before an LDAP request times out. Default = 15.
	LDAP Root	Root of the LDAP data. Default = o=Calabrio Communications.
	MONITOR DEVICE	Network card on which to sniff packets.
	Serial Number	Counter to indicate changes to site setup values. Default = 0.
	LASTLANGDATE	Synchronizes both servers with the latest updated language.

BIPPA

```
show uccx cad prefs BIPPAConfig
```

Table 4. BIPPAConfig key value

Pathkey	Key	Description
BIPPAConfig	TOMCAT HOME	Location of the Tomcat web server files. Default = /usr/local/thirdparty/jakarta-tomcat

Enterprise Service

Execute the following CLI commands:

- `show uccx cad prefs EnterpriseServiceSetup`
- `show uccx cad prefs EnterpriseServiceConfig`

Table 5. EnterpriseService key values

Pathkey	Key*	Description
EnterpriseService Setup	Max Wait Time	Maximum time, in milliseconds, to wait for enterprise data. Default = 100.
	Initial Time	Number of milliseconds to wait after the first request for enterprise data, if data is not guaranteed. Default = 10.
	Increment	Number of milliseconds to add to the retry time at each interval, if data is not guaranteed. Default = 20.
	Retry Sleep Interval	Number of milliseconds used to calculate the interval for retry attempts, if call is not known to enterprise. The interval is calculated by (retry sleep interval × retry attempt). Default = 150.
EnterpriseService Config	JavaClassPath	Lists jar files required by the Agent E-Mail service Java engine. Default: “log4j.jar,SplkStd4J.jar; EEM.jar;activation.jar;mail.jar”
	JavaHome	The path to the Java virtual machine that will be used for starting the E-Mail service Java engine. Default: “C:\Program Files\Java\jre1.6.0_24”
	JavaVMArguments	Additional arguments for the Java virtual machine. Default: "" (empty string)

* These key values need to be created only if there are timing issues when an agent requests data from the Enterprise service and the Enterprise service does not have the data yet. Use the set uccx cad prefs <pathkey> <key> <value> CLI command to create the key values. See "CLI Command Syntax" on page 15 for more information.

Recording & Playback Client

```
show uccx cad prefs RecordingPlaybackClientSetup
```

Table 6. RecordingPlaybackClient key values

Pathkey	Key	Description
RecordingPlaybackClientSetup	From Client Port	The port on the supervisor's desktop that is used to receive the "From Agent" audio stream for playback sessions.
	Jitter Buffer	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	End of range of port numbers to use for recording. Each simultaneous recording requires two ports.
	Port Range Start	Start of range of port numbers to use for recording. Each simultaneous recording requires two ports.
	Sound Buffers	The number of buffers used to hold audio data sent to the sound card. Default value = 30 ms. If sound quality is bad, increasing this number might improve the quality.
	To Client Port	The port on the supervisor's desktop that is used to receive the "To Agent" audio stream for playback sessions.
	VPN Port	The port used by the Recording service for its VPN address service that client applications use 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 service.

Recording & Playback Service

Execute the following CLI commands:

- `show uccx cad prefs RecordingPlaybackServiceSetup`
- `show uccx cad prefs RecordingPlaybackServiceConfig`

Table 7. RecordingPlaybackService key values

Pathkey	Key	Description
RecordingPlaybackServiceSetup	Maximum Playbacks	Maximum concurrent playbacks
	Maximum Recordings	Maximum concurrent recordings
	OmniOrbUsePort	The CORBA port on which the Recording service listens for client requests.
	VPN Port	The port on which the Recording 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.
RecordingPlaybackServiceConfig	Audio Directory	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.

VoIP Monitor Client

```
show uccx cad prefs VoIPMonitorClientConfig
```

Table 8. VoIPMonitorClientConfig key values

Pathkey	Key	Description
VoIPMonitorClientConfig	FROM AGENT PORT	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	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	Host name of the VoIP service.
	SOUND BUFFERS	Number of sound card buffers. Default = 30; minimum is 3. If the monitor sound quality is choppy, stuttering, or like a motorboat you might be able to make it sound better by adjusting this value higher. Setting the value higher increases the sound lag, and might cause a slight stutter at the beginning of a monitor session.
	TO AGENT PORT	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 Record Client (Optional)

These preferences key value pairs should not be needed because the VoIP Monitor API has built-in defaults. They can be used to override the defaults.

```
show uccx cad prefs VoIPMonitorClientSetup
```

Table 9. VoIPMonitorClientSetup key values

Pathkey	Key	Description
VoIPMonitorClientSetup	Recording Jitter Buffer	The number of milliseconds that a packet expires for recording.
	Recording Port Range Start	The starting port number for receiving UDP packets for recording.
	Recording Port Range End	The end port number for receiving UDP packets for recording.

VoIP Monitor Service

```
show uccx cad prefs VoIPMonitorServiceConfig
```

Table 10. VoIPMonitorServiceConfig key value

Pathkey	Key	Description
VoIPMonitorServiceConfig	App Version	Used by installation scripts to identify the version of the service software. The service itself does not use this entry.
	Update Version	Future use: tracks any hot fixes installed.
	Monitor Device	Network card on which to sniff packets.

Troubleshooting

Services

Restarting Services

If you have to stop the services, you can restart them in any order through the Unified CCX Administration application.

Service Names/Executables

See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 to verify whether a CAD service is running.

Table 11. Service names and executables

Service name as shown in Services Control Panel	Executable
Cisco Desktop Browser and IP Phone Agent Service	IPPASvr.exe
Cisco Desktop Agent E-Mail Service	EEMServer.exe
Cisco Desktop Call/Chat Service	FCCServer.exe
Cisco Desktop Enterprise Service	CTIStorageServer.exe
Cisco Desktop LDAP Monitor Service	LDAPmonSvr.exe, slapd.exe
Cisco Desktop Licensing and Resource Manager Service	LRMServer.exe
Cisco Desktop Recording and Statistics Service	FCRasSvr.exe
Cisco Desktop Recording Service	RPServer.exe
Cisco Desktop Sync Service	DirAccessSynSvr.exe
Cisco Desktop VoIP Monitor Service	FCVoIPMonSvr.exe

CAD License Usage

CAD licenses are categorized as seat, Desktop Administrator, Desktop Work Flow Administrator, and recording licenses.

Each agent logging into Agent Desktop, Supervisor Desktop, CAD-BE or IPPA consumes one seat license. The license is available to another agent only after the CAD application is closed.

Desktop Work Flow Administrator and Desktop Administrator come with one license each, so only one person can view and/or edit data in them at any one time. However, more than one instance can be open concurrently.

> **NOTE:** If Desktop Administrator is inactive for more than 15 minutes, the current user is logged out and another user can then log in and view/edit data.

Each Standard seat license provides for the concurrent operation of:

- IP Phone Agent
- Supervisor Desktop
- Desktop Administrator[1]
- Work Flow Administrator[1]

Each Enhanced or Premium seat license provides for the concurrent operation of:

- Agent Desktop, IP Phone Agent, or CAD-BE
- Supervisor Desktop
- Desktop Administrator[1]
- Work Flow Administrator[1]

Recording license is used whenever a supervisor or agent triggers the recording function, and is released when the recording is stopped. A license is also used whenever a supervisor opens the Supervisor Record Viewer, and is released when the Supervisor Record Viewer is closed.

The CLI command can be executed to view the IP addresses of clients that are consuming desktop seats or are running Desktop Administrator or Work Flow 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 Desktop Administrator, the IP address is the IP address of the CAD server.

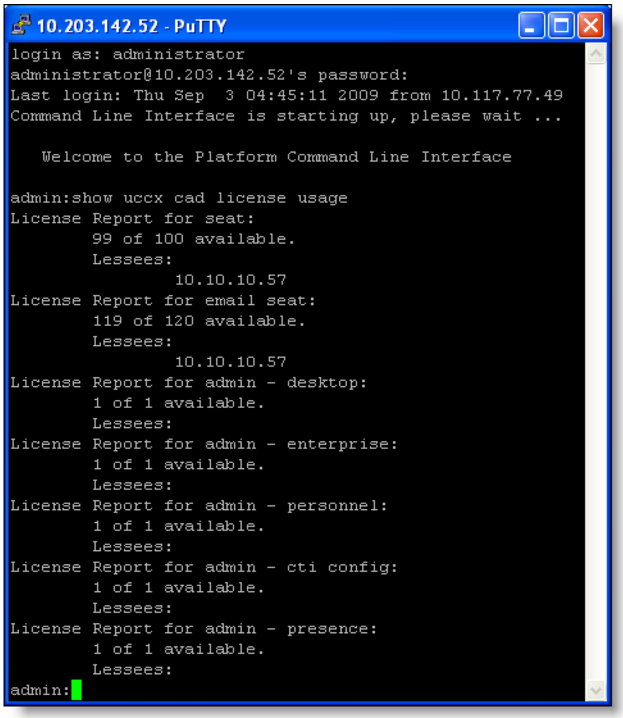
[1] Only one administrator can view and/or edit data in Desktop Administrator and Work Flow Administrator at any one time.

To view license usage:

1. Start CLI. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System.
2. At the admin prompt, execute the CLI command `show uccx cad license usage`. The command displays the available and used license information (Figure 1).

   NOTE: It might take a few seconds to retrieve the license details.

Figure 1. show uccx cad license usage command results



```
login as: administrator
administrator@10.203.142.52's password:
Last login: Thu Sep  3 04:45:11 2009 from 10.117.77.49
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

admin:show uccx cad license usage
License Report for seat:
        99 of 100 available.
        Lessees:
                10.10.10.57
License Report for email seat:
        119 of 120 available.
        Lessees:
                10.10.10.57
License Report for admin - desktop:
        1 of 1 available.
        Lessees:
License Report for admin - enterprise:
        1 of 1 available.
        Lessees:
License Report for admin - personnel:
        1 of 1 available.
        Lessees:
License Report for admin - cti config:
        1 of 1 available.
        Lessees:
License Report for admin - presence:
        1 of 1 available.
        Lessees:
admin:
```

Entries in the command window are described in Table 12.

Table 12. show uccx cad license usage result headings

Result Heading	Description
seat	Lists users of Cisco Agent Desktop, Cisco Agent Desktop—Browser Edition, Cisco IP Phone Agent, and Cisco Supervisor Desktop.
email seat	Lists users of Cisco Agent Desktop who are using the Agent E-mail.

Table 12. show uccx cad license usage result headings

Result Heading	Description
admin - desktop	Lists users of Cisco Work Flow Administrator.
admin - enterprise	Not used in this version.
admin - personnel	Not used in this version.
admin - cti config	Not used in this version.
admin - presence	Lists users of Cisco Desktop Administrator.

Recovering the LDAP Services Database

Corrupted LDAP Services Database

Possible indicators that the LDAP database is corrupted include the following:

- You cannot log in to Cisco Agent Desktop with a valid user ID and password.
- When CAD Configuration Setup is run on the server, some nodes are blank instead of showing connection information.
- When starting CAD desktop applications, you receive error messages indicating errors in connecting to Directory Services.

If restarting the LDAP Monitor service does not resolve this problem, it is likely that the LDAP database is corrupted.

To recover the LDAP Services database if corrupted:

1. Stop the LDAP Monitor service. See "Changing CAD Services Status" on page 65 for information on stopping services.
2. Start CLI. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System.
3. At the admin prompt, execute the following commands:
   - `utils service stop Cisco Desktop LDAP Monitor Service`
   - `utils uccx ldap recover`
   - `utils service start Cisco Desktop LDAP Monitor Service`

   NOTE: After the utils uccx ldap recover command is run to restore the database to a consistent state, all committed transactions will be present, but any uncommitted transactions will be lost. A high availability system will be unaffected by running this command.

Diagnostic Procedures

If you have problems with any of the services, perform the following checks in the order they are presented here.

Basic Checks

When CAD services has problems, check that:

- CAD services are running (see "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63).
- The Preferences' key value is correct (see "Preferences Check" on page 35).
- The network is set up correctly (see "Network Check" on page 35).
- The CAD services are running and active (see "Active Service Check").

Active Service Check

This section applies to the following services only: Agent E-Mail, LRM, Call/Chat, Enterprise, Recording and Statistics, BIPPA, and Sync.

For Nonredundant Systems

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

For Redundant Systems

- Check the service 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.

Preferences Check

- Verify that SiteSetup exists and contains the entries specified in "SiteSetup" on page 24.
- Verify keys used by specific services exist and are valid. See "Preferences" on page 24.

Memory and CPU Check

Memory and CPU usage by CAD services can be checked using RTMT. See "Monitoring Predefined System Objects" in the *Cisco Unified Real-Time Monitoring Tool Administration Guide,* available at:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

Network Check

- For CAD services, verify that the IP address in the SiteSetup for the IOR HOSTNAME value is the correct IP address of the public NIC. See "SiteSetup" on page 24 for more information.

- To view information about the NICs on the Unified Communications Operating System, execute the CLI command `show network eth0`. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System and execute CLI commands.
- Check the network connectivity by pinging on the Unified Communications Operating System, execute the CLI command `utils network ping`. See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.5* for information about this command, available at:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Blocked Ports Check

To check whether a port is blocked, execute the following CLI commands:

- `utils firewall ipv4 status`
- `utils firewall ipv4 list.`

See "Executing CLI Commands" on page 15 for executing a CLI command. See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.5* for information about the `utils firewall` command, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

CAD Desktop Applications in Windows

3

CAD Desktop Applications Autorecovery

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 Desktop Services in the case of a service restart or a network outage.

When Agent Desktop, CAD-BE, or Supervisor Desktop 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, CAD-BE, or Supervisor Desktop 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.

See "CAD Services Autorecovery" on page 12 for more information on how CAD services need to be handled during service failure.

Technical Package Information

Service Connection Types and Port Numbers

Consult the *Cisco Unified CCX (IP IVR and IPCC Express) Port Utilization Guide* for a complete listing of ports and connection types used in CAD 8.5.

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Registry Entries

Site Setup

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Site Setup
For 64-bit machines: HKEY_LOCAL_MACHINE\WOW32\SOFTWARE\Calabrio\CAD\Site Setup

Table 13. 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.
	CALLCENTERLANG	string	Language selected during installation.
	DEPLOYTYPE	string	Defines the Unified CM type.
	INSTALL DIRECTORY	string	Base install directory for Cisco software.
	INSTALLDIR	string	Parent directory of base install directory for Cisco software.
	IOR HOSTNAME	string	Hostname or IP address of the computer's NIC. Its value is only present on the CAD services computer.
	LDAP Bind DN	string	User ID used to log in to the LDAP service. Default = cn=Client, ou=People, ou=Calabrio 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.

Table 13. Site setup registry entries — *Continued*

Key	Value	Type	Description
Site Setup	LDAP Heartbeat Retry Time	dword	Heartbeat time, in milliseconds. Default = 10000.
	LDAP Host 1	string	LDAP service hostname/IP address. There can be multiple LDAP hosts.
	LDAP LCC	string	Default logical contact center
	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=Calabrio Communications.
	MONITOR DEVICE	string	Network card on which to sniff packets.
	ProductCode_Agent	string	Cisco Agent Desktop product code.
	ProductCode_Supervisor	string	Cisco Supervisor Desktop product code.
	ProductCode_Admin	string	Cisco Desktop Administrator product code.
	Serial Number	dword	Counter to indicate changes to site setup values. Default = 0.

Enterprise Service

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Enterprise Data
For 64-bit machines:
HKEY_LOCAL_MACHINE\WOW32\SOFTWARE\Calabrio\CAD\Enterprise Data

Table 14. Enterprise Service registry entries

Key	Value*	Type	Description
Setup	Max Wait Time	dword	Maximum time, in milliseconds, to wait for enterprise data. Default = 100.
	Initial Time	dword	Number of milliseconds to wait after the first request for enterprise data, if data is not guaranteed. Default = 10.
	Increment	dword	Number of milliseconds to add to the retry time at each interval, if data is not guaranteed. Default = 20.
	Retry Sleep Interval	dword	Number of milliseconds used to calculate the interval for retry attempts, if call is not known to enterprise. The interval is calculated by (retry sleep interval × retry attempt). Default = 150.

* These registry keys need to be created only if there are timing issues when an agent requests data from the Enterprise service and the Enterprise service does not have the data yet.

Recording & Playback Client

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Recording & Playback Client
For 64-bit machines:
HKEY_LOCAL_MACHINE\WOW32\SOFTWARE\Calabrio\CAD\Recording & Playback Client

Table 15. RecordingPlaybackClient key value

Key	Value*	Type	Description
Setup	From Client Port	number	The port on the supervisor's desktop that is used to receive the "From Agent" audio stream for playback sessions.
	Jitter Buffer	number	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	number	End of range of port numbers to use for recording. Each simultaneous recording requires two ports.
	Port Range Start	number	Start of range of port numbers to use for recording. Each simultaneous recording requires two ports.
	Sound Buffers	number	The number of buffers used to hold audio data sent to the sound card. Default value = 30 ms. If sound quality is bad, increasing this number might improve the quality.
	To Client Port	number	The port on the supervisor's desktop that is used to receive the "To Agent" audio stream for playback sessions.
	VPN Port	number	The port used by the Recording service for its VPN address service that client applications use 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 service.

* These registry keys need to be created only if there are audio issues when a supervisor requests data from the Recording & Playback client and the Recording & Playback client does not have the data yet.

Exporting Recordings From CAD

Recordings made by supervisors are archived using the CAD RAW format as voice data packets, and can only be reviewed using the Supervisor Record Viewer. If you want to export recordings from CAD and convert them to WAV format so that they can be reviewed using other media players, you can use either of two methods:

- In Supervisor Record Viewer, use the Play and Save function (for more information, see the *Cisco Supervisor Desktop User Guide*)
- From a machine on which Desktop Work Flow Administrator is installed, download recordings from the Unified CCX server and convert them to WAV format using the procedure below

To download and convert recordings from the RAW to WAV format, complete the following procedure.

To download and convert recordings:

1. Set the password for the uccxrecording user. For a detailed procedure, see "Setting the uccxrecording User Password" on page 44.
2. Create a folder on the machine on which Desktop Work Flow Administrator is installed. The folder must contain an SFTP client.

   NOTE: One SFTP client readily available on the internet is psftp.

3. In the same folder you created in step 2, create a text file named ftpcommands.txt that contains the following ftp commands.

   ```
   lcd "C:\Program Files\Cisco\Desktop_audio"
   mget *.Raw
   ```

   NOTE: You do not have to use the Desktop_audio folder; these steps use the Desktop_audio folder for purposes of illustration only. If you use a different folder, ensure you make the corresponding changes in step 4.

4. In the same folder you created in step 2, create a text file named convert.bat that contains the following commands:

   ```
   @echo off
   mkdir "C:\Program Files\Cisco\Desktop_audio"
   psftp <IP1> -l uccxrecording -pw <pw> -b ftpcommands.txt -batch
   psftp <IP2> -l uccxrecording -pw <pw> -b ftpcommands.txt -batch
   c:
   cd "C:\Program Files\Cisco\Desktop\bin"
   for %%c in (..\..\Desktop_audio\*.Raw) do raw2wav "%%~nc%%~xc"
   ```

   where:

- <IP1> is the IP address of the primary Unified CCX server
- <IP2> is the IP address of the secondary Unified CCX server
- <pw> is the uccxrecording user password you set in step 1

NOTE: When executed, these commands download all of the RAW recording files from the primary and secondary Unified CCX servers to the folder C:\Program Files\Cisco\Desktop_audio, convert the recordings to WAV format, and place the new WAV files in the folder C:\Program files\Cisco\Desktop_wav, leaving the original RAW files in the Desktop_audio folder. If desired, additional lines can be added to the batch file to copy the files to another folder or file server.

NOTE: The raw2wav 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.

5. Run the batch conversion file named convert.bat that you created in step 4.

Setting the uccxrecording User Password

To set the password for the uccxrecording user:

1. In the web browser, access https://<Unified CCX-server>/appadmin, where <Unified CCX server> is the Unified CCX server's IP address or host name.

   The Cisco Unified CCX Administration Authentication page appears.
2. Enter your Unified CCX username and password, and then click Login. The Cisco Unified CCX Administration home page appears.
3. Choose Tools > Password Management. The Password Management page appears.
4. For Recording SFTP User, enter the new password and enter it again to confirm the password.
5. Click Save. The password is set for the uccxrecording user.

Running the Conversion Batch File Automatically

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

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

NOTE: This assumes that convert.bat is in the C:\Program Files\Cisco\Desktop\bin folder.

About the RAW Format

Each RAW format recording is composed of the following files:

- <name>.To.Raw, containing data sent to the agent phone
- <name>.From.Raw, containing data sent from the agent phone

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

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

where:

- <YYYYMMDD> is the date the file was recorded
- <HHMMSS> is the time the file was recorded
- <counter> is the recording number; it is reset to 00000 every time an agent logs in and is incremented by one every time that agent is recorded
- <extension> is the extension of the agent recorded
- <agent ID> is the ID of the agent recorded

About the raw2wav Conversion Utility

The syntax to convert a RAW file to a WAV is:

```
raw2wav <filename> [<path>]
```

where:

- <filename> is either the <name>.To.Raw or <name>.From.Raw file.
- <path> is the location of the converted audio WAV files, if other than the default location; this parameter is optional

If the raw2wav utility finds a WAV file with a name that is identical to one that is about to be created, that file is not converted.

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

Diagnostic Procedures

If you have problems with any of the CAD desktop applications, perform the following checks in the order they are presented here.

Basic Checks

When Agent Desktop has problems, check that:

- The computers that host Agent Desktop services, unified CM, Unified CCX, and other system components are running.
- The registry is correct (see "Registry Check" on page 49).
- The network is set up correctly (see "Network Check" on page 49).
- The Agent Desktop services are running and active (see "Registry Check" on page 49).
- The Agent Desktop Configuration Setup utility has run correctly. See the *Cisco CAD Installation Guide* for more information.

E-Mail Connectivity Check

If you are having trouble connecting to the Microsoft Exchange server, you should verify that the account is set up correctly by using Microsoft Outlook or telnet.

Before testing the connection ensure you have the following:

- A Microsoft Exchange 2003, 2007, or 2010 server.
- A server set up to allow IMAP connections. This may be a secure or a plain text connection.
- A user account that can log into the IMAP server. This account must have an alias set up for each incoming e-mail address that you need for your call center.

  NOTE: Exchange 2007 does not properly handle e-mail aliases. While it will deliver them to the mail box, it will change the "To:" address back to the primary address for the account. The Agent E-Mail service needs a clean and unmodified "To" address in order to properly route e-mails. In order to get around this limitation, set up a distribution list for each incoming e-mail address with your Agent E-Mail service account as the only member.

- An SMTP server. (This can be on the Exchange server or a separate server.)

Testing Connections Using Outlook

You can configure Outlook to make an IMAP connection to the Exchange server; once connected you should be able to see folders and move messages around. You can also test the SMTP connection by sending a message from this account. Using Outlook, test the connection independently of the Agent E-Mail service and determine whether a connectivity issue is an Agent E-Mail issue or an Exchange configuration issue.

To configure an IMAP connection:

1. From the Outlook menu, choose Tools > E-mail Accounts. The E-mail Accounts wizard appears.
2. Select Add a new e-mail account, and then click Next. The E-mail Accounts - Server Type dialog box appears.
3. Select IMAP, and then click Next. The E-mail Accounts - Internet E-mail Settings (IMAP) dialog box appears.
4. Enter account information, and then click Next.

For detailed information on how to add users to Microsoft Exchange 2007, go to the following URL:

http://msexchangeteam.com/archive/2006/09/05/428833.aspx

Testing Connections Using Telnet

Perform the following steps to connect to IMAP using Telnet to test your e-mail connection.

1. Using Telnet, connect to IMAP by entering the following at a command prompt:

   ```
   telnet mail.myserver.com 143
   ```

   The above command should display a response similar to the following:

   ```
   telnet mail.myimapserver.com 143
   Trying 192.168.1.1...
   Connected to mail.myimapserver.com (192.168.1.1)
   Escape character is '^]'
   * OK IMAP4 ready
   ```

2. Log in using the login command. Type **. login** followed by your username and password, separated by spaces. If successful, a response similar to the following should appear:

   ```
   . login accountname@myserver.com *********
   . OK User logged in
   ```

   If necessary, refer to the following link for more detailed information on connecting to IMAP using Telnet:

   http://support.microsoft.com/kb/189326

Connecting to SMTP using Telnet

1. Run the following command from the command line of your CAD server:

   ```
   telnet mail.mysmtpserver.com 25
   ```

   If successful, a response similar to the following should appear:

   ```
   220 mail.mysmtpserver.com Microsoft ESMTP MAIL Service,
   Version: 6.0.3790.3959 ready at Mon, 10 Dec 2007 16:53:25 -0600
   ```

2. Specify your mail server domain by typing the following into your telnet session using your mailserver domain:

   ```
   EHLO mysmtpserver.com
   ```

   If successful, the last line within the group of lines beginning with 250 should appear as follows:

   ```
       *
   250 OK
   ```

3. Log into the SMTP server by typing **AUTH LOGIN** into your telnet session. The server responds with an encrypted prompt for your user name. Enter your username encrypted in base 64. The server responds with an encrypted base 64 prompt for your password.

   NOTE: There are many tools online to do this. Perform a web search on the keywords: base64 converter.

4. Enter your password encrypted in base 64.

   For example, if your username is <myname> and your password is <mypassword> the base64 conversions will be bXluYW1l and bXlwYXNzd29yZA== respectively. A login sequence using these will look similar to the following:

   ```
   AUTH LOGIN
   334 VXNlcm5hbWU6
   bXluYW1l
   334 UGFzc3dvcmQ6
   bXlwYXNzd29yZA==
   ```

   If successful you will see the following:

   ```
   235 2.7.0 Authentication successful.
   ```

5. You may also wish to test whether you can actually send an e-mail with this account by performing the following:

   ```
   MAIL FROM:myname@mysmtpserver.com
   250 2.1.0 myname@mysmtpserver.com....Sender OK
   RCPT TO:recipient@mysmtpserver.com
   250 2.1.5 recipient@mysmtpserver.com....Recpient OK
   DATA
   354 Please start mail input.
   ```

```
Test of telnet smtp
.
250 Mail queued for delivery
```

You can find additional information about testing SMTP communication using telnet at the following URLs:

http://support.microsoft.com/kb/q153119/

http://technet.microsoft.com/en-us/library/aa995718.aspx

Registry Check

Using Windows Regedit:

- Verify that HKEY_LOCAL_MACHINE\Software\Calabrio\CAD\Site Setup (in case of 64-bit machines, HKEY_LOCAL_MACHINE\WOW32\Software\Calabrio\CAD\Site Setup) exists and contains the entries specified in "Site Setup" on page 39.
- Verify that the registry entries used by specific services exist and are valid. See "Registry Entries" on page 39.

Network Check

- On the Agent Desktop services computer, verify that the IP address in the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Site Setup\IOR HOSTNAME (in case of 64-bit machines, HKEY_LOCAL_MACHINE\WOW32\Software\Calabrio\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:
  1. In the Control Panel, double-click Network and Dial-up Connections.
  2. From the menu bar, choose Advanced > Advanced Settings.
  3. 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 Agent Desktop services computer to others in the configuration, for example, the Unified CM computer. Then reverse it by pinging from the other computers to the Agent Desktop services computer. Do this using both hostnames and IP addresses and ensure that the ping results match.

- If hostnames are used, verify that the appropriate 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 host name of the computer where the service is running and <port> is the port used by the service.
- Use a network protocol analyzer like Ethereal (www.ethereal.com) to analyze network communications.

Memory Check

- Ensure that the amount of memory on the computer is at least the minimum required for Agent Desktop 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 Agent Desktop 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 **telnet <hostname/IP address> <port>** 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.
  3. If it is successful, the command window will clear with cursor at top left corner; you will need to close the window.
  4. If the Telnet fails, you will probably see a connection failure.
- Check firewall settings on the client and server computers.
- Check firewall logs.

Application Behavior under Microsoft Windows Power Options

Power Options in Microsoft Windows is a collection of settings that manages the power usage by your computer. You can access and configure power options in Microsoft Windows Control Panel.

Table 16 describes the application behavior under the following power options in Microsoft Windows.

Table 16. Behavior under Microsoft Windows Power Options

Application	When system is in the standby mode	When either monitor or hard disk is turned off
CAD	• CAD is disconnected from the CAD servers • UCCX server logs out the agent • Agent is not displayed on Supervisor Desktop • CAD neither displays phone activity nor provides call control • When the agent restores the system, CAD attempts auto-recovery • When CAD is recovered, agent logs in and is automatically moved to the Not Ready state	• CAD remains connected with the CAD servers • Agent is displayed on Supervisor Desktop • Agent can answer both ACD and non-ACD calls

Table 16. Behavior under Microsoft Windows Power Options

Application	When system is in the standby mode	When either monitor or hard disk is turned off
CAD-BE	• CAD-BE is disconnected from the CAD-BE servers • UCCX server logs out the agent • Agent is not displayed on Supervisor Desktop • CAD neither displays phone activity nor provides call control • When the agent restores the system, CAD-BE attempts auto-recovery • When CAD is recovered, agent logs in and is automatically moved to the Not Ready state	• CAD-BE remains connected with the CAD-BE servers • Agent is displayed on Supervisor Desktop • Agent can answer both ACD and non-ACD calls
CSD	• Supervisor is disconnected from the Chat server • When the system is restored, supervisor needs to select the team for it to display all the agents logged in to CAD along with their respective states	• Supervisor remains connected with the Chat server • When the system is restored, supervisor does not need to select the team to view all the agents logged in to CAD along with their respective states
CDA	• CDA retrieves connection from all the servers recovering from the standby mode	• CDA remains connected with all the servers

Configuration Files and Logs

4

Introduction

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

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

Table 17. 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 17. CAD event, error, and chat message logs — *Continued*

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
OpenLDAP	openldap.log
Recording & Playback service	RPServer.log

Table 17. CAD event, error, and chat message logs — *Continued*

Service/Application	Log Name
Recording and Statistics service	• FCRasSvr.log • db.cra_repl_ads.pub.sql.log • db.cra_repl_ads.sql.log • db.cra_repl_ads.sub.sql.log • db.cra_repl_base.fcrassvr.pub.sql.log • db.cra_repl_base.fcrassvr.sql.log • db.cra_repl_base.fcrassvr.sub.sql.log • db.cra_utils_base.fcrassvr.pub.sql.log • db.cra_utils_base.fcrassvr.sql.log • db.cra_utils_base.fcrassvr.sub.sql.log • db.instrasdb.fcrassvr.pub.sql.log • db.instrasdb.fcrassvr.sql.log • db.instrasdb.fcrassvr.sub.sql.log • db.repl_base.pub.sql.log • db.repl_base.sql.log • db.repl_base.sub.sql.log • db.sp_make_ publisher.fcrassvr.pub.sql.log • db.sp_make_ publisher.fcrassvr.sub.sql.log • db.sp_splk_drop_ publisher.fcrassvr.pub.sql.log • db.sp_splk_drop_ publisher.fcrassvr.sub.sql.log • db.sql.log • db.truncate.fcrassvr.pub.sql.log • db.truncate.fcrassvr.sub.sql.log **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

Cisco Agent Desktop Chat Logs

All Agent Desktop chat conversations are automatically archived in plain text log files and kept for one week. The logs are saved to the following folder on the agent's computer:

C:\Program Files\Cisco\Desktop\log\transcripts\

There is one log per day (named monday.txt, tuesday.txt, and so on). The files are overwritten every week. The log includes the following information for every chat message:

- Date
- Time
- Priority (0 for normal, 1 for high priority)
- Type (message to supervisor, message to user)
- Sender
- Recipient
- Message text

Configuration Files

Table 18 lists the configuration files used by CAD desktop applications. Table 19 lists the configuration files used by CAD services. See "Enabling Debugging for CAD-BE" on page 69 for information on modifying one of these configuration files to enable debugging.

Table 18. CAD desktop applications configuration files

Configuration File	Application
agent.cfg	Agent Desktop
EemApp.properties	Agent E-Mail on agent desktop
CadBE.properties	CAD-BE
EemSupervisor.properties	Supervisor Desktop (for E-Mail related actions)
Administrator.cfg, Splkview.cfg	Desktop Work Flow Administrator
PostInstall.cfg	CAD Configuration Setup
Supervisor.cfg	Supervisor Desktop
SupervisorLogViewer.cfg	Supervisor Record Viewer
SWFAdmin.cfg	Supervisor Workflow Administrator

Table 19. CAD services configuration files

Configuration File	Service
bars.properties	Backup and Restore utility
CTIStorageServer.cfg	Enterprise service
DirAccessSynSvr.cfg	Sync service
EEMServer.cfg	Agent E-Mail service
EEMServerJava.properties	Agent E-Mail service Java engine
FCCServer.cfg	Call/Chat service
FCRasSvr.cfg	Recording and Statistics service
FCVoIPMonSvr.cfg	VoIP Monitor service
IPPAClient.properties	BIPPA service JSP client
IPPASvr.cfg	BIPPA service

Table 19. CAD services configuration files — *Continued*

Configuration File	Service
LDAPMonSvr.cfg	LDAP Monitor service
LRMServer.cfg	LRM service
RPServer.cfg	Recording service
slapd.cfg	Directory Services
WebAdminLib.cfg, WebAdmin.properties	Desktop Administrator

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 20 summarizes the default and configured behavior settings.

Table 20. Outbound call statistic handling

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

To include outbound calls in totals:

1. Start CLI. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System.
2. At the admin prompt, execute the CLI command `set uccx cad config RascalService CallReportIncludesOutbound 1`.

   The Recording and Statistics Service configuration file is saved with the new setting. The new setting will go into effect when you restart the Recording and Statistics service.

Monitoring, and Debugging/Logging

5

Monitoring and Changing CAD Services Status

The CAD services are installed on the Cisco Unified Communications Operating System. You can monitor, and start, stop, or restart CAD services in the Cisco Unified CCX Serviceability page.

Logging into Unified CCX Serviceability and Monitoring CAD Services

You can access the Unified CCX Serviceability page by logging into one of these pages:

- The Unified CCX Serviceability Authentication page
- The Unified CCX Administration Authentication page

The Unified CCX Serviceability page enables you to monitor the status of CAD services. The server status is indicated by an M (active) or S (standby) icon next to the CAD services.

To log into the Unified CCX Serviceability Authentication page and display CAD Services:

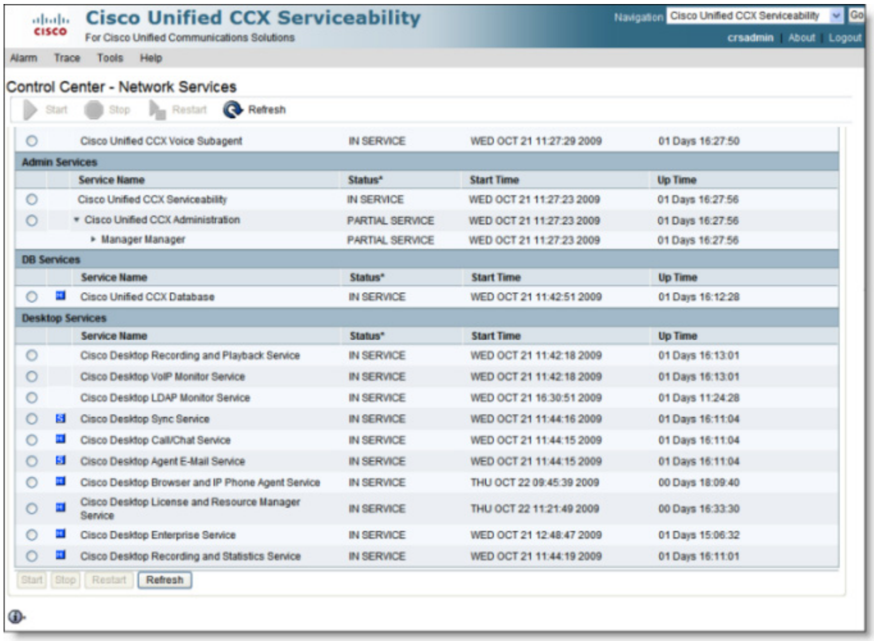
1. In the web browser, access https://<Unified CCX-server>/uccxservice, where <Unified CCX server> is the Unified CCX server's IP address or host name.

   The Cisco Unified CCX Serviceability Authentication page appears.

2. Enter your Unified CCX username and password, and then click Login. The Cisco Unified CCX Serviceability home page appears.
3. Choose Tools > Control Center - Network Services. The Control Center - Network Services page appears.

4. Select the server that hosts the CAD services from the Select Server drop-down list and then click Go. The services on that server are listed (Figure 2).

Figure 2. Control Center - Network Services


Cisco Unified CCX Serviceability
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CCX Serviceability
Go
crsadmin
About
Logout
Alarm
Trace
Tools
Help
Start
Stop
Restart
Refresh

Control Center - Network Services

	Service Name	Status*	Start Time	Up Time
○	Cisco Unified CCX Voice Subagent	IN SERVICE	WED OCT 21 11:27:29 2009	01 Days 16:27:50
Admin Services				
	Service Name	**Status***	**Start Time**	**Up Time**
○	Cisco Unified CCX Serviceability	IN SERVICE	WED OCT 21 11:27:23 2009	01 Days 16:27:56
○	▾ Cisco Unified CCX Administration	PARTIAL SERVICE	WED OCT 21 11:27:23 2009	01 Days 16:27:56
	▸ Manager Manager	PARTIAL SERVICE	WED OCT 21 11:27:23 2009	01 Days 16:27:56
DB Services				
	Service Name	**Status***	**Start Time**	**Up Time**
○	Cisco Unified CCX Database	IN SERVICE	WED OCT 21 11:42:51 2009	01 Days 16:12:28
Desktop Services				
	Service Name	**Status***	**Start Time**	**Up Time**
○	Cisco Desktop Recording and Playback Service	IN SERVICE	WED OCT 21 11:42:18 2009	01 Days 16:13:01
○	Cisco Desktop VoIP Monitor Service	IN SERVICE	WED OCT 21 11:42:18 2009	01 Days 16:13:01
○	Cisco Desktop LDAP Monitor Service	IN SERVICE	WED OCT 21 16:30:51 2009	01 Days 11:24:28
○	Cisco Desktop Sync Service	IN SERVICE	WED OCT 21 11:44:16 2009	01 Days 16:11:04
○	Cisco Desktop Call/Chat Service	IN SERVICE	WED OCT 21 11:44:15 2009	01 Days 16:11:04
○	Cisco Desktop Agent E-Mail Service	IN SERVICE	WED OCT 21 11:44:15 2009	01 Days 16:11:04
○	Cisco Desktop Browser and IP Phone Agent Service	IN SERVICE	THU OCT 22 09:45:39 2009	00 Days 18:09:40
○	Cisco Desktop License and Resource Manager Service	IN SERVICE	THU OCT 22 11:21:49 2009	00 Days 16:33:30
○	Cisco Desktop Enterprise Service	IN SERVICE	WED OCT 21 12:48:47 2009	01 Days 15:06:32
○	Cisco Desktop Recording and Statistics Service	IN SERVICE	WED OCT 21 11:44:19 2009	01 Days 16:11:01

5. Scroll down to the Desktop Services section.You can view and monitor the CAD services. See "Changing CAD Services Status" on page 65 for information on starting, stopping, or restarting CAD services.

To log into the Unified CCX Administration Authentication page and display CAD Services:

1. In the web browser, access https://<Unified CCX-server>/appadmin, where <Unified CCX server> is the Unified CCX server's IP address or host name.

   The Cisco Unified CCX Administration Authentication page appears.

2. Enter your Unified CCX username and password, and then click Login.The Cisco Unified CCX Administration home page appears.

3. Select Cisco Unified CCX Serviceability from the Navigation drop-down list and click Go. The Cisco Unified CCX Serviceability home page appears.

4. Repeat the steps 3 through 5 from the log into the Unified CCX Serviceability Authentication page and monitor CAD Services procedures.

Changing CAD Services Status

Each CAD services status can be changed as needed. The CAD services will be in one of these status.

- IN SERVICE
- PARTIAL SERVICE
- OUT OF SERVICE
- SHUTDOWN

You can change start, stop, or restart CAD services by either one of these methods:

- In the Unified CCX Serviceability page
- Executing CLI commands

To start, stop, or restart the CAD services in the Unified CCX Serviceability page:

1. Log in to Unified CCX Serviceability and display the CAD service whose status you want to change. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.
2. Select the CAD service that you want to start, stop, or restart.
3. Click Start, Stop, and Restart as needed.
4. Click Refresh to check if the changes are taken into effect.

To start, stop, or restart the CAD services by executing CLI commands:

1. Start CLI. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System
2. At the admin prompt, execute the following commands:
   - `utils service start` <CAD service> to start a CAD service
   - `utils service stop` <CAD service> to stop a CAD service
   - `utils service restart` <CAD service> to restart a CAD service

   See Table 1 on page 15 for information on CLI commands and Table 2 on page 22 for information on CAD services.

   The specified CAD service status changes.

Debugging and Logging

CAD can create debugging logs to help with troubleshooting.

> **NOTE:** When upgrading from CAD 6.4 to CAD 8.5, any configuration files you edited revert to their default settings.

Debugging information is written to the various debug files, all of which have a *.dbg suffix. Debugging files for CAD desktop applications are located in C:\Programs Files\Cisco\Desktop\log. Exceptions are:

- CAD-BE on Linux logs are located in the CAD-BE agent's home directory
- CAD-BE on Windows logs are located on the agent's Windows desktop

> **NOTE:** If you want to read a debugging log generated by a computer running Linux, and you are using a computer running Windows to view the log, the log file might not be formatted with line breaks. In this case, open the log file with an alternative editor, such as Microsoft Wordpad or Notepad++.

Debugging files for CAD services are located on the Unified CCX server. You can collect and view logs using RTMT. See "Collecting Log Files" on page 72 for information on collecting logs. See "Configuring Debugging" on page 67 for information on configuring CAD services/applications for generating logs.

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.

Configuring Debugging

You can set the debugging threshold for CAD services/applications. For instructions to change debugging threshold for CAD services/applications, see the section that corresponds to the service or application that you are configuring.

- For CAD services, see Configuring Debugging Thresholds for CAD Services (page 68).
- For CAD-BE, Enabling Debugging for CAD-BE (page 69).
- For all other CAD applications, see Configuring Debugging for non-Java Applications (page 71).
- For Java applications, Enabling Debugging for Java Applications (page 70).

For a complete list of services/applications and their corresponding configuration files, see Table 18 on page 60 and Table 19 on page 60.

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. Running services at a higher debugging threshold during normal operations can have a significant impact on performance. Table 21 lists the available debugging thresholds.

Table 21. 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. This is the default setting. Exceptions are Bars CLI, which is set to DUMP by default, and Cisco Desktop LDAP Service, which is set to OFF by default.
CALL	• Minor and frequently-occurring normal events • Entering and exiting functions
TRACE	• Minor and frequently-occurring normal events • Entering and exiting functions • Detail debugging (for instance, loops)
DUMP	• Minor and frequently-occurring normal events • Entering and exiting functions • Detail debugging (for instance, loops) • Byte dumps

Table 21. Debugging thresholds — *Continued*

Threshold	Events Recorded
OFF	Turns off debugging.

Configuring Debugging Thresholds for CAD Services

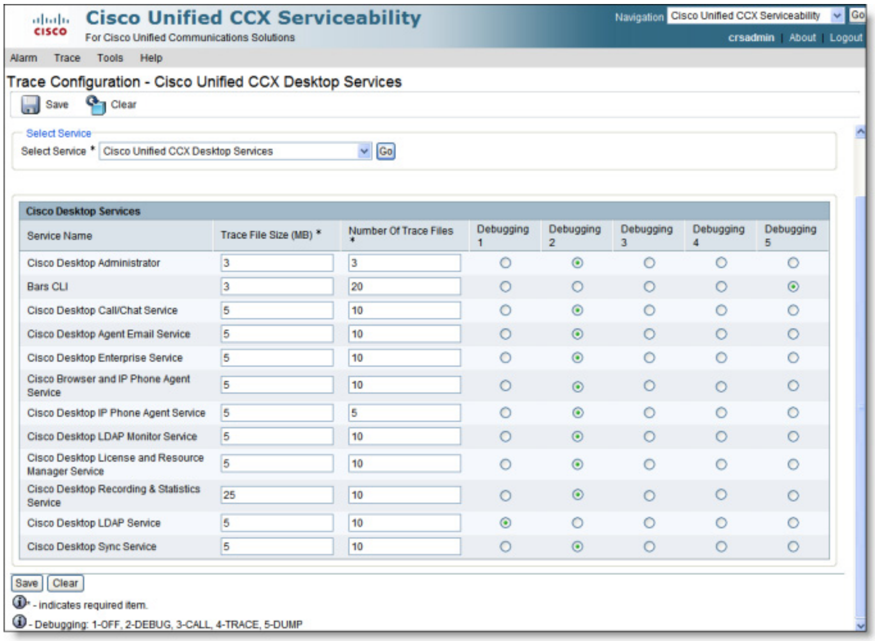
You can set the debugging option by either one of these methods:

- In the Unified CCX Serviceability page
- Executing CLI commands

To configure the CAD services for generating log files in the Unified CCX Serviceability page:

1. Access the Unified CCX Serviceability page. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging into Unified CCX Serviceability.
2. Choose Trace > Configuration. The Trace Configuration - Cisco Unified CCX Engine page appears.
3. Select the Cisco Unified CCX Desktop Services from the Select Service drop-down list and click GO. The Trace Configuration - Cisco Unified CCX Desktop Services page appears (Figure 3).

Figure 3. Trace Configuration - Cisco Unified CCX Desktop Services



Cisco Unified CCX Serviceability
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CCX Serviceability
Go
crsadmin
About
Logout
Alarm
Trace
Tools
Help

Trace Configuration - Cisco Unified CCX Desktop Services

Save
Clear
Select Service

Select Service * Cisco Unified CCX Desktop Services

Cisco Desktop Services

Service Name	Trace File Size (MB) *	Number Of Trace Files *	Debugging 1	Debugging 2	Debugging 3	Debugging 4	Debugging 5
Cisco Desktop Administrator	3	3	○	●	○	○	○
Bars CLI	3	20	○	○	○	○	●
Cisco Desktop Call/Chat Service	5	10	○	●	○	○	○
Cisco Desktop Agent Email Service	5	10	○	●	○	○	○
Cisco Desktop Enterprise Service	5	10	○	●	○	○	○
Cisco Browser and IP Phone Agent Service	5	10	○	●	○	○	○
Cisco Desktop IP Phone Agent Service	5	5	○	●	○	○	○
Cisco Desktop LDAP Monitor Service	5	10	○	●	○	○	○
Cisco Desktop License and Resource Manager Service	5	10	○	●	○	○	○
Cisco Desktop Recording & Statistics Service	25	10	○	●	○	○	○
Cisco Desktop LDAP Service	5	10	●	○	○	○	○
Cisco Desktop Sync Service	5	10	○	●	○	○	○

* - indicates required item.

- Debugging: 1-OFF, 2-DEBUG, 3-CALL, 4-TRACE, 5-DUMP

4. Enter the values in the Trace File Size (MB) and Number Of Trace Files fields.
5. Select the debugging option for each CAD service to configure them for generating log files. Table 21 on page 67 explains each debugging threshold. The available debugging thresholds are:
   - 1 sets debugging threshold to OFF.
   - 2 sets debugging threshold to DEBUG.
   - 3 sets debugging threshold to CALL.
   - 4 sets debugging threshold to TRACE.
   - 5 sets debugging threshold to DUMP.

   NOTE: By default, the Cisco Desktop LDAP Service debugging threshold is set to OFF. Do not turn up the debugging threshold for Cisco Desktop LDAP Service unless instructed by technical support, because this can significantly impact performance.

6. Click Save to save the changes.

To configure the CAD services for generating log files by executing CLI commands:

1. Start CLI. See "Executing CLI Commands" on page 15 for instructions on how to start CLI by logging into the Unified Communications Operating System.
2. At the admin prompt, execute the CLI command `set uccx cad log` <pathkey> <type> <key> <value>. The specified value is assigned to the key.

See Table 1 on page 15 for information on CLI commands and Table 2 on page 22 for information on CAD services's preferences files.

Enabling Debugging for CAD-BE

To enable debugging for CAD-BE, you must download the CadBE.properties file to the computer on which CAD-BE will be run, then edit the downloaded properties file to select the desired threshold. For instructions, see the following sections.

- Downloading the CadBE.properties File (page 69)
- Enabling Debugging for Java Applications (page 70)

Downloading the CadBE.properties File

To download the CadBE.properties file:

1. Open your web browser and access https://<CCX-server>/appadmin, where CCX-server is the hostname or IP address of the server that hosts Cisco Unified Contact Center Express.

   The Cisco Unified CCX Administration Authentication page appears.

2. Type the Unified CCX username and password.
3. Click Login. The Cisco Unified CCX Administration home page appears.
4. Choose Tools > Plug-ins. The Plug-ins page appears.
5. Click the Cisco Unified CCX Desktop Suites link.The Cisco Unified CCX page appears.
6. Right-click the hyperlink labeled CAD-BE logging and debugging file and save it to your computer. Table 22 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 22. Properties file location and additional actions

Operating System	Browser	Location of properties file/additional actions
Windows Vista and Windows 7	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 and Windows 7	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.

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 "Downloading the CadBE.properties File" on page 69.
   - For the Agent E-Mail applet, navigate to the folder C:\Program Files\Cisco\Desktop\config.
2. Open the properties file. The 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.calabrio.util.log.SplkLevel,LOG,DBG
#log4j.rootLogger=TRACE,LOG,DBG
#log4j.rootLogger=DUMP#com.calabrio.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.calabrio.util.log.SplkLevel,LOG,DBG
   #log4j.rootLogger=TRACE,LOG,DBG
   #log4j.rootLogger=DUMP#com.calabrio.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.

Configuring Debugging for non-Java Applications

To configure debugging for all other CAD applications, you must edit the appropriate configuration file on the computer on which the CAD applications are installed.

To configure debugging for non-Java applications:

1. 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. See "Collecting Log Files" on page 72 for more information. For example:

   ```
   Threshold=DEBUG
   ```

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

Collecting Log Files

Log files are generated when debugging log thresholds are configured (see "Configuring Debugging" on page 67). The generated log files are collected using the Real-Time Monitoring Tool (RTMT).

RTMT enables you to collect and view log files in several ways. These are:

- Trace & Log Central. Enables you to collect log files and save them on your machine to view them at later time.
- SysLog Viewer. Enables you to view logs in RTMT.

In addition, RTMT performs performance monitoring. This enables to check CPU, Memory, and Disk Usage. For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide,* available at:

> http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

Known Problems With Workarounds

6

Agent Desktop Problems

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 CPU usage on the 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 was able to start Agent Desktop, but was not able to 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 The agent received the error message, “The agent- or workflow-initiated action request failed.”

Solution This error message is displayed when a request to the Unified CCX engine, for example a call control action or agent state change, is rejected. Try the action again.

Problem The agent is unable to log in to Agent Desktop.

Symptom: An agent receives an error message when trying to log in to Agent Desktop. Possible error messages include the following:

- Failed to log into CTI Manager Server! Please talk to your administrator.
- The ID you entered was not found.
- Unable to log agent in.
- A critical error has been received. Either your phone or Unified CM is offline. If you are not already logged out, you may need to logout and try to log in again.

Cause. Depending upon the error message, the cause could be one of the following:

- If the error message involves the CTI Manager Server, the problem might be that the Enable CTI Application Use is not configured for the agent user ID, the CTIManager service is not running on the Unified CM server, or you are using an invalid password.

- If the ID you entered was not found, the ID could be invalid.
- If the agent cannot log in, the agent’s phone might not be associated with the RmCm provider in Unified CM.
- If you receive the critical error message, the Unified CM server might be offline or the agent’s IP phone has reset.

Solution Correct the problem related to the error message:

- If the message relates to the CTI Manager server, make sure that the CTIManager service is running on the Unified CM server.
- If the ID was not found, make sure that you are typing the user ID correctly. User IDs are case sensitive. Verify that you are using the correct password configured for the agent in Unified CM.
- If the agent's phone is not associated with the RmCm provider, access the Unified CM Administration application. Choose User Management > Application User, then select the RmCm provider. In the Device Information section on the Application User Configuration page, associate the agent's IP phone with the RmCm provider.
- If you receive the critical error message, make sure that the Unified CM server is online, and verify that the agent’s phone is in service.
- Unified CM is up and running, provided the Unified CCX setup is pointing to a cluster of Unified CM servers.
- Restart Cisco Desktop Sync Service.

Problem When you log in to Agent Desktop and Agent E-Mail is enabled, you receive multiple security and certificate warnings.

Cause. Warnings are received due to certificate errors, an untrusted publisher, or hostname mismatch while Agent E-Mail is loaded in the integrated browser.

Solution All certificate errors must be ignored, publishers must be trusted, hostnames must match, and content must be unblocked. Click the security or certificate warning displayed on the Information bar in the browser, and select an appropriate action depending on the available options to unblock the content or trust the publisher.

See the *Cisco CAD Installation Guide* for information on configuring the Internet settings to stop receiving these security and certificate warnings.

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 CCX server is not correctly passing enterprise data from the Enterprise service to Agent Desktop. 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 Configuration section in Desktop Administrator.
2. Stop and restart the Enterprise service.
3. If the problem persists, stop and restart the Unified CCX engine.

Problem E-mail Ready and Not Ready buttons are not available in the toolbar.

Solution Complete the following steps:

1. Verify that Agent E-Mail is properly configured.
2. In Application Administrator, verify that the agent belongs to a resource group that has at least one e-mail CSQ assigned to it.

Possible causes include the following:

- Agent E-Mail is only available in the premium package.
- Agent E-Mail has not been configured.
- The agent does not belong to any e-mail CSQs.

Problem The agent does not receive an e-mail when the E-Mail Ready button is activated.

Solution Complete the following steps:

1. Check the Contact Service Queue Statistics real time display and verify that there are e-mails in the queue.

2. Verify that the e-mail server has been configured correctly and that the Agent E-Mail service can connect to the Exchange server.

Possible causes include the following:

- There are no e-mails in any of the queues to which the agent belongs.
- Agent E-Mail has not been configured properly.

Problem A “Partial Service” or “No Service” message displays in the Agent Desktop status bar.

Symptom. The agent sees a message in the Agent Desktop status bar.

Cause. Agent Desktop 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 popup window. This window lists Agent Desktop features and indicates which features are affected by the service failure. When Agent Desktop 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 Agent toggles between Ready and Reserved states.

Symptom. The agent toggles between the Ready state and the Reserved state.

Cause. This might happen if a dial plan exists that starts with the same digit that the agent’s Unified CCX extension starts with. If the total number of digits in the agent’s extension in such a situation is less than the total number of digits configured for the dial plan, this symptom might occur.

Solution Make sure that the following two things do not happen concurrently:

- An agent’s Unified CCX extension starts with a digit for which a dial plan exists in Unified CM.

- The total number of digits in the agent's Unified CCX extension is less than the total number of digits configured for the dial plan.

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."

Symptom. Telnet tests from the agent PC to the LRM service on the Agent Desktop 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 Agent Desktop 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 Agent Desktop 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 F turns off by itself (approximately two 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 Every time the 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 Preferences and select either 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 The agent has changed Agent Desktop's window behavior (from the File menu), but when Agent Desktop is restarted, the setting has not been saved.

Solution Changes made to local settings via Agent Desktop are only temporary overrides of the global settings. Permanent changes must be made via Desktop Administrator.

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. Agent Desktop replaces the trunk number with <Unavailable>.

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 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 might cause the file to be opened in such a way that restricts other applications from opening the file.

Problem The 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 When the agent starts Agent Desktop, 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, Agent Desktop asks the CTI server for a snapshot of any existing phone calls to display to the user. Occasionally the CTI server returns invalid data. To dismiss the invalid data, the agent must click Drop. If the call appearance persists, the agent might have to close Agent Desktop, pick up the phone receiver to get a dial tone, hang up, and then restart Agent Desktop.

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. Exiting and restarting Agent Desktop 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 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 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. Ensure that the agent's phone is associated with the peripheral gateway JTAPI user.

Problem The agent is using Desktop Agent 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 Agent Desktop with an IP soft phone on a laptop that can connect to the network using either an Ethernet or wireless connection.)

Solution Each NIC has its own MAC address. Unified CM must be able to associate a MAC address with an extension in order for Agent Desktop 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's MAC address.

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 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 a 9 to get an outside line, while others require you to dial a 9. The dial string must take into account how the switch is set up.

Problem When agent receives an outbound reservation call, Agent Desktop displays the following error: “System Error. To correct this problem, please see your administrator. Error Code = 1051.”

Symptom. Agent Desktop automatically cancels the outbound reservation call and changes the agent state to Not Ready. The agent debug log contains the following message, “DESK1051: Agent received an outbound option reservation without proper buttons. Canceling the reservation.”

Cause. Agent Desktop is not configured properly to receive Outbound Dialer calls.

Solution There are two configurations necessary for an agent to process the Outbound Dialer calls:

- The agent must be assigned to the CSQ that is handling the Outbound Dialer calls.
- The work flow group to which the agent is assigned must have the Outbound Dialer toolbar. The administrator can do the following to include the Outbound Dialer toolbar:
  - Select the Direct Preview check box on the Toolbar tab of the User Interface node.
  - Manually configure the agent interface while creating or modifying a voice contact work flow by selecting all calls as agents' voice classification filter.

See the *Cisco Desktop Administrator User Guide* for more information on configuring Outbound Dialer calls.

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 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 might depend on previous actions executing correctly. Find out why the third action is failing and correct it.

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.

Problem The agent can’t find the Log Viewer executable.

Solution Log Viewer is part of Agent Desktop, not a separate executable, and can be accessed by choosing the option File—View Logs from the Agent Desktop menu bar.

Problem When opening the Log Viewer, <N/A> is displayed in the first row.

Solution If there is no data for the selected day, the first row of the log viewer is filled with <N/A>.

Problem The agent changed the viewing options but pressed cancel. Why weren’t the changes to the filters canceled?

Solution There is a Cancel button for each of the filter dialog boxes. Once a filter has been accepted, it is saved. The Cancel button on the options dialog box only cancels changes made to the columns.

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 might 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, where <milliseconds> is the desired length of delay. 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 might 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 might 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 might 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 might 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 When a macro is played back, it seems to be missing keystrokes, or the PC locks up.

Solution Due to the wide variety of systems and configurations, macro playback speed can vary. To slow down the rate at which a macro plays back keystrokes, add this section to the fastcalllocal.ini file:

```
[MacrosMisc]
DelayTime= <n milliseconds>
```

where n milliseconds is some value in milliseconds to delay between each macro event.

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 recording a macro. The Windows operating system unhooks the system keyboard hook when Start is pressed.

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

Solution In Agent Desktop 8.5, 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 or Agent Desktop. This is a limitation of the CTI server software.

Problem Increasing the font size in Agent desktop causes information in the status bar, including agent name and extension, to be truncated.

Solution After increasing the font size, you must restart Agent Desktop to display all of the information in the status bar without truncation.

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 clock may not be in the correct time zone.

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

Problem After an upgrade, the Report Font Size field is blank on the Accessibility Options tab of the Desktop Preferences dialog box in Agent Desktop.

Solution Select a font size from the drop-down list. The minimum report font size is 15.

Problem An agent's screen reader is not reading the contents of table cells in agent reports.

Solution Text in reports might not be readable initially by screen readers. Consult your screen reader's documentation for information on forcing the program to read text in report cells.

Problem After upgrading CAD from CAD 6.4(1) to CAD 8.5, agents do not see their global and/or personal phone books. The phone books were available before the upgrade.

Solution The phone books must be enabled in Cisco Desktop Administrator.

1. In Desktop Administrator, select Call Center 1 > Work Flow Configuration > Phone Book.

2. Ensure that the appropriate phone books (global and/or personal) are selected, and then click Apply.

Problem An administrator cannot telnet from the Unified CCX server to a desktop hosting a CAD application.

Solution Any firewall between the Unified CCX server and the desktop must have ports 59000–59030 open so that access to the desktop is allowed.

Problem Agent Desktop closes unexpectedly when agent is using the integrated browser.

Solution This error might be caused by an external web application running in the integrated browser that has issued a close command that not only closes the browser but also closes Agent Desktop itself. The web application must be rewritten so that it only closes the browser window instead of the whole application.

Problem Agent Desktop cannot be launched and one of a number of licensing errors is displayed.

Cause. You are not able to ping the IP address of the servers that host LDAP Host 1 and LDAP Host 2. If you launch Agent Desktop and it cannot access that IP address, then it is a networking issue.

Solution Verify the IP address of LDAP Host 1 and LDAP Host 2 in the preferences files and registry entries. See "SiteSetup" on page 24 and "Site Setup" on page 39 for more information. If the correct IP address still cannot be pinged, contact your network administrator to fix the network issue.

Problem The real time displays (reports) generated for the day of the week are not accurate.

Solution Reports are generated as expected only when the server and Agent Desktop are in the same time zone. When the server and Agent Desktop are in different time zones, reports might not include all expected data. This is because the range of data that appears in a report is based on the server's time zone and the server uses its clock to generate reports. To retrieve the missing data, you need to select a previous day or following day in order to display additional data.

NOTE: However, agent state logs do not allow selecting a previous or following day, as it stores data only for the current day.

For example, If the server is in India (local time is GMT + 5.5 hours) and Agent Desktop is in California (local time is GMT – 8 hours) and a call arrives at the agent at 21:00 GMT, the agent sees it arriving at 13:00 PST (21:00 – 8:00). However, since the server is in India, the call is timestamped as arriving at 02:30 IST (21:00 + 5:30), which is the next day.

Problem When an agent is completing an Outbound Dialer call and is in the Work state, some of the Outbound Dialer toolbar buttons become disabled.

Solution If an agent uses a multiline phone and displays calls on his or her non-ACD line while in the Work state, the enterprise data will be updated. This is the normal functionality for the non-ACD call, but Agent Desktop requires the enterprise data associated with the Outbound Dialer call in order to enable the toolbar buttons.

To work around this situation, disable multiline non-ACD calls. In Cisco Desktop Administrator, go to Services Configuration > Multiline, Monitoring & Recording > Display Settings and disable the Display Non-ACD Call check box.

Agent E-Mail Problems

Problem Cannot connect to IMAP or SMTP.

Solution The most likely cause for this problem is incorrect information entered for e-mail address or login/password. Use Outlook or telnet to check the connection. See "E-Mail Connectivity Check" on page 46 for more information.

Problem Cannot send e-mail or e-mails take a long time to send.

Solution After checking basic connectivity to the SMTP server using telnet, check to see if your virus checker, firewall, or other security software is interfering with the message. SMTP is a very common protocol for malware to use, and as a result virus checkers are very suspicious about programs that use it. Try turning virus checker, firewall, and other security software off momentarily to diagnose the problem.

Problem E-mails are not routed to agents.

Solution In order for e-mails to be routed to agents you must create e-mail distribution lists for each incoming address, and each of these addresses must be mapped via administration to a CSQ that has been configured for Agent E-Mail. Note that Exchange 2007 rewrites incoming e-mail “to:” addresses, which is the reason distribution lists must be used rather than aliases.

Problem The E-mail Ready or E-mail Not Ready buttons are not seen on my desktop.

Solution Agent E-Mail will only enable if the agent is licensed as premium and the agent belongs to at least one CSQ that is designated as an e-mail CSQ. Check to make sure you are licensed for premium and that the agent belongs to at least one e-mail CSQ.

Problem I'm sure my login is correct, but I still can't get logged in to IMAP, even though it works in Outlook.

Solution If outlook works, but Telnet does not, it is probably because the account you are using to log in is an NT domain account. When logging into IMAP you need to specify the login as follows:

NTDOMAIN/NTACCOUNT/ALIAS

For example, if your e-mail address is "Jane.Doe@myserver.com", your Windows NT login name is "jdoe", your NT domain name is "mydomain", and your Exchange mailbox name is "Jane Doe", you would then need to use a username of "mydomain/jdoe/Jane.Doe" when logging in.

Problem I finally got logged into IMAP, but now SMTP doesn't work.

Solution SMTP logins are not as complicated as IMAP logins. Use your account name; as in the previous example, use "jdoe."

Problem Some attachments don't make it through.

Solution Your e-mail server may limit messages to a certain maximum size. In addition, the server or a virus checker may filter certain attachment types that can contain malware.

Problem Agent Desktop does not save words for later use when you attempt to ignore an incorrect spelling or add a word to the dictionary during spell check.

Solution This is a known limitation in Agent Desktop. The ignored or added word stays in the dictionary until CAD is closed. Once CAD is relaunched, the ignored or added word is not taken into consideration.

Problem It looks like I'm sending my e-mails out, but they did not arrive at the destination address.

Solution The recipient’s mailbox may reject the e-mail, because the message is too large, or their mailbox is full, or they have attachment restrictions. Typically in this situation, the recipient SMTP server will send a delivery status message back to the sender. The Agent E-Mail service will detect this type of message, write a message to its log file and move the message to the System Status folder on the mail store. You can manually inspect this folder using Outlook, as described earlier, and associate the delivery status message with the sent and handled messages store in their respective folders. If you wish to requeue the handled message so that an agent can respond to it again, drag that message back to the inbox. Another alternative is to open the sent message and attempt to resend it manually if you suspect that the recipient will now be able to accept it. You would also be able to remove attachments before resending them if the reason for the failure was due to the attachments.

Problem An agent has draft e-mails but is not in the office, how can I requeue the e-mails so another agent can handle them?

Solution You can requeue the e-mails by logging in as that agent using the CAD desktop.

Problem A corrupt or malformed e-mail is in the inbox and I would like to remove it because it cannot be routed to or read by agents.

Solution Log in to Outlook as the other agent and manually delete the e-mail from the inbox.

Problem A supervisor cannot use a supervisor workflow action to send an e-mail. However, when the e-mail client is configured with the supervisor’s credentials, the supervisor can send an e-mail directly. The supervisor log files do not contain any error messages.

Solution Some virus checkers might prevent e-mails from being sent. Disable all virus checkers on the supervisor’s PC.

Problem Although there are many e-mails in the server mailbox, the Agent E-Mail service is not pulling any e-mails from the mailstore.

Symptom: The Agent E-Mail server could not connect to the Exchange Server via SMTP port 25.

Solution McAfee VirusScan 8.0 prevents sending mass mailing, thereby blocking telnet to port 25. To overcome this problem with McAfee VirusScan 8.0, follow these steps.

1. Start the VirusScan Console.
2. Select Access Protection Properties.
3. Under Ports to block, clear the Rule against Port 25 that says "Prevent mass mailing worms from sending mail." You will then be able to telnet to the mail server on port 25.

Problem Agent has no e-mail buttons.

Solution Verify the following:

- The contact center is using premium licenses.
- The agent services at least one e-mail CSQ.
- The integrated browser is enabled for the agent's workflow group.
- In workflow administrator, the e-mail buttons are visible for the agent's workflow group.

If any changes needed to be made, restart the agent desktop.

Problem The agent is not receiving any e-mail.

Solution Check if the Agent E-Mail account is locked out in Active Directory.

Problem When an agent selects an e-mail in the Contact Appearance pane, the error message, "An error has occurred" is displayed. The Unified CCX server is able to ping the Exchange server with its host name, but client desktops cannot.

Solution If host names are being used for the mail store, ensure that client desktops can resolve that host name. If not, use the IP address instead.

Problem Agent e-mail responses are not sent back to customers.

Microsoft Exchange has not been configured to allow the Cisco Agent Desktop SMTP user permission to send from the e-mail address specified in Cisco Desktop Administrator.

If this is the case, the EEMServerJavaXXXX.dbg log will show an error similar to the following while trying process messages in the outbox:

```
2008-10-06 13:06:30,334 DEBUG
[OutboxThread|Outbox#processOutbox:69] e.getMessage: 550
5.7.1 Client does not have permissions to send as this sender
```

The message is then moved to the Not Sendable folder on the mail store.

Solution To correct this problem, do the following (applicable to MS Exchange 2007):

1. Start the Exchange Management Shell.
2. At the prompt, execute the command:

   ```
   Add-ADPermission -Identity <distributionListId> -User
   <cadUserId> -2 -AccessRights extendedright
   -ExtendedRights "send as"
   ```

   Where <distribution list ID> is the distribution list identifier and <CAD user ID> is the user ID of the mailbox that CAD has been configured to use.
3. Repeat step 2 for every distribution list that you want CAD to be able to use to respond.
4. Close the Exchange Management Shell.
5. Restart the Agent E-mail service for the Exchange settings to take effect.
6. Use a third party IMAP client to move messages from the Not Routable folder back to the Outbox so that the Agent E-mail Service can attempt to process them again.

Problem An agent logged into CAD behind VPN is logged out after a failover. After the system fails back, the agent is unable to access Agent E-Mail.

Solution This issue occurs when engine failover occurs while Agent Desktop is in the process of downloading the applet. The Agent E-Mail applet is not completely downloaded when the failover happens, therefore the applet is not running and no failover occurs.

Problem CAD (with Microsoft Exchange 2007) is configured to route e-mails sent to a specific e-mail address to a specific CSQ (for example, e-mail sent to sales@example.com are routed to CSQ1). A customer puts that address in the BCC field of an e-mail message and nothing in the To or CC fields. The e-mail is delivered to the contact center but ends up in the Not Routable folder.

Solution Exchange 2007 is designed to remove the e-mail addresses from the BCC field. As a result, CAD cannot route the incoming e-mail to the appropriate CSQ and instead sends the e-mail to the Not Routable folder. The e-mail address in the BCC field cannot be recovered, and any e-mail using only the BCC field for the recipient e-mail will be routed to the Not Routable folder.

Problem Agent E-Mail is not working when an agent is using a Windows Vista or Windows 7.

Cause. The Agent E-Mail applet is not loaded and e-mail buttons are disabled.

Solution Make sure a supported JRE 1.6 is installed. Only JRE 1.6 Update 24 through Update 31 are supported. In the Windows Control Panel:

1. Double-click the Java (or Java Plug-In) icon to display the Java Control Panel.
2. Click the Advanced Tab.
3. In the Settings navigation tree, expand Java Plug-in and then clear the Enable the next-generation Java Plug-in (requires browser restart) checkbox.
4. Click OK.
5. Relaunch Agent Desktop if open.

Problem The Agent E-Mail mail box is filled up with automated responses from someone to whom an agent wrote a response.

Solution The automated response feature is enabled on both the customer’s end and in the contact center for the specific contact service queue. This creates an endless loop of responses to each other and fills up the mail box. To interrupt the loop, disable the automated response feature for the CSQ. In Cisco Desktop Administrator, navigate to the specific CSQ’s Contact Service Queue Settings page, and clear the Send Automatic Response check box. Using a third-party e-mail client, clear out the automated responses from the mail box, and then re-enable the automated response feature if desired.

Problem Agent E-Mail does not work.

Cause. A work flow that launches a third party application when an agent logs into Agent Desktop has been configured. When Agent Desktop starts, the third party application is launched and the agent attempts to enter data. However, the SSL warning dialog box that appears when Agent Desktop tries to launch Agent E-Mail steals the focus from the third party application. This can result in the agent inadvertently closing the SSL warning dialog box with a “no” answer and thus not launching Agent E-Mail, and the third party application showing incomplete data entered in it.

Solution This is expected and normal behavior. Some possible ways to avoid the problem are the following:

- Reconfigure the work flow so that the third party application is not launched on startup.
- Do not enter data in the third party application until Agent Desktop and all its features, including Agent E-Mail, has started successfully.
- Close the third party application when it starts.

Problem Agent E-Mail message routing performance is degraded and/or the logs show signs of connectivity issues.

Symptom. The following is present in the Event Viewer logs in the Exchange Management System:

- Event ID: 9646

- Type: Error
- Source: MSExchangeIS
- Description: Closing Mapi session "/o=Organization/ou=Administrative Group/cn=Recipients/cn=user" because it exceeded the maximum of 250 objects of type "objMessage".

Cause. By default, MS Exchange limits the number of messages sent per MAPI session to 250 and the number of attachments sent to 100. In contact centers with a large number of agents using Agent E-Mail these limits might be exceeded, which might result in messages not being sent.

Solution

Complete the following steps:

1. Ensure that MS Exchange is configured according to the "Message Throttling Policies in MS Exchange" section of the *Cisco CAD Installation Guide* before proceeding. Message routing performance is degraded if the MS Exchange server is not configured according to these settings.
2. Verify the expected routing times according to the "Agent E-Mail Routing Expectations" section of the *Cisco CAD Installation Guide*. Message routing performance should be within these specified parameters.

If you are still experiencing delays, modify the registry (applies to MS Exchange 2003, 2007, and 2010).

There are 13 MAPI-related constraints that might cause the above Event Viewer error. The Event Viewer message will specify which constraint is being exceeded.

Refer to the following article by Microsoft Support (Article ID: 830829) for more information about these MAPI-related settings and associated remedial steps:

http://support.microsoft.com/?kbid=830829

Symptom. On the MS Exchange server, the performance counter "MSExchangeIS\RPC Client Backoff/sec" indicates back-off requests are being sent to clients.

Cause. If the combined operations of the MS Exchange user account devoted to Agent E-Mail exceed the default RPC operations per second limitation, the MS Exchange server sends back-off requests to Agent E-Mail. Agent E-Mail does not conform with these back-off requests (and, even if it did, it would not improve message routing performance).

By not conforming with these requests, MS Exchange temporarily suspends communication with the offending clients. This in turn degrades message routing performance.

Solution

Because one MS Exchange user is used for all Agent E-Mail operations, you can avoid exceeding the default RPC operations per second limitation by disabling RPC Client Throttling altogether.

Perform the following steps to disable RPC Client Throttling:

1. On the MS Exchange Server, start the Registry Editor.
2. In the Registry Editor window, select HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > MSExchangeIS > ParametersSystem.
3. From the Edit menu, choose New > DWORD Value.
4. Enter RPC Throttling Factor as the entry name, and then press Enter again to display the Edit DWORD Value window.
5. In the Value data field, change the value to 0, and then click OK.
6. Close the Registry Editor window.
7. From the Start menu, select Run.
8. In the Open field, enter services.msc, and then click OK.
9. Select the Microsoft Exchange Information Store service, and then select Restart Service.

For more information, refer to *Understanding Client Throttling* at:

http://technet.microsoft.com/en-us/library/cc540454%28v=exchg.80%29.aspx

Solution

If neither of the solutions above resolve this issue, try completely disabling all MAPI session limits. To do so, perform the following steps:

1. Select the Start menu, then select Run.
2. In the Open field, enter regedit, and then click OK.
3. Select HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > MSExchangeIS > ParametersSystem.
4. If the Disable Session Limit setting does not exist, do the following:
5. Choose the Edit menu > New > DWORD Value.
6. Enter Disable Session Limit as the entry name.
7. Right-click Disable Session Limit and then select Modify from the popup menu.

8. Click Decimal, enter 0 (zero) in the Value data box, and then click OK.
9. Exit the Registry Editor.
10. Select the Start menu, then select Run.
11. In the Open field, enter services.msc, and then click OK.
12. Select the Microsoft Exchange Information Store service, and then select Restart Service.

Problem Throttling policies were configured on the MS Exchange Server as specified in the *Cisco CAD Installation Guide* and *Cisco CAD Troubleshooting Guide*. However, I am still experiencing issues with Agent E-Mail message routing performance and/or connectivity issues.

Solution The throttling policies must be applied to all MS Exchange Servers within the database availability group (DAG) used by the Agent E-Mail service. If the changes are not made to all servers, results will be inconsistent. For more information, see *Exchange Store Limits* at:

http://technet.microsoft.com/en-us/library/ff477612%28v=exchg.141%29.aspx

Problem Agent Desktop crashes when the e-mail state is changed to E-mail Ready.

Solution Perform the following steps to check if the Internet Explorer settings are configured properly:

1. Open Internet Explorer.
2. Navigate to Tools > Internet Options > Advanced.
3. In the Settings section, scroll to Browsing and do the following:
   - Check the Disable script debugging (Internet Explorer) check box.
   - Check the Disable script debugging (Other) check box.
4. Click OK.
5. Restart Internet Explorer for the changes to take effect.

Problem E-mail alert logs are not generated.

Solution In Agent Desktop 8.0(1), e-mail alerts are enabled by default. In Agent Desktop 8.0(2) and later, by default these alerts are disabled. To receive e-mail alerts, you must execute the following CLI command:

```
set uccx cad log EEMServerJava log Alarm Enable
```

See "CLI Command Syntax" on page 15 for more information.

Problem After an upgrade, the agent e-mail responses do not leave the CSQ and therefore are not delivered to customers.

Solution Restart the Cisco Desktop Agent E-Mail service (EEMServer.exe) in the Unified CCX Administration application. See "Restarting Services" on page 31 for more information.

Backup and Restore Problems

Problem BARS fails to back up files.

Solution Symptoms indicate that a client or server can't connect to LDAP on Side B. To correct this problem, restart Side B. If this does not fix the issue, restart both Side A and Side B.

Problem During a backup of Unified CCX, a Severity 2 alarm is generated in the Syslog that indicates that the LDAP Monitor service stopped unexpectedly or crashed.

Solution The LDAP Monitor service is temporarily stopped during a Unified CCX backup. This is normal behavior. You can ignore these alarms when they appear during a backup.

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 URLs is

https://<Unified CCX server>:<port>/cadbe/CAD-BE.jsp.

where:

- <Unified CCX server> is the IP address for the server that hosts Cisco Unified CCX.
- <port> is the port used by the Unified CCX server. Options are 8080 or 8443.

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.
- Check in Unified CCX Admin Control Center whether Cisco Unified CCX Administration on the BIPPA server is running.
- Make sure ports 8080 and 8443 are not blocked from the client or server computer.

Problem A popup 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 might 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 setting under Cisco Desktop Administrator on the BIPPA 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 3014 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.
- CAD-BE was running when the CAD server computer was upgraded. As a result, CAD-BE is a different version than the BIPPA service to which it was attempting to connect.
- CAD-BE timed out while attempting to reach the BIPPA service. Check the BIPPA server to make sure its CPU is not too high. Check that network latency between the desktop and BIPPA server computers is not too high.

Problem When starting up CAD-BE, the JRE plug-in installation begins.

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

Problem When starting up CAD-BE, the browser displays the following message: “This site might require the following ActiveX control ‘J2SE Runtime Environment 6.0 Update 12’ 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 on which the JRE plug-in is not installed. The browser security settings prevent the browser from automatically installing the JRE plug-in. 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 up 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 JRE plug-in from running. The JRE plug-in 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: 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 7 and 8and Mozilla Firefox 3.0 and above are the only supported browsers for this release.
- You do not have the required version of the JRE plug-in installed. CAD-BE will display messages pointing you to a valid location from which to install the correct version of JRE.
- 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 After upgrading CAD to a newer version, the browser displays an error message when trying to launch CAD-BE.

Solution The Java Archive (JAR) files used for Java applications may create problems when launching CAD-BE after an upgrade. Perform the following steps to remove the old Java cache files:

1. In the Control Panel, double-click Java. The Java Control Panel dialog box appears.
2. Click the General tab.
3. In the Temporary Internet Files section, click Settings. The Temporary Files Settings dialog box appears.
4. Click Delete Files. The Delete Temporary Files dialog box appears.
5. Check Applications and Applets check box and Trace and Log Files check box.
6. Click OK to save changes in the Delete Temporary Files dialog box.
7. Click OK to save changes in the Temporary File Settings dialog box.
8. Click OK to save the changes in the Java Control Panel dialog box.

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

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

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 cannot close windows. You can safely close this window yourself. Refer to the *Cisco CAD Installation Guide* for the correct browser settings to prevent the empty window from appearing.

Problem The agent is unable to log in. After the agent clicks OK on the Login dialog box, an error message appears that indicates one likely cause. The CAD-BE log file lists the message "CADBE3003: Unable to login agent. Cause <error code:error description>."

Solution If the error message is "Invalid agent ID/name and/or password":

- The wrong agent ID/name and/or password was entered. Try logging in again. If the error message appears again, reenter the agent password in Unified CCX Administration.
- The agent is configured correctly in Unified CCX, but the Sync service has not synchronized the CAD LDAP database with Unified CCX. Verify that the Sync service is running. In Desktop Administrator, manually synchronize Directory Services, then verify that the agent exists under the Personnel node.
- In Unified CCX, verify that the Enable CTI Application Use check box is selected for the agent user ID.

If the error message is "Invalid phone configuration":

- Wrong phone extension was entered. Try again and enter the correct information.
- Make sure the phone is associated with the Unified CCX agent and the agent's phone is associated with the RmCm provider in Unified CM.
- Phone is not pointing to the correct Unified CM server.
- Verify that the Unified CM server is online and that the agent's phone is in service and points to the same Unified CM (or Unified CM cluster) as Unified CCX.

If the error message is "No team found for agent":

- Agent does not belong to a team in Unified CCX. Associate the agent with a team in Unified CCX.

- The agent was configured correctly in Unified CCX but the Sync service has not synchronized the CAD LDAP database with Unified CCX. Verify that the Sync service is running. In Desktop Administrator, verify that the agent exists and belongs to the correct team.

If the error message is “CTI service is offline”:

- Make sure the CTI service is running and active again.

If the error message is “Invalid state change”:

- The agent is attempting to change to Ready state after logging in while there was an active call. Drop the call and try again.

If the error message is “CTI request timeout”:

- The network may be slow.

If the error message is “LRM service is down”:

- Start the LRM service if it is down.

If the error message is “No more licenses”:

- Wait a few minutes and retry.
- One or more CAD-BE agents might have exited their browsers without logging out first. Those sessions will continue to use up licenses for one minute after the browser exits.
- One or more 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 Not Ready state. Agent Desktop will continue to use the licenses until the application exits.
  IP Phone Agent will continue to use the licenses until the BIPPA service is restarted or until the agents login again and logout properly. CAD-BE will continue to use the licenses until the agents log out or one minute after CAD-BE is closed.
- Execute the CLI command `show uccx cad license usage` to locate clients using licenses. See "CAD License Usage" on page 32 for more information.

If the error message is “Forced login failed”:

- 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.

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 agent attempts to make a call by clicking Make Call.

Solution The agent is running CAD-BE on a computer that has an unsupported version of the JRE plug-in installed. Check if the version of the plug-in that is installed is compatible with CAD-BE.

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 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's MAC address.

Problem The agent is logged out unexpectedly.

Solution Possible reasons include:

- 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 In CAD-BE 8.5, 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 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 then 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 can 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.

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 the 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 A “Partial Service” or “No Service” message displays in the CAD-BE status bar.

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 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 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 Partial call history or partial data appears in the Enterprise Data fields for calls immediately 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 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 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 CCX 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 Configuration section in Desktop Administrator.
2. Stop and restart the Enterprise service.
3. 3. If the problem persists, stop and restart the Unified CCX engine.

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

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

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 log out and close the CAD-BE browser, pick up the phone receiver to get a dial tone, hang up, and then restart CAD-BE.

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 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. CAD-BE replaces the trunk number with <Unavailable>.

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.

Problem CAD-BE displays the following error on launching: “You do not have the required version of the JRE plug-in installed.You can install the JRE plug-in from the CAD Installation webpage.”

Solution Uninstall the current JRE version installed on the client PC and launch CAD-BE again. It will take you to the Unified CCX web page from where you can download a compatible JRE version.

Problem The BIPPA service crashes and logs indicate that the problem is with FreeImage, a library used by CAD to convert ICO images to PNG format.

Solution One of the CAD-BE toolbar icons is corrupted or invalid. Icons must conform to the following specifications:

- ICO format
- 50 Kb file size limit
- 16 × 16 or 32 × 32 pixels
- up to 256 colors

To change the corrupted or invalid icons, take the following actions:

1. Verify that the icons assigned to CAD-BE in Desktop Work Flow Administrator meet the icon specifications.
2. If an icon does not meet the specifications, fix it, and then reload it on the CAD-BE toolbar in Desktop Work Flow Administrator. For more information, see the “Toolbar” section in the *Cisco Desktop Administrator User Guide*.

Problem CAD-BE cannot be launched and displays the message that the standard bundle does not support CAD-BE.

Solution Launch CAD-BE after installation or restart of CAD services is complete on the active node.

Problem CAD-BE using JRE 1.6.0.17 and Firefox 3.6.3 freezes on login.

Solution Download and install JRE 1.6.0.24.

CAD Service Problems

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

Solution Verify if a CAD service is running, See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.

You can view CAD services status, and whether they are in an active (M) or standby (S) state.

Problem How can I check if the Unified CCX services are running?

Solution Verify if a Unified CCX services are running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.

You can view Unified CCX services status, and whether they are in an active (M) or standby (S) state.

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 a problem with the ACMI connection, look for problems with the CTI service. Also look for similar problems in the Enterprise service logs.
- If the logged error points to an LDAP error, make sure the LDAP service is running and the LDAP Host 1 registry setting in the following entry has the correct value:

  HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Site Setup (32-bit)

  HKEY_LOCAL_MACHINE\WOW32\SOFTWARE\Calabrio\CAD\Site Setup (64-bit)

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

Solution Perform the following tests:

- Verify if Unified CCX Administration and the BIPPA service are running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.
- Type the following URL in the address field of your web browser, where <Tomcat> is the IP address of the server on which Tomcat is installed.

```
http://<Tomcat>:6293/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 with JSP pages to the correct java servlets, web.xml, must be in the /usr/local/thirdparty/jakarta-tomcat/webapps/ipphone/web-inf directory.
- Verify that the TOMCAT HOME value for BIPPA preferences is /usr/local/thirdparty/jakarta-tomcat. If the value is incorrect, execute the set CLI command. See "CLI Command Syntax" on page 15 for information on changing key value pairs.

Problem The number and size of the log or debug files are smaller than specified in the application configuration file.

Symptom. The changed configuration file is copied to the $UCCX_HOME/desktop/config directory using File Transfer Protocol (FTP) or other methods. The configuration file is not copied completely and thus the application uses the old or incomplete configuration file.

Solution Restart the CAD service after transferring the configuration file through FTP.

Problem CAD client applications are slow to respond after the primary node goes down and fails over to the secondary node.

Solution Slow response time is expected behavior. There are numerous connections that must be made in order to determine that the primary node is down and to fail over the client application to the secondary node. Automated updating, if enabled, will also run at that time, adding to the delay. Depending on the type of node-down situation and how quickly connections are returned, it is possible for client applications to take longer than normal to log in and connect to all services.

Problem The Agent E-Mail, BIPPA, and Recording services are out of service.

This problem might be due to a setting in the Trend Micro OfficeScan antivirus software.

Solution To resolve the issue, do the following:

1. Log in to the Trend Micro OfficeScan WebConsole.
2. Navigate to the Networked Computers > Client Management node.
3. Select the Unified CCX server, and choose the options Settings > Real-Time Scan Settings from the menu.
4. Change the User Activity on Files, Scan files being: setting from “created/modified and retrieved” to “created/modified”.

Chat Problems

Problem After completing a conference call, the Chat client 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.

Call/Chat Service Problems

Problem The following error occurs when trying to start the Call/Chat service:

```
Could not start the Call/Chat Service on \\<computer>
Error 2140: An internal Windows error occurred.
```

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

1. To open SysLog Viewer and view logs using RTMT, see “Using SysLog Viewer” in the *Unified Real-Time Monitoring Tool Administration Guide*, available at:

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

4. In the Logs tab, double-click the Application Logs icon.
5. Look for messages that display FCCServer (the Call/Chat service) as the source. These messages should provide more information on the cause of the failure.

Problem How can I tell if the Call/Chat and LDAP Monitor services are running?

Solution Verify if the Call/Chat and LDAP Monitor services are running, See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services. The following two services should be listed:

- Cisco Desktop Call/Chat Service
- Cisco Desktop LDAP Monitor Service

If the status of either service is not Started, select the service and click Start.

Desktop Administrator Problems

Problem An imported phone book containing multibyte characters displays those characters as vertical lines (|||||). Desktop Administrator is running on a machine with a Windows XP English operating system.

Solution If Windows XP is not localized to the language that uses multibyte characters, those characters will be displayed incorrectly. To correct this issue, change the language for non-Unicode programs to the multibyte language. By default, this setting is set to the operating system language.

Select Start > Control Panel > Regional and Language Options. On the Advanced tab, select the multibyte language as the language to use for non-Unicode programs.

Problem The following error appeared while attempting to install Desktop Administrator configuration files on a network drive:

“The drive does not support long file names. You must choose a drive that support long file names. See your network administrator for more information.”

Solution You must enable long file name support on the network drive, or choose another drive that does support them. You can also install the configuration files on the administrator PC. You must enable File Sharing If you install the configuration files on the administrator PC.

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 When searching for subject matter experts from the Contact List page, no names are found, and this error message appears: “CDAUI2067 search did not complete successfully, and only partial results are displayed. Contact technical support."

Solution This error occurs when the parameters on the Unified Presence Cluster Settings page are not configured correctly. There are two possible causes of this problem: the user credentials are incorrect or the hostname/IP address is incorrect.

NOTE: 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.

To diagnose and resolve the problem, complete the following steps.

1. Choose Cisco Unified Presence Settings > Cisco Unified Presence Cluster Settings.
2. Click Verify.
   - If the hostname/IP address are incorrect, this error message appears: "CDAUI2033 Error communicating with the Unified Presence Server."
   - If the user credentials are incorrect, this error message appears: "CDAUI2034 Invalid Cisco Unified Presence Cluster user credentials. Configured user must be able to run SOAP queries."
3. Type the correct information in the appropriate fields, then click Verify to test the information you just entered. A message should appear, stating that the transaction was successful.
4. Click Save.

Problem An SME can log into Cisco Unified Personal Communicator, but cannot set his/her own Presence status or see the Presence status of his/her contacts. The Unified Personal Communicator log files also list the error message "401 (Unauthorized)."

Solution 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 on the phone 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.

- If the agent has access to Cisco Unified Personal Communicator, verify that the agent can log into Unified Personal Communicator and see SMEs.
- In Desktop Administrator, verify that the correct IP address for the Unified Presence server in the Cluster Configuration page is valid by clicking Verify.
- 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 agent is running Agent Desktop and is logged into Unified Presence. To log in, click Chat, then choose File > Log In.

  The File >Log In menu option is enabled only when the agent is logged out of Unified Presence and the server is up and running. This situation occurs only if (1) the agent’s Unified Presence username or password is different from the CAD username or password and (2) the agent clicks Cancel in the Login dialog box.

  If the agent is already logged into Unified Presence, the Log In menu option is disabled. If the Unified Presence server is down, the option is not available because when the server does come up, it tries to log the agent in automatically. If the automatic login fails the login dialog box is displayed, and if the agent cancels, the option will become available.

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 workflow 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 Agent Desktop or Supervisor Desktop.

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 Unified Presence. Verify that a phone number is configured for the SME in Unified Presence. You can find the number in the Active Directory that is associated with 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.

Problem An administrator cannot record macros from Desktop Administrator.

Solution Some virus checkers might prevent the macro recorder from running. Disable all virus checkers on the administrator’s PC.

Problem An administrator cannot save changes made in Desktop Administrator; the Save button is disabled.

Solution Another user logged into Desktop Administrator first on the same server. The web application is locked to anyone except that first user. In order for another user to be able to save changes, the following must occur:

- The first user logs out.
- The first user’s session is inactive for 15 minutes, after which time Desktop Administrator automatically times out.
- The first user closes the web browser without logging out, in which case Desktop Administrator is locked to all users for 15 minutes.

- The first user navigates away from Desktop Administrator without logging out. If the first user returns to Desktop Administrator within 15 minutes, that user is still logged in and can make changes. If the first user does not return to Desktop Administrator within 15 minutes, after 15 minutes that user is logged out and another user can make changes.

Desktop Work Flow Administrator Problems

Problem The administrator made some changes in Work Flow Setup, and then decided to cancel them. However, they were already saved.

Solution When a new action is created, any changes are automatically saved before returning to the Select Action dialog box.

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 might need to add quotes around the directory and executable. For example, the above would be “C:\Program Files\Acme\Search Database.exe” /t/x.

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 send an e-mail message, and changed the hint to Send E-mail (Ctrl+S). The shortcut keys do not work.

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

Problem An automated blind transfer to a route point or port in a workflow action is failing because the device is not responding quickly enough.

Solution Add a delay to the workflow action before the blind transfer occurs so that the device is ready and the operation can complete successfully.

Enterprise Data Problems

Problem Enterprise data does not display data on outbound calls.

Solution Enterprise data only displays data for inbound calls.

Problem Enterprise data does not display data for inbound calls.

Solution All devices the call goes through must be on the list of monitored devices (in Desktop Administrator, click Enterprise Data Configuration), or no data will be displayed. Make sure that the Enterprise service is properly installed and running. If everything appears to be working correctly, try rebooting the PC on which it is installed. After the PC has been rebooted, restart Agent Desktop on the agents' desktops.

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 How can I check to see if the Enterprise service is completely installed?

Solution Verify if the Enterprise service is completely installed. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services. The following two services should be listed:

- Cisco Desktop LDAP Monitor Service
- Cisco Desktop Enterprise Service

If these services are not listed, reinstall the Enterprise service.

Problem How can I tell if the LDAP Monitor service is running?

Solution Verify if the LDAP Monitor service is running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.

Check the status of the LDAP Monitor service. If the status is not Started, select the service and click Start.

Problem How can I tell if the Enterprise service is running?

Solution Verify if the Enterprise service is running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 63 for instructions on logging in and viewing CAD services.

Check the status of the Enterprise service. If the status is not Started, select the service and click Start.

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 error occurred.
```

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

1. To open SysLog Viewer and view logs using RTMT, see “Using SysLog Viewer” in the *Unified Real-Time Monitoring Tool Administration Guide*, available at:

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

6. In the Logs tab, double-click the Application Logs icon.
7. Select a message that displays Enterprise Server as the source. This should provide more information on the cause of the failure.

Problem No screen pops appear when the user makes calls to and from devices.

Solution Try the following:

- Use Enterprise Administrator to make sure the device is being monitored.
- Check to see if CTI Server is running.
- Check to see if an agent is logged in to the device.
- Check if the device is configured on Unified CCX.

Problem Nothing happens when the user calls a particular device.

Solution Try the following:

- Make sure the device is being monitored.
- Check the event log to see if there are any error messages for the device.

Problem Incomplete or no enterprise data is displayed when an agent received a call.

Solution Try the following:

- Check if the device is being monitored in the Enterprise service.
- Set debug threshold to DEBUG. Stop and restart Agent Desktop. Repeat the call scenario, and then check ssctihandler.dbg for warnings about non-monitored devices. Search for “monitoring” in the debug file.

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

```
Could not start the Cisco Desktop Enterprise Service on
\\<computer>
Error 2140: An internal Windows error occurred.
```

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

1. To open SysLog Viewer and view logs using RTMT, see “Using SysLog Viewer” in the *Unified Real-Time Monitoring Tool Administration Guide*, available at:

   http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html

8. In the Logs tab, double-click the Application Logs icon.
9. Select a message that displays Enterprise Server as the source. This should provide more information on the cause of the failure.

Installation Problems

Problem The Agent Desktop services have been upgraded from version 6.4(1) to version 8.5(1), and Automatic Updates are enabled. The Agent Desktop applications should automatically update the next time they are started. However, some desktops do not upgrade so there are mixed Agent Desktop versions operating in the contact center.

Solution The desktops that have not automatically upgraded must be upgraded individually from the Unified CCX Administration web application. See the *Cisco CAD Installation Guide* for more information.

Problem Automatic updates no longer occur on a machine where both Supervisor Desktop and Desktop Administrator are installed.

Cause. If an automated update of one desktop application completes successfully but an automated update of the other desktop application fails to complete for any reason, then automated updates will no longer work.

The installers for both Supervisor Desktop and Desktop Administrator use the same registry key to identify the version. If the one update is completed successfully, the registry is changed to the latest version even if the other update fails. Automated updates will not be triggered again.

Solution Download the latest version of the installer that failed and install it manually. The installers can be found at:

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

http://<server IP>:8088/TUP/CAD/Admin.html

where <server IP> is the IP address of the server that houses the CAD base services.

IP Phone Agent Problems

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

Solution The following are some reasons for the service to 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 is case sensitive. Enter it exactly as specified in the *Cisco CAD Installation Guide*.
- The Tomcat service is not running on the CAD services computer.
- The BIPPA service is not running on the CAD services computer.
- 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 agent's phone is not supported.
- The agent's phone has an incorrect phone load.
- The agent's phone does not support UTF-8 character set.

Problem The agent sees an error message that the IP Phone Agent 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, each pointing to a different BIPPA service, and all IP Phone Agent 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.

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, receive Skill Statistics screen updates, or see the Wrapup 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 the Unified CM authentication URL (one with authenticate.jsp) is used, 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 in to the phone.

- Verify that if the agent logs into Agent Desktop using the same phone and user ID, enterprise data does pop correctly.

Problem The agent sees nonsense characters in reason code, wrap-up data, caller data labels or values.

Solution The reason codes, wrapup data, caller data labels, or values configured in Desktop Workflow Administrator contain characters not supported by the phone or language. Examples are multibyte Chinese characters on a phone setup for English language. Make sure that no unsupported characters are used when configuring reason codes, wrapup data, caller data labels or values.

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

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

Problem Agents using the Cisco Unified IP Phone 9900 series are unable to exit the IP Phone Agent service by pressing the Exit or Close soft key.

Solution To exit the IP Phone Agent service, complete the following steps:

1. Press the Applications key on the IP Phone.
2. Select Running Applications on the screen.
3. Select the IP Phone Agent service you want to close.
4. Press the Close App soft key.
5. Select the Generic Application service.
6. Press the Close App soft key.

Problem The agent does not see the Enterprise Data screen when receiving/answering a call, receive CSQ Statistics screen updates, or see the Wrapup 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 the Unified CM authentication URL (one with authenticate.jsp) is used, 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 in to the phone.
- Verify that if the agent logs into Agent Desktop using the same phone and user ID, enterprise data does pop correctly.
- Verify that the BIPPA service is running and has established a connection to the Enterprise service. If not, restart the BIPPA service and check the connection again.

LDAP Monitor Problems

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. See "Corrupted LDAP Services Database" on page 34 for instructions on recovering the Directory Services database.

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.
- 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.

Recording and Statistics Service Problems

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

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

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

Problem Data appears to be in incorrect chronological order in Agent Desktop or Supervisor Desktop logs and reports, or in Supervisor Record Viewer. Unified CCX is in a redundant configuration, and a failover just occurred.

Solution If the system clocks on the redundant Unified CCX servers are not synchronized, report and log data will appear to be in the wrong order after a failover from one server to the other. To correct this situation, use a network time service to automatically synchronize all server system clocks, or manually adjust them so that they are in sync.

Problem In a High Availability (HA) environment the primary node computes 2.6 GB of maximum disk space available for recording, while the secondary node shows none.

Solution The maximum disk space available for recording for the single node in a Stand Alone environment is 2.6 GB, but the maximum recording space available for each node in a HA environment is half of that, or 1.3 GB. If the primary node in the HA environment displays 2.6 GB of recording space, then restart the Cisco Desktop Recording and Playback service on the primary node after adding the second node to the cluster.

Recording and Monitoring Problems

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

Problem Desktop-based silent monitoring does not work.

Solution The QoS RSVP service (a built-in Windows service) might be disabled on the agent's desktop. This service is required for Desktop-based monitoring and recording to work.

To resolve this issue, start the QoS RSVP service by completing these steps:

1. Launch the Windows Services utility from Control Panel (Control Panel > Administrative Tools > Services).
2. Right-click QoS RSVP in the list of services, and from the pop-up menu, select Start.

Supervisor Desktop Problems

Problem Error when trying to select skills in the Team View pane.

Symptom. When you try to select skills in the Team View pane in the Supervisor Desktop, the following message appears:

Message. Agent Desktop must be active before call intervention, call recording, and queue stats are available.

Cause. To view skill group statistics, you must log into Agent Desktop using your supervisor login.

Solution Log into Agent Desktop using your supervisor login.

Problem Agents are not displayed properly in Supervisor Desktop.

Symptom. The following symptoms related to the display of agents in the Supervisor Desktop can occur:

- Agents disappear from the Agent tree
- One or more agents are not displayed in the Agent tree

Cause. Incorrect configuration or IP connectivity issues between the agent PC and the Unified CCX system or the Unified CCX system and the supervisor PC.

Solution Check the following settings:

- Verify that the agent belongs to the team that the supervisor is monitoring. Refer to “Configuring Agents” in Chapter 5 of the *Cisco Desktop Administrator User Guide*.
- Verify that the CAD client desktop applications are at the same version as the CAD services.
- Determine whether the supervisor’s PC or agent’s PC has multiple NICs. If so, verify that the appropriate NIC is used to connect to the network.
- Determine whether any ports in the 59000–59030 range are blocked by a firewall, and if so, allow the ports to be connected.

- Determine if the client PC has the Internet Connection firewall enabled, and if so, disable it.
- To test for blocked ports, use telnet from the command line as follows with agent and supervisor logged in:
  - From the Chat service to agent, type the following command.
    `telnet <agent PC IP address> 59020`
  - From the Chat service to supervisor, type the following command.
    `telnet <supervisor PC IP address> 59021`
  - From agent to the Chat service, type the following command.
    `telnet <Unified CCX server IP address> 3001` (For Call/Chat Service – CORBA)
    `telnet <Unified CCX server IP address> 3002` (For Call/Chat Service – VPN)

  If you get a "failed to connect" error, then you need to determine why the port is blocked.

Problem The agent's state changed to Not Ready for no apparent reason.

Symptom. In some situations, an agent's state may change to Not Ready for no apparent reason.

Cause. To determine the reason, check the reason code:

- If the reason code is 32763, the agent's state became Not Ready because of Ring No Answer (RNA). If the agent phone is configured on Unified CM with auto-answer enabled, then this is likely a Unified CM issue since the call is not answered in time. Please consult Unified CM support.
- If the reason code is 32759, the agent's state became Not Ready because the phone went out of service. Check to make sure the phone is still functional and that you can call the phone directly. If everything seems fine, it is most likely a temporary problem and the phone has since recovered. If the phone is still down, it is most likely a Unified CM problem. Please consult Unified CM support.
- If the reason code is 32757, the agent's state became Not Ready because the phone rehomed due to a Unified CM failover. As long as the agent is able to go Ready after the failover, this is not an issue.

Solution In many cases, an agent's state becoming Not Ready is not a serious issue. Simply click Ready to change the agent's state to Ready.

To determine the reason code, do one of the following:

- Open the Agent State Report. From Agent Desktop, click Reports. Select Agent IPCC Express State Log. Look for the entry which says "Not Ready" at the time the agent's state became Not Ready. Check the reason code for this entry.
- Run the Agent State Detail Report, a Unified CCX Historical Report, and look for the "Not Ready" entry of the agent at the time the agent went to Not Ready state. Check the reason code for this entry.

In situations where the agent cannot change state to Ready because the phone is still down, contact Unified CM support.

Problem Agents who connect to the contact center through a VPN are not displayed in the Supervisor Desktop Team View pane. The agents disappeared from the Team View pane after disconnecting and then reconnecting to the VPN. The status bar displays "In Service."

Solution If either agents or supervisors use a VPN connection, their desktops must be restarted after disconnecting and then reconnecting to the VPN.

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 Agent Desktop servers.

Problem When the supervisor clicks on an agent to start 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 doesn’t see any of his teams or other personalized settings in the Supervisor Desktop window.

Solution If you add Supervisor Desktop to your Startup menu and your configuration files are on a network, it is possible that your configuration files aren’t loaded before Supervisor Desktop starts because your PC hasn’t had time to map the network drives. As a result, your personalized settings will not show.

Close Supervisor Desktop and start it again, and your personal settings will be loaded. To avoid the problem in the future, remove Supervisor

Desktop from the Startup menu, and create a desktop shortcut icon to use to start the program.

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 Record to record an agent conversation and nothing happened.

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

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 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 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, the Chat client 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 Call/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 Call/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 Call/Chat service.

Solution If a supervisor attempts to log into the Call/Chat service with the same ID as another supervisor, the Call/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 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.

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

Solution In CAD 8.5, 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, CAD-BE, or Agent Desktop. This is a limitation of the CTI service software.

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. The settings are configured with the Unified CM Administration application.

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 the Product Specific Configuration section of the Device Configuration screen, configure these settings as follows:

- 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 After an upgrade, the Report Font Size field is blank in the Preferences dialog box in Supervisor Desktop.

Solution Select a font size from the drop-down list. The minimum report font size is 15.

Problem A supervisor’s screen reader is not reading the contents of table cells in reports.

Solution Text in reports might not be readable initially by screen readers. Consult your screen reader’s documentation for information on forcing the program to read text in report cells.

Problem A supervisor logs out a CAD agent, and the agent still appears in the list of agents in Supervisor Desktop. The supervisor logs out a CAD-BE agent, and the agent disappears from the list of agents in Supervisor Desktop.

Solution This is normal behavior for CAD-BE.

Problem The real time displays (reports) generated for the day of the week are not accurate.

Solution Reports are generated as expected only when the server and Supervisor Desktop are in the same time zone. When the server and

Supervisor Desktop are in a different time zone, reports might not include all expected data. This is because the range of data that appears in a report is based on the server's time zone and the server uses its clock to generate reports. For retrieving the missing data, you need to select a previous day or following day for displaying additional data.

NOTE: However, agent state logs do not allow selecting a previous or following day, as it stores data only for the current day.

For example, If the server is in India (local time is GMT + 5.5 hours) and Supervisor Desktop is in Pacific time (local time is GMT - 8 hours) and a call arrives at the agent at 21:00 GMT, the agent sees it arriving at (21:00 - 8:00) = 13:00 PST. However, as per the server's time zone and its clock reads as the call is arrived at (21:00 + 5:30) = 02:30 IST, that is, the next day.

Problem Agents that are logged in after failover/failback incorrectly appear as logged out in Supervisor Desktop.

Cause: The Call/Chat service running on Supervisor Desktop does not send a message upon failback that the Chat connection was inactive. As a result, the team remains selected within the Supervisor Desktop even though the data displayed might be inaccurate.

Solution In Supervisor Desktop, from the team selection list drop down, select a different team, and then reselect the original team to refresh the team data.

Sync Service Problems

Problem How can I tell if the Sync service is running properly?

Solution In Desktop Administrator, perform a manual synchronization for a specific logical contact center. Make sure that all agents, supervisors, and teams are correctly listed for that logical contact center.

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 a problem with the Acmi connection, look for problems with the CTI server. Also look for similar problems in the Enterprise server logs. If the logged error points to an LDAP error, make sure the LDAP service is running and the LDAP Host 1 registry setting in SiteSetup has the correct value: See "SiteSetup" on page 24 for more information.

Unified CCX License Administration Problems

Problem The message, “There are no licenses available. Please contact your Administrator for help,” appears.

Solution All licenses are currently in use. Contact your sales representative to obtain additional licenses.

Problem Real-time reports shows the number of resources logged in, but it does not show the number of supervisors who are currently logged in. How can I view the number of supervisors who are currently logged in?

Solution To view the IP addresses of clients that are consuming desktop seats or are running a CAD administration application, execute the CLI command `show uccx cad license usage`. See "CAD License Usage" on page 32 for more information.

Note that for IP Phone Agent and CAD—Browser Edition seats, the IP address is the IP address of the active BIPPA service. For web-based Cisco Desktop Administrator, the IP address is the IP address of the CAD server.

VoIP Monitor Problems

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 Voice traffic generated by Desktop Monitoring and the VoIP Monitor service is not tagged for QoS (quality of service).

Solution Winsock QoS is disabled for Windows XP and Server 2000/2003 by default, and must be enabled through the Windows registry.

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

If you are running Windows XP or Windows Server 2003:

1. In the Registry Editor, under HKEY_LOCAL_MACHINE, access

   SYSTEM\CurrentControlSet\Services\TcpIp\Parameters

2. Choose Edit > New > DWORD Value.
3. 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.
4. 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 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 then reload the driver. Open a command window on the computer where the new NIC was installed and type these 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

A request from Cisco Remote Silent Monitoring (RSM) to start or stop monitoring an agent's call fails.

Description: This might happen if any of the following services or applications are down:

- VoIP Monitor service
- Chat service
- BIPPA service (if attempting to monitor a CAD-BE or an IP Phone agent)
- The instance of Cisco Agent Desktop on the monitored agent's PC (if attempting to monitor a CAD agent)

Another possibility is that the request to start or stop monitoring took more than 15 seconds to receive a response from any of these services.

Solution

Verify that the services and applications mentioned above are running. Check for network firewalls or delay. Check CPU usage on the server. For SPAN-based monitoring, check that SPAN is configured correctly.

Problem

There is a memory leak in the VoIP Monitor service when Cisco Remote Silent Monitoring (RSM) is used.

Description: Every successful request from RSM to the VoIP Monitor service to start monitoring a call must be followed by a request to stop the monitoring session. Otherwise it results in a memory leak in the VoIP Monitor service.

Solution Check the MIVR log as to why the request from RSM to the VoIP Monitor service to stop monitoring the call is unsuccessful.

Index