



CA NetQoS® Unified Communications Monitor

Version: 3.1

December 2010

These release notes provide information about known issues and product support for CA NetQoS Unified Communications Monitor (“UC Monitor”) version 3.1. This information supplements and, where applicable, supersedes information listed in the documentation. See “Product Documentation” on page 21.

These release notes provide the following information:

Topic	Page
“CA NetQoS Unified Communications Monitor Product Overview”	2
“What’s New?”	3
“Hardware and Software Specifications”	4
“Supported Hardware”	8
“Open Issues and Workarounds”	13
“Product Support”	20

CA NetQoS Unified Communications Monitor Product Overview

Unified Communications Monitor provides unified communications performance monitoring for enterprise networks. It tracks and measures VoIP and video call performance from one end of the network to the other without using desktop or server agents.

Unified Communications Monitor consists of two major software and hardware components: the **Collector** and the **Management Console**. The Collector monitors:

- Cisco IP telephony deployments that use a **Cisco Unified Communications Manager** for call processing.
- Avaya UC deployments that use the **Avaya Communication Manager** (including Avaya Aura).

Unified Communications Monitor also monitors unified communications in the **Microsoft Office Communications Server** 2007 and later environment. To monitor the Microsoft Office Communications Server, you must configure a Microsoft server to send call quality reports to the UC Monitor Management Console. The Microsoft server essentially becomes a UC Monitor collection device.

Product Components

CA Unified Communications Monitor version 3.1 includes the product components listed in the following table. The version numbers for the product components are important when checking for hotfixes and advisories on the CA Support Online Web site, as explained in “[Product Support](#)” on page 20.

Product Component	Version
Collector	3.1
Management Console	3.1

Upgrades from versions 2.1 and 3.0 of Unified Communications Monitor are supported. To upgrade from a version that predates version 2.1 of Unified Communications Monitor, first upgrade to version 2.1, and then upgrade to the present version.

More information about upgrades is provided in the “Installation” chapter of the *CA NetQoS Unified Communications Monitor Administrator Guide*.

Integration with the NetQoS Performance Center

NetQoS Performance Center versions 5.0 and later provide full integration with Unified Communications Monitor. Once the two products have been synchronized, you can perform administrative tasks for user accounts and roles in the NetQoS Performance Center interface and centralize these tasks for all NetQoS data source products, such as NetQoS ReporterAnalyzer and NetQoS NetVoyant.

NetQoS Performance Center version 6.0 or later and Unified Communications Monitor version 3.1 or later are required to support monitoring multiple domains.

The following table summarizes version compatibility for the two products:

Product	UC Monitor Version Compatibility
NetQoS Performance Center version 4.0	VoIP Monitor versions 1.2 and later Grouping support provided with 1.3 and later “VoIP” naming conventions used with version 2.0
NetQoS Performance Center version 4.1	VoIP Monitor versions 1.2 and later Grouping support provided with 1.3 and later “VoIP” naming conventions used with version 2.0
NetQoS Performance Center version 5.0	UC Monitor version 2.0 and later only
NetQoS Event Manager version 1.1 and later	UC Monitor version 2.1 and later NetQoS Performance Center v5.1 and later
NetQoS Performance Center version 5.1	UC Monitor version 2.0 and later
NetQoS Performance Center version 6.0 and later	UC Monitor version 3.0 and later

What's New?

This is the seventh release of the CA NetQoS Unified Communications Monitor product. The previous version (3.0) was released in March 2010. Future releases and enhancements are planned.

Version 3.1 of Unified Communications Monitor adds the following new features:

- Significantly **finer granularity** of metric data reporting. The 15-minute reporting interval of previous releases has been reduced to **five minutes** for all call setup and call quality metrics.
- New **Trunk Group reports** for Avaya environments. These reports provide volume and usage data needed for capacity planning with Avaya voice gateways.

-
- **Utilization reporting** for Avaya voice gateways.
 - Ability to report on multiple servers with overlapping IP addresses as separate **domains**.
 - Support for monitoring **Cisco Unified Communication Manager versions 7.1.3 and 8.0**.
 - **New, higher-performing server platform.** The UC Monitor Management Console or Standalone server and the Collector now run on 64-bit Microsoft Windows 2008.
 - Six **new data views** available in the CA NetQoS Performance Center to provide a top-*N* perspective on Location and individual phone performance.

What's Changed in this Release?

Be aware of the following changes to the product if you are upgrading from a previous version:

- New procedure for enabling automatic database backup operations. When you upgrade the UC Monitor software from a previous version, the former backup procedure still runs. However, the preferred method for performing backups is to download the CA NetQoS Database Tools Suite from CA Support Online. Do a search on <http://support.ca.com/> for the CA NetQoS Support Tools page.
- New Navigation links for the new Trunk Group reports. Find them under the **Capacity Planning > Trunk Group** link.
- Two different reporting intervals now in use. Call setup and call quality metrics are collected and reported at five-minute intervals. But call server metrics are still being reported at 15-minute intervals. As a result, while Call Performance Incidents are reported as frequently as every five minutes, all other Incidents (such as Call Server or Collector Incidents) are only reported every 15 minutes.

Hardware and Software Specifications

The UC Monitor hardware components are delivered to you with the required software already installed. This is true whether the solution delivered is a single standalone server or multiple servers.

Note: To learn more about the UC Monitor components and how they work together, see the introductory chapter of the *UC Monitor User Guide*.

A **Standalone** system can be used to monitor either single-vendor or smaller-scale hybrid deployments. It consists of a single server installed with all the software components listed in the following table:

Hardware System

Software Component

A server running Windows Server 2008 R2 (64-bit).

Intel Xeon dual-core processor (2.66 GHz, 1333 MHz FSB), 2 GB RAM, and six 73-GB SAS hard drives (RAID 5).

12 GB of hard disk space on the C: drive and at least 300 GB of hard disk space on the D: drive.

Intel Copper GB NIC, or Intel Fiber GB NIC.

UC Monitor Management Console

Collector

MySQL database

On some systems, a HASP device in a USB port provides product licensing.

A Standalone system is recommended for Microsoft environments. See “[Monitoring Microsoft Office Communications Server 2007 and Later](#)” on page 7 for more information about required components for monitoring Microsoft Office Communications Server 2007.

In a **Distributed** system, the Collector component is installed on a separate server from the Management Console and database components. Distributed systems are recommended for larger VoIP deployments, either Cisco-only, Avaya-only, or hybrid environments. A Distributed architecture is also available for smaller deployments of 1,000 phones or fewer if you purchase a special Small-Site Collector, which is described in a separate table below. The key point to remember is that the Collector component in a Distributed system is only needed for monitoring Cisco or Avaya deployments.

A typical **Distributed** configuration is shown in the following table:

Software Component

Hardware System

UC Monitor Management Console
MySQL database

A server running Windows Server 2008 R2 (64-bit).

Intel Xeon dual-core processor (2.66GHz, 1333MHz FSB), 2 GB RAM, and six 73-GB SAS hard drives (RAID 5).

12 GB of hard disk space on the C: drive and at least 300 GB of hard disk space on the D: drive.

Intel Copper GB NIC, or Intel Fiber GB NIC.

Supports up to 10 Collectors.

Collector

A server running Windows Server 2008 R2 (64-bit).

Intel Xeon dual-core processor (2.66GHz, 1333MHz FSB), 2 GB RAM, two 73-GB SAS hard drives (RAID 1).

Intel Copper GB NIC, or Intel Fiber GB NIC.

Supports up to 25,000 BHCA (Cisco) or up to 45,000 (Avaya).

In a **small-site deployment**, the Collector component is slightly different from a standard UC Monitor system. Small-site deployments are always in the distributed configuration and only monitor Cisco deployments. The Small-Site Collector has the following characteristics:

Software Component	Hardware System
Small-Site Collector	A server running Windows Server 2008 R2 (64-bit). Intel Xeon dual-core processor (2.66GHz, 1333MHz FSB), 2 GB RAM, and a SATA II 3.5" hard drive. Intel Copper GB NIC, or Intel Fiber GB NIC. Supports up to 1000 phones.

Monitoring Cisco Unified Communications Manager

When monitoring in a Cisco-only or hybrid environment, the standard NetQoS Collector (usually called “the Collector”) is deployed along with a Management Console. Both components can be running on a single server (the Standalone configuration). The following table describes the basic setup required for Cisco monitoring:

UC Monitor Component	Description
UC Monitor Management Console	Device (hardware and software) that processes, stores, and reports on VoIP-related network data. Includes a database component and a Web interface. Hardware is described above, in “Hardware and Software Specifications.”
Collector	Device that monitors VoIP network traffic in Cisco IP telephony environments. Performs the following functions: <ul style="list-style-type: none">• Passively collects VoIP-related performance data from a SPAN port on a core switch.• Collects UC-related performance data via active polling of phones during calls.• Aggregates and sends data to the Management Console for reporting.

The main installation chapter of the *UC Monitor Administrator Guide* explains the basic steps for deploying Unified Communications Monitor in a Cisco environment.

Monitoring Microsoft Office Communications Server 2007 and Later

When monitoring in a Microsoft-only environment, a standalone appliance from CA provides all the necessary UC Monitor components. During Management Console configuration, the Collector component is disabled. You must then configure a Microsoft server as a collection device by adding an OCS Collector. The following table describes the setup required for Microsoft:

UC Monitor Component	Description
UC Monitor Management Console	Device (hardware and software) that processes, stores, and reports on VoIP-related network data. Includes a database component and a Web interface. Hardware for the Standalone system is described above, in “ Hardware and Software Specifications .”
OCS Collector	A Microsoft server, configured to send call-quality reports to the UC Monitor Web service. <ul style="list-style-type: none">• For Office Communications Server 2007, the Microsoft Quality of Experience Monitoring Server, or QoE Monitoring Server.• For OCS R2, the Front-End server(s). Supports up to 40,000 endpoints if extra licenses are purchased.

The *UC Monitor Administrator Guide* contains a separate installation chapter that explains the requirements for deploying Unified Communications Monitor in a Microsoft Office Communications Server 2007 environment.

Monitoring Avaya Communication Manager

When monitoring in an Avaya-only or multi-vendor environment, a Standalone appliance from CA provides all the necessary UC Monitor components. The following table describes the setup required for Avaya:

UC Monitor Component	Description
UC Monitor Management Console	Device (hardware and software) that processes, stores, and reports on UC-related network data. Includes a database component and a Web interface. Hardware for the Standalone system is described above, in “ Hardware and Software Specifications .”

UC Monitor Component

Description

Collector

Device (hardware and software) that monitors UC-related network traffic. Performs the following functions:

- Receives and processes RTCP packets containing call-quality information.
 - Collects UC-related performance data reported by phones during calls.
 - Polls call servers for endpoint information using SNMP.
 - Sends the data to the Management Console.
-

The *UC Monitor Administrator Guide* contains a separate installation chapter that explains the requirements for deploying Unified Communications Monitor in an Avaya UC environment, and it also discusses bandwidth consumption under various usage scenarios.

Browser Support

You can access the UC Monitor user interface (the Management Console) using either:

- Microsoft Internet Explorer version 7, or
- Microsoft Internet Explorer version 8

Important: Microsoft Internet Explorer version 6 is no longer supported. If you are running this version of the browser, you must upgrade to a more recent version.

You may be able to view all reports and configuration information using recent versions of other browsers, but CA has not tested with them.

Supported Hardware

The following topics provide the most recent information available about the UC components that can be monitored with Unified Communications Monitor 3.1. All systems listed in these sections have been tested by the CA Quality Assurance team, unless otherwise noted. Cisco, Microsoft, and Avaya hardware devices are discussed separately.

Cisco Call Server Support

The Cisco Unified Communications Manager (CUCM; also called Cisco Unified CallManager) architecture enables a group, or cluster, of physical call servers to work together as a single IP PBX system. In some environments, a cluster of call servers may be distributed across an IP network to create redundancy and provide for resilience in failover situations. UC Monitor supports more traditional and distributed CUCM clusters.

The Collector supports Cisco Unified Communications Manager (CallManager) versions **4.2** through **8.0**. Earlier versions of CallManager are not supported due to limitations in their ability to collect call quality metrics. Version 3.1 of Unified Communications Monitor is required to support CUCM v7.1.3 and 8.0.

The Session Initiation Protocol (SIP) is monitored in environments where CUCM versions 5.0 and later are running. See “[SIP Limitations](#)” on page 20 for more information about SIP support.

Cisco Voice Gateway Support

The present release provides full support for voice (also called VoIP, or media) gateways from Cisco Systems with T1/E1-PRI connections. The H.323 and MGCP protocols are supported, as are SIP trunks to voice gateways.

Analog-type gateways are supported on a limited basis:

- Voice gateways that make an FXO connection are monitored for call performance data.
- Calls placed through an FXO connection are *only* monitored by the Call Watch feature if the H.323 protocol is used.

Cisco ATA 186 Analog Telephone Adapters are partially supported. Only call setup metrics are available. No call quality or Call Watch metrics can be collected from these devices. In addition, the Cisco VG-224 is supported. This type of gateway allows up to 24 analog phones to connect to an IP PBX (in this case, a Cisco Unified Communications Manager). All connected phones use the same IP address with different port numbers. If you are using a VG-224, the UC Monitor Administrator needs to add it as a new Voice Gateway definition to allow for correct reporting on the calls it handles. But be aware that the connected analog phones may generate additional abandoned call legs in UC Monitor reports if the handsets are not placed on hook correctly.

Gateways that make a T1-CAS connection are not supported. Cisco CUBE is not supported.

The Catalyst 6000 WS-X6608-T1/E1 Blade for Voice has some limitations due to a lack of SNMP support: Call Watch is not supported, and only limited call quality statistics are returned for performance reports.

CA Quality Assurance has tested with Cisco gateways of the indicated types using all the major call setup protocols (SIP, H.323, and MGCP).

Cisco IP Phone Support

Unified Communications Monitor supports the following Cisco IP phones:

- CP-6900 Series models
- CP-7900 Series models
- CP-8900 Series models
- CP-9900 Series models

As a best practice, update phone firmware as new releases become available.

As of firmware 9.0.2.0, Cisco 6900 Series phones do not provide enhanced call quality metrics. Future firmware releases may resolve this problem. As a result of this limitation, Unified Communications Monitor reports call volume statistics only, with a few exceptions, on these phones.

The following Cisco wireless phone models are also supported:

- CP-7920 (call performance monitoring only; no Call Watch)
- CP-7921

The Cisco IP Communicator, a soft phone, is supported, but it provides few metrics and does not support the Call Watch feature. Similarly, the Cisco Unified Personal Communicator version 7.0 is supported on a limited basis. Calls made to and from this client are included in call volume metrics, along with basic information about when the call was made, and call setup failures are reported.

The section titled “[SIP Limitations](#)” on page 20 details specific limitations on monitoring phones in environments where the SIP protocol is used for call setup.

In addition to English (U.S. and U.K.), the following phone localization settings are supported:

- German
- Danish
- Dutch
- Italian

-
- French
 - Spanish
 - Japanese

Other localization settings may be supported, but they have not been tested.

Microsoft Call Server Support

In a Microsoft UC deployment, the Microsoft Office Communications Server is used for call processing. A PBX to allow call routing to and from the PSTN is optional in a Microsoft UC environment; deployments with and without a PBX are supported.

Unless you are running Office Communications Server 2007 R2, a Quality of Experience Monitoring Server must be installed and running. Because this server sends quality reports to the UC Monitor Management Console, it is configured as a UC Monitor collection device (an OCS Collector) and monitored as a call server.

In OCS R2, the Front-End servers are used as UC Monitor collection devices and monitored as call servers. See the separate Microsoft installation chapter of the *UC Monitor Administrator Guide* for more information.

Microsoft Voice Gateway Support

Mediation Servers provide connectivity outside the Microsoft Office Communications Server environment and allow calls to and from the PSTN by means of a gateway connection. The Mediation Servers themselves are monitored by Unified Communications Monitor, but any gateways connected to them are not.

In a given Office Communications Server 2007 deployment, several media server roles may perform voice gateway functions and may be monitored as voice gateways. For example, a “hybrid” Mediation Server usually contains an interface directly to the PSTN, where other Mediation Servers are mainly transcoders between IP networks and have no communication with the PSTN.

Most media servers in an Office Communications Server environment can be monitored for call quality statistics. However, they are treated differently than the voice gateway devices in a Cisco deployment. The Collector can query Cisco voice gateways using SNMP to get performance data about call legs that terminate at a gateway, and by default, it also performs regular traceroute testing of these devices, reporting information about network paths in the Investigations Report.

By contrast, in the Microsoft secure environment, SNMP polling of media devices cannot be performed, nor is traceroute testing performed. But these devices do contribute to the call performance statistics shown in UC Monitor reports. Therefore, they are included in reports, listed in the Phone Details report, and displayed in a read-only list view in the Administration area of the UC Monitor Management Console.

Supported Microsoft Endpoints and Phones

For Microsoft, the following endpoints and phones send quality reports and are supported for quality monitoring, call volume, and other metrics:

- Office Communicator 2007 and R2
- Office Communicator 2007 and R2 Phone Edition
- Messenger for Mac 7
- Office Communications Server A/V MCU (Conferencing Server)
- Office Communications Server Mediation Server

Servers and endpoints that do not send quality reports are not monitored. In general, the phones and devices listed at the following link are supported:

<http://technet.microsoft.com/en-us/office/ocs/bb970310.aspx>

The following lists summarize the equipment NetQoS has tested:

Hard phones and USB Devices:

- Polycom CX100, CX200, and CX700
- LG Nortel IP8540 and IP8501

Servers and server endpoints that do not send quality reports:

- Office Communications Server Edge Server (Media Relay)
- Exchange 2007 Unified Messaging Server (including SP1)

Webcams:

- Microsoft LifeCam NX-3000 and NX-6000
- Microsoft LifeCam VX-5500 and VX-7000

Other USB handsets, USB speakerphones, Webcams, microphones, and sound cards supported by the tested Office Communications Server client endpoints should also work but have not been tested.

Avaya Hardware Support

The following list summarizes monitoring support for Avaya UC hardware:

- Avaya Communication Manager versions 3, 4, and 5.x; Avaya Aura Communication Manager 5.2 and later.
Call data record (CDR) collection must be enabled and set to send CDRs to the IP address of the UC Monitor Collector.
- All Avaya phones that send RTCP data to report call quality. Specifically:
 - Avaya 1600 Series (call center phones)
 - Avaya 4600 Series (basic desktop [hard] phone)
 - Avaya 9600 Series (business desktop phone [SIP or H.323])The only known phones at this time that do not support call-quality reporting via RTCP are Avaya digital phones and the Avaya one-X SIP softphone.
- All Avaya voice gateways that send call-quality reports using RTCP.

Open Issues and Workarounds

This section describes known issues and suggested workarounds. See also “[Monitoring Limitations](#)” on page 18.

Issue	Description and Workaround
24396: UCM Dashboard times out for week+ time period with 10-million call UCM DB bound to it	<p>The Unified Communications Dashboard report page in the CA NetQoS Performance Center times out without fully rendering the views if the UC Monitor database contains at least 10 million calls and a one-week or longer timeframe is selected.</p> <p>To work around this issue, the Administrator should split some of the UC Monitor data views into two custom NetQoS Performance Center reports. For example, the first custom report could be named “Performance” and would include the Worst Locations and Worst Phones views. The second could be named “Volume” and could contain the rest of the views associated with the Capacity Planning reports (that is, the “Volume,” Trunk Group, and Interface views). With fewer views, the Dashboard report successfully renders.</p>

Issue

23638: Voice Interfaces and Call Watch menus don't appear after server/gateway discovery

Description and Workaround

We've found a few cases where two of the Navigation links do not appear after a Cisco call server is discovered:

- Troubleshooting section: **Call Watch** link
- Capacity Planning section: **Voice Interfaces** link

To work around this problem, log out of the UC Monitor Management Console, and then log back in. If the menu items still do not appear, edit and save the role associated with the current user account, making no changes to it. For example, the default role for the Administrator account is Network Manager. The menu items should appear the next time the page is refreshed.

21574: Investigate initial setup workflow for Avaya - problem viewing Call Watch

If you are receiving RTCP call data from Avaya endpoints and do not see the navigation link to the Call Watch report (that is, **Troubleshooting > Call Watch**), ask the Administrator to edit the role associated with your user account (for example, Network Manager) and verify that the Call Watch check box is enabled to allow access to on-demand Call Watch. If it is, save the role anyway. Once the Administrator saves the role, you should be able to log back in with that account and see the Navigation link.

22230: Results from manual traceroutes shown multiple times in the Investigations List

After running a manual traceroute to a device, the result is shown multiple times in the Investigations report, with the same ID number.

22183: Initial add of Avaya-only Collector does not read Collector information: version, license, etc.

When you add an Avaya-only Collector, a few identifying items are not displayed immediately, such as the Collector version and available license values in the License Administration section. The workaround is simply to reload the Collector.

20574: Automatically adjust the timeframe for Call Watch Details when the call is < 15 minutes.

For large Call Watch volumes (that is, heavy-traffic Avaya environments), disable the auto-refresh option on the Call Watch Overview page, and change the timeframe to 15 minutes. Otherwise, reports can time out or enter an auto-refresh loop.

Unfortunately, you will have to do this for each separate login session.

Defect 21921: NPC Performance by Group report error: Invalid usage of aggregate function Sum()

On the Unified Communications Dashboard page in NetQoS Performance Center version 5.1 and earlier, the Call Performance by Group view is not supported. Once version 6.0 of the NetQoS Performance Center becomes available, upgrade to that version to resolve this issue. Or access this same data view exclusively from the UC Monitor Management Console.

Issue

Description and Workaround

Defect 20954: Max jitter < avg jitter for gateway calls

For calls that passed through an Avaya voice gateways, we have seen during lab testing that the max jitter values reported in the Call Watch Details report were lower than the avg jitter values reported. After some investigation, we have reported this issue to Avaya.

Defect 9753: Incident acknowledgement; Severity/Type changes; After incident acknowledged, entire incident is acknowledged

It's possible to acknowledge an Incident for a degraded performance condition and not be aware that the performance condition has deteriorated further. A degraded Incident can change to Excessive status while still appearing as acknowledged in reports.

As a workaround, configure an SNMP trap Incident response notification with Severity Updates enabled. The SNMP trap can notify you anytime an Incident's severity status changes.

Defect 9459: Call Watch: packet loss metric off by a factor of 10 from the CMR.

Depending on the type of Cisco IP phone being monitored, you may see a difference between the data shown in the Call Watch detailed report view and the data shown in the Call Performance Overview Metric Details Report. During testing with a consistent impairment tool, we found that the Cisco IP phone model 7940 can misreport packet loss as jitter buffer loss.

If you think you are seeing a discrepancy in data similar to this, use the data reported in the Call Watch detailed report instead of that shown in the Call Performance Overview Metric Details report; the former was more accurate in our testing.

Defect 10056: Call Watch: still seeing the Loss Packet drop and the JBL spike

This issue is related to Defect 9459.

With the Cisco IP phone model 7940, our testing found that the phone may periodically report a spike in jitter buffer loss.

When we tested with a constant source of packet loss on the network, the 7940 phone reported a packet loss metric of 0 for a brief period, with a simultaneous spike in jitter buffer loss almost equal to the previous packet loss percentage. Then the metrics returned to expected values.

Defect 16995: Jitter buffer loss: how to handle high concealment ratios when no packets received (silence suppression)

In our testing, we have occasionally observed some abnormally high values for jitter buffer loss. We determined that the spike in values occurs when there is a mismatch in voice activity detection (VAD) settings between the call server and the gateway. During periods of silence in the conversation, the phone may interpret 0 packets received as 100% concealment, which is then factored into the jitter buffer loss totals.

Issue	Description and Workaround
Defect 9855: Call Performance views—don't refresh screen every 60 seconds.	<p>The default setting in report views is to auto-refresh the browser window every 60 seconds so that any new collected data is reflected in the charts. The refresh may be burdensome because it also scrolls the page back to the top.</p> <p>A change to the code to make the auto-refresh occur less frequently may be implemented in a future release of UC Monitor. Until then, you can work around this problem by disabling auto-refresh; click the page menu on the report page (the orange arrow labeled OPTIONS). You should then press F5 to refresh the page every few minutes.</p>
Defect 9106: Call Watch Details--10-second call shows MOS value but no other metrics	<p>If a monitored call was too short to contain enough data for every call quality metric category, the call may appear in detailed reports with a MOS value but no other metrics. As a workaround, do not try to analyze data samples taken from calls with a duration of less than 30 seconds.</p>
Defect 12608: Bogus latency values reported by Call Watch for some phones	<p>During a Call Watch, latency values unexpectedly rise when certain phone models are being monitored. Latency values on these phones stay low for the first few minutes of a call, but then increase into the 50000 - 60000 ms range. Meanwhile, the MOS and all the other metrics indicate no problem. We have observed this issue with the Cisco CP-7941G phone with firmware version SIP41.8-3-1S, running with SIP and also running with SCCP. We saw it very consistently with IP Communicator versions earlier than version 7.0. An upgrade to IPC 7.0 should resolve the issue.</p> <p>The extent of this problem is not fully known. If you think you are observing it, contact NetQoS Support.</p>
Defect 15219: Call correlation problem when successive calls use same RTP port	<p>The Cisco Unified Personal Communicator sometimes uses the same RTP port for calls. As a result, if successive gateway calls are made to or from the same CUPC within 15 minutes, Unified Communications Monitor may not be able to correlate the call quality statistics correctly.</p>
Defects 15758; 15757; 15759: Codec identification	<p>Not all Microsoft endpoints that are able to send end-of-call quality reports identify the payload for the inbound call stream. For calls made with those endpoints, Unified Communications Monitor can only identify the codec for an inbound stream if one of the two conversing parties reports the necessary payload information.</p>

Scalability Limitations

In a Cisco environment, Unified Communications Monitor 3.1 can support call volumes of up to **10 million calls per month**, across **100** configured Locations and voice gateways.

The maximum Avaya call volume that can be processed by a single Management Console without performance impact is **2500-3000 simultaneous calls**, or roughly 45,000 calls/hour. Both the number of phones and the number of Collectors are irrelevant.

At these levels of usage, you might encounter some minor limitations due to database size:

- Upgrading the database from a previous version will take between 30 minutes and one hour.
- Call Performance Overview reports: long delays might occur when you are viewing one week of data. Disable the auto-refresh feature if you need to view this report.
- The Worst Phones report experiences poor performance when the number of calls in the database reaches about 10 million. The performance of this report does not depend on the total number of phones in the database, but rather, the number of *calls*. With about 5 million calls in the database, the report consistently loads in about 30 seconds, regardless of the time period selected. By contrast, with 10 million calls in the database, the report consistently takes over a minute to load.
- Selected reports with a week-long time period of data selected can take several minutes to display. The Call Performance Overview Report takes the longest: in our testing, it took as long as four minutes to completely display. The Call Leg Details can take some time as well: four to five minutes, in our testing. Call Leg Details reports for a full week's worth of data are only supported for Location-to-Location drilldown. The Call Details Export feature provides a good workaround.
- Reports based on a full day of data usually complete and display within 60 seconds. However, long delays might occur if you try to view the Call Leg Details Report with a one-day time period of data selected. Disable the auto-refresh feature if you need to view this report.
- The Unified Communications Dashboard Report, viewed in the NetQoS Performance Center: long delays might occur when you are viewing one week to 30 days of data.

The time it takes to create a new call quality threshold assignment is based on the total number of Location and voice gateway definitions in your system. If you have as many as 100 Locations and/or voice gateways defined, the Call Quality Threshold Assignment Properties page may take a few minutes to load.

Following are some more recommendations for dealing with large UC Monitor deployments:

- In our testing, we found that browser versions more recent than Microsoft Internet Explorer 7.0 perform better. For example, when we tested with Internet Explorer 8.0, Mozilla Firefox 3.0, and

Google Chrome 3.0, the Call Quality Threshold Assignment Properties page loaded in less than 3 seconds.

- Reports based on three-hour time periods of data generate reasonably fast, even with a very large database size.
- We recommend generating reports with a one-day time period if you find that reports based on a full week of data are taking too much time to generate.
- Pruning older data will keep the database at a manageable size and improve report generation.

Monitoring Limitations

This release of the UC Monitor product only supports UC systems that use:

- Cisco Unified Communications Manager versions 4.2 and later,
- Microsoft Office Communications Server 2007 and R2, or
- Avaya Communication Manager (including Aura Communication Manager)

Subsequent releases may support VoIP and video deployments from other vendors. Your NetQoS Sales representative can keep you up to date on the supported systems.

In environments where Cisco Unified Communications Manager (CallManager) servers earlier than version 5.1 are running, latency values may not be provided under certain circumstances. CA Support personnel can discuss this limitation with you. Version 5.0 or later of CallManager is required for SIP support.

For calls lasting < 10 seconds, the UC Monitor software reports whatever data is available. Cisco IP phones calculate MOS in 8-second intervals. Therefore, if a call lasted < 8 seconds, a MOS value would not be reported. However, call setup metrics would be available (delay to dial tone, post-dial delay), as would all the other quality statistics: lost packets, latency, and jitter buffer loss.

Because this issue stems from Cisco IP phone behavior, it does not apply to voice gateway call legs. Regardless of the duration of the call, the UC Monitor software reports all the metrics for these call legs.

During a Call Watch, a call that lasted < 8 seconds would most likely not produce any call quality information. The Collector would only collect call setup information and some information about the phone.

The Grade of Service metric shown in Capacity Planning reports is only calculated for Cisco voice interfaces and trunk groups when the interfaces are using MGCP. (This limitation does not apply to Avaya trunk groups, where the Grade of Service is calculated based on outbound call failures and

total call attempts.) On interfaces using H.323 or SIP, the Grade of Service metric does not apply to voice interfaces. Unified Communications Monitor cannot identify the interface for gateway call setup failures, so failures can only be shown in the Call Volume GoS chart.

For calls that involve a Media Termination Point (MTP), Unified Communications Monitor may not be able to correlate the call legs accurately. In these cases, a single call may show up as two calls. An example scenario would include outbound PSTN calls that use H.323 FastStart. These calls require an MTP, which receives data flows that would otherwise be exchanged directly between the phone and its gateway if no MTP were in use. Instead of correctly correlating data from the call legs traveling between the phone and the MTP, or between the gateway and the MTP in the opposite direction, Unified Communications Monitor reports two distinct calls in the Call Watch Overview Report and in the spreadsheet created during Calls Export.

Requirements for SIP Support

To take advantage of Unified Communications Monitor support for monitoring phones in environments where the Session Initiation Protocol (SIP) is being used for call setup, you must take a few steps to configure phones and call servers in a Cisco environment.

Note: These steps are not required if you are only monitoring Microsoft Office Communications Server 2007 or Avaya.

By default, SIP phones do not return quality metrics. The SIP Profile in Cisco Unified CallManager Administration contains a setting to enable “Call Stats.” You can either edit the Standard SIP Profile or create a new, voice-quality-enabled Profile.

To access the SIP Profile, click **Device Settings** on the Device menu, and select **SIP Profile**. In the profile, click to select the **Call Stats** check box. This setting enables voice quality statistics for each call.

You will then need to select the new or edited profile for your IP phones. On the Phone Configuration page, scroll down to the Protocol Specific Information section. Then select the voice-quality-enabled SIP Profile from the **SIP Profile** list.

SIP Limitations

In Cisco SIP environments, a few additional limitations apply:

- Monitoring of SIP call setup statistics is only supported on Communications Manager versions 5.0 and later.
- The following Cisco IP phone models are supported when running in “Basic SIP” mode: CP-7905G/7912G, CP-7940G/7960G. This support is limited; no MOS value, concealed seconds, post-dial delay, or delay to dial tone metrics are available. Neither Call Watch nor baseline traceroutes can be performed on phones running in “Basic SIP” mode.
- The following Cisco IP phone models are supported when running in “Advanced SIP” mode: CP-7906G/7911G, CP-7941G/7961G, CP-7970G/7971G. These phones are fully supported. However, if a call is put on hold (suspend/resume), metrics returned from these phones have the following limitation: the call quality metrics only represent the last portion of the call since it was resumed. Because the duration in the call record spans the entire call, the metrics are then weighted too heavily across the call duration. For example, the call quality metrics may only represent the last 10 seconds of a long phone call.
- Only voice gateway call legs are monitored; call legs routed by similar devices that act as SIP trunks or SIP proxies are not supported. The gateway call legs that run between the call servers and a managed gateway over a SIP trunk are monitored.

The distinction concerns whether the device routes calls to and from the PSTN (supported) or whether it routes sessions to other network domains, such as to another call server cluster, and does not perform protocol translation (not supported). If an ISP manages the device, the call legs that travel to it are not monitored.
- If a call leg terminates at a SIP trunk that is acting as a proxy (that is, the trunk disassociates itself from the call as soon as the connection is established), that call leg cannot be monitored, nor can the disconnect be detected. Such call legs are discarded by the Collector.

Product Support

CA provides a broad range of customer support and product documentation for Unified Communications Monitor. For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products.

At <https://support.ca.com/>, you can access the following:

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

You are instructed how to create a CA user account the first time you access the site. You can use this account to access the Knowledge Base, product advisories, and updates. We recommend regularly checking the Support by Product section for applicable updates and fixes.

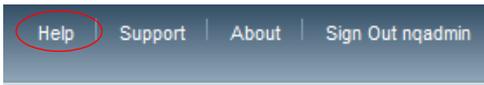
Product Documentation

The following documents support the product:

- *CA NetQoS Unified Communications Monitor Administrator Guide*
- *CA NetQoS Unified Communications Monitor User Guide*
- Online Help

You can access the UC Monitor product documentation in any of the following ways:

- Click the **Help** link in the upper right corner of the UC Monitor user interface:



This link opens the UC Monitor online Help file.

Click this link at any point to see context-sensitive Help about the current product page.

- Navigate to the following directory on the UC Monitor Management Console:

D:\NETQOS\UCMonitor\WebSite\Docs

This directory contains copies of the UC Monitor *User Guide* and *Administrator Guide* in Adobe Acrobat PDF format.

- Log into the CA Support Online site at <http://support.ca.com/>. Under the **Main Menu** heading, click the **Product Info & Downloads** link. In the menu, click the **SuperAgent** link.

The **Documentation** section provides links to the most recent versions of the SuperAgent and Multi-Port Collector documentation in Adobe Acrobat PDF format.

Knowledge Base articles, white papers, and other documentation are also available here.

Customer Support

If you have problems with or questions about a NetQoS product, go to the CA Support Online site at <http://support.ca.com/>. We recommend visiting this site regularly to see product advisories and download hotfixes.

If you do not have access to the Web and you are in the United States or Canada, contact CA at (877) 225-5224.

Copyright 2007-2010, CA. All rights reserved.

NetQoS, the NetQoS Logo, SuperAgent, ReporterAnalyzer, NetVoyant, and Allocate are trademarks or registered trademarks of CA | NetQoS, Inc. Other product and company names mentioned herein may be the trademark or registered trademarks of their respective organizations.