Contents

1 Introduction 7
  ■ CAD Documentation 7
    Obtaining Documentation and Submitting a Service Request 7
    Documentation Feedback 8
  ■ CAD 10.5 Applications 9
  ■ Version Information 10

2 CAD Services on Unified Communications Operating System 11
  ■ Guidelines for Sizing Deployments 11
  ■ CAD Services Autorecovery 12
    Fault Tolerance 12
    Agent Desktop and Supervisor Desktop 13
    BIPPA Service 14
    VoIP Monitor Service 14
    Agent E-Mail 14
  ■ Command Line Interface Tool and Commands 15
    Executing CLI Commands 15
    CLI Command Syntax 15
    Preferences and Configuration Files 23
  ■ Troubleshooting 32
    Services 32
    CAD License Usage 33
    Recovering the LDAP Services Database 35
    Diagnostic Procedures 36

3 CAD Desktop Applications in Windows 39
  ■ CAD Desktop Applications Autorecovery 39
    Agent Desktop and Supervisor Desktop 39
  ■ Technical Package Information 40
Contents

Service Connection Types and Port Numbers  40
Registry Entries  42
■ Exporting Recordings From CAD  47
■ Diagnostic Procedures  50
  Basic Checks  50
  Active Service Check  50
  E-Mail Connectivity Check  50
  Registry Check  53
  Network Check  53
  Memory Check  54
  CPU Check  55
  Blocked Ports Check  55
■ Application Behavior under Microsoft Windows Power Options  57

4  Configuration Files and Logs  59
■ Introduction  59
■ Event, Error, and Chat Logs  60
  Cisco Agent Desktop Chat Logs  63
■ Configuration Files  64
  Configuring the Recording and Statistics Service  65

5  Monitoring, and Debugging/Logging  67
■ Monitoring and Changing CAD Services Status  67
  Logging into Unified CCX Serviceability and Monitoring CAD Services  67
  Changing CAD Services Status  69
■ Debugging Logs  70
  Configuring Debugging  70
■ Collecting Log Files  75
Contents

6  Known Problems With Workarounds  77
   ■ Agent Desktop Problems  77
   ■ Agent E-Mail Problems  101
   ■ Backup and Restore Problems  115
   ■ CAD Service Problems  116
   ■ Chat Problems  119
   ■ Call/Chat Service Problems  120
   ■ Desktop Administrator Problems  121
   ■ Desktop Work Flow Administrator Problems  128
   ■ Enterprise Data Problems  131
   ■ Enterprise Service Problems  132
   ■ Installation Problems  133
   ■ IP Phone Agent Problems  134
   ■ LDAP Monitor Problems  138
   ■ Recording and Statistics Service Problems  139
   ■ Recording, Monitoring, and Playback Problems  140
   ■ Supervisor Desktop Problems  152
   ■ Sync Service Problems  161
   ■ Unified CCX License Administration Problems  162
   ■ VoIP Monitor Problems  163

Index  165
Contents
Introduction

CAD Documentation

The following documents contain additional information about CAD 10.5:

- 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
- 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:


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 10.5 Applications

CAD 10.5 includes the following applications:

**User Applications**
- Cisco Desktop Administrator (Desktop Administrator)
- Cisco Agent Desktop (Agent Desktop)
- Cisco Supervisor Desktop (Supervisor Desktop)
- Cisco IP Phone Agent (IP Phone Agent, IPPA)
- Cisco Desktop Work Flow Administrator (Desktop Work Flow Administrator)

**Services**
- Cisco Desktop Agent E-Mail Service (Agent E-Mail service)
- Cisco Desktop Browser and IP Phone Agent Service (BIPPA 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

For more information about CAD Express user applications and services, see the Cisco CAD Installation Guide.
Version Information

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

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

Version information is a series of four numbers separated by periods (for example, 10.5.1.56). From left to right, these represent:

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

CAD Services Autorecovery

Fault Tolerance

CAD 10.5 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 39 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 and recording is stopped. Monitoring and recording can be restarted manually after the failover when a new call is started.
- Enterprise data for the call in progress is lost at the time of the failure.
- Recordings might fail to initiate during a failover of the Recording and Statistics service.

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.

**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 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.
CAD supports high availability with Cisco Unified Presence Server. Integrating Unified Presence with CAD enables agents and supervisors to initiate chat sessions with non-agents, like subject matter experts (SMEs), through Unified Presence Client or Microsoft Office Communications Server (MOCS). During a failover of the Unified Presence Server, agents and supervisors are not able to chat with non-agents. Chat messages are not sent to or received by non-agents during failover. Once the failover is complete and communication is reestablished with the Unified Presence Server, agents and supervisors are able to chat with non-agents again and current Chat sessions with non-agents are restored. In rare instances, you might need to close your current Chat window and open a new one to restore full chatting capabilities.

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

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

**Agent Desktop and Supervisor Desktop**

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

When Agent Desktop and Supervisor Desktop detects that it is unable to communicate with a service (generally within three minutes 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 and 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 pop-up box that lists the application features and indicates if that feature is available or not due to the service outage.
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.

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

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 CSQ 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 some agents may still be monitored by one of the VoIP Monitor services. The only indication a supervisor receives that a particular agent is assigned to the downed VoIP Monitor service is an error message when attempting to monitor that agent.

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

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:

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 available at:


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 23 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show uccx cad license usage</td>
<td>Displays the available and used license information.</td>
</tr>
<tr>
<td>Command</td>
<td>Example / Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
| 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show uccx cad config &lt;pathkey&gt;</td>
<td>Displays configuration file values for the specified CAD service’s configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example: show uccx cad config CTIStorageServer</td>
</tr>
<tr>
<td>set uccx cad config &lt;pathkey&gt; &lt;key&gt; &lt;value&gt;</td>
<td>Sets the configuration file value with a new value for the specified CAD service’s configuration file.</td>
</tr>
<tr>
<td></td>
<td>• Pathkey: Name of the CAD service’s preferences.</td>
</tr>
<tr>
<td></td>
<td>• Key: The name of the key that you want to set with a new value.</td>
</tr>
<tr>
<td></td>
<td>• Value: Specify a new value.</td>
</tr>
<tr>
<td></td>
<td>Example: set uccx cad config RascalService CallReportIncludesOutbound 1</td>
</tr>
</tbody>
</table>

**Debugging log threshold, number, size, and alert preferences**

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show uccx cad log &lt;pathkey&gt;</td>
<td>Displays the specified CAD service’s log configuration details.</td>
</tr>
<tr>
<td></td>
<td>Example: show uccx cad log slapd</td>
</tr>
</tbody>
</table>
The Threshold key is used only with the debug type. You cannot set the Threshold key for Bars CLI.

- 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.
- 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils service restart &lt;CAD service&gt;</td>
<td>Restarts the specified CAD service. Example: utils service restart Cisco Desktop LDAP Monitor Service</td>
</tr>
<tr>
<td>utils service start &lt;CAD service&gt;</td>
<td>Starts the specified CAD service. Example: utils service start Cisco Desktop Sync Service</td>
</tr>
</tbody>
</table>
### Table 1. CLI Commands — *Continued*

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
</table>
| **utils service stop <CAD service>** | Stops the specified CAD service.  
Example:  
`utils service stop Cisco Desktop LDAP Monitor Service` |

### Recordings

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show uccx recordings allowed</strong></td>
<td>Displays the maximum amount of disk size allowed for recordings.</td>
</tr>
<tr>
<td><strong>show uccx recordings space</strong></td>
<td>Displays the total size of all the recording files.</td>
</tr>
</tbody>
</table>
| **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

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
</table>
| **utils uccx eemtables cleanup uid <uid1> [uid2] [uid3]** | 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` |

**NOTE:** Only one ID is required for this command, but additional IDs can be entered as desired.
Table 1. CLI Commands — Continued

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils uccx eemtables cleanup normal &lt;CSQ ID&gt; &lt;cutoff date&gt; &lt;e-mail state&gt;</td>
<td>Purges e-mail records from the database (Normal Mode). All e-mail records meeting the parameters you enter are removed from the database.</td>
</tr>
<tr>
<td></td>
<td>• &lt;CSQ ID&gt;: All records containing this CSQ ID are purged if other criteria are met. This must be an integer.</td>
</tr>
<tr>
<td></td>
<td>• &lt;cutoff date&gt;: Any recognizable date as specified by the Informix Date command. All e-mail records are purged up to, but not including, the cutoff date.</td>
</tr>
<tr>
<td></td>
<td>• &lt;e-mail state&gt;: Optional. If this parameter is not given, the command behaves as if the parameter all is used. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>Queued: use for e-mail statuses In Queue Waiting, Transferred, Requeued, and PeerReview.</td>
</tr>
<tr>
<td></td>
<td>Assigned: Use for e-mail statuses In process at agent and In draft at agent</td>
</tr>
<tr>
<td></td>
<td>Resolved: Use for e-mail statuses Pending Delete, Sent, and Deleted</td>
</tr>
<tr>
<td></td>
<td>All: Use to select all e-mail statuses.</td>
</tr>
<tr>
<td></td>
<td>Example: utils uccx eemtables cleanup normal 15 9/16/2010 all</td>
</tr>
</tbody>
</table>

LDAP utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Example / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils uccx ldap recover</td>
<td>Recovers the LDAP database from an inconsistent state.</td>
</tr>
<tr>
<td>utils uccx ldap archive</td>
<td>Displays the path of LDAP transaction log files that are currently not used.</td>
</tr>
<tr>
<td>utils uccx ldap stat</td>
<td>Displays the statistics of the LDAP database.</td>
</tr>
<tr>
<td>utils uccx ldap checkpoint</td>
<td>Inspects and clears all unused LDAP database transaction logs and exits.</td>
</tr>
<tr>
<td>utils uccx ldap index</td>
<td>Regenerates the LDAP service indices based on the current LDAP database.</td>
</tr>
<tr>
<td></td>
<td>Stop the LDAP service in the Unified CCX Serviceability page before executing this command.</td>
</tr>
</tbody>
</table>
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.
  Example:
  `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>
Stop the LDAP Monitor service in the Cisco Unified CCX Serviceability page before executing these commands.
  Example:
  `utils uccx ldap modify ldp_mod.ldif`

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.
  Example:
  `utils uccx ldap cat ldp_list.ldif`
Utilities

`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

<table>
<thead>
<tr>
<th>CAD services/applications</th>
<th>Pathkey</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Debugging log threshold, number, and size preferences, and Configuration files</strong></td>
<td></td>
</tr>
<tr>
<td>Bars CLI</td>
<td>BarsCLI</td>
</tr>
<tr>
<td>Cisco Desktop Browser and IP Phone Agent Service</td>
<td>BIPPAService</td>
</tr>
<tr>
<td>Cisco Desktop Call/Chat Service</td>
<td>ChatService</td>
</tr>
<tr>
<td>Cisco Desktop Enterprise Service</td>
<td>CTIStorageService</td>
</tr>
<tr>
<td>Cisco Desktop Sync Service</td>
<td>DirAccessSyncService</td>
</tr>
<tr>
<td>Cisco Desktop Agent E-Mail Service</td>
<td>EEMService, EEMServerJava</td>
</tr>
</tbody>
</table>
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.

### Table 2. Preferences files

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

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.
Site Setup

show uccx cad prefs SiteSetup

Table 3. SiteSetup key values

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteSetup</td>
<td>APP VERSION</td>
<td>Used by installation scripts to identify the version of the service software.</td>
</tr>
<tr>
<td></td>
<td>CALLCENTERLANG</td>
<td>Language selected during installation.</td>
</tr>
<tr>
<td></td>
<td>DEPLOYTYPE</td>
<td>Defines the Unified CM type.</td>
</tr>
<tr>
<td></td>
<td>INSTALL DIRECTORY</td>
<td>Base install directory for Cisco software.</td>
</tr>
<tr>
<td></td>
<td>INSTALLDIR</td>
<td>Parent directory of base install directory for Cisco software.</td>
</tr>
<tr>
<td></td>
<td>IOR HOSTNAME</td>
<td>Hostname or IP address of the computer’s NIC. Its value is only present on the CAD services computer.</td>
</tr>
<tr>
<td></td>
<td>LDAP Heartbeat Enabled</td>
<td>Is heartbeat enabled? 1=yes, 0=no. Default = 1.</td>
</tr>
</tbody>
</table>
Table 3. SiteSetup key values — Continued

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteSet up</td>
<td>LDAP Bind DN</td>
<td>User ID used to log in to the LDAP service. Default = cn=Client, ou=People, o=Spanlink Communications.</td>
</tr>
<tr>
<td></td>
<td>LDAP Connection Timeout</td>
<td>Maximum time, in seconds, before a connection attempt times out. Default = 15.</td>
</tr>
<tr>
<td></td>
<td>LDAP Heartbeat Retry Time</td>
<td>Heartbeat time, in milliseconds. Default = 10000.</td>
</tr>
<tr>
<td></td>
<td>LDAP Host 1</td>
<td>LDAP service hostname/IP address. There can be multiple LDAP hosts.</td>
</tr>
<tr>
<td></td>
<td>LDAP LCC</td>
<td>Default logical contact center</td>
</tr>
<tr>
<td></td>
<td>LDAP Port 1</td>
<td>LDAP service port. There can be multiple LDAP ports. Default = 3016.</td>
</tr>
<tr>
<td></td>
<td>LDAP Pwd</td>
<td>Encrypted user password</td>
</tr>
<tr>
<td></td>
<td>LDAP Request Timeout</td>
<td>Maximum time, in seconds, before an LDAP request times out. Default = 15.</td>
</tr>
<tr>
<td></td>
<td>LDAP Root</td>
<td>Root of the LDAP data. Default = o=Spanlink Communications.</td>
</tr>
<tr>
<td></td>
<td>MONITOR DEVICE</td>
<td>Network card on which to sniff packets.</td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
<td>Counter to indicate changes to site setup values. Default = 0.</td>
</tr>
<tr>
<td></td>
<td>LASTLANGDATE</td>
<td>Synchronizes both servers with the latest updated language.</td>
</tr>
</tbody>
</table>

**BIPPA**

show uccx cad prefs BIPPAConfig

Table 4. BIPPAConfig key value

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIPPAConfig</td>
<td>TOMCAT HOME</td>
<td>Location of the Tomcat web server files. Default = /usr/local/thirdparty/jakarta-tomcat</td>
</tr>
</tbody>
</table>
Enterprise Service

Execute the following CLI commands:

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

Table 5. EnterpriseService key values

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key*</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnterpiseService Setup</td>
<td>Max Wait Time</td>
<td>Maximum time, in milliseconds, to wait for enterprise data. Default = 100.</td>
</tr>
<tr>
<td></td>
<td>Initial Time</td>
<td>Number of milliseconds to wait after the first request for enterprise data, if data is not guaranteed. Default = 10.</td>
</tr>
<tr>
<td></td>
<td>Increment</td>
<td>Number of milliseconds to add to the retry time at each interval, if data is not guaranteed. Default = 20.</td>
</tr>
<tr>
<td></td>
<td>Retry Sleep Interval</td>
<td>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 \times retry attempt). Default = 150.</td>
</tr>
<tr>
<td>EnterpiseService Config</td>
<td>JavaClassPath</td>
<td>Lists jar files required by the Agent E-Mail service Java engine. Default: “log4j.jar,SplkStd4J.jar; EEM.jar;activation.jar;mail.jar”</td>
</tr>
<tr>
<td></td>
<td>JavaHome</td>
<td>The path to the Java virtual machine that will be used for starting the E-Mail service Java engine. Default: “C:\Program Files\Java\jre1.7.0_51”</td>
</tr>
<tr>
<td></td>
<td>JavaVMArguments</td>
<td>Additional arguments for the Java virtual machine. Default: ‘’ (empty string)</td>
</tr>
</tbody>
</table>

* 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 and Playback Client

**show uccx cad prefs RecordingPlaybackClientSetup**

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RecordingPlaybackClientSetup</td>
<td>From Client Port</td>
<td>The port on the supervisor’s desktop that is used to receive the “From Agent” audio stream for playback sessions.</td>
</tr>
<tr>
<td></td>
<td>Jitter Buffer</td>
<td>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 that the sound quality is good even on a congested network.</td>
</tr>
<tr>
<td></td>
<td>Port Range End</td>
<td>End of range of port numbers to use for recording. Each simultaneous recording requires two ports.</td>
</tr>
<tr>
<td></td>
<td>Port Range Start</td>
<td>Start of range of port numbers to use for recording. Each simultaneous recording requires two ports.</td>
</tr>
<tr>
<td></td>
<td>Sound Buffers</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To Client Port</td>
<td>The port on the supervisor’s desktop that is used to receive the “To Agent” audio stream for playback sessions.</td>
</tr>
<tr>
<td></td>
<td>VPN Port</td>
<td>The port used by the Recording and Playback 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 and Playback service.</td>
</tr>
</tbody>
</table>
Recording & Playback Service

Execute the following CLI commands:

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

Table 7. RecordingPlaybackService key values

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RecordingPlaybackServiceSetup</td>
<td>Maximum Playbacks</td>
<td>Maximum number of simultaneous outstanding playback requests.</td>
</tr>
<tr>
<td></td>
<td>Maximum Recordings</td>
<td>Maximum number of simultaneous outstanding recording requests.</td>
</tr>
<tr>
<td></td>
<td>OmniOrbUse Port</td>
<td>The CORBA port on which the Recording and Playback service listens for client requests.</td>
</tr>
<tr>
<td></td>
<td>VPN Port</td>
<td>The port on which the Recording and Playback service listens for requests from clients for their visible IP address. If you change this entry, you must also change the corresponding entry for all of the client applications.</td>
</tr>
<tr>
<td>RecordingPlaybackServiceConfig</td>
<td>Audio Directory</td>
<td>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.</td>
</tr>
</tbody>
</table>
VoIP Monitor Client

show uccx cad prefs VoIPMonitorClientConfig

Table 8. VoIPMonitorClientConfig key values

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolPMonitorClientConfig</td>
<td>FROM AGENT PORT</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>JITTER BUFFER</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SERVER HOST</td>
<td>Host name of the VoIP service.</td>
</tr>
<tr>
<td></td>
<td>SOUND BUFFERS</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>TO AGENT PORT</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolPMonitorClient Setup</td>
<td>Recording Jitter Buffer</td>
<td>The number of milliseconds that a packet expires for recording.</td>
</tr>
<tr>
<td></td>
<td>Recording Port Range Start</td>
<td>The starting port number for receiving UDP packets for recording.</td>
</tr>
<tr>
<td></td>
<td>Recording Port Range End</td>
<td>The end port number for receiving UDP packets for recording.</td>
</tr>
</tbody>
</table>
VoIP Monitor Service

show uccx cad prefs VoIPMonitorServiceConfig

<table>
<thead>
<tr>
<th>Pathkey</th>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIPMonitorServiceConfig</td>
<td>App Version</td>
<td>Used by installation scripts to identify the version of the service software. The service itself does not use this entry.</td>
</tr>
<tr>
<td></td>
<td>Update Version</td>
<td>Future use: tracks any hot fixes installed.</td>
</tr>
<tr>
<td></td>
<td>Monitor Device</td>
<td>Network card on which to sniff packets.</td>
</tr>
</tbody>
</table>
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 67 to verify whether a CAD service is running.

Table 11. Service names and executables

<table>
<thead>
<tr>
<th>Service name as shown in Services Control Panel</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Desktop Browser and IP Phone Agent Service</td>
<td>IPPASvr</td>
</tr>
<tr>
<td>Cisco Desktop Agent E-Mail Service</td>
<td>EEMServer</td>
</tr>
<tr>
<td>Cisco Desktop Call/Chat Service</td>
<td>FCCServer</td>
</tr>
<tr>
<td>Cisco Desktop Enterprise Service</td>
<td>CTIStorageServer</td>
</tr>
<tr>
<td>Cisco Desktop LDAP Monitor Service</td>
<td>LDAPmonSvr, slapd</td>
</tr>
<tr>
<td>Cisco Desktop Licensing and Resource Manager Service</td>
<td>LRMServer</td>
</tr>
<tr>
<td>Cisco Desktop Recording and Statistics Service</td>
<td>FCRasSvr</td>
</tr>
<tr>
<td>Cisco Desktop Recording Service</td>
<td>RPServer</td>
</tr>
<tr>
<td>Cisco Desktop Sync Service</td>
<td>DirAccessSynSvr</td>
</tr>
<tr>
<td>Cisco Desktop VoIP Monitor Service</td>
<td>FCVoIPMonSvr</td>
</tr>
</tbody>
</table>
CAD License Usage

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

Each agent logging into Agent Desktop, Supervisor Desktop 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
- Work Flow Administrator

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

- Agent Desktop or IP Phone Agent
- Supervisor Desktop
- Desktop Administrator
- Work Flow Administrator

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 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.
NOTE: An IP address that is listed twice reflects a user who is running both Supervisor Desktop and Agent Desktop. This user counts for only one seat license.

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

Entries in the command window are described in Table 12.

Table 12. show uccx cad license usage result headings

<table>
<thead>
<tr>
<th>Result Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seat</td>
<td>Lists users of Agent Desktop, IP Phone Agent, and Supervisor Desktop.</td>
</tr>
</tbody>
</table>
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 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 69 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 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:

- The computers that host Unified CCX, CAD services, Unified CM, Microsoft Exchange, and other system components are running (see "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 67).
- The Preferences' key value is correct (see "Preferences Check" on page 36).
- The network is set up correctly (see "Network Check" on page 37).
- The CAD services are running and active (see "Active Service Check" on page 36).

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 "Site Setup" on page 25.
- Verify keys used by specific services exist and are valid. 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.

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:

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 "Site Setup" on page 25 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.

- Verify that the hostname and IP address are as expected.

- Verify that the subnet mask is correct. It is probably 255.255.255.0.

- Check the network connectivity by pinging on the Unified Communications Operating System, execute the CLI command `utils network ping`. For information about the command, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions available at:


  Then reverse it by pinging from the other computers to the CAD services computer. Do this using both hostnames and IP addresses and ensure that the ping results match.

- If hostnames are used, verify that the DNS, WINS, and hosts files are correct.

- If there is a problem connecting to a particular service, try entering `telnet <IP address/hostname> <port>` in a command window, where `<IP address/hostname>` is the IP address or hostname of the computer where the service is running and `<port>` is the port used by the service.

  Do this on the machine hosting the CAD base services as well as any machine hosting a CAD desktop application.

  Consult the Port Utilization Guide for Cisco Unified Intelligent Contact Management Enterprise & Hosted for a the ports used by each CAD service.

- Use a network protocol analyzer like Ethereal to analyze network communications.

- If security or firewall software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports. Exceptions or rules should be configured to allow connects between CAD services and ports.

- Verify that dynamic IP is not being used on the CAD base services computer. Otherwise, the IP address can change and no longer match what is configured in the registry and the LDAP database.
**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. For information about the `utils firewall` command, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions available at:


To check whether a port is blocked using Telnet:

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

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

   - If the Telnet operation is successful, the command window will clear.
   - If the Telnet operation fails, a connection failure message will appear.

Do this on the machine hosting the CAD base services as well as any machine hosting a CAD desktop application.

Consult the Port Utilization Guide for Cisco Unified Intelligent Contact Management Enterprise & Hosted for the ports used by each CAD service.

- Check firewall settings on the client and server computers.
- Check firewall logs.
- If security software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports.
CAD Desktop Applications in Windows

CAD Desktop Applications Autorecovery

Agent Desktop and Supervisor Desktop

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

When Agent Desktop 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 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 10.5.


The terms in Table 13 are defined as follows:

- **Location**: Where the port needs to be opened
- **Port**: Port number
- **Protocol**: Network Protocol utilized by this port. Either TCP, UDP, or both.
- **Process**: The process that requires the port to be opened to receive network traffic
- **Client**: Client that will be sending network traffic to the port at the location
- **Notes**: Any other relevant details.

**NOTE**: All ports are designated for inbound traffic unless otherwise specified.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Process</th>
<th>Client</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>BIPPA</td>
<td>IP Phone Agent</td>
<td>Used for page push to phone from the BIPPA service.</td>
</tr>
<tr>
<td>3000</td>
<td>TCP</td>
<td>LRM</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3001</td>
<td>TCP</td>
<td>Chat</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3002</td>
<td>TCP</td>
<td>Chat</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3003</td>
<td>TCP</td>
<td>RASCAL</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3004</td>
<td>TCP</td>
<td>Enterprise</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3006</td>
<td>TCP</td>
<td>EEM</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3007</td>
<td>TCP</td>
<td>LDAP Monitor</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Process</td>
<td>Client</td>
<td>Notes</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------</td>
<td>---------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>3008</td>
<td>TCP</td>
<td>Sync</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3009</td>
<td>TCP</td>
<td>RPServer</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3010</td>
<td>TCP</td>
<td>RPServer</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3011</td>
<td>TCP</td>
<td>VoIP</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3012</td>
<td>TCP</td>
<td>VoIP</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3013</td>
<td>TCP</td>
<td>IPPA</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3014</td>
<td>TCP</td>
<td>IPPA</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3016,</td>
<td>TCP</td>
<td>LDAP</td>
<td>All CAD Services</td>
<td>OpenLDAP</td>
</tr>
<tr>
<td>38983</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3017</td>
<td>TCP</td>
<td>LDAP</td>
<td>All CAD Services</td>
<td>OpenLDAP</td>
</tr>
<tr>
<td>3102</td>
<td>TCP</td>
<td>IPPA</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3103</td>
<td>TCP</td>
<td>Enterprise</td>
<td>All CAD Services</td>
<td></td>
</tr>
<tr>
<td>3500 -</td>
<td>UDP</td>
<td>RPServer</td>
<td>Agent Desktop</td>
<td>RTP Traffic</td>
</tr>
<tr>
<td>3700</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Presence</td>
<td>Agent Desktop, Supervisor Desktop, Desktop Workflow Administrator</td>
<td></td>
</tr>
</tbody>
</table>

**Cisco Agent Desktop**  
**Location:** Client Desktop

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Process</th>
<th>Client</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>TCP</td>
<td>Chat Presence</td>
<td>Cisco Unified Presence Server</td>
<td></td>
</tr>
<tr>
<td>58000</td>
<td>UDP</td>
<td>IPC Receive event</td>
<td>custom application</td>
<td>Provides an interface to control Agent Desktop.</td>
</tr>
<tr>
<td>59015°</td>
<td>TCP</td>
<td>EemUi Java Applet</td>
<td>Agent Desktop</td>
<td></td>
</tr>
<tr>
<td>59020°</td>
<td>TCP</td>
<td>Chat Client, Monitoring &amp; Recording</td>
<td>Chat Server</td>
<td></td>
</tr>
</tbody>
</table>
Table 13. Port Utilization

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Process</th>
<th>Client</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>TCP</td>
<td>Chat Presence</td>
<td>Cisco Unified Presence Server</td>
<td></td>
</tr>
<tr>
<td>59010*</td>
<td>UDP</td>
<td>VoIP</td>
<td>VoIP Monitor Service (SPAN-based monitoring), Agent Desktop (desktop monitoring)</td>
<td></td>
</tr>
<tr>
<td>59012*</td>
<td>UDP</td>
<td>VoIP</td>
<td>VoIP Monitor Service (SPAN-based monitoring), Agent Desktop (desktop monitoring)</td>
<td></td>
</tr>
<tr>
<td>59014*</td>
<td>UDP</td>
<td>RPServer</td>
<td>Desktop Recording Service</td>
<td></td>
</tr>
<tr>
<td>59016*</td>
<td>UDP</td>
<td>RPServer</td>
<td>Desktop Recording Service</td>
<td></td>
</tr>
<tr>
<td>59021*</td>
<td>TCP</td>
<td>Chat Client</td>
<td>Chat Server</td>
<td></td>
</tr>
</tbody>
</table>

* In thin client environments (i.e. Citrix), any available port as specified by the OS ephemeral port range will be utilized.

Registry Entries

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

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

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Site Setup
For 64-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Calabrio\CAD\Site Setup

Table 14. Site setup registry entries

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Setup</td>
<td>APP VERSION</td>
<td>string</td>
<td>Used by installation scripts to identify the version of the service software.</td>
</tr>
<tr>
<td></td>
<td>CALLCENTERLANG</td>
<td>string</td>
<td>Language selected during installation.</td>
</tr>
<tr>
<td></td>
<td>DEPLOYTYPE</td>
<td>string</td>
<td>Defines the Unified CM type.</td>
</tr>
<tr>
<td></td>
<td>INSTALL DIRECTORY</td>
<td>string</td>
<td>Base install directory for Cisco software.</td>
</tr>
<tr>
<td></td>
<td>INSTALLDIR</td>
<td>string</td>
<td>Parent directory of base install directory for Cisco software.</td>
</tr>
<tr>
<td></td>
<td>IOR HOSTNAME</td>
<td>string</td>
<td>Hostname or IP address of the computer's public NIC. Value present only on the CAD services computer.</td>
</tr>
<tr>
<td></td>
<td>LDAP Bind DN</td>
<td>string</td>
<td>User ID used to log in to the LDAP service. Default = cn=Client, ou=People, ou=Spanlink Communications.</td>
</tr>
<tr>
<td></td>
<td>LDAP Connection Timeout</td>
<td>dword</td>
<td>Maximum time, in seconds, before a connection attempt times out. Default = 15.</td>
</tr>
<tr>
<td></td>
<td>LDAP Heartbeat Enabled</td>
<td>dword</td>
<td>Is heartbeat enabled? 1 = yes, 0 = no. Default = 1.</td>
</tr>
</tbody>
</table>
Table 14. Site setup registry entries — *Continued*

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Setup</td>
<td>LDAP Heartbeat Retry Time</td>
<td>dword</td>
<td>Heartbeat time, in milliseconds. Default = 10000.</td>
</tr>
<tr>
<td></td>
<td>LDAP Host 1</td>
<td>string</td>
<td>LDAP service hostname/IP address. There can be multiple LDAP hosts.</td>
</tr>
<tr>
<td></td>
<td>LDAP LCC</td>
<td>string</td>
<td>Default logical contact center</td>
</tr>
<tr>
<td></td>
<td>LDAP Port 1</td>
<td>dword</td>
<td>LDAP service port. There can be multiple LDAP ports. Default = 3016.</td>
</tr>
<tr>
<td></td>
<td>LDAP Pwd</td>
<td>string</td>
<td>Encrypted user password</td>
</tr>
<tr>
<td></td>
<td>LDAP Request Timeout</td>
<td>dword</td>
<td>Maximum time, in seconds, before an LDAP request times out. Default = 15.</td>
</tr>
<tr>
<td></td>
<td>LDAP Root</td>
<td>string</td>
<td>Root of the LDAP data. Default = o=Spanlink Communications.</td>
</tr>
<tr>
<td></td>
<td>MONITOR DEVICE</td>
<td>string</td>
<td>Network card on which to sniff packets.</td>
</tr>
<tr>
<td></td>
<td>ProductCode_Agent</td>
<td>string</td>
<td>Agent Desktop product code.</td>
</tr>
<tr>
<td></td>
<td>ProductCode_Supervisor</td>
<td>string</td>
<td>Supervisor Desktop product code.</td>
</tr>
<tr>
<td></td>
<td>ProductCode_Admin</td>
<td>string</td>
<td>Desktop Administrator product code.</td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
<td>dword</td>
<td>Counter to indicate changes to site setup values. Default = 0.</td>
</tr>
</tbody>
</table>
Enterprise Service

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Calabrio\CAD\Enterprise Data
For 64-bit machines:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Calabrio\CAD\Enterprise Data

Table 15. Enterprise Service registry entries

<table>
<thead>
<tr>
<th>Key</th>
<th>Value*</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>Max Wait Time</td>
<td>dword</td>
<td>Maximum time, in milliseconds, to wait for enterprise data. Default = 100.</td>
</tr>
<tr>
<td>Initial Time</td>
<td>dword</td>
<td></td>
<td>Number of milliseconds to wait after the first request for enterprise data, if data is not guaranteed. Default = 10.</td>
</tr>
<tr>
<td>Increment</td>
<td>dword</td>
<td></td>
<td>Number of milliseconds to add to the retry time at each interval, if data is not guaranteed. Default = 20.</td>
</tr>
<tr>
<td>Retry Sleep Interval</td>
<td>dword</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

* 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\SOFTWARE\Wow6432Node\Calabrio\CAD\Recording & Playback Client

Table 16. RecordingPlaybackClient key value

<table>
<thead>
<tr>
<th>Key</th>
<th>Value*</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup From Client Port</td>
<td>number</td>
<td>Port</td>
<td>The port on the supervisor’s desktop that is used to receive the “From Agent” audio stream for playback sessions.</td>
</tr>
<tr>
<td>Jitter Buffer number</td>
<td>number</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Port Range End number</td>
<td>number</td>
<td></td>
<td>End of range of port numbers to use for recording. Each simultaneous recording requires two ports.</td>
</tr>
<tr>
<td>Port Range Start number</td>
<td>number</td>
<td></td>
<td>Start of range of port numbers to use for recording. Each simultaneous recording requires two ports.</td>
</tr>
<tr>
<td>Sound Buffers number</td>
<td>number</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>To Client Port number</td>
<td>number</td>
<td></td>
<td>The port on the supervisor’s desktop that is used to receive the “To Agent” audio stream for playback sessions.</td>
</tr>
<tr>
<td>VPN Port number</td>
<td>number</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

* 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 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 48.

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
   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 reconveting 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.


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 comprised of two files:

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

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

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

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

where:

- `<YYYYMMDD>` 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 increased 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 CAD has problems, check that:

- The computers that host CAD services, Unified CM, Unified CCX, Microsoft Exchange and other system components are running.
- The registry is correct (see "Registry Check" on page 53).
- The network is set up correctly (see "Network Check" on page 53).
- The CAD services are running and active (see "Active Service Check" on page 50).
- The Agent Desktop Configuration Setup utility has run correctly. See the Cisco CAD Installation Guide for more information.

Active Service Check

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

For Nonredundant Systems

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

For Redundant Systems

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

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 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 Microsoft Support article (Article ID: 189326) 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:

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 VXNlc3hbwU6
bXluYWll
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....Recipient 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:
http://support.microsoft.com/kb/q153119/

Registry Check

Using Windows Regedit:

- Verify that HKEY_LOCAL_MACHINE\Software\Calabrio\CAD\Site Setup (in case of 64-bit machines, HKEY_LOCAL_MACHINE\Software\Wow6432Node\Calabrio\CAD\Site Setup) exists and contains the entries specified in "Site Setup" on page 43.
- Verify that the registry entries used by specific services exist and are valid. See "Registry Entries" on page 42.

Network Check

- To view information about the NICs on the CAD desktop 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 CAD desktop computer to others in the configuration, for example, the Unified CM computer. Then reverse it by pinging from the other computers to the CAD desktop 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. Do this on the machine hosting the CAD base services as well as any machine hosting a CAD desktop application.

Consult the Port Utilization Guide for Cisco Unified Intelligent Contact Management Enterprise & Hosted for the ports used by each CAD service.

- Use a network protocol analyzer like WireShark (www.wireshark.com) to analyze network communications.

- If security or firewall software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports. Exceptions or rules should be configured to allow connects between CAD services and ports.

- Verify that dynamic IP is not being used on the CAD base services computer. Otherwise, the IP address can change and no longer match what is configured in the registry and the LDAP database.

Memory Check

- Ensure that the amount of memory on the computer is at least the minimum required for CAD and other installed software. If the amount of memory is below the recommended level, it could be the source of the problem.

- Use Microsoft Perfmon (perfmon.exe) to perform most memory checking.

  Add the following counters for _Total and process of interest:

  - Private Bytes
  - Virtual Bytes
  - Handle Count
  - Thread Count
If the values for those counters keep growing without leveling or decreasing, it is likely the process has a memory leak.

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

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

### CPU Check

- Ensure that the computer’s processor is at least the minimum required for CAD and other installed software. If the processor is below the recommended level, it could be the cause of the problem.

- Use Task Manager to sort processes/applications by CPU usage. Check which process seems to be using the CPU most of the time.

- Use Windows Perfmon (perfmon.exe) for additional CPU checking.
  - Add the %Processor Time counter for Processor > _Total and each CPU as well as Process >_Total and process of interest.
  - Check which process seems to be using the CPU most of the time.
  - If the counter values for a process are a significant part of the total CPU use, it may be of concern. Short spikes are acceptable but a significant time with high CPU usage is of concern.

- Try rebooting the computer to see if it fixes the problem.

### Blocked Ports Check

To check whether a port is blocked:

- Using Telnet:
  1. Ensure that the service is running and active.
  2. From the command line, type 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.
If security software is running on the computer, check its reports and/or logs to see if it is blocking any communication or ports.
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 17 describes the application behavior under the following power options in Microsoft Windows.

Table 17. Behavior under Microsoft Windows Power Options

<table>
<thead>
<tr>
<th>Application</th>
<th>When system is in the standby mode</th>
<th>When either monitor or hard disk is turned off</th>
</tr>
</thead>
</table>
| Agent Desktop    | • Agent Desktop is disconnected from the CAD servers  
                    • UCCX server logs out the agent  
                    • Agent is not displayed on Supervisor Desktop  
                    • Agent Desktop neither displays phone activity nor provides call control  
                    • When the agent restores the system, Agent Desktop attempts auto-recovery  
                    • When Agent Desktop is recovered, agent logs in and is automatically moved to the Not Ready state | • Agent Desktop remains connected with the CAD servers  
                    • Agent is displayed on Supervisor Desktop  
                    • Agent can answer both ACD and non-ACD calls |
| Supervisor Desktop | • 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 |
### Table 17. Behavior under Microsoft Windows Power Options

<table>
<thead>
<tr>
<th>Application</th>
<th>When system is in the standby mode</th>
<th>When either monitor or hard disk is turned off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Work Flow Administrator</td>
<td>• Desktop Work Flow Administrator is disconnected from the CAD server</td>
<td>• Desktop Work Flow Administrator remains connected with the CAD server</td>
</tr>
<tr>
<td></td>
<td>• When the system is restored, Desktop Work Flow Administrator attempts autorecovery</td>
<td></td>
</tr>
</tbody>
</table>
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 (x86)\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 18 lists the event, error, and chat message logs generated by CAD.

<table>
<thead>
<tr>
<th>Service/Application</th>
<th>Log Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Desktop</td>
<td>agent.log</td>
</tr>
<tr>
<td>Backup and Restore utility</td>
<td>CDBRTool.log</td>
</tr>
<tr>
<td>BIPPA service</td>
<td>IPPASvr.log</td>
</tr>
<tr>
<td>BIPPA service JSP client</td>
<td>IPPAClient.log</td>
</tr>
<tr>
<td>CAD Configuration Setup</td>
<td>PostInstall.log</td>
</tr>
<tr>
<td>CAD uninstall process</td>
<td>fcuninstall.log</td>
</tr>
</tbody>
</table>
### Table 18. CAD event, error, and chat message logs — Continued

<table>
<thead>
<tr>
<th>Service/Application</th>
<th>Log Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat client</td>
<td>monday.txt, tuesday.txt, wednesday.txt, thursday.txt, friday.txt, saturday.txt, sunday.txt</td>
</tr>
<tr>
<td>Chat service</td>
<td>FCCServer.log</td>
</tr>
<tr>
<td>Desktop Administrator:</td>
<td></td>
</tr>
<tr>
<td>Desktop Configuration:</td>
<td>administrator.log</td>
</tr>
<tr>
<td>Desktop Administrator:</td>
<td></td>
</tr>
<tr>
<td>Enterprise Data Configuration:</td>
<td>TSSPAdm.log</td>
</tr>
<tr>
<td>Desktop Administrator:</td>
<td></td>
</tr>
<tr>
<td>framework</td>
<td>Splkview.log</td>
</tr>
<tr>
<td>Desktop Administrator:</td>
<td></td>
</tr>
<tr>
<td>Unified CCE Configuration:</td>
<td>IPCCAdm.log</td>
</tr>
<tr>
<td>Desktop Administrator:</td>
<td></td>
</tr>
<tr>
<td>Personnel Configuration:</td>
<td>personnel.log</td>
</tr>
<tr>
<td>Desktop Monitoring Console:</td>
<td>SMC.log, SMCGetServerList.log</td>
</tr>
<tr>
<td>Directory Services Replication:</td>
<td>slurpd.log</td>
</tr>
<tr>
<td>Enterprise service</td>
<td>CTIStorageServer.log, WorkflowEngine.log</td>
</tr>
<tr>
<td>LDAP Monitor service</td>
<td>LDAPMonSrv.log</td>
</tr>
<tr>
<td>License Administrator</td>
<td>LicensingAdmin.log</td>
</tr>
<tr>
<td>LRM service</td>
<td>LRMServer.log</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>openldap.log</td>
</tr>
<tr>
<td>Recording &amp; Playback service</td>
<td>RPServer.log</td>
</tr>
</tbody>
</table>
### Table 18. CAD event, error, and chat message logs — Continued

<table>
<thead>
<tr>
<th>Service/Application</th>
<th>Log Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording and Statistics service</td>
<td>• FCRasSvr.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_ads.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_ads.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_ads.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_base.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_base.fcrassvr.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_repl_base.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_utils_base.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_utils_base.fcrassvr.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.cra_utils_base.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.instrasdb.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.instrasdb.fcrassvr.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.instrasdb.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.repl_base.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.repl_base.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.repl_base.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.sp_make_publisher.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.sp_make_publisher.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.sp_spk_drop_publisher.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.sp_spk_drop_publisher.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.truncate.fcrassvr.pub.sql.log</td>
</tr>
<tr>
<td></td>
<td>• db.truncate.fcrassvr.sub.sql.log</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The db.*.log files exist only in systems that use SQL Server.</td>
</tr>
<tr>
<td>Supervisor Desktop, Supervisor Record Viewer</td>
<td>• supervisor.log</td>
</tr>
<tr>
<td></td>
<td>• EemSupervisor.log</td>
</tr>
<tr>
<td>Supervisor Workflow Administrator</td>
<td>SWFAdmin.log</td>
</tr>
<tr>
<td>Sync service</td>
<td>DirAccessSynSvr.log</td>
</tr>
<tr>
<td>VoIP Monitor service</td>
<td>FCVoIPMonSvr.log</td>
</tr>
</tbody>
</table>
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 (x86)\Cisco\Desktop\log\transcripts\n
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 19 lists the configuration files used by CAD desktop applications. Table 20 lists the configuration files used by CAD services.

Table 19. CAD desktop applications configuration files

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent.cfg</td>
<td>Agent Desktop</td>
</tr>
<tr>
<td>EemUi.properties</td>
<td>Agent E-Mail on agent desktop</td>
</tr>
<tr>
<td>EemSupervisor.properties</td>
<td>Supervisor Desktop (for E-Mail related actions)</td>
</tr>
<tr>
<td>Administrator.cfg, Splkview.cfg</td>
<td>Desktop Work Flow Administrator</td>
</tr>
<tr>
<td>PostInstall.cfg</td>
<td>CAD Configuration Setup</td>
</tr>
<tr>
<td>Supervisor.cfg</td>
<td>Supervisor Desktop</td>
</tr>
<tr>
<td>SupervisorLogViewer.cfg</td>
<td>Supervisor Record Viewer</td>
</tr>
<tr>
<td>SWFAdmin.cfg</td>
<td>Supervisor Work Flow Administrator</td>
</tr>
</tbody>
</table>

Table 20. CAD services configuration files

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>bars.properties</td>
<td>Backup and Restore utility</td>
</tr>
<tr>
<td>CTIStorageServer.cfg</td>
<td>Enterprise service</td>
</tr>
<tr>
<td>DirAccessSynSvr.cfg</td>
<td>Sync service</td>
</tr>
<tr>
<td>EEMServer.cfg</td>
<td>Agent E-Mail service</td>
</tr>
<tr>
<td>EEMServerJava.properties</td>
<td>Agent E-Mail service Java engine</td>
</tr>
<tr>
<td>FCCServer.cfg</td>
<td>Call/Chat service</td>
</tr>
<tr>
<td>FCRasSvr.cfg</td>
<td>Recording and Statistics service</td>
</tr>
<tr>
<td>FCVoIPMonSvr.cfg</td>
<td>VoIP Monitor service</td>
</tr>
<tr>
<td>IPPAClient.properties</td>
<td>BIPPA service JSP client</td>
</tr>
<tr>
<td>IPPASvr.cfg</td>
<td>BIPPA service</td>
</tr>
<tr>
<td>LDAPMonSvr.cfg</td>
<td>LDAP Monitor service</td>
</tr>
<tr>
<td>LRMServer.cfg</td>
<td>LRM service</td>
</tr>
</tbody>
</table>
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 21 summarizes the default and configured behavior settings.

Table 21. Outbound call statistic handling

<table>
<thead>
<tr>
<th>Total</th>
<th>Outbound Calls</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default behavior</td>
<td>Configured behavior</td>
</tr>
<tr>
<td>Calls Presented</td>
<td>Not counted</td>
<td>Counted</td>
</tr>
<tr>
<td>Calls Handled</td>
<td>Not counted</td>
<td>Counted if answered</td>
</tr>
</tbody>
</table>

**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.

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

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

5. Scroll down to the Desktop Services section. You can view and monitor the CAD services. See "Changing CAD Services Status" on page 69 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.


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 statuses.

- IN SERVICE
- PARTIAL SERVICE
- OUT OF SERVICE
- SHUTDOWN
- NOT CONFIGURED

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 67 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 23 for information on CAD services.

The specified CAD service status changes.
Debugging Logs

CAD can create debugging logs to help with troubleshooting.

**NOTE:** When upgrading from CAD 6.4 to CAD 10.5, 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 (x86)\Cisco\Desktop\log. Exceptions are:

**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 75 for information on collecting logs. See "Configuring Debugging" on page 70 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, Desktop Administrator, Backup and Restore, and Desktop IP Phone Agent Service (page 71).
- For all other CAD services and applications, see Configuring Debugging for non-Java Applications (page 74).
- For Java applications, Enabling Debugging for Java Applications (page 73).
For a complete list of services/applications and their corresponding configuration files, see Table 19 on page 64 and Table 20 on page 64.

**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 that the size of the debug file increases. Running services at a higher debugging threshold during normal operations can have a significant impact on performance. Table 22 lists the available debugging thresholds.

**Table 22. Debugging thresholds**

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Events Recorded</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 |
| OFF       | Turns off debugging. |

**Configuring Debugging Thresholds for CAD Services, Desktop Administrator, Backup and Restore, and Desktop IP Phone Agent Service**

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, Desktop Administrator, Backup and Restore, and Desktop IP Phone Agent Service 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 67 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).

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 22 on page 71 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.

You must restart the Cisco Unified CCX Administration for IP Phone Agent and Desktop Administration for the new settings to take effect.

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 23 for information on CAD services’s preferences files.

You must restart the Cisco Unified CCX Administration for IP Phone Agent and Desktop Administration for the new settings to take effect.

Enabling Debugging for Java Applications

To enable debugging for Java applications:

1. For the Agent E-Mail applet, navigate to the folder (default path) `C:\Program Files (x86)\Cisco\Desktop\EEM-config`.

2. Move the properties files to the folder `C:\Program Files (x86)\Cisco\Desktop\config`.

NOTE: When logging is enabled for Agent E-Mail, users might receive a security warning from the JRE when starting the application. For more information, refer to the following Oracle documentation: https://blogs.oracle.com/java-platform-group/entry/updated_security_baseline_7u45_impacts

3. 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
   ```
4. 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.

```plaintext
#log4j.rootLogger=INFO,LOG,DBG
#log4j.rootLogger=DEBUG,LOG,DBG
log4j.rootLogger=CALL#com.calabrio.util.log.SlkLevel,LOG,DBG
#log4j.rootLogger=TRACE,LOG,DBG
#log4j.rootLogger=DUMP#com.calabrio.util.log.SlkLevel,LOG,DBG
```

5. 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 (x86)\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 "Debugging Thresholds" on page 71 for more information. For example:
   ```plaintext
   Threshold=DEBUG
   ```
4. Save the configuration file with the new setting. You must restart the 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 70). 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 you to check CPU, Memory, and Disk Usage. For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at:

## Known Problems With Workarounds

### Agent Desktop Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>When starting Agent Desktop, the following warning pops up: Block potentially unsafe components from being run?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Causes</strong></td>
<td>This occurs if you are running JRE 7 update 45. However, Oracle increased the security baseline to a newer JRE 7 update. This prevents Agent E-Mail from functioning with JRE 7 update 45.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Click the Don’t Block button to continue using Agent Desktop. Agent E-Mail will not function correctly until JRE 7 update 51 or later is installed. Contact your administrator to update your machine.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Partial call history or partial data appears in the Enterprise Data fields for calls right after a failover.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symptom</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cause</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>This is expected behavior. A call that occurs when the Enterprise service is up and running after a failover will have complete data.</td>
</tr>
</tbody>
</table>
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.
Agent Desktop Problems

- 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.
- The correct JRE version is not installed.

---

**Problem**  
In Windows 7, some of the Agent Desktop interface is not displayed properly.

**Cause.** The custom DPI setting is above 150% and Use Windows XP style DPI scaling is selected in Control Panel > Display > Set custom text size (DPI).

**Solution**  
Clear the Use Windows XP style DPI scaling check box in Control Panel > Display > Set custom text size (DPI). This allows the client machine to use Vista style scaling with a DPI over 150%.

---

**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 MS 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: 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: Ensure that the following do not occur concurrently:

- An agent’s Unified CCX extension with the same digit as a dial plan 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 they are. 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 Floods 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 or Desktop Work Flow Administrator, but they are not showing up in Agent Desktop.

**Solution** Agent Desktop must be restarted in order for the changes to take effect.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agent has changed Agent Desktop's window behavior (from the File</td>
<td>Changes made to local settings via Agent Desktop are only temporary overrides of the global settings. Permanent changes must be made via Desktop Administrator.</td>
</tr>
<tr>
<td>menu), but when Agent Desktop is restarted, the setting has not been</td>
<td></td>
</tr>
<tr>
<td>saved.</td>
<td></td>
</tr>
<tr>
<td>Sometimes during a conference call, a conference member shows up as</td>
<td>&lt;Unavailable&gt; represents a party outside the switch. The switch sends the trunk number of the</td>
</tr>
<tr>
<td>&lt;Unavailable&gt;.</td>
<td>external party to the desktop, where it has no meaning. Agent Desktop replaces the trunk number with</td>
</tr>
<tr>
<td></td>
<td>&lt;Unavailable&gt;.</td>
</tr>
<tr>
<td>The agent sent the supervisor an emergency chat message but the</td>
<td>Supervisors receive emergency chat messages only if they are monitoring the team to which the agent</td>
</tr>
<tr>
<td>supervisor never received it.</td>
<td>who sent the message belongs.</td>
</tr>
<tr>
<td>While running Agent Desktop, the error message, “Macro file failed to</td>
<td>Turn off any virus scanning applications on the desktop. Virus scanning applications attempt to</td>
</tr>
<tr>
<td>open,” keeps appearing.</td>
<td>intercept calls to open a file to do their own processing first. This might cause the file to be</td>
</tr>
<tr>
<td></td>
<td>opened in such a way that restricts other applications from opening the file.</td>
</tr>
<tr>
<td>The agent cannot view any skills statistics in Agent Desktop.</td>
<td>If an agent is not assigned to a skill group, no skills statistics are available.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Problem: The agent is using Agent Desktop 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 and 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.
Agent Desktop Problems

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: When opening the Agent Real Time Displays, <N/A> is displayed in the first row.

Solution: If there is no data for the selected day, the first row of the log 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’s PC freezes when a macro executes at the same time that Outlook has focus.

**Message.**  The following message appears in the DesktopInteractive logs: “Possible cause is another application blocking macro processing. See the CAD Troubleshooting Guide for possible resolution.”

**Solution**  To resolve this issue, follow these steps:

1. On the client PC, open the Windows Registry and navigate to the following key:
   
   HKEY_CURRENT_USER\Control Panel\Desktop

2. Locate the value named “ForegroundLockTimeout”. If it does not exist, right-click the registry pane and create a new DWORD with that name.

3. Set the value data of the value to 0. This will cause the application to take the focus instantly.

4. Reboot the client PC.
Problem: While running in stealth mode, macros might fail to execute properly if Outlook has focus.

Solution: In order to have macro's execute properly while Outlook has focus, change the Agent Desktop preferences so that Agent Desktop runs in a mode OTHER than stealth mode.

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

Solution: In Agent Desktop, 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: The agent tries to complete a blind conference via workflow. However, the agent winds up with two separate calls. The agent connects to the conference destination and the original calling party is on hold.

Cause. The CAD workflow fails to complete a blind conference, because the dialed phone number contains too many digits which takes too long to complete through the Call Manager.

Solution: The agent should press the conference soft key on the IP phone to join all parties. Contact your administrator to configure the workflow with a phone number containing fewer digits.

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.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| When trying to view agent state or call logs, no data is presented. | 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. |

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>After an upgrade, the Report Font Size field is blank on the Accessibility Options tab of the Desktop Preferences dialog box in Agent Desktop.</td>
<td>Select a font size from the drop-down list. The minimum report font size is 15.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An agent’s screen reader is not reading the contents of table cells in agent reports.</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| After upgrading to CAD 10.5, agents do not see their global and/or personal phone books. The phone books were available before the upgrade. | The phone books must be enabled in Desktop Work Flow Administrator.  
1. In Desktop Work Flow 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. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An administrator cannot telnet from the Unified CCX server to a desktop hosting a CAD application.</td>
<td>Any firewall between the Unified CCX server and the desktop must have ports 59000–59030 open so that access to the desktop is allowed.</td>
</tr>
<tr>
<td>Agent Desktop closes unexpectedly when agent is using the integrated browser.</td>
<td>This issue 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.</td>
</tr>
<tr>
<td>Agent Desktop cannot be launched and one of a number of licensing errors is displayed.</td>
<td>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. Verify the IP address of LDAP Host 1 and LDAP Host 2 in the preferences files and registry entries. See &quot;Site Setup&quot; on page 25 and &quot;Site Setup&quot; on page 43 for more information. If the correct IP address still cannot be pinged, contact your network administrator to fix the network issue.</td>
</tr>
<tr>
<td>The real time displays (reports) generated for the day of the week are not accurate.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 while in the Work state, some of the Outbound Dialer toolbar buttons are disabled.

Solution
If an agent uses a multi-line 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 Desktop Administrator, go to Services Configuration > Multiline, Monitoring & Recording > Display Settings and disable the Display Non-ACD Call check box.

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

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

The agent can ignore the error message, close the message dialog box, and continue as before.
Problem: Agent Desktop does not start when the agent double-clicks the icon.

Solution: Open Task Manager. On the Processes tab, if agent.exe is listed, then Agent Desktop is already running. You cannot open more than one instance of Agent Desktop at the same time.

Select agent.exe and click End Process. Close Task Manager, and then relaunch Agent Desktop.

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

Solution: The OS variable SESSIONNAME was not updated when the agent logged out. If this variable is set to RDP-<session number> or ICA-<session number>, the system looks at the HOMESHARE variable for the agent’s home directory, where that agent’s logs and configuration files are stored. If the SESSIONNAME variable is not cleared, then Terminal Services sees the agent as logged in. This can happen if the agent does not log off of Terminal Services cleanly after logging out of CAD. To log out cleanly, the agent must select Log Out from the Terminal Services dialog box drop-down list and then click OK.

Problem: 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.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>During a failover, the agent receives an error message stating that an Agent State change failed.</td>
<td>Once the failover is complete, select OK to dismiss the dialog. Agent State changes should be successful going forward.</td>
</tr>
</tbody>
</table>
| The Ctrl+Shift+0 shortcut key does not select the first browser tab in Agent Desktop with Windows 7. | To workaround this issue, follow these steps:  
1. Select Control Panel > Region and Language, and then select the Keyboards and Languages tab.  
2. Click the Change keyboards button.  
3. On the Text Services and Input Languages window, select the Advanced Key Settings tab.  
4. Select Between input languages from the Action list, and then click the Change Key Sequence button.  
5. On the Change Key Sequence window, select Not Assigned in the Switch Input Language list and the Switch Keyboard Layout list.  
6. Click OK to save your changes and dismiss Change Key Sequence window.  
7. On the Text Services and Input Languages window, click Apply and then click OK to dismiss the window.  
8. On the Region and Language window, click OK to dismiss the window. |
Agent Desktop Problems

Problem
Agent Desktop crashes when the agent accesses a web site via the integrated browser. The agent is using Internet Explorer 8.

Cause: The website has formatting problems that forces IE 8 to attempt to go into compatibility mode and is suggested to emulate IE 9, but IE 8 is unable to do so and instead changes to a compatibility mode that has been known to crash the integrated browser.

Solution
To resolve this issue, try these options:

1. Upgrade to IE 9 or later.
2. Access Control Panel > Internet Options > Advanced tab and clear the check box for “Automatically recover from page layout errors with Compatibility View”. This prevents IE from forcing Compatibility view on sites you do not want it to.

If you must continue to use IE 8, edit the Windows registry as follows:

1. In the Windows registry, navigate to the following location:
   - 32-bit machine: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION
   - 64-bit machine: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION
2. Delete the following DWORD key values:
   - agent.exe  [Data value = 9999 (decimal)]
   - supervisor.exe  [Data value = 9999 (decimal)]

   If IE 8 is upgraded to IE 9 or later after this registry change is completed, the deleted key values must be re-added to the registry.

Problem
The integrated browser does not support web sites that use cross-domain Adobe Flash.

Symptom. Agent Desktop and Supervisor Desktop crash when the integrated browser accesses a web site that uses cross-domain Adobe Flash. This occurs on desktops using Windows 8.1 and Adobe Flash versions 13.0.0.182 through 13.0.0.214.
Solution  Uninstall Windows Updates for Flash starting with KB2942844 (Flash 13.0.0.182) through KB2961887 (Flash 13.0.0.214).
Agent E-Mail Problems

It is recommended that you apply the latest Service Packs, updates, and patches released by Microsoft to MS Exchange. However, doing so might result in the need to re-configure the settings.

---

**Problem**

Agent E-Mail does not work. The Agent E-Mail applet displays a “Loading...” animation that never completes. If you turn on the Java Console with Tracing, Logging, and Applet life cycle exceptions enabled, you can see the following message during Agent E-Mail start up:

security: LiveConnect (JavaScript) blocked due to security settings.

**Cause.** With Java 7 Update 25, Oracle introduced a feature that blocks LiveConnect when the user’s JRE does not meet the JRE security baseline. The security baseline is published by Oracle and updated as security vulnerabilities are fixed in newer JRE updates. When the Agent E-Mail applet starts, the JRE checks this security baseline. If the required JRE is higher than the JRE version the user is currently running, or if the security baseline cannot be found and the current JRE is expired, Agent E-Mail no longer works.

**Solution**

JRE 1.7 Update 45 is no longer supported due to Oracle changing the security baseline. You must update to JRE 1.7 Update 51 or later. Future JRE updates might render Agent E-Mail unusable due to the LiveConnect blocking feature and the security baseline. If this is the case, you must perform one of the following workarounds:

- Update each user’s JRE version to meet the security baseline.
- Move the security slider of each user’s Java Control Panel to a setting lower than High
- Add Cisco Agent Desktop to the Exception Site List. For more information, refer to the following Oracle documentation:

  [http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/exception_site_list.html](http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/exception_site_list.html)

- Create a Deployment Rule Set (DRS) and distribute it throughout the contact center. For more information on how to create and distribute your own DRS, refer to the following Oracle documentation:

  [http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/deployment_flow.html#rules](http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/deployment_flow.html#rules)
**Problem**  
Agent E-Mail does not work. The Agent E-Mail applet displays a “Loading...” animation that never completes. The Agent E-Mail buttons never become active.

**Cause.** If Agent E-Mail won’t load after JRE 7 Update 51 has been installed, then it is possible the Agent E-Mail Java applet was denied through user input when Agent Desktop launched previously. For example, the user might have selected Don't Run or Block in response to one of the Java security prompts that appear when starting Agent E-Mail.

**Solution**  
You can restore the security prompts that were hidden prior to installing Update 51.

To restore the prompts that were previously hidden:

1. Navigate to Control Panel > Java.
2. On the Java Control Panel window, select the Security tab. Click the Restore Security Prompts button.
3. When asked to confirm your selection, click Restore All.
4. Click Apply and then OK to close the window.

The next time Agent Desktop is opened, the security prompt will be shown. Select Don’t Block.

---

**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 50 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 MS 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 in Agent 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 MS 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 do not 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 Agent Desktop is closed. Once Agent Desktop 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 might 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 Agent 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 and manually delete the e-mail from the inbox. See the “Testing Access to the Agent E-Mail Account” section of the Cisco CAD Installation Guide.

Problem: A supervisor cannot use a supervisor work flow 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 MS 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.
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 work flow group.
- In Work Flow Administrator, the e-mail buttons are visible for the agent’s work flow group.
- The correct JRE version is installed.

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 MS 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.

MS Exchange has not been configured to allow the Agent Desktop SMTP user permission to send from the e-mail address specified in 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:

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.
5. Restart the Agent E-Mail service for the MS 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 Agent Desktop 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 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  MS Exchange 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 Windows 7.

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

**Solution**  
Make sure JRE 1.7 Update 51 is installed. 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 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.
Agent E-Mail Problems

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.

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\Parameters\System.

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:


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

The throttling policies have been 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:


---

**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. Select the Advanced tab.
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(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 32 for more information.

Problem: After an upgrade or downgrade, Agent E-Mail icons are disabled and e-mail messages are not loading successfully.

Solution: On each client machine, you must clear both the Internet Explorer history and the Java caches to ensure the proper applet files are downloaded again after the upgrade or downgrade.

To clear the browser history in Internet Explorer:
1. Navigate to Control Panel > Internet Options.
2. On the General tab, in the Browser history section, click the Delete button.
3. On the Delete Browsing History dialog, ensure that the Temporary Internet files and website files check box is selected, and then click Delete.
4. Click OK to dismiss the Internet Options dialog.

To clear the Java cache:
1. Navigate to Control Panel > Java.
2. On the Java Control Panel dialog, on the General tab, click the Settings button.
3. On the Temporary Files Settings dialog, click the Delete Files button, and then Click OK to dismiss the dialog.
4. Click OK on the Java Control Panel dialog to dismiss the dialog.

Problem: When Agent Desktop is started, the E-mail Ready and E-mail Not Ready toolbar buttons are disabled. The agent is assigned to an e-mail CSQ.

The Java Console or EemUi.dbg logs indicate that the email client cannot connect on port 59015.
Solution: This issue appears when CAD and/or Java have been recently installed on the system, and a system restart has not yet occurred.

To resolve this issue, restart the computer.

Problem: Syslog alerts show the following:

```
419: mc-spcr-ccx1.marketingconcepts.com: Feb 24 2015 13:45:31.892 UTC : %UC_FCRASSVR-3-FCRasServer2109: %[ServiceName=FCRasServer][error Id=FCRasServer2109][Message=Failure when executing query [INSERT INTO EEMEmailAgentStateDetail (agent, emailUIDonMailServer, eventStartDateTime, eventStartDa][ClusterID=][NodeId=mc-spcr-ccx1]: Failure when executing query
```

Condition: This issue is seen after an upgrade.

Solution: There is a column called “emailstatusFK” that is missing for the EEMEmailAgentStateDetail table during the upgrade from Windows versions. Because of this, all the inserts into the EEM Table will fail. You can check it via the following command:

```
show uccx dbtable schema db_cra EEMEmailAgentStateDetail
```

If this does not show the column, then this will have to be manually created using the following procedure:

```
IF NOT EXISTS (SELECT 1 FROM SysColumns WHERE ColName = 'emailstatusfk') THEN

ALTER TABLE EEMEmailAgentStateDetail ADD (emailStatusFK int);

END IF;
```

To do this:

1. Root the box.
2. su Informix
3. source /opt/cisco/uccx/bin/uccx_ids.env
4. 'dbaccess db_cra' and execute the above SQL
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 Service Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can I tell if a CAD service is running?</td>
<td>Verify if a CAD service is running. See &quot;Logging into Unified CCX Serviceability and Monitoring CAD Services&quot; on page 67 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.</td>
</tr>
<tr>
<td>How can I check if the Unified CCX services are running?</td>
<td>Verify if a Unified CCX services are running. See &quot;Logging into Unified CCX Serviceability and Monitoring CAD Services&quot; on page 67 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.</td>
</tr>
</tbody>
</table>
| The message, “At least one or more errors occurred during synchronization” appeared when the administrator performed synchronization in Desktop Administrator. | 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 and LDAP Host 2 in the preference files have the correct values. |
| How can I tell if the Tomcat webserver is installed correctly? | Perform the following tests: |
CAD Service Problems

- Verify if Unified CCX Administration and the BIPPA service are running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 67 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>/ipphone/jsp/sciphonexml/IPAgentInitial.jsp

If these tests fail, check the following:

- JRE is installed on the server.

- The file that maps URLs with JSP pages to the correct java servlets, web.xml, must be in the /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: 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: 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. 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 determined to be two representations of the same party.

Problem: Approximately 30 to 40 seconds after sending a chat message the agent receives the error message, “SYSTEM [##:##]:<Username> did not receive your message because the message could not be sent.”
Solution: This situation can arise when the Cisco Unified Presence server fails over. This is a known issue. No workaround is available. The problem persists until the failover has completed. The agent should wait and try sending the chat message again.
# Call/Chat Service Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>How can I tell if the Call/Chat and LDAP Monitor services are running?</th>
</tr>
</thead>
</table>
| Solution| Verify if the Call/Chat and LDAP Monitor services are running. See "Logging into Unified CCX Serviceability and Monitoring CAD Services" on page 67 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  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.

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.
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.

NOTE: If you are using digest authentication, verify that the digest credentials for the user match the password.

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 IM and Presence publish trunk is not configured correctly.

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

1. Log into Unified Presence Administration.
3. Verify that the correct trunk is selected in the CUCM IM and Presence Publish Trunk drop-down list.

For more information about publish trunks in Unified CM, see the Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND).
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 IM and Presence publish trunk is not configured correctly.

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

1. Log into Unified Presence Administration.
3. Verify that the correct trunk is selected in the CUCM IM and Presence 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 publish trunks in Unified CM, see the *Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)*.

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.

- In Unified Presence Administration, choose Presence > Settings. Verify that Allow users to view the availability of other users without being prompted for approval is enabled.

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

### Solution
Perform the following checks.

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

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

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

An agent or supervisor cannot log into Cisco Unified Presence.

**Solution**

The agent’s or supervisor’s Unified Presence login ID should match the format of the administrator’s Unified Presence login ID.

The following login ID formats are supported:

- `<username>`
- `<username>@<domain>`

If one format does not work, the agent or supervisor should log in using the other format.

**Problem**

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

**Solution**

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

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

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

1. Log into Unified Presence Administration.

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**  
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, one of 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.

---

**Problem**  
After upgrading Cisco Unified Presence, CAD is unable to log in to the Unified Presence server. Verifying Unified Presence credentials through Desktop Administrator does not work.

**Solution**  
After upgrading Unified Presence, you might need to add the CAD client type to Unified Presence Administration again. The CAD client type does not carry over. For more information, refer to the “Configuring the CAD Client Type” section of the *Cisco Desktop Administrator User Guide*. 
## Desktop Work Flow Administrator Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An imported phone book containing multibyte characters displays those</td>
<td>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 &gt; Control Panel &gt; Regional and Language Options. On the Advanced tab, select the multibyte language as the language to use for non-Unicode programs.</td>
</tr>
<tr>
<td>characters as vertical lines (</td>
<td></td>
</tr>
<tr>
<td>The administrator cannot create a new work flow group.</td>
<td>The work flow group name is already used for another group.</td>
</tr>
<tr>
<td>An administrator cannot record macros from Desktop Work Flow Administrator.</td>
<td>Some virus checkers might prevent the macro recorder from running. Disable all virus checkers on the administrator’s PC.</td>
</tr>
<tr>
<td>The administrator made some changes in Work Flow Setup, and then decided to cancel them. However, they were already saved.</td>
<td>When a new action is created, any changes are automatically saved before returning to the Select Action dialog box.</td>
</tr>
</tbody>
</table>
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 work flow action is failing because the device is not responding quickly enough.

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

Problem  When attempting to make changes in Desktop Administrator, you receive a message that Desktop Administrator is locked by another user even though you have successfully released the lock under the Force-Release CDA Lock node.

Solution  Desktop Administrator only releases the lock on the side to which you are connected in an HA environment. Connect to Desktop Administrator on the other side of the HA pair and release the lock.

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

Solution  Automated updates are disabled for Windows Vista. Other options are:
- Manual “over-the-top” installation
- Push installation
## Enterprise Data Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise data does not display data on outbound calls.</td>
<td>Enterprise data only displays data for inbound calls.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise data does not display data for inbound calls.</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise data displays data after a call has been dismissed.</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Enterprise Service Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can I tell if the Enterprise service is running?</td>
<td>Verify if the Enterprise service is running. See &quot;Logging into Unified CCX Serviceability and Monitoring CAD Services&quot; on page 67 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Incomplete or no enterprise data is displayed when an agent received a call. | 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. |
Installation Problems

Problem: The Agent Desktop services have been upgraded from version 6.4(1) to version 10.5(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 enter 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 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.

| 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 Work Flow 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. Ensure that the phone is configured in Unified CM with a phone locale that matches the language in CAD. |

| 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 | Partial call history or partial data appears in the Caller Data screen for calls right after a failover. |
| Solution | **Symptom.** When an agent receives a call, the Caller Data screen 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 No data appears in the Caller Data screen.

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

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

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

Problem The agent is logged out unexpectedly.

Solution Possible reasons are:
- Another agent with the same ID and 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 An agent has started recording a call successfully (the recording icon is displayed), but the recording icon disappears even though the agent did not stop the recording.

Solution Possible reasons include:
- A supervisor stopped the recording
- The recording service or VoIP Monitor service stopped
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 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 35 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.

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

Solution: Restarting LDAP Monitor service on a regular basis will remove log files.
### Recording and Statistics Service Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When trying to view agent state or call logs, no data is presented.</td>
<td>The agent might not have received a call or logged in for that particular day. The clock on the agent’s or supervisor’s PC might not be in the correct time zone. <strong>NOTE:</strong> All state and call times are based on server time.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>The maximum disk space available for recordings per server is 2.6 GB. Restart the Cisco Desktop Recording and Playback service on the primary node after adding the second node to the cluster.</td>
</tr>
</tbody>
</table>
Recording, Monitoring, and Playback

Problems

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop monitoring fails for agents who use Agent Desktop on their local LAN and also need to connect to another LAN via VPN.</td>
<td>Desktop monitoring fails if a VPN connection is active. CAD assumes that, if the VPN connection is active, then Agent Desktop is using it. As a result, CAD looks for RTP packets from the VPN connection rather than from the IP phone. To resolve this issue, use SPAN-based monitoring for agents who must use VPN in addition to Agent Desktop.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Recording &amp; Playback service is not recording the audio file.</td>
<td>If SPAN-based monitoring/recording is being used, make sure that a SPAN port has been created on the switch for the PC’s network port where the VoIP Monitor service is connected.</td>
</tr>
</tbody>
</table>

| Problem | Cause: This issue occurs when all the required connectivity and configuration seems correct to the software, but the monitoring service is not seeing voice packets on its network connection. The monitoring service refers to either the VoIP Monitor service running on the server or the desktop monitor running on the agent’s desktop. Solution | To troubleshoot this problem, follow the steps in the flowchart shown in Figure 4 and Figure 5. |
|---------|----------|
| 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. | |

Problem
Figure 4. Troubleshooting for inaudible monitored call

- **Problem:** Supervisor selects agent and clicks Monitor. Speaker icon appears next to call, but supervisor cannot hear anything.

  - Volume may be too low. Move volume slider all the way to the right.
  - Verify that PC sound card works.
  - Verify that no other application is using the sound card’s resources.
  - Verify that agent is on a call, and is talking.

  - Is supervisor monitoring a Media Terminated agent using a soft phone?
    - Yes
      - Verify that device is configured correctly in Desktop Administrator:
        - Desktop Monitor check box is clear.
        - If using multiple VoIP Monitor Services, either the device is assigned a VoIP Monitor Service or there is a default service.
    - No
      - Verify that phone is configured correctly in Unified CM:
        - Phone Type is "Cisco 30 SPx"
        - MAC address is for agent’s PC
        - Phone description is "SEP" followed by MAC address of agent’s PC
      - In Unified CM Administration, under System/Enterprise Parameters, in Security Parameters, verify that Device Security Mode is not set to "Encrypted".

  - Is VoIP Monitor Service being used to monitor agent?
    - No
      - Go to “Desktop Monitoring: No Speech” on Page 2
    - Yes
      - Verify switch SPAN port is configured correctly. If monitor server has moved or there are new agent IP phones, you may need to reconfigure SPAN port.
      - Verify registry entries for VoIP Monitor Service.
      - Attempt to monitor same agent with VoIP Monitor Server Test Tool.
      - Check VoIP Monitor Service log files for errors.
      - Open a TAC case.
Figure 5. Troubleshooting for inaudible monitored call (cont’d)

Problem: (continued)
Desktop Monitoring: No Speech

Verify that the device is configured correctly in the Cisco Desktop Administrator application; the Desktop Monitor box is checked.

Is the agent being monitored a Media Terminated agent using a soft phone?

Yes

Verify that the phone extension used by the agent to log on to CAD is the same extension as the configured soft phone.

No

Verify that the IP phone is a Cisco 7910, 7940, or 7960 IP phone.

Verify that the PC is connected to the phone in the 10/100 SW port.

Verify that the phone extension used by the agent to log on to CAD is the same extension of the attached IP phone.

On the Phone Configuration page for the phone(s) you are attempting to monitor, verify the following settings:
- PC Port is set to “Enabled”
- PC Voice VLAN Access is set to “Enabled”

Verify that the NIC card in the agent’s PC supports Desktop Monitoring.

Verify the CAD Desktop’s registry settings.

Attempt to monitor the same agent using the Desktop Monitor and VoIP Monitor Server Test Tools.

Check the CAD application logs for errors.

Open a TAC case.

End
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.

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

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

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

- **PC Port—Enabled.** If the PC Port is not enabled, the agent PC that is connected to the port will not have network access. No voice streams will be seen by the desktop monitor module.

- **PC Voice VLAN Access—Enabled.** If the PC Voice VLAN Access is not enabled, no voice streams will be seen by the desktop if the desktop is not a member of the same VLAN as the phone.

- **Span to PC Port—Enabled.** If the Span to PC Port is not enabled, the voice streams seen by the phone will not be seen by the desktop monitor module.

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

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

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

Another possible cause is that you attempted to monitor an agent whose phone call is on a non-ACD line, but monitoring of non-ACD calls has not been enabled. Non-ACD call monitoring and recording settings are configured in Desktop Administrator (Services Configuration > Multiline, Monitoring & Recording > Display Settings).
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.

Problem: Monitoring and Recording stop working after installing a new NIC.

Solution: This problem occurs because the network adapter used by the VoIP Monitoring software for sniffing is invalid or becomes invalid. The voice sniffing software running on the VoIP Monitor service box and the agent desktop (if desktop monitoring is being used) uses a specific network adapter (set at installation) to capture voice packets from the network. After installing a new or another NIC, this adapter might become invalid. There are also cases where the incorrect network adapter is chosen during the installation of the software. In either of these cases, monitoring and recording will not work correctly. You will need to run the CAD Configuration Setup utility to update the sniffing adapter name stored in the registry to fix the problem.

Problem: The first few seconds of silent monitoring sound choppy or distorted.

Solution: This might be caused by duplicate packets, which CAD cannot process. To resolve this issue, run a network monitoring tool (for example, WireShark) to ensure no duplicate packets are being generated by any device on the network.
**Problem**
The sound quality is poor and sounds choppy like a motorboat.

**Solution**
The motor-boating effect occurs if the jitter buffer is too small or the number of sound buffers is too low.

**Jitter Buffers:** Jitter buffers are used to buffer packets in a pool that is read by the monitoring and/or recording application. Although the packets coming from the network might arrive in bursts, pooling the packets smooths out the bursts for the monitor application. If the jitter buffer is too small, the monitor application empties the buffer more quickly than the buffer is filled. The monitor application must then wait for the buffer to be partially refilled before the monitor application can start reading packets again. The stops and starts cause the motor-boating effect.

The default value for the recording jitter buffer is 100 (packets). If you increase this value, increment in steps of 100 packets. The default value for the monitoring jitter buffer is 400 (packets). If you increase this value, increment in steps of 100 packets.

The applications that receive voice packets from the packet sniffing driver have jitter buffer settings. These applications include Supervisor Desktop for monitoring and the Recording and Statistics service for recording. Depending on the version of CAD you are using, these values are stored in one of three places: LDAP, the Windows registry of the machine on which Supervisor Desktop is running, or the Windows registry of the server on which the Recording and Statistics service is running.

**Sound Buffers:** The number of sound buffers indicates the amount of sound card buffer resources that are being used. If recordings sound normal, but the motor-boating effect occurs during monitoring, increase the number of sound buffers. To configure the number of sound buffers, you must edit the registry on the supervisor's PC.

---

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

**Solution**
The slow speech effect is due to duplicate voice packets being sent to the monitoring supervisor or the Recording and Statistics Service. This effect can only occur if the extension being monitored or recorded is using a VoIP Monitor service to capture the packets. You will not see this if using Desktop Monitor.
The root cause is that SPAN is not configured correctly on the switch that the agent phones are connected to. If SPAN is configured to monitor phone ports or a VLAN containing agent phones, and it is configured to copy both incoming and outgoing packets, you will see duplicate packets when you monitor a call between two agents on the same switch. You will see packet A as it leaves Agent-1's phone, and the same voice packet as it arrives at Agent-2's phone. To fix this issue, you need to reconfigure SPAN on the switch.

**Problem**
Only one party on a call is audible during monitoring or recording.

**Solution**
If you are only hearing one side of a conversation, first check the following:

- Two or more parties are actually on an active call
- All parties are actually speaking through the phone to each other
- The party that you cannot hear via monitoring/recording can be heard by the other parties on the call

If the party that you are able to monitor/record cannot hear the other party, the voice packets won't be seen by the monitor service either. Here are some common reasons that party A would not hear another party B:

- B is whispering.
- B is using a speaker phone and not speaking loudly enough to be heard or is too far from the phone for the speech to be picked up by the phone's microphone.
- B is using a headset or microphone and the microphone is turned off or is broken.

If you can eliminate these as causes, then the cause of this effect is due to a faulty configuration of SPAN on the switch. Since this is dealing with SPAN configuration, this will not apply if using Desktop Monitor for monitoring or recording.

Basically, the SPAN is configured in such a way that it is not capturing the voice packets from one of the parties on the call. To fix this issue, you need to reconfigure SPAN on the switch.
**Problem**  
A recording or monitoring session audio is faint and hard to hear.

**Solution**  
If only one of the parties being monitored or recorded has a lower volume, you can check these reasons (where Agent B is the agent that has a lower volume):

- B is whispering.
- B is using a speaker phone and not speaking loudly enough to be heard or is too far from the phone for the speech to be picked up by the phone's microphone.
- B is using a headset or microphone and the microphone is turned off or is broken.

If all parties are equally soft, then complete the following checks:

- If listening to a recording through Supervisor Desktop, make sure the volume slider is all the way to the right.
- If using headphones, check the volume setting for the headphones.
- If using speakers, check the volume setting for the speakers.
- Try both headphones and speakers to see if there is any difference.
- Try to monitor from another supervisor's desktop, using their speakers/headphones.
- Manually open a WAV file that is not a recording made from CAD and listen to it through the speakers or headphones.

There is nothing in the CAD software that alters volume of monitored or recorded calls except for the volume slider in the Supervisor Desktop application that allows the supervisor to listen to recorded calls. The advice is to make sure your sound hardware is working correctly on the machine being used by the supervisor.

---

**Problem**  
There are gaps in the audio of a recording or monitoring session.

**Solution**  
Gaps in speech, no speech, or speech that is excessively delayed (when monitoring), can be caused either by network congestion or by inadequate CPU time allocated to the application that is involved in monitoring/recording.
If the network is very congested, the packets will not arrive at the packet sniffing driver fast enough to produce good quality results. Also, packets being sent over the network from the VoIP Monitor service to Supervisor Desktop and the Recording and Statistics service will be delayed, affecting speech quality. Evaluate the load on your network and fix this problem to improve the monitoring quality.

If the network is not congested, gaps in audio can be caused by an overburdened CPU on one or more of the machines running the monitoring/recording software.

Table 23. Locating the overburdened CPU

<table>
<thead>
<tr>
<th>How agent is monitored/recorded</th>
<th>Computers to check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring with VoIP Monitor service</td>
<td>• VoIP Monitor service host</td>
</tr>
<tr>
<td></td>
<td>• Supervisor’s desktop</td>
</tr>
<tr>
<td>Monitoring with Desktop Monitoring</td>
<td>• Agent’s desktop</td>
</tr>
<tr>
<td></td>
<td>• Supervisor’s desktop</td>
</tr>
<tr>
<td>Recording with VoIP Monitor service</td>
<td>• VoIP Monitor service host</td>
</tr>
<tr>
<td></td>
<td>• Recording &amp; Statistics service host</td>
</tr>
<tr>
<td>Recording with Desktop Monitoring</td>
<td>• Agent’s desktop</td>
</tr>
<tr>
<td></td>
<td>• Recording &amp; Statistics service host</td>
</tr>
</tbody>
</table>

If you find one of these machines where its CPU usage is very high (over 75%), you will need to reduce the CPU usage on that machine to improve the quality of monitoring and recording.

The first thing to check is the debugging level for the Cisco applications. If these debugging levels are set very high, the software spends most of its time writing out to the debug file. This will, in some cases, drastically increase the CPU time for the application and, in turn, the computer itself. Turn off all the debugging for the service or application that you suspect, then try to monitor or record to see if that fixes the problem.

The next thing to do is to find out what other applications are running on the box in question, determine which application(s) and using the most CPU time, and shutting down or removing these applications from the box to improve performance.

For information on setting debugging levels for CAD applications, see "Debugging Thresholds" on page 71.
**Problem**
Extraneous noise is heard in the audio of a recording or monitoring session.

**Solution**
Pops, clicks, and other extraneous noises are most likely due to the parties on the call being in noisy environments. If the parties on the call are not hearing these noises, but the noises are heard by the monitoring supervisor or can be heard in the recorded WAV file, it might indicate a problem with the software.

---

**Problem**
Unexpected noise is heard instead of voices when monitoring or recording including beeping sounds (no speech) or very distorted speech or noise.

If the call is using the G.711 protocol, you will either hear silence or an irregular beeping sound. There can be other types of effects that we not encountered yet. If the call is using the G.729 protocol, the speech sounds very strange. It has been described as someone speaking in a foreign tongue while under water.

**Solution**
This problem occurs when voice encryption is configured on the Unified CM. Verify that Unified CM is not configured to send voice streams as encrypted data.

Unified CM supports voice stream encryption. The encrypted packets cannot be unencrypted by the monitor service software. The software processes the encrypted voice stream and outputs what it thinks is speech. In reality, the result is either a periodic beeping (for G.711) or distorted speech (for G.729). You might get other types of results, but the fix is to turn off encryption in Unified CM. Refer to the appropriate Unified CM documentation for instructions on how to do this.

---

**Problem**
When the supervisor uses USB speakers for monitoring and playback in Supervisor Desktop, there is no sound.

**Solution**
You must plug in the USB speakers before opening Supervisor Desktop.

To resolve this issue, close Supervisor Desktop, then plug in the USB speakers. Reopen Supervisor Desktop and restart monitoring or playback.
Problem When an agent logs in to Agent Desktop while already on a call, recording and monitoring does not work on that call.

Solution This is expected behavior. There is no workaround. Recording and monitoring will function properly for the agent’s next call.

Problem The supervisor starts recording or monitoring an agent’s conversation, but after a short time the recording or monitored speech stops by itself. The recording file is incomplete.

Solution This occurs when the recording or monitoring process is stopped prematurely by some system or application crashing.

1. 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.

2. Verify that the Recording and Statistics Service is configured with an appropriate percentage of disk space. When the Recording and Statistics Service is installed, it creates a directory for storing recording files.

3. Verify that the drive has space available for recording files.

4. Verify that all of the required applications are running.

The Recording and Statistics Service is configured to use a percentage of the available disk space and will stop accepting recording requests if it uses all of the disk space it is configured to use. To fix this problem, you must either tell the Recording and Statistics Service that it can use more of the disk to store recordings, or remove some of the recordings to make room for new recording files.

If the physical drive is out of space, the Recording and Statistics Service cannot write any recordings. If this is the case, you will see many other applications complaining of this as well. You will need to make space on the drive to continue working.
Problem: When an agent using Cisco IP Communicator 8.0 and later is recorded and monitored from Supervisor Desktop, recording and monitoring fail when the Cisco Unified Communications Manager is version 9.1.1a.

Solution: In Cisco Unified CM Administration, select Device > Phone. Search for the agent’s extension and select the MAC address for the agent’s IP Communicator. In the Phone Configuration window, set the Advertise G.722 Codec field to Disabled. Click Save to save your changes.

Problem: An agent receives a call immediately after logging in. A workflow has been configured to initiate recording when a call is received. However, the call is not recorded. The supervisor sees no recording icon on the call, and no call appears in the Supervisor Record Viewer.

Solution: This situation can arise when SPAN monitoring and recording is used. There must be about ten seconds between the time the agent logs in and when a call can be recorded or monitored.
### Supervisor Desktop Problems

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

> “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.

<table>
<thead>
<tr>
<th><strong>Problem</strong></th>
<th><strong>Agent Desktop Problems</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symptom.</strong></td>
<td>The following symptoms related to the display of agents in the Supervisor Desktop can occur:</td>
</tr>
<tr>
<td>■ Agents disappear from the Agent tree</td>
<td></td>
</tr>
<tr>
<td>■ One or more agents are not displayed in the Agent tree</td>
<td></td>
</tr>
<tr>
<td><strong>Cause.</strong></td>
<td>Incorrect configuration or IP connectivity issues between the agent PC and the Unified CCX system or the Unified CCX system and the supervisor PC.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Check the following settings:</td>
</tr>
<tr>
<td>■ Verify that the agent belongs to the team that the supervisor is monitoring. Refer to “Configuring Agents” in the Cisco Desktop Administrator User Guide.</td>
<td></td>
</tr>
<tr>
<td>■ Verify that the CAD client desktop applications are at the same version as the CAD services.</td>
<td></td>
</tr>
<tr>
<td>■ 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.</td>
<td></td>
</tr>
<tr>
<td>■ Determine whether any ports in the 59000–59030 range are blocked by a firewall, and if so, allow the ports to be connected.</td>
<td></td>
</tr>
<tr>
<td>■ Determine if the client PC has the Internet Connection firewall enabled, and if so, disable it.</td>
<td></td>
</tr>
</tbody>
</table>
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 unexpectedly changed to Not Ready.

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 was able to start Supervisor Desktop, but was not able to load a team or display any agent information.

**Solution**
Windows 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.

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

Problem
Recording and monitoring stops on an existing call after a failover.

Cause: This is due to the CTI signaling required for recording and monitoring to work properly. During a failover, the CTI server does not send RTP events. This information is needed for recording and monitoring to function properly, thus the call recording is stopped when the CTI connection goes down.

Solution
This is a known limitation in CAD. Recording and monitoring resume as normal when the existing call is dropped and a new call is started.

For more 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 supervisor does not 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 are not 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 when starting 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 and nothing happened.

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

The most common reason for this failure is that the VoIP Monitor service or the Recording and Statistics Service is down.

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

---

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

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

---

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

**Solution**
The supervisor is also an agent logged into the ACD. If the supervisor is inactive (in the Not Ready state) long enough he or she is logged out of the ACD.

The 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 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 SuperID field stored in Supervisor.cfg (located in the config folder).

---

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

**Solution** A blind conference is defined as adding an alerting party to a conference. All parties on a blind conference call might not show up in either Supervisor Desktop 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: 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: 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 While a recording is in progress, the reported duration of the recording is incorrect.

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

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

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

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

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

Solution This situation can arise when two events occur within the same second. This is expected behavior. No workaround is available.

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 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, click the Refresh button on the toolbar to refresh the team data.
## Sync Service Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can I tell if the Sync service is running properly?</td>
<td>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.</td>
</tr>
<tr>
<td>The message, &quot;At least one or more errors occurred during synchronization&quot; appeared when the administrator performed synchronization in Desktop Administrator.</td>
<td>Check the Sync service log file. If the logged error points to a problem with the CTI 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 preferences setting in SiteSetup has the correct value. See &quot;Site Setup&quot; on page 25 for more information.</td>
</tr>
</tbody>
</table>
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 33 for more information.

Note that for IP Phone Agent seats, the IP address is the IP address of the active BIPPA service. For web-based Desktop Administrator, the IP address is the IP address of the CAD server.
VoIP Monitor Problems

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 an IP Phone agent)
- The instance of 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.
<table>
<thead>
<tr>
<th><strong>Problem</strong></th>
<th>The VoIP Monitor service server might generate a core file and a Real-Time Monitoring Tool (RTMT) alert on system restarts, but no functionality loss is seen.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solution</strong></td>
<td>There is no workaround for this issue. The issue is benign and should result in no loss of functionality so it can be ignored.</td>
</tr>
</tbody>
</table>

## Index

<table>
<thead>
<tr>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>about RAW format 49</td>
</tr>
<tr>
<td>about raw2wav utility 49</td>
</tr>
<tr>
<td>Agent Desktop</td>
</tr>
<tr>
<td>autorecovery 39</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior under Microsoft Windows Power Options 57</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAD applications</td>
</tr>
<tr>
<td>user applications and services 9</td>
</tr>
<tr>
<td>CAD documentation 7</td>
</tr>
<tr>
<td>CAD license usage 33</td>
</tr>
<tr>
<td>CAD Services</td>
</tr>
<tr>
<td>collecting log files 75</td>
</tr>
<tr>
<td>enabling debugging thresholds 71</td>
</tr>
<tr>
<td>CAD services</td>
</tr>
<tr>
<td>autorecovery 12</td>
</tr>
<tr>
<td>chat problems 119</td>
</tr>
<tr>
<td>chat service problems 120</td>
</tr>
<tr>
<td>CLI</td>
</tr>
<tr>
<td>command syntax 15</td>
</tr>
<tr>
<td>CAD services' pathkeys 23</td>
</tr>
<tr>
<td>configuration files 16, 17</td>
</tr>
<tr>
<td>debugging log threshold, number, and size preferences 18</td>
</tr>
<tr>
<td>E-mail 20</td>
</tr>
<tr>
<td>LDAP utilities 21</td>
</tr>
<tr>
<td>others 16, 17</td>
</tr>
<tr>
<td>preferences 16, 17</td>
</tr>
<tr>
<td>recordings 20</td>
</tr>
<tr>
<td>restart, start, and stop CAD services 19</td>
</tr>
<tr>
<td>executing commands 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>collecting log files 75</td>
</tr>
<tr>
<td>converting recording file format 47</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Administrator problems 121</td>
</tr>
<tr>
<td>Directory Services database</td>
</tr>
<tr>
<td>becomes corrupted 35</td>
</tr>
<tr>
<td>recovering 35</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabling debugging thresholds 71</td>
</tr>
<tr>
<td>Enterprise Data problems 131</td>
</tr>
<tr>
<td>Enterprise Service problems 132</td>
</tr>
<tr>
<td>executables 32</td>
</tr>
<tr>
<td>executing CLI command 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>guidelines</td>
</tr>
<tr>
<td>capacity and performance 11, 39</td>
</tr>
<tr>
<td>sizing deployments 11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferences</td>
</tr>
<tr>
<td>BIPPA 26</td>
</tr>
<tr>
<td>enterprise service 27</td>
</tr>
<tr>
<td>recording and playback client 28</td>
</tr>
<tr>
<td>recording and playback service 29</td>
</tr>
<tr>
<td>SiteSetup 25</td>
</tr>
<tr>
<td>voice-over IP monitor client 30</td>
</tr>
</tbody>
</table>
voice-over IP monitor record client 30
voice-over IP monitor service 31

problems
chat 119
chat service 120
Desktop Administrator 121
Enterprise Data 131
Enterprise service 132
IPCC license administration 162
recording and statistic service 139
silent monitoring and recording 140
Sync service 161
work flow 128

R
recording and playback
client preferences 28
client registry entries 46
service preferences 29
recording and statistics service problems 139
registry entries 23
enterprise service 27, 45
recording and playback client 46
site setup 43
restarting services 32
running conversion automatically 48

S
service names 32
setting uccxrecording user password 48
silent monitoring and recording problems 140
Supervisor Desktop
autorecovery 39
Sync service problems 161
Syntax
CLI command 15

T
technical package information
Windows 40
troubleshooting
Unified CCX Administration application 32

U
Unified CCX license administration problems 162
Unified CCX Serviceability
changing CAD services status 69
enabling debugging thresholds 71