Configuration Guide for Cisco Unified Communications Environments

CA Unified Communications Monitor
Version 3.7
This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At [http://ca.com/support](http://ca.com/support), you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at [http://ca.com/docs](http://ca.com/docs).
## Contents

### Chapter 1: Introduction

Differences Between the SPAN and CDR Methods ................................................................. 7
Supported Systems and Devices ......................................................................................... 10
Architecture and Scalability ............................................................................................ 12

### Chapter 2: Configuration Tasks

Connecting the Collector to a SPAN Port ....................................................................................... 15
Configuring the Management Console as an FTP Recipient ............................................. 17
Enabling the Call Stats Setting ............................................................................................. 18
Enable the Collection of Voice Quality Metrics .................................................................... 19
Enabling Web Access and RTCP for IP Phones ..................................................................... 19

### Appendix A: Troubleshooting

Monitoring Authenticated SIP Traffic ..................................................................................... 21
Add or Remove SIP Ports for Monitoring ............................................................................. 21

### Index

23
Chapter 1: Introduction

CA Unified Communications Monitor (UC Monitor) supports environments that use Cisco Unified Communications Manager (CUCM) for call processing. You have two options for collecting call data from CUCM:

- **SPAN method**: Connect the UC Monitor collector server to a SPAN (Switched Port Analyzer) port on the switches that carry the signaling traffic to the CUCM.
- **CDR method**: Enable CUCM to use FTP to push call detail records (CDRs) and call management records (CMRs) to the UC Monitor management console. No SPAN is required.

This document helps a Cisco network engineer configure the SPAN method or the CDR method. In addition, this document provides instruction for configuration that is independent of the collection method, such as adding SIP ports.

**Note**: UC Monitor supports environments in which both the SPAN and CDR methods are configured. However, such a configuration is not recommended. With both methods configured, you risk duplication of the data in UC Monitor reports.

### Differences Between the SPAN and CDR Methods

#### Data Collection

**SPAN method**

The collector monitors call traffic through a SPAN port on a switch where CUCM call servers are connected. The collector regularly transmits the call data to the management console for display in UC Monitor reports.

**CDR method**

CUCM uses FTP to push CDRs (and CMRs) to the management console, where they are parsed for the data that appears in UC Monitor reports.

#### Configuration Tasks

**SPAN method**

Perform the following tasks to configure your environment:

- Configure SPAN ports to mirror signaling traffic to the collector.
- Enable the Call Stats setting in a voice-quality-enabled SIP profile.
- Enable the collection of voice quality metrics.
- Enable web access and RTCP on IP phones.
Differences Between the SPAN and CDR Methods

CDR method

Perform the following tasks to configure your environment:
- Configure the management console as an FTP recipient.
- Enable the Call Stats setting in a voice-quality-enabled SIP profile.
- Enable the collection of voice quality metrics.

Metrics and Features

<table>
<thead>
<tr>
<th>Metric</th>
<th>SPAN Method</th>
<th>CDR Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACOM</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Call Setup Failures</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Call Volume</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Concealment Ratio</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conversational MOS</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delay to Dial Tone</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ERL</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Jitter</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jitter Buffer Loss</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Latency</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Listening MOS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MOS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet Loss (Max)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Packets Lost</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Packets Received</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Post-dial Delay</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Severely Concealed Seconds</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Signal In/Out</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>SPAN Method</th>
<th>CDR Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Call Quality report</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic traceroute investigations</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Baseline traceroutes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Call quality incidents</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Call server group incidents
- **SPAN Method**: Yes
- **CDR Method**: No

### Call server incidents
- **SPAN Method**: Yes
- **CDR Method**: No

### Call setup incidents
- **SPAN Method**: Yes
- **CDR Method**: No

### Call Volume report
- **SPAN Method**: Yes
- **CDR Method**: Yes

### Call Watch
- **SPAN Method**: Yes
- **CDR Method**: No

### Collector incidents
- **SPAN Method**: Yes
- **CDR Method**: No

### Interface Utilization report
- **SPAN Method**: Yes
- **CDR Method**: No

### Top Interfaces report
- **SPAN Method**: Yes
- **CDR Method**: No

### Top Trunk Groups report
- **SPAN Method**: Yes
- **CDR Method**: No

### Top Volume Locations/Phones reports
- **SPAN Method**: Yes
- **CDR Method**: Yes

### Trunk Group Utilization report
- **SPAN Method**: Yes
- **CDR Method**: No

### Phone or Endpoint Information

<table>
<thead>
<tr>
<th>Phone or Endpoint Information</th>
<th>SPAN Method</th>
<th>CDR Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Server</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Codec</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Type</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IP Address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Last Activity</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Location</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Model/Type</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Previous Call Server</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Previous Status</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Status</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Status Time</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

*For CUCM 9.0, this metric can be empty or incorrect.*
### Supported Systems and Devices

UC Monitor supports the following Cisco unified communications systems and devices. CA Technologies tested UC Monitor with gateways of the indicated types using the major call setup protocols: SIP, H.323, and MGCP. UC Monitor supports call volumes of up to ten million calls per month.

**Cisco Unified Communications Manager**

**SPAN method:**
- Versions 7.1 through 9.1 are supported. Later versions may work but have not been tested.
- Support for versions 8.0 and later is available only with UC Monitor versions 3.1 and later.

**CDR method:**
- Versions 8.6 through 9.1 are supported. Later versions may work but have not been tested.
- Version 9.0 incorrectly reports the RTP port for calls, and it does not always identify the media IP address. These issues can cause call correlation problems and incorrect device discovery. We recommend that you not use version 9.0.

**Cisco Unified Border Element (CUBE), Enterprise Edition**
- The device on which CUBE is enabled is discovered as a Session Border Controller and appears in the management console on the Other Devices page.
- SNMP must be enabled on the device.
- End-of-call statistics in SIP BYE messages must be enabled on the device.
- Call Watch is not supported for CUBE.
- The SP Edition of CUBE is not supported.

**Cisco voice gateways, with T1/E1-PRI connections**
- Including the H.323 and MGCP protocols and SIP trunks to voice gateways.

**Analog-type gateways**
- Voice gateways that make an FXO connection are monitored for call performance data.
- Call Watch is supported for calls through an FXO connection only if the H.323 protocol is used.

<table>
<thead>
<tr>
<th>Switch Address</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Switch Port</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

10 CA Unified Communications Monitor
Cisco VG-224 gateways
- These devices provide only call setup metrics.
- Call quality reporting and Call Watch are not supported for these devices.

Cisco ATA 186 analog telephone adapters
- These devices provide only call setup metrics.
- Call quality reporting and Call Watch are not supported for these devices.

Catalyst 6000 WS-X6608-T1/E1 Blade for Voice
- Call Watch is not supported for this device.
- This device returns limited call quality metrics for UC Monitor performance reports.

Cisco Unified IP phones
- 6900 series
- 7920, for call performance metrics only. Call Watch is not supported for this phone.
- 792x, 794x, and 796x series
- 8941, 8945. The switch address, switch name, and switch port number for these phones may not be available on the Phone Details report.
- 8941, 8945, 8961, 9951, 9971. Video metrics can be available from these phones in a medianet environment.

Note: Install the latest firmware for these phones.

Cisco Unified IP phones, running in advanced SIP mode
7906, 7911, 7941, 7961, 7970, 7971

Note: Install the latest firmware for these phones.

Cisco IP Communicator softphone
- Version 2 provides few call quality metrics.
- Versions 7 and later provide packet loss, jitter, and call setup metrics.

Cisco Unified Personal Communicator, version 7.0
- Call volume data is obtained for calls to and from this client, such as when the calls were made and the locations of the endpoints.
- Call setup failures can be reported from this client.

Medianet-enabled devices
UC Monitor supports Cisco devices that send medianet performance information. For more information, consult the Cisco documentation for Cisco Networking Capabilities for Medianet.
Architecture and Scalability

Phone localization settings

UC Monitor supports the following settings. Other settings may work, but have not been tested.

- English (US and UK)
- German, Danish, Dutch
- Italian, French, Spanish
- Japanese

Architecture and Scalability

Architecture

For Cisco SPAN deployments, UC Monitor requires a management console and at least one collector. In general, one UC Monitor collector is required for every switch that handles call setup flows from the CUCM call server.

A standalone UC Monitor system is sufficient for Cisco CDR deployments, small SPAN deployments, or initial rollouts with only one CUCM cluster.

A distributed UC Monitor system is recommended for larger SPAN deployments.

The following diagram illustrates UC Monitor in a CUCM deployment that includes the SPAN and CDR methods* of data collection:

*Although enabling both collection methods simultaneously is not recommended, we include them here to illustrate their placement in the deployment.
Scalability

Cisco recommends that you deploy CUCM so as to ensure failover capability and processing redundancy:

- Do not allow the members of a call server cluster to share a VLAN or switch.
- Use different access switches. Connect them to the same distribution or core switch, or to different distribution or core switches.
- Place call servers in different buildings within the same LAN or WAN.
Chapter 2: Configuration Tasks

This section contains the following topics:

- Connecting the Collector to a SPAN Port (see page 15)
- Configuring the Management Console as an FTP Recipient (see page 17)
- Enabling the Call Stats Setting (see page 18)
- Enable the Collection of Voice Quality Metrics (see page 19)
- Enabling Web Access and RTCP for IP Phones (see page 19)

Connecting the Collector to a SPAN Port

In a Cisco environment, you can connect the collector to a SPAN port on the switches that carry VoIP traffic on your network. The collector must be able to inspect call setup-related packets that pass between the call servers and endpoints in your system. Connect the collector at an appropriate network location, using a properly configured SPAN switch port.

**If possible, SPAN only VoIP traffic and call server traffic**

- Add VLANs dedicated to voice traffic to the list of spanned ports.
- Configure an ACL to discard non-VoIP traffic before it is sent out of the SPAN port. An ACL has significant overhead on some switches, so use your best judgment in selecting a method to separate traffic.
- Use a VACL to filter for all traffic going to and from the IP addresses of the Cisco Unified Communication Managers.

**Install UC Monitor collectors near monitored call servers or voice gateways**

Calculations for server response times assume that the collector and the monitored server receive an inbound frame at approximately the same time. Similarly, traceroute investigations provide the most accurate path results when the collector is located close to the call server. The collector and call server share a router. This configuration helps ensure that traceroute results reflect the path taken by packets sent to and from the call server.

**Consider NIC usage**

A distributed collector and a standalone server use one NIC for the collector service and one NIC for management.

When a network tap is used, one NIC is used for management and two NICs are used for the collector service. A tap splits the transmitting and receiving flows of a full-duplex link across two physical ports. The collector receives the separated traffic from both NICs.
The collector works better with SPAN ports than with network taps

Plug the monitor NIC on the collector into the SPAN port. Configure a network tap only when the SPAN port is in use. You can configure remote spanning of switch traffic to another switch and connect the collector to the SPAN port on the remote switch. Having a dedicated collector for each switch is the recommended configuration.

Forward the following VoIP protocols to the collector:

- **SIP.** Session Initiation Protocol performs call setup and teardown, manages sessions, and determines user location, availability, and capabilities. Forward TCP and UDP traffic on port 5060 to the collector to get SIP flows. UC Monitor supports authenticated SIP flows, but it cannot interpret or report on calls from encrypted SIP flows.

  Note: Collectors can monitor only one port per protocol. To monitor multiple SIP ports on a single SPAN, contact [CA Technical Support](#).

- **H.323.** This family of protocols supports real-time transfer of data over packet networks by enabling communications between H.323-enabled devices, such as VoIP gateways. Forward the following traffic to the collector:
  - for H.225, TCP traffic on port 1720
  - for H.245, TCP traffic on ports above 11000 (dynamically selected)

- **SCCP.** The Skinny Call Control Protocol is a proprietary Cisco protocol used for messaging between skinny clients and a Cisco Unified Communications Manager. Forward TCP traffic on port 2000 to the collector to get SCCP flows. If SCCP signaling flows are encrypted, UC Monitor cannot interpret or report on calls.

- **MGCP.** The Media Gateway Control Protocol enables call-control devices, such as media gateway controllers, to control VoIP calls. Performs similar functions to H.323. Forward UDP traffic on port 2427 to the collector to get MGCP flows.

- **Q.931.** Call setup traffic is backhauled over a TCP connection to Cisco Unified Communications Manager to control the ISDN PRI for the voice gateway. The collector must see the Q.931 Setup and Alerting messages that are sent between the Unified Communications Manager and the gateway. Forward TCP traffic on port 2428 to the collector to get the PRI backhaul flows.

Verify that the SPAN port is not congested or misconfigured

Review the dropped packets statistics on the SPAN port where you want to connect the collector.
If you are running CA Application Delivery Analysis on the network, connect CA Application Delivery Analysis to a SPAN port on a different switch.

In some situations, however, both systems must monitor the same switch. Therefore, you can use a network tap to separate the traffic intended for CA Application Delivery Analysis from the traffic intended for UC Monitor. The collector can be connected to a standard tap (copper or fiber) or an aggregating tap rather than a SPAN port. CA Application Delivery Analysis supports a dual-NIC collector, which a standard tap requires. UC Monitor does not support this type of collector. Purchase a tap that sends the request and the response traffic over the same connection on the tap.

Consider traffic from Publishers and Subscribers

Cisco Unified Communications Manager servers act in multiple roles to provide failover and load balancing capabilities. Therefore, configure the SPAN port so that VoIP-related traffic is associated with both Publishers and Subscribers.

Voice gateways can register with either the Publisher or Subscriber and are often configured to perform failover duties. Signaling between a voice gateway and a call server must reach the collector so that all call traffic on the network is monitored.

In a large Cisco deployment, each cluster typically includes as many as four servers: one Publisher, two Subscribers to handle call processing, and one TFTP server. The Publisher and TFTP server act as backups for failover situations. In such a configuration, SPAN the traffic that goes to two of the servers in the cluster and send it to one collector. Then, send the traffic for the other two servers to a second collector. If the phones are load-balanced among the servers in the cluster, each collector sees data from only half the phones, which is a manageable load.

For more information, see the Best Practices for Data Acquisition guide in the CA Unified Communications Monitor bookshelf on the About page of the management console.

Configuring the Management Console as an FTP Recipient

For the CDR method, use the Cisco Unified Serviceability web interface to configure the management console server as the FTP recipient.

Follow these steps:
1. Log in to the Cisco Unified Serviceability web interface.
2. Click Tools, CDR Management.
3. In the Billing Application Server Parameters section, click 'Add new'.
Enabling the Call Stats Setting

Phones that use the Session Initiation Protocol (SIP) return quality metrics only when you enable the Call Stats setting in the Cisco Unified CM Administration web interface. You can change the standard SIP profile or you can create a new voice-quality-enabled profile.

After you enable the Call Stats setting on the SIP Profile Configuration window (Device, Device Settings, SIP Profile), apply the new or edited profile to your IP phones.

For information about editing or creating SIP profiles, consult the documentation for your version of CUCM.

4. Complete the parameters as appropriate for your environment. UC Monitor supports the following default parameter values:
   - **Host Name/IP Address.** The IP address of the management console server.
   - **User Name.** anonymous
   - **Password.** The email address associated with the anonymous user name.
   - **Protocol.** FTP
   - **Directory Path.** /Cisco/. Do not forget to include the final forward slash.

5. Click Add.

**Notes:**
- The UC Monitor installation process creates an FTP site on the management console that allows anonymous users to log in. For secure FTP, you can configure any server as the secure FTP recipient. That server must push the CDRs and CMRs to the following location on the management console:
  
  install directory\VoIPMonitor\FTPSite\Cisco

- UC Monitor support for the CDR method requires the CA UCM FTP site to be enabled. The installation creates the \VoipMonitor\FTPSite\Cisco folder regardless of the enabled or disabled status of FTP, and does not overwrite the existing FTP configuration. If you disabled the FTP site for a previous release of UC Monitor, then re-enable the site to facilitate support for the CDR method. Similarly, re-enable the site if you disabled it because you did not need Cisco CDR support, but you do want FTP to support another vendor.

- As a best practice, assign unique Cluster IDs when you have multiple clusters. Unique IDs guard against duplicate FTP filenames; CDRs use the Cluster ID in the FTP filename. Duplicate filenames can result in loss of data at the management console when one CDR is overwritten by another CDR with the same filename. You can assign Cluster IDs in the Enterprise Parameters Configuration section of the Cisco Unified CM Administration web interface.
Enable the Collection of Voice Quality Metrics

From the Cisco Unified CM Administration web interface, enable the collection of call detail records (CDRs) and call management records (CMRs). UC Monitor captures the CMR data from the SPAN of traffic going to and coming from the CUCM. Without the use of SPAN, the CUCM uses FTP to push CDRs (and CMRs) to the UC Monitor management console.

Follow these steps:

1. From the web interface, perform the following steps for each call server in each monitored cluster:
   a. Set the 'CDR Enabled Flag' service parameter to True.
   b. Set the 'Call Diagnostics Enabled' service parameter to True.

By default, both settings are disabled.

You do not need to restart the call server for the change to take effect.

Notes:

- Enable CDR and CMR collection on the call servers in each monitored cluster. Cisco has the following warning:
  "Generating CMRs without corresponding CDRs can cause uncontrolled disk space consumption. Cisco Systems recommends that you always enable CDRs when CMRs are enabled."

- For information about using the web interface, consult the documentation for your version of CUCM.

- CUCM may enable archiving of CDRs and CMRs. UC Monitor does not require the archiving of these records.

Enabling Web Access and RTCP for IP Phones

An IP phone’s internal web server lets other programs access the phone’s web page, which provides configuration and status information that the UC Monitor collector uses. The **Web Access** parameter on the phone indicates whether the internal web server is enabled.

You can disable the **Web Access** parameter for security reasons. Core monitoring functionality for UC Monitor does not require you to enable this setting. However, we encourage you to enable the setting to use the UC Monitor Call Watch feature and to view data about discovered phones.

Also, enable the **RTCP** parameter to allow UC Monitor to obtain latency values from discovered phones.
You can update 'Phone settings' from the Cisco Unified CM Administration web interface. For more information, consult the documentation for your version of Cisco Unified Communications Manager.
Appendix A: Troubleshooting

This section contains the following topics:

Monitoring Authenticated SIP Traffic (see page 21)
Add or Remove SIP Ports for Monitoring (see page 21)

Monitoring Authenticated SIP Traffic

UC Monitor automatically reports on call quality metrics from authenticated SIP traffic by parsing packets that contain Transport Layer Security (TLS) authenticated messages.

Cisco Unified Communications Manager uses port 5061 for authenticated SIP traffic.

You can use a different SIP port. For more information, see Add or Remove SIP Ports for Monitoring (see page 21).

Add or Remove SIP Ports for Monitoring

You can add or remove SIP ports for monitoring. In your environment, firewalls may prohibit monitoring on the default SIP ports. Or, the needs of your network may require that you monitor multiple SIP ports for load balancing, for example.

You can change port number in the vcAgentCurrentState.txt file.

Follow these steps:

1. Open a command-prompt window on the collector server that monitors the SIP ports.
2. Stop the CA UCM Collector Communication service.
   
   net stop “CA UCM Collector”
   
   **Important:** Stop the service before changing the vcAgentCurrentState.txt file. Otherwise, your changes may be overwritten because the collector saves configuration settings to the .txt file when it stops.
3. After the service stops, navigate to the following location:
   
   install directory\voipmonitor\bin
4. Open the vcAgentCurrentState.txt file in a text editor such as Notepad.
5. In the .txt file, search for text "SIP port=" as shown below. Ports 5060 and 5061 are monitored by default:

   Changed directives=0x7f009fbe
   Show summary dialog=0
   Save interval=1
   ...
   ...
   SCCP port=2000
   MGCP port=2427
   Q931 port=2428
   H225 port=1720
   **SIP port=5060;5061**
   TPKT capture=1

6. Add or remove port numbers on the **SIP port=** line. Separate port numbers with a semi-colon, but no space. For example:

   - To add port 5066: **SIP port=5060;5061;5066**
   - To remove port 5061: **SIP port=5060**

   **Important:** The **SIP port=** line can contain no more than 5 port numbers.

7. Save and close the text file.

8. In the command-prompt window, start the CA UCM Collector Communication service:

   net start “CA UCM Collector”

9. **(Optional)** To verify your changes, open the voipagent log in the **install directory\voipmonitor\logs directory**.

   Log entries similar to the following indicate that your changes were successful.

Index

A
architecture • 12
authenticated SIP traffic, monitoring • 21

B
billing application server parameters • 17

C
call diagnostics enabled flag • 19
call stats setting • 18
CDR enabled flag • 19
Cisco environments
  architecture • 12
  CDRs & CMRs • 7, 19
  FTP configuration • 17
  scalability • 12
  SIP ports • 21
  SIP profile • 18
  SPAN port configuration • 7, 15
  web server • 19

F
FTP configuration • 17

M
metric collection, enabling • 19

R
RTCP parameter • 19

S
scalability • 12
SIP ports, adding or removing • 21
SPAN ports, configuring • 15
supported CUCM versions • 10

W
web access parameter • 19